אבטחת מידע: האויב מבפנים


זאב נוימן


משה צבירן


יעקב מנדל

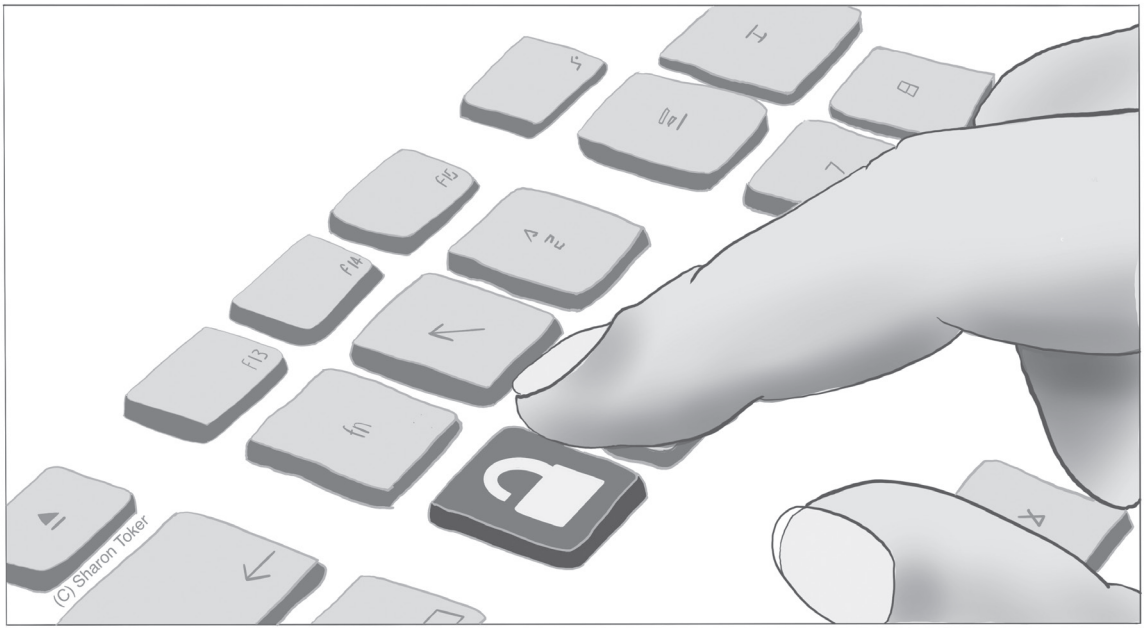
פרופ' זאב נוימן הוא פרופ' (אמריטוס) בפקולטה לניהול ע"ש קולר באוניברסיטת תל אביב. פרופ' נוימן ייסד את תחום ניהול מערכות המידע בפקולטה לניהול והיה מופקד על קתדרת מקסיקו למערכות מידע ניהולי באוניברסיטת תל אביב משנת 1986 ועד לפרישתו. כמו כן כיהן פעמיים כדקאן הפקולטה, בשנים 1973-1978 ובשנים 1985-1989. פרופ' נוימן הוא בוגר תואר ראשון בכלכלה וסטטיסטיקה מהאוניברסיטה העברית ותואר שני ושלישי במינהל עסקים מאוניברסיטת קליפורניה בלוס-אנג'לס (UCLA). הוא פרסם 12 ספרים ועשרות מאמרים בתחומי מערכות מידע וביטוח בכתבי עת אקדמיים מובילים. פרופ' נוימן כיהן כדירקטור במספר רב של חברות ציבוריות ופרטיות, וכן שימש כיועץ להנהלות ארגונים בישראל ובחו"ל.

פרופ' משה צבירן מכהן כדקאן הפקולטה לניהול על שם קולר באוניברסיטת תל אביב. פרופ' צבירן מופקד על קתדרת יצחק גילינסקי ליזמות, טכנולוגיה, חדשנות וניהול, וכן משמש כמנהל האקדמי של תוכנית ה-MBA בניהול טכנולוגיה יזמות וחדשנות וכראש מכון אלי הורוביץ לניהול אסטרטגי. פרופ' צבירן הוא בוגר תואר ראשון במתמטיקה ומדעי המחשב ותואר שני ושלישי במדעי הניהול – כולם מאוניברסיטת תל אביב. הוא פרסם שני ספרים ועשרות רבות של מאמרים מדעיים בכתבי עת אקדמיים מובילים. פרופ' צבירן גם פעיל בסביבה העסקית בישראל, ובין היתר כיהן ומכהן בדירקטוריונים של חברות ציבוריות ופרטיות ומשמש כיועץ בכיר לארגונים מובילים בארץ ובחו"ל.

