תיק עיתונות

יחסי ציבור (ישראל): אייזנברג אליאש

SPONSORS & PARTNERS

Distinguished Benefactor

THE SAGOL NETWORK

Esteemed Platinum Sponsors

IAI Creating a Difference

YL VENTURES

Platinum Sponsors

Check Point SOFTWARE TECHNOLOGIES LTD.

IBM

PENTERA

Gold Sponsors

BigID

Checkmarx

CYBERARK

Cyberstar For a Secure World

ELRON

Microsoft

Synamedia

SYNOPSYS

snyk

Silver Sponsors

BioCatch

BOSCH Invented for life

COMSEC GLOBAL

Kramer Levin

Steven E. Stern

SYGNIA

THETARAY

Bronze Sponsors

CISCO

cybereason

FIREEYE | MANDIANT

LUXEMBOURG TRADE & INVEST

MITIGA

NTT Innovation Laboratory Israel

Connect easily with thanks to: Cellcom

Partners

HELMHOLTZ RESEARCH FOR GRAND CHALLENGES

Embassy of the Federal Republic of Germany Tel Aviv

CYB TOGETHER Israel Cyber Security Association

ISRAEL TECH POLICY INSTITUTE

FUTURE OF PRIVACY FORUM

CICC

המרכז לחינוך סייבר CYBER EDUCATION CENTER

SOSA

רשות החדשנות Israel Innovation Authority

ASHDOD PORT THE PORT OF ISRAEL

conexx

IATI Israel Advanced Technology Industries

JLCW

KONFIDAS YOUR BUSINESS, SECURED

JETRO

CSA cloud security alliance

DSI DIGITAL SOCIETY INSTITUTE

ESMT BERLIN

START-UP NATION CENTRAL

SOPHIC by Israel Electric

CII Confederation of Indian Industry

ISRAEL SWEDEN Cyber Connect

ABOUT-FRAUD

Or-Hof

IDPF Israeli Data Protection Professionals Forum

SAE INTERNATIONAL

TEL AVIV UNIVERSITY ALUMNI ORGANIZATION

BSIDES TLV 2021

UK Israel Tech HUB

HiTech Ambassadors

CYBERTLV

TEL AVIV UNIVERSITY THE YUVAL NE'EMAN

גלובס

מערכות חלל ולוויינים: החזית הבאה של עימותי הסייבר?

לאחרונה חלה עלייה באיומי הסייבר על מערכות חלל • הנושא הפך לבעל חשיבות קריטית לביטחונן הלאומי של מדינות • על ישראל לנצל את כוח-האדם האיכותי ואת האקוסיסטם שלה כדי לייצר ידע ויכולות שיטיבו עם תעשיית הלוויינים המקומית ובהמשך יופנו גם כלפי השוק העולמי

מאת:עמרי וקסלר

למרחב החלל חשיבות כלכלית וביטחונית עצומה כתשתית תקשורת גלובלית, ועבור שירותי ניווט, חיזוי מזג אוויר ועוד. תהליכי מסחור מואץ של טכנולוגיות החלל ועלייה בשימוש במוצרי מדף אזרחיים, זולים ונגישים טומנים בחובם גם האצה וצמיחה של סיכונים ואיומי סייבר. ישראל, שהובילה את תהליך הסטנדרטיזציה של הסייבר עבור המשק האזרחי, יכולה גם להוביל בתחום פתרונות הגנת הסייבר עבור לוויינים.

בשנים האחרונות אנו עדים להתרחבות משמעותית של תעשיית החלל הבינלאומית ולמהפכה טכנולוגית-מסחרית המכונה "החלל החדש". מהפכה זו התבססה על השקעות ממשלתיות בתחום החלל ובהתפתחויות טכנולוגיות בתחומי התקשורת, הקישוריות וייצור הלוויינים שהגדילו את הפוטנציאל הכלכלי של תעשיית החלל.

במקביל להתפתחויות אלו, חלה עלייה באיומי הסייבר על מערכות חלל והנושא הפך לבעל חשיבות קריטית לביטחונן הלאומי של מדינות, כמו גם לסדר החיים האזרחי התקין הנסמך על מערכות לוויין. במסגרת איומים אלו יכולים גורמים זדוניים לשבש שירותי לוויין, כגון תקשורת ואינטרנט ללקוחות, ליירט ולגנוב מידע השייך למשתמשים ואף להשתלט על לוויינים, להפנותם מהמסלול ואף להשתמש בהם לצורך ניגוח של לוויינים אחרים.

הארץ

כך תשמור ישראל על מעמדה כמעצמת סייבר

מחקר בינ"ל קבע לאחרונה, כי ישראל הפכה לאחת המדינות המובילות בעולם בתחום הסייבר. מי שעמד על ערש לידתו של מיזם הסייבר הלאומי מסביר איך הגענו לכך ומה עלינו לעשות כדי להמשיך ולהיות שחקנים מובילים בתחום זה

אלוף (מיל') פרופי יצחק בן ישראל | צילום: יחיא

אלוף (מיל) פרופי יצחק בן ישראל

משקלה הגלובלי של תעשיית הסייבר בארץ הוא יבוא רושם. לרבים זה נראה מבע. אבל הרושם הם תוצאה של אסטרטגיה מתוכננת מראש.

תוך כעשור הפכה ישראל לאחד ממרכזי הסייבר העולמיים, ובתחומים מסוימים עקפה אפילו את ארה"ב. ישראל היא המדינה היחידה בעולם שבה ניתן ללמוד סייבר כמקצוע לבגרות, אחת הבודדות בהן לניהול הגנת הסייבר יש נרבך לאומי, ומספר חברות הסייבר בה, החל מרמת הסטארט-אפ וכלה בחברי קרן וחברות שערכן למעלה ממיליארד דולר, הוא מהר תקדים.

המספרים מדברים בעד עצמם. כך למשל, בשנת 2020 עמד היצוא הישראלי בתחום הסייבר על 6.85 מיליארד דולר. לזה יש להוסיף גיוסים של 2.9 מיליארד דולר וכ-20 עסקות רכש גדולות בשווי של 4.7 מיליארד דולר. אלו מספרים משמעותיים המהווים כ-10%-5% מהשוק האזרחי העולמי. כאשר מביטים על מדינות היעד אליהן מופנה סך כל ההשקעות הגלובליות במגזר העסקי בסייבר, מתברר שכל שנה הולך ועולה שיעור ההשקעות המופנה לישראל; בשנת 2018 הוא הגיע ל-18% מההשקעות הגלובליות, בשנת 2019 הוא עלה ל-21%, ובשנת 2020 הופנו 31% מההשקעות העולמיות לישראל. במחצית הראשונה של 2021 המספר גדל עוד יותר והגיע ל-45%. בכך עקפה ישראל אפילו את ארה"ב יותר דולרים של המגזר העסקי הושקעו בסייבר בי ישראל מאשר בארה"ב.

ואין מדובר רק בסטארט-אפים או בחברות קטנות. מידי שנה הולך ועולה השווי של חברות הסייבר הישראליות. כך למשל, בשנת 2020 נוספו חמש חברות סייבר ישראליות לרשימת חדי הקרן בעולם, במחצית הראשונה של 2021 נוספו עוד שבע חברות ובכך הגיע שיעור חברות הדור קרן הישראליות ל-33% (שלישי) ממספרן בעולם.

כאשר משקללים את היכולות הללו והתובנות בכלכלה, עם נדרשים נוספים, כמו הפעלה לצרכי ביטחון, הספעה על העולם, מספר ורמת העסקים בנושא, מחקר אקדמי, רמת ההגנה המודיעינית וכדומה, ניתן לקבל הערכה על עוצמה כוללת בסייבר ניסיון רציני לשקלל הרכה משתנים כאלו, נעשה לאחרונה ע"י המכון הבין-לאומי למחקרים אסטרטגיים (the International Institute for Strategic Studies), שמצא שבשכבה הראשונה (מעצמות על) נמצאת מדינה אחת: ארה"ב; בשכבה השנייה (מדינות מובילות בעולם) נמצאו המדינות הבאות: אוסטרליה, קנדה, סין, צרפת, ישראל, רוסיה ובריטניה.

מערכת כלים שלובים

איך הגענו לכך? מה הוליך אותנו להובלה עו

כך הפך שבוע הסייבר למוקד עלייה לרגל מכל העולם

חשוב להדגיש, כי כל הנערים שהוזכרו במאמר, הראשים טובעים ומתבקשים כמעט מאליהם, נעשו רק על-ידי מספר מצומצם של מדינות, שניתן למנותן על אצבעות יד אחת בלבד. זו הסיבה לכך שכנס שבוע הסייבר הנערך מדי שנה בקמפוס אוניברסיטת ת"א (https://cyberweek.tau.ac.il), הפך למוקד עלייה לרגל מכל העולם, וכשנים האחרונות השתתפו בו מדי שנה כמעט 10,000 איש שהגיעו מלמעלה מ-90 מדינות. הכנס יערך גם השנה (מחל ב-19 ביולי), למרות הקורונה.

לערת בסייבר?

יש לכך סיבות רבות שסורטנו בתרבות הסטארט-אפ בארץ (Start-up Nation), ועוד לפ ני כן בגודל הביטחוני של מדינה קטנה, המוקפת במדינות עוינות הנרדולות ממנה בהרבה, שהבינה כי אינה יכולה לעלות על אויביה בכמות ולכן עליה לעלות עליהם באיכות. והתרגום המעשי של אבות האומה לנרם "האיכות" היה שימת הנרום האנושי מתן, והשקעה נרולה במגזר הטכנולוגי מאידך. לא במקרה נוסדו האוניברסיטאות הראשונות בארץ (והטכניון והאוניברסיטה העברית בירושלים) כרבע מאה לפני שקמה המדינה.

אחת התוצאות של מדיניות זו היתה התבססות הולכת ונוברת של כלכלת המדינה על מה שק רוי בפינו "תעשיית ההיי-טק", כלומר זו העוסקת בעיקר בטכנולוגיות הקשורות למחשבים ותקשורת.

ללא משים נוצר מעין מעגל סגמים: ידע חדש נוצר באקדמיה, התעשייה נשענה על הידע הזה ופיתחה יכולות מתקדמות בעלות ערך מוסף נבוה, בהתאם לצרכי הביטחון תחילה והשוק העולמי בה׳ משך, מערכת הביטחון נהנתה מהידע והמיכולות שנוצרות, ובתורה תרמה כוח אדם מעולה, צרכים והבנה יחודיים שהזינו את האקדמיה ואת התע׳ שייה, וחוזר חלילה. באמצעות מעבר של אנשים מוכשרים ממערכת הביטחון לתעשייה ולאקדמיה, נוצרת מערכת כלים שלובים, שבה הידע עובר בין שלוש המערכות הללו (בשתן וממשלה, תעשייה ואקדמיה), מחקר מדעי ערכני על תרשנות מתאר את מידת השילוב בין שלוש המערכות הללו בנודם מכריע בתפוקות.

שיפה מערכת החרשנות לשנה פיתוח יכולות מובילות בעידן הנוכחי היה גם הרעיון המרכזי ברו"ח של מיזם הסייבר הלאומי, שהוגש על-ידי כותב שורות אלו לראש הממשלה במאי 2011 והסך להחלטת ממשלה באותה שנה.

הרו"ח כלל שזרה של המלצות על צעדים הנר נעים לא רק לטכנולוגיה, אלא גם לבניין היכולות של האקו-סיסטם בולו ; לשילוב בין התעשייה, לערת בסייבר?

יש לכך סיבות רבות שסורטנו בתרבות הסטארט-אפ בארץ (Start-up Nation), ועוד לפ ני כן בגודל הביטחוני של מדינה קטנה, המוקפת במדינות עוינות הנרדולות ממנה בהרבה, שהבינה כי אינה יכולה לעלות על אויביה בכמות ולכן עליה לעלות עליהם באיכות. והתרגום המעשי של אבות האומה לנרם "האיכות" היה שימת הנרום האנושי מתן, והשקעה נרולה במגזר הטכנולוגי מאידך. לא במקרה נוסדו האוניברסיטאות הראשונות בארץ (והטכניון והאוניברסיטה העברית בירושלים) כרבע מאה לפני שקמה המדינה.

אחת התוצאות של מדיניות זו היתה התבססות הולכת ונוברת של כלכלת המדינה על מה שק רוי בפינו "תעשיית ההיי-טק", כלומר זו העוסקת בעיקר בטכנולוגיות הקשורות למחשבים ותקשורת.

ללא משים נוצר מעין מעגל סגמים: ידע חדש נוצר באקדמיה, התעשייה נשענה על הידע הזה ופיתחה יכולות מתקדמות בעלות ערך מוסף נבוה,

בהתאם לצרכי הביטחון תחילה והשוק העולמי בה׳ משך, מערכת הביטחון נהנתה מהידע והמיכולות שנוצרות, ובתורה תרמה כוח אדם מעולה, צרכים והבנה יחודיים שהזינו את האקדמיה ואת התע׳ שייה, וחוזר חלילה. באמצעות מעבר של אנשים מוכשרים ממערכת הביטחון לתעשייה ולאקדמיה, נוצרת מערכת כלים שלובים, שבה הידע עובר בין שלוש המערכות הללו (בשתן וממשלה, תעשייה ואקדמיה), מחקר מדעי ערכני על תרשנות מתאר את מידת השילוב בין שלוש המערכות הללו כגודם מכריע בתפוקות.

שיפה מערכת החרשנות לשנה פיתוח יכולות מובילות בעידן הנוכחי היה גם הרעיון המרכזי ברו"ח של מיזם הסייבר הלאומי, שהוגש על-ידי כותב שורות אלו לראש הממשלה במאי 2011 והסך להחלטת ממשלה באותה שנה.

הרו"ח כלל שזרה של המלצות על צעדים הנר נעים לא רק לטכנולוגיה, אלא גם לבניין היכולות של האקו-סיסטם בולו ; לשילוב בין התעשייה,

הקפיצה הבאה

אך טכנולוגיית המחשוב אינה עומדת במקום. לא רחוק היום שבו נבצע את הקפיצה הבאה – לטכנולוגיית מחשוב קוונטי – שתגייל את ביצועי המחשבים במספר שקשה לעכלו: פי-עשרה בחזי קת 30. אין זו ההתפתחות היחידה הצפויה. העולם עומק כיום בהכנון של בית חכם, עיר חכמה, אינט רנט של הדברים וכדומה. הרעיון פשוט: להפוך כל מכשיר בחיינו (מקרה, רכב, מכונת כביסה) למכשיר מבוקר מחשב וליקשר את כל הדברים הללו ברשת תקשורת שתהיה "אינטרנט של הדברים" (IOT). הס פליגים אינם מסתפקים בכך אלא מדברים על עיר חכמה ואפילו על מדינה חכמה. יתרה מכך, ההתפ תחות בתחום האלגוריתמים הלומדים, לצד העלייה העצומה בכוח המחשוב, הזירזה למרכז הכמה את הבינה המלאכותית וזו החלה להיות משולבת בחזון הכלל.

אך אליה וקוץ בה: כבר אמרנו שאיומי הסייבר הם הצד האפל של טכנולוגיית המחשב. היתרון מחייב אפוא רמת אבטחת מיבשלית, שתאפשר את כל היתרונות הללו.

אם ברצוננו להמשיך להיות שחקנים מובילים בשוק הטכנולוגיה העולמית, ולהמשיך ליהנות מהן מקטר עיקרי לצמיחה הכלכלית, עלינו להשקיע כבר עכשיו בטכנולוגיה שתהיה שלטת בעולם ביע׳ תיד הקרוב – טכנולוגיות שבמרכזן יעמדו מערכות נבוות (AI) מאובטחות סייבר.

הכותב הוא ראש מרכז הסייבר ע"ש בלווטניק באוניברסיטת תל-אביב

איומים אלו נובעים מהיעדר תקנים לאבטחת סייבר ואסדרה מספקת של תחום החלל, מורכבות שרשראות האספקה של הלוויינים, מכך שלוויין מורכב מרכיבים רבים שכל אחד מהם עשוי להיות חשוף לאיומי סייבר, ועוד.

אבטחת סייבר נתפסת כמרכיב משני ויקר

בנוסף, תהליך פיתוח ושיגור הלוויינים הוא תהליך יקר ושיקולי עלות כלכלית וטכנית מהווים היבט משמעותי בתהליך הפיתוח. אבטחת סייבר של כל רכיבי הלוויין ושל הלוויין המוגמר, דורשת משאבים רבים, הן במישור הכלכלי והן במישור הטכני, כגון שימוש ברוחב פס. לרוע המזל, אבטחת סייבר אינה מתועדפת בשיקולי עלות ותועלת אלו, ונתפסת כמרכיב משני ויקר לתפקוד הלוויין.

כחלק מהתפתחות האיומים, אירעו בשנים האחרונות מספר תקיפות ופריצות לתשתיות קרקעיות המשמשות לשליטה על לוויינים. כחלק מכך, ב-2017 וב-2018 פרצו האקרים למחשבי המעבדה להנעה סילונית של נאס"א. כישלון בשיגור לוויין תצפית של איחוד האמירויות ביולי 2019 הוביל להערכות בכלי המדיה, לפיהן מקור התקרית הוא בתקיפת סייבר מטעם איראן.

במקביל להתפתחות האיומים, פעלו ממשלות לנסח אסטרטגיות ומסמכי מדיניות להתמודדות עם האיומים, להקים מרכזים לשיתוף המידע בנושא איומי סייבר חדשים בין הממשלה לתעשייה ולנסח קווים מנחים והמלצות ליצרניות מערכות וציוד לוויינים. כמו כן, מדינות כגון ארה"ב, רוסיה, סין, יפן, הודו וצרפת הקימו יחידות צבא ייעודיות להגנה על לוויינים.

גופי ממשלה וחברות קבלן הפועלות מטעמם החלו לפתח טכנולוגיות חדשות למזעור האיומים או לשדרג טכנולוגיות קיימות. דוגמה לכך הן פיתוח טכנולוגיות להגנה על התקשורת שבין הלוויין לקרקע מפני האזנות וירוט מידע ואף ניסויים בטכנולוגיות חדשות, כגון מחשוב קוונטי להגנה על תקשורת לוויינים מפני הפרעות ובינה מלאכותית לעדכון הגדרות ומשימות הלוויין מהקרקע.

בנושא המחקר והפיתוח של טכנולוגיות הגנה על לוויינים, על ישראל לנצל את כוח-האדם האיכותי ואת האקו-סיסטם שלה, המורכב מגופי האקדמיה, התעשייה ומערכת הביטחון, על מנת לייצר ידע ויכולות שיטיבו עם תעשיית הלוויינים המקומית, ובהמשך, יופנו גם כלפי השוק העולמי.

הכותב הוא חוקר בכיר ואחראי פרויקט הסייבר של סדנת יובל נאמן למדע, טכנולוגיה וביטחון באוניברסיטת תל אביב

וואלה

האם אנחנו בעיצומה של מלחמת סייבר עם איראן?

לקראת שבוע הסייבר השנתי שיתקיים בשבוע הבא, חוקרי ומומחי סייבר מסבירים מה עומד מאחורי מתקפות הסייבר באיראן ואיך זה משפיע על ישראל?

מאת: ינון בן שושן

מספר מתקפות סייבר פקדו את איראן בחודשים האחרונים, כאשר במהלך סוף השבוע האחרון הזרקור הופנה אל מערך הרכבות של איראן ומשרד התחבורה. תחילה דווח כי פעילות הרכבות באיראן שובשה ברחבי המדינה, והאחראיים למתקפה פרסמו על לוחות מידע בתחנות הרכבת כי מודבר במתקפת סייבר והציגו את מספר הטלפון של המנהיג העליון עלי חמינאי. יום אחרי, אתרי משרד התחבורה והפיתוח העירוני באיראן קרסו בעקבות מתקפת סייבר נוספת.

בשנים האחרונות אנו עדים להתגברות מתקפות סייבר על תשתיות קריטיות ואין ספק כי מדובר באחד מהיעדים הפופולאריים על האקרים. הקלות היחסית שבפריצה, שכן לרוב מדובר במערכות ישנות וארכאיות, אל מול הנזק הפוטנציאלי שיכול להיות הרסני במיוחד, הופכות את הענף ליעד מפתה.

באירועים האחרונים באיראן לא צוינו נסיבות המתקפה ואף ארגון לא לקח אחריות על המתקפה כמובן, אך המתקפות הללו גרמו לנזק תודעתי, הביאו לכאוס ובלגאן במדינה וככל הנראה התרחשו במטרה להעביר מסר לאיראנים.

שוחחנו עם 3 חוקרים מהמרכז למחקר סייבר באוניברסיטת תל אביב- מני ברזילי, ד"ר ליאור טבנסקי ועמרי וקסלר כדי לדון במצב ולהבין את ההשלכות של מתקפת הסייבר.

"אחת הדרכים לחלק התקפות סייבר לקבוצות היא לפי מטרות התקיפה. יש הבדל עצום בין התקפות שמטרתן איסוף מודיעין, התקפות שמטרתן פגיעה במערכות, התקפות שמטרתן קידום רעיון או אג'נדה (פוליטית/חברתית), והתקפות מסוגים אחרים", אומר מני ברזילי.

"מטרת ההתקפה משפיעה רבות על אופן הביצוע שלה (למשל תקיפה לאיסוף מודיעין היא תקיפה סמויה מאוד, ותקיפה לקידום רעיון או אג'נדה היא לרב תקיפה רועשת מאוד). כמו כן, מטרת ההתקפה יכולה ללמד אותנו הרבה על הגורם שעומד מאחוריה. במקרה הנוכחי, ההתקפה הייתה רועשת, יצרה נזק רב, ואפילו הגחיכה את חמינאי. תקיפה מהסוג הזה לא מתאימה לתקיפה מדינתית".

ברזילי מוסיף כי מעבר לעובדה שהיא לא מייצרת רווח פוליטי-מדיני, תקיפת סייבר גם חושפת יכולות ושיטות עבודה: "רוב תקיפות הסייבר המדינתיות הן סמויות מן העין, והמדינה התוקפת משקיעה מאמצים רבים בשביל לוודא שהקורבן לא ידע על התקיפה. לפיכך, אם הייתי צריך לנחש הייתי אומר שהתקיפה הנוכחית בוצעה על ידי האקרים עצמאיים, אופורטוניסטים שונאי המשטר באיראן".

"הם זיהו הזדמנות לייצר נזק ללא מאמץ רב, ועשו זאת. חלופה נוספת היא שאכן מדובר בהתקפה על ידי מדינה. אבל אם זה המצב, אז כנראה שיש תכלית נוספת להתקפה. במקרה כזה, ההתקפה כנראה מסתירה יעד חשוב יותר (למשל אפשר שהמדינה התוקפת רצתה למנוע את הגעתו של גורם מסוים ליעד מסוים)".

ד"ר ליאור טבנסקי, מציין כי "הנזק הישיר לרוב אינו בר הערכה, גם בשווקים מתקדמים כמו ארה"ב. אפשר לחשב עלויות זמן השבתה במובן של הפסד הכנסה. אפשר להעריך עלויות ישירות של חזרה לפעילות. אבל אפקטים מסדר שני אפשר להעריך במנעד רחב מאוד. אילו זו מתקפה מכוונת של יריבי איראן, ההישג העיקרי הוא המשך הפגיעה בביטחון העצמי של המשטר. עצם קרות הנזק בתוך איראן פוגע בניסיון להציג שהמשטר עובד, ויותר חשוב - מגביר החששות ופחד בקרב האליטות".

"אם לשפוט על פי הדיווחים הראשוניים מצד סוכנויות הידיעות האיראניות, ההאקרים כנראה התמקדו במערכות ה-IT של מערך הרכבות, ולא במערכת הטכנולוגיה התפעולית, המכונה OT", מציין עמרי וקסלר. "האבחנה הזאת חשובה, משום שעל ידי פגיעה במערכות טכנולוגיה תפעולית, ניתן לעיתים לגרום לנזק פיזי. בתקיפה הנוכחית, נראה כי התוקפים התמקדו בלוחות המידע שבתחנות ובמערכות למכירת כרטיסים. זו לא פגיעה שמטרתה לגרום לנזק פיזי אלא ליצור אי סדר, עומסים ובלבול."

חשש מהחמרה בעוצמת הפגיעה

"לישראל נח מאוד לשחק בזירת הסייבר במקום בזירה הפיסית, שם היא יכולה ליהנות מיכולת הכחשה יחסית גבוהה", מסביר ברזילי. "בנוסף בזירה הבינלאומית, התקפות בתחום הסייבר נחשבות פחות חמורות מהתקפות פיסיות ומקבלות פחות תהודה שלילית. לישראל יש עליונות ברורה בתחום הסייבר על פני איראן. עם זאת, צריך להכיר בזה, שהרבה יותר קל לתקוף מאשר להגן".

"גם לאיראנים נח לפעול כנגד ישראל בזירת הסייבר. על אף המוכנות הגבוהה יחסית של גופים שונים בישראל, אם היא תתמיד, מעת לעת איראן תצליח לרשום לעצמה הצלחות (קטנות ובינוניות). כולם צריכים לצאת מנקודת הנחה, שאיראן מפעילה יחידות סייבר שעסוקות באופן עקבי בתקיפה של מטרות בישראל ובאיסוף מודיעין".

"נכון לעכשיו, אף גורם לא לקח אחריות ובהינתן האופי החשאי של תקיפות סייבר, ניתן להעריך שזהות התוקף תישאר בצללים", מוסיף וקסלר. "צריך גם לזכור שהייחוס של תקיפות סייבר לתוקף הוא מלאכה מורכבת, בעיקר אם מדובר בגורם מדינתי שעומד מאחוריהן. לגורמים אלו יש לרוב את היכולת הטכנית הנדרשת כדי להסוות את פעילותם. בהקשר הישראלי, צריך לשאול מה האינטרס".

האם התשתיות הקריטיות בישראל ערוכות להתמודד עם סיטואציה דומה?

עמרי וקסלר (צילום: רובן לייטרסדורף)

"בישראל, רכבת ישראל מוגדרת כתשתית קריטית הנמצאת תחת הנחייתו של מערך הסייבר הלאומי", מסביר וקסלר. "ישראל בהקשר זה הייתה הראשונה שהבינה את מידת איום הסייבר על תשתיות ומערכות מידע חיוניות וכבר ב-2002 הטילה את האחריות להגנת מערכות מחשוב חיוניות על השב"כ, כשב-2011 האחריות לכך הועברה למטה הסייבר הלאומי, כיום מערך הסייבר".

"מאז פורסמו מספר יוזמות שמטרתן להגן על תשתיות קריטיות, ביניהן הרכבת. דוגמה אחת לכך היא מרכז SOC, שהוא מעיין מרכז בקרה לניטור תעבורת רשת ולניהול אירועי סייבר, שהוקם במטה רכבת ישראל בלוד. עם זאת, חשוב לזכור שלא לעולם חוסן, ובעיקר לא בעולם הסייבר".

ד"ר ליאור טבנסקי, מסביר כי "האתגר האסטרטגי העיקרי הוא לתכנן ולעשות שינויים מרחיקי לכת במבנה ארגוני הביטחון כך שיתאימו למציאות החדשה. לצד הצלחות - כמו האסטרטגיה מקיץ 2011 שהובילה להקמת מטה והבשלת יכולות מערך הסייבר הלאומי, נותרו אתגרים עצומים. אני חוקר את הדפוסים של חדשנות צבאית ותהליכי שינוי ארגוניים. ממצאי המחקר לא מעודדים: מגוון מחסומים מהותיים עומדי בפני כל שינוי משמעותי, אבל לצד זאת יש דרכי פעולה שמאפשרים ומעודדים חדשנות לא-טכנולוגית במגזר הביטחוני".

ברזילי, טבנסקי ווקסלר ייקחו חלק בשבוע הסייבר הלאומי השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, מטה הסייבר הלאומי במשרד רה"מ ומשרד החוץ, אשר יתקיים בתאריכים 19-22.07 באוניברסיטת תל אביב.

הכנס, בו ישתתפו רה"מ נפתלי בנט, רה"מ החליפי ושר החוץ יאיר לפיד ושר הביטחון בני גנץ, לצד עשרות בכירים נוספים מהארץ ומהעולם, מהווה נקודת מפגש מרכזית למומחי סייבר וחוקרים בולטים מהארץ ומהעולם, לצד סטארט-אפיסטים, קובעי מדיניות, גורמי ביטחון בינלאומיים, דיפלומטים ואנשי עסקים בכירים ומביא את הסוגיות והמגמות החדשות ביותר בתחום וביחס לתקופה, לצד הפיתוחים והמידע העדכניים ביותר.

בין הנושאים שיידונו השנה בכנס הם בין היתר: היבטים דיפלומטיים ושיתופי פעולה בינלאומיים, ניהול משברים, משפט וסייבר בישראל ובעולם, מגמות חדשות ופתרונות חדשניים להגנת סייבר, בינה מלאכותית, רפואה וסייבר, ענן, לוחמת סייבר, תעופה, כנס סייבר ימי ראשון בישראל שיתקיים בנמל אשדוד בהשתתפות בכירים מהעולם עוד.

N12

היועץ המיוחד לרשות הסייבר של ארה"ב: כך יראו מתקפות העתיד

בו וודס גויס כיועץ חיצוני מיוחד לרשות הסייבר האמריקנית בתקופת הקורונה כדי להביא לארגון חשיבה מחוץ לקופסה, ולהתמודד עם האיומים החדשים. "אנשים מתרכזים בזהות התוקפים ואם הם מגיעים מרוסיה או מסין – זה לא משנה", אומר בריאיון ל-Business. "היום פגיעה בארגון קטן יכולה להפיל מערכות של ארגוני ענק"

מאת: אורי ברקוביץ

"כלי הסייבר שחברות סייבר התקפי כמו NSO מספקות לארגוני אכיפת חוק, יכולים אמנם לסייע בשמירת החוק, אך הם גם עלולים להתגלגל לידיהם של ארגונים שמבצעים פעולות דכאניות. נוסף על כך, גם ארגוני אכיפת חוק יכולים להיות דכאניים בעצמם". כך אמר מומחה מדיניות הסייבר בו וודס, בריאיון ל-BUSINESS.

וודס, שביקר לאחרונה בישראל כדי לשאת דברים בכנס "סייבר וויק", שהתקיים במהלך כנס "סייבר-וויק" זו השנה ה-11 באוניברסיטת תל אביב, הוא יועץ בכיר לרשות הסייבר הפדרלית של ארה"ב CISA. על רקע פרשת NSO, הסביר וודס כי בתעשיית הסייבר העולמית "מנסים כיום ליצור מערכת נורמות מחייבות, וכחלק מהמהלך הזה דנים גם בשאלה כיצד ניתן להתיר אמצעים מסוימים של אכיפת חוק, תוך שבמקביל 'מסלקים מהשולחן' אמצעים דכאניים מדי".

אלא שמי שיפקח אוזן, לא יוכל עם זאת להתעלם מהרמז העבה לגישתו, שמקופל בהתחמקות: "אני מעדיף שלא לבטא את דעתי האישית על חברות כמו קבוצת NSO, או על קבוצות דומות לה בארה"ב, רוסיה וסין, שמתנהלות בתחום האפור, והמאוד דינמי הזה".

לדעת וודס, במקרים רבים, "שאלת הייחוס", או – מיהו הגורם אליו אפשר לייחס את המתקפה, כפי שנעשה למשל באירועי טרור – מיותרת. הסיבה לכך פשוטה: מתקפות סייבר, מעצם טבען, מתבצעות במקרים רבים על ידי חבירה של גורמים שונים שמשתפים פעולה ומשתמשים זה בזה כדי לשרת מגוון מטרות, כך שלעיתים קרובות קשה לזהות מיהו באמת הגורם שעומד מאחורי המתקפה, והאם מדובר בגורם מדיני, פלילי או אידיאולוגי.

הדבר בלט במיוחד במתקפת "סולרווינדס" בדצמבר 2020, שנחשבת אחת ממתקפות הסייבר החמורות ביותר שאירעו אי פעם. במסגרת המתקפה הדביקו האקרים מתוחכמים את חברת התוכנה "סולרווינדס" - תוכנת ניהול תשתיות IT שלה כ-300 אלף לקוחות ברחבי העולם, בהם גופי מימשל רבים בארה"ב ובעולם, ופגעו בשורה ארגונים שהבולטת שבהם היתה ענקית הטק מיקרוסופט.

במתקפת הסייבר המתוחכמת, נשלח ללקוחות החברה עדכון תוכנה, לאחר שהאקרים שתלו בו תוכנה זדונית. מדובר היה בעדכון שגרתי, מאלו שנשלחים ללקוחות בשגרה בכדי לתקן באגים, להוסיף פיצ'רים חדשים ולמרבה האירוניה – לסתום חורי אבטחה. האם זו הייתה סין כמו שטען בזמנו הנשיא דאז דונלד טראמפ, או שמא רוסיה? האם הן ביצעו פעולה זו ישירות או באמצעות פרוקסי – כמו ארגוני פשיעה למשל? ייתכן גם שלעולם לא נדע.

העיסוק בזהות התוקפים לא עזר גם לחברת "קולוניאל פייפליינס", לאחר שזו גילתה במאי השנה כי ספגה מתקפת כופרה. בעקבות המתקפה, נאלצה לסגור את הצינור שמחבר בין שמונה מדינות מניו יורק ועד טקסס, באופן שהשאיר עד 16 אחוזים מתחנות הדלק באותן מדינות ריקות לחלוטין. במקרה זה הודיעו ההאקרים עצמם כי עשו זאת למטרת בצע כסף.

העיסוק בזהות התוקפים מסתיר לטענת וודס את העובדה ש"אנו פשוט פגיעים". עם זאת, הוא אומר, ייתכן שהשינוי כבר בדרך: "ראיתי שמישהו שטען לפני שלוש שנים שהחשש המרכזי שלנו הוא מאיומי סייבר שמקורם במדינות, מצייץ ש'מתקפות כופרה הן אחד מהאיומים הגדולים ביותר על הביטחון הלאומי האמריקאי'". CISA, הגוף שלו ייעץ וודס, היא רשות פדרלית חדשה יחסית. גלגול של רשויות שונות שפעלו בעבר לכדי רשות פדרלית אחת, שמפקחת על הגנת כל הרשתות הלאומיות של ארה"ב, למעט הצבא, שאחראי על הגנתו שלו. בין יתר תפקידיה, מפקחת CISA גם על אבטחת הבחירות בארה"ב. מי שגייס את וודס לרשות היה ראש CISA דאז, כריס קרבס, שהתפרסם לאחר שבנובמבר האחרון פוטר על ידי נשיא ארה"ב לשעבר טראמפ, שהיה גם מי שמינה אותו ב-2018 לתפקיד הראש הראשון של הרשות. קרבס עצמו פוטר זמן קצר לאחר הבחירות לנשיאות, בעקבות הכרזתו כי הבחירות לנשיאות לא זויפו והגדיר אותן "הבטוחות ביותר בתולדות אמריקה".

המעמד של וודס מאפשר לו מצד אחד הצצה אל הנעשה בחדרי חדרים ובמרתפי הארגונים. מצד שני, כיועץ עצמאי הוא חופשי להתבטא הרבה יותר מגורמים רשמיים. וודס ביקש להדגיש שכל הנאמר בראיון הוא על דעתו, וכי הוא לא מייצג בדבריו את CISA. "הביאו אותנו לרשות בתחילת משבר הקורונה כדי לשפר את יכולת החשיבה שלהם מחוץ לקופסה, כדי שנביא איתנו קשרים, וכדי להבין איך המגזר הפרטי עושה דברים באופן שונה וטוב יותר", הוא מספר.

תחום ההתמחות של וודס הוא מערכות בריאות ושרשראות אספקה. שני תחומים שנפגשו במהלך משבר הקורונה בתחום החיסונים. "תתארו לעצמכם חוקרים במעבדת מחקר בתחום הפארמה, שצריכה לפתע להתמודד עם תוקפים מדינתיים. אחד המקרים הללו יצא לאור כשנחשפה מתקפה על יצרנית של ציוד של קירור מיוחד לחיסוני הקורונה. למרבה המזל, המתקפה, שנערכה גם היא על רקע פלילי, לא שיבשה את אספקת החיסונים", הוא מספר.

חשוב להבין, הוא מדגיש, "שגם ארגון קטן מאוד יכול להיות קריטי ביותר לשרשרת האספקה". בנוסף, הוא אומר, לא לכל השחקנים בשרשרת יש את אותם המשאבים להשקיע בהגנה. וודס מדבר על מה שמכונה "קו העוני של הסייבר", שתחתיו נמצאים ארגונים שלא משקיעים מספיק בסייבר, ובכך מסכנים את השרשרת כולה.

כשהוא נשאל, כמה מקרים כאלה התרחשו, מבלי שפורסמו, הוא משיב כי "קשה לומר", ומסביר כי "אחד האתגרים הגלובליים המשמעותיים בתחום הגנת הסייבר הוא שאין בנמצא פלטפורמה או רשות שירכזו דיווחים על מתקפות סייבר. לכן לממשלות ולארגונים אין יכולת לדעת כמה חברות באמת הותקפו וכמה באמת נפגעו.

בהקשר זה מעניין לציין כי במהלך הכנס הוכרז על הקמתה של פלטפורמת "גלובל סייברנט", המבוססת על רשת סייברנט הישראלית. את סייברנט פיתח מערך הסייבר הלאומי עבור המשק הישראלי, במטרה לשתף דיווחים על תקיפות סייבר, ולאחר מכן לבלום אותן ולטפל בהן.

גם על מלחמת הצללים שמנהלים גורמים שונים מול איראן בחזית הסייבר, סרב וודס להרחיב יותר מדי. הוא ציין כי הנושאים הללו נמצאים תחת אחריות משרד החוץ של ארה"ב (הסטייט דיפרטמנט), וכי הוא עצמו לא בדק לעומק את המתקפות במזרח התיכון. למרות זאת הוא ציין באופן כללי, "סייבר הוא לא זירה מתאימה לדיפלומטיה". זאת משום שלטענתו מדובר בזירה חדשה יחסית, ללא נורמות בשלות, ועם מידה רבה של אי בהירות. הסייבר, לדבריו, "מתנהל בתחום האפור, נתון לפרשנויות שגויות ולעמימות". במצב שכזה, לדבריו, "גם תאונות עלולות להידמות ולהיראות כמו מתקפת סייבר".

וודס מופיע לראיון בתספורת מוהאק קצרה צבועה לכחול, איתה גם עלה לדבר בפני הקהל שהתכנס באודיטוריום סמולרש באוניברסיטה. את השכלתו הטכנולוגית הוא רכש לבד, על "רצפת המפעל", החל מהיותו נער בבית ההורים, דרך מעבדת מחשבים מקומית, ובהמשך כמוקדן בדסק תמיכה בבית חולים.

בו וודס, היועץ המיוחד לרשות הסייבר האמריקנית

שיער צבוע וללא השכלה פורמלית. וודס

גם מחשבים הוא לא למד באופן מסודר ("ידעתי שאעשה משהו בעולם הטק, רק לא ידעתי מה"). למעשה הוא למד מחשבים במשך יום אחד בקולג', שלאחריו פרש. "פרשתי לאחר שראיתי שכולם בכיתה חכמים ממני ומתקדמים ממני בשנות אור. לא הבנתי לא את הבדיחות שלהם, ולא את התרבות שלהם, והנה אני פה עכשיו".

כלכליסט

"צריך לעשות אולימפיאדת האקרים עם כובע לבן לפני האולימפיאדה הבאה"

שניצ'י יוקהומה, בכיר בענקית הטלקומוניקציה היפנית NTT, ישתתף בשבוע הסייבר הלאומי השנתי. לכלכליסט הוא מספר על האתגרים בהקמת רשת תקשורת לאולימפיאדה ואבטחתה ועל מה צריכים לחשוב בפריז 2024 ולוס אנג'לס 2028

מאת: אוריאל דסקל

ענקית הטלקומוניקציה היפנית NTT - החברה ה-55 בגודלה בעולם והחמישית בגודלה ביפן (הכנסות של יותר מ-100 מיליארד דולר) - היא שותפה מקומית של אולימפיאדות טוקיו 2020 ואחראית על התקשורת ותשתיות התקשורת של האירוע שיתחיל ביום שישי הקרוב, ה-23 ביולי. כחלק מהחסות ושיתוף הפעולה עם מארגני טוקיו 2020, החברה בנתה והיתה אחראית על תשתית התקשורת של האולימפיאדה. 5,000 איש מהחברה (מתוך 300 אלף) עבדו על פרויקט האולימפיאדה ובכל מתקן אולימפי יש 5G, מה שהיה אמור להציג לצופים במגרשים עצמם חוויה ראשונית וייחודית מאוד של מציאות רבודה - משהו שככל הנראה היה הופך לסטנדרט בכל אולימפיאדה עתידית ואולי בכל מגרש ספורט עתידי.

"בבריכה, הקהל היה אמור לקבל משקפות שהיו מאפשרות לו לראות את המשחים דרך מציאות רבודה", מגלה בראיון לכלכליסט שניצ'י יוקהומה, בכיר ב-NTT. "הקהל היה אמור לשים את המשקפות ואז היה רואה את השחיינים עם פרטים עליהם - מדינה, גובה, שם וכו' וגם היה רואה את קו השחייה כפי שרואים בטלוויזיה ועוד. גם בגולף תוכנן שימוש בטכנולוגיה הזו, שמבוססת 5G ומטרתה להעצים את חווית הצופה במגרש. לצערי האולימפיאדה תהיה ללא קהל והדברים הללו, שלדעתי היו יכולים לשנות את כל הדרך בה צופים בספורט באצטדיונים בעולם, לא יוצגו".

יוקהומה, מנהל אבטחת המידע הראשי (CISO), אומר שמציאות רבודה לקהל היתה אמורה להיות החידוש העיקרי של NTT באולימפיאדה הזו. זה היה אמור להיות משהו שהוא "אקסטרה" ו"כייפי" למשחקים האולימפיים, שבשנים האחרונות סיפקו שעות על גבי שעות של עבודה ל-NTT.

יוקהומה ישתתף בשבוע הסייבר הלאומי השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ, שיתקיים מה-19 עד ה-23 ביולי (ימים שני עד שישי השבוע) באוניברסיטת ת"א. הוא ידבר על אבטחת הסייבר של המשחקים האולימפיים. לפני שיעשה זאת, הוא מדבר עם כלכליסט על הדברים שלמד מעבודה על פרויקט עצום ומורכב כמו אולימפיאדה וגם על מה פריז ולוס אנג'לס, שיארחו את האולימפיאדה ב-2024 ו-2028, יכולות ללמוד מהאתגרים.

סייבר הוא רק בעיה אחת

"המשחקים יהיו תלויים הרבה יותר ברשת בגלל שאין צופים", אומר יוקהומה. "הדרישות לרשת יהיו גדולות יותר. יותר אנשים תלויים עכשיו ברשת בלבד לצפייה במשחקים. יש לנו, למשל, רשת כפולה. אם אחת נופלת, השנייה תמשיך. אבל זה רק חלק מהרבה מאוד אתגרים לקיים אולימפיאדה. אנחנו עשויים לעמוד מול טייפון, גשם כבד מדי, אסון טבעי כמו רעידת אדמה. יש הרבה מאוד בעיות שיכולות לפגוע פיזית ברשתות שלנו. סייבר הוא רק בעיה פוטנציאלית אחת. צריך להיות מאוד מתואמים די לפתור את הבעיות הללו".

האתגרים הספציפיים קשורים לאבטחת מידע של האולימפיאדה הם "מורכבים ומסובכים" לפי יוקהומה. "אנחנו צריכים לאבטח את האצטדיון, את מתקני המים, את הכפר האולימפי ואת אנשי הוועד האולימפי - אבל זה רק דבר אחד שמאפשר לקיים משחקים אולימפיים. כמובן שגם תחנת הכוח צריכה להמשיך לעבוד, והרכבת צריכה לעבוד וכל התשתיות הקריטיות צריכות לעבוד ברמה גבוהה מאוד. תקשורת היא עוד תשתית קריטית למדינה ובטח לאירוע גדול כמו האולימפיאדה".

"תמיד הייתי טיפוס שלא היה איכפת לו ממוסכמות. הלכתי בדרכי שלי", הוא אומר. אך מאחר שלדבריו, "תמיד היה גיק", התגלגל בסופו של דבר דווקא ללימודי פסיכולוגיה. "הלכתי ללמוד פסיכולוגיה כדי לברוח מהגיקיות ומה שהפך אותי בסוף למומחה סייבר, כמאמרו של זוכה הפיזיקאי הדני זוכה פרס נובל נילס בוהר – היתה העובדה שעשיתי כל טעות אפשרית בתחום".

וודס, שכאמור עוסק בעיצוב מדיניות סייבר, מוטרד מרמת המודעות הלא מספיק גבוה לסיכונים בתחום בקרב הציבור ומקבלי ההחלטות. למעט אירועים יוצאי דופן, הוא אומר, רובן המכריע של המתקפות החמורות כלל לא מגיע לידיעת התקשורת. התוצאה, הוא מתריע, היא תחושת ביטחון מזויפת, שעלולה להביא בעקבותיה לשאננות.

מעבר לכך, הוא מתלונן על כך שגם שכבר מתפרסמים פרטים על אירועים חמורים, הם מתקשים לקבל תפוצה רחבה. כך היה לדבריו עם שני אירועים חמורים השנה שאירעו בשנה האחרונה בהם הותקפו כלי פיתוח תוכנה. מדובר במתקפות נגד חוליות רגישות במיוחד, משום שכמו במקרה של סולרווינדס, הקוד מזוהם עוד בשלב מוקדם של שרשרת האספקה, במקום בו הוא מיוצר, ומשם מופץ לכל עבר, דרך המשתמשים של אותן תוכנות.

"אני יודע שבאחד המקרים הללו, אחד התוקפים לא הסתפק בשתילת הקוד הזדוני, אלא גם שתה לחברה את רשימת הלקוחות אליהן היא היתה אמורה להישלח בהמשך הדרך", הוא מספר. לדבריו, רשימת לקוחות שכזו יכולה לכלול עשרות אלפי ארגונים שההאקרים יכולים לנסות תקוף מאוחר יותר". ולא שמדובר באירועים נדירים, הוא אומר עוד, "אירועים שכאלה קורים כל הזמן. הפורץ האופייני פועל לבדו ובניגוד למה שאפשר לדמיין, לא מדובר באיזה 'מאסטר קרימינלי'".

כמו בערך כל מומחי הסייבר, גם וודס מזהיר שמעט האירועים שמתפרסמים, אינם רק קצה הקרחון, אלא שזו רק ההתחלה. "העשור הקרוב יהיה העשור של מתקפות שרשרת אספקה. אנחנו רק מתחילים להבין כמה הן ארוכות, מורכבות ופגיעות. אנו צפויים לגלות עוד ועוד חולשות אבטחה חמורות בטרם נוכל בכלל לדעת איך להתמודד איתן ולהתחיל לשלם את הריבית על כל ה'אוברדראפט הטכנולוגי' שצברנו במשך עשורים, כשלא דאגנו לאבטחה ראויה".

מלבד הדברים שציינת, מהם כיום לדעתך האתגרים הכי משמעותיים שניצבים בפני עולם הסייבר וכיצד יהיה ניתן לפתור אותם?

"בראש ובראשונה יש להשקיע במקומות שבהם הסיכון משותף לכל השחקנים המעורבים. כמו בתשתית התקשורת הבסיסית של האינטרנט", הוא מסביר. "כי בלי תקשורת אחת לא יוכל להיות אינטרנט אחד, אלא אינטרנט מפוצל (ספלינטרנט). עניין נוסף הוא לנקות את שרשרת האספקה ולדאוג לאלטרנטיבות ראויות לחוליות החלשות. אם אתה יצרן של תוכנה שרבים עושים בה שימוש – אולי כדאי לפתוח חלקים ממנה כ'קוד פתוח' עבור גורמים חיצוניים, כדי שיוכלו לסייע לשפר את האבטחה".

"במקביל מתהווים טרנדים חדשים כמו ניתוח מתמטי, כזה שבעזרתו ניתן יהיה להעריך בעתיד אוטומטית את מידת העמידות של המערכות השונות בפני מתקפות, כמו גם את העלות שכרוכה בלהביא אותן למצב טוב".

"בכלל, הייתי רוצה שיהיה דבר כזה 'פילוסופים של סייבר'. אולי יש כבר כאלה, רק שטרם נתקלתי בהם. הייתי רוצה שיותר אנשים ישאלו שאלות כמו 'האם בדומה למדעים המדויקים, גם בסייבר יש עקרונות פשוטים שרלוונטיים לכולם?'. או: האם קיימים עקרונות מנחים בהם נוכל לדבוק כדי להפוך את העולם לבטוח יותר?".

מה הסיטואציה הכי גרועה שיכולה לקרות באולימפיאדה מבחינת הסייבר?

"הסיטואציה הכי גרועה ככל הנראה היא משהו שאנחנו לא יודעים ממנו. אנחנו מעריכים את הסיכונים כל הזמן. בכללי‍ות, כשזה מגיע לאולימפיאדה - חשוב מאוד שהרשת תהיה קיימת וחזקה כדי להעביר את המשחקים לעולם. במובן הזה הזמינות של הרשת (Availability) חשובה יותר משני האלמנטים האחרים בבסיס של העבודה שלנו - יושרה וסודיות (Integrity and Confidentiality)".

