דו"ח מדיניות וביטחון סייבר

נובמבר 2022

דורון פלדמן, אופיר בראל,

דניאל כהן, ניצן הררי

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

TEL AVIV UNIVERSITY אוניברסיטת תל אביב

Website: sectech.tau.ac.il | Tel: +972 (3) 6406041 | Email: icrc@tauex.tau.ac.il

תוכן עניינים

תקציר חודשי 2
ארה"ב 3
ממשל, אסטרטגיה ומדיניות 3
צבא וביטחון 5
אירופה 7
סיכום זירת הסייבר ברקע הפלישה הרוסית לאוקראינה 7
האיחוד האירופי 9
בריטניה 10
אפריקה והמזרח התיכון 11
איראן 11
ביטחון סייבר 11
איומי סייבר על תשתיות חיוניות 13
איומי סייבר על ענף האנרגיה 14
איומי סייבר על שרשראות אספקה 15
איומי מתקפות הכופרה 15
איומי סייבר על ענף הבריאות 17
איומי סייבר על ענף התחבורה 18
איומי סייבר על ענף התעופה 19
איומי סייבר על ענף הימאות 19
איומי סייבר על ענף הפיננסים 20
מחשוב קוונטי 21
מטבעות דיגיטליים 22
שיתופי פעולה 22

תקציר חודשי

נשיא ארה"ב, ג'ו ביידן, חתם על מִזְכָּר נשיאותי הכולל צעדים להתגוננות מפני איומי סייבר על מגזרי המזון והחקלאות. בנוסף, שוקל הנשיא לפרסם רפורמות בסמכויות מחלקת ההגנה ומחלקת המדינה בנושא תכנון וניהול מבצעי סייבר התקפיים. כמו כן, הסוכנות לאבטחת סייבר ותשתיות (CISA) פרסמה בקשה לקבלת מידע למטרת פיתוח פלטפורמה לשיתוף מודיעין איומי סייבר בקרב הממשל הפדראלי; מחלקת ההגנה פרסמה אסטרטגיה להטמעת עקרונות אפס אמון ברשתות המחלקה עד לשנת 2027. יתר על כן, חברת ה-IT האמריקנית, ECS זכתה בחוזה לפיתוח מערכת מתקדמת לאבטחת נקודות קצה בצבא היבשה האמריקני בסך 430 מיליון דולר. המערכת צפויה לשפר את יכולות מודיעין האיומים של הצבא, לשפר את אופן הגילוי והתגובה לאיומי סייבר ברשתות הצבא, לאפשר לנהל נכסי מידע באופן מרוכז ולסייע בהטמעת עקרונות אפס אמון בהגנה על רשתותיו.

ברקע תקיפות הסייבר שקבוצות האקרים רוסיות מקיימות כנגד מדינות התומכות באוקראינה, פורסם כי מספר בנקים בבריטניה מתכננים לשתף פעולה כך במקרה ואתר השייך לבנק מסוים יוּשְׁבַּת, לקוחותיו יוכלו לגשת לחשבונותיהם דרך אתרים השייכים לבנקים אחרים באמצעות שימוש בטכנולוגיית בנקאות פתוחה; המרכז הלאומי לאבטחת סייבר של בריטניה (NCSC), הציג יוזמה חדשה לסריקת מערכות ושרתים החשופים ברשת ושממוקמים בבריטניה, על מנת להקים מאגר נתונים על מצב חולשות האבטחה במדינה; חברת מודיעין איומי הסייבר, Mandiant, פרסמה את דו"ח תחזית איומי הסייבר שלה לשנת 2023, ולפיו צפויה עלייה במתקפות סייבר המשלבות אלמנטים מהמרחב הפיזי.

מחלקת האנרגיה האמריקנית הקצתה 15 מיליון דולר לטובת זיהוי, רכש והטמעה של טכנולוגיות ניטור וזיהוי אנומליות במערכות לבקרה תעשייתיות (ICS) ברשתות חשמל; חברת הבת האמריקנית של חברת ה-IT הקנדית, CGI Inc זכתה בחוזה בסך 17.4 מיליון דולר למטרת שיפור מידת אבטחת הסייבר של הוועדה לרגולציה על ענף האנרגיה הגרעינית האזרחית האמריקנית (NRC).[1] במסגרת החוזה תספק החברה מודיעין איומי סייבר, תנהל מעבדה דיגיטלית שתעסוק בזיהוי פלילי למטרת הפחתת איומי סייבר וכן תסייע ליישם תהליכים ולהטמיע טכנולוגיות חדשות; ממשלת אוסטרליה הציגה יוזמות וקווי מדיניות חדשים למאבק באיום מתקפות כופרה.

חברת Arianespace צפויה לשגר ברבעון האחרון של 2024 לוויין שישמש את סוכנות החלל של אירופה לביצוע ניסויים בהפצת והחלפה קוונטית של מפתח הצפנה. בנוסף, הבית הלבן פרסם מִזְכָּר חדש בנושא מעבר הממשל הפדראלי להצפנה פוסט-קוונטית; סוכנות דירוג האשראי Moody's פרסמה דו"ח בנושא איומי סייבר על ענף המסחר במטבעות דיגיטליים; שוודיה חנכה מעבדה לחקר איומי סייבר על כלי רכב המחוברים לרשת; הלשכה האמריקנית לספָּנוּת תקים עבור סינגפור מודלים וירטואליים לבחינת אבטחת הסייבר של ציוד OT בקרב כלי שיט; האיחוד האירופי הנחה את חברות התעופה ביבשת להקים מערך לזיהוי ומעקב אחר איומי סייבר; בריטניה, קנדה וסינגפור הודיעו כי ישתפו פעולה למטרת קידום ניסוח של תקנים בין-לאומיים והנחיות משותפות למגזר התעשייתי, לטובת עמידה בדרישות אבטחה מוכרות ומתואמות עבור רשתות ומכשירי IoT.

[1] Nuclear Regulatory Commission

ארה"ב

ממשל, אסטרטגיה ומדיניות

11 בנובמבר – הנשיא ביידן חתם על מזכר נשיאותי הכולל צעדים להתגוננות מפני איומי סייבר על מגזרי המזון והחקלאות – נשיא ארה"ב, ג'ו ביידן, חתם על מִזְכָּר ביטחון לאומי מספר 16 (NSM-16)[2] שמטרתו לתת מענה לאיומים על פעילותם של מגזרי המזון והחקלאות, לרבות איומי סייבר. המִזְכָּר קורא למחלקה לביטחון המולדת, מחלקת החקלאות, מחלקת המסחר וגופים פדראליים נוספים, לפתח ולקדם את הטמעתן של מערכות למעקב וניטור אחר איומים כימיים, ביולוגיים וגרעיניים, איומי סייבר ועוד. כמו כן, על מחלקת החקלאות, המחלקה לביטחון המולדת ומחלקות נוספות לנסח וליישם תוכניות הכשרה עבור מומחים בתעשיות המזון והחקלאות, לטובת הכשרתם להתמודדות עם איומי סייבר וכן לשתף מידע בנושא אפשרויות מימון וכלים שיסייעו לארגונים בענף להיערך ולהתמודד עם איומים ותקריות סייבר. בד בבד, על התובע הכללי והמחלקה לביטחון המולדת להוביל מהלכים לשיפור שיתוף המודיעין על איומי סייבר בקרב חברות חקלאות וייצור מזון, בהתאם לצו הנשיאותי 13636 משנת 2013.[3]

14 בנובמבר – משרד המבקר הממשלתי מצא ליקויים בתיעוד אירועי סייבר בקרב מחלקת ההגנה – על פי דו"ח שפרסם משרד המבקר הממשלתי (GAO), ספקי שירותי אבטחת הסייבר (CSSPs)[4] של המחלקה סיפקו דיווחים חלקיים בלבד על אירועי סייבר שהתרחשו ברשתות המידע של המחלקה. כך למשל, 91% מהדיווחים לא כללו את תאריך גילוי האירוע, מה שפוגע ביכולת המחלקה להסיק האם תקריות הסייבר מתגלות ומדווחות בפרקי זמן סבירים. כמו כן, המחלקה ניסחה נוהל בנושא יידוע קורבנות על דליפת מידע אישי השייך להם במסגרת תקיפות סייבר. אולם, המחלקה לא תיעדה האם דליפת מידע אישי אכן דווחה לקורבנות. במסגרת הדו"ח, GAO הציג שש המלצות וקרא למחלקה לפרסם נהלים מפורטים בנושא דיווח אירועי סייבר חמורים לבכירי המחלקה; לתעד שליחת הודעות לקורבנות דליפת מידע אישי; לבחון תמריצים שיעודדו חברות בתחום התעשייה הביטחונית לדווח בקביעות ובאופן מפורט על אירועי סייבר, ועוד.[5]

---

[2] National Security Memorandum
[3] הצו Improving Critical Infrastructure Cybersecurity, דורש מסוכנויות פדראליות לפתח ולהשתתף במסגרת, המיועדת לשפר את שיתוף המודיעין על איומי סייבר עם המגזר הפרטי; https://bit.ly/3Vf29HZ ; קישור למִזְכָּר: https://bit.ly/3i1XlHC
[4] cyber security service provider
[5] https://bit.ly/3TVqktZ ; קישור לדו"ח: https://bit.ly/3XmLl3I