ד"ר יעקב מנדל הוא חבר סגל בפקולטה לניהול ע"ש קולר באוניברסיטת תל אביב. ד"ר מנדל הוא יזם סייבר סדרתי, שימש כמנכ"ל מרכז הסייבר והמצוינות בחברת אינטל, בעל 16 פטנטים רשומים בתחום הסייבר והיה אחד היזמים של חברת SCsquare שנמכרה לחברת ברודקום. ד"ר מנדל בעל ניסיון עשיר ומגוון בתחומי הסייבר ההגנתי וההתקפי. ד"ר מנדל בעל תואר MBA מאוניברסיטת בן-גוריון בנגב ודוקטורט בכלכלה מאוניברסיטת פוזנן לכלכלה ועסקים. תחומי המחקר שלו מתמקדים בהיבטים הכלכליים של מתקפות סייבר, טכנולוגיית בלוקצ'יין, קוונטום, וכן היבטי פרטיות והמשכיות הפעילות העסקית תחת התקפות סייבר.

תקציר

הצמיחה המהירה של טכנולוגיות מידע ורשתות מביאה עימה דאגה מרכזית של ארגונים לסוגיית אבטחת המערכות והנתונים, כאשר היעדים העיקריים של אבטחת המידע הם סודיות, שלמות וזמינות המערכות והמידע. אבן הפינה של אבטחת המידע בארגונים טמונה באפיון ויישום נהלים ומנגנונים נאותים לאבטחת המערכות והמידע תוך איזון בין יעדי האבטחה לצורכי הארגון. אולם בעוד שרבים ממערכי ההגנה עוסקים בגילוי ומניעה של חדירת גורמים חיצוניים למערכות הארגון, רק תשומת לב מעטה ניתנת ל"אויב שמבפנים" – משתמשים מורשים מתוך הארגון שעלולים לפגוע באבטחת המערכות, בין אם בשוגג ובין אם בזדון. מאמר זה עוסק באפיון האיומים וגורמי הסיכון מתוך הארגון, דן בסיכונים הנשקפים מהם, ומציע דרכים לצמצום האיום ולהתגוננות מפניהם.



מבוא

המונח "המהפכה הדיגיטלית" או "מהפכת המידע" מתייחס למעבר מטכנולוגיה אנלוגית לטכנולוגיה דיגיטלית, ולהצפה של חידושים טכנולוגיים משבשים שמשפיעים על כל אורחות חיינו. המהפכה הדיגיטלית ועידן המידע, ששורשיהם העמיקו כבר במהלך הרבע האחרון של המאה ה-20, וכן הפרדיגמות הטכנולוגיות-כלכליות שנגזרות מהקדמה הטכנולוגית, משפיעים בצורה מהותית על כל תחומי חיינו, משנים מקצה לקצה את הדרך שבה אנו חיים, עובדים ומתקשרים זה עם זה, ומגבירים את תלותם של ארגונים ושל אנשים פרטיים בטכנולוגיות המידע. בניתוח רטרוספקטיבי של מהפכה זו ביחס לקודמותיה, ניתן לקבוע כי עוצמת השפעתה עולה על זו של המהפכה החקלאית והמהפכה התעשייתית, מפני שהמהפכות הקודמות התפתחו בקצב ליניארי, ואילו המהפכה הדיגיטלית מתפתחת בקצב אקספוננציאלי ומשפיעה הן ברמת המאקרו והן ברמת הפרט. ברמת המאקרו, היא משפיעה על כל ענף כלכלי, כאשר הרוחב והעומק של השפעתה מביאים לשינויים במערכות שלמות של ייצור, שירותים, ניהול וממשל. בתחילתו של העשור השלישי של המאה ה-21 ניכר כי המהפכה הדיגיטלית משנה גם את סביבתו הפיזית, החברתית והתרבותית של הפרט, מחוללת תמורות בדרכי התנהגותו, באורחות חייו, בדרכים שבהן הוא קולט ומעבד מידע, ואף באופן שבו הוא חושב. לפיכך, ארגונים ואנשים פרטיים נדרשים להגדיר ולשדרג את המערכות שלהם, לרכוש מיומנויות חדשות ולטפח מחשבות חדשות (Bojanova, 2014; Feenberg, 2010; Stenberg and Preiss, 2005; Von Krogh et al., 2000).

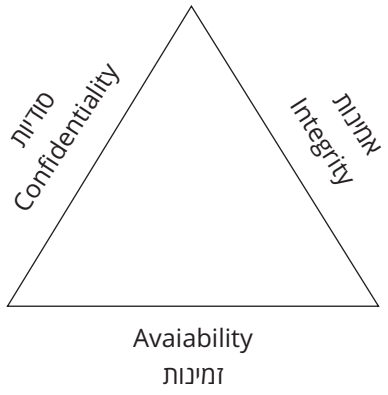
במקביל להתפתחותן של מערכות המידע ולהגברת תלותם של הארגונים בפעילותן התקינה, עלתה גם המודעות לסיכונים המאיימים על שלמותן וביטחונן של המערכות. כתוצאה מכך התפתח תחום אבטחת המידע (Information security) שהתמקד בהגנה רב-שכבתית על משאבי המידע של הארגון, ובכלל זה אבטחה פיזית של המבנה שבו נמצאות מערכות המחשב, אבטחה של מערכות החומרה והתוכנה, אבטחת רכיבי התקשורת ואבטחת המידע הנאגר בהן (Erlich and Zviran, 2010).