יוקהומה לא חושף את ניסיונות ההאקרים של לפגוע באולימפיאדה, אבל רומז שזה קרה יותר מפעם אחת. "התחלנו כבר לפני שנים את העבודה על האולימפיאדה. המבצע שלנו התחיל הרבה לפני שהספורטאים מתחילים להתחרות. זה רק טבעי שתהיה התקפה. אסור לי לדבר על זה".

יוקהומה מבהיר גם שהם השתמשו בטכנולוגיה ישראלית ושיתפו פעולה עם חברות ישראליות בכל הקשור לאבטחת התקשורת. NTT הקימה באחרונה מעבדת חדשנות בישראל, שמתמקדת בסייבר סקיוריטי, בריאות דיגיטלית, ורובוטיקה, במטרה לאתר טכנולוגיות ישראליות, למזג אותן ל-NTT ולשווקן ללקוחותיה ברחבי העולם, תוך קידום שיתופי פעולה במו"פ ואיתור השקעות בחברות ישראליות. מעבדת החדשנות בכפר סבא - NTT Innovation Laboratory Israel - תהווה מוקד עסקי בישראל לכל חברות הבת של NTT. המעבדה תשתף פעולה עם חברות ישראליות בפיתוח טכנולוגיות חדישות בתחומים שונים. המעבדה תפעל לשילוב הטכנולוגיות הישראליות בשירותים ובמוצרים המפותחים על ידי NTT, כמו גם לאיתור מוצרים וטכנולוגיות שניתן להפיץ ולשווק ללקוחות NTT.

טיפ לאולימפיאדה הבאה

יוקהומה מסכם את השיחה בטיפ לאולימפיאדות הבאות: "יש כל כך הרבה גורמים שמשפיעים על האולימפיאדה - ממשלה, ממשלות מקומיות, ועדה מארגנת, ועד אולימפי, נותני שירותים חיוניים ועוד. כל אלו חייבים, בסופו של דבר, לפעול על אותה תשתית תקשורתית, על אותה מערכת. אז ההמלצה הראשונה שלי היא לרכז את כולם תחת אותה קורת גג טכנית בכל הנוגע לאולימפיאדה.

והוא מוסיף רעיון: "כולם חייבים לשתף פעולה בשביל שהאולימפיאדה תצא לדרך. אנחנו לא עובדים לבד. זה שיתוף פעולה גלובלי. אנחנו בשיתוף פעולה עם חברות תקשורת אחרות ברחבי העולם וכך גם הוועדה המארגנת ובעצם כל מי שנוגע בזה. מחליפים אינפורמציה ועוזרים אחד לשני להוציא לפועל אירוע גלובלי.

"הרעיון שלי הוא שבגלל שהאקרים הם בעיה גלובלית - ההאקרים עצמם מגיעים מכל מקום בעולם - אנחנו צריכים גוף גלובלי של האקרים כובע לבן (האקר שמשתמש בידיעותיו במחשבים ובאבטחת מידע למטרות חיוביות ואתיות) שמורכב מהאקרים מרחבי העולם שיעזרו לאבטח את האולימפיאדה מפני האקרים כובע שחור.

"זה ארגון שאפילו גוף כמו האו"ם יכול להקים והוא עשוי להתגלות כמאוד יעיל ומועיל לאולימפיאדות הבאות. צריך לעשות אולימפיאדת ההאקרים הלבנים שיעזרו באבטחה ושמירה על אירוע גלובלי כמו האולימפיאדה, שם יחליפו מידע וידע. זה יכול להיות נכס לאנושות כולה. כדאי שיעשו זאת לפני האולימפיאדה הבאה".

מעריב

מומחה לסייבר מעריך: זה הנזק של מתקפת הסייבר הרוסית על החברות האמריקאיות

מני ברזילי ממרכז הסייבר באוניברסיטת תל אביב סיפר בראיון לענת דוידוב על המתקפה שנעשתה ככל הנראה על ידי קבוצה האקרים רוסית בשם REvil: "התקפה עצומה בשרשרת האספקה"

מני ברזילי ממרכז הסייבר באוניברסיטת תל אביב סיפר היום (ראשון) בתוכנית "איפה הכסף" עם ענת דוידוב ברדיו 103FM על מתקפת הסייבר הענקית שפגעה לפחות ב-200 חברות בעולם, רובן בארה"ב, ככל הנראה על ידי קבוצת האקרים רוסית בשם REvil: "זהו אחד האירועים הגדולים מסוגו, שהגיע בדיוק בזמן לארבעה ביולי, יום העצמאות האמריקאי. זאת התקפה עצומה בשרשרת האספקה – המשמעות של כך היא שחברה אחת נתקפת, וזה משפיע על המון חברות".

עוד אמר ברזילי כי "כרגע המספר עומד על 200 חברות שהותקפו, אך ההערכה היא שהמספר עוד יגדל. במתקפה מסוג זה, האקרים מוצאים דרך להשתלט על חברה שיש לה הרבה לקוחות. במקרה זה, ההאקרים השתלטו על חברה בשם קסייה שמיקומה במיאמי, והיא מנהלת מערכות מחשוב של חברות אחרות. יש להם כ-40 אלף לקוחות בעולם, אבל לא כולם משתמשים במוצר שהושפע".

ברזילי הוסיף כי "ההאקרים השתלטו על החברה, ודרכה התקינו במוצר שקיים אצל חלק מהלקוחות, משהו שאפשר להם להיכנס אל המחשבים של אותן חברות מרחוק. רוב הלקוחות של החברה הם בארה"ב, אבל צריך להניח שרוב החברות שהותקפו עדיין לא הוציאו פרסום לציבור, ולכן אם יש חברות ישראליות אנו נגלה על זה רק בהמשך".על קבוצת ההאקרים הרוסית REvil סיפר: "נראה שמדובר בקבוצה הרוסית, למרות שהדיווחים הם לא חד-משמעיים. הקבוצה הזאת היא אחת מקבוצות ההאקרים המפורסמות בעולם, היא עומדת מאחורי התקפות כופר מפורסמות, ועשתה מאות מיליוני דולרים ברווחים מהתקפות כופר בעבר".ברזילי התייחס לסיכונים הקיימים בעבור החברות הישראליות בכל הנוגע למתקפות סייבר: "ככל שהעולם תלוי יותר בטכנולוגיה, כך אנו הופכים להיות יותר חשופים. ככל שאנו הופכים להיות יותר מחוברים, כך התקפה במקום אחד יכולה להשפיע גם על חברות נוספות. סטטיסטיקת התקיפות בישראל היא מורכבת ותלויה במה שאנו מגדירים כמתקפת סייבר. סריקות פשוטות יכולות להיחשב כמתקפה ואז בישראל יש לנו בטח מילארדים של ניסיונות תקיפה ביום, ואילו ניסיונות תקיפה יותר מתוחכמים יש, כנראה, מאות ביום בישראל. זה ברמת הניחוש".

"אנחנו ברי מזל מספיק בשביל לחיות במדינה שהצליחה לעשות משהו יוצא דופן בתחום הסייבר", אמר ברזילי והוסיף כי "מכל מדינות העולם מגיעים לכאן כדי להבין איך אנחנו עושים את מה שאנחנו עושים. שבוע הסייבר הלאומי הוא אחד האירועים הכי חשובים מחוץ לארה"ב בנושאי סייבר, והרבה מהפתרונות המתקדמים בתחום הסייבר יצאו מישראל. זאת גאווה לאומית אמיתית".

ידיעות אחרונות
ממון חדשות
עורך: אסי חיים
calcala@yedioth.co.il

1 מכל 5 עסקים הותקף בסייבר

מאת **אודי עציון**

1 מכל 5 עסקים בישראל (18%) חווה תקיפת סייבר לחמישית מהם נגרם נזק למערכות המידע עקב אי־זמינות, הרס או דליפת מידע. כך עולה מסקר חדש של הלמ"ס ומערך הסייבר הלאומי.

"הסקר מציג לראשונה נתונים שמראים בבירור כי תקיפות סייבר על עסקים בישראל הפכו לתופעה נרחבת", אומר יגאל אונא, ראש מערך הסייבר הלאומי. "חלק מהארגונים הצליחו לבלום אותה, וכאן אנו עדים לשלב חשוב של זיהוי וגילוי התקיפה שארגונים רבים־מדי לו להעצים באחרונה. נזקי התקיפה הם בעלי השלכות כלכליות גדולות שכרוכות לעתים אובדן ימי עסקים ואף השבתה, ולכן כראי להשקיע במניעה ובגילוי".

הסקר יוצג בשבוע הסייבר שמתקיים בשיתוף מרכז לחקר הסייבר באוניברסיטת ת"א. מהסקר עולה כי התקיפות שכיחות בעיקר בקרב עסקים גדולים (250 עובדים ויותר): שניים מכל חמישה עסקים גדולים חווה תקיפת סייבר (42%) ובקרב תעשיית טכנולוגיית עילית (47%). בענפי ההיי־טק, אחת מכל שלוש חברות דיווחו על תקיפה (37%), וגם בענף שירותים מקצועיים, מדעיים וטכניים דיווחו על שיעור גבוה יחסית של תקיפות (27%). כ־15% מהעסקים הקטנים חוו מתקפת סייבר. התקיפות כוללות בין השאר גניבת מידע, השתלטות על מערכות מידע ודרישת דמי כופר.

מהסקר עולה כי 58% מהארגונים פועלים במידה רבה עד רבה מאוד, לתפיסתם, לצמצום סיכוני הסייבר, ו־31% במידה מעטה או מעטה מאוד. ככל שהארגון גדול יותר כך הוא פועל על טוב יותר בתחום הגנת הסייבר. רק 55% מהעסקים הקטנים מבצעים פעולות רבות בתחום לעומת 86% מהעסקים הגדולים. הענפים שדיווחו בשיעור גבוה על כך שחוו מתקפות – הייטק ושירותים מקצועיים, מדעיים וטכניים – דיווחו גם על מידה גבוהה של פעילות לצמצום הסיכון (89% ו־84% בהתאמה).

שלוש בקרות ההגנה השכיחות ביותר שבהן השתמשו עסקים הן עדכוני תוכנה (68%), אמצעים לגילוי זיהוי וסיכול נוזקות (65%), ומדיניות סיסמאות חזקות (62%). ל־68% מהארגונים יש עובדים העוסקים בנושא בארגון או במיקור חוץ, ואילו ל־32% מהארגונים אין כאלה כלל.

המרגם כלל כ־2,500 עסקים עם לפחות 10 מועסקים בכל הענפים מלבד פיננסים, בריאות ומינהל ציבורי. והוא פרק אחד מתוך סקר מקיף יותר בנושאי שימוש במחשבים ואינטרנט, שתוצאותיו יפורסמו בהמשך השנה על ידי הלמ"ס וישראל דיגיטלית.

נתונים: הלמ"ס

אנשים ומחשבים PC

צה"ל קיבל את אות יקיר הסייבר

האות, בצורת פסל של סוס טרויאני, הוענק לצבא על "עמידה רבת שנים בחזית המאבק בתחום, על הישגים רבים רבים שהושגו ועל קידום חוסן הסייבר בישראל", כך על פי נימוקי השופטים

מאת: יוסי הטוני

אות יקיר הסייבר הוענק לצבא ההגנה לישראל. האות, בצורת פסל של סוס טרויאני, הוענק לצבא על "עמידה רבת שנים בחזית המאבק בתחום, על הישגים רבים רבים שהושגו ועל קידום חוסן הסייבר בישראל".

האות הוענק היום (ג>) במסגרת שבוע הסייבר הישראלי, אשר נערך זו השנה ה־11. את שבוע הסייבר מובילים המרכז למחקר סייבר בינתחומי ע"ש בלווטניק באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ. את הפרס קיבלו בשם הצבא האלוף תמיר הימן, ראש אגף מודיעין, והאלוף ליאור כרמלי, ראש אגף התקשוב וההגנה בסייבר.

צה"ל הוא "שחקן מוביל בפיתוח טכנולוגיות הגנה"

אלוף (מיל>) יצחק בן ישראל, חבר ועדת השיפוט וראש מרכז הסייבר באוניברסיטת תל אביב, הקריא מעט מנימוקי השופטים: "צה"ל מגן בסייבר ופועל בתחום זמן רב. כבר בשנות ה־80> במאה הקודמת הבינו בצה"ל את חשיבות התחום, את ההזדמנויות הטמונות בחובו, ואת הפוטנציאל שלו לסגירת פערים טכנולוגים. כל השנים הללו בהן הוא עוסק בתחום, הפכו את הצבא לשחקן מוביל בפיתוח טכנולוגיות הגנה. צה"ל השקיע בתחום רבות. מעבר לתרומה של צה"ל לקידום תחום הסייבר, הצבא הוא גוף ייחודי בהכשרת ההון האנושי, עם אלפי הדרכות. כך הוא מסייע לפתח את יכולות המדינה בסייבר לטובת כל תחומי החיים, כלכלה תעשיה ואקדמיה".

אלוף הימן אמר כי "במסגרת המבצע האחרון בעזה, מידע שנאסף ממגוון מקורות – בין היתר ממרחב הסייבר – הותך יחד באמצעות יכולות עיבוד מתקדמות, בינה מלאכותית ולמידת מכונה – לכדי תפוקות מבצעיות. דבר זה אפשר לצה"ל לתפקד טוב יותר, מהר יותר, ועם פחות אבדות בחיי אדם".

"אתייחס לאיומים היומיומיים על מדינת ישראל בממד הסייבר – ישראל נמצאת תחת איום תמידי בסייבר, ומתקפות מבוצעות לעיתים נגדה. אנו מצליחים להתמודד עם מרבית האיומים באמצעות יכולות הגנה מתקדמות", אמר הימן.

"סייבר הוא כלי מרכזי בארגז הכלים שלנו", ציין, "הוא יכולת החוצה את כל צה"ל, מאחסון חכם של נתונים ועד ניתוחים מבוססי בינה מלאכותית".

"כמו בממדי הלחימה אחרים, הגנה לבד אינה מספקת", אמר ראש אמ"ן, "יש לנקוט צעדים נוספים, כדי לשמר את עליונות ישראל אל מול אויבנו. אלו שתוקפים את ישראל באוויר, בים, ביבשה – או בסייבר, צריכים להבין את הסיכון שהם לוקחים. כפי שהם נוכחים לראות פעם אחר פעם, תוקפנות תיענה באופן מידתי והולם. אני משוכנע שצה"ל, קהילת המודיעין, התעשיה והאקדמיה יבנו יחד יכולות סייבר שיהוו אלמנט קריטי ומכריע במדינה".

וואלה

קוקטייל וסייבר

מאת: הלאונג' מיכל גלנטי

קרן ההשקעות בסייבר YL Ventures ערכה ביום שני ב'ספיקאיזי' בתל-אביב, אירוע משותף עם הקרן האמריקאית הגדולה Scale Venture Partners המשקיעה בסטארט-אפים ישראלים. האירוע נערך במסגרת אירועי שבוע הסייבר השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ.

באירוע, שהתקיים בנוכחות יזמי סייבר ובכירים בתעשיית הסייבר הישראלית, החל בקוקטייל ונמשך בפאנל שעסק בעולם אבטחת המידע והסייבר ובהשקעות בסייבר. בפאנל דיברו עופר שרייבר שותף ומנהל הסניף הישראלי של YL Ventures, וונדי נאת'ר - ראשת הצוות המייעץ לאבטחת המידע בCisco, אנדי אליס שותף בYl Ventures, ריאן גורני CISO in Residence בקרן ורבים נוספים.

מעריב

הלאונג' מיכל גלנטי

4. וונדי נאת'ר ועופר שרייבר

4. קוקטייל וסייבר

קרן ההשקעות בסייבר YL Ventures ערכה ביום שני בספיקאיזי בתל אביב אירוע משותף עם הקרן האמריקאית הגדולה Scale Venture Partners, המשקיעה בסטארט־אפים ישראליים. האירוע נערך במסגרת אירועי שבוע הסייבר השנתי של המרכז למחקר סייבר באוניברסיטת תל אביב, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ.

האירוע, שהתקיים בנוכחות יזמי סייבר ובכירים בתעשיית הסייבר הישראלית, החל בקוקטייל ונמשך בפאנל שעסק בעולם אבטחת המידע והסייבר ובהשקעות בסייבר.

בפאנל דיברו **עופר שרייבר**, שותף ומנהל הסניף הישראלי של YL Ventures; **וונדי נאת'ר** – ראש הצוות המייעץ לאבטחת המידע ב־Cisco; **אנדי אליס**, שותף ב־YLVentures; **ריאן גורני**, CISO in Residence בקרן, ורבים נוספים.

ynet
ידיעות אחרונות

בנט: "מתקפות סייבר – אחד האיומים הגדולים על הביטחון הלאומי ועל העולם כולו"

ראש הממשלה נפתלי בנט אמר בכנס הסייבר השנתי באוניברסיטת תל אביב כי "אם בעבר מדינה רעה הייתה צריכה לשלוח מטוס עם חיילים ופצצות, היום הדרך הטובה ביותר זו מתקפת סייבר - כל מה שצריך זה מוחות, ידע, ניסיון וחיבור טוב לאינטרנט. כזה קל". לדבריו, "מדובר באחד האיומים הגדולים על הביטחון הלאומי ועל העולם כולו. מה עושים בקשר לזה? צריך את כוחות השוק הפרטי, בשילוב עם כוח הממשלה. בישראל יש לנו אנשים מאוד חכמים שנכנסים לשירות צבאי בתחום המודיעין בגיל מאוד צעיר, ו'נזרקים' לחברה הישראלית בגיל צעיר עם יכולות עצומות. אני הייתי אחד מהם לפני 29 שנה". בנט הוסיף: "אנחנו כמדינה מוכרחים להגן על עצמנו, ולכן ייצרנו גוף סייבר לאומי אחד שתפקידו לפקח על כל התעשיות בישראל - מים, חשמל וכו', והרשות הזאת אחראית גם על השוק הפרטי".

PC אנשים ומחשבים

בנט: "הכול פגיע ותחת מתקפה – המים, החשמל, האוכל, המכוניות והמטוסים שלנו"

יגאל אונא"החזר ההשקעה בביצוע מתקפות סייבר הוא מהיר ביותר, ולכן המתקפות תמשכנה לצמוח אקספוננציאלי - וזה מדאיג אותי", אמר נפתלי בנט, ראש הממשלה בכנס שבוע הסייבר הישראלי● "צריך לרסס את הרעים בספריי אדום, שכולם יידעו שהם האקרים"

מאת: יוסי הטוני

"הכל פגיע ומצוי תחת מתקפה: המים שלנו, החשמל, האוכל, המטוסים והמכוניות שלנו. למה זה ככה, למה כה הרבה מההיבטים בחיינו מותקפים בסייבר? כי זה קל. אם אתה מדינה רעה, ורוצה לתקוף, אז בעבר נדרשת לשלוח מטוס עם פצצות וחיילי קומנדו. כיום כל שנדרש הוא מחשב נייד, ידע וניסיון מקצועי בפריצה – וחיבור לקו אינטרנט. החזר ההשקעה בביצוע מתקפות סייבר הוא מהיר ביותר, הסיכוי להיתפס אינו גבוה, ולכן מתקפות הסייבר תמשכנה לצמוח באופן אקספוננציאלי. וזה מדאיג אותי", כך אמר נפתלי בנט, ראש הממשלה.

בנט היה דובר המפתח היום (ד') בכנס שבוע הסייבר הישראלי, אשר נערך זו השנה ה-11. את שבוע הסייבר מובילים המרכז למחקר סייבר בינתחומי ע"ש בלווטניק באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ.

הפריה הדדית בין התעשייה, הצבא האקדמיה והון סיכון

"כראש ממשלה", אמר בנט, "קבעתי כי איום הסייבר מצוי בעדיפות, וכי הוא אחד האיומים הגלובליים המחייבים אותנו לפעול בתחום. יש לנו תעשייה יצירתית, ואל לנו להפריע לה, עלינו לתת לה לשגשג. אין ממשלה בעולם, או שילוב של ממשלות, שיכולים לפתור

כלכליסט

רה"מ בנט: הקמנו יוזמת הגנת סייבר גלובלית עם מספר מדינות

בכנס שבוע סייבר הלאומי באוניברסיטת ת"א אמר בנט כי מטרת היוזמה, שמתוכננת להתרחב למדינות נוספות, היא להוות ארגון עולמי שיילחם בתקיפות סייבר. זאת בשל נתונים מטרידים לפיהם 1 מתוך 5 עסקים ישראליים הותקפו בשנה הקודמת. "התקפות סייבר הפכו לאיום עולמי משמעותי". בנט גם דיבר על הקמת מרכז הסייבר בב"ש: "מתוך כל 100 דולר שמושקעים בסייבר, 41 דולר מגיעים לסייבר ישראלי"

מאת: רפאל קאהאן

ראש הממשלה נפתלי בנט פתח את המושב העיקרי של כנס שבוע הסייבר הלאומי של אוניברסיטת תל אביב שנערך הבוקר (ד') בחשיפה מעניינת - הקמת סוכנות או יוזמת סייבר בינלאומית המיועדת להילחם במתקפות סייבר, שבין מטרותיה שילוב מדינות וחברות נוספות לשם כך. השם שניתן ליוזמה היא "מגן סייברנט גלובלי" וכעת כבר תריסר מדינות שותפות לה, לדברי בנט.

היוזמה החדשה הוקמה בשל מספרים מטרידים שהציג ראש מערך הסייבר הלאומי, יגאל אונא, מעט לפני עלייתו של בנט לנאום. לפיהם, אחד מתוך חמישה עסקים ישראלים סבלו מהתקפת סייבר בשנה הקודמת (2020), וכ-47% מחברות ההייטק הישראליות הותקפו. מדובר במספרים גדולים יחסית אבל לא ייחודיים לישראל. לפי הנתונים, משבר הקורונה הביא לזינוק אדיר במתקפות הסייבר בעולם וישראל לא לבד במערכה.

ראש הממשלה בנט הסביר זאת: "הכל תחת מתקפה, למה זה? כי זה קל. אם אתם רוצים לתקוף, השיטה הטובה, הקלה והזולה ביותר היא דרך מתקפת סייבר. זו הסיבה לכך שזה יגדל ככל שהזמן יעבור. אני מאמין שמתקפות סייבר הפכו לאחד האיומים המשמעותיים על שלום העולם".

המסקנה העיקרית של המצב החדש היא שאף מדינה לבד או אפילו קבוצת מדינות לא יכולה לפתור את הבעיה הזו לבדה. רק שילוב של מדינות ועסקים יכולה להתמודד עם מצב מעין זה. כך מסביר ראש הממשלה שבעברו הקים בעצמו חברת סייבר (סיוטה), שנמכרה לאחר מכן באקזיט של מאות מיליוני דולרים לענקית הסייבר האמריקאית RSA.

בנט גם הסביר את הרעיון של מרכז הסייבר בבאר שבע. לדבריו מדובר במערכת שמיועדת לייצר מצע שיזין את החדשנות והיצירתיות על ידי שילוב של גורמי אקדמיה, צבא והייטק, "סרן בת 25 שתיפגש לצהריים עם אנשי הון סיכון ואקדמאים מאוניברסיטת באר שבע. אנחנו מאפשרים להם לייצר חדשנות והזדמנות - מתוך כל 100 דולר שמושקעים בסייבר, 41 דולר מגיעים לסייבר ישראלי", אמר.

"יצרנו סוכנות סייבר ראשונה ויחידה במינה - מערך הסייבר הלאומי. כזו שמשלבת את כל היכולות. היא מאפשרת לכולם ליצור קשר איתה לסיוע. התפקיד שלה הוא להתריע אבל גם לסמן את העבריינים. מערך הסייבר עובד ביחד עם המוסד, השב"כ ו-8200. אבל החדשות העיקריות הן שאנחנו עוברים לעולם. אנחנו נפתחים לעולם עם מגן סייברנט בינלאומי. אם נילחם ביחד ננצח".

לדברי בנט, "נגיד שאיראן תוקפת את מערכות המים בבלגיה בלילה, קשה מאוד למצוא את מקור התקיפה במסגרת אלפי הסימנים שמנוטרים. אבל אם אתה תוקף מערכת מים בצילה או בהודו כמה דקות לאחר מכן. אם נשתף את המידע על שיטת הפעולה ניתן יהיה להתריע בזמן אמת ולהתמודד ישירות עם המתקפות האלה. זו הסיבה שבישראל אנו מאמינים ששיתוף פעולה ושילוב גורמים יביא לפתרון".

"כבר חתמנו הסכמים עם תריסר מדינות - במקום שכל מדינה או חברה תהיה לבדה ההגנה תהיה משולבת. אנחנו מזמינים מדינות טובות להצטרף אלינו ליוזמה הזו. כל מה שאתם צריכים לעשות זה להתקשר ליגאל אונא".

לבדו את אתגר איומי הסייבר. לא כל השכל נמצא בממשלות, לשם כך נדרש שיתוף פעולה עם המגזר הפרטי. יש לנו בישראל אוסף של חבורת אנשים חכמים, שבהיותם צעירים בצבא עשו דברים אחראיים וחשובים, שלאחר הצבא הגיעו בגיל צעיר לתעשיית ההיי-טק המקומית, והם האחראים ל'בום' שיש בתעשייה. הם יודעים מה הם עושים וזה הסוד, המרכיב, התבלין הסודי במתכון ההגנה בסייבר של ישראל".

"כאשר חבורת אנשים יושבים יחד, יש הפרייה הדדית", אמר ראש הממשלה, "בנינו 'עיר סייבר' בבאר שבע. זה מקום בו בארוחת הצהריים קצינה בת 25 תיפגש עם סמנכ"ל מו"פ, או תימצא בקשר חברתי עם מנהלי קרן הון סיכון, ויש סיכוי ששם הם יפגשו פרופסורית למתמטיקה מאוניברסיטת בן גוריון. ככה ארבעתם ייצרו חדשנות. חדשנות לא נוצרת ממתן פקודות. המטרה היא לאפשר לזה לקרות, ליצור היתוך ולתת להם לנוע. בהפצת חדשנות ורעיונות משותפת ניתן להטליא עוד טלאי, לסגור פער לפתור עוד בעיה".

41% מההשקעה העולמית בהגנת סייבר – בישראל

"תעשיית ההיי-טק הישראלית גדלה ב'בום', באופן מעריכי", אמר בנט. "על כל מאה דולרים בהשקעה עולמית בסייבר, 41 מהם מושקעים בחברות הגנת סייבר ישראליות".

"הבנו שעלינו, כממשלה, להגן על עצמנו", אמר ראש הממשלה. "היינו מהראשונים בעולם ליצור סוכנות סייבר, שתשמש כ-One Stop Shop, סוכנות אחת האחראית להגנת כל התשתיות הקריטיות, וגם – תהיה אחראית למגזר הפרטי".

"אם עולה לאוטובוס כייס, יש לרסס אותו בספריי בצבע אדום, שכולם ידעו שהוא פושע. ככה כולם יבינו ששיתוף היא הדרך הנכונה להגן על עצמנו, ביחד ולא לבד. מערך הסייבר הלאומי, בראשות יגאל אונא הוא התרסיס, הוא המגאפון המתריע בפני כולם 'הנה הבחור הרע'. המערך עובד על בסיס קבוע עם המוסד, השב"כ ויחידה 8200. זה אתגר גדול – אבל עובד. הם עובדים יחד, חושבים יחד, ומתקשרים ביניהם בצוותא. נרחיב את הרשת הלאומית הארצית למניעת מתקפות סייבר, ונהפוך אותה לגלובלית, כיפת ברזל עולמית, עם אותם עקרונות של שיתופיות וקישוריות".

"אם למשל", סיכם ראש הממשלה, "אירן תוקפת את תעלות המים בבלגיה, יהיה מאוד קשה לזהות כי זהו אות המבשר על מתקפה. הוא עלול להיבלע כרעש ולא כהתרעה. אבל אם נניח שהם יתקפו את צ'ילה ושלוש דקות לאחר מכן את הודו, אם כל המדינות יחלקו את המידע אחת עם השנייה ניתן יהיה למנוע את המשך המתקפה. כי הרעים בדרך כלל עובדים על ריבוי מתקפות, כי הם רוצים כסף. שיתוף המידע יביא לאבחנה טובה יותר בין אותות שהם התראה ובין רעשים. כך, עם הרשת הגלובלית, בזמן אמת ניתן יהיה לזהות, להרתיע, לחקור ולפתח חיסון – בתוך דקות. אנו מזמינים אך כל המדינות הטובות בעולם לאחד כוחות באופן גלובלי בהגנת סייבר ולבנות כיפת ברזל עולמית. חשוב שנעבוד ביחד. ישראל נמצאת בקשר עם מדינות רבות וכעת אנחנו רוצים לעלות מדרגה ולספק הגנה בסייבר לכולן. אם תילחם לבד – תפסיד, תילחם יחד – תנצח".

מעריב

בנט בכנס הסייבר השנתי: "תקיפות הסייבר הן איום קיומי על ישראל והעולם"

רה"מ נשא דברים בכנס ואמר כי כדי להתמודד עם האיום צריך "לתת לתעשיה לפרוח, שום מדינה או ממשלה לבדה יכולות לפתור את הבעיה הזו. זה חייב להיות מאמץ פרטי וממשלתי"

מאת: סתיו נמר

ברקע פרשת NSO: ראש הממשלה נפתלי בנט התארח היום (רביעי) בכנס שבוע הסייבר השנתי באוניברסיטת תל אביב ואמר כי תקיפות הסייבר "הן איום קיומי על מדינת ישראל והעולם". בנט הוסיף כי כדי להתמודד עם האיום צריך "לתת לתעשיה לפרוח, שום מדינה לבדה שום ממשלה או ממשלות יכולות לפתור את הבעיה הזו"."המים שלנו, חשמל, האוכל, המטוסים, הרכבים נתונים תחת מתקפה. ולמה? מכיוון שזה קל, מעולם לא היה קל יותר. בעבר, אם מדינה 'רעה' הייתה מעוניינת לתקוף, היא הייתה צריכה לעשות זאת באמצעות מטוסי קרב, אך היום היא יכולה לתקוף באמצעות סייבר, וכל מה שהיא צריכה זה מוחות וקו אינטרנט. עד כדי כך קל", הוסיף לדבר על האיום הקיברנטי.

ראש הממשלה הסביר כי "אנחנו צריכים את המגזר הפרטי כדי לפתור את הבעיה, וזה חייב להיות מאמץ פרטי וממשלתי משולב, כי המוחות לא נמצאים רק בממשלה. בישראל יש לנו אוסף אנשים מאוד חכמים שבגיל צעיר נכנסים לצבא ולמודיעין קבלים סמכויות עצומות".בנט המשיך לפרוס את משנתו, ואמר בסוף דבריו כי "חדשנות היא משהו שאי אפשר להנחות או לפקד עליו, אי אפשר לחוקק חוק שיש 'לחדש' פעמיים ביום. כל מה שאנו יכולים לעשות זה לאפשר למפגשים האלו לקרות ולתת לרעיונות לזוז. ההייטק בישראל מתפוצץ וההגנת סייבר מתפוצצת גם כן".יגאל אונא ראש מערך הסייבר הלאומי, דיבר גם הוא בכנס והציג נתונים מסקר חדש של הלמ"ס ומערך הסייבר הלאומי, אשר מהם עולה כי אחד מכל חמישה עסקים בישראל (18%) חווה תקיפת סייבר. מתוך העסקים שדיווחו שחוו תקיפה, לחמישית מהם נגרם נזק כלשהו למערכות כתוצאה מהתקיפה, שהתבטא בחוסר זמינות מידע, דלף מידע, או הרס והשחתה של מערכות המידע. "החורף כבר כאן – כך מראים המספרים והם ממשיכים לעלות. כמה קר זה יהיה, עוד נראה, אבל אנחנו כבר שם", אמר אונא.

PC אנשים ומחשבים

גנץ מגבה את NSO: "ישראל מתירה יצוא סייבר רק למטרות לגיטימיות"

שר הביטחון ציין, בעקבות התחקיר נגד NSO, ש-"המדינה מתירה יצוא של מוצרי סייבר אך ורק למניעה וחקירה של פשעים וטרור" - והרי כל עסקה של חברות כמותה בחו"ל מפוקחת על ידי המשרד● גנץ הבטיח שישראל תישאר המדינה החזקה באזור גם בתחום הסייבר

מאת: יוסי הטוני

חברת הסייבר ההתקפי הישראלית NSO סופגת בימים האחרונים ביקורות חריפות מרחבי העולם, בעקבות תחקיר עיתונאי רחב היקף שלפיו התוכנה שלה, פגסוס, משמשת למעקב אחרי פעילי זכויות אדם, עיתונאים ופוליטיקאים. בתקשורת העולמית מפרסמים שלל כותרות שליליות על החברה, האיחוד האירופי מגנה את מעשיה הנטענים – ולעומת זאת שר הביטחון, בני גנץ, מגבה אותה.

כחברה שמייצרת פתרונות סייבר, העסקאות של NSO בחו"ל מחויבות להיות מאושרות על ידי אגף הפיקוח על היצוא הביטחוני במשרד הביטחון. אלא שעל פי הממצאים החדשים, נראה שלמרות זאת, פגסוס הגיעה לידיים שכדאי שלא הייתה מגיעה אליהן.

לפי התחקיר נגד NSO, שמשותף ל-17 ארגוני חדשות מכובדים בעולם, פגסוס שימשה לפריצה לעשרות טלפונים חכמים של פעילי זכויות אדם, עיתונאים ואנשי עסקים, ואף הייתה מעורבת בחיסולו של העיתונאי מתנגד המשטר הסעודי ג'מאל חשוקג'י. אתמול (ג') פורסם כי בין המדינאים שנכללים ברשימה זו נמצאים נשיא צרפת, עמנואל מקרון, מלך מרוקו, מוחמד השישי, וראש הממשלה לשעבר של לבנון, סעד אל חרירי. את התחקיר הבינלאומי הוביל אמנסטי אינטרנשיונל, בשיתוף ארגון פורבידן סטוריז, והיו שותפים לו יותר מ-80 עיתונאים מ-10 מדינות.

מעריב

גנץ הגיב לתחקיר על NSO: "לומדים את המידע"

שר הביטחון נאם בכנס באוניברסיטת ת"א והגיב לתחקיר, בו הואשמה חברת NSO כי סיפקה לממשלות שונות תוכנה לריגול אחר עיתונאים. בנוסף, השר התייחס לירי הרקטות מלבנון

מאת: טל לב רם

שר הביטחון בני גנץ הגיב היום (שלישי) לתחקיר על חברת NSO, אשר בו עלתה טענה כי החברה סיפקה יכולות ריגול לממשלות שונות, אשר השתמשו בו עבור ריגול אחר עיתונאים. בדבריו אמר גנץ כי "כמדיניות, מדינת ישראל מאשרת את ייצוא הסייבר למדינות בלבד, רק לשימוש חוקי ולמניעת פשעים וחקירת טרור. מדינות שרוכשות את המערכות הללו צריכות לעמוד בעקרונות אלו וכעת אנו לומדים את המידע החדש בנושא". את הדברים אמר גנץ בנאומו בכנס בשבוע הסייבר השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ.

שר הביטחון מסר כי "ישראל, כדמוקרטיה מערבית ליברלית, מפקחת על יצוא מוצרי סייבר לפי חוק הפיקוח על הייצוא הביטחוני ובהתאם למשטרי פיקוח בין-לאומיים". גנץ אף התייחס לנושא התקפות הסייבר על ישראל וטען כי "בשנים האחרונות חלה עלייה משמעותית במספר ההתקפות שביצעו גורמים עוינים, כולל איראן ושלוחותיה, המבקשים לגשת למערכות התקשוב של התשתית הלאומית של ישראל".

עוד הוא הוסיף כי "לנוכח העלייה הזו - מכמה התקפות בודדות לעשרות התקפות בשנה - ישראל הוכיחה את היכולת לפתח את חוסנה, את היתרון הטכנולוגי שלה ואת היתרון האיכותי שלה באזור. ישראל פועלת באופן רציף להגנה מפני מתקפות סייבר. במאי 2019, כחלק מהסכסוך המתמשך של ישראל עם ארגוני הטרור ברצועת עזה, ביצעה ישראל לראשונה מתקפה קינטית על הבניין בו ישב פיקוד הסייבר של חמאס. במהלך מבצע "שומר החומות", פגענו בראש פיקוד הסייבר של חמאס, ג'ומעה טחלה. כמו כן זיהינו ופגענו בכמה תוקפי סייבר, ציוד ותשתיות אשר שימשו את פיקוד הסייבר של חמאס".

בנאומו התייחס גנץ גם לירי הרקטות משטח לבנון לישראל: "יש לנו אינטרס בלבנון יציבה ומשגשגת כלכלית. לצערנו, המצב בלבנון הולך ומחמיר, וחיזבאללה וארגוני טרור נוספים פועלים נגד האינטרסים של העם הלבנוני. הגבנו בלילה, ונמשיך להגיב ולפעול בזמן ובמקום הנכונים מול כל הפרה של ריבונות ישראל".

"מדינת לבנון היא האחראית לנעשה משטחה. אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטארי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות והפרת ריבונות ואני קורא לקהילה הבינלאומית לפעול להשבת היציבות בלבנון", סיכם השר.

מוקדם יותר השבוע פורסם בעיתון "הגארדיאן" התחקיר האמור, אשר חשף כי התוכנה "פגאסוס" של חברת הסייבר הישראלית NSO אפשרה לממשלות ברחבי העולם, בהן סעודיה, הונגריה ומקסיקו, לבצע מעקב אחרי יותר עשרות אלפי מספרי טלפון, ובהם יותר מ-180 עיתונאים.

לאחר פרסום התחקיר הודיעה התביעה הראשית של צרפת כי היא תפתח בחקירה בעניין הפרשה. החקירה נפתחה לאחר שאתר חדשות צרפתי הגיש תלונה לפיה שירות הביון של מרוקו השתמש בתוכנה כדי לעקוב אחר שניים מעובדיו, "על מנת להשתיק עיתונות עצמאית במרוקו ולדעת מה אנו חוקרים".

יש לציין ש-NSO הכחישה את ממצאי התחקיר וטענה שהוא מלא בעובדות לא נכונות. בין היתר, היא טענה שלא מדובר ב-50 אלף מכשירי סמארטפון וכי המאגר שממנו נשאבו הנתונים שמצוינים בתחקיר הוא מאגר חופשי ופתוח באינטרנט. בנוסף, החברה חזרה על טענתה שתוכנת פגסוס מסייעת במלחמה בטרור ובמניעתו – ובכך מצילה חיים.

בדברים שנשא אתמול במסגרת שבוע הסייבר באוניברסיטת תל אביב אמר גנץ כי "אנחנו מודעים לפרסומים האחרונים בנושא השימוש במערכות שפותחו על ידי חברות סייבר ישראליות מסוימות. ישראל, כדמוקרטיה מערבית ליברלית, עורכת בקרה על יצוא של מוצרי סייבר בהתאם לחוק הפיקוח על היצוא הביטחוני שלה, ועומדת בתקנות בקרת היצוא הבינלאומיות. כמדיניות, מדינת ישראל מתירה יצוא של מוצרי סייבר אך ורק לממשלות, אך ורק לשימוש חוקי ובלעדי – למטרות מניעה וחקירה של פשעים וטרור. על המדינות הרוכשות מערכות אלה לעמוד בהתחייבויותיהן לדרישות (הנלוות לרכישה – י"ה) אלה. אנחנו לומדים כעת את המידע המתפרסם בנושא".

"שיתוף הפעולה בסייבר מאפשר להגן על האינטרסים הלאומיים"

גנץ דיבר על מעמדה של ישראל בעולם הסייבר והעלה על נס את שיתופי הפעולה בין גופי הביטחון השונים בתחום. "ישראל היא מעצמת סייבר. בדיוק כמו בתחומים רבים אחרים, השגנו מעמד זה מתוך צורך – והרי הצורך הוא דלק ומניע החדשנות. הפכנו למובילים בתחום בזכות שיתוף הפעולה החריג בין המוסדות הרלוונטיים השונים – צה"ל, המוסד, המועצה לביטחון לאומי, מערך הסייבר הלאומי ומערכת הביטחון", אמר. "שיתוף פעולה זה, לרבות עם גופים ממשלתיים נוספים והמגזר הפרטי, מאפשרים לנו להתמודד עם איומים ולהגן על התשתית והאינטרסים הלאומיים שלנו. כולם מהווים מגן מפני כל מי שמבקש לפגוע בנו בתחום הסייבר".

"הסייבר הוא תחום חדש ומתפתח. זהו מרחב שמתווסף כיום לאלה של הים, האוויר והיבשה. מומחי הסייבר שלנו הופכים להיות בעלי תפקיד מרכזי יותר ויותר בשדה הקרב. הם רואים הכול – ובכל זאת נשארים בלתי נראים", ציין שר הביטחון.

הוא אמר כי "בשנים האחרונות חלה עלייה משמעותית במספר המתקפות שביצעו גורמים עוינים, כולל איראן ושלוחותיה, שמבקשים לגשת למערכות התקשוב של התשתית הלאומית של ישראל. לנוכח העלייה הזו – מכמה מתקפות בודדות לעשרות בשנה – ישראל הייתה גמישה והדגימה את התקדמותה הטכנולוגית והאיכותית".

גנץ ציין ש-"ישראל פועלת באופן רציף להגנה מפני מתקפות סייבר" והביא כדוגמה את "ההשבתה הקינטית" הראשונה שביצעה ישראל נגד גורם טרור – לפני כשנתיים. הקורבן היה בניין שאכלס את פיקוד הסייבר של החמאס. "המבצע נערך בעקבות פעילויות שמטרתן למנוע פגיעה בתשתיות הישראליות במרחב הסייבר, כפי שניסו לעשות מחבלי הסייבר של החמאס, בהנחיית איראן", אמר. הוא מנה כמה מהפעילויות שצה"ל ביצע בתחום הסייבר במהלך מבצע שומר החומות: "חיסלנו את ג'מעה טחלה, ראש מערך הסייבר של החמאס, ופגענו בכמה תוקפי סייבר, ציוד ותשתית שקשורים לפיקוד הסייבר של הארגון. המסר שלנו ברור: תהיה זו רקטה או מקלדת – לא נסבול מישהו שמאיים על האומה שלנו".

"העברת התקשוב לנגב – השקעה הכרחית לעתידנו"

"נדרשת עבודה קשה מאוד על מנת לשמור על היתרון שלנו בתחום הסייבר", אמר גנץ. "עבודה זו מתחילה בבית, וכוללת יצירת אקו-סיסטם שלם, מצפון ועד דרום. העברת בסיסי התקשוב והמודיעין של צה"ל לנגב היא חלק מההשקעות ההכרחיות לעתידנו. על מנת לצייד את צה"ל בחיילים המצטיינים בתחום הסייבר, כדי שהם 'ישמרו על גבולותינו המקוונים', עלינו לחבר בין המגזרים הפרטי, הביטחוני והאקדמי. בנוסף, אנחנו עובדים עם בעלי בריתנו בעולם כדי לחלוק מידע ומומחיות ולפתח יכולות חדשות. העבודה שיש לנו עם ארצות הברית ומדינות אחרות מעצימה אותנו. ישראל תמשיך לעבוד עם ארצות הברית ועם מדינות נוספות על מנת להבטיח שהיתרון הצבאי איכותי שלה יישמר גם במרחב הסייבר".

"לפנינו אתגרים רבים", סיכם שר הביטחון. "אני צופה שבשנים הקרובות יהיה צורך להשתמש בכלי סייבר בהיקף נרחב כדי להגן על האינטרסים החיוניים ועל הביטחון הלאומי של ישראל. נמשיך לשתף פעולה עם כל הארגונים הרלוונטיים ולפתח את היכולות שלנו ונחזק את מומחי הסייבר שלנו, עם חינוך והכלים הדרושים להם. בדיוק כפי שישראל ניצחה במלחמות השונות ובמבצעים הצבאיים, היא תצליח להתמודד גם מול איומי הסייבר החדשים. ישראל תישאר המדינה החזקה ביותר באזור – גם בתחום הסייבר".

גלובס

בני גנץ על NSO: "לומדים את המידע שפורסם בנושא"

שר הביטחון הגיב לראשונה על ההאשמות שהופנו כלפי NSO ואמר: "כמדיניות, מדינת ישראל מתירה לייצא מוצרי סייבר אך ורק לממשלות, רק לשימוש חוקי ואך ורק לשימוש במניעת פשע וטרור"

מאת: אסף גלעד

שר הביטחון בני גנץ הגיב לראשונה על ההאשמות שהופנו כלפי חברת NSO הישראלית במסגרת סדרת התחקירים שערכו עיתונים מובילים בעולם ביוזמת ארגון אמנסטי ופורבידן סטוריז. "ישראל היא דמוקרטיה מערבית ליברלית השולטת בייצוא מוצרי סייבר ועומדת בתקנות הייצוא הבינלאומיות. כמדיניות, מדינת ישראל מתירה לייצא מוצרי סייבר אך ורק לממשלות, רק לשימוש חוקי ואך ורק לשימוש במניעת פשע וטרור. כל היצואנים חייבים לציית להסכמים אלה. אנו לומדים כעת את המידע שפורסם בנושא זה".

את הדברים אמר גנץ במסגרת שבוע הסייבר הנערך באוניברסיטת תל אביב. אמש, מסר משרד הביטחון כי "ככל שמתברר כי נעשה שימוש בניגוד לתנאי הרשיון או בניגוד להצהרות מטעם המדינות הרוכשות, ננקטים הליכים מתאימים".

במסגרת סדרת התחקירים על NSO שפורסמו בעיתונים כגון הגרדיאן הבריטי, הוושיגנטון פוסט ולה-מונד, נקשרה טכנולוגיית הסייבר ההתקפי של NSO, תוכנת הריגול פגסוס, למעקב אחר עיתונאים, פעילי זכויות אדם, מתנגדי משטר ופוליטיקאים שביצעו רשויות בשורה מדינות בהן הודו, הונגריה, אזרבייג'ן וסעודיה. NSO טענה כי כל הפרה של זכויות אדם על ידי רשות כלשהי זוכה להפסקת ההסכם עמה וכי היא עומדת בתנאי הרגולציה של משרד הבטחון לייצוא נשק בטחוני.

גם האיחוד האירופי גינה אמש את החברה הישראלית. "חופש העיתונות והמידע הוא אחד מערכי הליבה שלנו באיחוד, והדבר בלתי מתקבל על הדעת, אם הוא אכן קרה", אמרה אורסולה ון-דר-ליין נשיאת האיחוד.

אמש צייץ פעיל זכויות האדם אדוארד סנודן דברים קשים כנגד NSO ונגד תעשיית הסייבר ההתקפי: "זו תעשייה שאסור לה להתקיים. הם לא מייצרים חיסונים, הדבר היחיד שהם מוכרים הוא הווירוס." (מייסדי NSO הקימו חברה המגינה על מכשירים מפני טכנולוגיות פולשניות בשם קיימרה- א"ג). אם לא נעשה משהו כדי לעצור מכירה של טכנולוגיה שכזו, אלה לא הולכים להיות רק 50 אלף מספרי טלפון כמטרות, אלה הולכים להיות 50 מיליון מטרות, וזה עשוי לקרות מהר יותר מכפי שחשבנו. כפי שאיננו מרשים לשוק הפרטי לסחור בנשק גרעיני, הדרך היחידה להגן על עצמינו היא לאסור את המסחר בטכנולוגיה שכזו."

הקול של העם 20

גנץ על ירי הרקטות משטח לבנון: "הגבנו בלילה ונמשיך להגיב"

שר הביטחון, בני גנץ, נאם היום – על הנושאים הביטחוניים, במסגרת שבוע הסייבר הבינלאומי של אוניברסיטת תל אביב: "המצב בלבנון הולך ומחמיר"

מאת: רועי שושה

בני גנץ, נאם היום (ג'), על כמה נושאים ביטחוניים, במסגרת שבוע הסייבר הבינלאומי של אוניברסיטת תל אביב, על ירי הרקטות משטח לבנון אמר: "למדינת ישראל יש אינטרס בלבנון יציבה ומשגשגת כלכלית. לצערנו, המצב בלבנון הולך ומחמיר, וחיזבאללה וארגוני טרור נוספים פועלים נגד האינטרסים של העם הלבנוני. הגבנו בלילה, ונמשיך להגיב ולפעול בזמן ובמקום הנכונים מול כל הפרה של ריבונות ישראל.

מדינת לבנון היא האחראית לנעשה משטחה. אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטארי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות והפרת ריבונות ואני קורא לקהילה הבינלאומית לפעול להשבת היציבות בלבנון."

על מבצע מבצע "שומר החומות" אמר כי: "פגענו בראש פיקוד הסייבר של חמאס, ג'ומעה טחלה. כמו כן זיהינו ופגענו בכמה תוקפי סייבר, ציוד ותשתיות אשר שימשו את פיקוד הסייבר של חמאס. המסר שלנו הוא ברור – תהיה זו רקטה או מקלדת – לא נסבול איום על אזרחי ישראל."

על היתרי הייצוא הביטחוני ממשרד הביטחון: "אנו מודעים לפרסומים האחרונים על שימוש במערכות שפותחו על ידי חברות סייבר ישראליות מסוימות. ישראל, כדמוקרטיה מערבית ליברלית, מפקחת על יצוא מוצרי סייבר לפי חוק הפיקוח על הייצוא הביטחוני ובהתאם למשטרי פיקוח בין-לאומיים.