15 בנובמבר – CISA פרסמה מדריך לתעדוף תיקון וטיפול בחולשות אבטחה בקרב ארגונים – CISA פרסמה את מדריך ה-SSVC,[6] המציג מודל עץ קבלת החלטות (Decision Tree), שמטרתו לסייע לארגוני ממשל ברמה הפדראלית, ברמה המדינה (state level) וברמה המקומית (local) להתמודד עם חולשות אבטחה. בבסיס המודל עומדת חלוקה של החולשות לארבע קטגוריות: (1) דרגת Track, לחולשות שדורשות מעקב בלבד; (2) דרגת *Track המגדירה חולשות שנדרש לעקוב אחר מאפיינים מסוימים שלהן; (3) דרגת Attend, המגדירה חולשות שיש לבקש עליהן מידע נוסף; (4) דרגת Act, המתייחסת לחולשות לגביהן ארגונים צריכים לקבל מידע נוסף על דרכים לתיקונן ואשר יש צורך לפרסם אזהרה לגביהן. סיווג החולשות לקטגוריות השונות נעשה על בסיס מספר פרמטרים, בהם ההשפעה הטכנית של החולשות והאופן שבו תוקפים עלולים לנצלן, האם ניתן לנצלן באופן אוטומטי ועוד.[7]

16 בנובמבר – ממשל ביידן השלים יוזמה אשר במסגרתה קלטו גופים מהמגזר הפרטי והממשלתי 7,000 מועסקים חדשים במקצועות אבטחת הסייבר – במסגרת יוזמה שהשיק ממשל ביידן שמטרתה לצמצם את פער כוח האדם הקיים במקצועות אבטחת הסייבר בארה"ב,[8] איגודי תעשייה, איגודי עובדים ומעסיקים פרטיים קלטו לשורות ארגוניהם יותר מ-7,000 מועסקים חדשים במסגרת תוכניות התמחות. היוזמה שנמשכה 120 ימים, הושקה כחלק מהפסגה הלאומית בנושא כוח עבודה וחינוך בתחום הסייבר שנערכה ביולי 2022, והובלה על ידי מחלקת המסחר, מחלקת העבודה, המחלקה לביטחון המולדת, משרד ראש הסייבר הלאומי (ONCD) וסוכנויות ממשל נוספות. בנוסף, קרוב ל-200 תוכניות התמחות בתחום אבטחת הסייבר אושרו על ידי מחלקת העבודה או נמצאות בשלבי תכנון. בה בעת, הגופים המשתתפים ביוזמה, בהם מחלקת ההגנה, חברות IBM, Cisco וחברות אחרות, הוסיפו לתוכניות ההתמחות המנוהלות בארגוניהם 120 תפקידים חדשים לאיוש במקצועות אבטחת הסייבר.[9]

21 בנובמבר – CISA פרסמה בקשה לקבלת מידע לפיתוח מערכת לשיתוף מודיעין איומי סייבר בקרב הממשל הפדראלי – הרשות לשירותים כלליים (GSA)[10] פרסמה בשם CISA בקשה לקבלת מידע בנושא נותני שירותי מודיעין איומי סייבר (TIES)[11] שיוכלו לסייע לסוכנות לפתח פלטפורמה לשיתוף מודיעין איומי סייבר. על פי הבקשה, האתגרים של שיתוף מידע יעיל בקרב גופי הממשל הפדראלי, כוללים מספר רב של היזנים (Feeds) המועברים בתצורות מידע שונות, קיומו של מידע חלקי הפוגע ביכולת קבלת ההחלטות ועוד.

---

[6] Stakeholder-Specific Vulnerability Categorization
[7] https://bit.ly/3gxeqZL ; https://bit.ly/3i8CBOC : קישור למדריך
[8] על פי הערכת הממשל הפדראלי ישנן 700 אלף משרות לא מאוישות במקצועות אבטחת הסייבר.
[9] https://bit.ly/3OwgyNR ; https://bit.ly/3Vg0HFo
[10] General Services Administration
[11] Threat Intelligence Enterprise Services

על פי הבקשה, המערכת תוטמע ביישומים מותאמים של CISA ויכולותיה יוצעו כמערך שירותים עבור קהילת המודיעין וגורמי אכיפת חוק פדראליים, גורמי ממשל מקומיים (local) וברמת המדינה (state). הפלטפורמה המוצעת תפעל באמצעות מיזוג התראות ממקורות מגוונים, בהם התראות הניתנות על ידי גורמים במגזר הפרטי ומערכת ה-AIS,[12] המופעלת על ידי CISA.[13]

<u>22 בנובמבר – הפנטגון פרסם אסטרטגיה להטמעת עקרונות אפס אמון ברשתותיו עד לשנת 2027</u> – מטרת האסטרטגיה היא לקדם הטמעה של עקרונות אפס האמון (Zero trust) בקרב רשתות מחלקת ההגנה עד לשנה הפיסקאלית 2027, מתוך תפיסה כי יש לעבור ממודל הגנה המבוסס על הגנה היקפית למודל המבוסס על אפס אמון.[14] האסטרטגיה כוללת ארבע מטרות: (1) קידום תרבות ארגונית, המבינה את חשיבות עקרון אפס האמון ומקדמת אותו; (2) שילוב עקרונות אפס האמון במערכות המידע של הארגון; (3) הטמעת פיתוחים טכנולוגיים נחוצים לשם מיזוג העקרונות בארכיטקטורת הרשת של המחלקה לצד קידום חדשנות המבוססת על עקרונות ה-Fail Fast;[15] (4) התאמת תהליכי המחלקה, הרכש והמימון למטרת הטמעת אפס האמון. כמו כן, בכוונת המחלקה לנסח תוכניות עתידיות להטמעת שירותים עסקיים ממשלתיים ומסחריים מבוססי ענן. לדברי דיוויד מקיאון (David McKeown), המכהן בפועל כסגן מנהל מערכות המידע של הפנטגון, המחלקה תפעל בשיתוף ספקיות שירותי הענן גוגל, AWS, Oracle ומיקרוסופט, על מנת לבחון את עקרונות אפס האמון בסביבות ענן ציבורי.[16]

צבא וביטחון

<u>8 בנובמבר – חברת IT אמריקנית זכתה בחוזה לפיתוח מערכת מתקדמת לאבטחת נקודות קצה של צבא היבשה</u> – חברת ה-IT האמריקנית, ECS זכתה בחוזה של פיקוד הסייבר של צבא היבשה (ARCYBER), בסך 430 מיליון דולר ולמשך חמש שנים, במסגרתו תפתח גִּרְסָה מתקדמת של הפלטפורמה הצבאית לאבטחת נקודות קצה (AESS).[17] לדברי נשיא ECS, ג'ון הנגאן (John Heneghan), AESS 2.0 צפויה לשפר את יכולות מודיעין האיומים של הצבא באמצעות מיזוג פעילותה עם פלטפורמת נתוני העתק (big data) של צבא היבשה, Gabriel Nimbus, יחד עם פלטפורמות מידע אחרות במחלקת ההגנה. בנוסף, תכלול ה-AESS 2.0 יכולות חדשות, שישפרו את אופן הגילוי והתגובה לאיומי סייבר ברשתות הצבא ותאפשר לו לנהל נכסי מידע באופן מרוכז.

---

[12] Automated Indicator Sharing; מערכת שפותחה בשנת 2016 ושמאפשרת לגורמים במגזר הציבורי והפרטי לשתף בזמן אמת מודיעין לא מסווג על איומי סייבר ומידע על צעדי התגוננות.
[13] https://bit.ly/3OMKDJf ; קישור לבקשה: https://bit.ly/3ihVKOe
[14] מודל ההגנה ההיקפית כולל הפרדה בין המרחב הפנימי, עליו מגנים, בין המרחב החיצוני, מתוך תפיסה כי מקור איומי הסייבר הוא חיצוני ולא פנימי.
[15] עקרונות ה-Fail Fast הם גישה ניהולית שנערכת מראש לאפשרות של קריסת מערכות ומכינה צעדי התמודדות וחזרה לשגרה.
[16] https://bit.ly/3Vz0Bc1 ; קישור למסמך האסטרטגיה: https://bit.ly/3XE1XnV
[17] Army Endpoint Security Solution; המערכת יכולה להגן על עד כ-800,000 נקודות קצה ברשתות מסווגות ובלתי מסווגות ברחבי צבא היבשה.

בנוסף, לדברי סגן נשיא ב-ECS, מארק מאגלין (Mark Maglin), פלטפורמת ה-AESS 2.0 תאפשר לצבא היבשה להטמיע את עקרון אפס אמון בהגנה על רשתותיו.[18]

17 בנובמבר – גורמי אכיפה וממשל חשפו פרטים על פעילות סייבר התקפית שביצעה ארה"ב ועל הרפורמות שהממשל מקדם בנושא תכנון והוצאה לפועל של מבצעי סייבר התקפיים – במסגרת עדות בפני הוועדה לביטחון המולדת של הסנאט, אמר ראש ה-FBI, כריסטופר ריי (Christopher Wray) כי ארגונו הוציא לפועל מבצעי סייבר התקפיים כחלק מהתמודדות הארגונית הכוללת עם איומי סייבר שמזוהים עם מדינות ושחקנים לא-מדינתיים. ריי לא סיפק פרטים נוספים על פעילות זו, אך ציין כי מבצעי סייבר התקפיים הם אחד האמצעים שנקט ארגונו לצד ביצוע מבצעי סיכול מודיעיניים, התמקדות בתשתיות של גורמים זדוניים, פגיעה במימון פעילות בלתי חוקית באמצעות מטבעות דיגיטליים והפללת עבריינים סייבר.[19] בנוסף, לדברי גורמים רשמיים שהתראיינו בעילום שם, שוקל הנשיא ביידן לפרסם גִּרְסָה עדכנית של התזכיר הנשיאותי בנושא ביטחון לאומי מספר 13 (NSPM 13), בתחום סמכויות מחלקת ההגנה לניהול מבצעי סייבר התקפיים לאחר הרפורמות שביצע בו בחודש במאי 2022. הגורם הבכיר ציין כי הגִּרְסָה הסופית של התזכיר תכלול הנחיות שיחייבו את מחלקת ההגנה לספק לבית הלבן פרטים על תוכניות ומבצעי סייבר לפני הוצאתם לפועל. בנוסף, הגורם ציין כי התזכיר העדכני יעניק למחלקת המדינה סמכות נרחבת יותר, אך לא בלעדית, בתהליך התכנון וההוצאה לפועל של מבצעי סייבר התקפיים.[20]

