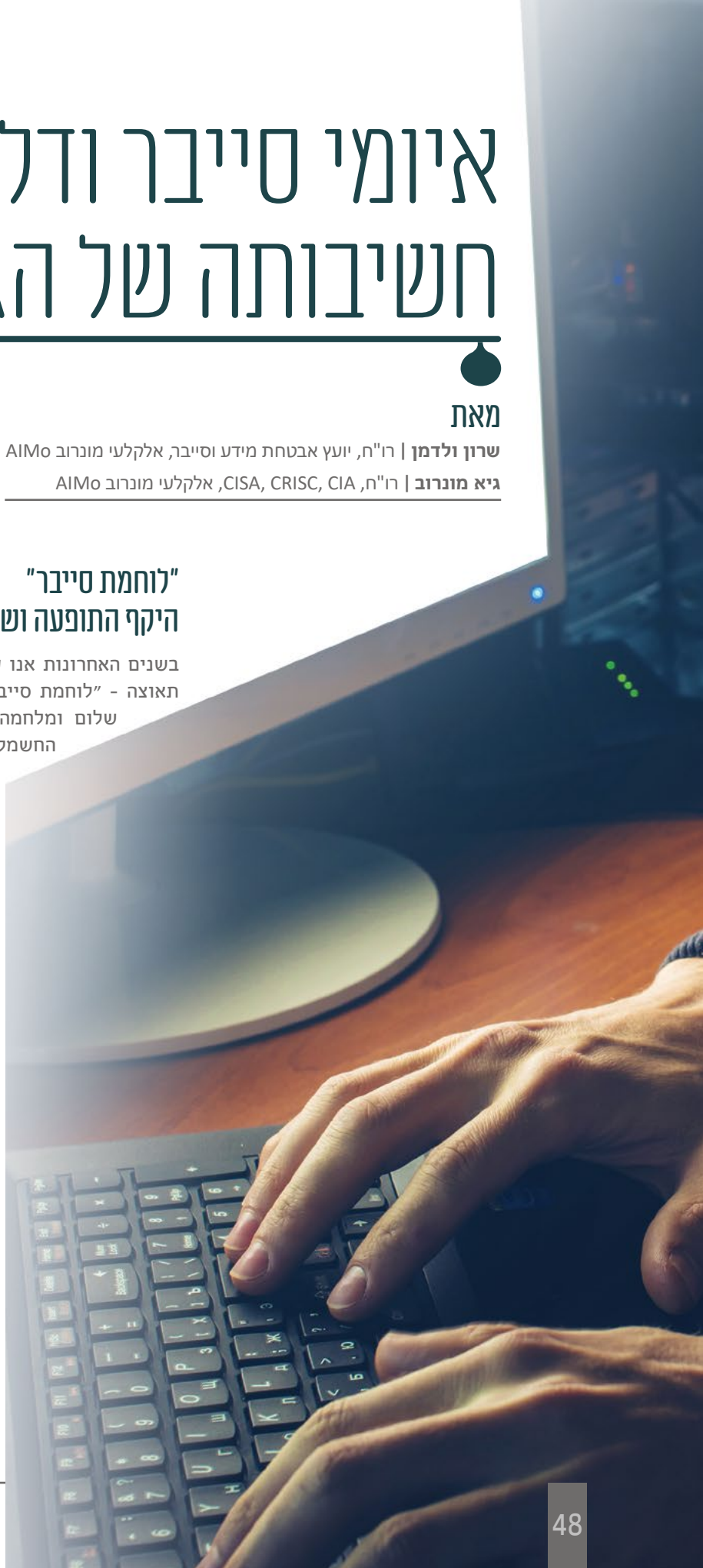
איומי סייבר ודלף מידע
חשיבותה של הגנה עצמית

מאת

שרון ולדמן | רו"ח, יועץ אבטחת מידע וסייבר, אלקלעי מונרוב AIMo

גיא מונרוב | רו"ח, CISA, CRISC, CIA, אלקלעי מונרוב AIMo



"לוחמת סייבר"
היקף התופעה ושכיחותה בימי חיינו

בשנים האחרונות אנו עדים לקיומה של תופעה מטרידה ההולכת וצוברת תאוצה - "לוחמת סייבר". לוחמה מסוג שכזה משפיעה על כולנו בעתות שלום ומלחמה; היא יכולה לשתק את פעילות הצבא, מערכות החשמל והמים של המדינה. כמו כן, פרטי חשבונות בנק, תוצאות בדיקות רפואיות ופרטים רגישים שלנו עלולים להיות חשופים לעיני פצחנים ערמומיים, וכאב הראש שנגרם מכך הוא של כולנו.