כמדיניות, מדינת ישראל מתירה ייצוא של מוצרי סייבר מפוקחים אך ורק לממשלות, אך ורק לשימוש חוקי, וספציפית למטרות מניעה וחקירה של פשעים וטרור. על המדינות הרוכשות מערכות אלה לעמוד בהתחייבויותיהן לדרישות אלה. אנו לומדים כעת את המידע המתפרסם בנושא."

מוקד החדשות של ישראל
כל החדשות במקום אחד!

גנץ הגיב לתחקיר על NSO: "לומדים את המידע"

שר הביטחון נאם בכנס באוניברסיטת ת"א והגיב לתחקיר, בו הואשמה חברת NSO כי סיפקה לממשלות שונות תוכנה לריגול אחר עיתונאים.

שר הביטחון בני גנץ הגיב לראשונה על ההאשמות שהופנו כלפי חברת NSO הישראלית במסגרת סדרת התחקירים שערכו עיתונים מובילים בעולם ביוזמת ארגון אמנסטי ופורבידן סטוריז. "ישראל היא דמוקרטיה מערבית ליברלית השולטת בייצוא מוצרי סייבר ועומדת בתקנות הייצוא הבינלאומיות. כמדיניות, מדינת ישראל מתירה לייצא מוצרי סייבר אך ורק לממשלות, רק לשימוש חוקי ואך ורק לשימוש במניעת פשע וטרור. כל היצואנים חייבים לציית להסכמים אלה. אנו לומדים כעת את המידע שפורסם בנושא זה".

את הדברים אמר גנץ במסגרת שבוע הסייבר הנערך באוניברסיטת תל אביב. אמש, מסר משרד הביטחון כי "ככל שמתברר כי נעשה שימוש בניגוד לתנאי הרשיון או בניגוד להצהרות מטעם המדינות הרוכשות, ננקטים הליכים מתאימים".

במסגרת סדרת התחקירים על NSO שפורסמו בעיתונים כגון הגרדיאן הבריטי, הוושיגנטון פוסט ולה-מונד, נקשרה טכנולוגיית הסייבר ההתקפי של NSO, תוכנת הריגול פגסוס, למעקב אחר עיתונאים, פעילי זכויות אדם, מתנגדי משטר ופוליטיקאים שביצעו רשויות בשורה מדינות בהן הודו, הונגריה, אזרבייג'ן וסעודיה. NSO טענה כי כל הפרה של זכויות אדם על ידי רשות כלשהי זוכה להפסקת ההסכם עמה וכי היא עומדת בתנאי הרגולציה של משרד הבטחון לייצוא נשק בטחוני.

גם האיחוד האירופי גינה אמש את החברה הישראלית. "חופש העיתונות והמידע הוא אחד מערכי הליבה שלנו באיחוד, והדבר בלתי מתקבל על הדעת, אם הוא אכן קרה", אמרה אורסולה ון-דר-ליין נשיאת האיחוד.

אמש צייץ פעיל זכויות האדם אדוארד סנודן דברים קשים כנגד NSO ונגד תעשיית הסייבר ההתקפי: "זו תעשייה שאסור לה להתקיים. הם לא מייצרים חיסונים, הדבר היחיד שהם מוכרים הוא הווירוס." (מייסדי NSO הקימו חברה המגינה על מכשירים מפני טכנולוגיות פולשניות בשם קיימרה- א"ג). אם לא נעשה משהו כדי לעצור מכירה של טכנולוגיה שכזו, אלה לא הולכים להיות רק 50 אלף מספרי טלפון כמטרות, אלה הולכים להיות 50 מיליון מטרות, וזה עשוי לקרות מהר יותר מכפי שחשבנו. כפי שאיננו מרשים לשוק הפרטי לסחור בנשק גרעיני, הדרך היחידה להגן על עצמינו היא לאסור את המסחר בטכנולוגיה שכזו."

News1 מחלקה ראשונה

"ישראל ביצעה מתקפה קינטית על בניין פיקוד הסייבר של חמאס"

המתקפה בוצעה בעקבות פעילויות שמטרתן הייתה לפגוע בתשתיות הישראליות במרחב הסייבר גנץ הוסיף: ישראל חווה עליה משמעותית במספר התקפות הסייבר - מכמה התקפות בודדות לעשרות בשנה

"בשנים האחרונות חלה עלייה משמעותית במספר ההתקפות שביצעו גורמים עוינים, כולל אירן ושלוחותיה, המבקשים לגשת למערכות התקשוב של התשתית הלאומית של ישראל. לנוכח העלייה הזו - מכמה התקפות בודדות לעשרות התקפות בשנה - ישראל הוכיחה את היכולת לפתח את חוסנה, את היתרון הטכנולוגי שלה ואת היתרון האיכותי שלה באזור". כך אמר (יום ג', 20.7.21) שר הביטחון בני גנץ במסגרת נאומו בכנס הסייבר הבינלאומי של אוניברסיטת תל אביב.

עוד אמר גנץ כי ישראל פועלת באופן רציף להגנה מפני מתקפות סייבר, וציין כי "במאי 2019, כחלק מהסכסוך המתמשך של ישראל עם ארגוני הטרור ברצועת עזה, ביצעה ישראל לראשונה מתקפה קינטית על הבניין בו ישב פיקוד הסייבר של חמאס. המתקפה בוצעה בעקבות פעילויות שמטרתן הייתה לפגוע בתשתיות הישראליות במרחב הסייבר, כפי שניסו לעשות תוקפי הסייבר של חמאס בהנחיית אירן".

עוד סיפר גנץ: "במהלך מבצע "שומר החומות", פגענו בראש פיקוד הסייבר של חמאס, ג'ומעה טחלה. כמו-כן זיהינו ופגענו בכמה תוקפי סייבר, ציוד ותשתיות אשר שימשו את פיקוד הסייבר של חמאס".

על ירי הרקטות משטח לבנון אמר גנץ: "למדינת ישראל יש אינטרס בלבנון יציבה ומשגשגת כלכלית. לצערנו, המצב בלבנון הולך ומחמיר, וחיזבאללה וארגוני טרור נוספים פועלים נגד האינטרסים של העם הלבנוני. הגבנו בלילה, ונמשיך להגיב ולפעול בזמן ובמקום הנכונים מול כל הפרה של ריבונות ישראל".

"מדינת לבנון היא האחראית לנעשה משטחה. אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטרי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות והפרת ריבונות ואני קורא לקהילה הבינלאומית לפעול להשבת היציבות בלבנון."

בחדרי חרדים

"נמשיך להגיב מול כל הפרה של ריבונות ישראל"

גנץ הוסיף ואמר: "אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטארי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות"

מאת: שי טולדנו

שר הביטחון, בני גנץ, נאם היום במסגרת שבוע הסייבר הבינלאומי של אוניברסיטת תל אביב. בדבריו התייחס גנץ לירי הרקטות משטח לבנון ואמר: "למדינת ישראל יש אינטרס בלבנון יציבה ומשגשגת כלכלית. לצערנו, המצב בלבנון הולך ומחמיר, וחיזבאללה וארגוני טרור נוספים פועלים נגד האינטרסים של העם הלבנוני".

"הגבנו בלילה, ונמשיך להגיב ולפעול בזמן ובמקום הנכונים מול כל הפרה של ריבונות ישראל. מדינת לבנון היא האחראית לנעשה משטחה. אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטארי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות והפרת ריבונות ואני קורא לקהילה הבינלאומית לפעול להשבת היציבות בלבנון".

על ניסיונות של מתקפות סייבר על ישראל אמר: "בשנים האחרונות חלה עלייה משמעותית במספר ההתקפות שביצעו גורמים עוינים, כולל איראן ושלוחותיה, המבקשים לגשת למערכות התקשוב של התשתית הלאומית של ישראל. לנוכח העלייה הזו – מכמה התקפות בודדות לעשרות התקפות בשנה – ישראל הוכיחה את היכולת לפתח את חוסנה, את היתרון הטכנולוגי שלה ואת היתרון האיכותי שלה באזור".

"ישראל פועלת באופן רציף להגנה מפני מתקפות סייבר – במאי 2019, כחלק מהסכסוך המתמשך של ישראל עם ארגוני הטרור ברצועת עזה, ביצעה ישראל לראשונה מתקפה קינטית על הבניין בו ישב פיקוד הסייבר של חמאס. המתקפה בוצעה בעקבות פעילויות שמטרתן הייתה לפגוע בתשתיות הישראליות במרחב הסייבר, כפי שניסו לעשות תוקפי הסייבר של חמאס בהנחיית איראן".

"במהלך מבצע "שומר החומות", פגענו בראש פיקוד הסייבר של חמאס, ג'ומעה טחלה. כמו כן זיהינו ופגענו בכמה תוקפי סייבר, ציוד ותשתיות אשר שימשו את פיקוד הסייבר של חמאס. המסר שלנו הוא ברור – תהיה זו רקטה או מקלדת – לא נסבול איום על אזרחי ישראל".

בין היתר התייחס גנץ להיתרי הייצוא הביטחוני ממשרד הביטחון: "אנו מודעים לפרסומים האחרונים על שימוש במערכות שפותחו על ידי חברות סייבר ישראליות מסוימות. ישראל, כדמוקרטיה מערבית ליברלית, מפקחת על יצוא מוצרי סייבר לפי חוק הפיקוח על הייצוא הביטחוני ובהתאם למשטרי פיקוח בין-לאומיים".

"כמדיניות, מדינת ישראל מתירה ייצוא של מוצרי סייבר מפוקחים אך ורק לממשלות, אך ורק לשימוש חוקי, וספציפית למטרות מניעה וחקירה של פשעים וטרור. על המדינות הרוכשות מערכות אלה לעמוד בהתחייבויותיהן לדרישות אלה. אנו לומדים כעת את המידע המתפרסם בנושא".

ISRAELDEFENSE

ראש מערך הסייבר: אחד מכל חמישה עסקים בישראל חווה תקיפת סייבר

יגאל אונא דיבר בכנס שבוע הסייבר באוניברסיטת ת"א, ואמר כי "החורף כבר כאן, והמספרים ממשיכים לעלות. עוד נראה כמה קר יהיה, אבל אנחנו כבר שם"

"החורף כבר כאן – כך מראים המספרים והם ממשיכים לעלות. כמה קר זה יהיה, עוד נראה, אבל אנחנו כבר שם", כך אמר יגאל אונא, ראש מערך הסייבר הלאומי, בכנס שבוע הסייבר שנערך באוניברסיטת תל אביב.

על פי הנתונים שהציג אונא מסקר חדש של הלמ"ס ומערך הסייבר הלאומי, אחד מכל חמישה עסקים בישראל (18%) חווה תקיפת סייבר. מתוך העסקים שדיווחו שחוו תקיפה, לחמישית מהם נגרם נזק כלשהו למערכות כתוצאה מהתקיפה, שהתבטא בחוסר זמינות מידע, דלף מידע, או הרס והשחתה של מערכות המידע. מהסקר עולה כי התקיפות שכיחות בעיקר בקרב עסקים גדולים (250 עובדים ומעלה): שניים מכל חמישה עסקים גדולים חווה תקיפת סייבר (42%). על פי הדיווחים בסקר, כ-15% מהעסקים הקטנים חוו מתקפת סייבר.

נתונים שהציג אונא מהעולם מראים כי ממוצע תשלום תקיפות כופרה בארה"ב הוא 178,254 דולר וכי התקיפות גורמות להשבתה של 16 יום בממוצע של הארגון. הנתונים נמצאים בעלייה מתמדת מדי שנה. "אנחנו רואים עלייה מדי שנה בחולשות שמתפרסמות בעולם, ורק באפריל האחרון נרשמו 1,400 חולשות. בעקבות כך אנחנו מחזקים במערך הסייבר הלאומי את היחידה להגנה פרואקטיבית", אמר.

אונא הציג את ההצטרפות של המערך התוכנית הבין-לאומית שמפעיל ארגון MITRE לדיווח ולקיטלוג של פגיעויות שהתגלו במוצרים טכנולוגיים, שאישר באחרונה את המערך כגוף מוסמך לרישום פגיעויות וחשיפות נפוצות (CVE) ברשימה העולמית:

"מאז שהצטרפנו לפני כשבועיים, התקבלו במערך עשרות דיווחים שחלקם נמצאים בתהליך רישום עולמי. בנוסף, בקרוב נשיק את התוכנית הרחבה בנושא שתכלול יכולות איתור וניטור חולשות במרחב הישראלי על מנת לסגור אותן מבעוד מועד ולמנוע תקיפות", אמר והוסיף כי מערך הסייבר השיק אתמול את "הגרסא החדשה של תורת ההגנה, המדריך והבסיס לבניית הגנת סייבר בארגון, בדגש על ראיית התוקף ובניית ההגנה מותאמת".

ISRAELDEFENSE

ראש אמ"ן: ישראל נמצאת תחת איום סייבר תמידי, התקפיות תענה בהתאם

אלוף הימן דיבר בכנס הסייבר הבינלאומי באוניברסיטת תל אביב בו קיבל את פרס "הסוס הטרויאני" בשם צה"ל

ראש אמ"ן, אלוף תמיר הימן, השתתף אתמול (ג') בכנס הסייבר הבינלאומי באוניברסיטת ת"א, בו קיבל בשם צה"ל את פרס "הסוס הטרויאני". בנאומו, התייחס האלוף לאיום הסייבר התמידי על ישראל.

"במסגרת המבצע האחרון בעזה, מידע שנאסף ממגוון מקורות - בין היתר ממרחב הסייבר, הותך יחד באמצעות יכולות עיבוד מתקדמות, בינה מלאכותית ולמידת מכונה לכדי תפוקות מבצעיות. דבר זה אפשר לצה"ל לתפקד טוב יותר, מהיר יותר, ועם פחות אבדות בחיי אדם", אמר אלוף הימן.

"אני רוצה להתייחס גם לאיומים היומיומיים על מדינת ישראל במימד הסייבר. ישראל נמצאת תחת איום תמידי במימד הסייבר, ומתקפות מבוצעות לעיתים נגדה. אנו מצליחים להתמודד עם מרבית האיומים באמצעות יכולות הגנה מתקדמות".

"כמו בממדי הלחימה אחרים, הגנה לבד אינה מספקת. יש לנקוט צעדים נוספים בכדי לשמר את עליונות ישראל אל מול אויבנו. אלו שתוקפים את ישראל באוויר, בים, ביבשה או בסייבר צריכים להבין את הסיכון שהם לוקחים. כפי שהם נוכחים לראות פעם אחר פעם, התקפיות תיענה בהתאם".

מעריב

ראש אמ"ן חשף: אמצעי סייבר מתקדמים הביאו תפוקות מבצעיות ב"שומר חומות"

האלוף תמיר הימן נשא דברים בכנס הסייבר הלאומי שהתקיים, במסגרתו התייחס גם למתקפות הסייבר בארץ, ואמר: "הגנה לבד אינה מספקת. יש לשמר את עליונות ישראל אל מול אויבנו"

מאת: טל לב רם

במסגרת כנס שבוע הסייבר הלאומי השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ, ראש אמ"ן, אלוף תמיר הימן, התייחס למלחמות הסייבר ולשימוש של צה"ל במומחיות שונות בתחום על מנת לפעול במהלך מבצע "שומר חומות. בכנס קיבל ראש אגף המודיעין את פרס "הסוס הטרויאני" בשם צה"ל.

"במסגרת המבצע האחרון בעזה", אמר ראש אמ"ן אלוף תמיר הימן, "מידע שנאסף ממגוון מקורות - בין היתר ממרחב הסייבר, הותך יחד באמצעות יכולות עיבוד מתקדמות, בינה מלאכותית ולמידת מכונה לכדי תפוקות מבצעיות. דבר זה אפשר לצה"ל לתפקד טוב יותר, מהיר יותר, ועם פחות אבדות בחיי אדם".

ראש אמ"ן התייחס גם לאיומים היומיומיים על מדינת ישראל בממד הסייבר. "ישראל נמצאת תחת איום תמידי בממד הסייבר, ומתקפות מבוצעות לעיתים נגדה. אנו מצליחים להתמודד עם מרבית האיומים באמצעות יכולות הגנה מתקדמות. כמו בממדי הלחימה אחרים, הגנה לבד אינה מספקת. יש לנקוט צעדים נוספים בכדי לשמר את עליונות ישראל אל מול אויבנו", אמר אלוף הימן.

"אלו שתוקפים את ישראל באוויר, בים, ביבשה או בסייבר צריכים להבין את הסיכון שהם לוקחים. כפי שהם נוכחים לראות פעם אחר פעם, התקפיות תיענה בהתאם", סיכם ראש אמ"ן.

ynet
ידיעות אחרונות

ראש אמ"ן: "ישראל נמצאת תחת איום תמידי במימד הסייבר"

ראש אמ"ן, האלוף תמיר הימן, אמר בשבוע הסייבר הלאומי באוניברסיטת תל אביב, שבו קיבל את פרס "אות יקיר הסייבר" בשם צה"ל, כי "במסגרת המבצע האחרון בעזה, מידע שנאסף ממגוון מקורות - בין היתר ממרחב הסייבר, הותך יחד באמצעות יכולות עיבוד מתקדמות, בינה מלאכותית ולמידת מכונה לכדי תפוקות מבצעיות". לדבריו, "דבר זה אפשר לצה"ל לתפקד טוב יותר, מהיר יותר ועם פחות אבדות בחיי אדם". על איומי הסייבר אמר הימן: "ישראל נמצאת תחת איום תמידי במימד הסייבר, ומתקפות מבוצעות לעיתים נגדה. אנו מצליחים להתמודד עם מרבית האיומים באמצעות יכולות הגנה מתקדמות". הימן הוסיף: "כמו במימדי הלחימה אחרים, הגנה לבד אינה מספקת. יש לנקוט בצעדים נוספים כדי לשמר את עליונות ישראל אל מול אויבנו".

מקור ראשון

רוני רימון

החוליה החלשה

לא יעשה טעות פעם נוספת. שר הביטחון בני גנץ בכנס הסייבר הבינלאומי של אוניברסיטת תל אביב. צילום: טל עוז / משרד הביטחון

מידי כמה ימים התקשורת הישראלית עיסקת בשאלת סיכויי הממשלה הנוכחית, ממשלת בנט, לשרוד. התקשורת, כהרגלה, מציינת את חולשות הממשלה, את הכישלונות בהצבעות, את הסעות של יו"ר הכנסת ח"כ מיקי לוי וכו'. התקשורת צודקת, ממשלת בנט היא ממשלה חלשה, כי קשה להסתיר את חילוקי הדעות בין שמונת חבריה. אין נושא אחד, כמעט, בו כולם בקואליציה מסכימים אחד עם השני. כל אחד ממרכיבי הקואליציה יכול בקלות להפיל את הממשלה, כי לכל אחד יש אג'נדה, סדר יום, משלו וברוך השם בקואליציה הנוכחית ישנם 8 מפלגות... וקשה, קשה ביותר, לנהל כזו קואליציה, ביודאי שבוודאי אם לא נשלח לה חומר כלשהו.

אחד האנשים הכי מתוסכלים במדינה הוא בני גנץ. גנץ הוא האיש שברצינות אין לבנט קואליציה, וברצונו ערך יותר הוא עצמו יכול להיבחר לראשות הממשלה בממשלה יחד עם נתניהו. הבעיה של גנץ היא שאם הוא ילך קדם עם ביבי - זה יהיה הסוף התדמיתי שלו בישראל. גנץ הפוף חזק מאוד על כך שהסכים ללכת עם שיטותיו בבחירות בשנת 2019 כמחזמני. הוא הפסיד בגדול את דעת הקהל. עד שזו סלחה לו והוא התאושש. אבל, אם עכשיו גנץ נוטש את ממשלת השינוי - זה לא יסולח לו בקהל! הוא. נכון, הוא יהיה ראש ממשלה, אבל לא יהיה לו שום בסיס אוהדים. אגב, לא בטוח שכל הח"כים שלו ילכו איתו, וגם כך לנתניהו, סמוטריץ והחרדים ישנם רק 52 מנדטים ועם גנץ הם מגיעים רק ל- 60. אה, ושוב הגענו לשיקלי, שיהיה הח"כ ה 61... או מה שיקרה? הערכה שלי - גנץ יישאר היכן שהוא עכשו ו"יסתפק" בתפקיד שר הביטחון. תפקיד מכובד לכל הדעות.

הר הבית בידינו?

"הר הבית בידינו" - זו הייתה קריאתו של משה גרוֹ משחרר ירושלים במלחמת ששת הימים. עברו 54 שנים ולא ברור בכלל שהר הבית באמת בידינו. נראה שהמוסלמים שולטים בו הרבה יותר מאשר היהודים. רוצים הוכחה: חברי כנסת יהודיים שביקשי לעלות השבוע להר הבית סרבו. למי כן ניתנה כניסה? לח"כ אחמד טיבי. פעם אחרי פעם אנחנו מתגלים כחסרי חוליות. אם קיימת הנחיה של קצין הכנסת שאין להתיר כניסת חב"ים להר הבית, אלא לאחר תיאום מראש - יש לכבד הנחיה זו. תגובת המשטרה לפיה כדי להמנע ממהומות הפעיל מפקד המחוז שיקול דעת - היא בדיוק המתכון ללחץ נוסף על ממשלת ישראל לבצע עוד ועוד ויתורים.

מתי יהיה לנו עמוד שידרה כמו שצריך ולפיו הממשלה תקבל החלטה ותעמוד בה גם אם המצב אינו פשוט. אי אפשר כל הזמן להיכנע. קניית השקט (?) על ידי ויתורים חוזרים ונשנים - טיבה להקופה קצרה בלבד. לטווח הארוך - הממשלה חייבת להיות יותר עמידה.

גלידה ציונית

ועכשיו אי אפשר בלי קצת גלידה. רשת בן אנד ג'רִיס הכריזה כי לא תאפשר למכור בעתיד גלידות מתוצרתה בשטחי יהודה ושומרון. סוגיה בעלת כמה וכמה פנים. ראשית, נתחיל במילה סובה - לבעלי הנציגות הישראלית של הרשת, אבי זינגר. הוא התייצב אל מול פני האומה והסביר במילים פשוטות שהחלטת החברה האם בארה"ב היא תוֹלדה של סירובו העיקש ללכת למולך של חרם על תושבי יהודה ושומרון. התוצאה הייתה שהחברה החליטה לסיים איתו את ההתקשרות בעוד שנה וחצי, לאחר למעלה מ-30 שנה בהן שימש כזכיין הרשת בישראל.

פן נוסף הוא כמובן קריאתם של פוליטיקאים רבים להחרים את הרשת בישראל. לדעתי, הפוך לגמרי. הרי הזכיין הישראלי נלחם נגד ההנהלה העולמית של הרשת. יתרה מזאת הוא מעסיק למעלה ממאה עיבדים בישראל. או את מי נחרים? את האדם שנלחם נגד החרם? את האדם שהיה לי אימץ לא להכנע? נהפוך הוא - צריך דווקא לדכדש יותר בן אנד ג'רִיס בשנה חצי הקרובות עד לסיום הזיכיון של אבי זינגר בישראל. אגב, ניחוש שלי - הסוגיה תיפתר. בן אנד ג'רִיס ימשיכו למכור בירוש והחרם יבוטל. זו רק שאלה של זמן...

חדשות מעודדות

אין ספק שמספר הנוגדנים בגופם של המחוסנים פוחת. איך אני יודע? אני ורעייתי יכולים לשמש כמדגם של שני אנשים. ביצענו בדיקות סרולוגיות לאחר החיסון בהדרש ינואר ופעם שניה - עכשיו. ואכן מספר הנוגדנים עדיין נמצא מעל המינימום, אבל פחת בכ-50%. לדאוג? לא לדאוג? אני מנסה לקחת את הקורונה, גם מזן החדש, בפרופורציה. כלומר, לא ללכת דווקא למקומות המונים, כמו אירועי ספורט וכדו' אבל, מצד שני לא להימנע מפגישות מקצועיות או משפחתיות.

החדשות הטובות בינתיים הן שהקורונה החדשה, כמעט ואינה מפילה חללים. גם מספר החולים קשה קטן, נכון יהיו נדבקים לא מעטים, אבל רובם יחלו באורח קל, יחסית. האם הממשלה מתפקדת כראוי? לא יודע, כי בינתיים הממשלה, כמעט ואינה מקבלת החלטות. אני מבין את הממשלה, היא לא רוצה להורוס שוב את המשק, או את הלימודים, אך מצד שני העם ממתין להחלטות.

אגב, גם החלטה לא להחליט, כלומר לשמר את המצב הקיים היא טוג של החלטה, אבל חייבים לעדכן את העם גם בהחלטה לא להחליט. מעבר לכך אני בעד דעתה של שרת החינוך יפעת שאשא ביטון ולפיה יש לפתוח את שנת הלימודים בסדרה (ביניתיים) וכמו כן להגביל את הבידודים המהמונים להם היינו עדים בפעמים הקודמות.

כמו כן, יש לברך על כך שבמגזר החרדי ישנה תחלואה מעטה יותר. הדבר ניבע, מן הסתם, מכך שבמגזר החרדי היו רבים שכבר חלו בקורונה ולכן הם יותר מחוסנים מהאחרים, חיסון טבעי. אלה הן חדשות מעודדות.

PC אנשים ומחשבים

"שיתופי פעולה בינלאומיים בסייבר – רק כך האור יגבר על החושך"

"העולם הקיברנטי הוא נטול גבולות, ולכן נדרשים שיתופי פעולה בינלאומיים", אמר השר לביטחון פנים, עומר בר לב ● בדבריו בשבוע הסייבר הוא האיר זרקור על פעילות גופי האכיפה בתחום

מאת: יוסי הטוני

"לפשעי הסייבר אין גבולות ופושעי הסייבר משתוללים בכל מקום. רק בניית והעמקת שיתופי פעולה בין מדינות ובתוך מדינות הם שיעניקו לנו את הניצחון, רק כך בני האור יצליחו לגבור על בני החושך", כך אמר השר לביטחון פנים, עומר בר לב.

השר בר לב דיבר היום (ג') במסגרת שבוע הסייבר הישראלי, שנערך זו השנה ה-11, בהובלת המרכז למחקר סייבר בינתחומי על שם בלווטניק באוניברסיטת תל אביב, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ.

לדבריו, "האינטרנט היה לחלק מהמרחב הציבורי, וככזה הוא הפך למרחב המשמש תשתית לפשיעת הסייבר. פשע הסייבר מחליף אט אט את הפשע ה-'מסורתי', והפושעים מנצלים אותו לטובתם. זהו מרחב התארגנות פורה ונוח".

הוא פירט את עבירות הסייבר שגופי האכיפה מטפלים בהם: "פשע פיננסי, מירמה, הלבנת הון, סחיטה, פריצה למערכות מידע ולרשתות תקשורת, ולמחשבי הקצה, וחדירה למאגרי מידע לטובת גניבה שלהם, או לשם עיוות נתונים".

הקורונה: פחות עבירות "מסורתיות", יותר פשעי סייבר

השר לביטחון פנים אמר כי "הקורונה הביאה לגידול בפשעי הסייבר, על חשבון ירידה ביכולת הפושעים לבצע עבירות מהסוג ה-'מסורתי'. המעבר לעבודה מרחוק הגדיל את משטחי התקיפה והאיץ את פעילות פושעי הסייבר במרחב". הוא ציין ש-"מדובר בפשיעה בהיקף נרחב, שמערבת סמי אמצעי לחימה, הימורים ופרוטקשן. כולם יחד מסבים נזקים של עשרות מיליארדי דולרים – וזהו רק קצה הקרחון".

"המאבק בפשיעה המקוונת הוא אתגר גדול", אמר בר לב. "החקירות, האכיפות והמאבק בעבריינות רשת הם דברים מאוד מורכבים. לתוקף קל יותר להסתתר מפני אימת הדין בחסות האפילה. האתגר צפוי להתעצם עם גידול הפשע הקיברנטי".

"בישראל", הוסיף, "יש שיתופי פעולה בין הגורמים השונים שעוסקים בתחום הסייבר – המשרד לביטחון פנים, המשטרה, מערך הסייבר הלאומי וגופי הביטחון. כל אחד מהם מביא את המומחיות שלו לשולחן. בנוסף, יש לנו שיתופי פעולה רבים ברמה הבינלאומית – ויש לכך חשיבות בעולם שבו פשיעת סייבר נעשית על גבי פלטפורמות שאנונימיות היא המאפיין שלהן. כך היה במקרים רבים. רק באחרונה נציג משטרת ישראל השתתף בפורום שהתכנס באיחוד האמירויות, שבמהלכו מוסד הקשר בין משטרות ישראל, דובאי ואבו דאבי. העולם הקיברנטי הוא נטול גבולות – לא פיזיים ולא ערכיים. לכן, אנחנו זקוקים להרחבת שיתופי הפעולה הבינלאומיים – רק כך נוכל לנצח".

ישראל היום
הכי ישראלי כל הזמן

בנט: "תקיפות סייבר – איום משמעותי לביטחון הלאומי"

ראש הממשלה נפתלי בנט השתתף אתמול בכנס הסייבר של אוניברסיטת תל אביב, שם נאם והתייחס לאתגרים המקו־מיים והעולמיים בכל הקשור לעולם הסייבר ולאבטחת המי־דע במאה ה־21.

"הכל תחת מתקפות סייבר, הכל רגיש בגלל שזה קל. בת־קיפת סייבר אתה פוגע בקלות במדינה אחרת, לכן זה ילך ויג־בר. וזה מדאיג אותי", אמר בנט, "כראש הממשלה של ישראל אני רואה את זה כאחד האיומים הגדולים שלנו, וצריך לפעול למול זה".

בנט הדגיש כי "שום ממשלה לא יכולה לפתור את זה. צריך מומחים, יוצאי צבא, צעירים, עם יכולות גבוהות. בגלל זה יש לנו את תופעת ה'בום' בהייי־טק. זה הסוד שלנו בישראל. אם מדי־נה נמצאת תחת התקפת סייבר, חשוב ששאר המדינות יידעו זאת ויידעו להיזהר ולהילחם בפושע. אנחנו יצרנו סוכנות המאחדת את מתקפות הסייבר ומתרייעה על התוקפים בסייבר לכולם".

רה"מ בנט הוסיף ואמר כי "אם תנסה להילחם לבד, תפסיד. אם, נניח, אירען תוקפת את תעלות המים בבלגיה, יהיה מאוד קשה לאותת על המתקפה הרעה הזאת לבד. לדעת להבחין מיהו האיש הרע ולפעול מולו. אנחנו כבר בקשר עם המון מדינות, ואנחנו רוצים לעלות את זה לשלב הבא, הגנה אינטרנטית לכולם. אנח־נו מזמינים את המדינות הטובות מכל העולם לאחד איתנו כוחות".

אריאל כהנא וגיא לוי

רה"מ בנט צילום: נדעון מרקוביץ'

וואלה

"אירוע משמעותי ביותר": הממשלה הקימה צוות מיוחד לטיפול במשבר NSO

הצוות שכולל בין היתר נציגים של משרדי הביטחון, החוץ המשפטים והמוסד אמור בין השאר לבצע בדיקה מול חברת הסייבר ההתקפי לגבי הטענות על השימוש בתוכנת "פגסוס" לריגול אחר עיתונאים, פעילי זכויות ופוליטיקאים. "חייבים לבדוק אם יש צורך בשינוי מדיניות", אמר בכיר ישראלי

מאת: ברק רביד

הממשלה הקימה בימים האחרונים צוות מיוחד לטיפול במשבר סביב חברת הסייבר ההתקפי NSO והפרסומים על השימוש בתוכנת "פגסוס" של חברת NSO לצורך ריגול אחרי עיתונאים, פעילי זכויות אדם ואנשי אופוזיציה בכמה מדינות בעולם - כך אמרו שני פקידים ישראלים בכירים.

הצוות שכולל נציגים של משרד הביטחון, משרד החוץ, משרד המשפטים, המוסד, אגף המודיעין בצה"ל וגורמים נוספים אמור לבצע בדיקה מול חברת NSO לגבי הטענות שמועלות בפרסומים השונים בתקשורת ולהיערך להתמודד עם ההשלכות הביטחוניות, המדיניות והמשפטיות של הפרשה. ישיבה ראשונה של הצוות התקיימה ביום ראשון בראשות מנכ"ל משרד הביטחון אמיר אשל דיון ומנכ"ל משרד החוץ אלון אושפיז.

עד כה המשבר הוא תדמיתי ותקשורתי בלבד על רקע שטף הפרסומים בתקשורת הבינלאומית על השימוש הפסול שנעשה בתוכנה של NSO. עם זאת, החשש בישראל הוא שבימים הקרובים המשבר יהפוך למדיני. רמז לכך נשמע הבוקר בנאומה של ראשת המרכז הלאומי לאבטחת סייבר של בריטניה לינדי קמרון בכנס הסייבר באוניברסיטת תל-אביב.

"אנחנו עדים עכשיו לתופעה של מדינות שאינן בעלות יכולות גבוהות, ומסוגלות לקנות אותה, עם פחות שליטה ישירה על ההשפעה הישירה והעקיפה של הפעילות שלהן", היא אמרה ברמז על הטכנולוגיה ש-NSO מכרה לכמה מדינות בעולם. "אנחנו מאמינים שאיומי הסייבר שאנחנו מתמודדים איתם הם איומים גלובליים. זה חשוב שכל שחקני הסייבר ישתמשו ביכולות שלהם באופן חוקי, אחראי ומידתי כדי להבטיח שהמרחב הקיברנטי יישאר מרחב בטוח ומשגשג עבור כולם. ואנחנו נעבוד עם בנות בריתנו כדי להבטיח את זה".

שר הביטחון בני גנץ שדיבר אחריה בכנס אמר כי ישראל "לומדת" את הפרסומים בתקשורת לגבי NSO. "אנחנו מאשרים ייצוא מוצרי סייבר רק לממשלות ורק לשימוש חוקי ולמניעת פשעים וטרור", אמר גנץ בנאום בכנס הסייבר באוניברסיטת תל אביב. "המדינות שרוכשות את המערכות האלה חייבות לעמוד בתנאי השימוש".

בכירים ישראלים ציינו כי הממשלה מתייחסת למשבר ברצינות רבה. לדבריהם, למרות שנראה שננקטו הצעדים הדרושים לגבי מתן רשיון הייצוא ל-NSO השאלה המרכזית היא כיצד הפרשה תשפיע על חברות אחרות ועל עסקאות עתידיות.

"זה אירוע משמעותי ביותר", אמר בכיר ישראלי. "אנחנו מנסים להבין את מלוא המשמעותיות שלו. נהיה חייבים לבדוק אם בעקבות הפרסומים האחרונים יש צורך בשינוי מדיניות בכל הנוגע לייצוא של מערכות סייבר התקפי למדינות בעולם".

לפי דיווחים שפורסמו הערב בכלי התקשורת שחשפו את הפרשה, בין המספרים שנכללו לכאורה ברשימת "פגסוס" היו אלו של נשיא צרפת עמנואל מקרון ומלך מרוקו מוחמד השישי, כמו גם של ראש ממשלת לבנון לשעבר סעד חרירי ונשיאי עיראק ודרום אפריקה.

חברת NSO עצמה מכחישה את הפרסומים בתקשורת הבינלאומית.

גלובס

ראש אמ"ן: "אלה שתוקפים את ישראל בסייבר צריכים להבין את הסיכון שהם לוקחים"

בנאום במסגרת שבוע הסייבר של אוניברסיטת תל אביב ציין ראש אמ"ן, אלוף תמיר הימן, כי במהלך מבצע "שומר החומות" מידע שנאסף ממרחב הסייבר "איפשר לצה"ל לתפקד טוב יותר, מהיר יותר ועם פחות אבדות בחיי אדם"

מאת: דני זקן

שר הביטחון בני גנץ אומר כי משרדו לומד כעת את הפרסומים בסוגיית שימוש במערכות שפותחו על ידי חברות סייבר ישראליות, בהתכוונו לפרסומים על מערכת ההאזנה והמעקב פגסוס של חברת NSO. לדבריו, הוא מודע לנושא וישראל, כדמוקרטיה מערבית ליברלית, מפקחת על יצוא מוצרי סייבר לפי חוק הפיקוח על הייצוא הביטחוני ובהתאם למשטרי פיקוח בין-לאומיים.

"כמדיניות, מדינת ישראל מתירה ייצוא של מוצרי סייבר מפוקחים אך ורק לממשלות, אך ורק לשימוש חוקי, וספציפית למטרות מניעה וחקירה של פשעים וטרור. על המדינות הרוכשות מערכות אלה לעמוד בהתחייבויותיהן לדרישות אלה. אנו לומדים כעת את המידע המתפרסם בנושא", אמר גנץ.

בנאום במסגרת שבוע הסייבר הבינלאומי של אוניברסיטת תל אביב אמר גנץ בעניין ירי הרקטות משטח לבנון אמש כי למדינת ישראל יש אינטרס בלבנון יציבה ומשגשגת כלכלית, אבל המצב בלבנון הולך ומחמיר, וחיזבאללה וארגוני טרור נוספים פועלים נגד האינטרסים של העם הלבנוני. "הגבנו בלילה, ונמשיך להגיב ולפעול בזמן ובמקום הנכונים מול כל הפרה של ריבונות ישראל. מדינת לבנון היא האחראית לנעשה משטחה. אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטארי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות והפרת ריבונות ואני קורא לקהילה הבינלאומית לפעול להשבת היציבות בלבנון".

בסוגיית הסייבר הדגיש כי "בשנים האחרונות חלה עלייה משמעותית במספר ההתקפות שביצעו גורמים עוינים, כולל איראן ושלוחותיה, המבקשים לגשת למערכות התקשוב של התשתית הלאומית של ישראל. לנוכח העלייה הזו - מכמה התקפות בודדות לעשרות התקפות בשנה - ישראל הוכיחה את היכולת לפתח את חוסנה, את היתרון הטכנולוגי שלה ואת היתרון האיכותי שלה באזור. ישראל פועלת באופן רציף להגנה מפני מתקפות סייבר". שר הביטחון גילה כי ישראל תקפה בשנים האחרונות כמה פעמים את פיקוד הסייבר של חמאס ובמאי האחרון חיסלה את מי שעבד בראש מערך הסייבר של ארגון הטרור ג'ומעה טחלה.

ראש אמ"ן, אלוף תמיר הימן, אמר בכנס כי במסגרת המבצע האחרון בעזה, מידע שנאסף ממגוון מקורות - בין היתר ממרחב הסייבר, הביא לתפוקות מבצעיות מעולות: "דבר זה איפשר לצה"ל לתפקד טוב יותר, מהיר יותר, ועם פחות אבדות בחיי אדם".

הוא הוסיף: "ישראל נמצאת תחת איום תמידי במימד הסייבר, ומתקפות מבוצעות לעיתים נגדה. אנו מצליחים להתמודד עם מרבית האיומים באמצעות יכולות הגנה מתקדמות. כמו בממדי הלחימה אחרים, הגנה לבד אינה מספקת. יש לנקוט צעדים נוספים בכדי לשמר את עליונות ישראל אל מול אויבנו. אלו שתוקפים את ישראל באוויר, בים, ביבשה או בסייבר צריכים להבין את הסיכון שהם לוקחים. כפי שהם נוכחים לראות פעם אחר פעם, התקפה תיענה בהתאם".

PC אנשים ומחשבים

"חורף הסייבר כבר כאן: 42% מהעסקים הגדולים חוו מתקפות"

"האיומים ממשיכים לגדול – מכל הכיוונים, וכבר קר ורע פה", אמר יגאל אונא, ראש מערך הסייבר הלאומי, וציטט נתונים שצריכים להדאיג אותנו ולהדיר שינה מעיני מקבלי ההחלטות

מאת: יוסי הטוני

"איומי הסייבר מכל הכיוונים – מדינות ופושעים – ממשיכים לגדול. כבר קר ורע פה. כמה? יש לחקור, אבל אנחנו שם", כך אמר יגאל אונא, ראש מערך הסייבר הלאומי.

אונא דיבר היום (ד) במסגרת שבוע הסייבר הישראלי, שנערך זו השנה ה-11 ושמובילים המרכז למחקר סייבר בינתחומי על שם בלווטניק באוניברסיטת תל אביב, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ. הוא ציטט סקר חדש שערך המערך יחד עם הלשכה המרכזית לסטטיסטיקה, שלפיו אחד מכל חמישה עסקים בישראל (18%) חווה מתקפת סייבר. כמו כן, התקיפות על חמישית מהעסקים שדיווחו שחוו אחת כזו גרמו נזק כלשהו למערכות שלהם – חוסר זמינות מידע, דלף מידע או הרס והשחתה של המערכות. בחלוקה לפי גודל הארגון, 42% – שתי חמישיות – מארגוני האנטרפרייז ו-15% מהעסקים הקטנים חוו לפחות מתקפת סייבר אחת.

"המסקנה מהסקר, ולא רק ממנו, היא שהחורף כבר כאן. הנתונים מתייחסים ל-2020 ואני חושש שב-2021 הם יהיו גרועים יותר, כי הם ממשיכים לעלות. כמה קר זה יהיה? עוד נראה, אבל אנחנו כבר שם", אמר אונא.

בהמשך הוא ציטט נתונים מהעולם – אם כי בפן אחר של הנושא. לדבריו, "ממוצע התשלום שארגונים בארצות הברית משלמים במתקפות כופרה הוא 178,254 דולר. מתקפות אלה גורמות להשבתת הארגון למשך 16 ימים בממוצע. הנתונים נמצאים בעלייה מתמדת מדי שנה, לרבות גידול של עשרות אחוזים במשך ההשבתה הממוצע – וזה נתון שצריך להדיר שינה מעינינו".

ראש מערך הסייבר הוסיף כי "אנחנו רואים עלייה שנתית במספר החולשות. רק באפריל האחרון נרשמו 1,400 חולשות. לכן, אנחנו מחזקים במערך הסייבר הלאומי את היחידה להגנה פרו-אקטיבית".

מה עושים?

אונא ציין שמערך הסייבר הצטרף לתוכנית הבינלאומית שמפעיל ארגון Mitre לדיווח ולקיטלוג של פגיעויות שהתגלו במוצרים טכנולוגיים. הארגון אישר באחרונה את המערך כגוף מוסמך לרישום פגיעויות וחשיפות נפוצות (CVE) ברשימה העולמית. "מאז שהצטרפנו לפני כשבועיים התקבלו במערך עשרות דיווחים, שחלקם נמצאים בתהליך רישום עולמי", ציין. "בנוסף, בקרוב נשיק תוכנית רחבה בתחום, שתכלול יכולות איתור וניטור חולשות במרחב הישראלי, על מנת לסגור אותן מבעוד מועד ולמנוע תקיפות".

לדברי אונא, "על מנת להתמודד עם מגוון איומי הסייבר, עלינו להיות מהירים יותר. אנחנו מתמודדים עם מגיפה של נוזקות וחולשות יותר מכל זמן אחר בהיסטוריה. עלינו להיות חכמים יותר. ואמנם, אתמול השקנו את הגרסה החדשה של תורת ההגנה, המדריך והבסיס לבניית הגנת סייבר בארגון, בדגש על ראיית התוקף ובניית ההגנה מותאמת. הגרסה הזו הושקה ארבע שנים לאחר הרסה הקודמת. כעת אנחנו מתקדמים, בוחנים איך התוקף פועל, מהם מניעיו, איך הוא רואה אותנו, ואז – איך בונים הגנה. עלינו להיות חזקים יותר, להפגין נחישות ואי סובלנות לטרור סייבר – בדיוק כמו ביחס לטרור פיזי".

הוא ציין שכדי להגן טוב יותר מפני מתקפות סייבר נדרשים שיתופי פעולה בינלאומיים. כחלק מזה, אמר אונא, "ערכנו באחרונה הסכם לשיתוף פעולה בתחום עם מרוקו. אנחנו מבינים שלמזלנו, עלינו לעבוד יחד, לטובת הגדלת החוסן, העמקת השותפויות, העצמת האמון והטמעת טכנולוגיות מתקדמות. הדרך להצלחה טמונה באנשים ובשותפויות".

פורטל הכרמל והצפון

אחד מכל חמישה עסקים בישראל חווה תקיפת סייבר

כך עולה מסקר חדש של הלמ"ס ומערך הסייבר הלאומי שיוצגו היום לראשונה על ידי יגאל אונא, ראש מערך הסייבר הלאומי. שניים מכל חמישה עסקים גדולים חווה תקיפת סייבר, השימוש באמצעי הגנת סייבר נפוץ יותר בעסקים גדולים מאשר בעסקים קטנים.

על פי הנתונים שיציג אונא, מתוך העסקים שדיווחו שחוו תקיפה, לחמישית מהם נגרם נזק כלשהו למערכות כתוצאה מהתקיפה. הנזק התבטא בחוסר זמינות מידע, דלף מידע, או הרס והשחתה של מערכות המידע. הסקר יוצג במסגרת שבוע הסייבר שמתקיים בשיתוף מרכז לחקר הסייבר באוניברסיטת ת"א.

"סקר מקיף מציג נתונים שמראים בבירור כי תקיפות סייבר על עסקים בישראל הפכו לתופעה נרחבת", אומר אונא. "חלק מהארגונים הצליחו לבלום את התקיפה ולמנוע ממנה מלגרום לנזק, וכאן אנו עדים לשלב חשוב של זיהוי וגילוי התקיפה שארגונים החלו להעצים באחרונה. נכון שעלויות של הגנת סייבר משמעותיות, אך הנזקים כתוצר מתקיפה הם בעלי השלכות כלכליות גדולות שכוללות עלויות התאוששות, אובדן ימי עסקים ואף השבתה ולכן כדאי להשקיע במניעה וגילוי".

מהסקר עולה כי התקיפות שכיחות בעיקר בקרב עסקים גדולים (250 עובדים ומעלה): שניים מכל חמישה עסקים גדולים חווה תקיפת סייבר (42%) וכן בקרב תעשיית טכנולוגיית עילית (47%). בענפי ההיי-טק, אחד מכל שלוש חברות דיווחו על תקיפה (37%). על פי הדיווחים בסקר, כ-15% מהעסקים הקטנים חוו מתקפת סייבר.

"לעיתים מתקפה על עסק קטן יכולה להיות הרסנית אף יותר בשל היכולת להתאושש ולשאת בעלויות ולכן החשיבות שבהגנה מבעוד מועד – בין פעולות בסיסיות ועד להטמעת טכנולוגיות והגנות", מסבירה יעל לדרמן ראש תחום קידום מדיניות במערך הסייבר הלאומי. "לעסקים יש אחריות לא רק כלפי עצמם אלא גם כלפי הלקוחות שלהם וכלפי המידע על הלקוחות שהם מחזיקים לעיתים רבות במחשב ללא כל הגנה בסיסית".

בהקשר לרמת הגנת הסייבר של ארגונים, מהסקר עולה כי 58% מהארגונים פועלים במידה רבה עד רבה מאוד, לתפיסתם, לצמצום סיכוני הסייבר ואילו 31% במידה מועטה או מועטה מאוד. מפילוח הנתונים עולה כי ככל שהארגון גדול יותר כך הוא פועל בצורה משמעותית יותר בתחום הגנת הסייבר. כך, רק 55% מה עסקים הקטנים מבצעים פעולות רבות בתחום הגנת הסייבר. בעוד ש-84% מהעסקים הגדולים מדווחים כי הם מבצעים פעולות רבות בנושא. כמו כן, אותם ענפים שדיווחו בשיעור גבוה על כך שחוו מתקפות – הייטק ושירותים מקצועיים, מדעיים וטכניים - דיווחו גם על מידה גבוהה של פעילות לצמצום הסיכון (89% ו-84% בהתאמה).

השימוש באמצעי הגנת סייבר נפוץ יותר בעסקים גדולים מאשר בעסקים קטנים. מהנתונים עולה כי ככל שהעסק גדול יותר כך נעשה שימוש ביותר אמצעים להגנות סייבר. שלושת בקרות ההגנה השכיחות ביותר שבהן עסקים מכל הסוגים עשו שימוש הן: עדכוני תוכנה (68%), אמצעים לגילוי זיהוי וסיכול נוזקות (65%), ומדיניות סיסמאות חזקות (62%). לעומתן, שלושת הבקרות שהיו בשימוש הפחות ביותר הן: ביטוח סייבר (11%), עריכת סקרי סיכונים תקופתי (17%) והגדרת מדיניות התאוששות מחירום (19%).

בתחום של העסקת כח אדם לנושא הגנת סייבר בארגון, עולה כי ל-68% מהארגונים יש עובדים שעוסקים בנושא בתוך הארגון או במיקור חוץ, ואילו ל-32% מהארגונים אין כלל כח אדם בתחום.

אחד מארבעה ארגונים במשק מכירים את מסמכי המלצות ההגנה (כגון תורת ההגנה לארגון) שמפרסם מערך הסייבר הלאומי ו-80% מהמכירים את ההמלצות, עושים בהן שימוש. כמו כן, 60% מהארגונים הגדולים שמכירים את ההמלצות גם עושים בהן שימוש.

המדגם כלל כ-2,500 עסקים עם לפחות עשרה מועסקים בכלל הענפים מלבד פיננסים, בריאות ומינהל ציבורי. הסקר בתחום הסייבר הוא פרק אחד מתוך סקר מקיף יותר בנושאי שימוש במחשבים ואינטרנט שתוצאותיו יפורסמו בהמשך השנה על ידי הלמ"ס וישראל דיגיטלית.

