לא רק רוסיה וטראמפ

מהן מתקפות הסייבר הנפוצות, מהם הנזקים האפשריים ובעיקר - כיצד ניתן להתמודד עימן > שרון ולדמן, גיא מונרוב

בשנים האחרונות אנו עדים לקיומה של תופעה מטרידה ההולכת וצוברת תאוצה – "לוחמת סייבר". לוחמה מסוג שכזה משפיעה על כולנו בעיתות שלום ומלחמה. היא עלולה לשתק את פעילות הצבא, מערכות החשמל והמים של המדינה. פרטי חשבונות בנק, תוצאות בדיקות רפואיות ופרטים רגישים שלנו עלולים להיות חשופים לעיני פצחנים ערמומיים.

לוחמת סייבר היא שם כולל לפעולות התקפיות המבוצעות ממניעים שונים במרחב הקיברנטי ואשר מכוונות נגד יעד מסוים. ניתן לחלק התקפות סייבר אלו למספר קטגוריות עיקריות: מתקפות על רקע טרור, פשיעה ומודיעין (לרוב על ידי ארגוני ביון ומדינות). טרור קיברנטי שם לו למטרה לפגוע בתשתיות קריטיות של מדינה, לזרוע הרס ופאניקה בקרב הציבור ואף להוביל למותם של בני אדם. מאידך, פשיעה במרחב הקיברנטי נועדה להשיג בדרך כלל רווח כספי ולעיתים אף להפגין כוח ועוצמה בלבד. בנוסף למתקפות אלו, קיימות מתקפות סייבר לצרכים פוליטיים, צבאיים ומודיעיניים, אשר לרוב מבוצעות על ידי מעצמות עולמיות וארגוני ביון נסתרים.

מאחר שהטכנולוגיה מתקדמת באופן מהיר ומאפשרת ביצוע פעולות באופן אנונימי תוך שימוש במניפולציות וכלים טכנולוגיים מתוחכמים, אנו עדים להתגברות משמעותית בהיקף ובתדירות של תקיפות הסייבר בעולם כולו. על פי הערכות הפורום הכלכלי העולמי, גובה הנזקים הגלובליים הנובעים מפשעי סייבר מגיע ל־445 מיליארד דולר בשנה, סכום המתקרב לתמ"ג של מדינות כמו בלגיה ופולין. על פי הערכות חברת המחקר גרטנר, חברות המספקות כלים טכנולוגיים ופתרונות בנושאי אבטחת מידע מגלגלות מחזור עולמי של 77 מיליארד דולר ועד שנת 2020 הסכומים יאמירו ל־170 מיליארד דולר. אם מישהו חשב שאיומי הסייבר הם תופעה שולית שעתידה לחלוף – מומלץ שישקול זאת שוב.

סקירה מהירה של החדשות בישראל ובעולם עשויה להמחיש בקלות עד כמה איומי הסייבר רציניים ומשפיעים עלינו כבר ממש עכשיו. האם ייתכן שנשיא ארה"ב, דונלד טראמפ, ניצח בבחירות (לאחר חודשים ארוכים של פליטות פה, ספינים ופרשיות ללא סוף) בזכות התערבות מכוונת שהגיעה מהקרמלין? על פי דוח של שירותי המודיעין בארה"ב, קיימות הוכחות מוצקות לכך שתקיפות סייבר בוצעו על ידי האקרים רוסיים, והן כללו פריצות למחשבים ודואר אלקטרוני של בכירים במפלגה הדמוקרטית והדלפת מידע רגיש מתוכם.

