דו"ח מדיניות וביטחון סייבר

אוקטובר 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
היערכות לבחירות לקונגרס נובמבר 2022..... 6
צבא ובטחון..... 6
אירופה..... 8
סיכום זירת הסייבר ברקע הפלישה הרוסית לאוקראינה..... 8
אסיה..... 11
דרום קוריאה..... 11
סינגפור..... 11
אפריקה והמזרח התיכון..... 12
איראן..... 12
האוקיינוס השקט..... 12
אוסטרליה..... 12
ביטחון סייבר..... 13
איומי סייבר על תשתיות חיוניות..... 14
איומי סייבר על שרשראות אספקה..... 16
איומי מתקפות הכופרה..... 17
איומי סייבר על ענף האנרגיה..... 17
איומי סייר על ענף הבריאות..... 18
איומי סייבר על ענף התחבורה..... 18
איומי סייבר על ענף התעופה..... 19
איומי סייבר על מערכות חלל..... 19
בינה מלאכותית..... 20
מחשוב קוונטי..... 20
שיתופי פעולה..... 21
השפעה, הטיית דעת קהל והסתה..... 22

תקציר חודשי

הממשל האמריקני הודיע על הוספת התעשייה הכימית לתוכנית הנשיאותית הוולונטרית להגנה על מערכות בקרה בתשתיות חיוניות משנת 2021, ICS Cybersecurity Initiative. בנוסף, הבית הלבן מתכוון להשיק תוכנית לאומית חדשה לדירוג מידת האבטחה של מכשירי IoT; סוכנויות ממשל וגופי אכיפה בארה"ב פרסמו אזהרות מפני קבוצות האקרים המזוהות עם סין ואיראן, שעלולות לנסות לפגוע בטוהר הליך הבחירות לקונגרס האמריקני בחודש נובמבר 2022, אולם ציינו כי עד כה, לא נצפו תקריות סייבר שפגעו ביכולת ההצבעה של בוחרים; חיל האוויר האמריקני יזם מחקר שוק המיועד לסייע בפיתוח תוכנית הכשרות בתחום לוחמת מידע וסייבר בשיתוף התעשייה.

ברקע המלחמה המתמשכת באוקראינה, אמר ראש מִינְהֶלֶת אבטחת הסייבר של ה-NSA, רוב ג'ויס (Rob Joyce) כי אחד הלקחים המרכזיים שהסוכנות למדה מהמלחמה הוא הצורך לשתף עם ספקי טכנולוגיה ותשתיות חיוניות והמגזר הפרטי מידע מודיעיני באופן יזום, לשם שיפור אבטחת הסייבר של אותם ארגונים וברמה הלאומית.

קבוצות האקרים המתנגדות למשטר האיראני פרצו לארגון לאנרגיה אטומית ולרשת הטלוויזיה הממלכתית במדינה; ברקע איומי צפון קוריאה, השתתפה דרום קוריאה לראשונה בתרגיל הגנת הסייבר הרב-לאומי השנתי של פיקוד הסייבר האמריקני, Cyber Flag; סינגפור השיקה תוכנית מורחבת לדירוג מידת אבטחת הסייבר של מכשירי IoT רפואיים וכן הקימה כוח משימה חדש למאבק באיומי מתקפות הכופרה; בכוונת אוסטרליה לנסח חוקים חדשים להגדלת הקנסות על דליפות מידע חמורות בקרב חברות פרטיות.

היורופול (Europol) פרסם דו"ח המציג משמעויות השימוש בפלטפורמת מטאברס (Metaverse) על פשיעת סייבר; ארגון אבטחת מידע בריטי הפועל ללא כוונת רווח השיק תוכנית לפיתוח כוח אדם מיומן במקצועות הסייבר במגזר האנרגיה הגרעינית האזרחית; המרכז הלאומי לאבטחת סייבר של בריטניה (NCSC) פרסם מסמך בנושא הגנה על שרשראות אספקה מפני איומי סייבר; חיל האוויר האמריקני חתם על חוזה בסך 22 מיליון דולר לטובת בניית מחשב קוונטי מתקדם; צוותי סייבר מצבאות ארה"ב ומספר מדינות מהמזרח התיכון השתתפו בתרגיל הגנת סייבר משותף לשם איתור חולשות ופעילות זדונית ברשת. בנוסף, רשויות אכיפת חוק באירופה עצרו עשרות בני אדם החשודים שהשתמשו בתוכנת מזויפת המתחזה לתוכנה לאיתור תקלות ברכב לשם גניבת כלי רכב ללא שימוש במַפְתֵחַ התנעה; תורכיה סייעה לפקיסטן להקים בחשאי יחידת סייבר למטרת השפעה על דעת הקהל בקרב מוסלמים בדרום-מזרח אסיה וכנגד ארה"ב והודו.

ממשל, אסטרטגיה ומדיניות

3 באוקטובר – משרד ראש הסייבר הלאומי פרסם בקשה למידע בנושא הכשרת כוח אדם מיומן במקצועות אבטחת הסייבר – משרד ראש הסייבר הלאומי (ONCD) פרסם בקשה למידע לטובת סיוע בגיבוש האסטרטגיה להכשרת כוח אדם מיומן במקצועות אבטחת הסייבר,[1] עליה הכריז ראש הסייבר הלאומי (NCD), כריס אינגליס (Chris Inglis) ביולי 2022. במסגרת הבקשה למידע, פנה ה-ONCD לקבל הצעות לשיטות עבודה מומלצות שעשויות לסייע לממשל הפדראלי להוביל, לתמוך ולעודד גורמי ממשל, תעשייה, ארגונים ללא כוונת רווח ואקדמיה לקדם הכשרה, חינוך ופיתוח של כוח אדם בעל רקע אתני ומגדרי מגוון, המיומן במקצועות אבטחת הסייבר. הבקשה למידע מדגישה עוד את כוונת ה-ONCD לוודא כי עובדי הממשל הפדראלי יהיו מודעים לנושא אבטחת הסייבר, גם אם הם אינם מאיישים תפקידים בתחום. ה-ONCD ביקש לקבל מידע עד ה-3 בנובמבר 2022 ולאחר מכן, יערוך המשרד מפגשים וירטואליים עם משיבים נבחרים כדי לדון איתם בהצעותיהם.[2]

4 באוקטובר – CISA פרסמה דירקטיבה העוסקת באיתור ודיווח חולשות אבטחה בנכסי IT בקרב סוכנויות פדראליות אזרחיות – על פי הדירקטיבה, סוכנויות ממשל אזרחיות יידרשו עד ל-3 באפריל 2023 להשתמש באמצעים אוטומטיים לזיהוי מערכות IT בכל שבעה ימים, לבצע סריקה (enumerate) לשם איתור חולשות במערכות ה-IT בכל 14 יום, להזין את פרטי החולשות שנמצאו אל לוח בקרה ייעודי של הסוכנות לאבטחת סייבר ותשתיות (CISA) בתוך 72 שעות מזמן גילוין,[3] לפתח יכולות להיענות לדרישות CISA לבצע סריקת חולשות אבטחה תוך 72 שעות מזמן הגשת הבקשה ולהחזיר את תוצאות הסריקה תוך שבעה ימים מקבלת הבקשה. כמו כן, הצהירה CISA כי בכוונתה לפרסם נוהל, שינחה את הסוכנויות הפדראליות כיצד יש לדווח על חולשות אבטחה שנמצאו. בנוסף, בסוף כל שנה פיסקאלית תדווח CISA למחלקה לבטחון המולדת, למשרד לניהול ותקציב (OMB)[4] ולראש הסייבר הלאומי על יישום הדירקטיבה וממצאיו.[5]

---

[1] Cybersecurity workforce, training, and education strategy.
[2] https://bit.ly/3Dnoc9q ; הקישור לבקשה למידע: https://bit.ly/3TPMA9k
[3] Continuous Diagnostics and Mitigation (CDM) dashboard; לוח בקרה המסייע לסוכנויות פדראליות להתמודד טוב יותר עם איומי סייבר.
[4] Office of Management and Budget
[5] https://bit.ly/3eOkEDN ; קישור לדירקטיבה: https://bit.ly/3U9CPmu