מעריב

2 במסגרת שבוע הסייבר השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ נאם והתארח רה"מ **נפתלי בנט**. במהלך הכנס פגש רה"מ את שותפיו לשעבר מייסדי הסטארט־אפ סאיוטה, אשר עדיין פועלים בתעשיית ההייטק הישראלית, **מיכל ברוורמן־בלומנשטיק**, מנכ"לית מיקרוסופט ישראל מחקר ופיתוח, **ואורי ריבנר**, מייסד הסטארט־אפ BioCatch.

2. מיכל ברוורמן־בלומנשטיק ונפתלי בנט

מעריב

2. מיכל ברוורמן־בלומנשטיק ונפתלי בנט

2 במסגרת שבוע הסייבר השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ נאם והתארח רה"מ **נפתלי בנט**. במהלך הכנס פגש רה"מ את שותפיו לשעבר מייסדי הסטארט־אפ סאיוטה, אשר עדיין פועלים בתעשיית ההייטק הישראלית, **מיכל ברוורמן־בלומנשטיק**, מנכ"לית מיקרוסופט ישראל מחקר ופיתוח, **ואורי ריבנר**, מייסד הסטארט־אפ BioCatch.

וואלה

בנט בסייבר

במסגרת שבוע הסייבר השנתי של המרכז למחקר סייבר באוניברסיטת ת"א, מערך הסייבר הלאומי, משרד הכלכלה ומשרד החוץ, נאם והתארח רה"מ נפתלי בנט.

במהלך הכנס פגש רה"מ את שותפיו לשעבר מייסדי הסטארט-אפ "סאיוטה", אשר עדיין פועלים בתעשיית ההייטק הישראלית, מיכל ברוורמן-בלומנשטיק, מנכ"לית מיקרוסופט ישראל מחקר ופיתוח ואורי ריבנר מייסד הסטארט-אפ BioCatch.

המבשר

הלמ"ס: אחד מכל חמשה עסקים בישראל חווה תקיפת סייבר

מאת **חיים מרגליות**

אחד מכל חמשה עסקים בי־שראל (18%) חווה תקיפת סייבר – כך עולה מסקר חדש של הלמ"ס ומערך הסייבר הלאומי.

על פי הנתונים, מתוך העסקים שדיווחו שחוו תקיפה, לחמישית מהם נגרם נזק כלשהו למערכות כתוצאה מהתקיפה, שהתבטא בחוסר זמינות מידע, דלף מידע, או הרס והשחתה של מערכות המידע. הסקר יוצג במסגרת שבוע הסייבר שמתקיים בשיתוף מרכז לחקר הסייבר באוניברסיטת ת"א.

"סקר מקיף מציג נתונים שמ־ראים בבירור כי תקיפות סייבר על עסקים בישראל הפכו לתר־פעה נרחבת", אומר ראש מערך הסייבר הלאומי יגאל אונא. "חלק מהארגונים הצליחו לבלום את התקיפה ולמנוע ממנה מלגרום לנזק, וכאן אנו עדים לשלב חשוב של זיהוי וגילוי התקיפה שאר־גונים החלו להעצים באחרונה. נכון שעלויות של הגנת סייבר משמעותיות, אך הנזקים כתוצר מתקיפה הם בעלי השלכות כל־כליות גדולות שכוללות עלויות התאוששות, אובדן ימי עסקים ואף השבתה ולכן כדאי להשקיע במניעה וגילוי".

מהסקר עולה כי התקיפות שכיחות בעיקר בקרב עסקים גדולים (250 עובדים ומעלה): שניים מכל חמשה עסקים גדולים חווה תקיפת סייבר (42%) וכן בקרב תעשיית טכנולוגיית עילית (47%). בענפי ההיי־טק, אחד מכל שלוש חברות דיווחו על תקיפה (37%). על פי הדיווחים בסקר, כ־15% מהעסקים הקטנים חוו מתקפת סייבר.

"לעיתים מתקפה על עסק קטן יכולה להיות הרסנית אף יותר בשל היכולת להתאושש ולשאת בעלויות ולכן החשיבות שבהגנה מבעוד מועד – בין פעולות בסי־סיות ועד להטמעת טכנולוגיות והגנות", מסבירה י. לדרמן ראש תחום קידום מדיניות במערך הסייבר הלאומי. "לעסקים יש אחריות לא רק כלפי עצמם אלא גם כלפי הלקוחות שלהם וכלפי המידע על הלקוחות שהם מחזי־קים לעיתים רבות במחשב ללא כל הגנה בסיסית".

בהקשר לרמת הגנת הסייבר של ארגונים, מהסקר עולה כי 58% מהארגונים פועלים במידה רבה עד רבה מאוד, לתפיסתם, לצמצום סיכוני הסייבר ואילו 31% במידה מועטה או מועטה מאוד. מפילוח הנתונים עולה כי ככל שהארגון גדול יותר כך הוא פועל בצורה משמעותית יותר בתחום הגנת הסייבר. כך, רק 55% מהעסקים הקטנים מבצעים פעו־לות רבות בתחום הגנת הסייבר. בעוד ש־84% מהעסקים הגדולים מדווחים כי הם מבצעים פעולות רבות בנושא. כמו כן, אותם ענ־פים שדיווחו בשיעור גבוה על כך שחוו מתקפות – הייטק ושירו־תים מקצועיים, מדעיים וטכניים - דיווחו גם על מידה גבוהה של פעילות לצמצום הסיכון (89% ו־84% בהתאמה).

השימוש באמצעי הגנת סייבר נפוץ יותר בעסקים גדולים מאשר בעסקים קטנים. מהנתונים עולה כי ככל שהעסק גדול יותר כך נעשה שימוש ביותר אמצעים להגנות סייבר. שלושת בקרות ההגנה השכיחות ביותר שבהן עסקים מכל הסוגים עשו שימוש הן: עדכוני תוכנה (68%), אמצעים לגילוי זיהוי וסיכול נוזקות (65%), ומדיניות סיסמאות חזקות (62%). לעומתן, שלושת הבקרות שהיו בשימוש הפחות ביותר הן: ביטוח סייבר (11%), עריכת סקרי סיכו־נים תקופתי (17%) והגדרת מדי־ניות התאוששות מחירום (19%).

בתחום של העסקת כח אדם לנושא הגנת סייבר בארגון, עולה כי ל־68% מהארגונים יש עובדים שעוסקים בנושא בתוך הארגון או במיקור חוץ, ואילו ל־32% מהארגונים אין כלל כח אדם בתחום.

אחד מארבעה ארגונים במ־שק מכירים את מסמכי המלצות ההגנה (כגון תורת ההגנה לארגון) שמפרסם מערך הסייבר הלאומי ו־80% מהמכירים את ההמלצות, עושים בהן שימוש. כמו כן, 60% מהארגונים הגדולים שמכירים את ההמלצות גם עושים בהן שימוש.

המדגם כלל כ־2,500 עסקים עם לפחות עשרה מועסקים בכלל הענפים מלבד פיננסים, בריאות ומינהל ציבורי.

ישראל היום
הכי ישראלי כל הזמן

שר הביטחון גנץ בתגובה לפרסומים על NSO: ישראל מתירה יצוא ביטחוני לממשלות, אך ורק לשימוש חוקי

גנץ הדגיש כי במערכת הביטחון בוחנים את המידע שהתפרסם, לפיו תוכנה ישראלית שימשה לרגל אחר אלפי עיתונאים ומנהיגי אופוזיציה • בכנס הסייבר הלאומי, אמר האלוף תמיר הימן: "אלו שתוקפים את ישראל צריכים להבין את הסיכון שהם לוקחים"

מאת: לילך שובל

"כמדיניות, מדינת ישראל מתירה יצוא של מוצרי סייבר מפוקחים אך ורק לממשלות, אך ורק לשימוש חוקי, וספציפית למטרות מניעה וחקירה של פשעים וטרור", כך אמר שר הביטחון, בני גנץ, שנאם היום (שלישי) במסגרת שבוע הסייבר הבינלאומי של אוניברסיטת תל אביב. זאת על רקע הפרסומים האחרונים על חברת NSO. כזכור, לפי הדיווחים האחרונים, התוכנה הישראלית "פגסוס" שימשה לריגול אחר עיתונאים וגורמי אופוזיציה.

עוד אמר שר הביטחון על היתרי היצוא הביטחוני ממשרד הביטחון: "אנו מודעים לפרסומים האחרונים על שימוש במערכות שפותחו על ידי חברות סייבר ישראליות מסוימות. ישראל, כדמוקרטיה מערבית-ליברלית, מפקחת על יצוא מוצרי סייבר לפי חוק הפיקוח על היצוא הביטחוני ובהתאם למשטרי פיקוח בין-לאומיים".

גנץ הדגיש כי "על המדינות הרוכשות מערכות אלה לעמוד בהתחייבויותיהן לדרישות אלה. אנו לומדים כעת את המידע המתפרסם בנושא".

כזכור, ב-NSO הגיבו לפרסומים באומרם בין היתר כי "מדובר בכותרות סנסציוניות וחסרות בסיס עובדתי. בדו"ח לכאורה שהועבר אין כל קשר בין רשימת 50,000 המספרים המדוברים לקבוצת NSO או למערכת 'פגסוס'. לא נמצא שום קשר בין הטכנולוגיות שלנו לבין הרצח המתועב של ג'מאל חאשוקג'י. הטכנולוגיות של קבוצת NSO מסייעות במניעת טרור, אלימות, פשעים ופיגועי טרור".

"נמשיך להגיב מול כל הפרה"

בעקבות ירי הרקטות במהלך הלילה מלבנון, אמר גנץ כי "למדינת ישראל יש אינטרס בלבנון יציבה ומשגשגת כלכלית. לצערנו, המצב בלבנון הולך ומחמיר, וחיזבאללה וארגוני טרור נוספים פועלים נגד האינטרסים של העם הלבנוני. הגבנו בלילה, ונמשיך להגיב ולפעול בזמן ובמקום הנכונים מול כל הפרה של ריבונות ישראל".

"מדינת לבנון היא האחראית לנעשה משטחה", הבהיר גנץ, "אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטארי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות והפרת ריבונות ואני קורא לקהילה הבינלאומית לפעול להשבת היציבות בלבנון".

"עלייה במספר התקפות הסייבר"

כשברקע ניסיונות של מתקפות סייבר על ישראל, שר הביטחון הבהיר כי "בשנים האחרונות חלה עלייה משמעותית במספר ההתקפות שביצעו גורמים עוינים, כולל איראן ושלוחותיה, המבקשים לגשת למערכות התקשוב של התשתית הלאומית של ישראל. לנוכח העלייה הזו - מכמה התקפות בודדות לעשרות התקפות בשנה - ישראל הוכיחה את היכולת לפתח את חוסנה, את היתרון הטכנולוגי שלה ואת היתרון האיכותי שלה באזור. ישראל פועלת באופן רציף להגנה מפני מתקפות סייבר. במאי 2019, כחלק מהסכסוך המתמשך של ישראל עם ארגוני הטרור ברצועת עזה, ביצעה ישראל לראשונה מתקפה קינטית על הבניין בו ישב פיקוד הסייבר של חמאס.

"המתקפה בוצעה בעקבות פעילויות שמטרתן הייתה לפגוע בתשתיות הישראליות במרחב הסייבר, כפי שניסו לעשות תוקפי הסייבר של חמאס בהנחיית איראן. במהלך מבצע 'שומר החומות', פגענו בראש פיקוד הסייבר של חמאס, ג'ומעה טחלה. כמו כן זיהינו ופגענו בכמה תוקפי סייבר, ציוד ותשתיות אשר שימשו את פיקוד הסייבר של חמאס. המסר שלנו הוא ברור - תהיה זו רקטה או מקלדת - לא נסבול איום על אזרחי ישראל", אמר גנץ.

ראש אמ"ן: הגנה לבד בסייבר אינה מספקת

כנס סייבר לאומי התקיים באוניברסיטת תל אביב, ובו ראש אמ"ן, אלוף תמיר הימן, קיבל את פרס הסוס הטרויאני בשם צה"ל. ראש אמ"ן התייחס למלחמות הסייבר אמר כי "במסגרת המבצע האחרון בעזה, מידע שנאסף ממגוון מקורות - בין היתר ממרחב הסייבר, הותך יחד באמצעות יכולות עיבוד מתקדמות, בינה מלאכותית ולמידת מכונה לכדי תפוקות מבצעיות. דבר זה אפשר לצה"ל לתפקד טוב יותר, מהיר יותר ועם פחות אבדות בחיי אדם".

עוד אמר: "אני רוצה להתייחס גם לאיומים היומיומיים על מדינת ישראל במימד הסייבר. ישראל נמצאת תחת איום תמידי בתחום, ומתקפות מבוצעות לעיתים נגדה. אנו מצליחים להתמודד עם מרבית האיומים באמצעות יכולות הגנה מתקדמות.

"כמו בממדי הלחימה אחרים, הגנה לבד אינה מספקת. יש לנקוט צעדים נוספים בכדי לשמר את עליונות ישראל אל מול אויבנו".

ראש אמ"ן הוסיף: "אלו שתוקפים את ישראל באוויר, בים, ביבשה או בסייבר צריכים להבין את הסיכון שהם לוקחים. כפי שהם נוכחים לראות פעם אחר פעם, התקפיות תיענה בהתאם".

"בעקבות משבר הקורונה והמגבלות אשר הוא הביא עימו, ירדה היכולת של ארגוני הפשיעה לפעול, אך עם זאת גדלה פעילות הפשיעה דרך הסייבר והדיגיטל - והנזקים נעמדים במאות מיליארדים", אמר השר לביטחון הפנים, עמר בר-לב.

"המעבר של הפשיעה לעולם המקוון מאתגר מאוד ודורש מאיתנו התמודדות מורכבת יותר. במדינת ישראל קיים שיתוף פעולה פורה בין גורמי הביטחון במלחמה נגד הסייבר".

מתקפות הסייבר בראי הקורונה

ריאיון עם פרופ' איציק בן ישראל לרדיו ת"א

Cyber Week
July 19th-22nd, 2021
Tel Aviv University, Israel

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University

ICRC Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber Israel National Cyber Directorate

In cooperation with: ISRAEL CYBER ALLIANCE

Ministry of Foreign Affairs Israel

כאן ב

ריאיון עם מני ברזילי לתכנית "מעבירים לראשון".

האזנה החל מדקה 1:52:33

103 FM
רדיו ללא הפסקה

ריאיון עם מני ברזילי לתכנית "איפה הכסף"

Cyber Week

July 19th-22nd, 2021

Tel Aviv University, Israel

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University

Blavatnik Interdisciplinary Cyber Research Center

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Cyber Israel National Cyber Directorate

In cooperation with: ISRAEL CYBER ALLIANCE

Ministry of Foreign Affairs Israel

חדשות גל"צ בני גנץ

בנט פתח שבוע הסייבר

Cyber Week

July 19th-22nd, 2021

Tel Aviv University, Israel

Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University

ICRC Blavatnik Interdisciplinary Cyber Research Center

Tel Aviv University אוניברסיטת תל אביב

Cyber Israel, National Cyber Directorate

In cooperation with: Israel Cyber Alliance

Ministry of Foreign Affairs, Israel

PEKA | IKD

IKD חדשות

הפלס
בטאון עולם התורה

בניסיון למנוע משבר מדיני: הממשלה הקימה צוות מיוחד שיטפל בפרשת חברת הסייבר הישראלית

■ מאת י. בן דוד

הממשלה הקימה בימים האחרונים צוות מיוחד לטיפול במשבר סביב חברת הסייבר ההתקפי NSO והפרסומים על השימוש בתוכנת "פגסוס" של חברת NSO לצורך ריגול אחרי עיתונאים, פעילי זכויות אדם ואנשי אופוזיציה בכמה מדינות בעולם.

הצוות שכולל נציגים של משרד הביטחון, משרד החוץ, משרד המשפטים, המוסד, אגף המודיעין בצה"ל וגורמים נוספים, אמור לבצע בדיקה מול חברת NSO לגבי הטענות שמועלות בפרסומים השונים בתקשורת, ולהיערך להתמודד עם ההשלכות הביטחוניות, המדיניות והמשפטיות של הפרשה. ישיבה ראשונה של הצוות התקיימה ביום ראשון בראשות מנכ"ל משרד הביטחון, אמיר אשל, ומנכ"ל משרד החוץ, אלון אושפיז.

עד כה המשבר הוא תדמיתי ותקשורתי בלבד, על רקע שטף הפרסומים בתקשורת הבינלאומית על השימוש הפסול שנעשה בתוכנה של NSO. עם זאת, החשש בישראל הוא שבימים הקרובים המשבר יהפוך למדיני. רמז לכך נשמע השבוע בנאומה של ראש המרכז הלאומי לאבטחת סייבר של בריטניה, לינדי קמרון, בכנס הסייבר באונ' תל-אביב.

"אנחנו עדים עכשיו לתופעה של מדינות שאינן בעלות יכולות גבוהות, ומסוגלות לקנות אותה, עם פחות שליטה ישירה על ההשפעה הישירה והעקיפה של הפעילות שלהן", היא אמרה ברמז על הטכנולוגיה ש-NSO מכרה לכמה מדינות בעולם. "אנחנו מאמינים שאיומי הסייבר שאנחנו מתמודדים איתם הם איומים גלובליים. זה חשוב שכל שחקני הסייבר ישתמשו ביכולות שלהם באופן חוקי, אחראי ומידתי, כדי להבטיח שהמרחב הקיברנטי יישאר מרחב בטוח ומשגשג עבור כולם, ואנחנו נעבוד עם בנות בריתנו כדי להבטיח את זה".

שר הביטחון בני גנץ שדיבר אחריה בכנס, אמר כי ישראל "לומדת" את הפרסומים בתקשורת לגבי NSO. "אנחנו מאשרים ייצוא מוצרי סייבר רק לממשלות ורק לשימוש חוקי ולמניעת פשעים וטרור", אמר גנץ בנאום בכנס הסייבר באונ' תל אביב. "המדינות שרוכשות את המערכות האלה חייבות לעמוד בתנאי השימוש".

בכירים ישראלים ציינו לכלי התקשורת כי הממשלה מתייחסת למשבר ברצינות רבה. לדבריהם, למרות שנראה שננקטו הצעדים הדרושים לגבי מתן רשיון הייצוא ל-NSO, השאלה המרכזית היא כיצד הפרשה תשפיע על חברות אחרות ועל עסקאות עתידיות.

לדברי הבכירים, מדובר באירוע משמעותי ביותר, אנחנו מנסים להבין את מלוא המשמעותיות שלו. נהיה חייבים לבדוק אם בעקבות הפרסומים האחרונים יש צורך בשינוי מדיניות בכל הנוגע לייצוא של מערכות סייבר התקפי למדינות בעולם.

כיכר השבת

סערת תוכנת הריגול הישראלית; גנץ מתייחס לפרסומים

במסגרת שבוע הסייבר הבינלאומי של אוניברסיטת תל אביב, נאם שר הביטחון גנץ; האשים את לבנון במתיחות בגבול הצפוני והתייחס לפרסומים נגד התכנה הישראלית (ביטחון)

מאת: ב. ניסני

שר הביטחון, בני גנץ, נאם היום (שלישי) במסגרת שבוע הסייבר הבינלאומי של אוניברסיטת תל אביב, והתייחס לאיומים וניסיונות התקיפה על ישראל, בזירת הסייבר והרשת ובאמצעות רקטות ואמצעי לחימה אחרים.

תחילה התייחס גנץ לירי הרקטות משטח לבנון אמש, ואמר: "למדינת ישראל יש אינטרס בלבנון יציבה ומשגשגת כלכלית. לצערנו, המצב בלבנון הולך ומחמיר, וחיזבאללה וארגוני טרור נוספים פועלים נגד האינטרסים של העם הלבנוני. הגבנו בלילה, ונמשיך להגיב ולפעול בזמן ובמקום הנכונים מול כל הפרה של ריבונות ישראל.

גנץ הוסיף: "מדינת לבנון היא האחראית לנעשה משטחה. אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטארי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות והפרת ריבונות ואני קורא לקהילה הבינלאומית לפעול להשבת היציבות בלבנון".

על ניסיונות של מתקפות סייבר על ישראל, אמר: "בשנים האחרונות חלה עלייה משמעותית במספר ההתקפות שביצעו גורמים עוינים, כולל איראן ושלוחותיה, המבקשים לגשת למערכות התקשוב של התשתית הלאומית של ישראל.

לנוכח העלייה הזו - מכמה התקפות בודדות לעשרות התקפות בשנה - ישראל הוכיחה את היכולת לפתח את חוסנה, את היתרון הטכנולוגי שלה ואת היתרון האיכותי שלה באזור".

גנץ הוסיף והדגיש: "המסר שלנו ברור. תהיה זו רקטה או מקלדת - לא נסבול איום על אזרחי ישראל".

בדבריו התייחס גנץ לסערת חברה ישראלית, שלפי תחקירים נגדה העניקה שירותים לרודנים ולמשטרים טריטוריאליים. גנץ אמר: "אנו מודעים לפרסומים האחרונים על שימוש במערכות שפותחו על ידי חברות סייבר ישראליות מסוימות. ישראל, כדמוקרטיה מערבית ליברלית, מפקחת על יצוא מוצרי סייבר לפי חוק הפיקוח על הייצוא הביטחוני ובהתאם למשטרי פיקוח בין-לאומיים.

"כמדיניות, מדינת ישראל מתירה ייצוא של מוצרי סייבר מפוקחים אך ורק לממשלות, אך ורק לשימוש חוקי, וספציפית למטרות מניעה וחקירה של פשעים וטרור. על המדינות הרוכשות מערכות אלה לעמוד בהתחייבויותיהן לדרישות אלה. אנו לומדים כעת את המידע המתפרסם בנושא".

כזכור, אתמול (שני) בצהרים, בהצהרה שמסרה, אמרה נשיאת הנציבות האירופית אורסולה פון דר ליין כי, אם התחקיר על שימוש שעושות ממשלות בתכנת הריגול "פגסוס" הישראלית, נכונות, הרי שזה "לחלוטין בלתי מתקבל על הדעת". פון דר ליין סייגה כי עדיין הדברים לא מאומתים.

במסגרת השימוש בתוכנה הישראלית, שמשרדיה שוכנים בהרצליה, ניתן - כך לפי הדיווחים - לפרוץ למכשירי טלפון, הן המופעלות במערכת הפעלה של אנדרואיד והן המופעלות במסגרת הפעלה של אפל, ולהגיע אל הודעות ותמונות ואף להפעיל את המצלמה ובאמצעות כך לעקוב בשעת מעשה אחר מקומו של מחזיק הטלפון.

מתחקיר שפורסם, שכלל רשימה ארוכה של מספרי טלפון של עשרות אלפי איש מ-45 מדינות ברחבי העולם, שככל הנראה היוו יעד לפריצה ולמעקב, עלה חשש כבד שהחברה משרתת רודנים ושליטים לדיכוי מתנגדי משטרך ואף לרציחתם.

NSO שמפעילה את החברה הגיבה לטענות, כי "מדובר בדו"ח שקרי שמבוסס על הנחות יסוד שגויות במסגרת קמפיין מאורגן ומתוזמר היטב על-ידי בעלי עניין ידועים". בחברה הוסיפו שהם שוקלים את צעדיהם המשפטיים "למול הטענות ההזויות המוצגות בדו"ח", והדגישו כי "מוצרי החברה נמכרים אך ורק לגופי מודיעין ואכיפת חוק כחלק מהמלחמה בטרור ובפשיעה חמורה ברחבי העולם".

שר הבטחון מזהיר: המצב בלבנון הולך ומחמיר

מאת: צבי רפפורט

גנץ חשף: "בשנים האחרונות חלה עלייה משמעותית במספר ההתקפות שביצעו גורמים עוינים, כולל איראן ושלוחותיה, המבקשים לגשת למערכות התקשוב של התשתית הלאומית"

שר הביטחון, בני גנץ, נאם היום במסגרת שבוע הסייבר הבינלאומי של אוניברסיטת תל אביב.

על ירי הרקטות משטח לבנון אמר: "למדינת ישראל יש אינטרס בלבנון יציבה ומשגשגת כלכלית. לצערנו, המצב בלבנון הולך ומחמיר, וחיזבאללה וארגוני טרור נוספים פועלים נגד האינטרסים של העם הלבנוני. הגבנו בלילה, ונמשיך להגיב ולפעול בזמן ובמקום הנכונים מול כל הפרה של ריבונות ישראל".

עוד אמר: "מדינת לבנון היא האחראית לנעשה משטחה. אנחנו הושטנו יד ללבנון והצענו לה סיוע הומניטארי. אותה היד שהושטה, היא גם אגרוף הברזל שיגיב מול כל תוקפנות והפרת ריבונות ואני קורא לקהילה הבינלאומית לפעול להשבת היציבות בלבנון".

על ניסיונות של מתקפות סייבר על ישראל: "בשנים האחרונות חלה עלייה משמעותית במספר ההתקפות שביצעו גורמים עוינים, כולל איראן ושלוחותיה, המבקשים לגשת למערכות התקשוב של התשתית הלאומית של ישראל. לנוכח העלייה הזו - מכמה התקפות בודדות לעשרות התקפות בשנה - ישראל הוכיחה את היכולת לפתח את חוסנה, את היתרון הטכנולוגי שלה ואת היתרון האיכותי שלה באזור".

גנץ אמר כי: "ישראל פועלת באופן רציף להגנה מפני מתקפות סייבר- במאי 2019, כחלק מהסכסוך המתמשך של ישראל עם ארגוני הטרור ברצועת עזה, ביצעה ישראל לראשונה מתקפה קינטית על הבניין בו ישב פיקוד הסייבר של חמאס".

עוד אמר: "המתקפה בוצעה בעקבות פעילויות שמטרתן הייתה לפגוע בתשתיות הישראליות במרחב הסייבר, כפי שניסו לעשות תוקפי הסייבר של חמאס בהנחיית איראן. במהלך מבצע "שומר החומות", פגענו בראש פיקוד הסייבר של חמאס, ג'ומעה טחלה. כמו כן זיהינו ופגענו בכמה תוקפי סייבר, ציוד ותשתיות אשר שימשו את פיקוד הסייבר של חמאס".

לסיום אמר: "המסר שלנו הוא ברור - תהיה זו רקטה או מקלדת - לא נסבול איום על אזרחי ישראל".

על היתרי הייצוא הביטחוני ממשרד הביטחון המאפשר לרגל אחרי אזרחים ונמצא בשימוש במשטרים דיקטטוריים ברחבי העולם: "אנו מודעים לפרסומים האחרונים על שימוש במערכות שפותחו על ידי חברות סייבר ישראליות מסוימות. ישראל, כדמוקרטיה מערבית ליברלית, מפקחת על יצוא מוצרי סייבר לפי חוק הפיקוח על הייצוא הביטחוני ובהתאם למשטרי פיקוח בין-לאומיים".

עוד הסביר: "כמדיניות, מדינת ישראל מתירה ייצוא של מוצרי סייבר מפוקחים אך ורק לממשלות, אך ורק לשימוש חוקי, וספציפית למטרות מניעה וחקירה של פשעים וטרור. על המדינות הרוכשות מערכות אלה לעמוד בהתחייבויותיהן לדרישות אלה. אנו לומדים כעת את המידע המתפרסם בנושא".

חמ"ל

20.07.2021 15:57 - לפני 54 ימים

ברק רביד, כתב מדיני - וואלה

גנץ: לומדים את הטענות נגד תוכנת הריגול של NSO

שר הביטחון בני גנץ התייחס היום (שלישי) לראשונה לפרסומים אודות שימוש לרעה בתוכנת הריגול פגסוס של החברה הישראלית NSO, ואמר כי ישראל "לומדת" את הנושא. ""אנחנו מאשרים ייצוא מוצרי סייבר רק לממשלות ורק לשימוש חוקי ולמניעת פשעים וטרור", אמר גנץ בנאום בכנס הסייבר באוניברסיטת תל אביב. "המדינות שרוכשות את המערכות האלה חייבות לעמוד בתנאי השימוש".

בני גנץ # משרד הביטחון

ynet
ידיעות אחרונות

מה שמזעזע הוא שפרשת NSO לא מזעזעת אתכם

חרף החשיפה שהמחישה את הכשל המוסרי בסחר הסייבר והנשק, הציבוריות הישראלית התמקדה השבוע בגלידה. היא לא אוהבת ששוחטים לה פרה קדושה

מאת: הגר בוחבוט

מדגם מייצג בשאלה מהו הסיפור החדשותי המטלטל ביותר בשבוע האחרון בישראל יעלה תשובה חד-משמעית: גלידה. ההחלטה של תאגיד המזון יוניליוור שלא להמשיך למכור את המותג "בן אנד ג'ריס" בהתנחלויות עוררה כאן אמוציות מהסוג ששמור רק למי שבאים עלינו לכלותינו. ואולי בצדק. מי לא אוהב צ'אנקי מאנקי, ועוד בחום הזה. אבל היה השבוע סיפור נוסף, מטלטל הרבה יותר, שאמנם זכה לטיפול תקשורתי מוקפד ומקיף, ועדיין לא הצליח לחלחל לעומק השיח הציבורי. התחקיר על מכונת הריגול הישראלית, בחסות חברת הסייבר ההתקפי הישראלית NSO ומוצר ה"פגסוס" שלה, העלה שאלות קשות - רגולטוריות, מוסריות, טכנולוגיות וחברתיות – שמשמעותן דרמטית פי כמה מסערת הגלידה-בשטחים-כן-או-לא.

ראש הממשלה נפתלי בנט, בעצמו איש הייטק לשעבר וזה שניסה לגייס את NSO למאבק בקורונה עם מערכת מעקב אחרי אזרחים ישראלים, ניצל אתמול (יום ד') את שבוע הסייבר השנתי כדי לנאום בנושא, אולם בדבריו שם הקפיד להתמקד רק בסכנות הנשקפות לישראל בגזרה. אף מילה על פרשת NSO.

פגיעה בזכויות אדם ובחופש העיתונות באמצעות אמצעי מעקב ומכירת נשק (גם אם הוא דיגיטלי), מבית היוצר של תעשייה ישראלית שפועלת בכל העולם כמעט באין מפריע (כנסו וגלו עד כמה באין מפריע), אמורה הייתה לזעזע אותנו ואת בנט לפחות כמו מאות התמונות של מארזי הגלידה שהושלכו לפח והופצו ברשתות החברתיות.

נכון, קשה להשוות. לכולם יש גלידה במקרר, ומנגד הסוגיות שבלב פרשיית הריגול מורכבות הרבה יותר. אבל לשני המקרים יש מכנה משותף: חוסר המסוגלות להכיל ביקורת על מוסדות וערכים שהם בבחינת פרות ארצישראליות קדושות: צה"ל, ציונות, התנחלויות, ובשנים האחרונות גם תעשיות ההייטק והסייבר, מושא גאוותנו. המוח היהודו-ישראלי מתקשה להתעסק עם הקווים האפורים של המוסר האנושי.

NSO היא רק דוגמה מייצגת. לצידה יש חברות שעוסקות בפעילות דומה אך בפרופיל תקשורתי נמוך בהרבה. בזום-אאוט נוסף מתגלה תעשיית נשק ענפה שמיוצאת כמעט לכל מקום, בהליכים רגולטוריים לא לגמרי שקופים. הסיפור הנוכחי אמור היה לעורר את הציבור בעוצמה ולתלות סימן שאלה מעל תהליכי הייצוא האלה שלמדנו לקבל בשתיקה ובהכנעה. לא מוכרחים להבין את נבכי הטכנולוגיה כדי לראות שקורה כאן משהו חמור. הווריד הציוני שקפץ במצח אל מול ההכרזה של "בן אנד ג'ריס" הוא זה שנרפה ונעלם כשאנחנו ניצבים מול סיפורים דוגמת זה של NSO.

החברות האלה, "8200 על סטרואידים" כפי שהן מכונות בתעשייה, מעסיקות את החכמים והמוצלחים שיש לישראל להציע. טובי בנינו מקימים אותן, מתחזקים אותן, מועסקים בהן, רובם ככולם יוצאי יחידות צבאיות מובחרות. ואולי כאן טמונה הבעיה. המעבר המדומיין ממסגרת צבאית-ביטחוניסטית - על תחושת השליחות והתודעה הקיומית הרעועה הנלווית לה - לשוק הפרטי, העשיר (לא רק בכסף), הגדוש בהזדמנויות, מפוקפקות יותר או פחות, הוא בעייתי למדי מבחינה מוסרית.

מי שבמשך כמה שנים פעלו בשם מדינת ישראל, עם כל הגיבוי הערכי הרלוונטי, ממשיכים לפעול רגע אחרי השחרור בשוק הפרטי והפרוץ, עם מערכות מסוכנות ומתוחכמות. חלקם, לפחות לפי שיחות פרטיות, רואים בעצמם שליחים של ממש; הישראלים שעושים סדר עולמי חדש ומחליטים מי בצד של הטובים ומי בצד של הרעים.

עד שלא נלמד להכיל ביקורת - גם אם פנימית בלבד - גם כלפי המוסדות הכי חשובים שלנו, נמשיך להזדעזע מגלידה ולעצום עיניים מול עסקאות ריגול, מעקב ונשק. ועד שלא נתחיל להתקומם מפרשיות ריגול ממש כאילו הזיזו לנו את הגלידה, לא נוכל למשוך אחרינו את נבחרי הציבור ואת הרגולטורים, ולהתחיל לתקן.

ISRAELDEFENSE

רה"מ בנט: מקימים מגן סייבר עולמי במטרה לשלב כוחות ומשאבים

"אם נילחם לבד – נפסיד, אבל אם נילחם ביחד – ננצח", אמר ראש הממשלה במהלך שבוע הסייבר השנתי המתקיים בימים אלה באוניברסיטת תל אביב

"כיום כל הענפים הם פגיעים ומהווים פוטנציאל למתקפת סייבר – המים, החשמל, המזון, המטוס והמכוניות שלנו. כיום המתקפה הטובה ביותר נגד מדינות היא מתקפת סייבר. אתה רק צריך ידע בסיסי וקו אינטרנט והמתקפות הללו יגדלו באופן אקספוננציאלי. אני רואה בכך את אחד האיומים העיקריים לביטחון המדינה ולביטחון העולם", כך אמר אתמול (ד') ראש הממשלה, נפתלי בנט במליאת שבוע הסייבר שנערך באוניברסיטת תל אביב.

הדבר החכם ביותר שעשינו כדי להתמודד עם איומי הסייבר היה לאפשר לתעשייה הפרטית לשגשג, ואנחנו זקוקים לעוצמתה", הוסיף ראש הממשלה. "בישראל יש לנו הרבה אנשים ממש חכמים שבגיל צעיר נכנסים לצבא ולוקחים על עצמם אחריות עצומה, ובזכות זה אנחנו רואים את הפריחה היום. זה הסוד של ישראל, לגרום לחבורה של אנשים חכמים באמת לשבת יחד. סייבר זה משהו שלא תוכלו לביים, כל מה שאנחנו יכולים לעשות זה לאפשר לזה לקרות, לאפשר לכל האנשים האלה להתכנס וליצור את ההיתוך הזה".

בנט התייחס גם לתעשיית הגנת הסייבר הישראלית ואמר כי "מתוך כל 100 דולר שהושקעו במגזר העסקי בסייבר ברחבי העולם, 41 דולר הושקעו בחברות הגנת סייבר ישראליות. הפצת רעיונות ולא ריכוזם במקום אחד מהווים את אחת החוזקות המשמעותיות של ישראל. אני חושב שאנחנו הראשונים בעולם שייצרו סוכנות סייבר לאומית אחת, גוף אחד שממוקד לנושא ובאחריותו להגן על כל התשתיות הקריטיות בישראל לצד סיוע ועבודה מול המגזר הפרטי, מתוך מטרה לעבוד ביחד, לחקור ולשתף מידע.

"כשמדינה תוקפת את אחת החברות שלנו אנו רוצים שכולם יידעו. אם אתה באוטובוס צפוף ויש כייס שמנסה לגנוב את חפציך אתה יכול לשתוק או שתוכל להוציא ספריי, לרסס אותו בפרצוף ולסמן אותו על מנת שאחרים ידעו להתאגד ולהגן על עצמם. סוכנות הסייבר הלאומית היא הריסוס והמגפון ההוא. מערך הסייבר עובד עם כל סוכנויות הביטחון שלנו – המוסד, השב"כ, 8200, עכשיו אנחנו מתרחבים ופונים לכל העולם ומכריזים על מגן הסייבר העולמי, תוך שימוש באותם עקרונות של קישוריות סייבר, כי אם אתה נלחם לבד – תפסיד, אבל אם נילחם ביחד – ננצח".

"אם איראן תתקוף מתקן מים בבלגיה בשעה 10:35, הם (הבלגים) יתקשו לזהות לבד מה זדוני, אך מאחר ובד"כ מתקפות סייבר נעשות במספר מוקדים – עבודה ביחד תסייע לאתר את המקור מהר ולהתמודד בהתאם. אם התוקפים יתקפו מתקן מים צ'יליאני כעבור דקה ומתקן הודי כעבור שלוש דקות, על ידי שיתוף מידע ניתן מיד להבדיל להתריע בזמן אמת, לאחד משאבים משותפים, לאתר את הפורץ ולפתח חיסון ולפזר אותו לכל החברות הנמצאות ברשת זו".

ראש הממשלה חשף כי כבר נחתמו הסכמי הבנות עם מדינות שונות, "אבל עכשיו אנחנו לוקחים את זה לשלב הבא למגן סייבר בזמן אמת והיום אנו מזמינים את כל המדינות ברחבי העולם לשלב כוחות במגן הגנת הסייבר העולמי".

EDULUGU. Iisraelis õpivad lapsed küberturvalisust põhikoolis, siis lähevad nad armee küberüksustesse ja seejärel asuta

Iisraeli küberseemned on hakanud vi

MERILI ARJAKAS
toimetaja, Tel Aviv

Tel Avivi ülikooli andmetel müüdi eelmisel aastal Iisraeli küberturvalisuse tehnoloogiat 6,85 miljardi dollari eest. Iisraeli riikliku küberdirektoraadi (Israel National Cyber Directorate, INCD) andmetel kaasasid 2021. aasta esimesel poolaastal riigi küberturvalisuse ettevõtted investeeringuteks 3,4 miljardit dollarit, mis on 41 protsenti kogu maailma investeeringutest selles valdkonnas.

«Rohkem USA dollareid investeeritakse küberturvalisusesse Iisraelis kui USAs,» lausus Tel Avivis toimunud konverentsil Cyber Week Iisraeli juhtiv küber- ja tehnoloogiajulgeoleku ekspert erukindral Isaac Ben-Israel.

Juba on ületatud eelmise aasta kogutulu 2,9 miljardit dollarit, mis oli toona 70 protsenti rohkem kui aasta varem. Sealhulgas moodustavad riigi rahaeraldised küberturvalisus- ja finantstehnoloogia investeeringutest väga väikese osa, sest lisaturgutust enam andma ei pea.

Rohkem kui kolmandik maailma küberturvalisuse ükssarvikutest on Iisraeli päritolu. Kokku on Iisraelis umbes 70 ükssarvikut ehk üle miljardi dollari väärt idufirmat. Umbes, sest isegi selles valdkonnas tööstavad inimesed ei oska täpselt öelda, kui palju sellel aastal juurde on tulnud: kahe aastaga on ükssarvikute arv peaaegu neljakordistunud.

Rohkem kui kolmandik maailma küberturvalisuse ükssarvikutest on Iisraeli päritolu.

Inimeste harimine ja koostöö

Iisraeli kõrgtehnoloogia eduloost on jutustatud üle kümne aasta. 2009. aastal avaldasid Dan Senor ja Saul Singer menuraamatu «Start-up Nation», mis uuris, kuidas on keerulises regioonis asetsevas ja ilma loodusvaradeta riigis suudetud luua inimese kohta rohkem iduettevõtteid kui kusagil mujal: 2021. aastal üks 1400 inimese kohta, mis on ligi kaks korda enam kui Eestis.

«Isegi mina ei oodanud selliseid tulemusi, mis meil täna on,» sõnas Ben-Israel, kes on praegu Tel Avivi ülikooli küberuuringute keskuse direktor. Kogu oma karjääri jooksul sõjaväes, parlamendi liikmena ja peaministri nõunikuna on ta olnud Iisraeli küberarengu eestvedaja.

Ben-Israeli sõnul põhineb Iisraeli küberedu kolmel sambal: inimkapital, ettevõtted ja valitsus. Kolme elemendi koosmõjus on võimalik luua keskkond, mis võimaldab inimestel kiiresti kohaneda ning valida välja õigeid tegutsemisviise. «Me nimetame seda *start-up*-kultuuriks,» ütles Ben-Israel.

See on alt-üles-põhimõttel töötav süsteem, kus noored inimesed tulevad uute ideedega ja proovivad neid ellu viia. 95 protsenti idufirmadest surebki, aga seda ei nähta mitte süsteemi puuduse, vaid edu tagajana: ellu jäävad vaid need, millel on potentsiaali. Lähtkukkumine on tavaline, mistõttu ei takista üks või mitu luhtaminekut uue idufirma loomist ja investeeringute kaasamist.

«Me tapamegi ettevõtteid,» selgitas Iisraeli innovatsiooniameti juht Sagi Dagan agentuuri rolli. Nende ülesanne pole mitte riigi toetusest sõltuvaid ettevõtteid poputada, vaid kindlustada, et idufirmad tõuseksid oma jalgadele. Kes seda ei suuda, kaotab valitsuse toetuse kiiresti.

Ettevõtetesse ei pumbata niisama raha sisse, vaid laene antakse vaid juhul, kui idufirma suudab ise kaasata vähemalt sama palju erainvesteeringuid.

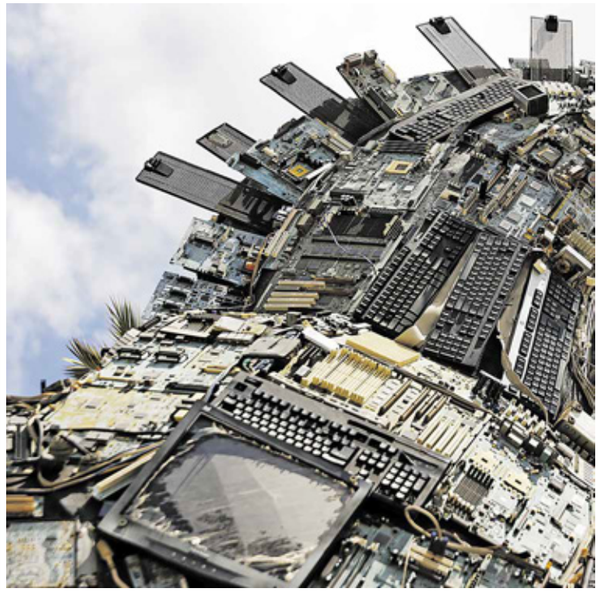
Ka see ei taga, et idufirmast saab tulu teeniv ettevõte, sest 70 protsenti valitsuse investeeringutest muutub grantideks ehk rahasüstideks, mis tagasi ei teeni. Valitsus on valmis riskima, sest edukad investeeringud kannavad vilja nii otseselt maksurahast kui ka kaudselt, luues ettevõtlust soosiva kultuuri.

Investeeringud teadusesse ja arendusse

Iisrael investeerib teadus- ja arendustegevusse maailmas kõige rohkem: 2018. aastal ligi viis protsenti riigieelarvest. Teaduse ja arenduse tähtsustamise eest on Iisrael tänu võlgu Prantsusmaa presidendile Charles de Gaulle'ile, kes pärast kuuepäevast sõda kehtestas 1968. aastal Iisraelile relvamüügiembargo. «Me saime aru, et peame hakkama ise oma tehnoloogiat arendama,» selgitas Dagan, kuidas Iisrael reageeris.

Poole sajandi jooksul on Iisrael muutunud teaduse ja arenduse maast iduettevõtete riigiks ning viimase kümnendi jooksul on põhirõhk läinud sellele, kuidas olemasolevat suureks kasvatada (nn *scale-up*).

Investeeringutest üksi ei piisa, kui pole haritud inimesi. Kohustuslikku sõjaväeteenistust võib vaadelda kui hariduse lisataset. Iga aasta lahkub Iisraeli kaitseväest tuhandeid sõdureid, kelle tehnilised oskused on võrreldavad professionaalide omaga mujal maailmas. Pärast ajateenistuse lõppemist lähevad nad tööle Iisraeli või välismaistesse tehnoloogiafirmadesse või asutavad oma iduettevõtte.



Ajakirjanik külis konverentsil Cyber Week 2021 Iisraeli välisministeeriumi kutsel.

Kõrbelinnakust on saamas uus kõrgtehnoloogia- ja innovatsioonikeskus

Juulikuu südapäeval on Be'er-Shevas 36 kraadi, puhub kuum kõrbetuul. Ainsad väljas liikujad hüppavad ühest jahutatud majast teise.

Be'er-Shevas elab veidi üle 200 000 inimese. Erinevalt mitmest teisest Iisraeli linnast on see ehitiselt ja usuliselt võrdlemisi mitmekesine: araabia beduiinidest immigratsioonilainetes tulnud Lähis-Ida päritolu sefardi, India ja Etioopia juutideni. Nõukogude Liidu kokkuvarisemise järel Iisandusid nn vene juudid, kes pärast sõlma ülekaalukat esindusega reaalaladel. Värsket hingamist toob juurde linnas asuv Ben Gurioni ülikool, mis on Iisraelis suuruselt kolmas.

Kogu Negevi kõrberegioonis elab umbes kümme protsenti Iisraeli elanikkonnast, kuigi see moodustab 60 protsenti riigi maa-alast. Ressurssi ei saa kõrvale jätta, sest Iisraeli elanikkond on ligi seitse korda suurem kui Eesti oma, kuid maa-ala kaks korda väiksem – okupeeritud territooriume arvestamata, sest Iisraeli valitsus seab palestiinlaste liikumisele piiranguid.

Mõne aasta eest tehtud küsitlus näitas, et pooled tudengitest tahaksid pärast lõpetamist Be'er-Shevasse elama jääda, kui neil oleks võimalik leida hea töökoht. Seega on olemas nii maa kui ka inimeste tahe seal elada. Kuidas aga luua sobiv keskkond?

Ben Gurioni ülikooli professor Dan Blumberg ütles, et Be'er-Shevast on saanud Iisraeli viimane kõrgtehnoloogia keskus. Esimene koostöölepe Deutsche Telekomiga sõlmiti 2004. aastal, misjärel hakkas ülikooli ülles ehitama võimekust teha koostöödd akadeemia ja rahvusvaheliste korporatsioonide vahel.

Suur hüpe on aga toimunud viimase seitsme aasta jooksul. Ülikooli kõrgtehnoloogia tööstuspargis on valmis ehitatud neli hoonet ning mõnesajast tehnoloogiasektori töökohast jõutud paari tuhandeni. Kavandatud on tosin hoonet, mis ühendaks ettevõtted, ülikooli uuriminiskeskused, riigiasutused ja MTÜd.

Tööstuspargi inimesed rõhutavad ettekannetes füüsilise lähedluse tähtsust: neli hoonet, neli restorani. Kõik kohtuvad kõigiga. «Me tahame saada esimeseks innovatsioonipiirkonnaks Iisraelis,» avaldas Blumberg tööstuspargi ambitsiooni.

Innovatsioon aga ei põhine ainult majandusel, vaid ka sotsiaalsel arengul. MTÜ Tech7 juht Daniel Einhorn kirjeldab seda kui kogukonna ülesehitamist alt üles. Nad said valitsuselt ligi 300 000 euro suuruse grandi, et arendada Be'er-Shevasse küberkogukonda. Selle eest on nad toonud kokku idufirmades töötavaid inimesi, loonud inkubaatori alustavate ettevõtjate toetamiseks ning korraldavad töötube gümnaasiumiõpilastele, kes tahavad arvutiteadusi õppida.

Valitsus hakkas tööstusparki investeerima 2014. aastal, ent rahasüstidest ehk tähtsamgi on plaan tuua rohkem sõjaväe tehnoloogiaüksuseid Be'er-Shevasse. 2018. aastal leidis ajaleht Haaretz, et Iisraeli 700 kübertehnoloogiafirma asutajatest 80 protsenti on läbinud Iisraeli sõjaväe luureteenistuse.

Be'er-Sheva tehnoloogiaparki on üle toodud Iisraeli riiklik küberdirektoraat (INCD), mis sarnaneb Eesti riikliku infosüsteemide ametiga ning mille eesmärk on tugevdada Iisraeli positsiooni kübervaldkonnas.

Ben Gurioni ülikooli kõrgtehnoloogia tööstuspark.
FOTO: TWITTER

ıvad oma idufirmasid.

.lja kandma

Tuhandetest pahavaraga nakatunud arvuti- te ja nutitelefonide tükkidest kokku pandud «Küberhobune» Tel Avivi ülikooli ees.
FOTO: AMIR COHEN / REUTERS / SCANPIX

Isaac Ben-Israel: arendada tuleb ökosüsteemi tervikuna

Pole muud viisi ühiskonna kerksuse suurendamiseks kui haridus, ütles intervjuus Postimehele Iisraeli juhtiv küber- ja tehnoloogiajulgeoleku ekspert erukindral Isaac Ben-Israel.

Mida peaksid teised riigid nagu Eesti tegema, et olla kübermaailmas edukad?