18 בנובמבר – בכיר במחלקת ההגנה: חברות קבלן אינן מדווחות למחלקה על פעילותן בתחום אבטחת הסייבר – לדברי דיוויד מקיאון (David McKeown), המכהן בפועל כסגן מנהל מערכות המידע של הפנטגון, העובדה כי חברות קבלן העובדות עם מחלקת ההגנה אינן מחויבות לדווח על מהלכיהן בתחום אבטחת הסייבר, הובילה לכך שמרביתן לא עומדות בדרישות האבטחה שהוגדרו להן. מקיאון הוסיף כי המחלקה מציעה לחברות הללו אמצעים רבים וחינמיים לשיפור רמת האבטחה שלהן, כגון שירותי הגנה על חשבונות דוא"ל, שיתוף מודיעין על איומים ועוד, אך רק חלק זעום מהן אכן מנצל אותם. בהתאם לכך, הסביר מקיאון כי גרסתה השנייה של תוכנית תקני אבטחת הסייבר עבור חברות קבלן של מחלקת ההגנה (CMMC 2.0)[21] הצפויה להיכנס לתוקף בתחילת 2023, תחייב את כלל החברות העובדות עם מחלקת ההגנה לעבור תהליך להערכת אבטחת הסייבר שלהן על ידי גורם צד-שלישי.[22]

---

[18] https://bit.ly/3Auy2EP
[19] https://bit.ly/3iaJSh6 ; https://bit.ly/3OrZN6F
[20] https://bit.ly/3AE01Sh ; התזכיר נחתם על ידי נשיא ארה"ב לשעבר, דונלד טראמפ, ומעניק למחלקת ההגנה סמכויות נרחבות להוציא לפועל מבצעי סייבר ללא אישור הבית הלבן. מטרת הרפורמות שקידם ביידן היא להגביר את מידת הפיקוח והמעורבות של הבית הלבן ושל מחלקת המדינה בתכנון ובהוצאה לפועל של מבצעי סייבר התקפיים.
[21] Cybersecurity Maturity Model Certification ; מודל לניסוח תקני אבטחת סייבר עבור חברות קבלן העובדות עם מחלקת ההגנה.
[22] https://bit.ly/3UZfy7A

אירופה

סיכום זירת הסייבר ברקע הפלישה הרוסית לאוקראינה

החודש נמשכו מאמציהן של אוקראינה ובעלות בריתה לסכל תקיפות סייבר המזוהות עם רוסיה ולשפר את הגנת הסייבר שלהן לקראת התמודדות עם איומי סייבר עתידיים. במקביל, התפרסמו דו"חות ומחקרים המתארים את דפוסי התקיפה הנפוצים של גורמים רוסיים במרחב הסייבר, לצד סקירות על ההשלכות וההשפעות של הסיוע שאוקראינה קיבלה במהלך המלחמה מחברות פרטיות ומדינות ידידותיות.

ב-11 בנובמבר, מרכז מודיעין איומי הסייבר של חברת מיקרוסופט (MSTIC)[23] ייחס את מתקפות הכופרה שחוו חברות תחבורה ולוגיסטיקה באוקראינה ובפולין ב-14 באוקטובר לקבוצת ההאקרים הרוסית Sandworm, המקושרת למודיעין הצבאי של רוסיה (GRU). על פי MSTIC, מעורבותה של Sandworm בביצוע המתקפות מציגה סיכון מוגבר לארגונים המספקים סיוע הומניטרי או צבאי לאוקראינה במסגרת המלחמה.[24]

בנוסף למתקפות הסייבר שיוחסו לרוסיה, ב-13 בנובמבר הודיע צוות ה-CERT הלאומי של אוקראינה כי קבוצת האקרים האקטיביסטים רוסית המכונה בשם From Russia with Love,[25] הדביקה מספר ארגונים באוקראינה בסוג חדש של כופרה המכונה בשם Somnia. לפי צוות ה-CERT, קבוצת ההאקרים השתמשה באתרים מזויפים המחקים את תוכנת Advanced IP Scanner, כדי לגרום לעובדי הארגון האוקראיני להוריד נוזקה מסוג Vidar המאפשרת לתוקפים להשתלט על חשבון ה-Telegram של הקורבן ולגנוב הרשאות גישה לשירותי VPN. לאחר מכן, ההאקרים השיגו גישה לרשת הארגונית וגנבו מידע רגיש.[26]

במקביל לנתונים שפורסמו בנושא תקיפות סייבר שיוחסו לגורמים פרו-רוסיים, חשפו מדינות, ובראשן בריטניה, תוכניות שמטרתן לסייע לאוקראינה להתגונן מפני תקיפות סייבר מצד רוסיה ומצד גורמים זדוניים הפועלים בחסותה. ב-1 בנובמבר חשף משרד החוץ של בריטניה את תוכנית ה-Ukraine Cyber Programme, במסגרתה מסייעת בריטניה לאוקראינה להגן על תשתיות חיוניות בשטחה מפני מתקפות סייבר מצד רוסיה.

---

[23] Microsoft Threat Intelligence Center

[24] בהודעת הבלוג שפורסמה ב-14 באוקטובר 2022, טען מרכז מודיעין איומי הסייבר של מיקרוסופט (MSTIC) כי קבוצת האקרים לא מזוהה המכונה בשם DEV-0960 השתמשה בכופרה חדשה המכונה בשם Prestige במתקפותיה על חברות התחבורה האוקראינית והפולנית; https://bit.ly/3OyrdYl ; https://bit.ly/3V0IKev

[25] הקבוצה מכונה עוד בשמות Z-Team או UAC-0118.

[26] https://bit.ly/3OwoiQ4

התוכנית, שעלותה הכוללת היא 6.35 מיליון ליש"ט (כ-7.55 מיליון דולר), הושקה עם פלישת צבא רוסיה לאוקראינה וכוללת סיוע בתגובה לתקריות סייבר והגנה על תשתיות חיוניות, סיוע בחקירות פורנזיות למטרת למידה על מתקפות סייבר ואספקת פתרונות חומרה ותוכנה כגון אמצעים להגנה מפני תקיפות DDoS ופתרונות Firewall.[27]

כמו כן, ב-12 בנובמבר פורסם כי בכוונת בנקים בבריטניה לשתף פעולה על מנת למזער את הנזק כתוצאה מתקיפת DDoS רוסית אפשרית. במסגרת זו, במקרה בו אתר השייך לבנק מסוים יוּשְׁבַּת, לקוחותיו יוכלו לגשת לחשבונותיהם דרך אתרים השייכים לבנקים אחרים, באמצעות שימוש בטכנולוגיית בנקאות פתוחה, המאפשרת שיתוף פרטי מידע המוסכמים על לקוחותיהם. תוכנית זו הינה חלק מהמעקב השוטף של הבנקים בבריטניה, בשיתוף הרשות לניהול פיננסי (FCA),[28] אחר איומי סייבר פוטנציאליים מצד רוסיה מאז פלישתה לאוקראינה.[29]

לבסוף, ב-28 בנובמבר הודיע פיקוד הסייבר של ארה"ב, כי החל מדצמבר 2021 ביצע מבצעי סייבר הגנתיים (Hunt Forward) בשיתוף כוחות הסייבר של ממשלת אוקראינה, שנמשכו עד מספר ימים לפני פלישת רוסיה למדינה. המבצעים שפרטיהם אודותיהם לא פורסמו, נערכו כחלק מאמץ נרחב יותר לחזק את חסינות הסייבר של תשתיות חיוניות באוקראינה.[30]

מעבר לכך, החודש התפרסמו מחקרים בנושא מגמות שנרשמו במהלך חודשי הלחימה במרחב הסייבר. כך למשל, ב-3 בנובמבר פרסם מכון המחקר האמריקני Carnegie Endowment for International Peace מאמר, העוסק בתמיכה הבין-לאומית הניתנת לאוקראינה בתחום אבטחת הסייבר. על פי המאמר, הסיוע שחברות אמזון, מיקרוסופט ו-Google העניקו לאוקראינה במעבר לשירותי ענן מבוזרים, שיפרו את יכולותיה בתחום הגנת הסייבר, הרבה מעבר למה שהייתה מסוגלת להשיג באופן עצמאי. אולם, מחבר המאמר הזהיר כי בעוד שאוקראינה והמערב נוטים להתמקד בפעולות סייבר רוסיות שעלולות לגרום לשיבוש התפקוד של הגופים שהותקפו, ניסיון העבר מלמד כי רוסיה מבצעת פריצות רשת רבות גם למטרת איסוף מודיעין. פעולות אלו קשות לגילוי והשפעתן המיידית פחותה.[31] בנוסף, ב-3 בנובמבר פרסמה הסוכנות האירופית לאבטחת מידע ורשתות (ENISA) את דו"ח איומי הסייבר השנתי שלה, ממנו עולה כי עימותים גאו-פוליטיים ובהם המלחמה באוקראינה שינו באופן משמעותי את מפת האיומים במרחב הסייבר. מחברי הדו"ח הצביעו על עלייה בפעילותם של האקטיביסטים, ועל שימוש גובר בתקיפות סייבר בשילוב ובתיאום עם מתקפות קינטיות. כמו כן, מחברי הדו"ח ציינו כי מגמה זו עשויה להגדיר מחדש נורמות בין-לאומיות במרחב הסייבר הקשורות למתקפות סייבר הנעשות בחסות מדינות וכן לגבי פגיעה בתשתית אזרחית חיונית.[32]