השימוש בלוחמת סייבר קיים גם במישור הבטחוני־צבאי. בספטמבר 2010 הצהירה איראן, כי חשפה תולעת Stuxnet ברשתות הפנימיות של מתקניה הגרעיניים. התולעת צוידה בקוד המנצל מספר פגיעויות בלתי ידועות במערכות השליטה ובקרה (SCADA), לרבות חתימה מזויפת ויכולת לשבש את הפקודות והתהליכים הקשורים למהירות מתקני הצנטריפוגה לזיקוק אורניום ופלוטוניום. שיבוש התהליכים במערכות השליטה והבקרה הוביל להטעיית המפקחים באתר הגרעין, אשר לא חשו בשינויים במהירות מתקני הצנטריפוגה. האחריות לביצוע יוחסה לישראל ואף למדינות נוספות כגון ארצות הברית ובריטניה.

דוגמא נוספת לעוצמת ההשפעה של מתקפות סייבר מגיעה מתחום הפיננסים, כאשר בפברואר 2016 בוצעה אחת מגניבות הסייבר הגדולות בהיסטוריה. קבוצה של האקרים סיניים הצליחה לפרוץ את מערכות המחשב של הבנק המרכזי של בנגלדש ולהעביר 81 מיליון דולר מהחשבונות שלו בבנק הפדראלי של ניו־יורק לבתי קזינו בפיליפינים. לטענת מומחי אבטחת מידע, גניבת הכספים בוצעה באמצעות פריצה לתוכנה המשויכת לפלטפורמת העברת הכספים SWIFT, אשר מהווה מסלקה בינלאומית בין גופים פיננסיים בעולם, תוך טשטוש עקבותיהם באמצעות נוזקה. הפריצה הביאה להתפטרותו של נגיד הבנק המרכזי של בנגלדש, אטיור רחמן. לדברי סנטור בפיליפינים המעורב בחקירת המקרה, 30 מיליון דולר מהכסף שנגנב הועברו במזומן לאזרח סיני שחי במנילה.

מתקפת סייבר: קווים לדמותה

מדי יום אנו נחשפים לשיטות תקיפה חדשות אשר משתכללות לנגד עינינו וקצרה היריעה מלפרט את כולן. במסגרת חלק מהמתקפות נעשה שימוש בנוזקות, המכילות קוד זדוני ונשתלות במחשבו של המשתמש ללא ידיעתו, מתוך מטרה לפגוע או לשבש את הפעילות השוטפת או לאסוף מידע רגיש אודות הקורבן. בקטגוריה זו ניתן למצוא וירוסים, תולעת (Worm), סוס טרויאני (Trojan horse) רוגלה ועוד. המכנה המשותף לנוזקות אלו הוא שהן מתוכנתות לשרת את ההאקר התוקף, ומסוגלות להפיץ ולשכפל את עצמן בין קבצים שונים ובין מחשבים שונים באותה הרשת. הן נשלטות מרחוק תוך ניצול משאבי התקשורת וגורמות להאטת הביצועים, שיבוש ומחיקת נתונים רגישים, הדלפת מידע ועוד.

בתקופה האחרונה אנו עדים לתקיפות מסוג Phishing ותוכנות זדון מפותחות, אשר צוברות תאוצה ומכונות "וירוס

רו"ח שרון ולדמן; רו"ח גיא מונרוב, CISA, CRISC, CIA; אלקלעי־מונרוב AlMo בקרה וניהול סיכונים

מאחר שהטכנולוגיה מתקדמת באופן מהיר ומאפשרת ביצוע פעולות באופן אנונימי תוך שימוש במניפולציות וכלים טכנולוגיים מתוחכמים, אנו עדים להתגברות משמעותית בהיקף ובתדירות של תקיפות הסייבר בעולם כולו. על פי הערכות הפורום הכלכלי העולמי, גובה הנזקים הגלובליים הנובעים מפשעי סייבר מגיע ל-445 מיליארד דולר בשנה

הכופר" (Ransomware). המשותף לסוגי תקיפות אלו הוא שהן מסתמכות ברובן על הגורם האנושי, אשר קיימת הסכמה רחבה בקרב מומחי אבטחת מידע, כי הוא החוליה החלשה בכל הקשור להגנה על המידע והמערכות הממוחשבות בארגון.