Kogu küsimus on selles, kui palju investeerida tehnoloogiasse. Eesti, nagu ka Iisrael, on võrdlemisi arvutipõhine riik. Seetõttu oli DDoS-rünnak (teenusetõkestusrünne ehk arvutivõrgu ülekoormamine – M. A.) 2007. aastal mõne nädala jooksul tõhus. DDoS-rünnakute eest on end võrdlemisi lihtne kaitsta, kui osata neid oodata. Aga see oli esimene kord, kui rünne oli seotud riigiga. Ründasid nn vihased Vene kodanikud – me kõik oleme üsna kindlad, et selle taga oli Vene valitsus. Pärast seda on Eesti teinud enda kaitsmisel head tööd.

Mis on siiski Iisraeli edu võti?

Iisrael liigub nii kiiresti edasi, sest meil oli valitsuse plaan, mida toetasid kõik ministrid. Küberturvalisuse puhul pole küsimus ainult parima tehnoloogia arendamises või ostmises, vaid kogu ökosüsteemi edendamises. Peaminister [Naftali Bennett] tõi [konverentsil Cyber Week 2021] näite, et kui arendaja läheb Iisraelis lõunasoögile, siis kohtub ta inimestega ettevõtetest, ülikoolidest, sõjaväe küberüksustest. Nad kõik tegelevad küberturvalisusega, aga eri nurkade alt. Iisrael on nii väike riik, et inimesed kohtuvad, midagi juhtub – ma isegi ei oska öelda, mis see on, aga sünnib midagi uut. Seetõttu usume tugevalt interdistsiplinaarsusesse.

21. sajandil lahendame probleeme tehnoloogia abil, aga probleemid ise ei ole puhtalt tehnoloogilised. Küberturvalisuse probleeme ei saa mõista, kui ei võta arvesse inimpsühholoogiat. Näiteks öngitsejaid peab teadma, mis peibutaks ohvrit nupule vajutama. Peale selle peab võtma arvesse ühiskonna psühholoogiat, juriidikat ning turvalisuse ja privaatsuse vastuolu.

Võtame näiteks info jagamise, mida riikidel on väga keeruline teha; aga see ei ole oma olemuselt tehnoloogiline probleem, vaid seotud inimolemusega. Juba 16. sajandil ütles Francis Bacon, et teadmine on jõud. Inimesed usuvad, et teadmisi jagades annavad nad jõudu ära.

Iisraelis aga on info jagamine olnud kübertehnoloogia edu alus, sest ilma avaliku uurimistööta innovatsioon nii kiiresti ei edene.

Kübiturvalisuse eesmärk on tagada turvalisus ja usaldus ühiskonnas. Kuidas suurendada ühiskonna kerksust ajal, kui küberrünnakud on sagenemas?

Pole muud viisi ühiskonna kerksuse suurendamiseks kui haridus. Me õpetame kübiturvalisuse vajalikkust kõikidele, aga selle lihtsamaid põhitõdesid juba algkoolis: kuidas elada kübermaailmas. See on nagu autosõiduga. Juhiloa saamiseks peab Iisraelis olema vähemalt 17 aastat vana, aga juba algklassides õpitakse, kuidas teed ületada.

Samamoodi õpitakse algkoolis, millised probleemid võivad kaasneda Facebooki või postitamisega ehk mis on privaatsus sotsiaalmeedias. Me õpetame, kuidas ületada küberteed kübermaailmas.

Kas Iisrael õpetab programmeerimist kõikidele koolilastele?

Ei, see sõltub õpilasest. Meil on keskkooli lõpus riigieksamid. Heebrea keel, inglise keel ja matemaatika on kohustuslikud, aga on nimekiri valikainetest, milles eksam teha. Me lisasime arvutiteadused sellesse loendisse. Kui õpilased saavad selle eksami valida, siis koolid peaksid võimaldama arvutiõpet. Peaaegu iga keskkool seda ka teeb.

Professor Isaac Ben-Israel Cyber Week 2021 konverentsil avakõnet pidamas.
FOTO: GIDEON MARKOWICZ / SCANPIX

PIKEMALT LOE POSTIMEES.EE

Nuhkvara valmistab inimõiguslastele peavalu

Iisraeli kõrgtehnoloogia ettevõtte NSO Group telefonide häkkimise nuhkvara Pegasust ümbritsevad skandaalid avavad Iisraeli kõrgtehnoloogia pimedamat poolt.
FOTO: DADO RUVIC / REUTERS / SCANPIX

Vahetult enne Cyber Weeki konverentsi algust avaliikustas rahvusvaheline meedia, et Iisraeli kõrgtehnoloogia ettevõtte täht NSO Group on müümud teleforide häkkimise nuhkvara Pegasus autoritaarsete riikide valitsustele, et nood saaksid luurata poliitilistе dissidentide, ajakirjanike, inimõigusaktivistide ja teiste riigijuhtide järele.

Nuhkvara annab luurajatele võimaluse lugeda kõiki telefonisõnumeid, tuvastada kasutaja asukohta ning pääseda telefoni kaamerale ja mikrofonile ligi selle omaniku teadmata.

NSO üles, et nemad müüvad Pegasuse nuhkvara vaid Iisraeli valitsuse heakskiidul teistele riikidele kuritegevuse ja terrorismi ennetamiseks. Meedias avaliikustatud andmetel on aga Pegasust kasutatud ajakirjanike ja opositsioonitegelaste järel luuramiseks vähemalt 2016. aastast.

Pegasust ümbritsevad skandaalid iseloomustavad Iisraeli kõrgtehnoloogia pimedamat poolt. Peaaegu ükski konverentsil osaleja ei olnud nõus avalikult NSO tegevust laitma. Korduvalt tõmmatakse paralleele teiste rünnakvahenditega: kas pistoleid tootvat riiki saab pidada vastutavaks selle eest, kui nende relvaga lastakse mõni süütu inimene maha?

ÜRO eksperdid ei pea NSO õigustusi piisavaks. 12. augustil kutsus rühm ÜRO eriraportööre üles kehtestama ülemaailmset moratooriumi nuhkvara müügile ning nõudis, et NSO ja Iisrael avaliikustaksid rohkem, milliseid samme nad on astunud, et takistada tarkvara kasutamist inimõiguste rikkumiseks.

Palestiina inimõigusaktivistid heidavad ette, et Iisrael on luureteenistuse laboriks, kus sõjaväe kõige salajasemates üksustes saavad noored ajateenijad väljaõppe palestiinlaste ja teiste Lähis-Ida riikide elanike järel nuhkimiseks, et siis oma teadmisi ära kasutada erasektoris vähekontrollitud tegevuseks.

Haaretzi 2018. aasta uurimus leidis, et Iisraelist on saanud tsiviilelanike järel nuhkiva tehnoloogia suurim eksportija. Iisraeli kaitseministeeriumi peab heaks kiitma kõik relvamüügitehingud, aga lepingute üksikasjad on salastatud. Igal aastal avaldab ministeerium ainult müügitehingute koguväärtuse ning arvu, mitmesse riiki on tehnoloogiat müüdud.

Lisaks Iisraeli relvastusele liiguvad ringi ka Iisraeli töötajad. Üheks Iisraeli töötajatest huvitatud firmaks peetakse Araabia Ühendemiraatides (AÜE) tegutsevat erafirmat DarkMatter, mis Reutersi andmetel täidab lepinguid AÜE valitsuse jaoks. Inimõigusorganisatsioonid süüdistavad AÜE valitsust laialdases inimõiguste rikkumises.

Iisraeli väljaande Yedioth Ahronoth andmetel palkas DarkMatter Iisraeli kaitseväes Unit 8200s teenistuse läbinud inimesi mitu aastat enne seda, kui AÜE ja Iisrael teineteist tunnustasid.

Küberrünnakuteks valmistuti enne nende levikut

Iisrael oli 1980. aastatel Ameerika Ühendriikide, Nõukogude Liidu, Suurbritannia ja Prantsusmaa kõrval üks riikidest, mille luureagentuurid mõistsid, et kübertehnoloogiat saab kasutada rünnakvahendina, selgitas Isaac Ben-Israel. Varasemal aastakümnel hakati laiemalt kasutama esimesi personaalarvuteid, mis tähendas, et esimest korda hoiustati teavet digiteeritud kujul.

See omakorda pakkus magusat sihtmärki salateenistustele. Paralleelselt asendusid arvutitega ka senised telefonikeskjaamad, mis tähendas, et telefonisidе jälitamiseks ja pealtkuulamiseks pidid luureagentuurid tungima arvutivõrku.

Iisraeli julgeolekuasutused jõudsid järeldusele, et peale spioneerimise saab kübertehnoloogiat kasutada ka relvana. Ben-Israel tõi näiteks lennunduse.

Vietnami sõja ajal tekkis elektroonilne sõjapidamine, kui hakati segama lennukite elektroonikasüsteeme. Seejärel muutusid 1990. aastatel lennukid sõltuvaks paroolid olevatest arvutitest, mis andis sõjaväele luurevõimaluse kaitsta riiki luureagentuuride sisse häkkides.

Ben-Israel töötas 1990. aastate lõpus Iisraeli lennuväe luures ning saatis toonasele peaministrile Ehud Barakile kirja, kus selgitas, et kübertehnoloogiat saab kasutada iga arvutitel põhineva süsteemi vastu. Seni kuni seda tõika mõistavad vähesed, on Iisraeli valitsusel eelis.

Ben-Israel aga hoiatas, et ühel päeval näevad kõik arvutirünnakuteks potentsiaali ning plussist saab kohe miinus, sest Iisrael on digiriik. Peaminister võttis kindlalt hoiatust tõsiselt ning andis riigikaitsenõukogule ülesande hakata arendama kübervõimekust. 2002. aastal asutas valitsus esimese riigina riikliku infoturvalisuse ameti kriitilise infrastruktuuri arvutivõrkude kaitsmiseks. Selle alla lähevad tsiviilsüsteemid, nagu energiatootmine, veevarude tagamine, tervishoid ja transport.

«Me tegime seda enne, kui meid rünnati, sest kartsime, et meil pole piisavalt aega reageerimiseks. Tegemist on võrdlemisi lihtsa tehnoloogiaga,» selgitas Ben-Israel valitsuse valmisolekut uade tehnoloogiasse panustada.

«Seejärel, 2010. aastal ründas keegi Iraani tuumatsentrifuuge, mida kasutatakse uraani rikastamiseks,» ütles ta (rünnakut on omistatud Iisraelile ja USA-le, aga kumbki riik pole seda kinnitanud – M. A.).

Ben-Israeli sõnul kajastati Stuxneti juhtumit kogu maailma meedias, sest esiteks oli see hea lugu virtuaalsest viirusest ning teiseks oli see esimene kord, kui kübirrünnak tõi kaasa otsese kahju füüsilises maailmas.

Ben-Israeli sõnul võttis ta rünnaku järel ühendust peaminister Benjamin Netanyahuga ning tuletas meelde varem valitsusele saadetud kirja, öeldes, et nüüd sai kogu maailm teada kübertehnoloogia sõjalisest potentsiaalist.

R. REPUBLICWORLD.COM

'Cyber Horse' Made Of IT Waste Stands Tall At Israel Cyberweek: Here's What It Symbolizes

During the Cyber Week conference at Israel's Tel Aviv University on Sunday, the Cyber Horse exhibit made of IT waste was given prime of place near the entrance

Vidit Dhawan

During the annual Cyber Week conference at Israel's Tel Aviv University on Sunday, the well known Cyber Horse exhibit was once again in the limelight, placed as it was at the entrance of the event. The exhibit is constructed with used computer and mobile phone parts infected by viruses and malware. Israel-based creative group 'No, No, No, No, Yes' sculpted the Cyber Horse as a means of referencing the Trojan horse in Greek mythology. The group had attempted to make a statement about the dangerous effects of malware, with the horse representing a carrier of potentially "bad news" trying to infiltrate cyberspace.

What does the 'Cyber Horse' symbolize?

In computing, a Trojan Horse, nicknamed a "Cyber Horse," is any malware that misleads users of its true intent. The term is derived from the ancient Greek story where a deceptive Trojan Horse led to the fall of the city of Troy. 'Trojans' are usually spread by some form of social engineering. For example, a disguised email attachment or a fake advertisement on social media could be used to mislead users to retrieve access to a users' personal information such as passwords.

What is Tel Aviv University's Cyber Horse made of?

Tel Aviv University's Cyber Horse status is made out of thousands of computer and cell phone components that were once working fine before they became infected with viruses. The Cyber Horse was the idea of Gideon Amichay, an Israeli designer and communication artist. The Cyber Horse was built as a tribute to 2016's Cyber Week at Tel-Aviv University. Israel is a country that is well known for its advanced security technology.

Cybersecurity: How to recognize a Trojan virus?

A Trojan horse virus is a dangerous virus as it can not only remain on a user's device for months but also the user is often not aware that their device has been affected. While it is difficult to identify a Trojan virus it is not impossible. A Trojan virus causes a user's computer settings to constantly change and is often also accompanied by a loss in computer performance. The best way to recognize a Trojan virus is by searching a device using a Trojan scanner or malware removal software.

HAMODIA
THE DAILY NEWSPAPER OF TORAH JEWRY

Spyware Allegations Roil Indian Parliament

India's Parliament erupted in protests on Tuesday as opposition lawmakers accused Prime Minister Narendra Modi's government of using military-grade spyware to monitor political opponents, journalists and activists.

The session was disrupted repeatedly as opposition lawmakers shouted slogans against Modi's government and demanded an investigation into how the spyware, known as Pegasus, was used in India.

"This is a national security threat," an opposition Congress party official, Kapil Sibal, said at a news conference.

The protests came after an investigation by a global media consortium was published on Sunday. Based on leaked targeting data, the findings provided evidence that the spyware from Israel-based NSO Group, the world's most infamous hacker-for-hire company, was used to allegedly infiltrate devices belonging to a range of targets, including journalists, activists and political opponents in 50 countries.

In India, the list of potential surveillance targets included senior Congress party leader Rahul Gandhi, at least 40 journalists, a veteran election strategist critical of Modi and a top virologist, according to the investigation.

Newly appointed information technology minister Ashwani Vaishnaw dismissed the allegations on Monday, calling them "highly sensational," "over the top," and "an attempt to malign the Indian democracy."

Minutes after his statement in Parliament, India's independent The Wire website – part of the media consortium – revealed that his name also appeared on the list as a potential surveillance target in 2017. He was not a member of Modi's Bharatiya Janata Party at that time.

NSO Group has said it only sells its spyware to "vetted government agencies" for use against terrorists and major criminals. The Indian government has so far dodged questions over whether it is a client of the group.

Defense Minister Benny Gantz said that his office will investigate the charges and "take appropriate action" if indicated.

Gantz on Tuesday stressed that "as a matter of policy, the State of Israel authorizes the export of cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism. The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject," The Times of Israel quoted him as saying.

Gantz, who was speaking at a Cyber Week conference at Tel Aviv University, did not mention NSO Group by name.

In India, the investigation fueled a slew of angry reactions from officials.

Home Minister Amit Shah called the investigation an attempt to "derail India's development trajectory through their conspiracies" and said it was "timed to cause disruptions in Parliament."

The former IT minister, Ravi Shankar Prasad, said there was "not a shred of evidence linking Indian government or the BJP" to the allegations. Prasad called it an international plot to defame India.

Rights groups say the findings bolster accusations that not just autocratic regimes but also democratic governments, including India, have used the spyware for political ends.

It has also intensified concerns of a democratic backsliding and erosion of civil liberties under Modi. Recently, the Washington-based Freedom House downgraded India, the world's most populous democracy, from "free" to "partly free."

CISION
PR Newswire

Israel's 11th Annual Cyber Week Conference Highlights Record Cyber Funding and Critical Need For Coordinated Cyber Response

Israel's top politicians, global cyber policymakers, and C-level executives from multinational companies and cutting-edge start-ups from 80+ countries took part in Cyber Week

Attendees and speakers tackled unprecedented cyber challenges and methods to counter those threats and strengthen cybersecurity

TEL AVIV, Israel, July 21, 2021 /PRNewswire/ -- Prime Minister Naftali Bennett, Defense Minister Benny Gantz, and Minister of Public Security, Omer Bar Lev addressed national level cyber threats at Israel's 11th annual Cyber Week Conference, and were joined by cyber heads from the US, UK, Germany, Singapore, Czech Republic, and elsewhere. Private sector giants such as IAI, IBM, Checkpoint and Microsoft also took part alongside cutting edge cyber startups and investors such as YL Ventures.

Cyber Week's hybrid in-person-online conference, which is hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology and Security, occurred against the backdrop of unprecedented opportunities and challenges in the cyber sphere. Ransomware attacks nearly doubled in the past year to top 300M and the biggest ever publicly acknowledged payout to hackers was set at $40 million. Cyber warfare continues its rapidly growing military importance, and investments in cyber security tech reached $7.8 billion, a record level, two-thirds of which went to US and Israeli companies.

The conference touched upon the themes of today's unprecedented cyber business environment, Israel's Prime Minister Naftali Bennett pointed out that $41 out of every $100 dollars world wide is going to an Israeli startup and investment worldwide is skyrocketing. Conference speakers also touched upon the increasing frequency and danger of cyberattacks to global supply chains and the critical need to share information and mount of coordinated defense. Priminister Bennett and others highlighted Israel's efforts, including 24 MOUs and establishment of a dedicated National Cyber Directorate led by Yigal Unna. Lastly, the Prime Minister invited other nations to join a global cybernet shield initiative to jointly coordinate the fight against cyber threats globally.

"Today the best bang for your buck is a cyber attack and it's just going to grow exponentially, and that makes me worried. As Prime Minister of Israel, I view this as one of the top threats to Israel's national security and the world's security," said Israeli Prime Minister Naftali Bennett.

Prime Minster Bennett also spoke about the need for further cooperation, "If you're on a crowded bus and there is a pickpocket who tries to steal your things you can be silent or you can take out red spray, spray him in the face, and mark him as a criminal so everyone else can band together and defend themselves, our national cyber agency is that spray and that megaphone. That same national network [Israel's National Cyber Directorate] is opening up and we're announcing the global Cybernet Shield, using the very same principles of cyber connectivity because if you fight alone you will lose, but if we fight together we will win."

Israel's Defense Minister, Benny Gantz, expressed similar sentiments and called for a cyber version of Israel's famous anti-missile defense system, Iron Dome, "Cyber is now a vulnerable space that must be protected like the sea, space, air, and ground," He also called for a no-tolerance policy by the Israeli government when it comes to Cyber attacks, "Our message is very clear - be it a rocket, or a keyboard, we will not tolerate anyone to threaten our people."

About CyberWeek:

Cyber Week is a leading international cybersecurity event that provides the unique opportunity for experts from industry, government and academia to share their knowledge about the challenges and opportunities in the field. Cyber Week is hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology and Security, at Tel Aviv University, headed by Major Gen. (Ret.) Prof. Isaac Ben-Israel together with the National Cyber Directorate at the Prime Minister's Office, The Ministry of Economy and Industry and the Ministry of Foreign Affairs.

“Acum pregătesc un program pentru guvern, aşa cum am făcut în urmă cu zece ani pentru securitate cibernetică, dar acesta are scopul de a face Israelul una din primele cinci ţări din lume în Inteligenţă Artificială (IA). Nu a fost încă discutat de guvern, dar azi dimineaţă (20 iulie - n.r.) l-am informat pe prim-ministrul Naftali Bennett despre stadiul acestui program. L-am numit Programul naţional pentru o Inteligenţă Artificială Sigură pentru că IA, care este o disciplină care se dezvoltă foarte repede, ne va face mai vulnerabili la atacuri cibernetice. Cu excepţia situaţiei în care o construim de la început să fie sigură”, a mai afirmat Isaac Ben-Israel.

“Avem şi clienţi care vin la noi când ‘casa le arde’ “

Pavel Gurvich, cofondator şi CEO al companiei de securitate cibernetică Guardicore, este unul dintre tinerii din armata israeliană care a urmat drumul spre antreprenoriat după ce s-a întors la viaţa civilă.

“Am vrut să stau în armată minim posibil, trei ani, dar am ajuns să petrec în armată aproape 13 ani. Deci nu a mers cum mă aşteptam, dar am cunoscut mulţi oameni interesanţi şi am învăţat multe. După aceea, împreună cu un prieten, ne-am gândit să deschidem compania”, a povestit el cu umor.

Guardicore are circa 280 de angajaţi, din care 150 în Israel, iar restul în America de Nord, Europa şi Asia. Firma, “care este într-o creştere foarte rapidă”, a reuşit să atragă investiţii de 110 milioane de dolari până acum şi are clienţi pe cinci continente.

“Suntem o companie care a dezvoltat o soluţie de software pentru a segmenta reţelele. Am folosit conceptul ‘zero trust’, care înseamnă că oamenii nu se pot abţine să facă ce nu trebuie, furnizând soluţii de software care segmentează reţelele în bucăţi mai mici. Conceptul în sine nu este nou. Oamenii construiesc aşa nave din secolul al XV-lea, în ideea ca o singură spărtură să nu scufunde întreaga navă. În cazul reţelelor, dacă ceva rău pătrunde în ele, nu infectează întreaga reţea. Asta este ideea fundamentală”, a spus Pavel Gurvich în cadrul unei întâlniri cu jurnalişti străini.

El spune că orice organizaţie mare, în pofida eforturilor sale, se va infecta la un moment dat cu un malware. “Ai sute de mii de angajaţi, ai zeci de locaţii, iar cineva va face la un moment dat o greşeală - va deschide e-mailul greşit, va da click pe ceva, etc. Întrebarea care se pune este: Cum voi preveni ca acest ransomware să se răspândească lateral în reţeaua mea? Iar implicaţiile pentru afacere pot fi catastrofale”, a afirmat Gurvich.

Deşi cei mai mulţi clienţi apelează la serviciile companiei pentru a se proteja de un atac de tip ransomware, există şi firme care fac asta după ce au suferit deja consecinţele unei astfel de vulnerabilităţi.

“Mulţi clienţi ne cumpără pentru că îi ajutăm să se protejeze împotriva unui atac de tip ransomware. Cei mai mulţi recurg la serviciile noastre înainte de un atac şi pentru a preveni un atac sau a-i limita implicaţiile. Dar avem şi clienţi care vin la noi când ‘casa le arde’. Mulţi vin la noi trimişi de societăţi de răspuns la incidente sau de societăţi de asigurări. Spun că reţeaua lor este căzută, este infectată şi vor s-o reconstruiască. Ce facem atunci? Creăm o subreţea, cu două servere în ea, care sunt curate, şi apoi le extindem puţin câte puţin. În lumea fizică este un proces foarte dificil. În software este foarte uşor”, a relatat Pavel Gurvich.

Potrivit CEO-ului Guardicore, “afacerea a crescut semnificativ din cauza pandemiei. Iar anul ăsta e chiar mai bine. Pentru că foarte mulţi oameni lucrează de la distanţă. Iar serverele trebuie protejate”.

“Avem competitori foarte buni care împing industria înainte”

O altă companie cu o creştere vertiginoasă în domeniu este Orca Security, care furnizează servicii de securitate în cloud.

“Orca a fost fondată la începutul lui 2019, de opt persoane, ceea ce este ceva rar pentru un start-up. Am devenit un unicorn din 2019 până în 2021 şi aproape ne-am dublat operaţiunile în ultimele două luni. Suntem una dintre

The necessity of pursuing a proactive approach, in order to identify subtle and low key attacks on one hand, and the ability to predict sophisticated attacks based on indicative signals on the other hand.

Addressing the modern combat arena challenges requires a shift from platform-centric warfare to a real-time network-centric approach. How is IAI approaching this?

IAI developed the CyConcerto platform which is a modular solution that dramatically improve the capability of governments to build and maintain a cyber security national situational awareness picture, and to assign incident response capabilities, as needed, based on the situational picture and the analysis of the potential impact of an incident and the effectiveness of the entity’s response.

The CyConcerto platform is a multiple pillar modular solution that focus on preserving and augmenting existing investments while improving the detection and response across sectors, geographies and hierarchies.

"În fiecare săptămână creşte numărul de unicorni, companii private care valorează peste un miliard de dolari. Numărul era de 68 în urmă cu şase săptămâni, iar astăzi este de 73", a declarat el.

Autoritatea pentru inovare, înfiinţată în 2017, este un organism guvernamental care susţine iniţiative de mare risc, iar anul trecut a cheltuit 700 de milioane de dolari în acest scop, după ce a primit circa 4.000 de cereri de finanţare.

"70% dintre investiţiile noastre devin granturi, ceea ce este un mod drăguţ de a spune că am eşuat în 70% din proiecte. Dar este high-tech. Dacă nu eşti dispus să eşuezi, nu vor fi start-up-uri şi iniţiative private de mare risc. În Israel dacă eşuezi cu un start-up nu este doar acceptabil, în unele cazuri oamenii chiar te admiră pentru asta, pentru că ai încercat să faci altceva", a spus Sagie Dagan la o întâlnire cu un grup de jurnalişti străini.

"Ne axăm pe risc ridicat, căutăm proiecte din marile companii, start-up-uri mici sau iniţiative din mediul academic. Acordăm împrumuturi condiţionate, deci dacă un proiect este de succes banii sunt returnaţi, dacă nu se întâmplă asta, atunci creditul s-a transformat într-un grant. Mereu suntem co-investitori, dacă guvernul ar fi singurul investitor, atunci nu ar exista companii private. Asta este concepţia noastră asupra lumii şi într-o economie ca Israelul aşa funcţionează lucrurile", a adăugat el.

După cum mărturiseşte Sagie Dagan, una dintre sarcinile cel mai puţin plăcute ale Autorităţii pentru inovare este de "a omorî companii".

"Prima cale este să nu le dăm aprobarea, iar pentru cei cărora le spunem 'da' şi nu găsesc co-finanţare în trei luni se întâmplă acelaşi lucru. Indiferent dacă eşti guvern sau nu, nu este uşor 'să omori' companii. Dar am creat o activitate rapidă şi investitorii au ieşit din defensivă. Anul trecut, investiţiile în start-up-uri au scăzut în Europa, China şi SUA au avut o mică creştere, Israelul a avut o creştere de 15%, într-un an teribil", mai spus oficialul isralian.

"Simt că am pus piatra de temelie pentru o carieră"

Evident, odată cu dezvoltarea sectorului securităţii cibernetice, apare şi problema forţei de muncă specializate, care nu mai ţine pasul cu ritmul de creştere. Există însă o soluţie şi pentru asta, care într-un fel ajunge să rupă barierele sociale.

"În Israel ne concentrăm acum pe atragerea celor tineri care nu servesc în armată, arabii israelieni, 20% din populaţie, şi ultraortodocşii. Ei nu servesc în armată dar vrem ca ei să intre în industria securităţii cibernetice, care este flămândă de forţă de muncă. Este un câştig pentru toată lumea", a declarat Yigal Unna, directorul Directoratului Naţional pentru Securitate Cibernetică (INCD).

În acest scop, INCD a dezvoltat, împreună cu ONG-uri partenere şi instituţii de învăţământ, patru programe speciale, care îşi propun să descopere şi să folosească talente din zone insuficient valorificate ale populaţiei.

Primul program este numit "Cyber Force" şi este destinat foştilor soldaţi, bărbaţi şi femei, care după ce pleacă din armată sunt instruiţi să activeze în domeniul activităţii cibernetice.

Costa, de 22 de ani, din Beer Sheva, este unul dintre militarii care au absolvit acest program. El, împreună cu alţi tineri şi adolescenţi care au trecut prin programele de instruire în securitate cibernetică, s-au întâlnit cu un grup de jurnalişti străini la Universitatea din Tel Aviv.

"Am absolvit tabăra de instrucţie Cyber Force, sunt din a doua cohortă, ceea ce înseamnă că abia am absolvit. În noiembrie 2020 am încheiat serviciul militar şi nu eram sigur ce voi face. Am fost sunat, printr-o coincidenţă, în aceeaşi zi în care am fost lăsat la vatră şi mi s-a propus această oportunitate, de a urma pregătirea Cyber Foce", a relatat el.

"Am trecut printr-o perioadă de testare de peste o lună. A fost apoi un curs foarte intens de şase luni. Nu este uşor, dar cu siguranţă merită. Acum simt că am pus piatra de temelie pentru o carieră în industria de securitate cibernetică, în care nu este uşor să intri. Sunt foarte optimist în privinţa viitorului meu", a mai spus Costa.

companiile cu cea mai rapidă creştere la nivel global", a declarat Gil Geron, CPO şi cofondator al companiei.

Prima finanţare obţinută de companie în februarie 2019 a fost de 6,5 milioane de dolari. "Acum avem peste 300 de milioane şi suntem peste 140 de oameni. Suntem o firmă în extindere. Mergem în Austria, Bulgaria, Regatul Unit, Asia, deschidem mereu filiale în noi regiuni. Avem o nouă entitate şi în Franţa. Practic ne extindem la nivel global", a relatat el.

"În circa cinci luni de la fondarea companiei am avut prima instalare a soluţiei noastre. Când faci ceva atât de diferit, una dintre principalele probleme pe care le ai este că lumea nu crede că poţi face acel lucru. Într-o lună şi jumătate clientul a cumpărat pachetul şi a fost un indiciu pentru noi că am dat lovitura", a mai spus Gil Geron.

Practic, compania a privit asigurarea securităţii în cloud ca pe o oportunitate bună de afaceri, în contextul în care tot mai multe organizaţii migrează spre cloud. Apoi a identificat două probleme la care s-a gândit că trebuie să ofere răspunsuri dacă vrea să ofere o soluţie competitivă.

"Prima problemă este că majoritatea instrumentelor de securitate necesită agenţi, deoarece aceasta este cea mai bună cale pentru tine de a obţine acces la un hardware fizic. Asta se întâmpla înainte de cloud, pentru era cea mai bună oportunitate tehnică de a proteja un bun. De exemplu, pe laptop cu toţii avem instalat un antivirus. În cloud aceasta nu este în mod necesar calea de urmat. Ai o infrastructură care este virtualizată, poţi folosi această infrastructură pentru a proteja toate bunurile fără a instala nimic", a spus el într-o întâlnire cu un grup de jurnalişti străini.

"A doua problemă este că, din cauza faptului că mediul creşte atât de repede adesea se întâmplă că nu ştii de unde să începi, ai atât de multe bunuri încât problema creşte semnificativ. În medie, când te uiţi la 100 de bunuri în cloud poţi găsi 10.000 de riscuri de securitate. Nu este ceva diferit de perioada de dinainte, dar în cloud, din cauza acestei scalabilităţi, problema se schimbă semnificativ, nu o mai poţi privi la fel ca în lumea fizică", a adăugat cofondatorul Orca Security.

Soluţia companiei la aceste probleme a fost o tehnică numită "sidescanning", care practic elimină nevoia de agenţi.

"Gândiţi-vă la ea ca, de exemplu, la faptul că, în loc să vă întreb dacă vreţi să beţi ceva, fac o scanare cu rezonanţă magnetică a corpurilor voastre şi iau decizia cui îi este sete şi cui nu. Asta e posibil numai în cloud, dar îţi permite să afli o mulţime de detalii suplimentare - cui îi este foame, cine nu se simte prea bine, etc.", a explicat Geron.

Practic, tehnica brevetată de Orca îi permite companiei să înţeleagă imediat riscurile asupra întregii infrastructuri de cloud a clientului, indiferent că acesta are mii sau zeci de mii de unităţi.

Până în prezent la serviciile companiei au apelat peste 200 de companii, printre care institute medicale, giganţi ai tehnologiei sau firme din topul "Fortune 50". Cu toate acestea, Orca trebuie să dezvolte mereu nou soluţii, pentru că domeniul evoluează constant.

"Din fericire, avem competitori foarte buni care împing industria înainte. În acest sens, ne extindem mereu serviciile pe care le furnizăm, platforma şi instrumentele pe care le utilizăm, şi pe care le înlocuim constant, iar motivul este că atunci când ai o abordare holistică a problemei aduci mai multă valoare. Şi asta caută oamenii astăzi, caută o soluţie care poate furniza o umbrelă mare de protecţie. Orca este o firmă de vârf în extinderea capabilităţilor platformei şi a furnizării mai multor servicii în contextul protejării cloud-ului. Scopul nostru este să asigurăm servicii oricărei companii din lume care utilizează serviciile de cloud", a mai afirmat cofondatorul său.

"Nu este uşor 'să omori' companii"

Vicepreşedintele pentru creştere al Autorităţii pentru inovare, Sagie Dagan, a pus în context această dezvoltare a sectorului securităţii cibernetice din Israel, unde "tehnologia este motorul de creştere ".

"Am făcut multe recomandări guvernului care au început să fie implementate în 2011 şi astăzi suntem la zece ani după aceea. Una dintre ele a fost să predăm securitate cibernetică în licee. Israelul este singura ţară din lume în care securitatea cibernetică se predă la liceu. În 2011 nu exista nicio universitatea din lume, nu vorbesc despre Israel, în care puteai să iei o diplomă în securitate cibernetică. Altă recomandare a mea a fost ca fiecare universitate de cercetare din Israel să aibă o diplomă în securitate cibernetică. De asemenea, am recomandat ca fiecare universitate de cercetare din Israel să deschidă un centru de cercetare în domeniul securităţii cibernetice", a povestit el.

La Universitatea din Tel Aviv s-a înfiinţat primul astfel de centru de cercetare, care are acum peste 300 de cercetători.

"Guvernul nu le poate spune cetăţenilor să facă un start-up într-un domeniu sau altul, dar guvernul poate susţine mai mult un start-up dacă e în securitate cibernetică decât dacă e în tehnologie auto sau feroviară. Deci am construim un mecanism prin care susţinem mai mult start-up-urile din securitate cibernetică decât din alte domenii", a declarat Ben-Israel.

Bineînţeles, totul se suprapune peste "cultura start-up-urilor unică pentru Israel", datorată în mare parte faptului că acest stat are un serviciu militar obligatoriu de trei ani, care poate fi "tratat ca o şcoală".

"În fiecare an apar 1.500 de start-up-uri în Israel. Oameni tineri, cu noi idei. Aceşti tineri vin din armată, au idei şi mulţi dintre ei încearcă să fondeze noi start-up-uri pentru a-şi aplica ideile şi a reuşi în viaţa civilă. Este un ciclu uriaş, iar dacă te întrebi câte start-up-uri devin companii mature, răspunsul este în jur de 5%. Deci dacă cineva începe un start-up există o şansă de 95% de eşec", a spus el.

"Nu-mi imaginam că vom obţine aceste rezultate"

Totuşi, armata are meritul de a le da curajul să încerce astfel de iniţiative şi de a-i orienta, în multe cazuri, în viitoarea carieră, crede profesorul Ben-Israel.

"Avem copii care studiază securitate cibernetică în liceu, apoi, când au 17 ani, la testele pre-recrutare, mulţi sunt selectaţi să servească în unităţi cyber. După 3 ani, când se întorc în viaţa civilă, merg la universităţi sau în industrie. Iar aceşti oameni ajung în industrie şi aceasta face profit pentru că am fost primii care am făcut-o. Nu suntem primii care au inventat tehnologia cibernetică, dar suntem primii care au deschis domeniul. Suntem primii care l-au scos din dulap, cum le spun studenţilor mei, care l-au făcut legitim pentru activitatea comercială", a mai spus Ben-Israel.

Faptul că securitatea cibernetică a devenit obiect de cercetare în universităţi, în care se publică studii ce pot fi citite de toată lumea, a schimbat datele problemei. "Până când am făcut noi acest lucru, toată lumea a tratat asta ca pe un secret. Iar din acest motiv nu exista cercetare deschisă. Iar dacă nu există cercetare deschisă, capacitatea de a crea noi cunoştinţe este mult mai mică", a afirmat Isaac Ben-Israel.

"Dacă mă uit înapoi, dacă compar situaţia de acum cu cea din urmă cu zece ani, pot să spun că nu-mi imaginam că vom obţine aceste rezultate", a dat el asigurări. Israelul stă acum mai bine decât multe alte ţări în domeniul investiţiilor în securitate cibernetică, iar explicaţia este una simplă, potrivit sursei citate.

"Dacă vorbim despre investiţiile în acest sector, fără sumele alocate de guverne, la nivel global, în 2018, 18% au mers către Israel. În 2019 ele au ajuns la 26%, în 2020 la 31%, iar în prima jumătate din 2021 la peste 40%. Asta înseamnă că mai mulţi dolari americani sunt investiţi în Israel decât în SUA în securitate cibernetică", a declarat Isaac Ben-Israel.

"În total, exporturile Israelului în servicii de tehnologie cibernetică reprezintă 10% din piaţa globală. Iar motivul este că am început să facem asta cu câţiva ani înaintea celorlalţi", a conchis el.

Iar Israelul nu se opreşte aici. Peste un alt deceniu s-ar putea vorbi despre rezultate de vârf în Inteligenţa Artificială, unde acum se lucrează la o strategie care să-l facă lider în domeniu.

Al doilea program, "Cyber Elite", este destinat evreilor ortodocşi şi ultraortodocşi, bărbaţi şi femei, cu diplome de studii ştiinţifice, asigurându-le acestora pregătire pentru a deveni cercetători în industria de apărare cibernetică.

Yechiel, care are 32 de ani şi provine dintr-o familie ultraortodoxă cu şapte copii, este unul dintre cei care au trecut prin programul "Cyber Elite", după ce a absolvit Colegiul tehnologic din Ierusalim, o unitate de învăţământ cu 7.000 de studenţi ortodocşi şi ultraortodocşi. Deşi reuşise să promoveze ca inginer după un singur an într-o firmă de electronice, el şi-a dorit o carieră în securitate cibernetică.

"M-am alăturat acestui program, l-am urmat, şi acum sunt cercetător într-o firmă care dezvoltă instrumente pentru securitate cibernetică. Am căpătat multă încredere şi cunoştinţe", a spus el.

"O lume s-a deschis pentru noi"

Al treilea program este numit "Rising Up" şi este destinat tinerelor din medii religioase care de obicei nu merg în armată, dar prestează "un serviciu naţional". Până acum ele nu au avut acces la slujbe din domeniul tehnologic, alegându-şi de obicei profesii mai tradiţionale precum profesoare sau asistente medicale.

Elia, în vârstă de 18 ani, care a terminat liceul în urmă cu o lună, este una dintre elevele care au urmat acest program.

"Până acum, pentru că suntem dintr-o comunitate religioasă, nu am avut aceste oportunităţi să fim parte din lumea tehnologică. Deci când am primit oportunitatea de a face parte din acest program, o lume s-a deschis pentru noi. Am dezvoltat atât de multe aptitudini şi am învăţat atât de multe despre mine. Acum pot să fac multe lucruri şi am înţeles că faptul că provin dintr-o comunitate religioasă nu înseamnă că nu pot ajunge departe în industria cibernetică", a spus ea.

Al patrulea program dezvoltat de INCD şi instituţiile partenere este "Odyssey Cyber Track", destinat adolescenţilor foarte talentaţi, mai precis cooptării lor încă din liceu pe traseul unei cariere în cercetare în securitate cibernetică.

"Odyssey începe în clasa a noua şi durează patru ani şi operează pe un număr de 'track'-uri, iar astăzi vorbim despre un 'track' în securitate cibernetică. Acesta operează în trei universităţi şi este un program foarte intens. Elevii învaţă şi la şcoală şi în program. Este interesant că studiază într-un mod conceput pentru vârsta şi nevoile lor, nu sunt aruncaţi în populaţia generală de studenţi", a declarat reprezentantul unui ONG implicat în proiect.

"Când termină clasa a XII-a, am creat o reţea de absolvenţi şi vom continua să investim în ei pe parcursul facultăţii şi al anilor profesionali, atât în termeni de dezvoltare cât şi de dezvoltare a unei comunităţi", a mai spus el.

Emanuel, în vârstă de 15 ani, este unul din adolescenţii înscrişi în program. Pentru că a început să facă programare de la patru ani, el spune că a avut puţine dubii când a descoperit despre ce este vorba.

"Am aflat despre program de pe internet şi m-am înscris, dar nu m-am aşteptat să trec de primele stadii. Acest program mi-a dat multe oportunităţi, mi-a ameliorat capacităţile de studiu şi de a relaţiona social. Una peste alta mi-a asigurat încrederea în sine de care aveam nevoie pentru a fi puştiul ăla ciudat de 15 ani căruia îi place tehnologia cibernetică", a spus el.AGERPRES/(A - autor: Florin Ştefan, editor: Mariana Ionescu, editor online: Andreea Lăzăroiu)

platform for cyber training and simulation.

It is important to mention that establishing national level cyber centers requires a lot of technology and know how and therefore, we tend to perform these projects together with our partners are the Israeli Cyber Companies Consortium, which IAI is leading. A few names worth mentioning are Check Point, CyberArk, Cognyte and Mellanox.

You work with systems that require extensive, proprietary know-how. What are the most notable obstacles to developing technologies and systems resilient to cyber attacks?

We can divide the challenge to two parts. The first challenge is developing a solution that will provide actional insights or an automated operation to reduce the "alert fatigue syndrome" which affects most of today's security operations centers (SOCs). The second challenge is to recruit, train and maintain cyber professionals, and for that we need to develop and utilize advanced methodologies and technologies.

When discussing national level cyber security operations center, we need to remember that national grade challenges require national grade solutions. These solutions have to incorporate several elements: state of the art technology; effective, field proven methodology; constant innovation, since the cyber domain is constantly evolving; collaboration (and I already elaborated about the Israeli Cyber Companies Consortium) and finally capacity buildup, addressing the human factor – training, certification and awareness.

IAI has ample experience in developing unique state of the art systems, and delivering them to our customers in the framework of national cyber projects. Yes, it's challenging. However, IAI is up to the challenge, has a stellar track record, and our excellent teams are constantly working toward tackling the new emerging cyber trends.

What national cybersecurity challenges are governments facing in a post-COVID world?

One of the main challenges for governments is to draw the line between the entities and the government responsibility regarding prevention, detection and response to cyber incidents. On one hand, each entity has the responsibility for their systems and customers. However, national cyber resilience consists of the resilience of each and every entity and can be compromised if certain entities will be compromised.

We just witnessed such an incident with Colonial Pipeline.

The way to address this challenge is by adopting national security model that will be able to monitor the entire national cyber eco-system, will be able to assist the entities on ways improving their security posture or security response activities, and will be able to intervene in case of unresolved crisis.

Some further challenges that our national level customers are facing in the post COVID-19 world are the following:

The skills deficit, essentially, there is a huge global shortage in cyber defenders.

The necessity of balancing cyber security and business continuity, especially in an era (post COVID-19) where the digital transformation is accelerated. This essentially leads to a paradigm shift from cyber security to cyber resilience.

AGENȚIA NAȚIONALĂ DE PRESĂ AGERPRES
Actualitatea sub lupă.

'Unciorn Fram" or how Israle has taken over the US in unicorn investments

Israelul a avut nu mai puţin de şapte unicorni în securitate cibernetică în prima jumătate a anului 2021, iar unul din trei unicorni din lume în domeniu este israelian - este rezultatul la care a ajuns acest stat la zece ani după ce a întocmit o strategie naţională prin care guvernul a stimulat iniţiativa şi investiţiile în domeniu, totul în cadrul unui ecosistem care are la bază o caracteristică unică a Israelului.

Mai mult, 41% din investiţiile la nivel mondial în securitate cibernetică sunt efectuate în Israel, o sumă în creştere accentuată în ultimii trei ani şi care a făcut ca Israelul să aibă o situaţie chiar mai bună decât SUA din acest punct de vedere. Este o informaţie care poate părea surprinzătoare, mai ales că, după cum susţine Autoritatea pentru inovare de la Tel Aviv, doar 5% din start-up-urile din lume în domeniul securităţii cibernetice sunt înfiinţate în Israel.

Totuşi, Israelul adună o cărămidă peste alta de zece ani în domeniul securităţii cibernetice, a cărui fundaţie, ca multe altele în acest stat, a fost realizată din dorinţa de a asigura apărarea ţării de o serie de vulnerabilităţi noi. În acelaşi timp, totul s-a construit pe fondul unei culturi a start-up-urilor unică pentru Israel, unde nu mai puţin de 95% din noile afaceri sunt sortite eşecului. Însă, dacă într-adevăr pot exista locuri în lume în care curajul de a fonda un start-up care a eşuat să-ţi aducă respect, cu siguranţă că Israelul este unul dintre acestea.

Nu în ultimul rând, un factor favorizant este că Israelul are un sector high-tech foarte dezvoltat, care reprezintă 15% din PIB-ul naţional, iar 43% din exporturile acestui stat sunt atribuite sectorului. Potrivit ultimei statistici din 2020 publicate de Autoritatea pentru inovare, securitatea cibernetică s-a bucurat de cele mai mari investiţii în hight-tech în Israel, de 2,9 miliarde de dolari, urmată de "Fin tech" (tehnologie financiară) - 1,7 miliarde de dolari şi mobilitate inteligentă - 1,3 miliarde de dolari.

"Israelul, singura ţară din lume în care securitatea cibernetică se predă la liceu"

Isaac Ben-Israel, preşedintele conferinţei Cyber Week 2021, care s-a desfăşurat în a doua jumătate a lunii iulie la Universitatea din Tel Aviv, şi directorul Centrului de cercetare interdisciplinar în domeniul cibernetic (ICRC) al acestei instituţii, a rememorat cum s-a ajuns ca Israelul să dezvolte strategia ale cărei roade le culege acum în domeniul securităţii cibernetice.

După cum a povestit el în cadrul unei întâlniri cu jurnalişti străini, premierul de la acea vreme, Benjamin Netanyahu, i-a cerut în urmă cu un deceniu să întocmească un plan pentru dezvoltarea securităţii cibernetice în Israel, care să includă măsuri pentru fiecare din următorii cinci ani. Profesorul Ben-Israel, care a fost şi şef al cercetării pentru armata israeliană, i-a răspuns că ameninţările din securitate cibernetică nu pot fi previzionate pentru mai mult de un an înainte, dar că există factori care pot ajuta statul să ofere răspunsul adecvat la acest nou tip de ameninţări.

"I-am spus că avem nevoie de factorul uman şi de multe start-up-uri în securitate cibernetică. De fapt sunt trei factori: educaţie, industrie şi guvern. Iar guvernul joacă un rol mai important decât în orice ţară din lume", a afirmat Isaac Ben-Israel.

the algemeiner

Cryptocurrency Technology Is 'The New Engine' for Cybercrime, Argues Israel's Check Point

"To understand the crypto evolution, you need to look at it from the perspective of the invention of the engine," said Check Point's head of product vulnerability research Oded Vanunu. "At the start, it was a bicycle. Then it was a motorcycle, and then it was a small plane, a big plane, a missile, and so on... the blockchain technology is the new engine and it's something that is going to be with us for a long time."

Those with Bitcoin in their digital wallets have long understood the prevalence of cryptocurrencies and how blockchain technology can flourish. And while a new anonymous and decentralized way to send and receive money is attractive for some, the adoption of cryptocurrencies has added a new layer to the ability of criminals to attack companies and governments. And attackers are today walking away with million-dollar payouts.

"Cybercrime started to have the ability to cash out because the whole crypto thing is anonymous," he continued. "You don't need to identify yourself. The evolution in the last 10 years is cybercrime going from a garage into whole organizations with CEOs, CTOs, operational managers, CFOs, where every attack is money. Every attack is a cashout."

According to Vanunu, who has been at Check Point for 18 years, conventional virus campaigns and cybercrimes were 'evil initiatives' that did not seek to make a profit, but rather carried out by social activists "to take data and attack it because a company is doing bad things." Today, the shift into decentralized and anonymous behavior makes it easier than ever before to exploit companies – and governments – for financial gain.

As of 2019, Check Point had 5,000 employees who provide products for IT security, including network security, endpoint security, cloud security, mobile security, data security, and security management. Today more than ever, Vanunu is warning organizations on the importance of security defense, and laments the fact that governments spend too much on cyber offense.

"Organizations need to prioritize their budgets differently for cyber defense," he told CTech. "This is the reality and they need to understand that today they are facing state-sponsored levels (of cybercrime)."

The United States — which has the largest military to attack in the world — has been shown to have comparatively low levels of defense against such attacks. In late 2020, the U.S Government was hacked by Russian hackers. Earlier this month, Reuters reported that 1,500 businesses were affected by a ransomware attack on Kaseya, a Miami-based IT firm believed to be conducted by criminals acting on direction from the Russian government. In June, President Biden told Vladamir Putin that certain cyberattacks should be 'off-limits', a statement evidently given in vain.

In Israel, the potential of cybercrime and protection against it has been a priority set up by the government. Through education, higher budgets, and a new emphasis on it placed by the IDF, Vanunu says generations of children are being raised in Israel on the importance of a strong defense system against cybercrime.

"This is one of the fundamentals," he concluded. "Innovation, technology and cyber... it's one of the fundamentals of the Israeli economy."

+ HELPNETSECURITY

Elevating cyber resilience and tackling government information security challenges

Esti Peshin is VP, General Manager, Cyber Division, Israel Aerospace Industries (IAI). Previously, she served 11 years in the Israeli Defense Forces, in an elite technology unit, where she was Deputy Director.

Peshin recently spoke at Cyber Week 2021 in Tel Aviv, and in this interview with Help Net Security, she discusses national defense and security challenges, as well as developing technologies and systems resilient to cyber attacks.

What were the most important takeaways from your 11 years in the Israeli Defense Forces? How did being part of this elite technology unit shape your vision of cybersecurity protection?