---

[27] https://bit.ly/3tcAM5B
[28] Financial Conduct Authority; גוף רגולטורי המפקח על פעילותם של מוסדות פיננסיים בבריטניה.
[29] https://bit.ly/3GvTvAV
[30] https://bit.ly/3VkNqM6
[31] https://bit.ly/3g1E7RU
[32] https://bit.ly/3fNhsJ2 ; קישור לדו"ח: https://bit.ly/3UlYEQ0

האיחוד האירופי

10 בנובמבר – האיחוד האירופי פרסם מדיניות הגנת סייבר חדשה – הנציג העליון של האיחוד האירופי לענייני חוץ ומדיניות ביטחון, ז'וזף בורל (Josep Borrell) והנציבות האירופית, הודיעו כי האיחוד פועל לנסח מדיניות הגנת סייבר שמטרתה לשפר את מידת ההגנה על אזרחים ותשתיות חיוניות ולהגביר את התיאום ושיתוף הפעולה בין גופים אזרחיים וצבאיים העוסקים בתחום אבטחת הסייבר, בהם גופי אכיפת חוק ומשרדים דיפלומטיים. כמו כן, מטרת המדיניות היא לשפר את ניהול משברי הסייבר בקרב שטחי האיחוד האירופי, להפחית בתלות האסטרטגית בטכנולוגיות סייבר חיוניות ולחזק את בסיס ההגנה הטכנולוגי והתעשייתי של האיחוד (EDTIB).[33] כמו כן, במסגרת המדיניות החדשה, ינסחו מדינות האיחוד תקני אבטחת סייבר להגנה על מרכיבי תוכנות הנמצאות בשימוש צבאי ואזרחי וירחיבו את ההשקעה בפיתוח משותף של יכולות הגנת סייבר צבאיות. נציגי האיחוד הצהירו עוד כי יציגו בעתיד דו"ח מעקב שנתי על יישום המדיניות.[34] בנוסף, ב-15 בנובמבר, כחלק מהחלטה על הגדלת תקציב ההגנה של האיחוד האירופי, חתמו 18 שרי ההגנה של מדינות האיחוד על הקמת צוות CERT צבאי (MICNET),[35] שמטרתו לעודד שיתוף מידע בין המדינות, קהילות הסייבר הצבאיות והאזרחיות ולהגביר שיתוף ידע ומומחיות בתחום, לאור העלייה במתקפות סייבר כנגד האיחוד האירופי והמדינות החברות בו.[36]

14 בנובמבר – הסוכנות האירופית לאבטחת מידע ורשתות פרסמה את רשימת עשרת איומי הסייבר הצפויים לקראת שנת 2030 – ENISA פרסמה את רשימת האיומים על בסיס תרגיל אבטחת סייבר, שנערך בחודשים מרץ-אוגוסט 2022 בשיתוף הרשת האירופית לאירועי סייבר (EU-CyCLONe),[37] רשת צוותי תגובה לאירועי סייבר (CRISTs)[38] ו-ENISA, ושמטרתו למצוא פתרונות לאיומי סייבר שעשויים לעלות בשנת 2030. על פי רשימת האיומים, האקרים עלולים להשיג מידע ממכשירים חכמים המחוברים לרשת על מנת לבצע מתקפות סייבר מתוחכמות יותר, המותאמות יותר למטרותיהם. בד בבד, הצורך בהשבחה והחלפת מערכות מיושנות והמחסור בכוח אדם ביחס למערכות סייבר-פיזיות, כגון מערכות בקרה תעשייתיות (ICS), עלולים להגדיל את סיכוני האבטחה עליהן. כמו כן, הממשק בין מערכות חלל מסחריות לבין מערכות חלל ציבוריות והפער באבטחת הסייבר של מרכיבי חלל מסחריים עשויים להוות סיכון לפעילותן.[39]

---

[33] The European Union's Defense Technological and Industrial Base

[34] https://bit.ly/3V9DWmE ; קישור להודעה הרשמית: https://bit.ly/3ArBPTn

[35] Military Computer Emergency Response Team Operational Network

[36] https://bit.ly/3GIG0xK

[37] European Cyber Crises Liaison Organisation Network , גוף האחראי על תיאום התגובה לתקריות סייבר המתרחשות בקנה מידה רחב.

[38] Computer Security Incident Response Team

[39] איומים נוספים שצוינו ברשימה הם: גידול במתקפות סייבר המשלבות אלמנטים פיזיים בשל עלייה בשימוש במכשירים חכמים, תשתיות ענן ופלטפורמות חברתיות; עלייה במתקפות על שרשראות אספקה בשל שימוש ביותר רכיבים ושירותים הניתנים על ידי צד שלישי; שימוש בקטעי deepfake להפצת מידע כוזב ממניעים פוליטיים או כלכליים; ניסיונות לתקף מאגרי זהות דיגיטליים או מערכות זיהוי פנים מצד גורמים עבריינים; עלייה במתקפות סייבר נגד ארגונים הסובלים ממחסור ניכר בכוח אדם המיומן במקצועות אבטחת הסייבר; ניצול לרעה של טכנולוגיות בינה מלאכותית; וביצוע מתקפות נגד מערכות ICT בתשתיות חיוניות. https://bit.ly/3OoauqA ; קישור לרשימת האיומים המלאה: https://bit.ly/3UNWvgi

בריטניה

3 בנובמבר – המרכז הלאומי לאבטחת סייבר הציג יוזמה לסריקת מערכות הממוקמות בבריטניה לאיתור חולשות אבטחה – המרכז הלאומי לאבטחת סייבר (NCSC) הציג יוזמה חדשה לסריקת מערכות ושרתים החשופים ברשת וממוקמים בבריטניה, על מנת להקים מאגר נתונים על מצב חולשות האבטחה במדינה. במסגרת תהליך הסריקה, יתמקד ה-NCSC באיסוף מידע טכני, כגון תשובות HTTP וכתובות IP. היקף המידע האישי והטכני שייאסף, יהיה מינימלי ובהתאם לצורך. לדברי המנהל הטכני של NCSC, איאן לוי (Ian Levy), ה-NCSC ישתמש תחילה בטכניקות סריקה פשוטות ולאחר מכן יעבור באופן מבוקר להשתמש בשיטות סריקה מורכבות יותר. באמצעות יוזמה זו, מקווה ה-NCSC להבין טוב יותר את מצב חולשות האבטחה הכולל בבריטניה, לייעץ לבעלי מערכות על מצב האבטחה שלהם על בסיס יומיומי ולהגיב מהר יותר לאירועי אבטחה שונים, כגון ניצול חולשות יום אפס (Zero-day).[40]

8 בנובמבר – המרכז הלאומי לאבטחת סייבר פרסם את הסקירה השנתית של פעילותו – על פי הסקירה השנתית שפרסם המרכז הלאומי לאבטחת סייבר של בריטניה (NCSC), בתקופה שבין ספטמבר 2021 לאוגוסט 2022, התרחשו בבריטניה 18 מתקפות כופרה שחייבו תיאום תגובה ברמה הלאומית, בהן מתקפות על גופים במגזר העסקי ועל גופים ציבוריים, בהם שירות הבריאות הלאומי (NHS) ומתקן לאספקת מים בצפון-מערב אנגליה. בנוסף, ה-NCSC העריך כי לצד איומי הסייבר שמקורם ברוסיה, התפתחותה הטכנולוגית של סין עשויה להוות את המרכיב החשוב ביותר המשפיע על אבטחת הסייבר בבריטניה, מאחר ופעילות הסייבר של סין נעשית מתוחכמת יותר והיא מרבה לתקוף שרשראות אספקה ולנצל חולשות אבטחה בתוכנות. ה-NCSC ציין בסקירה כי בכוונתו להרחיב בעתיד את תוכנית הגנת הסייבר האקטיבית (ACD),[41] כך שתכלול שירות שיסייע לארגונים להבין לעומק את חולשות האבטחה אליהן הם חשופים. בה בעת, בכוונת ה-NCSC לשפר גם את שירותי התוכנית למומחי אבטחה בארגונים גדולים, בייחוד אלו המועסקים במגזר הציבורי ובענפי התשתיות החיוניות, באמצעות הרחבת שירותים כגון ביצוע סריקות לאיתור חולשות.[42]

---

[40] https://bit.ly/3DSQKH7
[41] Active Cyber Defence
[42] https://bit.ly/3UQdQ8h ; קישור לסקירה: https://bit.ly/3VgmY69

אפריקה והמזרח התיכון

איראן

18 בנובמבר – CISA וה-FBI פרסמו אזהרה על פעילות קבוצות APT איראניות נגד סוכנות פדראלית אזרחית בארה"ב – על פי האזהרה, בפברואר 2022, קבוצות APT המזוהות עם המשטר האיראני פרצו לרשת פדראלית אזרחית לאחר שניצלו את חולשת האבטחה Log4Shell בשרת השייך לפלטפורמת Vmware Horizon,[43] ביצעו תנועה רוחבית בבקר הדומיין (domain controller)[44] וגנבו הרשאות. במסגרת האזהרה, CISA וה-FBI המליצו לארגונים להגן על הרשאות באמצעות הגבלת אופני השימוש בהן ובחשבונות, לעשות שימוש באימות רב-שלבי ועוד.[45] במסגרת שימוע שנערך בוועדת הסנאט לביטחון המולדת ולענייני ממשל, טען מזכיר המחלקה לביטחון המולדת, אלחנדרו מאיורקס (Alejandro Mayorkas), כי הפעילות האיראנית עשויה להיחשב כאירוע סייבר משמעותי, על פי ההגדרות בחוק ה-FISMA.[46]