6 באוקטובר – חברת אבטחת סייבר ספרדית זכתה בחוזה בסך 26 מיליון דולר לשם זיהוי וניטור פעילות זדונית ברשתות הממשל הפדראלי ומחלקת ההגנה – חברת אבטחת הסייבר הספרדית, CounterCraft זכתה בחוזה בסך 26 מיליון דולר, במסגרתו, תספק החברה למחלקת ההגנה ולסוכנויות ממשל נוספות יכולות זיהוי והתרעה מפני גישה לא מורשית או פריצה לרשתות הממשל הפדראלי ולמידה על דרכי הפעולה של האקרים בזמן אמת; סיוע בהטמעת הפלטפורמה ברשתות הממשל עם יכולת להוסיף לה רכיבים חדשים בעתיד; הכשרת סוכנויות ממשל כיצד לפרוס ולהשתמש בפלטפורמה כדי להעצים את יכולות איסוף מודיעין האיומים בנושא הטכניקות והטקטיקות (TTPs) של גורמי איום שונים. החברה מספקת פלטפורמת הטעיה (Distributed deception platform), המאפשרת לייצר מלכודות Honeypots וללמוד על דפוס הפעולה של התוקפים.[6]

17 באוקטובר – המחלקה לבטחון המולדת פרסמה בקשה למידע בנושא רכש שירותים בתחומי ניהול תשתית ענן ואבטחת סייבר – המחלקה לבטחון המולדת פרסמה בקשה למידע בנושא רכישת שירותי ענן, ניהול רשתות ואבטחת סייבר עבור מרכז התפעול ואבטחת הרשת המאוחד של המחלקה (NOSC),[7] שעל הקמתו הכריזה בספטמבר 2020. במסגרת הבקשה, מעוניינת המחלקה לאתר גורמים בתעשייה שיכולים לספק שירותי ניהול תשתיות ושירותי ענן, ניהול רשתות ומערכות ושירותי תמיכה בתחום אבטחת סייבר, עבור מתקני NOSC הממוקמים בוושינגטון הבירה (Washington D.C.), מדינת מיסיסיפי (Mississippi) ומדינת אריזונה (Arizona). בנוסף, ביקשה המחלקה משוב מהתעשייה על המבנה המוצע של המרכז המגבש את תחומי אחריותו וכן בנושא כמות כוח האדם המינימלית הנדרשת לטובת תפעולו.[8]

20 באוקטובר – בכוונת ממשל ביידן להשיק תוכנית לאומית חדשה לשיפור האבטחה של מכשירי IoT – על פי הודעת דובר מועצת הביטחון הלאומית, בכוונת ממשל ביידן להשיק באביב 2023 תוכנית חדשה לשיפור אבטחת סייבר בקרב מכשירי IoT. במסגרת התוכנית שתנוסח בהתייעצות עם חברות הטכנולוגיה הגדולות ואיגודי מסחר בארה"ב, מכשירי IoT ידורגו באמצעות תוויות קלות לזיהוי, שיאפשרו לצרכנים אמריקנים וברחבי העולם להגביר את מודעותם לסיכוני אבטחה ולעשות שימוש בטוח בהתקנים בביתם. כמו כן, כוללת התוכנית תמריצים עבור יצרנים וקמעונאים לייצר ולשווק מוצרים העומדים בתקני האבטחה של ממשלת ארה"ב וגורמים מוסמכים אחרים. התוכנית תתמקד תחילה בנתבים ובמצלמות ביתיות, הנפוצים בשימוש ביתי.[9]

---

[6] https://bit.ly/3Tn31dk ; https://bit.ly/3TlNE4O

[7] Network Operations and Security Center, יורכב מששת מרכזי תפעול הרשת (NOCs) וחמישה מרכזי תפעול האבטחה של המחלקה (SOCs). המרכז המתהווה יסייע בזיהוי, הגנה, תכנון תגובה והתאוששות מכלל סוגי אירועי IT ברשתות המטה של המחלקה לבטחון המולדת ומערכות עיבוד המידע שלה.

[8] https://bit.ly/3D1DuiT ; https://bit.ly/3Tyi8AD ; קישור לבקשה למידע: https://bit.ly/3TulYur

[9] https://bit.ly/3Ttib0F ; https://bit.ly/3SrNIP6

27 באוקטובר – הבית הלבן הודיע כי ירחיב את התוכנית הנשיאותית להגנה על מערכות לבקרה תעשייתית

גם לענף תעשיית הכימיקלים – הבית הלבן הודיע כי ירחיב את יוזמת ה-ICS Cybersecurity Initiative הוולונטרית לענף תעשיית הכימיקלים.[10] מטרת התוכנית, שצפויה להימשך כ-100 ימים, היא לסייע לגופי התעשייה להעריך את מצב אבטחת הסייבר שלהם ולהפיק לקחים שנלמדו במסגרת הטמעת היוזמה בקרב ארגונים בענפי החשמל, המים וצינורות הדלק. כמו כן, תעודד היוזמה את מפעילי המערכות להטמיע אמצעי אבטחה וזיהוי אנומליות במערכות ה-ICS תוך התמקדות בהגנה על מתקנים המצויים ברמת סיכון גבוהה. בנוסף, תעודד התוכנית שיתוף מודיעין ושיתוף פעולה בניתוח מצב אבטחת הסייבר בין תעשיית הכימיקלים והממשל הפדראלי ובקידום שיתופי פעולה בין גורמים בכירים בענף לבין בעלי מפעלים, לשם הטמעת אמצעי אבטחה, המותאמים באופן פרטני לארכיטקטורה של כל מפעל.[11]

27 באוקטובר – המחלקה לבטחון המולדת פרסמה טיוטת מסמך עקרונות אבטחת סייבר למנהלי מצבי חירום

– הסוכנות הפדראלית לניהול מצבי חירום (FEMA)[12] פרסמה לתגובות הציבור טיוטת מסמך, המיועד לסייע לגופים ברמה המקומית (local) וברמת המדינה (state) שתפקידם להתמודד עם מצבי חירום, להיערך לאיומי סייבר הרלוונטיים להם. מחברי המסמך הציגו את השלבים אותם מנהלי מצבי חירום צריכים ליישם, על מנת לגבש תוכנית אבטחת סייבר המותאמת לצרכיהם, בהם קידום שותפויות, תקשורת ומְעוֹרְבוּת מצד בעלי ומפעילי שירותים חיוניים; הערכת סיכוני סייבר לשירותים חיוניים; ויצירת סדר עדיפויות בהגנה על המערכות והרכיבים של התשתיות החיוניות; הגדרת תפקידים ותחומי אחריות; ופיתוח תוכנית תגובה לאירועי סייבר. בנוסף, המסמך מציג הנחיות בנושא תקשורת והעברת מסרים בזמן אירועי סייבר הכוללות את נושא תיאום המסרים בין הגורמים הרלוונטיים ואת נושא פרסומם לציבור.[13]

[10] היוזמה הושקה ביולי 2021 במטרה לשפר את אבטחת הסייבר של מערכות ICS בענפי החשמל, צינורות הדלק והמים, באמצעות הטמעת אמצעי ניטור אנומליות, מעקב אחר אירועי אבטחה ושיתוף מידע בין מפעילי מערכות ICS לבין הרשויות ובעלי עניין נוספים.
[11] https://bit.ly/3zt2q1w
[12] Federal Emergencies Management Agency
[13] https://bit.ly/3WesTd0 ; קישור למסמך: https://bit.ly/3SQHxV9

היערכות לבחירות לקונגרס נובמבר 2022

5 באוקטובר – סוכנויות ממשל וגופי אכיפה פרסמו הערכות ואזהרות בנושא איומי סייבר על בחירות אמצע הקדנציה – ב-5 באוקטובר, פרסמו ה-FBI ו-CISA הודעה משותפת לפיה מתקפות סייבר כנגד תשתיות מערכת הבחירות לא צפויות לגרום לשיבושים משמעותיים או לפגיעה ביכולת ההצבעה של בוחרים. הסוכנויות ציינו כי עד כה לא נצפתה או דווחה פעילות סייבר שמנעה מבוחרים להצביע, פגעה באמינות ההצבעות או בדיוק של מידע רישום הבוחר. כמו כן, הסוכנויות הציגו המלצות לסיכול ניסיונות התערבות בבחירות, בהן הסתמכות על מקורות רשמיים וממשלתיים לקבלת מידע בנושאי רישום והצבעה.[14] לצד זאת, ב-6 באוקטובר, קבוצת ההאקרים הפרו-רוסית, Killnet, לקחה אחריות על תקיפת סייבר שהובילה להשבתה זמנית של אתר האינטרנט של מועצת הבחירות במדינת קנטאקי (Kentucky), בו מתפרסם מידע על דרכי הרישום של בוחרים להצבעה.[15] בד בבד, ב-8 באוקטובר, הזהיר ה-FBI כי האקרים סינים סורקים את רשתות המטות של המפלגות הדמוקרטית והרפובליקנית הפועלים במדינות ארה"ב לשם איתור מערכות פגיעות אליהן הם עלולים לפרוץ לפני הבחירות לקונגרס.[16] ב-21 באוקטובר, פרסם ה-FBI אזהרה, לפיה קבוצת האקרים המזוהה עם המשטר האיראני, Emennet Pasargad, שבה לפעילות, לאחר שבעבר ניסתה להתערב בבחירות לנשיאות 2020.[17] על רקע זה, הציעה מחלקת המדינה פרס בסך עשרה מיליון דולר עבור קבלת מידע אודות חברי Emennet Pasargad כחלק מתוכנית Rewards for Justice,[18] שמנהלת המחלקה.[19]