לוחמת סייבר היא שם כולל לפעולות התקפיות המבוצעות ממניעים שונים במרחב הקיברנטי ומכוונות 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. נוסף על מתקפות אלו, קיימות מתקפות סייבר לצרכים פוליטיים, צבאיים ומודיעיניים שלרוב מבוצעות על ידי מעצמות עולמיות וארגוני ביון נסתרים. מכיוון שהטכנולוגיה מתקדמת באופן מהיר ומאפשרת ביצוע פעולות באופן אנונימי תוך שימוש במניפולציות וכלים טכנולוגיים מתוחכמים,

אנו עדים להתגברות משמעותית בהיקף ותדירות תקיפות הסייבר בעולם כולו.

על פי הערכות הפורום הכלכלי העולמי, גובה הנזקים הגלובליים הנובעים מפשעי סייבר מגיע לכ-445 מיליארד דולר בשנה(!), סכום המתקרב לתמ"ג של מדינות מערביות מפותחות כמו בלגיה ופולין. על פי הערכות חברת המחקר "גרטנר", חברות המספקות כלים טכנולוגיים ופתרונות בנושאי אבטחת מידע מגלגלות מחזור עולמי של כ-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.

"מומחי אבטחת מאמינים שהגורם האנושי הוא החוליה החלשה בכל הקשור בהגנה על המידע הארגוני"

סקירה מהירה של עיתוני חדשות בישראל ובעולם עשויה להמחיש בקלות עד כמה איומי הסייבר רציניים ומשפיעים עלינו כבר 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, ובמסגרת התקיפות הללו נפרצו מחשבים ודואר אלקטרוני של בכירים במפלגה הדמוקרטית והודלף מידע רגיש אודותיהם. ניצחונו של טראמפ בבחירות לנשיאות ארצות הברית התקבל בברכה ובשמחה גלויה מצד פקידי ממשל רוסים בכירים. ימים יגידו האם הכינוי "הבובה של פוטין" שהוצמד לטרמאפ על ידי יריבתו, הילרי קלינטון, יצדיק את עצמו או לאו.

השימוש בלוחמת סייבר קיים גם במישור הביטחוני-צבאי. בחודש ספטמבר 2010 עיני העולם כולו היו נשואות לאיראן שהצהירה 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, מפני שהם לא חשו בשינויים במהירות מתקני הצנטריפוגה. על פי מקורות זרים האחריות לביצוע יוחסה לישראל ואף למדינות נוספות כגון ארצות הברית ובריטניה.

דוגמה נוספת לעוצמת ההשפעה של מתקפות סייבר מגיעה מתחום הפיננסיים. בתחילת פברואר 2016 בוצעה אחת מגניבות הסייבר הגדולות בהיסטוריה. קבוצה של האקרים סינים 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 המהווה מסלקה בינלאומית בין גופים פיננסיים שונים בעולם תוך טשטוש עקבותיהם באמצעות נוזקה. בעקבות המחדל החמור, נגיד הבנק המרכזי של בנגלדש, אטיור רחמן, הודיע על התפטרותו. על פי דברי סנטור בפיליפינים המעורב בחקירת המקרה, מעל 30 מיליון דולר מהכסף שנגנב הועברו במזומן לאזרח סיני שחי במנילה. מהבנק הפדראלי של ניו יורק נמסר כי לא נתגלתה פריצה במערכות הבנק וכי הם משתפים פעולה עם הבנק המרכזי של בנגלדש.

מתקפת סייבר קווים לדמותה

מדי יום אנו נחשפים לשיטות תקיפה חדשות שמשתכללות 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 (Spyware) ועוד. המכנה המשותף לנוזקות אלו הוא שהן מתוכנתות לשרת את התוקף ומסוגלות להפיץ ולשכפל את עצמן בין קבצים שונים ובין מחשבים שונים באותה הרשת, ואף נשלטות מרחוק תוך ניצול משאבי התקשורת וגורמות להאטת הביצועים, שיבוש ומחיקת נתונים רגישים, דלף מידע ועוד.