Phishing הוא שם כולל להתחזות וגניבת זהות באינטרנט, מתוך מטרה לגרוף רווחים כספיים באמצעות ביצוע פעולות בחשבונות בנק, או עסקאות העושות שימוש בפרטי כרטיסי אשראי ללא ידיעת הקורבן. לעיתים, מטרת הונאת Phishing היא גניבת מידע רגיש בלבד, ללא ניסיון להפיק טובת הנאה כספית מיידית. הונאות מסוג זה מבוצעות בדרך כלל על ידי שליחת קישור תמים בדואר אלקטרוני המוביל לאתר מזויף, ושתילת פרסומת רגילה (למראית עין) באתר אינטרנט או פורום. לאחר שהמשתמש התמים מזין פרטים רגישים כגון סיסמאות, מספר כרטיס אשראי או מספר תעודת זהות, נתוניו האישיים מגיעים לידי התוקף. רק לאחר פרק זמן מסוים ההונאה תתגלה ותחושת חוסר האונים תשתלט על הקורבן.

"וירוס הכופר" הוא שיטת תקיפה חדשה הצוברת תאוצה וזכתה לתהודה עולמית לאחרונה בשל המתקפה חסרת התקדים על מערכות המחשוב בבתי חולים בבריטניה, יצרניות רכב בצרפת וגופים רבים אחרים. המתקפה האחרונה כונתה על ידי מומחי אבטחת מידע "מתקפת הסייבר הגדולה בהיסטוריה". במסגרת תקיפה שכזו, הווירוס מבצע הצפנה של נתוני המחשב השייכים לבעלים ומציג הודעה מאיימת הדורשת תשלום נכבד (כופר) עבור הסרת האיום, שחזור הנתונים והשבת המצב לקדמותו. ההדבקה בווירוס מסוג זה מתרחשת לרוב לאחר לחיצה על קישורים לא־מוכרים המגיעים במייל או באתרי אינטרנט שונים. לאחר שהקורבן מעביר את התשלום בהתאם להוראות הגורם התוקף, נשלח לו קוד הצפנה אשר באמצעותו ניתן לשחרר את החסימה ולפתוח את הקבצים.

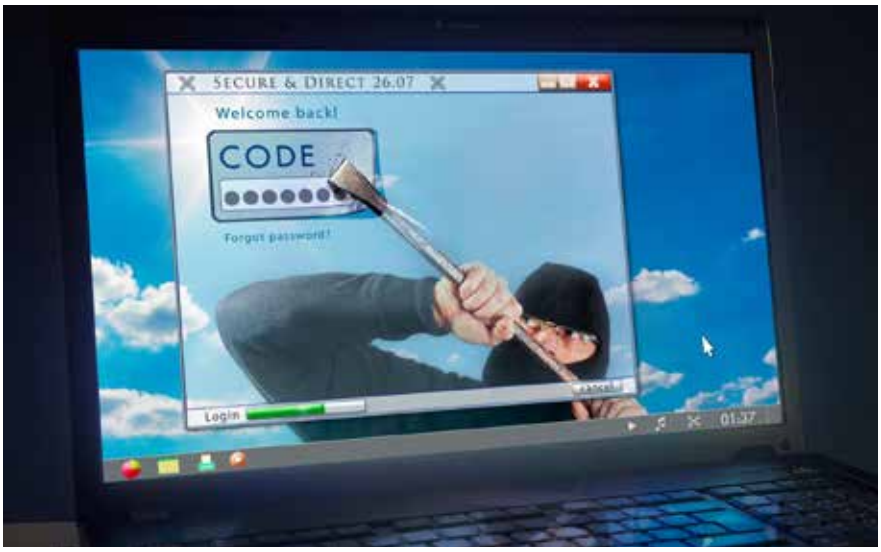
על מנת לצמצם באופן משמעותי את הסיכון להיפגע מהונאות פישינג ומהשתלטות וירוס הכופר על מערכות המחשוב, אסור בשום פנים ואופן להתפתות וללחוץ על קישורים וקבצים שאינם מוכרים לנו או לבצע עסקאות באתרי אינטרנט מפוקפקים. בנוסף, קיימת חשיבות רבה לביצוע גיבויים מלאים של הנתונים בתדירות מספקת, לרבות אחסונם באתר מאובטח.