ביטחון סייבר

3 בנובמבר – TikTok הודיעה על שינוי במדיניות הפרטיות להגבלת הגישה של עובדיה לנתונים השייכים למשתמשים באירופה – הרשת החברתית TikTok הודיעה כי עדכנה את מדיניות הפרטיות שלה עבור האזור הכלכלי האירופי (EEA),[47] בריטניה ושוויץ, שצפויה להיכנס לתוקף ב-2 בדצמבר 2022. במסגרת העדכון, עובדי החברה המוצבים במקומות שונים בעולם, לרבות סין, יוכלו לקבל גישה לנתונים השייכים למשתמשים באירופה, רק לאחר שהוכח מעל לכל ספק, כי הגישה למידע נחוצה לשם הבטחת עבודתה התקינה של TikTok ובכפוף לתקנות ה-GDPR ובקרות אבטחה.[48] על פי הודעת החברה, השינוי הוא חלק מתהליך רחב, שנועד להגביל את גישת עובדיה למידע על משתמשים באירופה, לצמצם הדלפות נתונים ולאחסן אותם באופן מקומי.[49]

---

[43] פלטפורמה המשמשת לניהול שולחנות עבודה וירטואליים ויישומים בתשתיות ענן היברידיות.
[44] שרת המגיב לבקשות אימות לצרכי אבטחה ברשת מחשבים.
[45] https://bit.ly/3EqgR8x ; קישור לאזהרה: https://bit.ly/3TYsPMb
[46] על פי חוק ה-FISMA, אירועים אלו מוגדרים כתקריות שעלולות להסב נזק ניכר לביטחון הלאומי של ארה"ב. על פי החוק, חובה לדווח על תקריות אלו לקונגרס עד שבעה ימים לאחר הגדרתם במונח זה; https://bit.ly/3i26Syy
[47] European Economic Area
[48] https://bit.ly/3ThbYnp
[49] https://bit.ly/3zWq3zS

בנוסף, ב-17 בנובמבר במסגרת שימוע שנערך במסגרת וועדת בית הנבחרים האמריקני לביטחון המולדת, אמר ראש ה-FBI, כריסטופר ריי (Christopher Wray), כי קיימת סכנה לביטחון הלאומי של ארה"ב כתוצאה משימוש של הציבור האמריקני באפליקציית TikTok. ריי הזכיר כי ממשלת סין עושה שימוש באפליקציה לצורך איסוף נתונים על משתמשים, ניצול לרעה של האלגוריתם של TikTok לשם צנזור או קידום סרטונים מסוימים במטרה להשפיע על אזרחים אמריקנים, או לצורך שליטה באפליקציה שתאפשר פריצה ושליטה על מכשירים אישיים.[50]

8 בנובמבר – חברת Mandiant פרסמה את תחזית איומי הסייבר שלה לשנת 2023 – על פי הדו"ח שפרסמה חברת מודיעין איומי הסייבר Mandiant, במרוצת הזמן האקרים שינו את שיטת תקיפתם מהשתלטות על נקודות קצה להשגת גישה להרשאות כניסה וחשבונות של קורבנותיהם. כתוצאה מכך, צופים מחברי הדו"ח כי בשנת 2023 ההאקרים ישלבו מספר שיטות תקיפה על מנת לגנוב את זהותם של קורבנותיהם, בהן שימוש באמצעי הנדסה חברתית למטרת גניבת נתונים ממאגרי מידע פנימיים. בד בבד, צופים מחברי הדו"ח עלייה במתקפות הסייבר המשלבות אלמנטים מהמרחב הפיזי, כגון הודעות על קבלת דבר דואר, הכוללות קוד QR המפנה לאתר המשמש לגניבת פרטי כרטיסי אשראי. בנוסף, חברת Mandiant צופה כי במהלך שנת 2023 איומי הסייבר על יבשת אירופה צפויים לגבור באופן משמעותי, הן בשל התרחבות תקיפות הסייבר מצד גורמים רוסיים והן בשל הפיכתה הצפויה ליעד המרכזי של מתקפות כופרה בעולם. כמו כן, מחברי הדו"ח ציינו כי מערכות בחירות שצפויות להיערך במספר מדינות באזור דרום-מזרח אסיה וכן מגזר ייצור חומרים מוליכים למחצה, עלולים להוות מטרות נפוצות לתקיפות סייבר באזור זה במהלך שנת 2023.[51]

[50] https://bit.ly/3GRt7l0
[51] https://bit.ly/3UUYm2E ; גישה לדו"ח: https://bit.ly/3GfTG3m

<u>2 בנובמבר – מחלקת האנרגיה האמריקנית הקצתה 15 מיליון דולר לחיזוק אבטחת הסייבר של מערכות בקרה תעשייתיות ברשתות חשמל</u> – מחלקת האנרגיה העניקה 15 מיליון דולר לאגודה השיתופית לרשתות חשמל באזורים כפריים (NRECA)[52] לטובת זיהוי, רכש והטמעה של טכנולוגיות ניטור וזיהוי אנומליות במערכות לבקרה תעשייתית (ICS). על פי תוכנית המחלקה, כלל הסכום מיועד לתקופה של שלוש שנים, כאשר 10 מיליון דולר ניתנו עבור שנת 2022 וחמישה מיליון דולר עבור השנתיים העוקבות.[53]

<u>7 בנובמבר – NIST פרסם בקשה לקבלת מידע מהציבור על פרויקט חדש שמטרתו לגבש עקרונות אבטחת סייבר בקרב מתקני מים עירוניים</u> – המרכז הלאומי למצוינות בתחום אבטחת הסייבר (NCCoE),[54] הכפוף ל-NIST פרסם לתגובות הציבור מסמך המציג פרויקט חדש, שמטרתו לגבש מודל ארכיטקטורה מאובטחת בקרב מתקני מים עירוניים ושיטות עבודה מומלצות להגנה על מערכות מים. כמו כן, מתמקד הפרויקט בנושא ניהול נכסי מידע בקרב מתקני מים, הגנה על אמינות (integrity) המידע, לרבות בסביבת הטכנולוגיה התפעולית (OT); ניהול גישה מרחוק; וחלוקת רשתות למקטעים (Segmentation). במסגרת הפרויקט, יבחן NCCoE את השימוש באמצעים המצויים במגזר הפרטי לפתרון בעיות אבטחת סייבר בארבעת התחומים ובסיומו צפוי להתפרסם מסמך שיציג עקרונות אבטחת סייבר למתקני מים עירוניים.[55]

<u>18 בנובמבר – משרד המבקר הממשלתי: תשתית הנפט והגז הימית של ארה"ב עומדת בפני סיכוני אבטחת סייבר משמעותיים</u> – GAO פרסם דו"ח המזהיר מפני סיכון הולך וגובר של התקפות סייבר על רשתותיהם של כ-1,600 מתקנים ימיים, כגון אסדות, האחראים לעיקר תפוקת הנפט והגז בארה"ב והמסתמכים על טכנולוגיה לניטור ובקרה מרחוק של ציוד. מחברי הדו"ח הזהירו כי גורמים זדוניים המזוהים עם סין, איראן, צפון קוריאה ורוסיה עלולים לנסות להוציא לפועל מתקפות סייבר כנגד ארגונים מענפי הגז והנפט, וכן הדגישו כי תוקפים עלולים לנצל חולשות אבטחה הקיימות בקרב מערכות ה-OT המשמשות לשליטה מרחוק ולשמירה על בטיחות.

---

[52] National Rural Electric Cooperative Association ; ארגון המייצג כ-900 איגודים במגזר החשמל ב-47 מדינות בארה"ב.
[53] https://bit.ly/3zXokKD
[54] National Cybersecurity Center of Excellence
[55] https://bit.ly/3AgHPxZ ; קישור למסמך המציג את פרטי הפרויקט: https://bit.ly/3UUJgtT

המחברים ציינו כי תשתית OT מיושנת זו הנמצאת בשימוש במתקנים בענף האנרגיה, מועדת לפגיעה עקב היעדרם של אמצעי אבטחת סייבר נאותים ועדכוני אבטחה והוסיפו כי הדבר מקשה על זיהוי פעילות זדונית ברשת. המחברים המליצו ללשכה לבטיחות ולאכיפה סביבתית של מחלקת הפנים האמריקנית (BSSE)[56] ליישם אסטרטגיית אבטחת סייבר לטיפול בסיכונים על תשתיות ימיות, הכוללת ביצוע הערכת ומזעור הסיכונים; קביעת יעדים, ופעילויות לביצוע והגדרת מדדים למדידת עמידה ביעדים; קביעת תפקידים ותחומי אחריות באופן מתואם; וזיהוי המשאבים וההשקעות הנדרשים לשם כך.[57]

<u>22 בנובמבר – CISA פרסמה עדכון למסגרת העוסקת בהגנת תשתיות חיוניות מפני איומי סייבר</u> – CISA פרסמה גִּרְסָה עדכנית למסגרת ה-IRPF,[58] שפורסמה לראשונה באוקטובר 2021 על מנת לסייע למומחי אבטחה לחזק את ההגנה על תשתיות חיוניות מאיומים שונים, לרבות איומי סייבר. על פי המדריך, בעת הגדרת מאפייני התשתיות החיוניות שעליהן רוצים להגן, יש להגדיר גם את כלל מערך התשתיות והנכסים, בהם מערכות מחשבים, מערכות בקרה, תוכנות וחומרות לאחסון ועיבוד מידע וספקי תשתיות ענן. המסמך המעודכן כולל גישה למאגרי נתונים על נכסי תשתיות חיוניות, המספקים מידע ציבורי נוסף על נכסי תשתיות חיוניות. מלבד זאת, המסמך מרכז מקורות ידע פדראליים נוספים לגיבוש מדיניות אבטחת סייבר, כגון מסגרת אבטחת הסייבר של NIST,[59] הכולל עקרונות מנחים וולונטריים לניהול סוגיות באבטחת סייבר.[60]