בתקופה האחרונה אנו עדים לתקיפות מסוג Phishing ותוכנות זדוניות מפותחות שצוברות תאוצה ומכונות בשם "וירוס הכופר"

המשותף לסוגי תקיפות אלו הוא שהן מסתמכות ברובן על הגורם האנושי, וקיימת הסכמה רחבה בקרב מומחי אבטחת מידע שזו החוליה החלשה בכל הקשור להגנה על המידע והמערכות הממוחשבות בארגון.

הונאות מסוג Phishing הן שם כולל להתחזות וגניבת זהות באינטרנט, במטרה לגרוף רווחים כספיים באמצעות ביצוע פעולות בחשבונות בנק או עסקאות העושות שימוש בפרטי כרטיסי אשראי ללא ידיעת הקורבן. לעיתים מטרת הונאת ה- Phishing יכולה להיות גניבת מידע רגיש בלבד, ללא שום ניסיון להפיק טובת הנאה כספית. הונאות מסוג זה מבוצעות בדרך כלל על ידי שליחת קישור תמים בדואר אלקטרוני המוביל לאתר מזויף (למשל: דרישה לעדכון פרטי חשבון באתר פייפאל בכתובת הבאה: service@paypl.com) 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, ורק לאחר פרק זמן מסוים ההונאה תתגלה והקורבן יגלה שהוא חסר אונים אל מול המתקפה.

"וירוס הכופר" הוא שיטת תקיפה הצוברת תאוצה. שיטה זו זכתה לתהודה עולמית בחודש מאי 2017 בשל המתקפה חסרת התקדים שניחתה על מערכות המחשוב בבתי חולים בבריטניה, יצרניות רכב בצרפת וגופים רבים אחרים בעולם שנדבקו בתוכנת הכופר הידועה לשמצה "WannaCry". 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 בדואר אלקטרוני או באתרי אינטרנט שונים. לאחר שהקורבן מעביר את התשלום בהתאם להוראות הגורם התוקף, נשלח לו קוד הצפנה שבאמצעותו ניתן לשחרר את החסימה ולפתוח את הקבצים (ולעיתים תשלום הכופר הוא לשווא וקוד ההצפנה אינו נשלח לקורבן חסר האונים).

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

מעבר למתקפות הסייבר שתוארו לעיל, התגלמות נוספת לתופעת "לוחמת הסייבר" באה לידי ביטוי באמצעות "מתקפות מניעת שירות מבוזרות" (DDOS). מדובר בשיטת התקפה המנוהלת מרחוק על ידי גורם בודד או מספר גורמים ששולטים בו-זמנית במחשבים תמימים רבים הנגועים מלכתחילה 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. אחת משיטות התקיפה שנעשה בה שימוש רב היא "מתקפת נפח", במסגרתה התוקף מנצל את העובדה כי הרשת בנויה להתמודדות עם נפח תעבורה נתון ולמעשה מציף אותה בנפחים גדולים משמעותית המשתקים את הגישה ברשת. דוגמה 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, נטפליקס ועוד. מתקפת הסייבר נמשכה מעל ל-10 שעות ועוררה הדים רבים בעולם ועד כה אין תשובה חד-משמעית לגבי זהות האחראיים למתקפה הזו.

התמודדות עם איומי אבטחת המידע והסייבר במדינת ישראל

לאור ההבנה כי לא ניתן להקל ראש בהתייחס לאיומי הסייבר ההולכים וגוברים, הוקמו בישראל ובעולם גופים האמונים על קידום הנושא ועל פיתוח מענה טכנולוגי מתאים, לרבות תיאום 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 הגנה על התחום הקיברנטי בארץ, תיאום בין הגורמים השונים העוסקים בתחום, הרחבת מעטפת ההגנה על תשתיות לאומיות מפני התקפות קיברנטיות, וקידום הנושא בענף התעשייתי.