איור מס' 1 מציג את שלושת היעדים העיקריים של אבטחת מידע:

- **סודיות** (Confidentiality) נועדה להבטיח שהמידע יהיה נגיש אך ורק לגורמים מורשים, ולהם בלבד.
- **זמינות** (Availability) מתייחסת לצורך שמערכות המידע והמידע האגור בהן יהיו זמינים למשתמשים המורשים בכל זמן נתון.

- **שלמות** (Integrity) נועדה להבטיח שהמידע האגור במערכת יהיה מוגן מפני שינוי זדוני או השמדה.

איור מס 1: השילוש הקדוש של אבטחת מידע



ההתפתחויות המהירות בעולם המידע ובתחום הרשתות, והשימוש הנרחב בטכנולוגיות מידע בעולם הסייבר (שבו שולטות הקישוריות והנגישות לכל דבר ומכל מקום), יצרו עלייה מקבילה בדאגה לביטחון המידע. לפיכך תחום אבטחת המידע קיבל תפנית משמעותית והתפתח מאבטחת מידע בלבד לאבטחת מידע וסייבר (Cybersecurity). בהתאם, הגבול בין מערכות המידע ברמת הארגון ליכולות הדיגיטליות ברמת הפרט (*למשל* באמצעות שירותי ענן, טלפונים חכמים, התקנים מתקדמים ועוד) הולך ומיטשטש, ומאגרי מידע רבים, המשמשים יחידים, תאגידים ומדינות, מאוחסנים כיום בענן או על גבי מחשבים המקושרים לאינטרנט באופן שמאפשר (לפחות מבחינה תיאורטית) גישה לכל דבר ומכל מקום. לכן נדרשת מערכת אבטחה כוללת, שנועדה להגן על נכסי המידע מפני גישה, שימוש, חשיפה, ציתות, שיבוש, העתקה או השמדה *של* מידע, בין אם בזדון ובין אם בשוגג. אך בעוד שרבים ממערכי ההגנה עוסקים בגילוי ומניעה *של* חדירה *של* גורמים חיצוניים למערכות הארגון, רק תשומת לב מעטה ניתנת ל"איוב שמבפנים" – משתמשים מורשים מתוך הארגון שעלולים לפגוע באבטחת המערכות, בין אם בשוגג ובין אם בזדון.

האויב מבפנים

איום פנימי (Insider threat) מוגדר כסיכון לאבטחת המערכות או המידע שמקורו בארגון. בדרך כלל סיכון זה כרוך בישות שהארגון נותן בה אמון – ישות פנימית כגון עובד פעיל או עובד לשעבר, או ישות חיצונית כגון שותף עסקי או קבלן משנה – שמַפָרה חוק אחד או יותר ממדיניות האבטחה *של* הארגון ועושה שימוש לרעה בגישה מורשית לצורך נקיטת פעולות המשפיעות לרעה על סודיות, שלמות או זמינות *של* המידע ו/או מערכות המידע *של* הארגון (Liu et al., 2018). למושג "אמון" (Trust) היה תמיד תפקיד חשוב בזיהוי הגבולות *של* ארגון – מי "בפנים" ומי "בחוץ". האיום הפנימי מתרחש כאשר ישות ברת-אמון בארגון פוגעת באמון שניתן לה. התקפת סייבר מוצלחת מתרחשת כאשר אדם מהימן (שקיבל את אמון הארגון) ומחזיק מידע רגיש (בנאמנות), מפר את חובת הנאמנות (Bishop, 2005). מאידך, גוף או גופים חיצוניים לארגון יכולים לשחד עובדים בתוך הארגון כדי להשיג מידע רגיש כגון סודות מסחריים או טכנולוגיה מתקדמת (גם אם היא מוגנת בפטנטים).

מרבית האיומים וההתקפות על משאבי המידע *של* הארגון נובעים מגורמים פנימיים (Ding et al., 2018; Liu et al., 2018). כך *למשל*, בדיון בשנת 2017 בבית הנבחרים *של* מדינת קליפורניה על חקיקה בתחום סודות מסחריים, נאמר כי "יותר מ-80% ממקרי גניבת מידע מארגונים עסקיים בארה"ב מתרחשים מבפנים. המשמעות היא שהאיום הגדול ביותר לאובדן מידע רגיש *של* הארגון מקורו מבפנים – מעובדי הארגון" (Wiseman, 2018). סקר אחר שנערך בארה"ב בשנת 2015 מצא כי 60% מפרצות האבטחה שנסקרו היו כתוצאה מטעויות אנוש *של* עובדים, ו-70% מהפרצות נגרמו על ידי עובדים פנימיים (Kroll, 2015). באופן דומה, סקרים שנערכו בבריטניה בשנת 2015 ייחסו 60% מפרצות האבטחה לטעויות אנוש (PwC, 2015). גם דוח *של* האיחוד האירופי קבע בבירור שהאיומים מבפנים עולים בשכיחותם ובחומרתם על האיומים המגיעים מחוץ לגבולות הארגון (Marinos and Lourenço, 2019).