The most important takeaway from the service in the IDF is that nothing is impossible. If there is a need, there is a way. The means will be identified and it just a matter of creativity to find the right way to achieve any goal. This is, in my view, the essence of Israeli entrepreneurship, and one of the reasons the cyber eco-system is striving in Israel.

IAI leverages state-of-the-art technology for national defense and security challenges. Based on the feedback from your clients, which technologies are most in demand today?

We, at IAI, believe that most important and sought technologies are those that help organizations to detect that something bad is happening, at a very early stage. Preferably, even allowing organizations to predict that something bad can happen or is about to happen, and to direct the organization on how to avoid it or mitigate it.

The main problem with most of the common cyber monitoring technologies available today is that they generate large number of alerts without prioritizing them. Therefore technologies that can generate actionable insights are the key to improving cyber resilience.

Therefore, the main solution that is sought by our national level customers is establishing national level cyber security operation centers. These centers, essentially proactively monitor national cyber space in order to perform the following operations:

Conduct a national level, on going and real time, cyber risk assessment

Monitor national cyberspace in real time in order to identity cyber attacks or predict attacks based on indicative signals

Provide effective tools for incident response and cyber forensics

Allow effective knowledge sharing between the national stakeholders and constituents.

IAI's CyConcerto platform, incorporating CyScan, for national risk assessment, CyFo, for forensics and incident response and CyShare for knowledge and information sharing, is a leading platform tailored especially for national level end users.

Furthermore and in view of the huge shortage of cyber experts, our end users seek the establishment of Cyber Academies to train cyber experts. The Academies utilize our TAME Range cyber range, which is a state-of-the-art

"It's not just really cybersecurity," says Ben Dov. It's a culture of "being very scrappy, doing a lot with very little resources, being able to have the chutzpah essence, not necessarily...listening to authority. I think that's a lot of what makes entrepreneurs good. Because if entrepreneurs don't dream big, and if entrepreneurs listen to voices saying they can't do this or that, these are barriers; if people listen to the barriers, they will never take risks and they will never dream big and become entrepreneurs. So that's a lot of inherently what Israelis have, what the Israeli character and mentality has, which enables Israel to become a hotbed for entrepreneurship as a whole."

Offensive and defensive cybersecurity

Despite the positive news coming out of Cyber Week, the NSO scandal still hung over the industry as a whole, raising ethical and legal questions.

Amir Einav, Chief Revenue Officer (CRO) at IoT and automotive cybersecurity company Karamba, tells NoCamels that offensive cybersecurity companies like NSO have legitimate businesses. "They sell weapons, next-generation weapons for next-generation wars. The equivalent is companies like IAI [Israel Aerospace Industries] and Elbit developing missiles and guns and so on," Einav says.

"Is it legal? Is it moral? Everyone has their own decision to make here. But it is a business. A government-regulated business subject to export laws," he says.

Barzilay says Israel needs offensive cybersecurity solutions. "They are an important aspect of cybersecurity and Israel must continue investing in these types of technologies. All countries do or they will get left behind."

But controls must be in place to make sure "people don't use such tech in the wrong way," he adds.

The Jewish Voice

IDF General Warns Against Cyber Attacks; "We Will Not Tolerate a Threat to Israel"

Attacks on Israel "will be answered accordingly," said Maj. Gen. Tamir Heyman, Director of the IDF's Military Intelligence, saying that cyber-attacks should be treated just as any other in the real world.

Speaking on Tuesday at the 2021 Cyber Week at Tel Aviv University, Heyman said that as part of the recent Operation Guardian of the Walls in Gaza against Hamas, "information gathered from a variety of sources – including cyber realm, was fused together through advanced processing capabilities, Artificial Intelligence and machine learning into operational outputs. This allowed the IDF to function better, faster, and with fewer casualties."

The IDF was able to collect accurate and real-team intelligence on the whereabouts of senior Hamas commanders, killing several of them in remarkable operations.

Touching on the daily cyber threats Israel faces, Heyman said that "Israel is under constant threat in the cyber dimension, and attacks are sometimes carried out against it. We are able to deal with most of the threats through advanced defense capabilities."

Israel has an advanced cyber-security apparatus and fends off thousands of cyber-attacks on a daily basis.

"As with other dimensions of combat, defense alone is not enough. Additional steps must be taken to preserve Israel's supremacy over our enemies," he stated, warning that "those who attack Israel by air, sea, land or cyber need to understand the risk they are taking. As they see time and time again, the attacks will be answered accordingly."

Minister of Defense Benny Gantz conveyed a similar message at the event, saying that "in recent years, there has been a significant increase in the number of attacks carried out by hostile elements, including Iran and its affiliates, seeking to access the IT systems of Israel's national infrastructure."

"In the face of this increase – from a few single attacks to dozens of attacks a year – Israel has demonstrated the ability to develop its resilience, its technological advantage and its qualitative advantage in the region," he said. "Israel works continuously to protect against cyber-attacks."

He said that during Operation Guardian of the Walls, the IDF hit the head of Hamas' cyber command, Jum'a Tahla. The IDF also identified and damaged several cyber-attackers, equipment and infrastructure that served Hamas' cyber command.

"Our message is clear – be it a rocket or a keyboard – we will not tolerate a threat to the citizens of Israel," he declared.

The Washington Post reported in May that Israel was behind the May 9 cyber-attack on Iran's Shahid Rajaee port in Bandar Abbas, the largest in the country, which brought the shipping traffic to an abrupt and inexplicable halt for days, generating backups for miles.

Israel – a cybersecurity superpower

Israel's unique cybersecurity ecosystem is made up of big cyber companies, global multinational firms with Israeli R&D arms, new startups, army training, and government support for both private and public endeavors. Together, these components have created an effective, sought-after community that is bringing much-needed cybersecurity solutions to market.

"Israel has become a hub for excellence in cybersecurity and we are seeing huge investments in Israeli cyber companies," says cybersecurity expert and entrepreneur Menny Barzilay.

"Israel has to be good at cybersecurity because we have very smart enemies; we are in a constant state of conflict and naturally have a security orientation. We have to be creative and innovate in this space," Barzilay tells NoCamels on the sidelines of the Cyber Week event where he served as panel moderator and speaker.

He says the overarching theme at the event this year has been the role of cybersecurity companies in enabling businesses to continue operating remotely, safely and securely, as the COVID-19 pandemic hit every aspect of our lives.

From safe remote access, security management, cloud management and so on, cybersecurity companies have been "innovation enablers," allowing companies and employees to deal effectively with the challenges brought on by the pandemic.

Naama Ben Dov, an associate at Israeli investment firm YL Ventures, expresses a similar sentiment. When we look at the cybersecurity market as a whole, she tells NoCamels, the coronavirus pandemic accelerated solutions "because everything was remote, everything went online; and therefore all the threats of online presence became much more emphasized and much more prioritized."

"So you see a lot more companies bringing in budgets, bringing in board-level attention to cybersecurity technologies, products, and methodologies, to contend with this new threat which has come to the fore even more strongly during [the pandemic] and remote work," she says.

The cybersecurity industry will continue to attract massive funds, Barzilay predicts, because it is part all of sectors. "When you look at AVs [autonomous vehicles], robotics, AI, medical tech, biotech, etc – we need more cybersecurity solutions to sustain the use of these technologies," he tells NoCamels.

And Israel will continue to lead in this sector, in part because of its compulsory military service, government support, and strong collaboration between academia and industry, Barzilay explains.

"Everyone goes to the IDF, and when they leave they already have 3-4 years experience as part of a huge defense operation, they are mature but they still very young and they are free to do whatever they want," he says.

"You get tons and tons of people enlisting to cybersecurity-related roles at the age of 18, making Israeli a hotbed for very young talent in the cybersecurity domain," concurs Ben Dov.

SEE ALSO: Cyber Attacks On Healthcare Organizations Soared In Israel In 2020 — Report

There's also something to be said about the Israeli mentality of taking risks, making mistakes, doing away with social hierarchies, and going directly to the source. And it applies to every domain.

"Our enemies know no boundaries – just as they fire rockets at civilians, they aim to harm civilian facilities via cyber space while endangering human lives, added Gantz, calling for a no-tolerance policy when it comes to cyber attacks.

This year, the hybrid in-person-online confab came in the wake of bombshell reporting by 17 media organizations this week that a powerful cyberweapon, Pegasus, developed by Israeli cyber intelligence and surveillance firm NSO Group was used by dozens of governments and government agencies to target journalists, human rights defenders, political dissidents and opponents, business executives, and lawyers. The investigation was based on a list of 50,000 phone numbers leaked to Amnesty International and Paris-based rights group Forbidden Stories, and found that it included people targeted by the governments of Azerbaijan, Bahrain, Mexico, Morocco, Saudi Arabia, Hungary, and India, among others.

Pegasus is a powerful, invasive piece of spyware that can access private data including passwords, web history phone call logs, contact lists, and text messages, and monitor live calls from messaging apps. It can also turn on phone cameras and microphones to track events in the vicinity and use the GPS function to monitor a target's location and movements. Though NSO claims its software makes the world a safer place "by providing authorized governments with technology that helps them combat terror and crime," its tools have been linked to a number of high-profile cases including the 2018 murder of Washington Post journalist and Saudi dissident Jamal Khashoggi and the targeting of journalists and dissidents in Mexico and other countries, according to extensive research by Citizen Lab, a research facility at The University of Toronto's Munk School of Global Affairs.

On Thursday, the Israeli company denied the recent reports that its tools have been used for malicious activity and indicated that it had no knowledge or involvement in compiling the alleged list of 50,000 potential targets. NSO has also maintained that it licenses its software to vetted government clients with approval from the Israeli government, and that the reports were part of efforts "to smear all the Israeli cyber[security] industry."

But the dust-up has been significant, with France, Germany, the UN and the EU calling for more regulation and tougher government controls of spyware. Some of the countries mentioned in the reports, including Morocco, Mexico and Saudi Arabia also denied using the software.

The Israeli government, meanwhile, has set up a commission headed by the defense establishment to review the allegations of misuse and said there may be "corrections" after the assessment is completed. NSO said it welcomed the inquiry "so that we'd be able to clear our name," the company's chief executive Shalev Hulio told Army Radio on Thursday.

At Cyber Week, Gantz addressed the controversy without mentioning NSO by name, telling the audience that Israel complies with international law

"We are aware of recent publications regarding the use of systems developed by certain Israeli cyber companies. Israel, as a liberal western democracy, controls exports of cyber products in accordance with its defense export control law, complying with international export control regimes. As a matter of policy, the State of Israel authorizes the export of cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism. The countries acquiring these systems must abide by their commitments to these requirements," said the Israeli defense minister.

CTECH

Cryptocurrency technology is "the new engine" for cybercrime, says Check Point

Speaking to CTech during Cyber Week, Check Point's Oded Vanunu shares how cybercrime has evolved on the blockchain, and what governments can do to protect against attacks

"To understand the crypto evolution, you need to look at it from the perspective of the invention of the engine," said Check Point's head of product vulnerability research Oded Vanunu. "At the start, it was a bicycle. Then it was a motorcycle, and then it was a small plane, a big plane, a missile, and so on... the blockchain technology is the new engine and it's something that is going to be with us for a long time."

Those with Bitcoin in their digital wallets have long understood the prevalence of cryptocurrencies and how blockchain technology can flourish. And while a new anonymous and decentralized way to send and receive money is attractive for some, the adoption of cryptocurrencies has added a new layer to the ability of criminals to attack companies and governments. And attackers are today walking away with million-dollar payouts.

"Cybercrime started to have the ability to cash out because the whole crypto thing is anonymous," he continued. "You don't need to identify yourself. The evolution in the last 10 years is cybercrime going from a garage into whole organizations with CEOs, CTOs, operational managers, CFOs, where every attack is money. Every attack is a cashout."

According to Vanunu, who has been at Check Point for 18 years, conventional virus campaigns and cybercrimes were 'evil initiatives' that did not seek to make a profit, but rather carried out by social activists "to take data and attack it because a company is doing bad things." Today, the shift into decentralized and anonymous behavior makes it easier than ever before to exploit companies - and governments - for financial gain.

As of 2019, Check Point had 5,000 employees who provide products for IT security, including network security, endpoint security, cloud security, mobile security, data security, and security management. Today more than ever, Vanunu is warning organizations on the importance of security defense, and laments the fact that governments spend too much on cyber offense.

"Organizations need to prioritize their budgets differently for cyber defense," he told CTech. "This is the reality and they need to understand that today they are facing state-sponsored levels (of cybercrime)."

nocamels
ISRAELI INNOVATION NEWS

Amid NSO Fallout, Israel Hosts Cyber Week Confab Highlighting Record Funding Year

Israel held its annual Cyber Week conference in Tel Aviv this week, welcoming top politicians, public figures, global cyber policymakers from over 80 countries, and executives from cybersecurity startups and multinational companies such as IBM, Checkpoint, and Microsoft.

The event came amid a record funding year for Israeli cybersecurity companies and startups, which raised over $3 billion in just the first half of 2021 (or 41 percent of the global sector investment) as well as a marked increase in cyber threats and attacks across the world, specifically ransomware. One of the biggest publicly acknowledged payouts to hackers in recent years was set at $40 million.

"Today the best bang for your buck is a cyber attack and it's just going to grow exponentially, and that makes me worried," said Israeli Prime Minister Naftali Bennett at the event this week, hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University.

"As prime minister of Israel, I view this as one of the top threats to Israel's national security and the world's security," he added, calling for more international cooperation and coordinated defenses against cyber threats. "Israel is opening up and announcing a 'Global Cybernet Shield,'" Bennett said, "using the very same principles of cyber connectivity because if you fight alone you will lose, but if we fight together we will win."

During his address, Israeli Defense Minister Benny Gantz called for a cyber version of Israel's famous anti-missile defense system Iron Dome. "Cyber is now a vulnerable space that must be protected like the sea, space, air, and ground," he said.

THE TIMES OF ISRAEL

Reporters Without Borders urges Israel to stop exporting spyware

Reporters Without Borders Wednesday urged Israel on Wednesday to suspend exports of spying technology amid allegations it was used to target more than a dozen heads of state and hundreds of journalists.

"We call on Israeli Prime Minister Naftali Bennett to impose an immediate moratorium on surveillance technology exports until a protective regulatory framework has been established," Reporters Without Borders head Christophe Deloire of the Paris-based group said in a statement.

His call came after a list was leaked of some 50,000 phone numbers believed to have been chosen by clients of Israel's NSO Group for possible surveillance, according to an international reporting effort.

The list contained numbers for 14 heads of state including French President Emmanuel Macron and Morocco's King Mohammed VI.

NSO's flagship program Pegasus can hack into mobile phones without users knowing, enabling clients to read every message, track a user's location and tap into the phone's camera and microphone.

The company does not identify its customers. However, rights group Amnesty International and the Paris-based organization Forbidden Stories that obtained the list said NSO's government clients include Bahrain, India, Mexico, Morocco, Rwanda and Saudi Arabia.

Reporting by media outlets including The Guardian, Le Monde and The Washington Post found that nearly 200 journalists from organizations including AFP were on the list.

"Enabling governments to install spyware that is used in practice to monitor hundreds of journalists and their sources throughout the world poses a major democratic problem," Deloire said.

Spokespeople for NSO, Bennett and Defence Minister Benny Gantz did not respond to questions from AFP on Wednesday.

NSO is a giant of Israeli tech with 850 employees.

Its CEO Shalev Hulio, 39, denied in an interview with Israel's 103FM radio on Tuesday that his company was engaged in mass surveillance.

He said NSO had "no connection" to the list of thousands of phone numbers.

On Wednesday, Bennett touted Israeli technological prowess at a cyber conference in Tel Aviv.

"Of every $100 invested in cyber defense across the world, $41 of those were invested in Israeli cyber defense firms," he said.

"We as a government, we as a nation, have to defend ourselves," Bennett added.

He suggested global interest in Israeli technology remained robust, saying "dozens of countries" signed memorandums to obtain Israeli tools that defend against cyberattack.

On Tuesday, Gantz said Israel approves export of technology only to governments "exclusively for the purposes of preventing and investigating crime and terrorism."

He said Israel is "studying" recent publications on the subject.

mid-day

Pegasus: Israeli Defence Ministry studying investigation into NSO Group

'We are aware of recent publications regarding the use of systems developed by certain Israeli cyber companies,' Benny Gantz said at Cyber Week at Tel Aviv University, without naming the Herzliya-based company

The Israeli Defence Ministry is studying the investigation into NSO Group, Defence Minister Benny Gantz said after it was revealed that the Israeli cyber company has been selling spyware to foreign governments to target journalists and activists, Jerusalem Post reported.

"We are aware of recent publications regarding the use of systems developed by certain Israeli cyber companies," Gantz said at Cyber Week at Tel Aviv University, without naming the Herzliya-based company.

On July 18, the Pegasus Project revealed that the spyware sold by NSO (Pegasus) had been identified on the phones of individuals targeted by the governments of Azerbaijan, Bahrain, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, the United Arab Emirates and more.

The investigation was carried out by 17 media organisations, led by the Paris-based journalism nonprofit Forbidden Stories, and sponsored by Amnesty International. At the centre of it was a leaked list of 50,000 phone numbers belonging to journalists, senior politicians and business people.

The report said Gantz asserted that as a matter of policy, Israel authorises the export of cyber products "solely to governments, only for lawful use and exclusively for the purposes of preventing and investigating crime and terrorism" and that the country controls the exports of such products and complies with international export control regimes.

"The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject," Gantz said. In a statement released after the investigation was published, the Defence Ministry said that it will take "appropriate action" if NSO Group violated the terms of its export licenses or end use certificates, the report added.

THE TIMES OF ISRAEL

After NSO bombshell, Gantz asserts that Israel complies with international law

Defense minister says ministry 'studying' claims company's Pegasus software has been used by governments to target journalists and activists

Responding to an in-depth investigation that revealed that Israel's NSO Group has been selling spyware used by foreign governments to target journalists and activists, Defense Minister Benny Gantz asserted Tuesday that Israel operates fully within international law.

"We are aware of recent publications regarding the use of systems developed in certain Israeli cyber companies," said Gantz in a speech to Cyber Week at Tel Aviv University, without mentioning NSO Group by name. "Israel, as a liberal Western democracy, controls exports of cyber products in accordance with its defense export control law, complying with international export control regimes."

Gantz added that, "as a matter of policy, the State of Israel authorizes the export of cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism. The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject."

On Sunday, an in-depth investigation led by 17 major international news organizations claimed that NSO Group has sold cellphone malware used to target journalists, activists and politicians in dozens of countries.

The reporting focused on Pegasus, a spyware tool sold by NSO that the investigation said is being used by dozens of governmental clients. The analysis carried out on a leaked list of 50,000 phone numbers found that the list included people targeted by the governments of Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, and the United Arab Emirates.

The Guardian's report on Pegasus claimed that Gantz "closely regulates NSO" and approves each individual export license before the surveillance software is sold to a new country. In its response, NSO stated that "you falsely claim that the Israeli government monitors the use of our customers' systems, which is the type of conspiracy theory that our critics peddle," adding: "Regarding export licenses, NSO is subject to various export control regimes including the Israeli MoD, similar to existing regulations in other democratic countries."

In a statement on Monday, the Defense Ministry said if it finds that the NSO Group violated the terms of its export licenses, it will "take appropriate action." The ministry said that Israel only permits companies to export cybersecurity products to "government figures only for legal purposes and to prevent and investigate crimes and to combat terrorism. And this is dependent upon commitments regarding the end use/user from the purchasing country, which must abide by these conditions."

In his speech on Tuesday, Gantz also weighed in on an overnight exchange of fire between Israel and Lebanon.

Israel's Defense Ministry said in a statement that it "approves the export of cyber products exclusively to governmental entities, for lawful use, and only for the purpose of preventing and investigating crime and counterterrorism." It said national security and strategic considerations are taken into account.

Last year, an Israeli court dismissed an Amnesty International lawsuit seeking to strip NSO of its export license, citing insufficient evidence.

United Nations human rights chief Michelle Bachelet on Monday said the apparent widespread use of the Pegasus spyware to illegally undermine the rights of those under surveillance, including journalists and politicians, was "extremely alarming" and confirmed "some of the worst fears" surrounding the potential misuse of such technology.

The recent reports have caused considerable embarrassment within Israel's diplomatic-security echelon. NSO operates from Israel and its products are exported under DECA's oversight. Moreover, official Israeli representatives have helped the company sell its products in several countries with which Israel doesn't have official diplomatic relations. The purpose of these efforts, allegedly, was to help these countries fight terrorist groups, and pave the path for the sale of additional Israeli products. The New York Times reported earlier this week that such help was provided in Saudi Arabia, among other countries.

Defense Minister Benny Gantz asserted Tuesday that Israel operates fully within international law.

"We are aware of recent publications regarding the use of systems developed in certain Israeli cyber companies," said Gantz in a speech to Cyber Week at Tel Aviv University, without mentioning NSO Group by name. "Israel, as a liberal Western democracy, controls exports of cyber products in accordance with its defense export control law, complying with international export control regimes."

Gantz added that "as a matter of policy, the State of Israel authorizes the export of cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism. The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject."

However, other officials in Israel said Tuesday that the severity of the affair and its possible repercussions obligate "clearer actions and statements" from the government.

The officials expressed concern that sufficing with "studying" the issue won't reduce the international criticism against Israel. Some officials warned that a "critical mass" of pressure could form and that failing to launch a public and transparent investigation could create the impression that Israel had something to hide, and that Pegasus was used for illegal purposes with the knowledge and approval of the government.

However, other officials said such an investigation could complicate relations with numerous sensitive countries, such as Saudi Arabia, the UAE, Morocco and Bahrain. In their view, Israel has a vested and clear interest in cooperating with the rulers of these countries against shared threats, such as Iran and Islamic terror, and said such an investigation could embarrass some of them and directly harm diplomatic relations.

Shalev Hulio, founder and CEO of NSO Group, responded Tuesday to the growing firestorm surrounding his company, saying he "wishes the Israeli government would launch an investigation to clear us of these false accusations."

Hulio said the "wrong" report published on Sunday against his company was "based on incorrect premises, within the framework of a well-organized and well-timed campaign by known interested parties. The company is weighing its legal steps against the delusional claims put forth in the report.

Speaking to 103FM Radio, Hulio said, "The platform that we create is a platform that saves lives and prevents terrorist attacks, and that needs to be understood. NSO has no list of targets. We made some decisions that are like the NSO Group constitution, and they accompany us to this day. The first is that we only sell to governments and intelligence agencies, not to individuals or [private] organizations."

"The second decision was that we won't sell to every government, since there are some governments that should not have such tools," he said.

The reporting focused on Pegasus, a spyware tool sold by NSO that the investigation said is being used by dozens of governmental clients. The analysis carried out on a leaked list of 50,000 phone numbers found that the list included people targeted by the governments of Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, and the United Arab Emirates.

The Guardian's report on Pegasus claimed that Gantz "closely regulates NSO" and approves each individual export license before the surveillance software is sold to a new country. In its response, NSO stated that "you falsely claim that the Israeli government monitors the use of our customers' systems, which is the type of conspiracy theory that our critics peddle," adding: "Regarding export licenses, NSO is subject to various export control regimes including the Israeli MoD, similar to existing regulations in other democratic countries."

In a statement on Monday, the Defense Ministry said if it finds that the NSO Group violated the terms of its export licenses, it will "take appropriate action." The ministry said that Israel only permits companies to export cybersecurity products to "government figures only for legal purposes and to prevent and investigate crimes and to combat terrorism. And this is dependent upon commitments regarding the end use/user from the purchasing country, which must abide by these conditions."

NSO Group has denied selling the software to authoritarian governments for the purposes of spying on dissenters, labeling the allegations "false."

ISRAEL HAYOM
This is where we stand

Israeli officials: NSO probe could jeopardize sensitive diplomatic relations

Israel says it will launch an inquiry into claims that private Israeli firm NSO Group's "Pegasus" spyware was used by governments across the globe to spy on political rivals, journalists, and human rights activists.

Israel will launch an inquiry into claims that private Israeli firm NSO Group's "Pegasus" spyware was used by governments across the globe to spy on political rivals, journalists, and human rights activists.

Follow Israel Hayom on Facebook and Twitter

The inquiry team is expected to include representatives from the Defense Ministry, National Security Council, Mossad, other agencies, and legal experts. Its goal will be to determine whether NSO Group acted in contravention of the defense export permit it received from the Defense Ministry's Defense Exports Control Agency (DECA), and whether its products were used by various clients in contravention of the conditions of the permit.

The decision to launch the inquiry came on the heels of an investigation by 17 media organizations into NSO's spyware published on Sunday on how it was being used to target prominent individuals.

The cellphones of French President Emmanuel Macron and 15 members of the French government may have been among potential targets in 2019 of the surveillance spyware, according to French newspaper Le Monde.

An official in Macron's office said authorities would investigate Le Monde's report, and if the targeting is proven, it would be "extremely grave."

Le Monde quoted NSO as saying the French president was never targeted by its clients.

Fifty people close to Mexico's president, Andres Manuel Lopez Obrador, were also on the potential target list. They include his wife, children, aides and cardiologist. Lopez Obrador was in opposition at the time. A Mexican reporter whose phone number was added to the list in that time period, Cecilio Pineda, was assassinated in 2017.

After Mexico, the largest share of potential targets was located in the Middle East, where Saudi Arabia is reported to be among NSO clients. Also on the list were numbers in Bahrain, the United Arab Emirates, India, Hungary, Azerbaijan, Kazakhstan and Pakistan, Morocco and Rwanda.

Radio France reported on Tuesday that Moroccan King Mohammed VI's phone was on a list of numbers of people identified as potential Pegasus spyware targets by Morocco's intelligence services.

Morocco on Monday denied the allegations, saying it had "never acquired computer software to infiltrate communication devices."

Jean Asselborn, the foreign minister of Luxembourg, said Tuesday NSO Group was present in Luxembourg via its subsidiaries, and that he would be writing a letter to the directors of those Luxembourg units of NSO to remind them of the importance of protecting human rights.

NSO denies ever maintaining a list of "potential, past or existing targets." It claims to sell only to "vetted government agencies" for use against terrorists and major criminals.

El a acuzat Rusia şi Iranul că au făcut eforturi pentru a se amesteca în alegerile din 2020, vizând sistemele de vot de la nivelul statelor, dar şi locale.

"Ritmul şi severitatea atacurilor au crescut, adversarii noştrii recurg tot mai mult la atacuri cibernetice pentru a semăna discordie. Securitatea cibernetică nu mai poate fi ceva care apare după evenimentul propriu-zis", a subliniat el, completând că "așa cum tacticile se îmbunătățesc, acelaşi lucru trebuie să se întâmple cu capabilităţile".

Oficialul american a afirmat că CISA este angajată pentru a asigura o apărare cibernetică colectivă, la nivel internațional, și a făcut apel la cooperare la toate nivelurile guvernelor şi industriilor din toate ţările pentru a permite un răspuns rapid la astfel de riscuri.

"Niciun atac, niciun compromis nu trebuie să se producă mai mult de o singură dată. Trebuie să reducem la minim amploarea şi consecinţele împărtăşind informaţii despre grupurile criminale şi tacticile lor", a mai spus Brandon Wales.

Lindy Cameron, director executiv al Centrului naţional de securitate cibernetică din Regatul Unit, a mărturisit marţi că participă pentru prima la o conferinţă alături de omologii ei după ce a fost numită în funcţie, în urmă cu un an.

"Pandemia de COVID-19 a adus o schimbare dramatică în modul în care trăim şi muncim, iar tehnologia a fost un mare sprijin în această perioadă dificilă. Securitatea cibernetică nu a fost niciodată mai importantă", a subliniat ea.

Lindy Cameron susţine că centrul pe care îl conduce a răspuns la peste 3.000 de incidente care au vizat în primul rând serviciile sanitare, colaborând cu 5.000 de organizaţii pentru a le întări rezistenţa.

La fel ca şi omologii ei, ea a militat pentru intensificarea colaborării operaţionale între state. "Securitatea cibernetică nu poate fi asigurată de o singură organizaţie", a afirmat Lindy Cameron, afirmând că serviciile de securitate publică, sectorul privat şi simplii cetăţeni trebuie să fie cu toţii implicaţi.AGERPRES/(A - autor: Florin Ştefan, editor: Ionuţ Mareş, editor online: Anda Badea)

THE TIMES OF ISRAEL

Government said to form team to deal with fallout of NSO spyware revelations

Report says officials looking into PR, diplomatic consequences from allegations that firm's Pegasus software was used by countries to spy on politicians, journalists

The government has appointed a special team to handle the fallout of revelations that Israel-based NSO Group sold spyware allegedly used by governments to target politicians, journalists and others worldwide, according to a Tuesday report.

Citing two unnamed senior Israeli officials, the Walla news site said the interagency team will examine the allegations against NSO published in numerous international outlets and what the potential security, diplomatic and legal consequences could be. The team, which reportedly first met on Sunday, includes representatives from the Defense Ministry, Foreign Ministry, Justice Ministry, Mossad and Military Intelligence.

The officials said the government was treating the matter very seriously and that the main question was how to deal with other companies and future agreements, as standard procedures appeared to have been taken in granting export licenses to NSO.

"This is a very significant event," one of the officials was quoted saying. "We are trying to understand its full significance. We must check if after the latest publications there is a need for a change in policy concerning the expert of offensive cyber systems to other countries."

The news site also cited concerns in Israel that though the initial damage has been confined to public and media criticism, the allegations could lead to diplomatic fallout.

The report came as the NGO that leaked the list of 50,000 potential targets for NSO's Pegasus software said French President Emmanuel Macron's phone number was among them, and French radio reported that Moroccan King Mohammed VI's number was identified a list of possible targets by Morocco's intelligence services.

Earlier Tuesday, Defense Minister Benny Gantz asserted Israel operates fully within international law in its granting of export licenses.

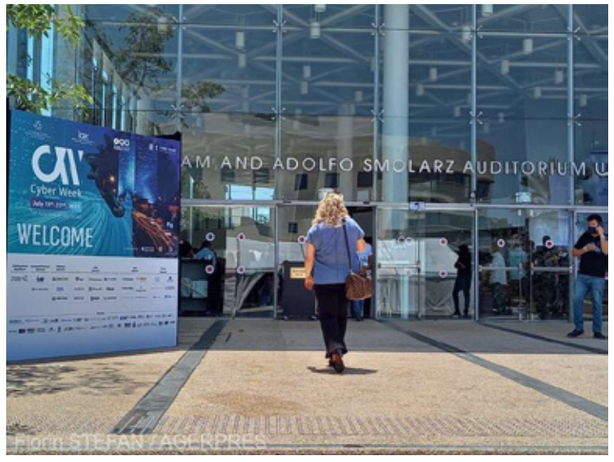
"We are aware of recent publications regarding the use of systems developed in certain Israeli cyber companies," said Gantz in a speech to Cyber Week at Tel Aviv University, without mentioning NSO Group by name. "Israel, as a liberal Western democracy, controls exports of cyber products in accordance with its defense export control law, complying with international export control regimes."

Gantz added that, "as a matter of policy, the State of Israel authorizes the export of cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism. The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject."

On Sunday, an in-depth investigation led by 17 major international news organizations claimed that NSO Group has sold cellphone malware used to target journalists, activists and politicians in dozens of countries.

AGENȚIA ROMÂNĂ DE PRESĂ AGERPRES
Actualizează-te!

Ministrul israelian al Apărării: ''Rachetă sau tastatură, nu vom tolera pe nimeni care ne ameninţă poporul''



Ministrul Apărării din Israel, Benny Gantz, a transmis marţi, în prima zi a conferinţei Cyber Week 2021 de la Tel Aviv, un mesaj de fermitate faţă de "duşmanii" ţării, afirmând că, indiferent dacă e vorba de "rachetă sau tastatură, nu vom tolera pe nimeni care ne ameninţă poporul", lansând însă în acelaşi timp şi un apel la cooperare în domeniul securităţii cibernetice între statele partenere.

"Atacurile asupra Israelului vor primi un răspuns adecvat", a declarat şi general maiorul Tamir Heyman, director al serviciului de informaţii militare al IDF (Forţele Defensive Israeliene), care a ridicat premiul pentru securitate cibernetică la Cyber Week 2021, decernat chiar armatei.

El a mai afirmat că atacurile cibernetice trebuie tratate la fel ca cele care au loc în lumea reală.

Tamir Heyman a spus că, în cadrul recentei operaţiuni 'Guardian of the Walls' împotriva Hamas din Fâşia Gaza, informaţii adunate din mai multe surse, inclusiv din spaţiul cibernetic, au fost utilizate prin capabilităţi de procesare avansate, printre care şi inteligenţa artificială, şi au dus la rezultate operaţionale.

"Asta a permis IDF să funcţioneze mai bine, mai repede şi cu mai puţine victime", a afirmat el. IDF a putut astfel să adune informaţii cu un mare grad de acurateţe privind locurile în care se aflau mai mulţi comandanţi de rang înalt din Hamas, lichidând mai mulţi dintre ei, a adăugat el.

Referindu-se la ameninţările cu care se confruntă în prezent Israelul, Heyman a spus că cele din spaţiul cibernetic apar constant.

"Putem să răspundem majorităţii ameninţărilor prin intermediul unor capabilităţi avansate de apărare. Israelul are un aparat de securitate avansat şi reuşeşte să dejoace mii de atacuri cibernetice zilnic", a dat el asigurări.

Însă, ca şi în alte dimensiuni ale luptei, doar apărarea în sine nu este de ajuns. "Sunt necesari paşi suplimentari pentru a păstra supremaţia Israelului asupra duşmanilor săi", a afirmat el, avertizând că toţi cei care atacă Israelul în aer, pe mare sau la sol trebuie să înţeleagă riscurile pe care şi le asumă.

Benny Gantz, ministrul apărării din Israel, a felicitat IDF pentru că a câştigat premiul pentru securitate cibernetică la ediţia din 2021 a Cyber Week şi a dat asigurări că ţara sa depune constant eforturi pentru a-şi îmbunătăţi securitatea cibernetică.

El a afirmat că în ultimii ani a existat o înmulţire semnificativă a numărului atacurilor comise de elemente ostile, inclusiv de Iran şi statele afiliate, care încearcă să obţină acces la sistemele IT ale infrastructurilor naţionale ale Israelului.

"Israelul a demonstrat abilitatea de a-şi dezvolta reziliența, avantajele tehnologic şi calitativ în regiune", a afirmat Gantz.

Ministrul a reamintit că, în timpul operaţiunii 'Guardian of the Walls', Israelul a reuşit să-l elimine pe şeful diviziei cibernetice a Hamas, Juma Tahla, şi că IDF a distrus mai multe echipamente şi infrastructuri de care se folosea organizaţia jihadistă.

"Mesajul nostru este foarte clar: indiferent dacă e vorba de rachetă sau tastatură, nu vom tolera pe nimeni care ne ameninţă poporul. Multă muncă este necesară pentru a ne menţine avantajul în domeniu. Asta presupune crearea unui întreg ecosistem", a spus ministrul israelian al Apărării.

"Facem apel la prietenii noştri din întreaga lume să facă schimb de informaţii şi expertiză şi să dezvolte noi capabilităţi. Noile grupuri de lucru pe care le avem cu SUA şi alte ţări sunt foarte importante. În acest context, Israelul vrea ca, împreună cu SUA, să se asigure că securitatea este menţinută şi în spaţiul cibernetic", a mai afirmat el.

Gantz a subliniat că Israelul va continua să colaboreze cu toate organizaţiile relevante şi să-şi dezvolte capabilităţile, dotându-şi experţii în securitate cibernetică cu toate instrumentele de care au nevoie.

"Vom continua să acţionăm împotriva tuturor celor care ne ameninţă cetăţenii, fie că lansează rachete sau încearcă să atace un spital. La fel cum Israelul a învins în războaiele din Orientul Mijlociu, va avea câştig de cauză şi în înfruntarea noii ameninţări cibernetice. Statul Israel va rămâne cea mai puternică ţară din regiune şi în acest domeniu", a încheiat el.

Brandon Wales, director executiv al Agenţiei americane pentru securitate cibernetică şi a infrastructurii (CISA), a spus, la rândul său, că "peisajul ameninţărilor cibernetice este mai dinamic ca niciodată".

"Adversarii noştri sunt diverşi - de la state ostile, ca Rusia, China şi Iran - până la infractori cibernetici. În ultimul an am asistat la incident cibernetic după incident cibernetic", a adăugat responsabilul american, afirmând că infractorii cibernetici au profitat de pandemie, pe care au folosit-o ca pe o oportunitate "de a fura date, de a-i viza pe dezvoltatorii de vaccinuri şi lanţurile de aprovizionare".

"Trebuie să abordăm schimbările de mâine într-un ecosistem mai amplu. Trebuie să ne continuăm să ne întrebăm: Cum putem face reţelele mai sigure? Cum putem să ne asigurăm că va exista forţa de muncă în domeniu adaptată la asta? Ce inovaţii avem nevoie de a schimba paradigma în securitate cibernetică? Răspunsul trebuie să vină în urma unor consultări cu toţi actorii, de la marile companii, agenţii guvernamentale şi până la mediul academic. Avem nevoie de mai multă colaborare şi de mai multă inovare", a subliniat Brandon Wales.

THE TIMES OF ISRAEL

After alleged Iranian cyberattack, Israel's Water Authority beefs up defenses

Israel's Water Authority hired a cybersecurity company to protect its machinery following an attack on water infrastructure last year that Israel blamed on Iran, the firm said Wednesday.

The company, SIGA OT Solutions, said it signed an agreement with the authority to "to counter cyberthreats to the machinery and equipment that comprise the critical infrastructure," as well as defend them against ransomware attacks.

Last April, six Water Authority facilities were targeted in the cyberattack in which hackers attempted to increase the amount of chlorine in the water supply to dangerously high levels. The attacks were countered before any damage could be caused. However, the incident raised major concerns about the ability of the Water Authority to protect itself from future cyberattacks.

Before receiving the contract, SIGA tested out its cyber defense system SigaGuard at a number of water installations. According to the firm, the product tracks the underlying electrical signals in the water systems to "detect initial evolvements of anomalies in the process behavior and gains direct visibility into the operational technologies process."

"Water utilities are at the forefront of global cyberattacks. But utilities have minimal tolerance for a downtime in service, and no utility would agree to a hacker deciding whether its infrastructure will operate or not," Amir Samoiloff, co-founder and CEO of SIGA, said in a statement.

On Tuesday, the outgoing head of Military Intelligence said Israel is facing constant cyberthreats and will respond to attacks as it does to any other type of aggression.

"Israel is under constant threat in the cyber dimension, and attacks are sometimes carried out against it. We are able to deal with most of the threats through advanced defense capabilities," Maj. Gen. Tamir Hayman said at a conference at Tel Aviv University.

Hayman said that like in other military theaters, defense alone is not sufficient and "additional steps must be taken to preserve Israel's [tactical] superiority over our enemies."

"Those who attack Israel by air, sea, land, or cyber need to understand the risk they are taking," Hayman declared.

"As seen time and time again, the attacks will be answered accordingly," he warned.

Emanuel Fabian contributed to this report.

THE TIMES OF ISRAEL

IDF intel chief says Israel under nonstop cyber-threats, is retaliating

Maj. Gen. Tamir Hayman says defense alone does not suffice, steps must be taken to 'preserve Israel's superiority'

The head of Military Intelligence on Tuesday said Israel is facing constant cyber threats and will respond to attacks as it does to any other type of aggression.

"Israel is under constant threat in the cyber dimension, and attacks are sometimes carried out against it. We are able to deal with most of the threats through advanced defense capabilities," Maj. Gen. Tamir Hayman said at a conference at Tel Aviv University.

Hayman said that like in other military theaters, defense alone is not sufficient and "additional steps must be taken to preserve Israel's [tactical] superiority over our enemies."

"Those who attack Israel by air, sea, land, or cyber need to understand the risk they are taking," Hayman declared.

"As seen time and time again, the attacks will be answered accordingly," he warned.

Hayman also said that during the recent 11-day war between Israel and the Hamas terror group in Gaza, the Israel Defense Forces used online sources, alongside artificial intelligence and machine learning, to assist in planning and conducting operations.

"This allowed the IDF to function better, faster, and with fewer casualties," he said.

This led Military Intelligence officials to declare the Gaza campaign the world's "first AI war."

ARUTZ SHEVA 7
israelnationalnews.com

Gantz: All rocket fire from Lebanon will be met with an iron fist

Defense Minister Benny Gantz addressed the Cyber Week which is being held at Tel Aviv University Tuesday.

Regarding the rocket fire from Lebanese territory early Tuesday morning, he said: "I would like to address the terror attack that took place on our northern border. The State of Israel is interested in seeing a prosperous, peaceful and stable Lebanon. Unfortunately, the situation in Lebanon is worsening, since Hezbollah and additional terrorist organizations are operating against the interests of Lebanese citizens. We have responded overnight to the rocket fire, which violated Israel's sovereignty. I would like to emphasize that the State of Lebanon is responsible for this violation. Israel extended a helping hand and offered humanitarian aid to Lebanon, yet every security threat will be met with an 'iron fist' from the same hand that was extended. I call on the international community to take action to return stability to Lebanon."

On defense export licenses from the Ministry of Defense, Gantz said: "I wish to address recent developments – we are aware of recent publications regarding the use of systems developed by certain Israeli cyber companies. Israel, as a liberal western democracy, controls exports of cyber products in accordance with its defense export control law, complying with international export control regimes. As a matter of policy, the State of Israel authorizes the export of cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism. The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject."

Regarding cyber-attacks against Israel, he said: "In recent years there has been a significant increase in the number of attacks perpetrated by hostile actors, including Iran and its proxies, which seek to access the ICT systems of Israel's national infrastructure. In the face of this rise - from several individual attacks to dozens of attacks per year- Israel has been resilient, and demonstrated its technological advance and Qualitative Military Edge."

ARUTZ SHEVA 7
israelnationalnews.com

Gantz: Lebanon responsible for attack on northern border

Minister of Defense Benny Gantz addresses participants of Cyber Week at Tel Aviv University.

Today, Minister of Defense Benny Gantz addressed participants of Cyber Week at Tel Aviv University.

"I would like to address the terror attack that took place on our northern border," he said. "The State of Israel is interested in seeing a prosperous, peaceful and stable Lebanon. Unfortunately, the situation in Lebanon is worsening, since Hezbollah and additional terrorist organizations are operating against the interests of Lebanese citizens. We have responded overnight to the rocket fire, which violated Israel's sovereignty. I would like to emphasize that the State of Lebanon is responsible for this violation. Israel extended a helping hand and offered humanitarian aid to Lebanon, yet every security threat will be met with an 'iron fist' from the same hand that was extended. I call on the international community to take action to return stability to Lebanon."

On defense export licenses from the Ministry of Defense, he said: "I wish to address recent developments – we are aware of recent publications regarding the use of systems developed by certain Israeli cyber companies. Israel, as a liberal western democracy, controls exports of cyber products in accordance with its defense export control law, complying with international export control regimes. As a matter of policy, the State of Israel authorizes the export of cyber products solely to governments, only for lawful use, and exclusively for the purposes of preventing and investigating crime and terrorism. The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject."

Regarding cyber-attacks against Israel. he said: "In recent years there has been a significant increase in the number of attacks perpetrated by hostile actors, including Iran and its proxies, which seek to access the ICT systems of Israel's national infrastructure. In the face of this rise - from several individual attacks to dozens of attacks per year- Israel has been resilient, and demonstrated its technological advance and Qualitative Military Edge."

"Our message is clear – be it a rocket or a keyboard – we will not tolerate anyone who threatens our people," Gantz said.

Also at the event the "Cyber Shield" award was presented to the IDF for "inspiring and groundbreaking achievements in promoting Israeli cyber and bringing Israel to the status of a global cyber power," the organizers said.

The award was presented to the head of Military Intelligence Maj.-Gen. Tamir Heiman and the head of the C4I Directorate Maj.-Gen. Lior Carmeli.

Heiman said that the IDF was able to function "better, faster and with fewer casualties" during the May fighting due to intelligence that had been gathered from a variety of sources and "fused together" by advanced processing capabilities such as artificial intelligence and machine learning.

Echoing Gantz, Heiman said that Israel is "under constant threat" in the cyber sphere and is able to deal with them via advanced defense capabilities.

"As in other sorts of combat, defense alone is not enough. Additional steps must be taken to preserve Israel's supremacy over our enemies," he said. "Those who attack Israel by air, sea, land or cyber need to understand the risk they are taking. As they are able to see time and time again, the attacks will be answered accordingly."

THE JPOST.com JERUSALEM POST

Cyber Week: How the Start-Up Nation became a world leader in cyber tech and investment

• By SETH J. FRANTZMAN

'IN ABSOLUTE numbers, Israeli [cyber] exports are almost 10% of the global market,' says Prof. Isaac Ben-Israel. View of the Tel Aviv skyline. (Miriam Alster/Flash90)

Israel has become one of the world leaders in cybersecurity. One of those who played a key role in Israel's pioneering role in this field, which is now emerging as one of the most important aspects of our global economy and security, is Prof. Isaac Ben-Israel.

"I was in effect the one in 2010-11 that was asked by the previous prime minister Benjamin Netanyahu how to make Israel one of top five countries in cyber security and my report was approved and turned into a government resolution in 2011," he says. "That was ten years ago and now you can see the results around you, the approach of the report was interdisciplinary, our recommendations were not limited to technology, but also the other aspects of our lives."

Ben-Israel, the director of the Interdisciplinary Cyber Research Center at Tel Aviv University, is an expert in mathematics, physics and philosophy; he earned his PhD in 1988. The center at TAU has some 300 members and is interdisciplinary, meaning it takes into account not just computers and what we may think of as "cyber" but also other fields such as experts from social sciences. Ben-Israel envisioned it this way

It will be one of the focuses of Cyber Week, the annual summit meeting of the heads of global and local cyber industry. Led by the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University along with the Israel National Cyber Directorate, the Ministry of Economy and the Ministry of Foreign Affairs, the event will be held on July 19-22, at Tel Aviv University this year. Past events have seen thousands of attendees from dozens of countries and over 50 roundtables and workshops.

This year's conference will be attended by Prime Minister Naftali Bennett, Defense Minister Benny Gantz and Minister of Public Security, Omer Bar Lev along with dozens of other senior officials from Israel and abroad. Organizers say it is "a meeting point for prominent cyber experts and researchers from Israel and around the world. Senior diplomats and businessmen bring the latest issues and trends in the field and in relation to the period, along with the most updated developments and information."

Cyber isn't just about cyber defense or cyberattacks, which is how we often hear about this buzzword in the news. It is also about diplomacy and crisis management and the new laws that govern cyber issues around the world. This can include cyber defenses, artificial intelligence, medicine and cloud storage. Organizers say that the first marine cyber conference in Israel is to be held at the Ashdod port in participation with senior officials from around the world.

BEN-ISRAEL served in the IDF until retiring in 2002. During his service, he held posts in operations, intelligence and weapon development units and research and development in the IDF, according to Tel Aviv University. He also serves as chairman of the Israeli Space Agency.

He looks back on those important years as Israel sought to establish itself as a cyber power. "One recommendation was to create in every university a cyber research center. In those days there was no research on cybersecurity because it was sensitive and secret and used by intelligence services. In Israel, as you know, we have research and teach cybersecurity now in high schools, which was one of our recommendations; that is about building human capital and also starting with start-ups and [business] unicorns and then government regulations and budgets."

It's difficult to measure cyber power, he says. "You can measure jobs, patents, publications, or how many capabilities were demonstrated." Recently the International Institute for Security Studies published an index of leading cyber countries and found that while the US was the cyber superpower, Israel is in the second tier of leaders along with China, Russia, the UK and others.

Ben-Israel says that in the last year, Israel's cyber exports have exceeded $7 billion, which is more than defense exports. "If you look at the whole business sector globally, and you look at [the] whole sum and how much investment from [the] business sector goes to Israel, in 2018 it was 18% and 2019 it was 26% and in 2020 to 31% and the first half of 2021 it is 45% putting Israel first on the list, more invested in Israel than the US. In absolute numbers, Israeli exports are almost 10% of [the] global market," he says. This is massive.

Today we hear a lot about cyber attacks. Ben-Israel notes that in recent years ransomware attacks have become common. This means "someone locks the information in your computer and if you don't give money they won't give [the] key to open the lock. The number in [the] last year or two increased by a huge factor." As companies during COVID-19 rely more on computer communication, this also put wind in the sails of the ransomware attackers because they can be at the jugular of international trade. There are other factors

will influence the Israeli hi-tech world.

"Israel does a lot of innovation for good, but there's also this," Shwartz Altshuler said. Scandals like the Pegasus Project "hurt Israel's good name. Israel is trying to promote hi-tech and be the Start-Up Nation, but the other side spoils it."

Tabansky pointed to reports on ties between the Kaspersky antivirus software and the Russian government, followed by a ban on using it on US government computers starting in 2017, or when Edward Snowden leaked evidence in 2013 that the US's NSA was surveilling Americans' phones, plus those of foreign leaders.

"We've been arguing about this for quite a long time," he said. "Now [the NSO leak] is joining those other major events." •

THE JPOST.com JERUSALEM POST

Gantz: Defense Ministry looking into NSO Group investigation

Israel seeing a significant rise in cyber attacks targeting its national infrastructure.