צבא ובטחון

14 באוקטובר – דארפ"א הודיעה על בחירת שמונה צוותים עבור תוכנית לפיתוח כלים לחיזוי חולשות אבטחה – במסגרת תוכנית HARDEN,[20] המתוכננת להימשך ארבע שנים, צוותים משמונה מוסדות מחקר וחברות אבטחת סייבר יפתחו כלים ושיטות לחיזוי התנהגות מצד תוכנות שעלולה להוביל להופעתן של חולשות אבטחה, ולהגנה על תוכנות לאורך כל מחזור חייהן.[21] במסגרת התוכנית צפויים להשתתף גם האקרים white hats, שצפויים לספק מידע על דרכי תקיפה פוטנציאליות.[22]

---

[14] https://bit.ly/3zsybb9 ; https://bit.ly/3TMJz9X ; קישור להודעה: https://bit.ly/3sLOZpU
[15] https://cnn.it/3eGurMg
[16] https://bit.ly/3zjrisT
[17] באוקטובר 2020, ה-FBI הכריז כי המודיעין האיראני אחראי לניסיון השפעה על בחירות 2020 בארה"ב, כאשר מצביעים דמוקרטים שנרשמו להצביע במדינת פלורידה קיבלו בשבועות שלפני הבחירות מיילים מאיימים שהורו להם לעבור למפלגה הרפובליקנית. החתומים לכאורה על הודעת הדוא"ל היו קבוצת The Proud Boys, ארגון ימני קיצוני של תומכי טראמפ.
[18] תוכנית ללוחמה בטרור של שירות הביטחון הדיפלומטי של מחלקת המדינה. כחלק מהתוכנית מוצעים תגמולים כספיים עבור מידע שמסייע בסיכול פעולות טרור בינלאומיות נגד ארה"ב.
[19] https://nbcnews.to/3DjEYF5 ; קישור לאזהרת ה-FBI: https://bit.ly/3Noz3DD
[20] Hardening Development Toolchains Against Emergent Execution Engines
[21] https://bit.ly/3gdU8UE
[22] https://bit.ly/3yPdYMj

מלבד הצוותים שנבחרו, חברת אבטחת הסייבר האמריקנית, Cromulence ואוניברסיטת אילינוי באורבנה-שמפיין (University of Illinois Urbana-Champaign) יבחנו את יעילותם של האמצעים שיפותחו על ידי הצוותים.[23]

<u>17 באוקטובר – צבא היבשה פרסם תוכניות העוסקות בשימוש בתשתיות ענן ובניהול וניתוח מאגרי מידע</u> – מטרתה העיקרית של התוכנית הראשונה היא להרחיב את תשתית הענן של צבא היבשה וליישם בה את עקרונות ארכיטקטורת אפס האמון שתאפשר לצבא להעביר נתונים בין היחידות השונות הפרוסות ברחבי העולם תוך שימוש בחומרה לשימוש מסחרי ובתקשורת לוויינים. כמו כן, בכוונת צבא היבשה להרחיב את תשתיות הענן שבשימושו ואת כוח האדם המיומן בטכנולוגיות ענן. התוכנית השנייה מבוססת על ההנחה, שיש לפתח את השימוש במאגרי מידע וניתוחם, על מנת להעניק לצבא מיומנויות שיסייעו לו במלחמות העתיד, כגון קבלת החלטות במהירות גבוהה. אחת המשימות הכלולות בתוכנית היא קיום תרגילים בהשתתפות מספר מצומצם של יחידות, מהם יהיה ניתן לגזור מסקנות לגבי הצבא כולו.[24] נוסף על כך, הודיע מנהל המידע הראשי של צבא היבשה (CIO), ד"ר ראג' אייר (Raj Iyer), כי בכוונת צבא היבשה לחתום עד ליוני 2023 על חוזה בהיקף של כמיליארד דולר, שיסייע לקדם את יעדי הצבא בנושא השימוש בענן, כגון האצת המעבר לשימוש בתשתיות ענן, האצת פיתוח תוכנות, קבלת החלטות המבוססות על ניתוח נתונים וצמצום עלויות. במסגרת החוזה, הסוכנות לניהול ענן ברמת התאגיד של צבא היבשה (ECMA),[25] תסייע לפשט את תהליך המעבר באמצעות ניסוח חוזים, סיוע בהעברת מידע לענן, ועוד.[26]

<u>24 באוקטובר – חיל האוויר האמריקני יזם מחקר שוק לאיתור גורמי תעשייה לתמיכה בפיתוח תוכנית הכשרות בתחום לוחמת המידע והסייבר</u> – חיל האוויר יזם מחקר שוק לטובת איתור גורמי תעשייה שיכולים לתמוך בתוכנית ההכשרה למקצועות לוחמת המידע והסייבר, המנוהלת על ידי טייסת 39, יחידת ההדרכה להכשרות מבצעי הסייבר והמידע של פיקוד הסייבר של חיל האוויר, המְכֻנֶּה חיל האוויר ה-16 (16th Air Force).[27] על פי הבקשה, בכוונת הפיקוד לחתום על חוזה בסך 100 מיליון דולר למשך חמש שנים, במסגרתו החברה שתיבחר תתמוך בפיתוח תוכנית ההכשרה ותסייע בתמיכה מנהלתית, בהכשרת מדריכים בניהול רשתות, בתחזוקת תשתיות וחומרה ובכתיבה טכנית.[28]

---

[23] https://bit.ly/3gdU8UE
[24] https://bit.ly/3VLqfeN ; קישור לתוכנית הענן: https://bit.ly/3DdciyP ; קישור לתוכנית ניהול המידע: https://bit.ly/3TAvDzj
[25] Enterprise Cloud Management Agency
[26] https://bit.ly/3SwR2sk ; https://bit.ly/3zghAax
[27] 39th Information Operations Squadron
[28] https://bit.ly/3gx6nf5

סיכום זירת הסייבר ברקע הפלישה הרוסית לאוקראינה

במקביל להימשכות מתקפת הנגד של צבא אוקראינה והתארגנות הצבא הרוסי להמשך הלחימה, נרשמו מתקפות סייבר מצד קבוצות המזוהות עם רוסיה כנגד אתרים ממשלתיים בקרב מדינות ברית נאט"ו ובראשן ארה"ב, לצד מתקפות של קבוצות האקרים פרו-אוקראיניות, המתנגדות למשטר הרוסי, אשר תקפו חברת תקשורת לוויינים מרוסיה וכן חברות רוסיות המספקות עבור ממשלת רוסיה שירותים טכנולוגיים ובטחוניים.

ב-10 באוקטובר, עשרות מאתרי האינטרנט של שדות התעופה הגדולים בארה"ב, בהם אתרי שדות התעופה של שיקגו, אטלנטה (Atlanta), דנבר (Denver), לוס-אנג'לס, ניו-יורק ואחרים הושבתו במסגרת תקיפות DDoS. לדברי ראש יחידת ניתוח המודיעין של חברת Mandiant, ג'ון הולטקוויסט (John Hultquist), קבוצת ההאקרים הפרו-רוסית, Killnet, עמדה ככל הנראה מאחורי המתקפה וכן לא נמצאו עדויות למעורבות ישירה של ממשלת רוסיה.[29]

ב-15 באוקטובר, חוו מספר אתרים פרטיים וממשלתיים בבולגריה, בהם אתרי משרדי הנשיאות, ההגנה, הפנים, המשפטים, מס ההכנסה, חברות וכלי תקשורת, שדות תעופה ובנקים תקיפות DDoS נרחבות. ב-16 באוקטובר, אמר סגן התובע הראשי וראש שירות החקירות הלאומי של בולגריה, בוריסלב סראפוב (Borislav Sarafov), כי כתובתו של הגורם העומד מאחורי התקיפה זוהתה, בעיר הרוסית מגניטוגורסק (Magnitogorsk). שר ההגנה הזמני של בולגריה, דימיטר סטויאנוב (Dimitar Stoyanov), הוסיף כי ייתכן ורוסיה אחראית למתקפה, לאחר שטענה כי בולגריה הייתה מעורבת בפיצוץ הגשר המחבר את רוסיה עם חצי האי קרים ב-8 באוקטובר 2022. האשמה זו הופרכה על-ידי הרשויות בבולגריה.[30]