סוגי איומי הפנים כוללים כוונת זדון בקטגוריה אחת, ורשלנות או חוסר זהירות בקטגוריה שנייה.

כוונת זדון – איום מכוון על ידי גורם פנימי בעל יכולת גישה מורשית למשאבי המידע בארגון, העושה שימוש לרעה ביכולת זו כדי לגרום נזק לארגון או כדי לגנוב מידע לצורך תמריצים כספיים או אישיים. גורם פנימי זדוני הוא כל ישות מתוך הארגון שמפרה בכוונה את הוראות הארגון ומשתמשת לרעה בסמכותה כדי לשתף או להפיץ או לגנוב מידע מסווג או

מידע רגיש, או לחילופין להפעיל ביודעין התקפה על מערכות המחשוב של הארגון כדי לגרום נזק. ניתן להתייחס לפרופיל של עובד זדוני בהקשר של מניע, תפקיד בארגון ויכולת. מניעים של איומים מבפנים יכולים להיות מרמור, עבריינות, סחיטה, קשיים כספיים, נקמה, הלשנה על כשלים אתיים וכדומה. רמת התפקיד בארגון משקפת את רמת ההזדמנות של העובד לממש את האיום, ואילו היכולת תלויה ברמת הידע והתחכום הטכני של העובד. מלבד עובדים אורגניים בארגון, עובדי מיקור חוץ וקבלני משנה הם מקור מובהק לאיומים מבפנים. ארגונים רבים מעסיקים עובדים אלו כדי להקטין עלויות, ובמקרים אחרים כדי להאיץ לוחות זמנים לצורך סיום פרויקטים. בדרך כלל לעובדים אלו יש רמה נמוכה יותר של מחויבות ונאמנות לארגון, מפני שהם נחשבים ל"פנימיים" לתקופה מוגבלת ויהפכו לבלתי נגישים למערכות הארגון כשהחוזה שלהם יסתיים. סטטיסטיקת האיומים הפנימיים של גרטנר מעלה כי כשליש מהפרות אבטחת המידע הנעשות על ידי גורמים מתוך הארגון מבוצעות ממניעים כלכלים, ועושות שימוש במידע סודי כדי לייצר רווח כלכלי אישי באמצעות הונאה או על ידי מכירת מידע וסודות מסחריים. מקור מובהק אחר של איומים מבפנים קשור בעובדים (בהווה או לשעבר) שמבצעים חבלה מכוונת במערכות המידע הארגוניות באמצעות "פצצה לוגית"– קוד תוכנה זדוני שהותקן במערכות הארגון ומופעל כאשר תנאי מסוים או קבוצת תנאים מתקיימים. כאמור, צורת תקיפה זו אופיינית לעובדים ממורמרים, עובדים שפוטרו או לעובדים שעוברים לעבוד בארגון מתחרה.

מתקפה זדונית מבפנים נחשבת לפשע. למרות העיסוק הממושך בנושא, טרם הצליחו לייצר פרופיל של עבריינים הפועלים מתוך הארגון ולהבין את הפסיכולוגיה והמניעים שלהם. הבנת הפסיכולוגיה של עבריין פוטנציאלי מבפנים היא חלק מהפתרון אך לא הפתרון המלא. אינדיקטורים פסיכולוגיים-התנהגותיים ואישיותיים יכולים לכלול אישיות תוקפנית, עבר פלילי, אינטראקציה בלתי מדווחת עם אנשים או ארגונים מתחרים, ניסיונות חוזרים של גישה למידע בלתי מורשה, תלונות על בעיות כספיות או על סירוב לקידום במעמד או במשכורת, וסימנים ברורים של צריכת סמים או התמכרות לאלכוהול. עם זאת, חשוב להדגיש כי בעוד שגורמים פסיכולוגיים יכולים לשמש סימני אזהרה לכך שעובד מהווה איום פנימי פוטנציאלי, ניסיון ליצור פרופיל של התנהגות (או בניית מודלים של סימולציה שמחקים התנהגות) יכול להביא לתוצאות שגויות (Eldardiry, 2013).

רשלנות או חוסר זהירות – קטגוריה זו מתייחסת לאיומים לא מכוונים של גורמים פנימיים החושפים את המערכת לאיומים חיצוניים בשל רשלנות או חוסר זהירות, אך ללא כוונת זדון. דוגמאות להתממשות איומים מסוג זה כוללות, בין השאר, מחיקת מידע ללא כוונה, אובדן רכיבי זיכרון, לחיצה על קישור לא מאובטח והדבקת המערכת בתוכנה זדונית, עובד שאין לו כוונת זדון אך ללא ידיעתו מהווה פרוקסי להתקפה חיצונית ועוד. איומים מסוג זה הם איומי הפנים הנפוצים ביותר, והסיבות העיקריות להתממשותם הן:

איור מס 2: קטע עיתון המתאר דוגמה לשימוש בלתי מורשה תוך יישום כוונת זדון

הותר לפרסום: מחלקת הסייבר בפרקליטות המדינה הגישה הבוקר (שלישי) כתב אישום לבית משפט השלום ברחובות נגד עובדת בוועדה לאנרגיה אטומית (וא"א), בגין ביצוע עבירות של חדירה לחומר מחשב ופגיעה בפרטיות. הנאשמת חדרה בעשרות הזדמנויות שונות למערכת מחשוב, שאליה לא הייתה לה הרשאת כניסה, וערכה חיפושים ממוקדים שלא כדין ובניגוד לחוק הגנת הפרטיות.