<u>3 בנובמבר – חברת טכנולוגיית מידע זכתה בחוזה בסך 17.4 מיליון דולר במסגרתו תסייע לשפר את אבטחת הסייבר של הוועדה לרגולציה על ענף האנרגיה הגרעינית האזרחית האמריקנית</u> – חברת הבת CGI Federal Inc האמריקנית של חברת ה-IT הקנדית, CGI Inc זכתה בחוזה בסך 17.4 מיליון דולר למטרת שיפור מידת אבטחת הסייבר של הוועדה לרגולציה על ענף האנרגיה הגרעינית האזרחית האמריקנית (NRC).[61]

---

[56] The Department of the Interior's Bureau of Safety and Environmental Enforcement
[57] https://bit.ly/3VdMlFO ; הקישור לדו"ח המלא: https://bit.ly/3Xod6cn
[58] Infrastructure Resilience Planning Framework
[59] NIST Cybersecurity Framework ; https://bit.ly/3FbejfZ
[60] https://bit.ly/3XHbP03 ; קישור למסמך המסגרת: https://bit.ly/3u9fRRp
[61] Nuclear Regulatory Commission

GCI Federal תסייע ל-NRC ליישם תהליכים ולהטמיע טכנולוגיות חדשות, שיסייעו לה לשפר את מידת אבטחת הסייבר שלה וכן תספק לה מודיעין איומי הסייבר. בנוסף, CGI Federal תנהל מעבדה דיגיטלית שתעסוק בזיהוי פלילי, שתפעל למטרת הפחתת איומים הנובעים מגורמים פנימיים ומקבוצות APT.[62]

15 בנובמבר – דו"ח חדש: בתי ספר ציבוריים בארה"ב אינם ערוכים מספיק להתמודדות עם מגוון איומי סייבר – על פי דו"ח שפרסם המרכז ללא מטרות רווח לאבטחת האינטרנט (CIS),[63] יכולותיהם של בתי ספר ציבוריים בארה"ב בגילאי גן ילדים ועד התיכון (K-12) בתחום אבטחת הסייבר פחותות ביחס לארגונים במגזרים אחרים. מחברי הדו"ח מציינים כי בתי ספר בארה"ב היו יעד מרכזי לתקיפות סייבר שנצפו במהלך שנת 2022 עקב מעבר להוראה מקוונת והיברידית ומחבריו מציינים עוד כי המגמה עלולה להתגבר בשנת 2023. רוב בתי ספר מהווים יעד מועדף למתקפות כופרה וכן מצד האקטיביסטיים הפועלים על רקע אידאולוגי ומבקשים לטפח את המוניטין שלהם. מחברי הדו"ח ממליצים לבתי ספר להטמיע מערכות IDS לאיתור איומים ברשת וכן פתרונות EDR[64]; להיעזר בשירותים החינמיים שה-CIS מציע, הכוללים שיתוף מודיעין איומי סייבר וביצוע הערכת מצב אבטחת הסייבר, ועוד.[65]

1 בנובמבר – דו"ח חדש: רוסיה מזוהה עם חלק ניכר ממתקפות הכופרה שנרשמו בסוף שנת 2021 – הרשות לאכיפת פשעים פיננסיים (FinCEN),[66] סוכנות במחלקת האוצר האמריקנית, פרסמה דו"ח במסגרתו בחנה דפוסים ומגמות של שימוש בתוכנות כופרה על בסיס נתונים שדווחו על ידי מוסדות פיננסיים אמריקנים. על פי הדו"ח, 594 מתקפות כופרה זוהו עם רוסיה או עם גורמים הפועלים מטעמה, מתוך סך של 793 מתקפות כופרה שדווחו בין חודש יולי 2021 לחודש דצמבר 2021.

---

[62] https://bit.ly/3EftYcF ; https://bit.ly/3TzXDTm
[63] Center for Internet Security
[64] Endpoint Detection & Response.
[65] https://bit.ly/3ADvQei ; הקישור לדו"ח: https://bit.ly/3gxuqLp
[66] Financial Crimes Enforcement Network

בנוסף, העלות הכוללת הנגרמת עקב תקריות הכופרה בתקופה זו עמדה על 488 מיליון דולר. כמו כן, 58% מתוך 84 סוגים של תוכנות כופרה שהחוקרים בחנו, נקשרו לגורמי סייבר מרוסיה. בנוסף, על פי הממצאים, מספר מתקפות הכופרה שנרשמו בשנת 2021 הוכפל ל-1,251 מתקפות, לעומת 602 מתקפות ב-2020.[67]

1 בנובמבר – הבית הלבן כינס את הפסגה הבין-לאומית השנייה למאבק באיומי מתקפות הכופרה – הפסגה הבין-לאומית השנתית השנייה למאבק באיומי מתקפות הכופרה התכנסה בהשתתפות 36 מדינות בהן ישראל, אוסטרליה, בריטניה, צרפת, גרמניה ואחרות וכן בהשתתפות נציגים מהמגזר הפרטי, לצורך תיאום המאבק באיומי מתקפות הכופרה ברחבי העולם. במסגרת הפסגה, התחייבו נציגי המדינות המשתתפות להקים כוח משימה בין-לאומי למאבק במתקפות כופרה (ICRTF)[68] בהובלת אוסטרליה והמרכז לשיתוף מידע בנושא איומי תוכנות הכופרה במרכז הגנת הסייבר האזורי של ליטא (RCDC).[69] כמו כן, התחייבו נציגי המדינות לנקוט צעדים משותפים למניעת השימוש של עבריינים כופרה במטבעות דיגיטליים, לערוך סדנה להתמודדות עם מימון בלתי חוקי ולפיתוח יכולת מעקב וניתוח אחר איומים בטכנולוגיית Blockchain, לקיים תרגילים דו-שנתיים להתמודדות עם איומי מתקפות הכופרה, לפרסם מסמכים אסטרטגיים ומסמכי ייעוץ משותפים המתארים טכניקות וטקטיקות (TTPs) שניתן לנקוט כנגד עבריינים כופרה בולטים שזוהו, ועוד.[70]

12 בנובמבר – ממשלת אוסטרליה הציגה יוזמות וקווי מדיניות חדשים למאבק במתקפות כופרה – על פי הודעה מטעם משרדי ההגנה והפנים, המשרד לאבטחת סייבר והתובע הכללי של ממשלת אוסטרליה, הממשלה הקימה את כוח המשימה המשותף (JSO),[71] הכולל 100 אנשי צוות ממִנְהֵלת הסיגינט של אוסטרליה (ASD)[72] ומהמשטרה הפדראלית ושמטרתו להיאבק בפעילותן של קבוצות עבריינים סייבר, תוך התמקדות בקבוצות עבריינים כופרה. במסגרת תפקידו, יתמקד ה-JSO גם במעקב ובשיבוש פעילותם של ארגוני פשיעת סייבר בין-לאומיים, תוך שיתוף פעולה ותיאום עם גורמי אכיפה ממדינות זרות. בנוסף, הודיעה שרת הפנים ואבטחת הסייבר, קלייר אוניל (Clare O'Neil), כי כחלק מאסטרטגיית אבטחת הסייבר הלאומית, הממשלה שוקלת לאסור בחוק את תשלום דמי הכופר במסגרת מתקפות כופרה.[73]

---

[67] https://bit.ly/3EsMK1m ; קישור לדו"ח: https://bit.ly/3tnLVR6
[68] International Counter Ransomware Task Force
[69] Regional Cyber Defense Centre
[70] https://bit.ly/3UYoTvZ ; קישור להודעת הבית הלבן: https://bit.ly/3TzNw0K
[71] Joint Standing Operation
[72] Australian Signals Directorate
[73] https://bit.ly/3GugXys

איומי סייבר על ענף הבריאות

14 בנובמבר – תאגיד MITRE פרסם מסמך העוסק באבטחת סייבר של מכשור רפואי – על פי המסמך שפרסם תאגיד MITRE, על ארגוני בריאות להגדיר את תחומי האחריות של גורמים האחראיים על תגובה לאירועי סייבר, בתוך ומחוץ למרכזים הרפואיים, על מנת לשפר את התקשורת עם יצרני ציוד רפואי, גופי ממשל פדראליים ומקומיים וארגוני בריאות אחרים. כמו כן, על פי הגְרְסָה הנוכחית, במקרה של זיהוי אירועי סייבר, יש ליידע על כך את יצרן המכשור שהותקף ובמידת האפשר גם את הארגון לשיתוף וניתוח מידע בנושאי בריאות (H-ISAC).[74] בנוסף, המסמך מציג טבלה בעלת ארבע קטגוריות לסיווג אירועי סייבר, כאשר הדרגה הבסיסית (קטגוריה 3) כוללת אירועים בעלי השפעה זניחה והדרגה העליונה (קטגוריה 0) כוללת אירועי סייבר חמורים, להם נדרשת תגובה מיידית. אל המסמך המרכזי צורף מסמך עזר, הכולל מקורות נוספים, אשר יכולים לסייע ביישום כלל חלקי המסמך המרכזי.[75]

16 בנובמבר – מחלקת הבריאות ושירותי האנוש האמריקנית פרסמה דו"ח המצביע על ליקויים במדיניות אבטחת הסייבר המחלקתית – משרד המפקח הכללי במחלקת הבריאות ושירותי האנוש (OIG)[76] פרסם את דו"ח הביקורת השנתי שלו, המצביע על צורך לעדכן את גישת המחלקה בנושא אבטחת סייבר, בהתאם לצו הנשיאותי שנחתם במאי 2021.[77] עדכון זה כולל, בין היתר, מעבר לארכיטקטורת רשת מבוססת על עקרונות אפס האמון. בנוסף, מחברת הדו"ח ציינה כי המחלקה הצליחה אמנם לשפר את הדרכים בהן היא אוספת, משתפת ומגנה על מידע המצוי ברשותה, אך מידת הצלחתה תלויה ביכולתה להחליף מערכות IT מיושנות ומאגרי מידע מבודדים (data silos),[78] שאינם מתאימים לעקרונות מדיניות עדכניים בניהול מידע.[79]