ב-27 באוקטובר, חוו אתר הסנאט הפולני ואתר הפרלמנט הסלובקי תקיפות DDoS שיוחסו לקבוצות האקרים המזוהות עם רוסיה, והשביתו לזמן קצר את האתרים ומערכות ה-IT שלהם, ואת מערכת ההצבעה של הפרלמנט הסלובקי. המתקפה התרחשה כיממה לאחר החלטת הסנאט הפולני להכיר ברוסיה כמשטר תומך טרור. הפרלמנט הסלובקי הודיע כי כלל ישיבות הפרלמנט נדחו וכן כי עלות החלפת המערכות שנפגעו מוערכת כ-20 מיליון יורו (20 מיליון דולר), אף כי אתר הפרלמנט שב לפעולה.[31]

[29] https://abcn.ws/3yR0kIA
[30] https://bit.ly/3CMxmdZ ; https://bit.ly/3MJfu8D
[31] https://bit.ly/3DkEGxS

במקביל לתקריות הסייבר שחוו בעלות בריתה של אוקראינה, ב-2 באוקטובר דיווח אתר החדשות האוקראיני Kyiv Post, כי קבוצת האקרים רוסית מתנגדת משטר המכונה בשם NRA,[32] טענה כי ביצעה מתקפת כופרה כנגד חברת פיתוח התוכנה הרוסית Unisoftware, המספקת שירותים למוסדות ומשרדי ממשל במדינה. קבוצת ההאקרים טענה כי ביצעה את התקיפה כצעד מחאתי על פלישתה לאוקראינה. בנוסף, הקבוצה הודיעה כי גנבה העתקים של כלל הנתונים המסחריים והאישיים של עובדיה ולקוחותיה של Unisoftware, אותם איימה לפרסם.[33] ב-17 באוקטובר, הודיעה הקבוצה כי הצליחה לפרוץ למערכות חברת הטכנולוגיה Technoserv, ספקית שירותי התשתית (SI)[34] הגדולה ברוסיה וכן לחברות נוספות המספקות שירותים בטחוניים עבור ממשלת רוסיה. הקבוצה טענה כי גנבה נתונים במשקל 1.2 טרה-בייט, בהם מסמכים המעידים כי לחברה קשרים עם שירות הביטחון הרוסי (FSB).[35] כהוכחה לטענתה, הציגה צילומי מסך מהתקיפה שלכאורה ביצעה ואיימה לבצע מתקפות נוספות בעתיד כנגד ממשלת רוסיה.[36]

בנוסף, ב-5 באוקטובר טענה קבוצת ההאקרים OneFist, התומכת באוקראינה, כי הצליחה לפרוץ לרשת של חברת תקשורת הלוויינים הרוסית Gonets לאחר שהשיגה גישה למערכת לניהול קשרי לקוחות שלה (CRM)[37] ונעזרה בהגדרה לקויה על מנת לקבל גישה לרשת. הקבוצה הוסיפה כי מחקה מאגר נתונים החיוני לפעילות הרשת. לדברי הקבוצה, המכונה גם Thraxman, כמחצית מ-97 הלקוחות המשתמשים ב-Gonets מזוהים עם ארגונים מתעשיות הטילים וטכנולוגיות החלל של רוסיה.[38]

במקביל למתקפות שזוהו עם האקרים פרו-אוקראינים, ב-18 באוקטובר, הדיחה שרת הפנים של גרמניה, ננסי פאסר (Nancy Faeser), את ראש המשרד לאבטחת טכנולוגיות מידע של גרמניה (BSI),[39] ארנה שונבוהם (Arne Schönbohm) מתפקידו, עקב דיווחים של כלי תקשורת במדינה, לפיהם שונבוהם ניהל קשרים עם אנשי המודיעין הרוסי וחברות המופעלות על-ידי גורמים רוסיים בגרמניה.[40]

---

[32] The National Republican Army of Russia
[33] https://bit.ly/3SqrNYv ; https://bit.ly/3TA0QmU
[34] System integrator
[35] Federal Security Service of Russia
[36] https://bit.ly/3FAFr8T ; https://bit.ly/3frWajX
[37] customer relationship management
[38] https://bit.ly/3VAjAE4
[39] .Federal Office for Information Security
[40] https://bit.ly/3EPbVvx ; https://bit.ly/3TheXgK

בנוסף, ב-11 באוקטובר, במסגרת וועידת שרי ההגנה של מדינות ברית נאט"ו שנערכה ברקע הפיצוצים שאירעו בצינורות הגז הטבעי נורד סטרים 1 ו-2 בים הבלטי בספטמבר 2022, הזהיר מזכ"ל הברית, ינס סטולטנברג (Jens Stoltenberg) כי כל התקפה מכוונת נגד תשתית חיונית של בעלות ברית, לרבות מתקפות סייבר והיברידיות עלולות להוביל להפעלת סעיף 5 של אמנת הברית להגנה קולקטיבית.[41] כמו כן, ב-19 באוקטובר, טען ראש מִינְהֶלֶת אבטחת הסייבר של ה-NSA, רוב ג'ויס (Rob Joyce) כי אחד הלקחים המרכזיים שלמדה הסוכנות מהמלחמה הוא הצורך לשתף עם ספקי טכנולוגיה ותשתיות חיוניות מידע מודיעיני באופן יזום לשם שיפור אבטחת הסייבר של אותם ארגונים וברמה הלאומית בכלל.[42]

בד בבד, החודש התפרסמו מספר דו"חות ומחקרים, המתארים את מאפייני הפעילות של קבוצות פרו-רוסיות ברשתות החברתיות לשם תמיכה במאמץ המלחמתי של רוסיה. ב-5 באוקטובר, חברת אבטחת הסייבר האמריקנית Nisos פרסמה דו"ח, לפיו רוסיה משתמשת בערוץ Telegram כאמצעי אחסון דיגיטלי לאלפי סרטונים ב-18 שפות שונות לשם להפצת מידע כוזב ולשם התחמקות ממנגנונים לאיתורו ולהסרתו.[43]

ב-12 באוקטובר, פרסמה חברת מערכות האבטחה הישראלית-אמריקנית, Radware, דו"ח לפיו במהלך חודש יולי 2022 קבוצת איומי הסייבר הפרו-רוסית המכונה NoName057(16), השיקה ברשת החברתית Telegram קמפיין בשם DDOSIA Project, במסגרתו הציעה תשלום כספי למתנדבים האקטיביסטים כדי שאלו יבצעו מתקפות DDoS באמצעות בוטים כנגד ממשלות ותאגידים מערביים. הקבוצה הציעה למתנדבים שיבצעו את גלי המתקפות היעילים ביותר סכומים בסך של עד 80,000 רובל (כ-1,300 דולר) שישולמו דרך ארנק דיגיטלי. לאחר תקיפות ה-DDoS שביצעה Killnet כנגד שדות תעופה בארה"ב (ראו עמ' 8), הציעה NoName057(16) תמריצים כספיים נוספים לעוקביה ברשת Telegram, תמורת ביצוע מתקפות דומות.[44]

[41] https://bit.ly/3SdzOjm ; https://bit.ly/3D6kAsq
[42] https://bit.ly/3gIWMlE
[43] https://bit.ly/3eM6Qti ; קישור לדו"ח: https://bit.ly/3yUKYTq
[44] https://bit.ly/3CPXHIo ; הקישור לדו"ח: https://bit.ly/3CFVkru

דרום קוריאה

24 באוקטובר – דרום קוריאה השתתפה בפעם הראשונה בתרגיל סייבר בהובלת ארה"ב – צבא דרום קוריאה לקח חלק בפעם הראשונה בתרגיל הגנת הסייבר הרב-לאומי השנתי של פיקוד הסייבר האמריקני, Cyber Flag שנערך ברקע האיומים הביטחוניים מצד צפון קוריאה.[45] במסגרת התרגיל, יותר מ-250 מומחי סייבר משמונה מדינות פעלו במסגרת 13 צוותים לאומיים ורב-לאומיים, אשר התמקדו לראשונה באיומים פוטנציאליים שמקורם באזור אסיה-פסיפיק. לצד התרגיל, התקיימו גם סימפוזיון ותרגיל שולחן עגול (Tabletop Exercise), בהשתתפות יותר מ-30 נציגים מארה"ב ומרחבי העולם, שהתמקדו באיומי סייבר ובפעולות בנושא שיתופי פעולה בהגנה.[46]