על-פי כתב האישום, החל מסוף חודש אוגוסט 2018 ועד לינואר 2020 חדרה העובדת למערכת המחשוב בין 100-70 פעמים וערכה בה חיפושים אסורים. עם הגשת כתב האישום, קיבל בית המשפט את בקשת המדינה והורה על איסור פרסום ודלתיים סגורות בתיק. זאת מטעמים של ביטחון המדינה והגנה על הפרטיות.

מקור: מעריב, 20/3/2020

(1) טיפול שגוי או חסר בהתמודדות עם נתונים רגישים; (2) חוסר הדרכה, אימון והטמעה מספיקים של יישום מדיניות אבטחה בארגון; (3) עומס יתר בעבודה וריבוי משימות המובילים להפחתת תשומת הלב ממדיניות האבטחה של הארגון; (4) מדיניות אבטחה נוקשה שגורמת לאי נוחות למשתמשים ומובילה להתעלמות מהם.

האיום "התמים" הנובע מרשלנות או מחוסר זהירות, ומתייחס בדרך כלל לארבעה טיפוסי עובדים (Wall, 2011). הטיפוס "החתרן" כולל עובדים שמתעלמים או חותרים תחת הוראות אבטחה כדי להקל על עבודתם השגרתית. דוגמאות לכך כוללות עובדים המשתפים את הסיסמאות שלהם, משתמשים בסיסמאות פשוטות מאוד, או פותחים מיילים ממקורות מפוקפקים ובעייתיים וכו'. הטיפוס "השאפתני מדי" כולל עובדים המודעים לחשיבות ההקפדה על נוהלי אבטחה, אך לוקחים במודע סיכונים. הם מתעלמים מנוהלי אבטחה ועוקפים תהליכי אבטחה ארוכים ושגרתיים כדי להיות יעילים יותר. בדרך כלל עובדים אלו מתייחסים לנוהלי האבטחה כמסורבלים מדי ומונעים על ידי הרצון לבצע עבודה מהירה. הטיפוס "המהונדס חברתית" כולל עובדים הנופלים למלכודת של ישויות בלתי מורשות, פנימיות או חיצוניות לארגון, בעלות כוונה זדונית, ומתפתים לספק מידע מסווג או הרשאות במענה למישהו שהם תופסים כבעל סמכות. הטיפוס המכונה "מדליף מידע" כולל עובדים, שמסיבות אתיות או בלתי אתיות מדליפים לציבור דרך רשתות חברתיות מידע פנים ארגוני שלדעתם הציבור חייב לדעת (לדוגמה: ויקיליקס). עובדים אלה מאמינים שמעשיהם אינם זדוניים, מכיוון שהם לכאורה מדליפים מידע שמטרתו לתרום לציבור. אולם כל עובד שמפר בכוונה נוהלי

איור מס 3: קטע עיתון המתאר דוגמה לנזק לארגון כתוצאה מרשלנות ללא כוונת זדון

Data on 130,000 criminals lost

Confidential information on almost 130,000 orisoners and dangerous criminals has been lost by the Home Office, sparking yet another Government data crisis.

By Robert Winnett and Jon Swaine
9:31AM BST 22 Aug 2008

The loss of the details, which were stored on as unencypted computer memory stick, has raised fears that the taxpayer may now face a multi-million pound compensation bill from criminals whose safety may have been compromised and police informants who could be at risk of reprisals.

The home addresses of some of Britain's most prolific and serious offenders - including those who have committed violent and sexual crimes - are understood to be among the missing data.

A full investigation is now underway to find the memory stick – containing information on all 84,000 prisoners in England and Wales, including sone release dates, plus details of 43,000 most serious and persistent offenders – which was described as a 'toxic liability' by David Smith, the Deputy Information Commissioner.

מקור: The Telegraph, 22 August 2008

אבטחה ומשתמש לרעה בסמכותו כדי לשתף או לגנוב מידע מסווג או רגיש, הוא למעשה עובד פנימי זדוני, ללא קשר למניע. טיפוס זה של "מדליף מידע" יכול להיחשב כתמים ובלתי זדוני רק במקרה שבו אין בארגון הנחיות ברורות לגבי העובדה שהמידע המודלף אמור להיות מסווג (דבר שמצביע על כשל מובנה בנוהלי האבטחה בארגון). עובדים פנימיים משתמשים בדרך כלל באישורים מזויפים כדי להשיג גישה למידע שאסור עבורם, או לחילופין משתמשים באישורים החוקיים שלהם למטרה זו.