By ANNA AHRONHEIM

The Defense Ministry is studying the investigation into NSO Group, Defense Minister Benny Gantz said Tuesday after it was revealed that the Israeli cyber company has been selling spyware to foreign governments to target journalists and activists.

"We are aware of recent publications regarding the use of systems developed by certain Israeli cyber companies," Gantz said Tuesday at Cyber Week at Tel Aviv University, without naming the Herzliya-based company.

On Sunday, the Pegasus Project revealed that the spyware sold by NSO (Pegasus) had been identified on the phones of individuals targeted by the governments of Azerbaijan, Bahrain, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, the United Arab Emirates and more.

The investigation was carried out by 17 media organizations and led by the Paris-based journalism nonprofit Forbidden Stories, and sponsored by Amnesty International. At the center of it was a leaked list of 50,000 phone numbers belonging to journalists, senior politicians and business people.

Gantz asserted that as a matter of policy Israel authorizes the export of cyber products "solely to governments, only for lawful use and exclusively for the purposes of preventing and investigating crime and terrorism" and that the country controls the exports of such products and complies with international export control regimes.

"The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject," Gantz said.

In a statement released after the investigation was published, the Defense Ministry said that it will take "appropriate action" if NSO Group violated the terms of its export licenses or end use certificates.

Touching on cyber in Israel, Gantz said that there has been a "significant increase" in the number of cyberattacks targeting Israeli national infrastructure in recent years, including by Iran and its proxies.

"Our enemies know no boundaries – just as they fire rockets at civilians, they aim to harm civilian facilities via cyberspace while endangering human lives," he said, adding that Israel works around the clock to prevent cyberattacks and has demonstrated "its technological advance and qualitative military edge."

Gantz said that a lot of hard work is required to maintain Israel's advantage in the cyber sphere and is working with partners "around the world" to share information, expertise and develop new capabilities.

Touching on the recent fighting with Gaza, the former chief of staff mentioned the targeting of the AP building that housed various media outlets as well as Hamas "cyber terrorists under Iranian guidance" who attempted to damage Israeli infrastructure through cyberattacks.

During the fighting, the IDF also struck the head of Hamas's cyber command, Jamaa Tahla, as well as several cyberattackers, related equipment and infrastructure used by the terror group's cyber command.

Defense Minister Benny Gantz warned at Cyber Week that the government approves cyber products to be sold only "to governments and only for lawful use in order to prevent crime and terrorism. Countries who purchase those systems must adhere to the conditions of use."

The Knesset Foreign Affairs and Defense Committee also plans to review the matter, with the panel's chairman, Ram Ben Barak of Yesh Atid saying "we certainly need to take a new look at the whole topic of licenses given by DECA."

"Truth be told," Ben Barak told Army Radio, "[Pegasus] has uncovered a lot of terrorist cells and crime families and helped many people. If it has been misused, or sold to irresponsible parties, that must be examined."

Shwartz Altshuler suggested that greater transparency would vastly improve DECA's results. She called for it to be moved from the Defense Ministry to the Economy Ministry, so that it would be subject to the Freedom of Information Law.

"All the rot happens behind the scenes," she said. "If there is no transparency, there is corruption."

The IDI researcher said there are strong ties between members of the defense establishment and cybersecurity companies like NSO. For example, former IDF chief censor Ariella Ben-Avraham immediately moved to NSO after leaving the military, and the IDF censors elements of news reporting about NSO, as determined by DECA.

AS FAR as the international implications of the NSO scandal are concerned, a senior Israeli diplomatic source said that, at the moment, the damage is mostly in the public sphere and not in government-to-government relations, but there is potential for diplomatic tensions.

The reports come soon after Operation Guardian of the Walls, when there was massive anti-Israel activity. Soon after the NSO story broke, Ben & Jerry's announced that it will stop doing business in Judea and Samaria, and its board said it wants to boycott Israel entirely. Cybersecurity and ice cream don't have a lot to do with each other, but the negative stories about Israel compound each other.

The NSO story specifically "connects us to countries that are not 'like-minded,'" meaning not liberal democracies, the diplomatic source said. "From the outside, it makes us look like facilitators of countries with human rights problems."

For example, prominent political scientist and a former minister in the Portuguese government Bruno Maçães, who has a history of support for Israel, pointed to the fact that Hungary blocks anti-Israel decisions in the EU and was an authorized NSO client. Maçães tweeted: "So am I right in concluding that Israel is part of the global forces spreading autocracy worldwide?... Israel seems to have decided its national interest is advanced by supporting autocracies."

Still, the diplomatic source argued that criticism in that vein "ignores the fact that other countries sell similar products."

Tabansky said "it's very easy to create an association between the wicked activities of an Israeli company and the State of Israel or the Jews in general. That is obviously not a new phenomenon; we know how this works.

"Nobody talked about the truck manufacturers in terrorist attacks in Nice or Berlin," he added.

Shwartz Altshuler said that Israel may lose cybersecurity as a tool that it used to improve its international relations, "but maybe it's justified.

"Part of our pride is that we're the Start-Up Nation, which is how we draw big companies to open research and development centers here," she said. "There has been a lot of pressure on Facebook to close its center in Israel in the wake of Guardian of the Walls.... If Israeli technology has the reputation of being arms dealers, think how that used Israeli technology as a way of strengthening Israel's diplomatic standing, bringing it closer to more countries.

But the prestige of Israeli cybersecurity prowess has taken a hit following the NSO report, which has dented Israel's public image at a sensitive time and could have negative reverberations in its foreign relations. The report also revealed weaknesses in how Israel regulates sales of defense technology.

PEGASUS IS not a classic cybersecurity product, in that it is not purely defensive. It is considered a "dual use" product – meaning, it can be weaponized – and as such, it needs multiple authorizations from the Defense Export Controls Agency before each sale is made.

DECA was established in 2006, after Israel tried to sell airborne early-warning systems to China, infuriating the US, which demanded greater regulation of Israeli arms deals.

Today, any security-related product must go through four stages before a sale. First, the company must register as a security exporter. Next, it needs to register each product it wants to sell; about 20% of the products are confidential, and dealing with them requires a security clearance, ranging from protected to top secret.

Next, the company needs a marketing license for the product, which means permission to negotiate a deal with a specific country about a specific product. A new license is required for each product in each country.

The final step is for DECA to review the deal and give authorization to sell the product.

Israel's considerations in providing licenses include its immediate security needs, such as ensuring the defense technology won't get into Iran's hands, as well as international relations, as in the case of the American uproar over selling Phalcon airborne early-warning systems to China, and as such the Foreign Ministry is also involved in DECA.

Dr. Lior Tabansky, head of research development for the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, which organizes Cyber Week, argued on this week's Jerusalem Post podcast that, because of the heavy government regulation, Pegasus is "definitely not exported to countries that are known abusers of international norms and liberties.

"The publication of this week is completely strange because there really is no connection between the list of phone numbers that they call evidence and NSO's potential customers," he said.

Tabansky also said that NSO sells to governments, which in turn decide whom to target: "That's not something that is up to the decisions of tech providers."

Plus, in the case of NSO, it has an internal auditing program to assess risks prior and during the contract. If someone is caught abusing its product, NSO can stop giving the government agency access to it.

However, Tehilla Shwartz Altshuler, head of the Democracy in the Information Age program at the Israel Democracy Institute, said that defense exports have "the heaviest regulation in the market," and therefore "there is no way the State of Israel didn't know who NSO is selling to, what it's selling and under what conditions."

The NSO story has been framed by much of the international media as something wrong that Israel has done, while much of the Israeli media has reported it as though NSO is a private company doing bad things, Shwartz Altshuler said, calling the Israeli framing "nonsense."

"There is nothing they sold that wasn't encouraged by the state," she posited.

THE DEFENSE Ministry, Foreign Ministry, Justice Ministry, Mossad and other Israeli government agencies are now working on a task force to look into the media reports about NSO and determine if something went wrong in the regulatory process.

Cyber Week
July 19th-22nd, 2021
Tel Aviv University, Israel

Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University
Blavatnik Interdisciplinary Cyber Research Center
Tel Aviv University
Cyber Israel National Cyber Directorate
In cooperation with: Israel Cyber Alliance
Ministry of Foreign Affairs Israel

THE JERUSALEM POST
THE JPOST.com

Cyber sensitivity
Gantz: Defense Ministry may open probe of NSO Group
Page 2

Gantz: We're considering probe into NSO Group

Israel sees sharp rise in cyber attacks targeting infrastructure

• By ANNA AHRONHEIM

The Defense Ministry is studying the investigation into NSO Group, Defense Minister Benny Gantz said Tuesday after it was revealed that the Israeli cyber company has been selling spyware to foreign governments to target journalists and activists.

"We are aware of recent publications regarding the use of systems developed by certain Israeli cyber companies," Gantz said Tuesday at Cyber Week at Tel Aviv University, without naming the Herzliya-based company.

On Sunday, the Pegasus Project revealed that the spyware sold by NSO (Pegasus) had been identified on the phones of individuals targeted by the governments of Azerbaijan, Bahrain, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, the United Arab Emirates and more.

The investigation was carried out by 17 media organizations and led by the Paris-based journalism nonprofit Forbidden Stories, and sponsored by Amnesty International. At the center of it was a leaked list of 50,000 phone numbers belonging to journalists, senior politicians and business people.

Gantz asserted that as a matter of policy Israel authorizes the export of cyber products "solely to governments, only for lawful use and exclusively for the purposes of preventing and investigating crime and terrorism" and that the country controls the exports of such products and complies with international export control regimes.

"The countries acquiring these systems must abide by their commitments to these requirements. We are currently studying the information that is published on the subject," Gantz said.

In a statement released after the investigation was published, the Defense Ministry said that it will take "appropriate action" if NSO Group violated the terms of its export licenses or end use certificates.

Touching on cyber in Israel, Gantz said that there has been a "significant increase" in the number of cyberattacks targeting Israeli national infrastructure in recent years, including by Iran and its proxies.

"Our enemies know no boundaries – just as they fire rockets at civilians, they aim to harm civilian facilities via cyberspace while endangering human lives," he said, adding that Israel works around the clock to prevent cyberattacks and has demonstrated "its technological advance and qualitative military edge."

DEFENSE MINISTER Benny Gantz addresses Cyber Week at Tel Aviv University yesterday. (Chen Galili/Tel Aviv University Cyber Week)

Gantz said that a lot of hard work is required to maintain Israel's advantage in the cyber sphere and is working with partners "around the world" to share information, expertise and develop new capabilities.

Touching on the recent fighting with Gaza, the former chief of staff mentioned the targeting of the AP building that housed various media outlets as well as Hamas "cyber terrorists under Iranian guidance" who attempted to damage Israeli infrastructure through cyberattacks.

During the fighting, the IDF also struck the head of Hamas's cyber command, Jamaa Tahla, as well as several cyberattackers, related equipment and infrastructure used by the terror group's cyber command.

"Our message is clear – be it a rocket or a keyboard – we will not tolerate anyone who threatens our people," Gantz said.

Also at the event the "Cyber Shield" award was presented to the IDF for "inspiring and groundbreaking achievements in promoting Israeli cyber and bringing Israel to the status of a global cyber power," the organizers said.

The award was presented to the head of Military Intelligence Maj.-Gen. Tamir Heiman and the head of the C4I Directorate Maj.-Gen. Lior Carmeli.

Heiman said that the IDF was able to function "better, faster and with fewer casualties" during the May fighting due to intelligence that had been gathered from a variety of sources and "fused together" by advanced processing capabilities such as artificial intelligence and machine learning.

Echoing Gantz, Heiman said that Israel is "under constant threat" in the cyber sphere and is able to deal with them via advanced defense capabilities.

"As in other sorts of combat, defense alone is not enough. Additional steps must be taken to preserve Israel's supremacy over our enemies," he said. "Those who attack Israel by air, sea, land or cyber need to understand the risk they are taking. As they are able to see time and time again, the attacks will be answered accordingly."

THE JERUSALEM POST
THE JPOST.com

NSO, surveillance and the double-edged sword of the Start-Up Nation

The damning reports on the controversial tech company raise questions about how Israeli defense exports are regulated, and put a dent in Israel's prestige as a cybersecurity giant

By LAHAV HARKOV

This week, media outlets around the world published an investigation by Paris-based media nonprofit Forbidden Stories, in cooperation with Amnesty International, that claimed that Israeli firm NSO's Pegasus software was being used by governments to hack journalists, activists and even national leaders and royalty.

Pegasus was meant to give law enforcement and intelligence agencies access to criminals' and terrorists' smartphones, but the reports in 17 media outlets said they had a leaked list over 50,000 phone numbers of "people of interest" to NSO's clients in countries with which Israel has grown closer in recent years, such as Saudi Arabia, the UAE, Bahrain, Azerbaijan, Hungary and India.

Those targets included leaders such as French President Emmanuel Macron, Pakistani Prime Minister Imran Khan and Moroccan King Mohammad VI, and 180 journalists, including one who was murdered in Mexico after reporting on government corruption, as well as countless activists and dissidents.cyberattackers, related equipment and infrastructure used by the terror group's cyber command.

NSO, however, said it investigated the claims and the report is "full of wrong assumptions and uncorroborated theories." The list on which the news stories rely is easily accessible data that have nothing to do with the NSO customer list and did not come from its servers, the company said.

In addition, NSO does not operate its system once it is sold to its clients, which are all law enforcement and intelligence agencies of governments approved by the Israeli government for the sale.

Days later, Prime Minister Naftali Bennett stood on a stage and hailed Israel's cybersecurity industry, in which he made his fortune as the CEO of Cyota 15 years ago. Bennett announced at Cyber Week, an annual international conference at Tel Aviv University, that Israel would be launching the "Global Cybernet Shield," a network that like-minded countries can join to warn one another against cyberattacks and threats.

The Global Cybernet Shield, which is still in development, is an international version of Cybernet, Israel's domestic cyber defense network, led by the Israel National Cyber Directorate with over 1,500 members, including government ministries and major corporations. The National Cyber Directorate uses Cybernet to swiftly disseminate warnings about cyberattacks and isolate online viruses so they don't spread, as well as to explain to organizations how to prepare their systems.

Israel is the first and possibly only country to have such a network, National Cyber Directorate Executive Director of Strategy and International Cooperation Aviram Atzaba explained this week, and foreign governments' cybersecurity units have expressed interest in joining it.

Bennett's idea to take Cybernet global is not only a smart way of protecting Israel and its allies from cyberattacks by bad actors such as Iran, which he singled out for opprobrium in his speech. Israeli prime ministers have long

THE JPOST.com JERUSALEM POST

PM Bennett: We won't tolerate rocket fire from Lebanon

Two rockets were fired from south Lebanon towards Israel early Tuesday morning, IDF responded with tank fire.

By ANNA AHRONHEIM

Israel will not tolerate rocket fire from Lebanon, Prime Minister Naftali Bennett said Tuesday after two rockets were fired into Israeli territory early in the morning.

"I say this sharply and clearly: We will not allow harm to Israel's sovereignty and security," he said during a visit to Ma'alot-Tarshiha in the Upper Galilee several hours after the rocket fire. "Whoever tries to harm us will pay a painful price."

"Lebanon is on the verge of collapse, like any country in which Iran bases itself," Bennett said. "Its citizens were taken hostage by [Iranian Supreme Leader Ayatollah Ali] Khamenei and [Hezbollah Secretary-General Hassan] Nasrallah for the sake of Iranian interests... This is unfortunate, but we will not accept a spillover of the situation in Lebanon into Israel."cyberattackers, related equipment and infrastructure used by the terror group's cyber command.

The two rockets were fired at northern Israel from Lebanon at around 4 a.m. Tuesday morning, setting off incoming rocket sirens in communities along the border, including Rosh Hanikra, Shlomi, Kibbutz Kabri (near Nahariya) and Hanita.

One rocket was intercepted by the Iron Dome air-defense system, and the other fell harmlessly in an open field, the IDF said. There were no casualties or damage, and there were no special instructions for residents, it said. In response, the IDF fired tank shells toward Hamoul Valley from where the rockets had been fired, it said.

Lebanon was responsible for the rocket fire, Defense Minister Benny Gantz said.

"Lebanon is responsible for the nighttime firing because it allows terrorist acts from inside its territory," he said. "The State of Israel will act in the face of any threat to its sovereignty and its citizens and will respond in accordance with its interests at the relevant time and place."

Israel wants to see a "prosperous, peaceful and stable Lebanon," Gantz said later at Tel Aviv University's Cyber Week cybersecurity conference, adding that the situation is worsening because of Hezbollah and other terrorist groups that are acting against the interests of Lebanese citizens.

"Israel extended a helping hand and offered humanitarian aid to Lebanon," he said. "But every security threat will be met with an iron fist from the same hand that was extended."

Lebanon was in a state of collapse, and Hezbollah had a role in that, but Israel will not accept any sort of rocket fire due to that internal state of affairs, IDF Chief of Staff Lt.-Gen. Aviv Kohavi said.

"We will respond in an overt or covert way, or both together, to all violations of our sovereignty from Lebanon – whoever it is," he said.

The attack came several hours after clashes on the Temple Mount between police and Muslim protesters on Tisha Be'av and ahead of Eid al-Adha (Feast of the Sacrifice).

The rocket fire also came a year after a junior Hezbollah operative was killed in an alleged Israeli airstrike in Syria, an attack for which Hezbollah vowed to take revenge.

In May, during Operation Guardian of the Walls, a dozen rockets were fired into Israel from the same area in Lebanon. Several people were injured while running to find shelter.

For the first time since the Second Lebanon War in 2006, incoming rocket sirens were activated in the Lower Galilee and Haifa's bayside suburbs of Kiryat Bialik and Kiryat Motzkin after four rockets were fired.

Several days earlier, six rockets were fired from Rachaya Al Foukhar, north of Kfarchouba in southern Lebanon. They all landed inside Lebanese territory, the IDF said, adding that one of them might have reached Israel. In response, the IDF fired more than 20 tank and artillery shells toward the source of the rocket launches.

It is still unclear who fired the rockets early on Tuesday morning, but the IDF believes it was the same Palestinian militants who fired the rockets in May. Hezbollah is not believed to be behind the rocket fire.

The Lebanese army said three Grad rocket launchers were found in Al Qulaya'ah, "one of them with a missile prepared for firing, and it was then disabled by specialized army units," Lebanon's MTV News reported.

The United Nations peacekeepers said in a statement: "UNIFIL radar monitored the firing of rockets from the northwest area of Qalila towards Israel and then spotted artillery fire from the Israeli army."

UNIFIL, which opened an investigation into the incident, said it was "in direct contact with the Lebanese army and Israel" and is "urging maximum restraint to avoid further escalation."

With the Lebanese economy in a free fall, the IDF is concerned that there may be an increase of incidents along its northern border, Col. Raz Haimlich, commander of the Artillery Corps Fire Brigade 411th "Keren" Battalion, told The Jerusalem Post in a recent interview.

"The Lebanese economy is not good, and that can lead to things happening on the border," he said.

Haimlich's battalion has responded to several incidents along the Lebanese border, including during the recent fighting with Hamas in the Gaza Strip, when Lebanese rioters damaged the border fence and crossed into Israel near Metulla.

The rocket fire on Tuesday came shortly after Israel was said to have struck targets near Al-Safirah in Syria's Aleppo province. The strikes targeted a weapons depot belonging to Iranian-backed militias inside Syrian Army bases, according to the UK-based Syrian Observatory for Human Rights.

The most notable event was the espionage campaign that compromised the IT firm SolarWind's software and impacted 18,000 organizations around the world, including 9 U.S. federal agencies. The incident was characterized by the U.S. federal administration as exceeding the accepted acts of cyber espionage. Recent major incidents also include the Accellion File Transfer Application breach which affected government financial agencies, oil companies, hospitals and universities, the breach into IT firm SITA, which affected millions of airline passengers and the breach into IT firm Kaseya which infected hundreds of its customers with ransomware.

Supply chain attacks prompted governmental responses, the broadest of which was an executive order to strengthen federal cybersecurity, signed by President Biden last May. Among many other cybersecurity-related clauses, the order directs the Director of the National Institute of Standards and Technology (NIST) to identify and develop new standards, tools and best practices to evaluate software security and security practices of developers and suppliers. Accordingly, Israel's National Cyber Directorate (INCD) announced a new initiative that sets cybersecurity standards for web hosting services.

3. Influence Operations

Influence operations remain a widespread phenomenon and a strategy of choice for nation-state actors and foreign governments seeking to change public opinion, interfere in democratic procedures, and exacerbate societal tensions. These include disinformation and fake news campaigns aimed at undermining the public's confidence in COVID-19 vaccines, hack & leak operations aimed at embarrassing public figures, the spread of fake news on sensitive issues in order to polarize societies and more.

According to the U.S. intelligence's Global Trends report from 2021, disinformation campaigns are likely to proliferate in the coming years while determining what is true will become increasingly difficult.

Emerging technologies, such as Artificial Intelligence (AI) are accelerating influence operations and disinformation campaigns rendering them more widespread, sophisticated and difficult to detect. In January, social media analysis company Graphika identified a network of fake Twitter accounts using profile pictures that were artificially created by deep learning techniques (GANs). The accounts had published automated content and texts attacking the Belgian government's decision to limit the access of Chinese companies to the country's 5G networks layout project. According to the annual security assessment of Estonia's Foreign Intelligence Service, Russia's intelligence agencies seek to further develop 'Deepfake' technologies and are likely to exploit them as part of future influence operations aimed to sow discord among Western societies.

4. Critical Infrastructure

Critical Infrastructure continues to serve as a prime target for nation-state actors and criminals. Aside from incidents such as the attack on the U.S. largest pipeline operator Colonial Pipeline, other critical infrastructure facilities were attacked in order to cause physical damage. In January and February, water treatment facilities in California and Florida were targeted by unidentified hackers utilizing credentials for old TeamViewer software and outdated operating systems.

The phenomenon of cyberattacks on critical infrastructure also continues as part of conflicts between nation-states, portraying another means to establish deterrence and cause physical damage. In February, Recorded Future released a report analyzing the electricity outage that had taken place in the city of Mumbai in October 2020. The report suggests it was a part of a broader Chinese response to a border dispute in the Galwan Valley.

5. Increasing role of Artificial Intelligence

Governments and international organizations continue to prepare for the adoption and use by cyber attackers of emerging technologies, such as artificial intelligence (AI), and formulate principles and ethical guidelines for its use and development.

In January, the European Parliament voted in favor of a call for an EU legal framework on AI. The framework includes AI definitions and ethical guiding principles for military and non-military use. The report calls to limit the use and development of lethal autonomous weapon systems (LAWS), to maintain human control and decision making in the public health and justice systems and to ban highly intrusive AI technologies that may be used for mass surveillance. In April, the European Commission proposed a legal framework in an attempt to set global standards for key AI technologies. The proposal limits the use of AI in critical infrastructure sectors and in law enforcement, immigration and social scoring for general purposes done by public authorities.

In February, the Australian Department of Defence released a report noting that cybersecurity will be a key component in achieving and preserving autonomous systems' trust and integrity. According to the report, AI systems must be resilient as well as their communication feeds and training datasets. In addition, the UK's Government Communications Headquarters (GCHQ) published a report outlining how the agency plans to ensure a transparent, ethical and proportional use of AI for national security.

A Way Forward

Despite increased governmental attention to cybersecurity, existing cyber threats are here to stay and are likely to evolve at a faster pace than implemented countermeasures. The pace of threat evolution will be dictated by the pace of digital transformation accelerated by global human crises, such as the COVID-19 pandemic as well as breakthroughs in emerging and disruptive technologies. The growth and proliferation of cyber threats and their intersection with emerging technologies necessitates a coordinated international response that includes information sharing on new threats between governments and between governments and the private sector, cooperation between law enforcement agencies, and an intergovernmental mechanism to inflict costs on foreign governments involved in cyberattacks on critical sectors.

Omree Wechsler is a Senior Researcher at the Yuval Ne'eman Workshop for Science, Technology and Security at Tel Aviv University. Wechsler's report will be presented during Cyber Week 2021 to be held at Tel Aviv University in collaboration with the National Cyber Directorate, the Ministry of Economy, the Ministry of Foreign Affairs, between July 19-22.

I ne samo to, u svemu tome rame uz rame sa njima učestvuje i univerzitet Ben Gurion, koji uveliko "pravi" kadrove za programe specijalizovane za sajber tehnologiju i bezbednost. Kampus univerziteta tik je uz tehnološki park u Ber Ševi, u kome ne manjka ni istraživačkih centara. U prevodu, jedan miks edukacije i prakse, sve na jednom mestu.

Sestrinski Niš

Inače, izraelski grad Ber Ševa i srpski Niš su takozvani sestrinski gradovi. Još jedna zanimljivost, pre izvesnog vremena je formirana Srpsko-Izraelska asocijacija sa ciljem da radi na promociji i ohrabrivanju saradnje sa Izraelom.

CTECH

The 5 biggest global cyber threats of 2021

"Despite increased governmental attention to cybersecurity, existing cyber threats are here to stay and are likely to evolve at a faster pace than implemented countermeasures," writes Omree Wechsler, a Senior Researcher at Tel Aviv University

Omree Wechsler

The COVID-19 pandemic and the need to communicate and work remotely have increased our dependence on computers and the internet, accelerating cyber risks, or what could be defined as the cyber pandemic. From its initial outbreak, through 2020 and well into 2021, many trends that were witnessed in 2020, such as the sharp increase in supply chain attacks and customized ransomware campaigns, as well as attacks on the healthcare sector, continue to wreak havoc on business and government agencies and are not likely to disappear.

1. The Ransomware Threat

While ransomware is not a new threat, threat actors are growing bolder and more sophisticated as their methodologies are evolving. One of the current main trends is the employment of additional extortion tactics such as leaking stolen information, publishing the incident to the media, notifying the victim's partners and customers of the incident etc. Another trend is the rise of the Ransomware-as-a-Service (RaaS) business model that allows ransomware developers to lease their tools and techniques to other criminals. thus giving them access to sophisticated tools and methods.

Several ransomware incidents made headlines since the beginning of 2021 and drew a prompt reaction from governments. These include the attack on the U.S. largest pipeline operator, Colonial Pipeline, which caused fuel supply disruptions in southeastern states, and the attack on the world's largest meatpacking company, JBS.

The damage caused, along with the headlines, have pushed governments, led by the Biden administration to seek solutions. Many of the solutions pursued focused on coordinating government-wide efforts and law enforcement operations aimed at disrupting and deterring cybercriminal groups operating from foreign countries as well as rendering the ransomware market unprofitable by seizing the ransom paid.

In the international arena, the U.S. has promoted the discussion on ransomware and the role of cryptocurrency in cyberattacks within NATO's and the G7 leaders' summits. According to the declaration of the G7 countries, countries that harbor ransomware groups will be held accountable for their lack of action. It may be the first signal of an international cooperation aimed at combating the phenomenon.

they need to understand that today they are facing state-sponsored levels (of cybercrime)."

2. Supply Chain Attacks

Attacks on supply chains that comprise a third party's software or services to access their customers' systems and networks sent shockwaves throughout the world with an unprecedented scale and sophistication.

BLIC

SVETSKA SAJBER SUPERILA Izrael se za deceniju popeo na sam svetski vrh: Glavni tehnološki grad im je usred pustinje, koji ima veze sa jednim mestom U SRBIJI (VIDEO)

Ni po ekonomskoj, ni po vojnoj moći, niti po energentima, ali ako je reč o industriji sajber bezbednosti, Izrael se svrstao na listu supersila i to rame uz rame sa najrazvijenijim i najbogatijim zemljama sveta.

I ne samo da se na toj listi nalazi, već se u sam njen vrh popeo za maltene jednu deceniju, a tamošnji "nou hau" (know how) postao je jedan od vodećih izvoznih "proizvoda". Da je tako, svedoče i podaci koji kažu da su ulaganja u sajber tehnologiju prošle godine bila gotovo tri milijarde dolara, što je bio rekordan iznos.

Međutim, 2021. godina tek obećava jer su investicije za samo šest meseci premašile prošlogodišnje (3,3 milijarde dolara), i potpuno je jasno da se na tome neće stati.

Sve ovo nije samo "izraelska stvar", jer su tamošnji proizvodi na polju sajber bezbednosti, starapovi koji se bave ovom oblašću (ima ih više 1.000) i stručnjaci koji se prave od maltene malih nogu, postali globalni igrači koji čuvaju svetske firme, infrastrukturu raznih zemalja, banke, finansijske insitucije, transport, zdravstvene sisteme, energetske sektore...

U prevodu, granice više ne postoje, njih ne poznaju ni oni koji su čuvani ni oni koji napadaju, a sve se dešava maltene iz fotelje, i to je nešto što danas gotovo svi prepoznaju kao potencijalnu opasnost za sopstvene poslove, kompanije, podatke, i uopšte svakodnevni život.

Sajber štit kao vakcina

Otuda ovih dana stiže i jedan globalni predlog, i to od izraelskog premijera Naftalija Beneta, koji je pozvao sve one koji razmišljaju na sličan način kao i Izraelci, koji ne samo da su svesni ovakvih pretnji, već ih i sa velikim uspehom sprečavaju i to veoma uspešno.

On je tokom "Sajber nedelje" koja je održana u Tel Avivu pozvao partnerske vlade da se pridruže mreži za otkrivanje, upozoravanja i reagovanja na sajber napade i to u realnom vremenu.

Pozvao je i na zajednički rad na razvoju rešenja koje je čak nazvao i "vakcinom", koja bi mogle da "prime" sve zemlje koje se odluče da postanu deo mreže.

- Ujedinjeni stojimo, razjedinjeni padamo - rekao je on, dodavši da sajber pretnje predstavljaju jednu od najvećih pretnji bezbednosti u Izraelu i svetu.

Da bi ovo, zapravo moglo da uspe, svedoči i podatak da Izrael danas ima saradnju u oblasti sajber bezbednosti sa čak 90 zemalja.

Svaka peta kompanija žrtva napada

A kako bi ona mogla da izgleda? Nešto poput izraelskog Nacionalnog sajber direktorata, koja je zadužen za nacionalnu sajber odbranu čitave zemlje, uključujući i privatni sektor, pojedince i privatna lica.

Koliko sajber napadi ne da nisu daleko od svakodnevnog života, već su njegov sastavni deo, posvedočio je i Igal Una, šef izraelske Nacionalne direkcije, koji objašnjava da pretnje stižu sa svih strana, i da su napadi ove vrste u porastu. Ilustracije radi, jedna od pet kompanija u Izraelu postala je tokom prošle godine žrtva ove vrste napada.

A te žrtve su sve, samo ne obične. Una je pojasnio da su čak polovina napadnutih bile kompanije visoke tehnologije, a više od 40 odsto radilo se o napadima na velika preduzeća. Imao je i primer: sajber napadi su u proseku izazivali zastoje u radu od oko 16 dana, kao i da je prosečna prosečna otkupnina plaćena u Americi zbog njih u proseku bila 178.000 dolara.

Drugi primer je još konkretniji: Tokom skorašnjih borbi u pojasu Gaze, Hamas koga Izraelci smatraju terorističkom grupom, pokušao je upravo sajber napade na Izrael.

- Uspeli smo da "skinemo glavu" njihovom sajber šefu i drugim sajber teroristima - rekao je on.

Mete su voda, struja, hrana...

Ratovi se danas, čini se, on onih svima na žalost dobro poznatih, premeštaju na jedan sasvim novi teren - virtuelni, ali sa štetama koje je ranije bilo teško zamisliti, a meta može biti sve: voda, struja, hrana, saobraćaj...

Kako se došlo do ovoga?

Primer bi mogao biti avion, kojim pilot ne upravlja samostalno, već to čini uz pomoć kompjutera, i dovoljan je samo jedan hakerski napad da bi se softver promenio, a posledice postale nesagledive.

- Shvatili smo da se takve stvari mogu desiti svakom sistemu koji koristi kompjuter, i odatle zapravo počinje priča o bezbednosti i sigurnosti - objašnjava profesor Isak Ben Izrael sa Univerziteta u Tel Avivu, koji je inače penzionisani general, bivšeg šef izraelske Službe za sajber bezbednost i zapravo čovek koji je, praktično, postavio na noge ono što Izrael danas radi na polju sajber bezbednosti.

Poziv Natanjahua

Pre gotovo 20 godina, zemlja postaje među prvima u svetu koja osniva nacionalnu službu protiv sajber napada, a ovaj profesor uključen je u to od samog početka. Priča i da ga je pre više od 10 godina bivši izraelski premijer Benjamin Natanjahu pozvao da, kako kaže, "napravi plan o novom dobu koje dolazi".

- Rekao sam da možemo da napravimo ljudski kapital za ono što dolazi, koji će biti spremni za novo vreme koje stiže. Predložio sam, između ostalog, da se u svim školama i univerzitetima pokrenu programi u vezi sa sajber tehnologijom - pojašnjava profesor.

Rezultat toga je danas i više nego jasan: start ap kompanije kojih je u Izraelu veliki broj, zajednički rad države, škola, univerziteta i vojske, veliki broj inžinjera koji se ovim poslovima bave, od bezbednosti do razvoja novih tehnologija u svim oblastima.

Sajber grad u pustinji

Dobar deo svega toga događa se ni manje ni više nego u izraelskoj pustinji Negev, tačnije u gradu Ber Ševa, koji je od jednog običnog gradića postao glavni sajber grad cele zemlje sa više od 2.000 inžinjera, u kome su smeštene ispostave najvećih svetskih IT kompanija, od "Dojče telekoma", preko IBM-a, do "Pej pala".

THE STRAITS TIMES

Beware the Trojan 'cyber horse'

The head of a Cyber Horse exhibit, constructed with used computer and mobile phone parts infected by viruses and malware, is displayed near the entrance to the Cyber Week conference at Tel Aviv University in Israel yesterday. Israel-based creative group No, No, No, No, No, Yes, who sculpted the Cyber Horse in reference to the Trojan horse in Greek mythology, had sought to make a statement about the hazardous effects of malware, with the horse symbolising a carrier of potentially "bad news" attempting to infiltrate cyberspace.

ISRAEL HAYOM
This is where we stand

PM calls for 'global defense shield' against cyber threats

According to the Israel National Cyber Directorate, one in five Israeli businesses and about 47% of Israeli high-tech firms suffered a cyberattack in 2020.

By Ariel Kahana , Guy Levy and JNS

Speaking at the annual Cyber Week conference at Tel Aviv University Bennet said, "We have already signed agreements with a dozen countries – instead of each country or company being alone the defense will be integrated. We invite good countries to join us in this initiative."

Israel decided an international effort was needed after reaching the conclusion that recent threats to cybersecurity were too great for any one country to handle alone, according to the report.

The prime minister also spoke of establishing a cyber center in Beersheba, saying, "For every $100 invested in cyber, $41 is invested in Israeli cyber."

Israel National Cyber Directorate Head Yigal Unna, who also spoke at the conference, presented statistics regarding cyberattacks during the past year, according to which one in five Israeli businesses suffered an online attack in 2020.

About 47% of Israeli high-tech companies were attacked last year as well. The high numbers are not unique to Israel and were spurred in part by the coronavirus pandemic that led to a jump in cybercrime, he said.

"Everything is under attack. Why is that? Because it's easy," said Bennett. "If you want to attack, the best, easiest and cheapest method is through a cyber attack. That is why it will increase as time goes on. I believe cyberattacks have become one of the significant threats to world peace."

THE JERUSALEM POST
JPOST.com

Bennett invites allies to form joint global cyber security network

Prime Minister Naftali Bennett said he views cyberattacks as one of the greatest threats not only to Israel's national security, but to that of the world

By LAHAV HARKOV

Israel is launching an international cybersecurity network for like-minded countries to fight threats together, Prime Minister Naftali Bennett announced at the Cyber Week conference at Tel Aviv University on Wednesday.

"Israel is opening up and announcing a Global Cybernet Shield," Bennett said. "If you try and fight alone, you're going to lose. If you fight together, you're going to win."

Israel already has dozens of memoranda of understanding with other countries on cybersecurity, the prime minister said, but the Global Cybernet Shield is meant to "bring it to the next level of online, real-time network defense."

cyberattackers, related equipment and infrastructure used by the terror group's cyber command.

The shield is still in development, and is meant to be an international version of Israel's "Cybernet" online-defense system.

"I invite all like-minded countries to join today. Call Yigal Unna," Bennett said, referring to the director of Israel's National Cyber Directorate (INCD).

Bennett, the former CEO of a cybersecurity company, gave a TED-style speech at Cyber Week titled "Israel's Cyber Defense –What's Coming Next." He walked across an empty stage with a visual presentation behind him, featuring slides that showed the components of Israel's cyber defense network, and a map of the world with arrows emanating from Iran to show who it has threatened with cyberattacks.

"Everything is under attack: our water, electricity, food, airplanes, cars. Everything is vulnerable," Bennett warned.

The prime minister pointed out that cyberattacks are much easier than traditional ones.

"If you're a bad country trying to harm or attack someone else, in the past you needed to send an airplane with commandos or a bomber, but today, the best ROI" – return on investment – "is a cyberattack. You just need brains, knowledge, experience and a good Internet line. That's as easy as it gets," Bennett said.

"Today, the biggest bang for your buck in trying to attack another country, industry or anyone is a cyberattack, and that's why it's going to happen more and more," he said.

Bennett said he views cyberattacks as one of the greatest threats not only to Israel's national security, but to that of the world.

The Global Cybernet Shield would use the "principles of connectivity" Israel uses for cyber defense internally, but on an international level, he explained.

THIS PRINCIPLE is put into practice in the way the private and public sectors work together to defend Israel from cyberattacks.

The INCD is tasked with defending the state's critical infrastructure from attack, but it also has a shared responsibility for the private sector.

Bennett compared a cybersecurity threat to a pickpocket on a bus; if one person loudly declares what the pickpocket is doing, others will know how to defend themselves.

Private companies are able to contact the directorate when they are under attack, which shares information across Israel.

"If one of those countries out there are attacking one of our companies, we want everyone else to know," Bennett said.

Aviram Atzaba, INCD executive director of strategy and international cooperation, explained that Israel developed its Cybernet system several years ago, in which over 1,500 organizations, including major Israeli companies, government ministries and more, share information about cyberattacks. Companies send warnings to the directorate, which anonymizes the messages and sends them to all the network's members.

"We can spread information without compromising the company that was attacked, and thus stop a pandemic in the cyber world," Atzaba explained.

In the newest edition of Cybernet, the INCD also sends the organizations information on how to defend themselves by patching their own systems.

The system's major advantage is its speed in warning organizations about attacks, Atzaba said.

The system has been very successful in Israel, he said, and foreign cybersecurity units have expressed interest in joining. Bennett himself suggested that the network be made international to allow like-minded states to cooperate in the cyber-defense effort.

In his address, Bennett also acknowledged that most Israeli innovation comes from the private sector, but said the government created an environment in which the industry can thrive. That includes the IDF giving young people major responsibilities, whether in cybersecurity and intelligence units, or, like Bennett himself, in combat units.

In addition, the prime minister commended the creation of a cybersecurity and technology hub in Beersheba, where IDF cyber experts, private tech developers and venture capital firm associates can easily meet, network and innovate.

"Innovation is something you can't command, force or direct," he said. "There is no law we could create that will say 'we want you to innovate twice a day' – it doesn't work that way. All we can do is allow it to happen, allow all these folks to get together, create this fusion and let them move."

şi resursele", a spus el, adăugând că este necesar ca multe naţiuni să se alăture acestei noi iniţiative, pentru că "dacă luptăm singuri, vom pierde, dar dacă luptăm împreună, vom câştiga".

Prim-ministrul israelian a mai spus că 41% din toţi banii investiţi în securitate cibernetică la nivel mondial au ajuns la firme din Israel. "Răspândirea ideilor, în loc să le concentrăm într-un singur loc, este unul dintre atuurile semnificative ale Israelului", a adăugat premierul israelian.

El a explicat că în Israel există o autoritate în domeniul apărării cibernetice care lucrează împreună cu firmele din sectorul privat pentru a proteja interesele ţării.

Bennett a prezentat mai multe exemple ipotetice privind modul în care naţiunile pot face o treabă mai bună în apărarea cibernetică dacă lucrează împreună. El a atras atenţia că multe atacuri pot fi lansate în acelaşi timp împotriva a diferite naţiuni şi a subliniat că, dacă acest lucru s-ar întâmpla, cooperarea internaţională ar fi esenţială.

Yigal Unna, directorul general al Directoratului Naţional pentru Securitate Cibernetică (INCD) al statului Israel, a afirmat la conferinţă că "una din cinci afaceri cade victimă atacurilor cibernetice şi jumătate din cele din industria high tech". De asemenea, a atras el atenţia, "una din 30 de afaceri raportează pierderi provocate de atacuri cibernetice".

"Mi-e teamă că 2021 arată chiar mai rău şi am suspiciuni că situaţia din Israel nu este diferită de cea din alte ţări", a mai afirmat şeful INCD.

În plus, a atras el atenţia, atacurile de tip ransomware au rezultat în plăţi care au crescut foarte mult, "în medie la aproape 200.000 de dolari". Şi mai important, potrivit lui Yigal Unna, este faptul că timpul în care instalaţiile atacate nu funcţionează a crescut, în medie, la 16 zile.

Cu acelaşi prilej, directorul general al INCD a anunţat înfiinţarea unei Unităţi proactive de apărare cibernetică, care este în prezent consolidată.

"Suntem bine poziţionaţi să depistăm viitoare trenduri în materie de vulnerabilitate şi luăm măsuri proactive", a mai spus Unna.

El a subliniat că Israelul este un jucător global în materie de securitate cibernetică şi că "am ajuns acum la peste 90 de ţări care cooperează cu noi şi am semnat 24 de memorandumuri de înţelegere, inclusiv cu ONG-uri precum Banca Mondială". Al 24-lea memorandum de înţelegere în domeniu a fost semnat chiar săptămâna trecută cu Marocul.

"În această săptămână am publicat Strategia internaţională de securitate cibernetică a Israelului în cadrul Cyber Week şi ne axăm pe întărirea cooperării pentru securitatea IT&C, construirea de capacităţi şi pregătirea pentru tehnologiile emergente", a mai spus Yigal Unna.AGERPRES/(A - autor: Florin Ştefan, editor: Mariana Ionescu, editor online: Adrian Dădârlat)

AGENŢIA NAŢIONALĂ DE PRESĂ AGERPRES Actualizează lumea.

Şeful INCD din Israel vrea să colaboreze îndeaproape cu centrul de competenţe în materie de securitate cibernetică al UE de la Bucureşti

Yigal Unna, director general al Directoratului Naţional pentru Securitate Cibernetică (INCD) al statului Israel, a declarat luni că speră ca în lunile următoare să vină la Bucureşti pentru a împărtăşi din experienţa sa cu conducerea noului centru de competenţe în materie de securitate cibernetică care urmează a fi lansat în România.

"Suntem foarte bucuroşi pentru că România a preluat iniţiativa. Există o bază puternică, fundamentală, pentru o bună securitate cibernetică în mod tradiţional în România, aşa că este o bună alegere a Uniunii Europene", a declarat Yigal Unna, directorul general al INCD, în cadrul unei întâlniri cu jurnaliştii străini, întrebat fiind despre posibila cooperare cu conducerea noului centru de competenţe în materie de securitate cibernetica, care a primit undă verde din partea UE.

"Lucrăm foarte îndeaproape cu prietenii noştri de acolo de ani de zile şi în mod specific asupra acestei chestiuni. Sper poate chiar că vom veni în lunile următoare la Bucureşti", a adăugat el.

Yigal Unna a spus că este posibil ca şi experţii români în domeniu să viziteze INCD pentru a învăţa din experienţa instituţiei, dar a glumit spunând că îi place Bucureştiul atât de mult că probabil va folosi orice scuză pentru a veni în capitala României.

Centrul european de competenţe industriale, tehnologice şi de cercetare în domeniul securităţii cibernetice de la Bucureşti a primit undă verde din partea Consiliului UE pe 20 aprilie, iar Parlamentul European şi-a dat votul pentru concretizarea iniţiativei o lună mai târziu, pe 20 mai.AGERPRES/(A - autor: Florin Ştefan, editor: Mariana Ionescu, editor online: Ada Vîlceanu)

CTECH

Israel PM Bennett calls for global 'defense shield' against cyber threats

"Today we invite all like-minded good countries across the world to join forces in the global cyber defense shield," said Bennett

"Everything is under attack, everything. Our water, electricity, food, airplanes, and cars. Everything is vulnerable and everything is under attack," said Israel Prime Minister Naftali Bennett, speaking on Wednesday at the Cyber Week conference held at Tel Aviv University. Bennett said Israel will establish a "global defense shield" with the aim of collaborating with governments globally against the dangers of cyberattacks.

"If you fight alone you will lose, but if you fight together you will win," said Bennett. "We've already signed MOUs, but now we're taking it to the next level to a real-time cyber shield. Today we invite all like-minded good countries across the world to join forces in the global cyber defense shield."

The Prime Minister said the new network will operate in a similar fashion to the Israel National Cyber Directorate, working with both the private sector and other government entities.

"I think we're the first country in the world to create one national cyber agency, a one-stop-shop whose responsibility is to defend all critical infrastructure in Israel," said Bennett. "That same agency is also responsible for the private sector. That's not to say we're in charge of their private decisions, but they have a phone to call where they can ask to investigate and share information and that's grown into a network.

"If you're a bad country and you're trying to harm or attack someone else you would need an airplane, commandos, a bomber, but today the best ROI is a cyber attack. You just need a brain, knowledge, experience, and an internet line," added Bennett. "Today the best bang for your buck is a cyber attack and it's just going to grow exponentially, and that makes me worried. As Prime Minister of Israel, I view this as one of the top threats to Israel's national security and the world's security."

Bennett said part of Israel's secret sauce is spreading ideas and not concentrating them in one place. He noted that of every $100 invested in cyber across the world, $41 were invested in Israeli cyber defense firms.

"The biggest thing we did to counter cyber threats was to allow the private industry to thrive and we need the prowess of the private industry because the brains are not only in government, to say the least," he said. "In Israel, we've got a lot of really smart people that at a young age enter the army and take on a massive amount of responsibility and that's why we're seeing the boom today. Cyber is something that you can't direct, all we can do is allow it to happen, to allow all these folks to get together and create this fusion."

The annual cyber week is led by the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, the Israel National Cyber Directorate, the Ministry of Economy, and the Ministry of Foreign Affairs.

AGERPRES
AGENȚIA NAȚIONALĂ DE PRESĂ
Actualizează lumea.

Naftali Bennett: Atacurile cibernetice, una dintre principalele ameninţări la adresa securităţii naţionale a Israeluluicibernetică al UE de la Bucureşti

Atacurile cibernetice reprezintă una dintre principalele ameninţări la adresa securităţii naţionale a Israelului şi la nivel global, a declarat miercuri premierul israelian Naftali Bennett, în a doua zi a conferinţei Cyber Week 2021 de la Tel Aviv.

El a explicat că în prezent toate industriile sunt vulnerabile la atacuri cibernetice, de la furnizarea apei, electricitate, alimentaţie, până la aviaţie şi sectorul auto.

"Totul este vulnerabil şi totul este atacat. De ce atât de multe lucruri din viaţa noastră sunt atacate astăzi? Pentru că este uşor. Nu a fost niciodată mai uşor", a spus şeful guvernului israelian.

"Dacă eşti o ţară cu intenţii rele şi în trecut aveai nevoie pentru un atac de un avion, de comandouri sau de un atentator cu bombă, acum poţi face asta doar cu un atac cibernetic. Ai nevoie de inteligenţă, cunoştinţe, experienţă şi un bun acces la internet. Azi cea mai bună cale de a ataca o altă ţară, o altă industrie este un atac cibernetic. Asta se va întâmpla din ce în ce mai mult. Va creşte exponenţial. Iar asta mă îngrijorează. Ca prim-ministru al Israelului văd asta ca una dintre principalele ameninţări la adresa securităţii naţionale şi cred că atacurile cibernetice din întreaga lume sunt una dintre principalele ameninţări globale", a mai spus Bennett.

El a continuat afirmând că cel mai important lucru pe care l-a făcut Israelul în această privinţă a fost să creeze o industrie şi să o lase să prospere.

"Nicio ţară singură, niciun guvern sau combinaţie de guverne nu poate să rezolve această problemă. Avem nevoie de ce este mai bun din industria privată. Şi trebuie să fie o combinaţie de mediu privat şi guvern pentru că oamenii foarte inteligenţi nu sunt numai în guvern, ca să nu spun mai mult", a declarat premierul israelian.

Potrivit lui Bennett, există un secret pentru care Israelul a reuşit să aibă rezultatele pe care le are în domeniul securităţii cibernetice.

"Ceea ce am făcut în Israel este că mulţi oameni foarte tineri, foarte inteligenţi au intrat în armată, în serviciile de informaţii militare, şi şi-au asumat responsabilităţi uriaşe, fiind, la 20-21 de ani, în unităţi de luptă şi unităţi de securitate cibernetică. Au ajuns apoi în societatea israeliană foarte tineri, cu capacităţi uriaşe. Şi de aceea vedem acest boom hitgh-tech. Am fost unul dintre aceşti tineri în urmă cu 20 de ani (...). Acesta este secretul Israelului, să aducem împreună atât de mulţi oameni inteligenţi", le-a povestit premierul israelian participanţilor la Cyber Week 2021.

Cu acelaşi prilej, Naftali Bennett a anunţat planuri privind o nouă iniţiativă în domeniul securităţii cibernetice la nivel internaţional. În discursul său de la universitatea din Tel Aviv, Bennett le-a cerut celorlalte state să se alăture Israelului în acest demers.