סינגפור

20 באוקטובר – סינגפור השיקה תוכנית מורחבת לדירוג מידת אבטחת הסייבר של מכשירים רפואיים והקימה כוח משימה למאבק באיומי מתקפות כופרה – סוכנות אבטחת הסייבר של סינגפור (CSA)[47] הודיעה על הרחבת תוכנית סימון מידת אבטחת הסייבר של מכשירים רפואיים (SLC)[48] כך שתחול גם על מכשירי IoT בבתי חולים ותדרג את רמת אבטחת הסייבר שלהם על פני ארבע רמות של אבטחה. במסגרת המהלך מקווה ה-CSA כי יצרני המכשירים יטמיעו עקרונות אבטחת סייבר בתהליך הפיתוח והייצור של מכשירים רפואיים על מנת להעלות את רמת אבטחת הכללית של הציוד המסופק למרכזים רפואיים.[49] בנוסף, השיקה הממשלה את כוח המשימה למאבק באיומי מתקפות כופרה (CRTF),[50] שמטרתו לסייע לעסקים, למוסדות מחקר וחינוך ולספקים של תשתיות מידע חיוניות לשפר את מידת ההגנה שלהם מפני איום מתקפות הכופרה. הכוח יורכב מגורמים בכירים מה-CSA, סוכנות הטכנולוגיה הממשלתית (GovTech),[51] הרשות לפיתוח מדיה[52] ונציגים ממשרדי הפנים, ההגנה, התקשורת והמידע, הרשות המוניטארית של סינגפור,[53] והמשטרה הלאומית.[54]

---

[45] https://bit.ly/3TJtK3L
[46] https://bit.ly/3Ev59L7
[47] Cyber Security Agency of Singapore
[48] Cybersecurity Labelling Scheme; תוכנית לסימון ולדירוג מכשירים חכמים על סמך מאפייני אבטחת הסייבר שלהם, מה שיאפשר לצרכנים לזהות מכשירים בעלי רמת אבטחה גבוהה יותר.
[49] https://bit.ly/3W2fBjI
[50] The Counter Ransomware Task Force
[51] Government Technology Agency
[52] Infocomm Media Development Authority
[53] Monetary Authority of Singapore
[54] https://bit.ly/3zxe37N

איראן

8 באוקטובר – קבוצות האקרים המתנגדות למשטר האיראני פרצו לארגון לאנרגיה אטומית ולרשת הטלוויזיה הממלכתית במדינה – במסגרת ההפגנות העממיות המתחוללות באיראן מספטמבר 2022, הודיעה קבוצת האקטיביסטים המכונה בשם Edaalate Ali,[55] כי פרצה לרשת הטלוויזיה בבעלות המדינה והציגה במהלך אחד השידורים הישירים של הרשת מסרים ותמונות בגנות המשטר והמנהיג העליון של הרפובליקה האסלאמית, עלי ח'מנאי וכן קראה לציבור האיראני להתקומם כנגד המשטר.[56] ב-23 באוקטובר קבוצת האקרים אנונימית המכונה בשם Black Reward טענה כי גנבה נתונים במשקל 50 ג'יגה-בייט השייכים לארגון לאנרגיה אטומית של איראן,[57] שכללו תכתובות דוא"ל פנים-ארגוניות, חוזים ותוכניות בנייה הקשורות לתחנת הכוח הגרעינית של איראן בעיר בושהר (Bushehr). הקבוצה פרסמה את הנתונים שגנבה ברשת החברתית Telegram ודרשה מהמשטר לשחרר 50 אסירים פוליטיים שנכלאו במסגרת המחאות במדינה.[58]

אוסטרליה

17 באוקטובר – מחקר חדש: מרבית החברות הפרטיות באוסטרליה חוששות מפגיעה מסחרית עקב דרישות גוברות לשקיפות בנושאי סייבר – חברת השירותים והייעוץ PwC, המתמחה בשיפור ביצועים ובניהול משברים, פרסמה ממצאי סקר בנושא אבטחת סייבר שנערך בקרב 3,522 מנהלים בכירים בחברות פרטיות באוסטרליה בין החודשים יולי-אוגוסט 2022. לפי הממצאים, 90% מהמנהלים חוששים ששיתוף מידע לציבור בנושא אירועי סייבר עלול לפגוע בחברות ובתדמיתן, ולהעניק יתרון למתחרים.

[55] הקבוצה מזוהה עוד בשם Ali's Justice.
[56] https://bbc.in/3TGeaWt ; https://bit.ly/3VGYGDh
[57] Iran's Atomic Energy Organization
[58] https://bit.ly/3gGnN9d

81% ציינו שחובת דיווח עלולה למעשה להרתיע אותם לשתף מידע של חברות עם רשויות אכיפת החוק. לצד זאת, ה-PwC והמרכז לאבטחת סייבר של אוסטרליה (ACSC)[59] הזהירו מפני עלייה בתדירות ותחכום מתקפות סייבר, ועל כן ממליצים על שיתוף מידע פומבי בין חברות כאמצעי לשיפור ההתמודדות עם איום הסייבר ברמה הלאומית. בנוסף, נמצא במחקר כי חברות אוסטרליות מודאגות ביותר מאיומים של כנופיות פושעי סייבר וקבוצות האקטיביסטים וכי 60% מהארגונים שנשאלו מתכננים להגדיל את תקציב הסייבר שלהם ב-2023.[60]

<u>23 באוקטובר – בכוונת אוסטרליה לנסח חוקים להגדלת קנסות על דליפות מידע חמורות בקרב חברות פרטיות</u> – התובע הכללי של אוסטרליה, מארק דרייפוס (Mark Dreyfus), הודיע כי בכוונת ממשלת אוסטרליה להציג חוקים לפרלמנט לטובת הגדלה משמעותית של קנסות המוטלים על חברות פרטיות בגין הפרות חוזרות ונשנות או חמורות של תקנות הגנת פרטיות המידע, וכן שורת תיקונים לחוקי הפרטיות הקיימים. השינויים המוצעים יגדילו את הקנס המרבי הקיים על דליפות מידע חמורות, העומד על 2.22 מיליון דולר אוסטרלי (כ-1.4 מיליון דולר), לכ-50 מיליון דולר אוסטרלי (כ-32 מיליון דולר), או בסכום שווה ערך ל-30% ממחזור העסקים בתקופה הרלוונטית.[61]

<u>24 באוקטובר – היורופול פרסם דו"ח המציג את משמעויות השימוש ב-Metaverse על פשיעת סייבר</u> – על פי הדו"ח, שפורסם על ידי מעבדת החדשנות של היורופול, שימוש הולך וגובר בטכנולוגיית המטאברס (Metaverse) עלול לייצר איומי סייבר חדשים ולהוביל לצמיחתם של איומים קיימים, כגון מתקפות כופרה כנגד מכשירי מציאות מדומה (VR), גניבת זהויות של משתמשים באמצעות גניבת פרטיהם הביומטריים, ביצוע הלבנות כספים במטבעות מבוזרים ובאסימונים חסרי תחליף (NFT) וביצוע תקיפות מיניות במרחב הווירטואלי. מחברי הדו"ח הביעו חשש כי צמיחת השימוש ב-Metaverse תקל על הפצת מידע כוזב ומסרים מסיתים וכן על גיוס והכשרת פעילים לשם קידום אידיאולוגיות קיצוניות.