---

[74] Health Information Sharing and Analysis Center ; ארגון עולמי הפועל ללא כוונת רווח, ובמסגרתו ארגוני בריאות משתפים מידע על איומי אבטחה פיזית ואבטחת סייבר ומשתפים ביניהם פעולה מול איומים אלו.
[75] https://bit.ly/3VfJKLs ; קישור למסמך המרכזי: https://bit.ly/3XhiM81 ; קישור למסמך העזר: https://bit.ly/3V0XV7i
[76] HHS Office of the Inspector General.
[77] Executive Order (EO) 14028, "Improving the Nation's Cybersecurity" ; https://bit.ly/3FafigB
[78] קיומם של מאגרי מידע המבודדים משאר המחלקות שבארגונים מציבה בעיות רבות, בהן היעדר יכולת לאכוף תקנות אבטחה מידע עליהם.
[79] https://bit.ly/3OzDzj8

18 בנובמבר – הממשל האמריקני פרסם אזהרה מפני מתקפות סייבר של קבוצת עבריינים כופרה Hive על ארגוני בריאות – CISA, ה-HHS וה-FBI פרסמו אזהרה, לפיה בתקופה שבין יוני 2021 לנובמבר 2022, קבוצת עבריינים הכופרה Hive תקפה 1,300 ארגונים מרחבי העולם, ביניהם מוסדות בריאות רבים. במסגרת תקיפותיה, עושה קבוצת Hive שימוש בטכניקות שונות, בהן ניצול פרוטוקולי RDP לגישה מרחוק ושימוש ב-VPN.[80] שלושת הגופים המליצו לארגונים, בייחוד אלו השייכים למגזר הבריאות, להתקין עדכוני תוכנות באופן שוטף ובייחוד אלו השייכים לשרתי VPN, תוכנות לגישה מרחוק ותוכנות לניהול מערכות וירטואליות (Supervisors). בנוסף, הסוכנויות המליצו לארגונים ליישם אימות רב-שלבי בשירותים רבים ככל הניתן. בד בבד, על הארגונים לאבטח פרוטוקולי RDP על ידי הגבלת הגישה למשאבים פנימיים ובחינת ההגדרות התקינות של מכשירים. לבסוף, יש להבטיח כי כלל המידע המצוי בארגון מוצפן ולא ניתן לשינוי או למחיקה.[81]

24 בנובמבר – שוודיה חנכה מעבדה לחקר איומי סייבר על כלי רכב המחוברים לרשת – מכון המחקר של שוודיה (RISE),[82] הנמצא בבעלות ממשלת שוודיה, השיק את מעבדת ה-RISE Cyber Test Lab for Automotive, שתאפשר לבחון את אבטחת הסייבר של כלי רכב המחוברים לרשת בשיתוף מומחי תקשורת והאקרים white hats. במסגרת פעילותה, תתמקד המעבדה באבחון אבטחת הסייבר של תוכנות המוטמעות בכלי רכב (ECU)[83] ותוכנות עבור כלי רכב הנמצאות בענן, תוך שימוש במודלים תאומים דיגיטליים (digital twins),[84] בחינת מערכות מִשְׁנֶה ובחינת רכבים בסביבות מבוקרות. המעבדה צפויה לפעול בהיקף מלא בתחילת 2023, כאשר עד למועד זה היא תקיים הדמיות של מתקפות סייבר על כלי רכב ועל תשתיות טעינת רכבים חשמליים.[85]

---

[80] Remote Desktop Protocol
[81] https://bit.ly/3EwYyhP ; קישור לאזהרה : https://bit.ly/3U9iVr3
[82] Research Institutes of Sweden
[83] embedded software in vehicle units
[84] מודלים וירטואליים שנועדו לדמות אובייקטים פיזיים.
[85] https://bit.ly/3ENCLCB

2 בנובמבר – האיחוד האירופי הנחה את חברות התעופה ביבשת להקים מערך למעקב ולהתמודדות עם איומי סייבר – ההנחיה, שגובשה על ידי הסוכנות האירופית לבטיחות בתעופה (EASA),[86] צפויה לחול על גורמים רבים במגזר התעופה, בהם חברות תעופה, נמלי תעופה, יצרניות מטוסים ובתי ספר לטיסה וצפויה להיכנס לתוקף בשנת 2025. במסגרת ההנחיה, על גופי הענף לעשות שימוש בתוכנות לזיהוי ומעקב אחר איומי סייבר, שעלולים לפגוע בבטיחות הטיסות וליישם אמצעי הגנה למניעתם. הפיקוח על יישום דרישה זו יבוצע על ידי רשויות התעופה הלאומיות וכן באמצעות בעל תפקיד ייעודי, אשר ימונה בכל חברה בענף התעופה. לדברי מנהל התפעול הראשי של אגודת התעופה העסקית באירופה (EBAA),[87] רוברט באלטוס (Robert Baltus), יישום הדרישה עלול להשית עלויות רבות על חברות תעופה, שיצטרכו עקב כך להקצות משאבים למינוי גורמים שיפקחו על השימוש במערכת, שיכשירו עובדים לעשות בה שימוש ולרכוש אמצעים המרכיבים אותה.[88]

7 בנובמבר – הלשכה האמריקנית לספנות תבנה עבור סינגפור מודלים וירטואליים לבחינת אבטחת הסייבר של ציוד OT בכלי שיט – הלשכה האמריקנית לסַפָּנוּת (ABS)[89] צפויה לבנות עבור המרכז לחקר אבטחת סייבר במרכז המחקר iTrust שבאוניברסיטה של סינגפור לטכנולוגיה ולעיצוב (SUTD)[90] והמרכז למצוינות בבטיחות ימית (CMES)[91] סדרת מודלים וירטואליים של רשתות טכנולוגיות עבור כלי שיט, למטרת בחינת אבטחת הסייבר של ציוד OT. בניית הרשתות נעשית כחלק מפרויקט MariOT,[92] שמטרתו לפתח טכנולוגיות אבטחת סייבר חדשות להגנה על מערכות OT בכלי שיט.[93]

---

[86] European Union Aviation Safety Agency
[87] European Business Aviation Association
[88] https://bit.ly/3XmGcsw ; https://on.wsj.com/3EwNscy
[89] American Bureau of Shipping, ארגון א-ממשלתי העוסק בקידום תקנים לתכנון, בנייה והפעלה של כלי שייט.
[90] Singapore University of Technology and Design
[91] Centre of Excellence in Maritime Safety
[92] Maritime Testbed of Shipboard Operational Technology Systems project
[93] https://bit.ly/3VA2xkB

איומי סייבר על ענף הפיננסים

15 בנובמבר – חברת IT אמריקנית פרסמה ממצאים בנושא מעבר לענן בקרב ארגונים במגזר הפיננסי – על פי ממצאים שפרסמה חברת ה-IT האמריקנית Netwirx,[94] שלושת האתגרים המרכזיים העומדים בפני ארגונים במגזר הפיננסי במעבר לתשתיות ענן הם היעדר מומחיות מקצועית בנושא, פערי כוח אדם בקרב צוותי ה-IT וצוותי האבטחה וחוסר נראות של נתונים רגישים הנמצאים בענן. בנוסף, 61% מהמשיבים לסקר עליו התבססו הנתונים טענו כי במהלך השנה החולפת חוו מתקפות סייבר נגד תשתיות הענן בהן הם השתמשו, וכן כי תקיפות דיוג היו שיטות התקיפה הנפוצות ביותר. כמו כן, שלושת האמצעים השכיחים ביותר שארגונים יישמו על מנת להגן על המידע שבענן היו הטמעת אימות רב שלבי, הצפנה וניהול גיבויים.[95]

28 בנובמבר – הפרלמנט האירופי אישר שתי דירקטיבות בנושא אבטחת סייבר של תשתיות חיוניות ומוסדות פיננסיים – הפרלמנט האירופי אישר את דירקטיבת DORA,[96] הכוללת דרישות בנושא אבטחת הסייבר עבור ארגונים במגזר הפיננסי, כגון בנקים, חברות ביטוח ובתי השקעות וכן כלפי חברות המספקות להם שירותי ICT, כגון ספקי שירותי ענן.[97] במסגרת הדירקטיבה, על כלל החברות לבצע פעם בשנה מבדקי חדירות למערכות ICT חיוניות על ידי בוחנים חיצוניים.[98] בד בבד, אישר הפרלמנט את דירקטיבת NIS2 לאבטחת סייבר על תשתיות ושירותים חיוניים, שתחליף את דירקטיבת NIS שנכנסה לתוקף בשנת 2016 ושתיצור אחידות בנושא בקרב מדינות האיחוד. במסגרת הדירקטיבה, הארגונים הכפופים לה יידרשו ליישם מספר צעדים כלליים בתחום אבטחת סייבר, כגון בחינת חולשות אבטחה בשרשראות אספקה. יחד עם זאת, דרישות האבטחה המדויקות שכל ארגון נדרש ליישם למטרת עמידה בהוראות הדירקטיבה תלויות במאפייניו הייחודיים, כגון גודלו ומידת חשיפתו לסיכוני סייבר.[99] כמו כן, תוקם הרשת האירופית לניהול משברי סייבר (EU-CyCLONe),[100] שתהיה אחראית על תיאום התגובה לתקריות סייבר המתרחשות בקנה מידה רחב.[101]

---

[94] הממצאים מהווים עדכון לדו"ח שפרסמה החברה מוקדם יותר השנה.
[95] https://bit.ly/3gv12p0 ; קישור לממצאים: https://bit.ly/3EytCxF
[96] Digital Operational Resilience Act
[97] https://bit.ly/3OP8NTx
[98] https://bit.ly/3AYChsl
[99] https://bit.ly/3u8HFW6
[100] European Cyber Crises Liaison Organisation Network
[101] https://bit.ly/3gMASOJ