מעבר למתקפות הסייבר הללו, בזמן האחרון אנו עדים לעלייה בשכיחות "מתקפות מניעת שירות מבוזרות" (DDOS). מדובר בשיטת התקפה המנוהלת מרחוק על ידי גורם בודד או מספר גורמים, אשר שולטים בו זמנית במחשבים תמימים רבים, הנגועים בנוזקה שהושתלה בהם ללא ידיעת בעליהם. ברגע שהגורם האחראי מחליט על ביצוע המתקפה, הוא מגייס את כל המחשבים הנתונים למרותו באמצעות כלי מרוחק, ומורה להם לתקוף את הקורבן.

שיטת תקיפה בה נעשה שימוש רב היא "מתקפת נפח", במסגרתה התוקף מנצל את העובדה שהרשת בנויה להתמודדות עם נפח תעבורה נתון, ולמעשה מציף אותה בנפחים גדולים משמעותית כך שישתקו את הגישה. דוגמא לכך היא מתקפת הסייבר שהתרחשה באוקטובר 2016 נגד חברת תשתיות האינטרנט האמריקאית דיין (Dyn). בעקבות המתקפה סבלו מיליוני גולשים ברחבי העולם מהאטה משמעותית בפעילות אתרי אינטרנט גדולים כגון טוויטר, אמזון ונטפליקס. מתקפת הסייבר נמשכה יותר מעשר שעות ועוררה הדים רבים בעולם, ועד כה אין תשובה חד־משמעית לגבי זהות האחראים למתקפה הזו.

ההתמודדות בישראל

לאור ההבנה שלא ניתן להקל ראש בהתייחס לאיומי הסייבר ההולכים וגוברים, הוקמו בישראל ובעולם גופים האמונים על קידום הנושא, פיתוח מענה טכנולוגי ותיאום דרכי התמודדות ותגובה עם גופים שונים בתחומי התעשייה, הביטחון הפיננסים ועוד. באוגוסט 2011 אישרה ממשלת ישראל את הקמתו של "מטה הסייבר הלאומי", האמון על פיתוח התחום הקיברנטי בארץ, תיאום בין הגורמים השונים העוסקים בתחום, הרחבת



מעטפת ההגנה על תשתיות לאומיות מפני התקפות קיברנטיות וקידום הנושא במגזר הפרטי.

בשנים האחרונות אנו עדים לעלייה ניכרת במודעות לעולם אבטחת המידע והסייבר בקרב מקבלי ההחלטות וגורמים רגולטורים בישראל. בפברואר 2015 פרסם מנכ"ל משרד הבריאות חוזר בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות", אשר מפרט את עיקרי איומי אבטחת מידע וסייבר העלולים להשפיע על מערכת הבריאות וביניהם: מתקפת מניעת שירות, גניבת מידע, שיבוש מידע והפצת קוד זדוני בתחנות קצה. במסגרת ההתמודדות עם איומים אלו, החוזר מפרט קווים מנחים לפיהם גופים במערכת הבריאות בישראל צריכים לנהוג תוך התייחסות לסוגיות שונות כגון אופן הטיפול באירועי אבטחת מידע, ניהול הרשאות משתמשים, שימוש בכלים טכנולוגיים לניטור ובקרה אחר משתמשים, הצפנת מידע רגיש וכדומה.

במארס 2015 פרסם המפקח על הבנקים נוהל ניהול בנקאי תקין שכותרתו "ניהול הגנת הסייבר". הנוהל מחייב את התאגידים הבנקאיים בישראל לנקוט בצעדים הכרחיים לניהול אפקטיבי של סיכוני אבטחת המידע והסייבר בפרט. בנוהל קיימת התייחסות לעקרונות היסוד לניהול הגנת הסייבר:

› זיהוי – ביצוע בירור ראשוני אודות היתכנות של אירוע סייבר, לרבות נקיטת דרכי פעולה מיידיות לטיפול.