[59] Australian Cyber Security Centre
[60] https://ab.co/3sdSNjk ; קישור למחקר: https://pwc.to/3CZn8XT
[61] https://bit.ly/3NgWbnp

לצד זאת, מעריך היורופול כי השימוש ב-Metaverse יוביל לפיתוח דרכים להתמודד עם סכנות אלו, כגון שיתוף פעולה מרחוק בין צוותי משטרה, שיפור תוכניות הכשרה וירטואליות ושימוש בטכנולוגיית מציאות מדומה לשיפור הליכים משפטיים. מחברי הדו"ח קראו לגופי אכיפה להתחיל להיערך לסכנות הטמונות ב-Metaverse על-ידי השקת שיתופי פעולה עם חברות המעורבות בפיתוח הטכנולוגיה.[62]

<u>5 באוקטובר – פורסם מחקר הבוחן איומי סייבר על נמלים ומתקנים ימיים בארה"ב</u> – חברת הייעוץ המשפטי האמריקנית Jones Walker פרסמה תוצאות מחקר בנושא אבטחת הסייבר של נמלים ומתקנים ימיים המתבסס על סקר בהשתתפות 125 מנהלי נמלים ומסופים ימיים בארה"ב. על פי תוצאות הסקר, 74% מהמשיבים טענו כי מערכותיהם או המידע של ארגוניהם היה מטרות לתקיפות סייבר במהלך השנה שקדמה לעריכת הסקר. ב-38% מבין תקיפות אלו, נתון המהווה את רוב התקיפות, וקטור התקיפה הנפוץ ביותר היה תקיפת פרוטוקולי עבודה מרחוק (RDP).[63] בד בבד, 45% מהמשיבים ציינו כי איום מתקפות הכופרה הוא איום האבטחה העיקרי על ארגוניהם, זאת בהשוואה ל-20% מהמשיבים שציינו כי ארגוניהם חוו מתקפת כופרה. כמו כן, 11% מהתקיפות שחוו הנמלים הובילו לדליפת מידע בעוד ש-14% מהן גרמו לחסימת הגישה למידע שנגנב. בנושא ההיערכות להתמודדות עם תקריות סייבר, 57% מהמשיבים מנמלים השוכנים לחופי ים (Blue-water facilities) השיבו כי ארגוניהם מקיימים הכשרות סייבר לכל הפחות אחת לשנה, זאת לעומת 25% בלבד מהנמלים השוכנים לחופי נהרות (Brown-water facilities).[64]

<u>14 באוקטובר – חברת אספקת חשמל הגדולה בהודו חוותה מתקפת סייבר</u> – חברת אספקת החשמל הגדולה ביותר בהודו, Tata Power, שבעיר מומבאי (Mumbai), הודיעה כי חוותה מתקפת סייבר במסגרתה נפגעו חלקים ממערך ה-IT שלה, אולם כלל המערכות התפעוליות החיוניות המשיכו לפעול כסדרן.

[62] https://bit.ly/3TznjjM ; קישור לדו"ח: https://bit.ly/3gNliCg
[63] Remote Desktop Protocol
[64] https://bit.ly/3FiOco2 ; קישור למסמך: https://bit.ly/3TEp92Y

החברה לא מסרה פרטים נוספים על התקרית, אך פרסמה כי בתגובה למתקפה הגבילה את הגישה לפורטלים שלה החשופים לאינטרנט ופעלה לאתחל ולשחזר את מערכות ה-IT שלה.[65]

17 באוקטובר – חברת אבטחת סייבר פרסמה דו"ח חדש בנושא איומי הסייבר על תשתיות המים בארה"ב – על פי דו"ח שפרסמה חברת אבטחת הסייבר האמריקנית Nozomi Networks, ענף מתקני המים בארה"ב מבוזר וארגונים רבים עובדים באופן עצמאי, דבר שמקשה על שיתוף מידע בנושא איומי סייבר ועל גיבוש תקני אבטחה אחידים. בד בבד, רק 23% מארגונים בענף המים בארה"ב מקיימים הערכות שנתיות בנושא איומי סייבר וכן כ-38% מהארגונים מקדישים 1% בלבד מתקציביהם לתחום אבטחת סייבר. החברה המליצה לארגונים בתחום תשתיות מים להכשיר את עובדיהם לזהות סימנים פיזיים ודיגיטליים מוקדמים, שעלולים להעיד על התרחשותה של מתקפת סייבר. בנוסף, מחברי הדו"ח קראו לארגונים לשתף יותר מידע בנושא איומי סייבר וחולשות אבטחה ולבחון באופן שוטף את מדיניות אבטחת הסייבר וניהול הסיכונים, על מנת להתאימם לשינויים בזירת האיומים.[66]

18 באוקטובר – הרשות האמריקנית לאבטחת התחבורה פרסמה דירקטיבה לאבטחת סייבר של רכבות משא ונוסעים – במסגרת הדירקטיבה, מפעילי ובעלי רכבות משא ונוסעים נדרשים לגבש ולמסור לרשות האמריקנית לאבטחת התחבורה (TSA)[67] תוכנית אבטחת סייבר שתכלול את חלוקת הרשת למקטעים (segmentation) והפרדת מערכות ה-OT מרשת ה-IT, הטמעת אמצעי בקרת גישה בקרב מערכות חיוניות, יישום מדיניות ותהליכים לאיתור איומי סייבר ואנומליות ותהליכי התקנת עדכוני אבטחה למערכות אבטחה, יישומים וקְשִׁחָה. בנוסף, על מפעילי ובעלי הרכבות להגיש ל-TSA תוכנית הערכת אבטחת סייבר שנתית, במסגרתה יפרטו כיצד בכוונתם להעריך באופן שוטף את יעילות הגנת הסייבר ולתקן חולשות אבטחה.[68]

28 באוקטובר – CISA פרסמה מסמך המציג יעדים לביצוע בנושא אבטחת סייבר של תשתיות חיוניות – הדו"ח התפרסם בעקבות התזכיר הנשיאותי מיולי 2021, המנחה את CISA ואת NIST לנסח רשימת יעדים לביצוע (CPG)[69] בתחום אבטחת הסייבר עבור מפעילי תשתיות חיוניות.

[65] https://bit.ly/3Tf6sm9 ; https://bit.ly/3ggL1T9
[66] https://bit.ly/3TDZRSf ; גישה לדו"ח המלא: https://bit.ly/3TfqjlP
[67] Transport Security Administration
[68] https://bit.ly/3WdQzyd ; קישור לדירקטיבה: https://bit.ly/3FCQ1fk
[69] Cybersecurity Performance Goals

רשימת היעדים מתמקדת בשמונה תחומים, בהם אבטחת חשבונות משתמשים ומכשירים, הגנה על נתונים, ניהול חולשות, משילות והכשרת כוח אדם, וניהול שרשראות אספקה. היעדים הוגדרו כחלקיים בלבד והעמידה בהם וולונטרית וכן הסוכנות הודיעה כי בכוונתה לעדכן את שורת היעדים אחת למספר חודשים.[70]

4 באוקטובר – חברות לייצור ביטחוני בארה"ב ובקנדה חוו מתקפות סייבר – ב-1 באוקטובר, הודיעה קבוצת עברייני הכופרה BlackCat כי תקפה את חברת הייצור הביטחוני הקנדית Simex Defence, המספקת ציוד לחימה ותקשורת לכוחות צבא קנדה ולצבאות מדינות החברות בברית נאט"ו. לדברי מנהל תחומי השיווק והפיתוח העסקי בחברה, פארס חמאדה (Fares Hamade), החברה הצליחה להסיר את הנוזקה מרשתות החברה, אך לא ציין האם דלף מידע במסגרת התקיפה.[71] כמו כן, ב-4 באוקטובר פרסמו ה-NSA, ה-FBI ו-CISA אזהרה, לפיה מספר קבוצות APT תקפו בשנים 2021-2022 את רשתותיה של חברת ייצור ביטחוני אמריקנית, המשמשת כחברת קבלן של מחלקת ההגנה. במסגרת מתקפות אלו ניצלו ההאקרים חולשות אבטחה בשרתי Microsoft Exchange על מנת להתקין web shells מסוג China Chopper, דבר שהעניק לתוקפים גישה לשרת השייך לחברה ואִפְשֵׁר להם לגנוב מידע רגיש מרשתותיה.[72]

13 באוקטובר – המרכז הלאומי לאבטחת סייבר של בריטניה פרסם מסמך בנושא הגנה על שרשראות אספקה מפני איומי סייבר – המרכז הלאומי לאבטחת סייבר של בריטניה (NCSC) פרסם מסמך שמטרתו לסייע לארגונים בינוניים וגדולים במגזר הציבורי ובמגזר הפרטי לשפר את אבטחת הסייבר של שרשראות האספקה שלהם. המדריך, המהווה תוספת למדריך דומה שפורסם בשנת 2018,[73] מבוסס על חמישה עקרונות: הבנת ניהול הסיכונים של הארגון; ניסוח גישה להערכת אבטחת הסייבר של ספקי הארגון; הטמעת הגישה במערכת היחסים וביחסי העבודה עם ספקים חדשים; מיזוג הגישה החדשה במסגרת העבודה עם ספקים קיימים; ובחינה תקופתית של גישת האבטחה שנבחרה כנגד איומים חדשים.[74]