9 בנובמבר - חברת Arianespace צפויה לשגר ברבעון האחרון של 2024 לוויין לביצוע ניסויים בהפצה קוונטית של מפתחות הצפנה עבור סוכנות החלל של אירופה – שיגור הלוויין Eagle-1 צפוי להתבצע ברבעון האחרון של שנת 2024, במסגרת הסכם שנחתם בספטמבר 2022 בין סוכנות החלל האירופית (ESA)[102] לבין תאגיד חברות בהובלת חברת התקשורת מלוקסמבורג, SES. במסגרת ההסכם, יפתח התאגיד את הלוויין במטרה שישמש לביצוע ניסויים בהפצה קוונטית והחלפת מפתחות הצפנה (QKD).[103] הלוויין צפוי לפעול במסלול במשך שלוש שנים ושיגורו יאפשר ל-ESA להקים מערכת חלל אירופית ראשונה מבוססת QKD, שתאפשר העברת נתונים ברמת אבטחה גבוהה ושמלבד הלוויין תכלול גם מרכז תפעולי שיוקם בלוקסמבורג.[104]

18 בנובמבר – הבית הלבן פרסם מזכר חדש בנושא מעבר הממשל הפדראלי לשימוש בהצפנה פוסט-קוונטית – המשרד לניהול ולתקציב (OMB)[105] פרסם מִזְכָּר חדש הכולל רשימת צעדים מקדימים שעל סוכנויות פדראליות לבצע במסגרת תהליך המעבר לשימוש בפתרונות להצפנה פוסט-קוונטית. על פי המִזְכָּר, עד ל-4 במאי 2023, על הסוכנויות לשלוח למשרד ראש המודיעין הלאומי (ONCD), למחלקה לביטחון המולדת ול-CISA רשימות מצאי, שיכללו פרטים על מערכות חומרה ותוכנה מבוססות הצפנה שברשותן, תוך התמקדות בנכסים בעלי ערך גבוה המחייבים יישום צעדי אבטחה נוספים. בנוסף, בכל שנה, על הסוכנויות לשלוח ל-OMB ול-ONCD הערכות לגבי היקף התקציב הנחוץ להן, על מנת לעבור לשימוש במערכות ובפתרונות להצפנה פוסט-קוונטית במהלך השנה הפיסקאלית העוקבת. בד בבד, CISA, בשיתוף עם NIST ותוכנית ה-FedRAMP,[106] ייסדו תהליך שיבסס חילופי מידע בין סוכנויות ממשל והמגזר הפרטי, בנושא בחינת ציוד להצפנה פוסט-קוונטית שטרם עבר תקינה.[107]

---

[102] European Space Agency

[103] Quantum Key Distribution, משמש כשיטה להחלפה והפצת מפתחות, המתבססת על עקרונות פיזיקאליים ממכניקת הקוונטים, עקרון השימוש מבוסס על יצירה משותפת של מפתח פרטי סימטרי בין שני הצדדים באמצעות ערוצים קוונטים וערוצים קלאסיים (סיבים אופטיים או ערוצים אלחוטיים); https://bit.ly/3FC4HKr

[104] https://bit.ly/3tIyV8Z

[105] Office of Management and Budget

[106] Federal Risk and Authorization Management Program; FedRAMP היא תוכנית ממשלתית שמטרתה לספק גישה אחידה להערכת מצב האבטחה וניטור מתמשך של מוצרי ושירותי ענן. התוכנית כוללת שורת בקרות אבטחה להגנה על מידע ועל מערכות בענן.

[107] https://bit.ly/3U1IaLZ ; קישור למִזְכָּר: https://bit.ly/3EWupKk

מטבעות דיגיטליים

16 בנובמבר – סוכנות דירוג האשראי Moody's פרסמה דו"ח בנושא איומי סייבר על מטבעות דיגיטליים – על פי הדו"ח, אחת הסיבות לאיום הסייבר הגובר על ענף המסחר במטבעות דיגיטליים הוא השימוש בפרוטוקול DeFi,[108] המשתמש בחוזים חכמים (smart contracts) על מנת לתת למשתמשים גישה לשירותים פיננסיים.[109] פרוטוקולים אלו מבוססים על קוד פתוח, דבר שמאפשר להאקרים לאתר במהירות חולשות אבטחה ולנצלן. זאת, בניגוד ליישומים מסורתיים יותר, בהם החולשות עשויות להישאר חבויות במשך זמן רב. בנוסף, מחברי הדו"ח הצביעו על כך, שבעוד שבשנת 2018, 5% מכלל מתקפות הסייבר בתחום המטבעות הדיגיטליים בוצעו נגד פרוטוקול DeFi, הרי שבשנת 2022 הן היוו 90% מהן. הגידול במתקפות יכול להיות מוסבר בשימוש המרובה בחוזים חכמים ובעובדה שרכיבים מבוזרים בפלטפורמת DeFi מחזיקים סכומים גדולים של כסף. בנוסף, חברות הזנק רבות המתמחות בפלטפורמת DeFi, ממהרות להפיץ את מוצריהן לשוק מבלי לבחון קודם לכן את אבטחת הסייבר שלהם באופן ראוי. מחברי הדו"ח הציגו אמצעים שונים להתמודדות עם האיומים, בהם קיום תחרויות לאיתור חולשות אבטחה (bug bounty) והקמת צוותי תגובה מהירה לתקריות.[110]

שיתופי פעולה

8 בנובמבר – יחידת סייבר משטרתית בהודו קיימה סדרת הכשרות משותפת עם צרפת למטרת מאבק בפשעי סייבר – היחידה למאבק בפשעי סייבר של משטרת דלהי (Delhi) (IFSO),[111] בשיתוף פעולה עם המרכז לתיאום המאבק בפשעי סייבר של הודו (I4C)[112] ושגרירות צרפת בהודו, קיימו סדרת הכשרות בת שלושה ימים להיערכות למאבק בתקריות של פשיעת סייבר ולפיתוח אסטרטגיות ושיטות חקירה לגילוי ולהתמודדות עם פשעי הסייבר ברמה בין-לאומית.

---

[108] Decentralized Finance; פלטפורמות המסייעות לבצע פעולות פיננסיות בין גורמים אנושיים, שבנסיבות אחרות מצריכות שימוש בגורם שלישי ומסורתי, כגון בנק או תַּוָּכָן (ברוקר). להרחבה, ראו: https://bit.ly/3L8Ooa3

[109] חוזה דיגיטלי מבוזר על רשת Blockchain, המסוגל לקבל ולשדר נתונים ולבצע פעולות מסוימות, למשל, העברת כספים בתנאים מסוימים, באופן אוטומטי.

[110] https://bit.ly/3ACi2R8 ; https://bit.ly/3i5ThGJ

[111] The Intelligence Fusion and Strategic Operations unit of Delhi Police

[112] The Indian Cyber Crime Coordination Centre

שלושה מומחי סייבר מצוות חקירות פשעי הסייבר הצרפתי, שני אנשי צוות התמיכה של השגרירות הצרפתית ושלושה מומחי סייבר מהודו ניהלו את סדרת ההכשרות.[113]

10 בנובמבר – בריטניה, קנדה וסינגפור הודיעו על שיתוף פעולה לשיפור אבטחת סייבר בקרב מכשירי ה-IoT – ממשלות בריטניה, קנדה וסינגפור, הכריזו כי יפעלו לקידום ניסוח של תקנים בין-לאומיים והנחיות משותפות למגזר התעשייתי, לטובת עמידה בדרישות אבטחה מוכרות ומתואמות ברמה הבין-לאומית עבור מכשירי ורשתות IoT. הממשלות הדגישו עוד את חשיבות קידום המאמץ המתואם בין גורמי ממשל, אקדמיה וחברה אזרחית באימוץ התקנים הבין-לאומיים כדי להפחית סיכוני סייבר על מכשירי ורשתות IoT.[114]

10 בנובמבר – נאט"ו קיימה את וועידת הגנת הסייבר לשנת 2022 – ארצות הברית, איטליה והצוות הבין-לאומי של מדינות ברית נאט"ו (IS),[115] קיימו את וועידת הגנת הסייבר לשנת 2022. במסגרת הוועידה, התמקדו נציגי המדינות בדיון על חוסן, מוכנות ותגובה לאיומי סייבר על תשתיות חיוניות, ברמה הלאומית ובמסגרת מדינות הברית. בפתיחת הוועידה, הזהיר מזכ"ל נאט"ו, ינס סטולטנברג (Jens Stoltenberg), מפני איומי הסייבר הגוברים בעולם, הדגיש את תמיכתה ומחויבותה של ברית נאט"ו לאוקראינה, וקרא לחברות הברית להתחייב לעקרונות הגנת סייבר בין-לאומית משותפת למען הגברת ההגנה הקולקטיבית של הברית.[116] בנוסף, סגנית היועץ לביטחון לאומי לענייני סייבר וטכנולוגיות מתפתחות בממשל האמריקני, אן נויברגר (Anne Neuberger), הדגישה את חשיבותה של תגובה אקטיבית ומהירה מצד חברות נאט"ו למתקפות סייבר שחוות יתר חברות הברית, ואת חשיבות ההשקעה בתחום אבטחת סייבר, על רקע מתקפות סייבר מצד רוסיה על אוקראינה.[117]

---

113 https://bit.ly/3hV72rm
114 https://bit.ly/3hSYn94
115 International Staff. ה-IS מספק שירותי ייעוץ, הדרכה ותמיכה מנהלית לחברות נאט"ו, ואחראי על תכנון ומעקב אחר פעולות המועצה הצפון-אטלנטית של נאט"ו (North Atlantic Council).
116 https://bit.ly/3tIGXyo
117 https://bit.ly/3Gs08El ; https://bit.ly/3ghQidy