› ניתוח – ביצוע בירור מקיף ומעמיק לגבי האירוע לשם אימוץ דפוסי פעולה הכרחיים, תוך בחינת חלופות אפשריות לבלימה והתמודדות עם האירוע.

› הכלה – השגת שליטה ראשונית של האירוע לצורך הכלתו ועצירת החמרת השפעתו על פעילות התאגיד.

› הכרעה – נטרול רכיבי התקיפה שמצויים במערכות התאגיד הבנקאי תוך שאיפה למזעור הנזק שנגרם בשל המתקפה.

› השבה – חזרה לתקינות ופעילות מלאה של התאגיד הבנקאי המותקף.

הוראת המפקח על הבנקים דורשת, כי על כל שלב יתבצע דיווח לגורמים הפנימיים והחיצוניים הרלוונטיים, וכי יתקיים מהלך מקיף לתחקור האירוע והפקת לקחים. כמו כן, מוטלת אחריות על דירקטוריון הבנק והנהלתו ליצור מסגרת אפקטיבית לניהול סיכוני הסייבר, לרבות גיבוש אסטרטגיה ודרכי התמודדות עם האיומים השונים.

עולם ניהול סיכוני אבטחת המידע והסייבר אינו יודע רגע דל ומשתנה לנגד עינינו מדי יום. חלק מהותי מהשמירה על הפעילות השוטפת של הארגון ואבטחת שרידותו הוא באמצעות מערך הגנה אפקטיבי ונקיטת אמצעים להתמודדות יעילה בעת משבר, ובפרט בעת התרחשות מתקפת סייבר המכוונת נגד הארגון. על מנת להבטיח קיום מערך הגנה אפקטיבי ומתמשך, נדרשת מחויבותם של הדירקטוריון והנהלת הארגון להתוות מדיניות ברורה ועקבית בנושא זה, לרבות הקצאת משאבים הולמים.

קיימת חשיבות רבה להגברת המודעות לאיומי אבטחת המידע והסייבר בקרב כלל העובדים בארגון. סוגיית ההתמודדות עם איומי אבטחת המידע והסייבר צריכה לטפס אל ראש סדר העדיפויות, ומי שלא ישכיל להיערך בהתאם – עלול באחד מן הימים להינזק קשות. ממשלת ישראל הבינה את המשמעות של פגיעה כתוצאה ממתקפות סייבר על המשק הישראלי, וביוני 2017 פרסמה הרשות הלאומית להגנת הסייבר את החוברת "תורת ההגנה בסייבר לארגון", אשר ניתנת להורדה בחינם מהאינטרנט ורצוי ביותר שתהיה בידי כל ארגון. ●

ביבליוגרפיה

"היקף נזקי פשעי הסייבר בעולם: 500 מיליארד דולר בשנה". www.globes.co.il/news/article.aspx?did=1001114422

סקירת אירועי סייבר מהותיים, חברת הייעוץ See Secure Consulting. www.see-secure.com

"רוסיה התערבה באמצעות סייבר בתוצאות הבחירות בארה"ב". www.israeldefense.co.il/he/node/28166

גניבת הכספים מהבנק המרכזי של בנגלדש. www.themarker.com/wallstreet/1.2925998

"מתקפות מניעת שירות מבוזרות". cert.gov.il/Professionals/SiteAssets/DDoSTypes.pdf

מתקפת הסייבר נגד חברת דיין. www.themarker.com/wallstreet/1.3100714

חוזר מנכ"ל משרד הבריאות בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות". www.health.gov.il/hozer/mk03_2015.pdf

נוהל ניהול בנקאי תקין 361, "ניהול הגנת הסייבר". www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf

"תורת ההגנה בסייבר לארגון". www.gov.il/he/Departments/policies/cyber_security_methodology_for_organizations