[70] https://bit.ly/3Fp6ofE ; קישור למסמך: https://bit.ly/3DLOpyG
[71] https://bit.ly/3sdgNmR
[72] https://bit.ly/3VGYZxW ; גישה לאזהרה: https://bit.ly/3gj70Jc
[73] NCSC's Supply Chain Principles ; https://bit.ly/3eCAW2q
[74] https://bit.ly/3CER0sE ; קישור למדריך: https://bit.ly/3Tt75bp

14 באוקטובר – חברות תחבורה ולוגיסטיקה באוקראינה ופולין חוו מתקפות כופרה מסוג חדש – מרכז מודיעין איומי הסייבר של חברת מיקרוסופט (MSTIC)[75] פרסם ב-14 באוקטובר הודעת בלוג,[76] לפיה קבוצת האקרים שטרם זוהתה ביצעה סדרת מתקפות כופרה נגד חברות תחבורה ולוגיסטיקה באוקראינה ובפולין באמצעות כופרה חדשה המכונה Prestige, שבאמצעותה השתלטה הקבוצה על גישת מנהל המערכת ואישורי גישה נוספים. המרכז ציין כי הדבקה נרחבת של תאגידים בכופרה איננה נפוצה באוקראינה, וכי הפעילות איננה קשורה לאף אחת מ-94 קבוצות הכופרה הפעילות הנמצאות תחת מעקב החברה. עם זאת, חוקרים הצביעו על חפיפה בין המטרות והמדינות שנבחרו במסגרת שורת המתקפות לבין הארגונים שהותקפו על ידי נוזקת HermeticWiper שהובילה למחיקת המידע של ארגונים שונים באוקראינה בימים שקדמו לפלישת צבא רוסיה.[77]

6 באוקטובר – ארגון אבטחת מידע בריטי השיק תוכנית לפיתוח כוח האדם מיומן במקצועות אבטחת הסייבר במגזר האנרגיה הגרעינית האזרחית – המכון המוסמך לאבטחת מידע (CIISec)[78] הפועל ללא כוונת רווח, הודיע על השקת תוכנית ה-Nuclear Sector Hub, שמטרתה לשפר את מיומנויותיו של כוח האדם המיומן במקצועות אבטחת סייבר במגזר האנרגיה הגרעינית האזרחי בבריטניה. התוכנית כוללת יעדים כגון גיוס עובדים חדשים, שיפור הכישורים המקצועיים של כוח האדם הקיים ושיתוף שיטות עבודה מומלצות. כמו כן, תעודד התוכנית שיתופי פעולה בקרב קבוצות עובדים שונות ברחבי המגזר.[79]

[75] Microsoft Threat Intelligence Center
[76] קישור להודעת הבלוג: https://bit.ly/3MYTnuQ
[77] המוכרת גם בשם HermeticWiper ; https://bit.ly/3TCFLaP
[78] Chartered Institute of Information Security ; ארגון בריטי ללא כוונת רווח, המיועד לקדם את הרמה המקצועית של מומחי אבטחת מידע.
[79] https://bit.ly/3yUzWgS

13 באוקטובר – ארגון הבריאות האמריקני ללא כוונת רווח CommonSpirit Health חווה מתקפת כופרה – אחת ממערכות הבריאות הגדולות בארה"ב הפועלת שלא למטרת רווח, CommonSpirit Health, ומחזיקה ביותר מ-1,500 אתרי טיפול ו-142 בתי חולים ב-21 מדינות בארה"ב, הודיעה כי חוותה מתקפת כופרה. המתקפה שיבשה את הגישה לרשומות רפואיות אלקטרוניות, גרמה לעיכוב בטיפול במאושפזים באזורים נרחבים ולהסטת אמבולנסים ממחלקת החירום של אחד המרכזים הרפואיים למתקנים רפואיים אחרים. CommonSpirit Health הודיעה כי השיבה את מערכותיה לפעילות במהירות, פתחה בבדיקת התקרית ופנתה למומחים לצורך סיוע. הארגון לא מסר פרטים נוספים על התקרית, כגון אם התוקפים השיגו גישה לרשומות רפואיות של מטופלים ומתי זוהתה הפריצה.[80]

29 באוקטובר – מפעילת הרכבות הגדולה בדנמרק חוותה תקיפת סייבר שהשביתה את תנועה הרכבות במדינה – מפעילת הרכבות הגדולה בדנמרק, DBS חוותה תקיפת סייבר שהשביתה את תנועת הרכבות במדינה למשך מספר שעות. תנועת הרכבות נעצרה לאחר שהחברה הדנית, Supeo, המספקת פתרונות ניהול נכסים ארגוניים לחברות תפעול בענף התחבורה, חוותה תקרית אבטחת מידע במסגרתה השביתה את שרתיה ואת התוכנה המשמשת את נהגי הרכבות. Supeo מסרה כי מדובר בתקיפה על רקע פיננסי, אך לא ציינה פרטים נוספים על התקרית.[81]

[80] https://bit.ly/3Dcoksd ; https://bit.ly/3Sb4t0U
[81] https://bit.ly/3Urojqu ; https://bit.ly/3A5dhPA

17 באוקטובר – סנאטורית אמריקנית ביקשה מידע על דרכי ההתמודדות של ממשלת ארה"ב עם איומי סייבר על ענף התעופה – במסגרת מכתב ששלחה יו"ר וועדת המשנה של הסנאט לקידום תיירות, מסחר וייצוא, הסנאטורית ג'קי רוזן (Jacky Rosen), למחלקת התחבורה האמריקנית ול-CISA, ביקשה רוזן מהסוכנויות לספק מידע בנושא צעדיהן לשיפור אבטחת הסייבר של ענף התעופה.[82] הסוכנויות התבקשו לספק מידע בנושא תקיפות ה-DDoS שהשביתו את אתרי האינטרנט של שדות תעופה גדולים בארה"ב בתחילת אוקטובר 2022 (ראו עמ' 8). במכתב ביקשה רוזן לדעת כיצד פועלות הסוכנויות בתיאום עם רשויות נמלי התעופה ועם חברות תעופה שחוו תקיפות סייבר, האם הן פועלות להפחית סיכוני סייבר, האם הן מעניקות סיוע טכני לארגוני ענף התעופה והאם הן מודעות לאיומי סייבר נוספים ומיידיים המתמקדים בענף התעופה במדינה.[83]

7 באוקטובר – מפעילת הלווייני הצרפתית Eutelsat האשימה את איראן בשיבוש פעילות שני לווייני תקשורת שבבעלותה –חברת Eutelast פרסמה הצהרה שלפיה, החל מ-26 בספטמבר 2022 שני לווייני תקשורת שבבעלותה חוו פעולות שיבוש אותות (Jamming), שהובילו להפרעות בשידורי טלוויזיה ורדיו, בהם שידורי חדשות בשפה הפרסית שמקורם מחוץ לאיראן. לאחר הפעלת מערכת ייעודית לזיהוי השיבושים, הגיעה Eutelsat למסקנה כי מקורן של פעולות השיבוש מגיע מתוך גבולות איראן. בתגובה לפעולות אלו, פנתה Eutelsat לממשלת איראן בדרישה להפסיק את פעולות השיבוש, האסורות על פי תקנות שידורי הרדיו הבינלאומיות של איגוד התקשורת הבינלאומי (ITU).[84]

[82] קישור למכתב: https://bit.ly/3eXFTmL
[83] https://yhoo.it/3gjkvsh
[84] International Telecommunication Union ; https://bit.ly/3W9Bn5n

<u>26 באוקטובר – דארפ"א פרסמה בקשה לקבלת הצעות לתוכנית חדשה לשימוש בטכנולוגיית בינה מלאכותית לחיזוק אבטחת סייבר של רשתות מחשבים</u> – דארפ"א פרסמה בקשה לקבלת הצעות לתוכנית חדשה, CASTLE,[85] שמטרתה לפתח תהליכים אוטומטיים להערכה ולבחינה של אבטחת הסייבר של רשתות. התוכנית תתמקד בפיתוח כלים אוטומטיים להקמת סביבות רשת,[86] בלימוד מבצעי הגנת סייבר ובאיתור וקטורים ושיטות תקיפה חדשות. במסגרת התוכנית, שצפויה להימשך ארבע שנים, הצוותים המשתתפים ישתמשו בלמידת חיזוק (reinforcement learning)[87] כבסיס לאוטומציית התהליך להפחתת מספר החולשות ברשתות וכן יפתחו תוכנת קוד פתוח, שתסייע למגני הרשתות לחזות אילו חולשות האקרים עלולים לנצל במסגרת תקיפותיהם.[88]

<u>19 באוקטובר – חיל האוויר האמריקני חתם על חוזה בסך 22 מיליון דולר לטובת בניית מחשב קוונטי מתקדם</u>