בשנים האחרונות אנו עדים לעלייה ניכרת במודעות לעולם אבטחת המידע והסייבר בקרב מקבלי ההחלטות וגורמים רגולטוריים בישראל. בחודש פברואר 2015 פורסם על ידי מנכ"ל משרד הבריאות חוזר בנושא "הגנה על מידע במערכות ממוחשבות במערכת הבריאות" המפרט את עיקרי איומי אבטחת מידע וסייבר העלולים להשפיע על מערכת הבריאות, ובהם: מתקפת מניעת שירות (Denial Of Service), 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, ומתייחס לסוגיות שונות כגון אופן הטיפול באירועי אבטחת מידע, ניהול הרשאות משתמשים, שימוש בכלים טכנולוגיים לניטור ובקרה אחר משתמשים, הצפנת מידע רגיש וכדומה.

בחודש מרץ 2015 פורסם נוהל בנקאי תקין מספר 361 "ניהול הגנת הסייבר" על ידי המפקח על הבנקים, המחייב את התאגידים הבנקאיים בישראל לנקוט צעדים הכרחיים לצורך ניהול אפקטיבי של סיכוני אבטחת המידע והסייבר בפרט. קיימת התייחסות בנוהל לעקרונות היסוד לניהול הגנת הסייבר כמפורט להלן:

א. **זיהוי** - ביצוע בירור ראשוני אודות היתכנות של אירוע סייבר, לרבות נקיטת דרכי פעולה מיידיות לטיפול.

ב. **ניתוח** - ביצוע בירור מקיף ומעמיק לגבי האירוע לשם אימוץ דפוסי פעולה הכרחיים תוך בחינת חלופות אפשריות לבלימה והתמודדות עם האירוע.

ג. **הכלה** - השגת שליטה ראשונית של האירוע לצורך הכלתו ועצירת החמרת השפעתו על פעילות התאגיד.

ד. **הכרעה** - נטרול רכיבי התקיפה שמצויים במערכות התאגיד הבנקאי תוך שאיפה למזעור הנזק שנגרם בשל המתקפה.

ה. **השבה** - חזרה לתקינות ופעילות מלאה של התאגיד הבנקאי המותקף.

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

סיכום

עולם ניהול סיכוני אבטחת המידע והסייבר אינו יודע רגע דל ומשתנה לנגד עינינו מדי יום. חלק מהותי בשמירה על הפעילות השוטפת של הארגון (לרבות הגנה על 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. כמו כן, 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, מפני שמי שלא ישכיל להיערך בהתאם עלול באחד מן הימים להינזק קשות. נראה כי מדינת ישראל הבינה את המשמעות של פגיעה כתוצאה ממתקפות סייבר על המשק הישראלי, ובמהלך יוני 2017 יצאה גרסה מס׳ 1.0 של ״תורת ההגנה בסייבר לארגון״ על ידי הרשות הלאומית להגנת הסייבר, חוברת חובה בכל ארגון הניתנת להורדה בחינם באינטרנט.

תפקידו של המבקר הפנימי מחייב אותו להיות ער לתמורות ולשינויים בתחום אבטחת המידע והסייבר. הסתמכות הארגונים על מערכות המחשוב הולכת וגוברת עם השנים, ולכן המבקר הפנימי חייב לשים דגש במסגרת עבודתו על היבטי אבטחת מידע שונים תוך הקפדה על בניית תוכנית ביקורת אפקטיבית המותאמת לאופיו של הארגון הנבדק.

ראוי כי תוכנית הביקורת תכלול התייחסות להיבטים שונים, כגון קיום מדיניות ונהלים בנושא, אסטרטגיה ותוכנית עבודה רב-שנתית, אבטחה לוגית ופיזית, אופן התמודדות הארגון עם אירועי אבטחת מידע וסייבר, התאוששות מאסון והמשכיות עסקית, יישום תקנים מקצועיים בנושא ועוד. נדרש כי המבקר הפנימי יתריע בפני ההנהלה והדירקטוריון על חולשות וליקויים בתחום אבטחת המידע והסייבר על מנת להבטיח קיום מהלך שוטף לתיקון הפרצות ושיפור מתמיד של מערך ההגנה הכולל בארגון.

״מי שלא ישכיל להיערך בהתאם עלול באחד מן הימים להינזק קשות״