חשוב לציין כי אחת הבעיות המרכזיות בהבנת התרחשותם וחומרתם של איומים מבפנים ופיתוח פתרונות מותאמים נגד איומים אלה היא המידע המוגבל על אירועים ונזקים. בסקר נרחב שבוצע בארה"ב בשנת 2016 נמצא שרק רבע מהמחקרים בתחום התבססו על נתוני אמת, ואילו היתר התבססו על מודלים סינטטיים (Moore et al., 2016). סיבה אחת לחיסרון בנתוני אמת נעוצה בעובדה שארגונים שחוו מתקפות מבפנים שואפים בדרך כלל להסתיר את ההתרחשות ולמנוע מעין הציבור חשיפה של אירועי אבטחה. סיבה נוספת היא שארגונים רבים כלל אינם יודעים שהותקפו, אלא רק בדיעבד, לאחר אירוע התקיפה, ולכן אינם יכולים לנתח את האירוע באופן מדויק.

אסטרטגיות לזיהוי וטיפול

על אף כל העדויות לגבי שכיחותם של איומי פנים, מרבית הארגונים עוסקים בעיקר בטיפול ובמניעה של איומים מבחוץ ומשקיעים את מרב המשאבים במערכות הגנה מפניהם. רק בשני העשורים האחרונים קיבל נושא ההגנה מול איומים מבפנים תשומת לב ותנופה, הן במחקר האקדמי, הן במישור הפרקטי והן במספר החברות העוסקות ביישום פתרונות לאבטחת מידע מפני איומים מבפנים. סדנה ייעודית שאורגנה בשנת 2000 על ידי מכון RAND הייתה בין הראשונות לסקור את נושא הטיפול באיומים מבפנים (Anderson et al., 2000). בסדנה זו זיהו שלושה רכיבים של מודל האיום מבפנים: (1) אנשים, (2) טכנולוגיה, (3) סביבה ותרבות ארגונית. הפתרונות שהוצעו באותה תקופה היו בעיקר ניטור של יומני שרתים, בקרת גישה וסינון קוד זדוני. בשלב הבא, ולאור ריבוי המקרים שבהם עובדים פנימיים פוגעים שלא במתכוון באבטחת המידע בארגון עקב נפילת קורבן לתוכנה זדונית (נוזקה - Malware) – תפיסת ההגנה התרחבה מעבר למיקוד הטכנולוגי וכללה גם המלצות על עקרונות של מדיניות ארגונית ומאמצים לבניית מודעות לאבטחת מידע בתוך הארגון. השלב הבא במאבק באיומים פנימיים שילב פתרונות טכנולוגיים מתקדמים תוך הישענות על שיטות המבוססות על פרופילים התנהגותיים. שלב זה התבסס על תוצאות של מחקרים בבינה מלאכותית ובלמידת מכונה, תוך שימוש בניתוח נתוני עתק (Big data). פתרונות אלה אפשרו פיתוח מהיר של סימולציות מורכבות של סביבות ארגוניות מגוונות, והדבר סייע מאוד לארגונים שהחלו להשתמש בסימולציות כדי לנתח בעיות אבטחה בכלל ובעיות הנובעות מאיומי פנים בפרט (Early and Stott, 2015). עם זאת, סביבה ארגונית אמיתית שונה מסביבת הסימולציות, ולכן זיהוי איומים המבוסס אך ורק על סימולציות צריך להיעשות בזהירות רבה מאוד כדי למנוע טעויות ומסקנות שגויות.

לאור הבנת המקורות של איומים מבפנים והסיבות למימושם, חשוב שכל ארגון יגדיר ויאמץ אסטרטגיה רב שכבתית, הכוללת מגוון של בקרות ותהליכי אבטחה להתמודדות עם האיום מבפנים, ובהתאם לאסטרטגיה זו ליישם מערכות הגנה כנגד איומים אלו (Erlich and Zviran, 2010). בבסיסה של אסטרטגיה זו עומדים מספר אמצעי הגנה שאמורים לשלב פיקוח וניטור התנהגות פנים:

- **הגדרה, יישום, הטמעה ואכיפה של מדיניות אבטחה–** כל ארגון חייב להגדיר, לתעד, ליישם ולהטמיע מדיניות ברורה בתחום אבטחת המידע, תוך התייחסות ספציפית לאיומים מבפנים. מדיניות זו תבהיר את כללי השמירה על נכסי המידע של הארגון ותאפשר את אכיפתם. כל עובד בארגון צריך להיות מודע למדיניות האבטחה ולקיים אותה.
- **הדרכה והכשרה קבועים של המנהלים והעובדים –** טעויות אנוש הן מציאות מבצעית, ולא פעם הגורם האנושי הוא החוליה החלשה בשרשרת האבטחה. שיפור המודעות לאבטחה והכשרת העובדים לגבי חובות אבטחת המידע שלהם, ובכלל זה הגנה על נתונים, מניעת דיוג (Phishing) וניהול סיסמאות, הם צעדים מכריעים להפחתת הסיכון לאירועי אבטחה פנימיים. גם הגדלת הנראות בתחום זה ויישום שינויים תרבותיים הם כלי יעיל בהרתעה ובמיגור רשלנות ואיומים זדוניים.
- **ניהול צמוד ושוטף של הרשאות ובקרת גישה –** ניהול צמוד ושוטף של הרשאות חיוני כדי להגביל את הסיכון לאירועי אבטחה זדוניים, בין אם ישירות על ידי עובד ובין אם בעקיפין על ידי גורם חיצוני שקיבל גישה למשאבי המידע של הארגון. בהקשר הזה חשוב שארגונים יישמו

מדיניות של רמת הרשאות מינימלית שמבטיחה לעובדים, לקבלנים ולשותפים עסקיים רק את רמת ההרשאות המינימלית הנדרשת למילוי תפקידם. חשוב גם לבדוק באופן שוטף את ההרשאות ולוודא כי ההרשאות מותאמות ככל שצורכי העבודה משתנים ונשללות מיד עם שינוי בתפקידם של בעלי ההרשאה או עזיבתם.

- **יישום מדיניות ניהול מכשירי קצה** – בארגונים רבים מיושמת כיום מדיניות של Bring Your Own Device - (BYOD), שלפיה העובדים מורשים להתחבר למשאבי המידע של הארגון ממגוון רחב של רשתות ומכשירים (מחשבים אישיים, טאבלט, טלפונים חכמים וכו') ומכל מיקום אפשרי. אולם רשתות ומכשירים לא מאובטחים מציבים מגוון של סיכוני אבטחה, ולכן ארגונים צריכים להבטיח שהגישה תותר רק מהתקני עובדים שבהם מותקנת תוכנת אבטחת נקודות קצה, להפעיל בקרת יישומים על ידי יצירת רשימת אפליקציות מאושרת, וכן להשבית (או לכל הפחות לעקוב אחר) נקודות USB במכשירים עם סיכון גבוה הנגישים למשאבי המידע של הארגון.
- **ניטור יזום של המערכות והרשתות** – אבטחה פרואקטיבית ברשת, לרבות ניטור תעבורה ברשתות ונקודות קצה, וניתוח דפוסי התנהגות של משתמשים וגורמים תוך שילוב של טכנולוגיות ייעודיות, מיועדת לאתר ולנטרל איומים ידועים ובלתי ידועים על ידי שימוש בטכניקות מתקדמות המזהות פעילות חריגה. UEBA היא קטגוריה של פתרונות אבטחה שמשתמשת בגישות של למידת מכונה ולמידה עמוקה כדי לדגום את התנהגות המשתמשים והמכשירים ברשתות ארגוניות, לזהות התנהגות לא תקינה, לקבוע אם להתנהגות זו יש השלכות אבטחה, ולהתריע על כך בפני צוותי האבטחה. מערכות ניטור נוספות כוללות מערכות לבקרה וניטור חדירות (Intrusion Detection Systems - IDS), מערכות לניהול אירועי אבטחה (Security Information and Event Management - SIEM), ומערכות לניהול ובקרת נקודות קצה (Endpoint Detection and Response - EDR). מערכות הניטור יעילות בזיהוי ובתגובה לאיומי פנים לפני שהם גורמים נזק ושיבוש. הניטור מתחיל באפיון וסימון פעילות תקינה, ובהתאם ניתן לנתח דפוסי התנהגות חריגים כדי לבחון אם הם בעלי אופי לא מורשה או זדוני ולזהות הפרות אבטחה. כחלק מפעילות הניטור ניתן להשתמש בטכנולוגיית הטעיה כדי לפתות גורמים רשלניים או בעלי כוונת זדון מתוך הארגון ולחשוף את כוונותיהם או מעשיהם (Liu et al., 2018).

סיכום

הצמיחה המהירה בתחומי טכנולוגיות מידע ורשתות הביאה לעלייה אקספוננציאלית בשימוש במערכות אלו בכל תחומי החיים, אך יחד עם הקדמה הגיעה גם דאגה מרכזית של ארגונים לסוגיית אבטחת המערכות והנתונים. אולם בעוד שרבים ממערכי ההגנה עוסקים בגילוי ומניעה של חדירה של גורמים חיצוניים למערכות המידע הארגוניות, רק תשומת לב מעטה ניתנת ל"אויב שמבפנים" – משתמשים מורשים מתוך הארגון שעלולים לפגוע באבטחת המערכות, בין אם בשוגג ובין אם בזדון.