– מעבדת המחקר של חיל האוויר האמריקני (AFRL)[89] חתמה על חוזה בסך 22 מיליון דולר עם החברה לייצור תוכנה PsiQuantum, לטובת בניית המחשב הקוונטי הראשון בעולם מסוג utility scale.[90] לשם כך, במסגרת החוזה יקדמו הצדדים יישום גישת מחקר פוטונית בתחום המחשוב הקוונטי וייצור שבבים פוטוניים קוונטיים (quantum photonic chips).[91] לדברי סגן מנהל המעבדה, מייקל היידוק (Michael Hayduk), יצור מחשב מסוג זה חיוני לשם מתן מענה לאתגרים הולכים וגוברים בבטחון הלאומי.[92]

---

[85] Cyber Agents for Security Testing and Learning Environments
[86] realistic network environments, סביבות רשת שניתן לבצע עליהן בדיקות של מידת האבטחה.
[87] סוג של למידת תוכנה, בה המחשב איננו מבצע את תהליך הלמידה על סמך מאגרי מידע מוכנים, אלא הוא יוצר את המידע במסגרת תהליך למידה.
[88] https://bit.ly/3Urq5b5
[89] Air Force Research Laboratory
[90] על פי דארפ"א, מדובר במחשב קוונטי שערכו החישובי עולה על ההוצאות הכרוכות בהפעלתו. להערכת מדענים מסוימים, הדרך לייצור מחשב מסוג זה, תארך עוד זמן רב.
[91] פוטוניקה עוסקת ביצירה ובעיבוד של פוטונים (חלקיקי אור). במחשוב קוונטי מבוסס פוטוניקה, הפוטונים משמשים כיחידת המידע הקוונטית. בשבבים פוטוניים, הרכיבים האלקטרוניים שבשבבים רגילים מוחלפים ברכיבים פוטוניים.
[92] https://bit.ly/3gHT9wa

<u>3 באוקטובר – הסכם שיתוף נתונים בין ארה"ב ובריטניה לצורך סיכול פשעים במרחב הדיגיטלי נכנס לתוקף</u>

– במסגרת הסכם ה-CLOUD Act Agreement[93] הראשון מסוגו, ישתפו ארה"ב ובריטניה פעולה במאבק בפשעים במרחב הדיגיטלי. ההסכם יאפשר לגופי אכיפת החוק מארה"ב ובריטניה[94] לקבל גישה לנתונים המצויים בידיהם של ספקי שירותי אינטרנט הממוקמים במדינה האחרת, לצורך שיפור יכולתן של שתי המדינות למנוע, לזהות, לחקור ולהעמיק לדין עבריינים המעורבים בתקריות פשיעה חמורות, לרבות טרור, פשע מאורגן רב-לאומי, ניצול ילדים ועוד. במסגרת ההסכם, יכולות המדינות להגיש בקשה לקבלת נתונים הקשורים לאירוע פשיעה חמור. עם זאת, בקשות לקבלת מידע אינן יכולות לכלול בקשה למידע השייך לאזרחים.[95]

<u>14 באוקטובר – צוותי סייבר צבאיים מארה"ב ומהמזרח התיכון השתתפו בתרגיל הגנת סייבר</u> – הארמייה השלישית בצבא ארה"ב ארגנה את תחרות ה-Best Cyber Warrior השנתית, במסגרתה 56 צוותים מצבאות ארה"ב, כוויית, ירדן, עיראק, ערב הסעודית ועומאן השתתפו במשימות לאיתור חולשות ופעילות זדונית ברשת, וכן בתרגילים שמטרתם לבחון מוכנות, מיומנויות וטכניקות בתחום הגנת הסייבר. במסגרת התחרות, שהתקיימה זו השנה השמינית, נדרשו הצוותים לנתח סממנים לפריצה ועקבות דיגיטליים (Digital fingerprints) על מנת לזהות מתקפת סייבר שחוו וכן להגן על רשתותיהם מפני תקיפות סייבר מצד יריבים.[96]

<u>17 באוקטובר – רשויות אכיפת חוק באירופה עצרו 31 חשודים בגין גניבת כלי רכב באמצעות טכנולוגיית פריצה ללא שימוש במַפְתֵּחַ התנעה</u> – רשויות אכיפת החוק בצרפת, ספרד ולטביה,[97] בשיתוף עם היורופול (Europol) והסוכנות האירופית לשיתוף פעולה משפטי (Eurojust) סיכלו את פעילותה של קבוצת עבריינים שהשתמשה בתוכנה מזויפת המתחזה לתוכנה לאיתור תקלות ברכב לצורך גניבת כלי רכב ללא שימוש במַפְתֵּחַ התנעה.

---

[93] U.S. Clarifying Lawful Overseas Use of ,ההסכם מורשה בהתאם לחוק Access to Electronic Data for the Purpose of Countering Serious Crime Act (״CLOUD״) Data.

[94] משרד העניינים הבינלאומיים של מחלקת המשפטים (OIA) תהיה אמונה על יישום ההסכם מטעם ארה״ב, בעוד שיחידת סמכויות החקירה של משרד הפנים של בריטניה, יבצע את ההסכם מטעמה.

[95] https://bit.ly/3s8Q2Qj ; https://bit.ly/3saebGh

[96] https://bit.ly/3s5VDXQ

[97] מטעם צרפת השתתפו יחידת הסייבר של סמכות השיפוט הלאומית נגד פשע מאורגן (JUNALCO) והז׳נדרמריה הצרפתית, מטעם לטביה השתתפה משטרת המדינה, ומטעם ספרד - Investigative Court num. 2 in Palma de Mallorca Balearic Islands PPO.

הקבוצה התמקדה בתקיפת כלי רכב עם מערכות שאפשרו את פתיחת הדלתות ואת ההתנעה ללא מפתח מתוצרת שתי יצרניות רכב צרפתיות.[98]

<u>20 באוקטובר – מדינות איגוד דרום-מזרח אסיה הקימו צוות CERT משותף</u> – עשר מדינות איגוד דרום-מזרח אסיה (Asean),[99] הכולל בין השאר את סינגפור, מלזיה ואינדונזיה, השלימו את הקמת צוות ה-CERT המשותף, לאחר שב-2018 סיכמו לקדם את הקמתו לצורך שיתוף פעולה בתחום אבטחת הסייבר. כאשר יהפוך למבצעי, צוות ה-CERT יאפשר לגורמים הרלוונטיים במדינות החברות לשתף מידע בזמן אמת על תקריות אבטחת סייבר, לרבות התקפות על שרשרת אספקה המתרחשות בכל אחת מהן ובהגנה על תשתיות מידע חיוניות (CII).[100] הצוות יסייע עוד בקידום שותפויות בין המדינות לבין גורמי תעשייה ואקדמיה, על מנת להגביר את מוכנותן המבצעית של המדינות.[101]

<u>24 באוקטובר – תורכיה סייעה לפקיסטן להקים בחשאי יחידת סייבר לשם השפעה על דעת הקהל של מוסלמים בדרום-מזרח אסיה וכנגד ארה"ב והודו</u> – תורכיה סייעה לפקיסטן להכשיר יחידת סייבר שמטרתה לערער את הביקורת כנגד השלטונות במדינה, להשפיע על דעת הקהל המקומית בפקיסטן ועל קהלים מוסלמים בדרום-מזרח אסיה ולהיאבק במבצעי השפעה שניהלו לכאורה ארה"ב, הודו ומדינות זרות אחרות ברשתות החברתיות כנגד פקיסטן. יחידת הסייבר הפקיסטנית הוקמה לבקשת השלטונות באופן חשאי והוסוותה במסגרת הסכם בילטרלי עליו חתמו המדינות, לכאורה לשם מאבק משותף בפשעי סייבר. במסגרת הקמת היחידה מאז 2018, סייעו משרד הפנים ומשטרת תורכיה (GDS)[102] בהובלת שר הפנים התורכי, סולימן סוילו (Suleyman Soylu), להכשיר 6,000 מאנשי יחידת הסייבר של פקיסטן, הנמנית על כוחות המשטרה הלאומית במדינה.[103]

[98] https://bit.ly/3TzTCyI
[99] Association of Southeast Asian Nations, הכולל את אינדונזיה, מלזיה, תאילנד, הפיליפינים, וייטנאם, סינגפור, מיאנמר, לאוס, קמבודיה וברוניי.
[100] Critical information infrastructure
[101] https://zd.net/3TTb7du
[102] General Directorate of Security
[103] https://bit.ly/3O4cyUx