"Lucrăm la formarea unei agenţii globale de securitate cibernetică cu scopul de a ne uni şi de a ne combina forţele

enforcement community or in the intelligence community around the threat, maybe engaging with the private sector that has been a victim of a cyber incident."

And then there is his long-term work, he said, in which the agency tries to stay on top of efforts "to build a more secure federal cybersecurity system to make sure that our federal networks are protected."

Bolder, more sophisticated

Hackers have gotten bolder and more sophisticated, he said, and have the resources to wreak damage on the most critical functions of society. The threat landscape will become even tougher, and the global response must be unified and coordinated.

"Actors across the spectrum, whether nation-states or cyber criminals, have grown bolder in targeting more consequential targets," he said, including infrastructure targets like the Israeli water system last year, and US pipelines and the JBS meat processor this year.

"The sophistication of our adversaries has continued to grow as well," Wales said. "They're using more advanced tactics, ones that are better designed to evade detection.

"And so, we believe that the threat landscape will continue to evolve and that just puts more pressure on the network defense community to come together and to be as bold and be as resourceful as our adversaries."

Wales was adamant that business or other entities should not give in to ransomware attacks. The growth of these attacks, he said, "has been fueled by the success of the business model. People have continued to pay, and that has emboldened the ransomware operators, and every ransom that is paid is money that has fueled the epidemic."

On Wednesday Prime Minister Naftali Bennett said that Israel is setting up a "global network shield" based on a partnership with global governments to collaborate, detect and respond to cybersecurity attacks.

"We want to learn more about it," Wales said, referring to the initiative. CISA already has a close relationship with the Israel National Cyber Directorate, working on actual incidents, sharing information and tactics. Similar collaborations have also been set up between the US and other countries, he said.

And yes, he added, there are also connections with Russia and China, if information about malicious activity needs to be provided. "But the relationship is obviously different," he said "There's more ongoing and direct partnership with countries like Israel, like the United Kingdom and others, where we have kind of close and continuing contact."

Global collaboration to fight cybersecurity attacks is essential, he said, "but

there's no silver bullet, there's no one action that is going to be successful here."

Multiple layers of security and resilience must be put in place on individual networks, he said, and on a national and global level countries need to get better at sharing cyber defense information to help to stop future attacks.

Wales said what he is most concerned about in the longer term is potential disruption to critical infrastructure. The systems that enable society's "most critical functions, that enable our society to operate, are at risk," he warned.

And because malicious players want to target these critical infrastructures, "they will seek the means to do so. And it means that we need to work extra hard to prevent that from happening."

PRESSTV

NCSC head uses first major speech to praise Israel's cyber warfare capabilities

The chief executive officer of the UK's National Cyber Security Center (NCSC), Lindy Cameron, has used her first international speech to heap praise on Israel's cyber capabilities.

Addressing Tel Aviv University on Tuesday (July 20), Cameron, who was appointed head of the GCHQ-led NCSC in July 2020, described Israel as "a long standing, like-minded and highly capable partner" in the cyber warfare domain.

Speaking at the Cyber Week conference hosted by Israel's leading university, Cameron boasted that "we [British and Israelis] are absolutely committed to working together to protect our citizens and build confidence in a digital future".

Describing the UK-Israel cyber security relationship as "long-standing" and "enduring", Cameron revealed that "operational collaborations" between the two states is "strong and well developed".

"Israel is a cyber nation. You don't have to dive too deep into the Israeli cyber eco-system to find inspiration", Cameron told her captive audience.

Cameron's speech at Tel Aviv University is the strongest sign yet of what many have suspected for a long time; namely that the UK and Israel cooperate in the cyber warfare domain at the most sensitive operational levels.

It is also a sign that contrary to the consistent messaging of British leaders and officials, GCHQ and the wider British cyber security community are more focused on offensive cyber capabilities as opposed to cyber defense.

Cyber Week
July 19th-22nd, 2021
Tel Aviv University, Israel

Yuval Ne'eman Workshop for Science, Technology and Security Tel Aviv University
ICRC Blavatnik Interdisciplinary Cyber Research Center
TEL AVIV UNIVERSITY אוניברסיטת תל אביב
Cyber Israel National Cyber Directorate
In cooperation with: ISRAEL CYBER ALLIANCE
Ministry of Foreign Affairs Israel

THE TIMES OF ISRAEL

Hackers are as dogged as Romans besieging Masada — US cybersecurity exec

The West has to work harder in war against increasingly bold cybercrooks, says Brandon Wales, executive director at the DHS's Cybersecurity and Infrastructure Security Agency

By SHOSHANNA SOLOMON

The Western world has not been vanquished by cybercriminals, but it needs to do much more to keep the growing threat of cyberattacks in check or else it will face a cyber-Masada, the head of the leading US cybersecurity agency has warned.

"I don't think the Western world is losing the cybersecurity war," said Brandon Wales, executive director at the Cybersecurity and Infrastructure Security Agency (CISA) of the US Department of Homeland Security. "I think that we collectively recognize that we've got a lot more work to do."

"We have tremendous capabilities. We have a vibrant private sector cybersecurity community that is developed, in the United States in Israel and elsewhere. And we need to harness that, governments and private sector capabilities together, to achieve the positive cybersecurity outcomes that we all want," said Wales, speaking with The Times of Israel on Wednesday on the sidelines of the Cyber Week conference at Tel Aviv University.

In his Tuesday speech at the conference, Wales compared the perseverance of the cyberattackers to that of the Romans during their siege of the ostensibly impregnable mountaintop fortress of Masada in the first century CE. When the Romans finally breached the fortress, tradition says, they discovered that the 960 Jewish rebels and their families had committed mass suicide rather than surrender.

"These rebels had tremendous defensive advantages both in natural terrain and fortification," Wales said in his speech. "But a patient, well-resourced and determined adversary was able to overwhelm them. Their 12-year hold on Masada came to an end after a yearlong siege by the Roman Empire. Today, we face a variety of well resourced, determined adversaries. And like those Jewish rebels, operating alone, even our best defenses will simply not be good enough."

There are "thousands of attempts a day," he said. When they get thwarted, by governments or companies, they "don't necessarily get recognized the same way that the disruptions from ransomware and other cyber security incidents do." But the successful attacks "point us to the places where we need to do more work."

Cybersecurity threats are not bound by national borders, Wales said in the Tuesday speech, and "the cyber threat landscape is as dynamic and forbidding as we have ever seen it. Our adversaries are diverse, from hostile nation states such as Russia, China and Iran to cyber criminals. They are growing bolder. Their targets more consequential. Their techniques more sophisticated."

Over the past year the US has "witnessed cyber incident after cyber incident," with widespread attacks that tested CISA and the entire cybersecurity community, Wales said in his speech.

Cybercriminals and nation-states have used the coronavirus pandemic as an opportunity to deliver malicious software, steal data, disrupt operations, and target vaccine developers and supply chains, he said. "They exploited the digital transformation brought about by remote work and education, targeting this expanded and increasingly difficult to manage attack surface."

At the same time, Russia and Iran launched efforts to interfere in the 2020 US election, plus some US state and local election systems.

As the acting director of CISA, a post he held from November 2020 to July 12, Wales oversaw CISA's efforts to defend civilian networks, manage the risk to national critical functions, and work with partners to beef up the security cyber and physical infrastructure.

Wales has led the agency's response to a number of recent cybersecurity attacks: the SolarWinds Orion Supply Chain Attacks, in which US government networks were compromised by a hack blamed on Russia; the Microsoft Exchange vulnerabilities, a unusually aggressive Chinese cyber-espionage campaign; the Colonial Pipeline ransomware attack, which impacted the computerized equipment managing the US oil pipeline system; the Pulse Connect Secure vulnerabilities, which affected a number of US government agencies, critical infrastructure entities and other private sector organizations; and the Kaseya VSA supply chain ransomware attack, the single biggest global ransomware attack on record, conducted by a Russia-linked gang.

The perpetuators of the cybersecurity attacks must be held accountable, Wales said during the interview, and the Biden administration is determined that that will happen.

"The Biden administration has been very clear from the beginning that malicious cyber actors need to be held accountable," Wales said. "And that accountability is critical to deterring and dissuading them from conducting attacks in the future."

The private sector must be enabled "to spot, detect and stop" any malicious activity. At the same time, it has "obligations" to protect and secure its networks, he added.

Wales is responsible for leading and developing long-term strategy at CISA, ensuring national and international collaborations and managing policy initiatives. He is also on hand when significant cybersecurity breaches occur.

"There is no such thing as a typical day," he said. His agenda is shaped by what is happening on the ground. "If there's significant cyber activity happening, we may be engaging with critical US government partners in the law

THE TIMES OF ISRAEL

Bennett: Israel to set up 'global network shield' against growing cyberthreat

PM calls on 'like-minded' nations to join network to detect, alert and respond to attacks in real time; Israel cybersecurity chief warns: 'Cyber winter is here'

By SHOSHANNA SOLOMON

Prime Minister Naftali Bennett said Wednesday that Israel was setting up a "global network shield" within which partner-governments globally will collaborate in real time to identify cybersecurity attacks, raise the alert and work together to develop solutions.

It will be an "online, real-time global network defense," Bennett said at the Cyber Week conference in Tel Aviv. "We invite all like-minded good countries to join forces."

In the face of cyberthreats, the partnership will "alert, investigate, together develop a 'vaccine' and disperse the 'vaccine' to all countries in the network. United we stand, divided we fall," he said.

The new network will operate similarly to the Israel National Cyber Directorate, which is in charge of national cyber defense. It works with the private sector and other government entities to help defend the nation from the growing threat of cyberattacks.

Cyberthreats constitute one of the top threats to security in Israel and the world. Terrorists and other bad actors realize that their best return on investment is via a cyberattack, Bennett said.

The head of the Israel National Cyber Directorate, Yigal Unna, who last year warned that "cyber winter is coming," said at the conference on Wednesday: "Cyber winter is here."

"Threats are coming from all actors," he said, and cyberattacks are on the rise. "How cold this winter is going to be is something to be discovered, but yes, we are there," he said.

One out of five businesses in Israel fell victim to cyberattacks in 2020, Unna said. Half of them were high-tech companies and almost 42% were large businesses. One in 30 businesses reported losses from cyberattacks in 2020, and "2021 looks even worse," he said.

Ransomware attacks caused an average downtime of some 16 days, he said, and the average ransom paid in the US was $178,254.

Cooperation among nations is key to fight these attacks, he said, and the response needs to be fast, smart and stronger.

Unna said that during the recent round of fighting with Gaza, the Hamas terror group attempted cyberattacks against Israel. "We managed to behead their cyber chief and other cyber terrorists," Unna said, in a "clear message" that Israel will not tolerate such attacks.

Israel today has cybersecurity cooperation with 90 countries, he said.

In the first half of the year, Israeli cybersecurity companies raised $3.4 billion in 50 deals and seven of them became unicorns, or private companies valued at over $1 billion, the National Cyber Directorate said earlier this month.

The money raised in the first six months of this year exceeds the sum raised by Israeli cybersecurity startups in the whole of last year, itself a record-breaking $2.9 billion, the directorate said. The half-year figure accounts for 41% of the total funds raised by cybersecurity firms worldwide, and is three times the amount raised in the same period a year earlier, the data shows.

The Washington Post

Israeli defense minister in France with Pegasus spyware on the agenda

PARIS — Israeli Defense Minister Benny Gantz met with his French counterpart on Wednesday as Israel ramped up its investigation of a spyware firm accused of facilitating surveillance against human rights activists, dissidents, as well as world leaders, including France's Emmanuel Macron.

"Israel is investigating the matter with the utmost seriousness," Gantz said in the meeting, according to a statement released Wednesday by Israel's Defense Ministry. He said "representatives" of several Israeli security branches had visited the Herzliya office of NSO Group that morning to advance the investigation into the allegations against the Israeli surveillance giant.

Gantz added that "Israel gives cyber licenses exclusively to countries, and exclusively for dealing with terrorism and crime," according to the statement.

The Washington Post and other news organizations reported last week that phone numbers for Macron and other world leaders, as well as for activists and journalists, were found on a list that included some people targeted by government clients of NSO Group and its Pegasus spyware tool.

None of the world leaders' devices were forensically examined by The Post or its reporting partners, but tests of other phones on the list turned up evidence of attempted or successful spyware intrusions.

On the list: Ten prime ministers, three presidents and a king

NSO Group has said the inclusion of numbers on the list does not prove the phones were selected for surveillance. But in France and other countries, the revelations have prompted uncomfortable questions for the company, its presumed clients and Israeli diplomats. The numbers of several French ministers also were on the list.

Ahead of the Israeli-French meeting, French government spokesman Gabriel Attal said Wednesday afternoon that Defense Minister Florence Parly would use the talks to "question her counterpart about the knowledge the Israeli government had of the activities of NSO's clients."

Attal said the French minister would also inquire about what measures have been put in place, or will be in place in the future, "to prevent a misuse of these tools that are highly intrusive."

The Élysée presidential palace has emphasized that further investigation into the Pegasus allegations is needed. But in a sign that French officials are taking the reports seriously, Macron called an emergency cybersecurity meeting to discuss the revelations last Thursday, and the government has ordered several investigations.

Attal cautioned that those inquiries are ongoing, but he suggested Wednesday that the government may take additional measures if the accusations are confirmed.

In a statement Tuesday, Israel's Defense Ministry said Gantz would "update [Parly] on the topic of NSO" during his visit. The ministry added that they would also discuss "the crisis in Lebanon and the developing agreement with Iran."

The Israeli statement said "the trip was planned approximately one month ago, regardless of the NSO issue."

The recent revelations have significantly raised the diplomatic stakes of the visit, amid heightened public scrutiny of Israel's role. "Victims of Pegasus spyware should not only point the finger at the countries that targeted them," France's Le Monde newspaper wrote in an editorial Tuesday. "Their complaints should also be addressed to Israeli authorities, who validated the contracts concluded by the NSO Group."

Israel has set up a task force of senior officials to examine the spyware allegations, Reuters reported last week, citing two Israeli sources.

Gantz said last week at a cyber conference at Tel Aviv University that Israel authorizes the "export of cyber-products solely to governments, only for lawful use and exclusively for the purposes of preventing and investigating crime and terrorism." He added that countries acquiring the systems "must abide by their commitments" to those requirements.

The recent revelations have also prompted unease among French journalists and activists. Reporters Without Borders said in a statement last week that the group, along with two journalists holding joint French and Moroccan nationality, has filed a complaint with French prosecutors alleging invasion of privacy and other crimes based on the Pegasus allegations.

Forensic analysis also showed that phones belonging to staffers with the investigative French news site Mediapart were infected with Pegasus software. Mediapart has complained to the Paris prosecutor's office, accusing Morocco of being behind the surveillance.

Moroccan officials have denied the accusations. In a statement, the Moroccan government also expressed "great astonishment" at the publication of "erroneous allegations … that Morocco has infiltrated the telephones of several national and foreign public figures and officials of international organizations."

Rubin reported from Tel Aviv. Michael Birnbaum in Riga, Latvia, and Drew Harwell in Washington contributed to this report.

HELPNETSECURITY

World Health Organization CISO suggests a holistic approach to cybersecurity

Flavio Aggio, CISO at the World Health Organization, has had a challenging year. Since the onset of the COVID-19 pandemic, the WHO has become a significant target for cybercriminals, and cyber attacks against the organization have skyrocketed.

He recently spoke at Cyber Week 2021 in Tel Aviv, and in this interview with Help Net Security, Aggio talks about the modern threat landscape and offers tips for organizations that want to increase their security posture.

Prior to joining WHO, you were the CTO of the City and County of San Francisco. How did your previous work experiences help you in your current CISO role?

Prior to joining the World Health Organization, I was the CTO at the City and County of San Francisco, where I developed technology solutions to modernize and protect the city. Before that, I held technical leadership positions in Enterprise Architecture, Project Management, Telecommunications, and IT operations with Unisys, ASML, Dow Chemical, and Rohm & Haas.

These experiences confirmed cybersecurity is an ever evolving, changing, and challenging field, and they helped me to understand how people, process, and technology are the key factors in digital transformations and risk management. Cybersecurity must be part of every solution from development to operations.

Since the start of the COVID-19 pandemic, the WHO has become a big target for cybercriminals. How has your team adapted to a significant increase in cyber attacks? Are related organizations looking at you for guidance?

Since the start of the COVID-19 pandemic, WHO has seen a dramatic increase in the number and complexity of cyberattacks directed at its staff, and email scams targeting the public at large. My team has worked with the private sector to establish more robust cybersecurity systems and to strengthen security measures and to educate staff on cybersecurity risks.

Cybersecurity collaboration with related organizations increased dramatically due to the increase in the number and complexity of cyberattacks. There is a lot of guidance exchanged by helping organizations to be more prepared.

One example of guidance received by WHO is the implementation of DMARC (Domain-based Message Authentication, Reporting and Conformance) to reduce the number of email impersonations. After the implementation of DMARC, my team is giving the same DMARC guidance to other organizations. Another example of guidance given by my team is the monthly phishing exercise method adopted at WHO.

Pandemic-related phishing attacks and disinformation campaigns continue to create trouble. What advice would you give to organizations considering security awareness programs, but are unsure about what they need?

Phishing attacks have been widely used by cybercriminals as basic doors to organizations. Attackers can easily manipulate people into clicking links or open files. By having a cybersecurity awareness campaign with constant phishing exercises, any organization can prepare themselves to deal with this type of attack as any preventive technology can be bypassed eventually. Having email phishing prevention technology is a must, but it is not sufficient to stop phishing attacks. A cybersecurity awareness campaign is essential.

When you look at the threat landscape in general, what are you most worried about? How do you expect current threats to evolve? What will, most likely, be a massive problem a few years down the line? How can CISOs prepare for the unknown?

I am most worried about organizations only relying on technology to be cyber safe. Cybercriminals will always find ways to trick people to bypass technologies and processes implemented by organizations. It is essential for organizations to adopt a holistic approach by including people, process, and technology in their cybersecurity programs.

By relying only on technology and digital transformation efforts, organizations will not understand cyber risks well, and may be impacted by AI, supply chain, and other types of cyberattacks.

CISOs must initiate the zero-trust principles in their organizations, so any solutions must always be able to never trust any user or device until they are properly authenticated. Identity is the new perimeter.

Security leaders must make multi-factor authentication mandatory and have additional identity verification measures to ensure only approved devices can access the organization systems.

THE JPOST.com JERUSALEM POST

Cyber Week: How Israel became a leader in cyber tech and investment

Israel has become one of the world leaders in cyber security. But how did we get there?

By SETH J. FRANTZMAN

Israel has become one of the world leaders in cybersecurity. One of those who played a key role in Israel's pioneering role in this field, which is now emerging as one of the most important aspects of our global economy and security, is Prof. Isaac Ben-Israel.

"I was in effect the one in 2010-11 that was asked by the previous prime minister Benjamin Netanyahu how to make Israel one of top five countries in cybersecurity and my report was approved and turned into a government resolution in 2011," he says. "That was ten years ago and now you can see the results around you, the approach of the report was interdisciplinary, our recommendations were not limited to technology, but also the other aspects of our lives."

Ben-Israel, the director of the Interdisciplinary Cyber Research Center at Tel Aviv University, is an expert in mathematics, physics and philosophy; he earned his PhD in 1988. The center at TAU has some 300 members and is interdisciplinary, meaning it takes into account not just computers and what we may think of as "cyber" but also other fields such as experts from social sciences. Ben-Israel envisioned it this way

It will be one of the focuses of Cyber Week, the annual summit meeting of the heads of global and local cyber industry. Led by the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University along with the Israel National Cyber Directorate, the Ministry of Economy and the Ministry of Foreign Affairs, the event will be held on July 19-22, at Tel Aviv University this year. Past events have seen thousands of attendees from dozens of countries and over 50 roundtables and workshops.

This year's conference will be attended by Prime Minister Naftali Bennett, Defense Minister Benny Gantz and Minister of Public Security, Omer Bar Lev along with dozens of other senior officials from Israel and abroad. Organizers say it is "a meeting point for prominent cyber experts and researchers from Israel and around the world. Senior diplomats and businessmen bring the latest issues and trends in the field and in relation to the period, along with the most updated developments and information."

Cyber isn't just about cyber defense or cyberattacks, which is how we often hear about this buzzword in the news. It is also about diplomacy and crisis management and the new laws that govern cyber issues around the world. This can include cyber defenses, artificial intelligence, medicine and cloud storage. Organizers say that the first marine cyber conference in Israel is to be held at the Ashdod port in participation with senior officials from around the world.

BEN-ISRAEL served in the IDF until retiring in 2002. During his service, he held posts in operations, intelligence and weapon development units and research and development in the IDF, according to Tel Aviv University. He also serves as Chairman of the Israeli Space Agency.

He looks back on those important years as Israel sought to establish itself as a cyber power. "One recommendation was to create in every university a cyber research center. In those days there was no research on cybersecurity because it was sensitive and secret and used by intelligence services. In Israel, as you know, we have research and teach cybersecurity now in high schools, which was one of our recommendations; that is about building human capital and also starting with start-ups and [business] unicorns and then government regulations and budgets."

It's difficult to measure cyber power, he says. "You can measure jobs, patents, publications, or how many capabilities were demonstrated." Recently the International Institute for Security Studies published an index of leading cyber countries and found that while the US was the cyber superpower, Israel is in the second tier of leaders along with China, Russia, the UK and others.

Ben-Israel says that in the last year, Israel's cyber exports have exceeded $7 billion, which is more than defense exports. "If you look at the whole business sector globally, and you look at [the] whole sum and how much investment from [the] business sector goes to Israel, in 2018 it was 18% and 2019 it was 26% and in 2020 to 31% and the first half of 2021 it is 45% putting Israel first on the list, more invested in Israel than the US. In absolute numbers, Israeli exports are almost 10% of the global market," he says. This is massive.

Today we hear a lot about cyber attacks. Ben-Israel notes that in recent years ransomware attacks have become common. This means "someone locks the information in your computer and if you don't give money they won't give the key to open the lock. The number in [the] last year or two increased by a huge factor." As companies during COVID-19 rely more on computer communication, this also put wind in the sails of the ransomware attackers because they can be at the jugular of international trade. There are other factors as well, such as governments that support these attacks or criminal and terror groups.

COUNTRIES HAVE suffered increased cyber threats as well. This is because so many systems are run by computers, you can hack in and turn off machines that run water systems or electric power. In addition, cyber attacks like the one that harmed Iran's centrifuges in the period around 2010, caused them to spin out of control and be destroyed. Recently Iran's train system reportedly suffered a cyber attack.

Ben-Israel notes that back in the day he used to wear a uniform. He says in the 1990s when Ehud Barak was prime minister, he drafted a letter explaining the concerns relating to cyber. "As long as no one understands what cyber can do, we have an advantage. I was in charge of MAFAT, the Research and Development Directorate at the time, and as long as no one understands it [cyber], one day everyone will understand the potential, and then because we are more developed and because everything is controlled by computers, then the advantage will turn to a disadvantage," he says. Israel began in 2002 to protect its key infrastructure from cyber attacks. "We had a government agency with [the] mission of protecting critical infrastructure." He says Israel has suffered threats and attempted attacks over the years but none succeeded.

The next step for Israel is integrating the technologies we call artificial intelligence, he says. Israel is a leader in AI and this will result in machines that can replace humans in some tasks. "Dependence on computers will be much greater, instead of a person doing it, a computer will do it, and we will become more vulnerable," he says. "Second there are certain things that you can do in cybersecurity that you couldn't do before, AI is based on machine learning, and so from these aspects, the next step the whole world will go strongly toward developing and applying and using AI technology and therefore the effort that should be put in from the design stage in cybersecurity will grow enormously," he notes.

Israel lacked a government over the last several years and budgets were not devoted to the goal of making Israel a leader in AI. Nevertheless, he has hopes that budgets will be allocated now to teaching about artificial intelligence in schools and educating the next generation.

"Only if you take the whole ecosystem, then you can come out with something that enables you to compete," he says, remarking on the need to create the ecosystem to develop AI.

ComputerWeekly

NCSC's Cameron urges deeper cyber alliance-building

Speaking to an event in Israel, NCSC CEO Lindy Cameron has praised joint UK-Israeli efforts on security collaboration

National Cyber Security Centre (NCSC) CEO Lindy Cameron has again talked up the importance of international alliance-building in the fight against cyber threats, in a speech delivered to an audience at Tel Aviv University in Israel.

Addressing the university's annual Cyber Week, Cameron said the UK was "absolutely committed" to working with Israeli organisations to protect citizens and build confidence in digital technology.

She described Israel as a long-standing, like-minded and highly capable partner to the UK as she focused on the strength of the two countries' relationship in tackling shared threats, both from cyber criminals and state-backed actors. Security, she said, is a "global team sport" in which continued cooperation carries mutual benefits.

"Covid has been a shared challenge across the world – and like coronavirus, cyber security does not recognise geographic borders," said Cameron. "Nations face shared threats from cyber criminals and state actors who seek to do our nations harm. And we can learn so much from one another.

"Operational collaboration between our agencies – and many other agencies represented at this conference – is strong and well-developed. It focuses on exchanges of threat reporting and analysis of trends, something I am pleased to say continued successfully throughout lockdown.

"The UK and its allies share a belief that a nation's cyber security cannot simply be done by one government organisation. Everybody has their part to play – public sector, private sector and citizens. And the NCSC and INCD [Israeli National Cyber Directorate] here in Israel both see partnering with the private sector as an explicit priority and have pioneered taking this to a different level."

Cameron added: "Israel is a cyber nation. You don't have to dive too deep into the Israeli cyber ecosystem to find inspiration. So much of what any country achieves in cyber security depends on its work with international allies – because the stronger any one of us is, the stronger we all will become."

Israel has a wealth of cyber expertise and has spawned multiple globally renowned security companies that contribute over $6bn a year to the country's economy. Many of them were founded by veterans of the Israeli Defence Forces' (IDF's) signals intelligence brigade, Unit 8200, which serves as a proving ground for advanced security technology.

Cameron highlighted a recent successful project that saw the Software Security Knowledge Area of the UK's Cyber Body of Knowledge, or CyBOK translated into Hebrew at the request of the INCD. She said: "The CyBOK is an NCSC-sponsored guide distilling the knowledge of the world's leading cyber security experts. It's not a short read, but through this sharing of expertise, we all grow stronger together."

She also touched on the global challenge posed by the current epidemic of ransomware attacks, describing it as the most disruptive threat facing defenders as incidents grow larger and more complex – the recent attack on the systems of Kaseya being a timely example.

The day after the UK and US joined forces to condemn an alleged China-backed campaign of cyber attacks, Cameron also warned against the illegal and irresponsible use of offensive cyber capabilities by nation states, and noted in particular that some states that cannot build high-end capability themselves are now able to buy it.

"We believe the cyber security threats we face are shared globally," she said. "So it is vital that all cyber actors use capabilities in a way that is legal, responsible and proportionate to ensure cyber space remains a safe and prosperous place for everyone. And we will work with allies to achieve this."

Vanunu: Nein, es gibt sehr viele Probleme in diesem Bereich, zum Beispiel One-Day-Exploits. Also Schwachstellen, die bereits bekannt sind, aber noch nicht geschlossen wurden. Das wirklich große Problem ist aber, dass heute alles digital ist. Und wie ich schon gesagt habe, gibt es dabei zwei Hauptvektoren: einerseits Kryptowährungen, die wie Benzin für Cyberkriminalität sind. Und andererseits den Wechsel zu Ende-zu-Ende-Verschlüsselung. Das verändert das gesamte Konzept, wie Angriffe ablaufen. Denn wenn man den Client (das Endgerät, Anm.) angreifen muss, wird er viel aggressiver. Während alles verbunden ist, glaube ich zudem nicht, dass Unternehmen Sicherheit ernst genug nehmen. Abwehr heißt heute aber sowohl die Abwehr von staatlich gesponserten Akteuren als auch von hochentwickelten Cyberkriminellen. Man braucht also erfahrenes Personal und Budget.
STANDARD: Was ist mit kleineren Firmen? Nicht alle können sich ein ausgeklügeltes System und das richtige Personal leisten.
Vanunu: Dem stimme ich nicht zu. Kleine Unternehmen geben vielleicht mehr Geld für Dinge aus, die weniger relevant sind als der Schutz ihrer Daten. Ein Angriff kann dein Geschäft auslöschen. Die oberste Priorität sollte der Chief Technical Officer (CTO) und die Abwehr von Cyberangriffen sein. Darauf kann man eine Firma aufbauen, weil die Firma selbst auf Daten und geistigem Eigentum aufbaut.
STANDARD: Inwiefern unterscheiden sich Spyware und Ransomware?
Vanunu: Die Methoden und Techniken sind sehr unterschiedlich. Bei Ransomware kommen üblicherweise zwei Techniken zum Einsatz. Eine davon ist Spearfishing, man verschickt also Millionen E-Mails, und eine davon ist erfolgreich und infiltriert die Organisation. Die zweite Möglichkeit ist, die Firma tatsächlich zu hacken. Dafür wird eine Schwachstelle genutzt. Üblicherweise geht es dabei nicht um Zero-Days, sondern nicht geschlossene One-Days. Firmen werden also penetriert, die Daten gestohlen und anschließend verschlüsselt. Spyware ist in der Regel von Staaten gesponsert und sehr teuer. Meistens geht es dabei um Zero-Clicks, das heißt, es werden Sicherheitslücken ausgenutzt, ohne dass das Angriffsziel es bemerkt. Dafür werden üblicherweise Zero-Day-Lücken genutzt.
STANDARD: Gibt es wirklich eine Möglichkeit, sich vor Spyware-Angriffen zu schützen?
Vanunu: Es gibt die Möglichkeit, die Gefahren zu minimieren. Das Wichtigste ist, das Betriebssystem immer auf den neuesten Stand zu bringen, weil es ständig neue Sicherheitsfixes gibt. Hackergruppen vergleichen immer Updates mit der letzten Software-Version. Dadurch sehen sie, was gepatcht wurde, und bauen darauf basierend ihre Angriffstools. Außerdem gibt es heutzutage mobile Applikationen, die auffällige Aktivitäten auf dem Smartphone erkennen können. Also eine Art Antivirusprogramm. Die Installation eines Zero-Days kann man dadurch nicht erkennen, sobald er aber aktiv wird, gibt es die Möglichkeit. Die Gefahren kann man also minimieren, es ist aber sehr schwer, sich vor staatlich gesponserten Zero-Days zu verteidigen.
STANDARD: Schon jetzt wird von einer Ransomware-Pandemie gesprochen. Worauf muss man sich in den kommenden Jahren einstellen?
Vanunu: Meiner Meinung nach werden Cyberkriminelle weiterhin stark auf kritische Infrastruktur abzielen. Diese Firmen zahlen gutes Geld, um sich zu befreien und ihren Ruf zu retten. Außerdem wird der Ransomware-Bereich weiter wachsen. Während früher nur ein paar tausend Dollar gefordert wurden, sind es inzwischen mehrere Millionen. Außerdem werden staatliche Hackeraktivitäten weiterhin eskalieren. Wir werden Regierungen sehen, die sich gegenseitig angreifen. Ein vierter Vektor sind Deep Fakes, die dem Cyberkrieg eine weitere Dimension hinzufügen. Mit Software kann man somit zum Beispiel mein Gesicht und meine Stimme auf einen anderen Körper setzen. Das ist ein Trend, den wir vor allem im Bereich der Fake-News wiedersehen werden. Und wir brauchen Lösungen, um das zu erkennen. Doch das wird schwierig sein. (Mickey Manakas aus Tel Aviv, 22.7.2021)

CTECH

Israel PM Bennett calls for global 'defense shield' against cyber threats

"Today we invite all like-minded good countries across the world to join forces in the global cyber defense shield," said Bennett

"Everything is under attack, everything. Our water, electricity, food, airplanes, and cars. Everything is vulnerable and everything is under attack," said Israel Prime Minister Naftali Bennett, speaking on Wednesday at the Cyber Week conference held at Tel Aviv University. Bennett said Israel will establish a "global defense shield" with the aim of collaborating with governments globally against the dangers of cyberattacks.

"If you fight alone you will lose, but if you fight together you will win," said Bennett. "We've already signed MOUs, but now we're taking it to the next level to a real-time cyber shield. Today we invite all like-minded good countries across the world to join forces in the global cyber defense shield."

The Prime Minister said the new network will operate in a similar fashion to the Israel National Cyber Directorate, working with both the private sector and other government entities.

"I think we're the first country in the world to create one national cyber agency, a one-stop-shop whose responsibility is to defend all critical infrastructure in Israel," said Bennett. "That same agency is also responsible for the private sector. That's not to say we're in charge of their private decisions, but they have a phone to call where they can ask to investigate and share information and that's grown into a network.

"If you're a bad country and you're trying to harm or attack someone else you would need an airplane, commandos, a bomber, but today the best ROI is a cyber attack. You just need a brain, knowledge, experience, and an internet line," added Bennett. "Today the best bang for your buck is a cyber attack and it's just going to grow exponentially, and that makes me worried. As Prime Minister of Israel, I view this as one of the top threats to Israel's national security and the world's security."

Bennett said part of Israel's secret sauce is spreading ideas and not concentrating them in one place. He noted that of every $100 invested in cyber across the world, $41 were invested in Israeli cyber defense firms.

"The biggest thing we did to counter cyber threats was to allow the private industry to thrive and we need the prowess of the private industry because the brains are not only in government, to say the least," he said. "In Israel, we've got a lot of really smart people that at a young age enter the army and take on a massive amount of responsibility and that's why we're seeing the boom today. Cyber is something that you can't direct, all we can do is allow it to happen, to allow all these folks to get together and create this fusion."

The annual cyber week is led by the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University, the Israel National Cyber Directorate, the Ministry of Economy, and the Ministry of Foreign Affairs.

DERSTANDARD

“Jedes Land hat Cyberstreitkräfte”: Warum Pegasus nur ein Teil des Problems ist

Der israelische Cybersecurity-Experte Oded Vanunu erklärt im Interview mit dem STANDARD, warum Pegasus nur ein Teil des Problems ist. Staatliche Angriffe dieser Art werden künftig weiter zunehmen

Die Enthüllungen rund um Pegasus, also die Spyware der israelischen NSO Group, halten die Welt noch immer auf Trab. Ein internationales Journalistenkonsortium konnte aufdecken, dass sie für die Überwachung tausender Menschen, darunter zahlreiche Politiker, Menschenrechtsaktivisten und Journalisten, genutzt wurde. Auch ein österreichischer Unternehmer war betroffen. Der Fall wirft zahlreiche Fragen auf, immerhin gelangte die Software trotz Exportkontrollen des israelischen Verteidigungsministeriums in die Hände autoritärer Staaten. Zudem geriet das Unternehmen wegen ähnlicher Vorfälle schon mehrfach in die Schlagzeilen.

Trotz allem scheint es sich bei den Geschäften der NSO Group nur um einen kleinen Baustein im – inzwischen – sehr ertragreichen Ökosystem der Cyberattacken zu handeln. Während private Akteure realisiert haben, dass mit Ransomware große Geldsummen verdient werden können, haben auch Regierungen ihre Verteidigungs- und vor allem Angriffskapazitäten ausgebaut.

Über die aktuellen Entwicklungen hat DER STANDARD mit Oded Vanunu, Head of Vulnerability Research bei Check Point, gesprochen. Mit 18 Jahren Erfahrung bei einem der größten und wahrscheinlich dem bekanntesten israelischen Anbieter von Cybersicherheitslösungen ist er tagtäglich auf der Suche nach Schwachstellen in reichweitenstarken Plattformen, in den letzten zwei Jahren entdeckte sein Team schwerwiegende Schwachstellen bei Konzernen wie Facebook, Whatsapp, Telegram, Tiktok, aber auch bei Apple und Amazons Alexa.

STANDARD: In den letzten Monaten gab es mehrere schwerwiegende Ransomware-Angriffe, zum Beispiel auf Solar Winds, Colonial Pipelines und den US-Fleischproduzenten JBS. Nun wurde publik, dass eine Spyware namens Pegasus genutzt wurde, um Journalisten, Politiker und Aktivisten abzuhören. Was ist der Grund für die steigenden Zahlen?

Vanunu: Ich sage schon seit mehreren Jahren, dass eine sehr aggressive Cyber-Ära beginnt und dass wir deshalb verstehen müssen, wie das Cyber-Ökosystem funktioniert. Dafür müssen wir wissen, was hinter dem Vorhang passiert. Also warum dieses Ökosystem genau so handelt, wie es derzeit handelt – und was die Kräfte sind, die es bewegen. Dafür müssen wir das konventionelle Wettrüsten betrachten. Vor rund zehn Jahren gab es nämlich weltweit Regierungsentscheidungen, Budgets von konventionellen Waffen zu Cyberwaffen zu verschieben. Sie haben also Cyberstreitkräfte geschaffen. Am Ende des Tages muss nämlich jede Regierung andere Staaten infiltrieren, um an Informationen und Daten zu gelangen. Das Problem dabei ist, dass damit Staaten wie China, Russland, USA und Israel begonnen haben. Dadurch wurde dieses Aufrüsten zu einem Standard, und in den letzten zehn Jahren wurde eine Privatwirtschaft erschaffen, die Cyberwaffen liefert.

STANDARD: Wie hat sich die Art des Angriffs über die Jahre hinweg verändert?

Vanunu: Es gab eine Evolution. Die Angriffsmethoden haben sich entwickelt, da immer ausgeklügeltere Waffen gebraucht werden, um Nutzer angreifen können. Außerdem hat sich die Angriffsfläche bewegt. Während früher zentralisierte Verschlüsselung zum Einsatz kam, ist heute alles Ende-zu-Ende-verschlüsselt. Das heißt, das Rüstungsrennen konzentriert sich inzwischen auf das Endgerät (zum Beispiel das Smartphone, Anm.). Will man heutzutage noch an Daten gelangen, muss man den Client angreifen, man muss also Betriebssysteme von Apple, Google und Microsoft infiltrieren. Aber auch Applikationen, weil sie das Tor für die zu stehlenden Daten sind. Die Angriffe werden also immer ausgeklügelter. Und dabei beziehe ich mich ausschließlich auf Regierungen.

STANDARD: Wie sieht es mit privaten Akteuren aus?

Vanunu: Cyberkriminelle Organisationen sind heutzutage aufgebaut wie Unternehmen. Sie haben einen CEO, einen CTO, einen Operations-Manager, einen CFO – denn wegen des Aufstiegs der Kryptowährungen haben sie die Möglichkeit, Geld zu verdienen. Seit den Angriffen auf die US-Wahlen 2016 haben wir außerdem gesehen, wie weit Angreifer gehen. Fälle wie Solar Winds und Colonial Pipelines sind Beispiele für Hackergruppen und Regierungen, die keine rote Linie kennen. Dadurch ist es das erste Mal vorgekommen, dass eine Regierung mit einem aktiven Gegenangriff reagiert hat, um einen Angreifer offline zu nehmen.

STANDARD: Bei den oben genannten Beispielen handelt es sich um Ransomware-Angriffe. Was ist der Unterschied zu Spyware wie Pegasus?

Vanunu: Es ist genau so, wie ich es seit Jahren sage: Regierungen bauen Unternehmen auf, die ihre Bedürfnisse stillen. Firmen wie NSO bauen die Technologie, sie sind nicht für die Nachfrage verantwortlich. Und sie sind nicht die einzigen am Markt. Regierungen brauchen Cyberwaffen, und sie beauftragen private Unternehmen, um ihnen diese Waffen zur Verfügung zu stellen. NSO ist dabei nur Teil eines Marktes. Ein anderes Beispiel ist Zerodium, das auf seiner öffentlichen Website die Preise auflistet, die für die Lieferung von Schwachstellen gezahlt werden. Wenn man zum Beispiel einen Zero-Day für Windows liefert, zahlen sie eine Million Dollar. Dabei geht es allerdings nicht nur um Desktopcomputer und Server, sondern auch um Mobilgeräte wie Android. Ein One-Click für letzteres Betriebssystem kostet 2,5 Millionen Dollar. Ein Zero-Day für iOS bringt zwei Millionen Dollar ein. Ich brauche also nur eine Schwachstelle zu finden, um in den Ruhestand zu gehen. Der Markt ist also viel größer als nur NSO. Natürlich ist es nicht in Ordnung, dass Regierungen Zero-Days nutzen, um Journalisten zu überwachen. Aber sich nur auf eine Firma zu konzentrieren, ist ignorant, wenn man bedenkt, dass es hunderte solcher Unternehmen gibt.

STANDARD: Man bekam in den letzten Monaten das Gefühl, dass Zero-Days, also vom Entwickler noch nicht entdeckte Sicherheitslücken, das derzeit größte Problem in Sachen Cybersicherheit sind. Stimmt das?

yahoo!finance

Israel's 11th Annual Cyber Week Conference Highlights Record Cyber Funding and Critical Need For Coordinated Cyber Response

Israel's top politicians, global cyber policymakers, and C-level executives from multinational companies and cutting-edge start-ups from 80+ countries took part in Cyber Week
Attendees and speakers tackled unprecedented cyber challenges and methods to counter those threats and strengthen cybersecurity

Prime Minister Naftali Bennett, Defense Minister Benny Gantz, and Minister of Public Security, Omer Bar Lev addressed national level cyber threats at Israel's 11th annual Cyber Week Conference, and were joined by cyber heads from the US, UK, Germany, Singapore, Czech Republic, and elsewhere. Private sector giants such as IAI, IBM, Checkpoint and Microsoft also took part alongside cutting edge cyber startups and investors such as YL Ventures.

Cyber Week's hybrid in-person-online conference, which is hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology and Security, occurred against the backdrop of unprecedented opportunities and challenges in the cyber sphere. Ransomware attacks nearly doubled in the past year to top 300M and the biggest ever publicly acknowledged payout to hackers was set at $40 million. Cyber warfare continues its rapidly growing military importance, and investments in cyber security tech reached $7.8 billion, a record level, two-thirds of which went to US and Israeli companies.

The conference touched upon the themes of today's unprecedented cyber business environment, Israel's Prime Minister Naftali Bennett pointed out that $41 out of every $100 dollars world wide is going to an Israeli startup and investment worldwide is skyrocketing. Conference speakers also touched upon the increasing frequency and danger of cyberattacks to global supply chains and the critical need to share information and mount of coordinated defense. Priminister Bennett and others highlighted Israel's efforts, including 24 MOUs and establishment of a dedicated National Cyber Directorate led by Yigal Unna. Lastly, the Prime Minister invited other nations to join a global cybernet shield initiative to jointly coordinate the fight against cyber threats globally.

"Today the best bang for your buck is a cyber attack and it's just going to grow exponentially, and that makes me worried. As Prime Minister of Israel, I view this as one of the top threats to Israel's national security and the world's security," said Israeli Prime Minister Naftali Bennett.

Prime Minster Bennett also spoke about the need for further cooperation, "If you're on a crowded bus and there is a pickpocket who tries to steal your things you can be silent or you can take out red spray, spray him in the face, and mark him as a criminal so everyone else can band together and defend themselves, our national cyber agency is that spray and that megaphone. That same national network [Israel's National Cyber Directorate] is opening up and we're announcing the global Cybernet Shield, using the very same principles of cyber connectivity because if you fight alone you will lose, but if we fight together we will win."

Israel's Defense Minister, Benny Gantz, expressed similar sentiments and called for a cyber version of Israel's famous anti-missile defense system, Iron Dome, "Cyber is now a vulnerable space that must be protected like the sea, space, air, and ground," He also called for a no-tolerance policy by the Israeli government when it comes to Cyber attacks, "Our message is very clear - be it a rocket, or a keyboard, we will not tolerate anyone to threaten our people."

About CyberWeek:

Cyber Week is a leading international cybersecurity event that provides the unique opportunity for experts from industry, government and academia to share their knowledge about the challenges and opportunities in the field. Cyber Week is hosted by the Blavatnik Interdisciplinary Cyber Research Center and the Yuval Ne'eman Workshop for Science, Technology and Security, at Tel Aviv University, headed by Major Gen. (Ret.) Prof. Isaac Ben-Israel together with the National Cyber Directorate at the Prime Minister's Office, The Ministry of Economy and Industry and the Ministry of Foreign Affairs.

The New Times

Why cybersecurity is critical today more than ever

The dominant technology since the middle of the 20th century until today is computer technology. Now, if you want to be an advanced economy, you need to base on the dominant technology.

By Hudson Kuteesa

As African countries continue to jump onto the bandwagon of using computerized systems to run their economies and governance, cybersecurity is getting more and more important.

Cybersecurity is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

According to the Information Systems Audit and Control Association (ISACA), an international professional association focused on IT governance, global cybercrime damages are expected to reach USD 6 trillion by the end of this year.

Africa has not been quite as affected by large-scale cyberattacks as other parts of the world, however, the continent is no stranger to the problem in general, as hacking incidents into bank accounts of individuals and institutions are not new here.

With continuous steps towards computer-driven economies that are characterized by the Internet of Things (IoT) and Artificial Intelligence (AI), Africa may soon become a bigger target for cybercrime.

Israel, a nation that is arguably leading the world in cybersecurity is a great example of how African countries should attach serious importance to cyber-safety if they will be able to successfully pursue and attain computer-driven economies and governance.

Among other things, the country established a National Cyber Directorate responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational defense in cyberspace.

It provides incident handling services and guidance for all civilian entities as well as all critical infrastructures in the Israeli economy, and works towards increasing the resilience of the civilian cyberspace.

According to Yigal Unna, the Director-General of the Directorate, they have in place a hotline for citizens to call and report any incident that may look like a cyber threat.

These are some of the things that showcase Israel's great attention to cyber-safety, but that is not all.

The country also invests heavily in the sector, offering hundreds of millions of dollars to cyber-tech startups every year, in addition to providing robust education to the young generations in regard to cyber-tech.

In an interview with media, Isaac Ben-Israel, a professor at Tel Aviv University, who is one of the pioneers in the cyber industry highlighted the importance of computer technologies in driving economies, but noted that there is a "dark side" to it that the users should pay attention to.

"The dominant technology since the middle of the 20th century until today is computer technology. Now, if you want to be an advanced economy, you need to base on the dominant technology. However, you have to remember that once you progress economically, there is a dark side to it. A lot of problems arise, and cyber-attacks are one of them," he said.

So there is need to invest in adequate protective mechanisms to all infrastructures that use computerized systems, keep building the capacity of the people that will have enough cyber knowledge to defend companies, countries, and so on, in addition to sensitizing the public to be careful and responsible while using computerized systems.

During the Cyber Week Conference that took place last week in Israel, Prime Minister Naftali Bennett talked about launching the "Global Cybernet," a network for sharing information about cyber defense between countries.

The network currently comprises about 1,400 cyber professionals in Israel, including analysts, researchers and information security managers, from various organizations in the country who share information about attacks or their suspicions.

SPONSORS & PARTNERS

Distinguished Benefactor

THE SAGOL NETWORK

Esteemed Platinum Sponsors

IAI Creating a Difference

YL VENTURES

Platinum Sponsors

Check Point SOFTWARE TECHNOLOGIES LTD.

IBM

PENTERA

Gold Sponsors

BigID

Checkmarx

CYBERARK

Cyberstar For a Secure World

ELRON

Microsoft

Synamedia

SYNOPSYS

snyk

Silver Sponsors

BioCatch

BOSCH Invented for life

COMSEC GLOBAL

Kramer Levin

Steven E. Stern

SYGNIA

THETARAY

Bronze Sponsors

CISCO

cybereason

FIREEYE | MANDIANT

LUXEMBOURG TRADE & INVEST

MITIGA

NTT Innovation Laboratory Israel

Connect easily with thanks to: Cellcom

Partners

HELMHOLTZ RESEARCH FOR GRAND CHALLENGES

Embassy of the Federal Republic of Germany Tel Aviv

CYBTOGETHER Israeli Cyber Security Association

ISRAEL TECH POLICY INSTITUTE

FUTURE OF PRIVACY FORUM

CICC

המרכז לחינוך סייבר CYBER EDUCATION CENTER

sosa רשות החדשנות Israel Innovation Authority

ASHDOD PORT THE PORT OF ISRAEL

conexx

iATI Israel Advanced Technology Industries

JLCW

KONFIDAS YOUR BUSINESS, SECURED

JETRO

CSA cloud security alliance®

DSI DIGITAL SOCIETY INSTITUTE

ESMT BERLIN

STARTUP NATION CENTRAL

SOPHIC™ by Israel Electric

CII Confederation of Indian Industry

Embassy of India

Israel-India Chamber of Commerce

ISRAEL SWEDEN

ABOUT-FRAUD

Or-Hof

IDPF Israeli Data Protection Professionals Forum

SAE INTERNATIONAL

TEL AVIV UNIVERSITY ALUMNI ORGANIZATION

BSIDES TLV 2021

UK Israel Tech HUB

HiTech Ambassadors

CYBERTLV

TEL AVIV UNIVERSITY THE ISRAELI FRIENDS


Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University
ICRC
Blavatnik Interdisciplinary
Cyber Research Center
TEL AVIV UNIVERSITY
אוניברסיטת תל אביב
Cyber Israel
National Cyber Directorate
In cooperation with:
ISRAEL CYBER ALLIANCE
Ministry of Foreign Affairs
Israel
Cyber Week
July 19th-22nd, 2021
Tel Aviv University, Israel

Press Kit