ההכרה בקיומו של "האיום מבפנים" והצורך להתמודד עימו התפתחו בהדרגה, בעיקר בשני העשורים האחרונים, כאשר אותן התפתחויות טכנולוגיות שהעצימו את האיומים למערכות המידע הן גם אלו שאפשרו מידול וניתוח מידע ופיתוח מהיר של כלים לאיתור וניטור איומים פוטנציאליים מבפנים. יישומה של אסטרטגיה רב שכבתית לזיהוי, איתור וניטור איומים מבפנים היא אבן בניין הכרחית בהתמודדות עם "האיום מבפנים", אבל האיום הזה עדיין מהווה אתגר משמעותי להנהלת הארגון בכלל ולמנהלי מערכות המידע בפרט – בעיקר כי ההתנהגות האנושית אינה תואמת במדויק למודלים.

מאמר זה מתמקד באיום מבפנים בארגונים, אך לתחום הסייבר בכלל ולאיום מבפנים בפרט יש גם היבטים והקשרים מדינתיים ובין-לאומיים. גורמי סייבר מדינתיים מפרסמים מידע רלוונטי מתוך תקווה שההמלצות, הכלים והאמצעים יאומצו כנורמות בסיסיות ומקובלות ברמת הארגון. על הארגון ללמוד מקרוב על התרעות והמלצות של ארגוני הסייבר הלאומיים ולמלא אחר הרגולציה בתחום. כמו כן, במקרה של תקיפת סייבר (חיצונית או פנימית) הארגונים יכולים לפנות לקבל סיוע מהמדינה. סיכוני האיום מבפנים מתגברים בצורה משמעותית בארגונים רב-לאומיים בגלל הפריסה הגיאוגרפית הרחבה והשוני התרבותי. בנוסף, ארגונים בפריסה רב-לאומית נדרשים גם לעמוד (לפעמים במקביל) בסטנדרטים ותקנות שמשתנים בין מדינות, ולעקוב אחר פרסומי סייבר והתראות במדינות היעד שבהן הם פועלים כדי לענות לדרישות מקומיות שמשפיעות על הסביבה העסקית במדינה. נושא זה מהווה אפיק מעניין למחקרי המשך בתחום.

פרופ' משה צבירן zviran@tau.ac.il

רשימת המקורות

Anderson R.H., Bozek T., Longstaff T., Meitzler W., Skroch M., and Van Wyk K., (2000), Research on Mitigating the Insider Threat to Information Systems, *Proceedings of a Workshop* (August 2000), Santa Monica, CA: RAND Corporation.

Bishop M., (2005), Position: Insider is Relative, *Proceedings of the New Security Paradigms Workshop*, ACM press, New York, USA.

Bojanova I., (2014), The Digital Revolution: What's on the Horizon? *IT Professional*, 16(1), 8-12.

Ding O., Han Q.-L., Xiang Y., Ge X. and Zhang X.M., (2018), A survey on security control and attack detection for industrial cyber-physical systems, *Neurocomputing*, 275 (1), 1674-1683.

Early G. and Stott, W., (2015), Preemptive Security through Information Analytics, *Information Security Journal*, *24*(1), 48-56.

Eldardiry H., Bart E., Liu, J. Hanley J., Price B. and Brdiczka O., (2013), Multi-Domain Information Fusion for Insider Threat Detection, *IEEE Security and Privacy Workshops*, San Francisco, CA, 2013, 45-51.

Erlich Z. and Zviran M., (2010), Goals and Practices in Maintaining Information Systems Security, *International Journal of Information Security and Privacy*, *4*(3), 40–49.

Feenberg A. (2010), *Between Reason and Experience: Essays in Technology and Modernity*, MIT Press, Boston, Massachusetts, USA.

Krogh G., Ichijo K. and Nonaka I., (2000), *Enabling Knowledge Creation: How to Unlock the Mystery of Tacit Knowledge and Release the Power of Innovation*, Oxford University Press, New York, USA.

Kroll , *Annual Data Breach Trends*, www.kroll.com/en-us/data-breach-trends-report, 2015

Liu L., De Vel O., Han Q., Zhang J., and Xiang Y., (2018), Detecting and Preventing Cyber Insider Threats: A Survey, *IEEE Communications Surveys & Tutorials*, *20*(2), 1397-1417.

Louis, M., Adrian, B., & Evangelos, R. (2016), *Threat Landscape 2015*, ENISA - European Union Agency for Network and Information Security.

Moore A.P, Kennedy K.A. and Dover T.J., (2016), Introduction to the Special Issue on Insider Threat Modeling and Simulation, *Computation and Mathematical Organization Theory*, *22*(3), 261-272.

PwC/HM Government (2015), *2015 Information Security Breaches Survey*. PwC, United Kingdom

Stenberg R. and Preiss D., (2005), *Intelligence and technology: The impact of tools on the nature and development of human abilities*, Erlbaum, New Jersey, USA.

Wall, D.S., (2011), Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders, *White Paper: Data Loss Prevention*, Symantec, Mountain View, CA, 2011, 9-10.

Wiseman D., (2018), *An Introduction to California Trade Secrets law*, https://corporate.findlaw.com/intellectual-property/an-introduction-to-california-trade-secrets-law.html ,October 2018.