קווים מנחים לניהול סיכוני סייבר

גבי סיבוני והדס קליין

תהליך הניהול של סיכוני סייבר הוא בעל חשיבות גבוהה ביותר כדי לשפר את מידת המוגנות והמוכנות הארגונית לאירוע סייבר. תהליך זה מהווה נדבך חשוב בניהול הסיכונים התפעוליים וכן בניהול הסיכונים הכולל של הארגון. במספר מגזרים במדינת ישראל מחויבים הארגונים לקיים תהליך ניהול של סיכוני סייבר על פי הנחיות הרגולטור. מטרתו של מאמר זה היא לבחון את המתודה של ניהול הסיכונים ולהציע קווים מנחים לניהול סיכונים במרחב הסייבר, תוך אפיון השלבים העיקריים בתהליך זה.

מילות מפתח: ניהול סיכונים, המשכיות עיסקית, סיכוני סייבר, מרחב הסייבר

מבוא

במאי 2017 התפרסמו ידיעות בתקשורת על גניבת פרטי לקוחות של חברת Kmart. זוהי הפעם השנייה בתוך שלוש שנים שפרטי לקוחות החברה נגנבים. מספר בנקים קטנים בארצות הברית דיווחו שקיבלו התראות מחברות כרטיסי אשראי על כמה קבוצות של כרטיסי אשראי גנובים, שלכולם היה מכנה משותף: שימוש לצורך רכישות בענקית הקמעונאות Kmart. חברת "סירס", החברת האם של Kmart, אישרה בעקבות הפרסום שחלק ממערכות התשלומים שלה נפגעו על ידי קוד עוין. לדברי החברה, לא ניתן היה לזהות את הקוד באמצעות מערכות הגילוי המוקדם, אולם לאחר זיהוי האירוע, הנוזקה הוסרה מהמערכות. החברה האם לא התייחסה לשאלה כמה מ־735 החנויות של Kmart נפגעו מהאירוע.[1]

תגובתה של חברת "סירס" היא עדות נוספת לתובנה הידועה כי יש חשיבות קריטית למניעת אירוע סייבר, אף יותר מהיכולת לזהותו ולהתאושש ממנו. במקרה

ד"ר גבי סיבוני הוא ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. הדס קליין היא חוקרת בתוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

1 Brian Krebs, "Credit Card Breach at Kmart Stores. Again", *KrebsOnSecurity*, May 2017, https://krebsonsecurity.com/2017/05/credit-card-breach-at-kmart-stores-again.

של Kmart, הדבר היה משמעותי במיוחד: החברה הותקפה לראשונה באוקטובר 2014 וטרם התאוששה מאז; מכירותיה ירדו ב־72 אחוזים ומחיר המניה שלה ירד ב־88 אחוזים מאז אירוע הסייבר הראשון.[2]

ההתייחסות לאירועי תקיפה אלה כרצף של אירועים בודדים ולא ככשל מערכתי עלולה להיות בעייתית, במיוחד כאשר היא גוררת התייחסות חסרה לפתרון שצריך להיות מערכתי. תהליכי ניהול סיכונים בסייבר ובמערכות המחשוב התומכות באים לענות בדיוק על בעיות מערכתיות כאלו. חברת Kmart לא סיפקה נתונים מפורטים על האירוע, אולם גורמים המעורים בנושא ציינו, שאף כי יתכן שמקור הבעיה היה גורם בשרשרת האספקה או רשלנות של עובד, ניתן להניח ששורש הבעיה בשני המקרים היה זהה: ניהול סיכונים גרוע, חוסר שקיפות בין־ארגונית וקושי לזהות קשרי גומלין בין מערכות שונות.[3]

ניהול סיכונים תפעוליים ופיננסיים בארגונים הינו תורה מפותחת הממומשת כיום באופן נרחב, וארגונים רבים מיישמים גישה זאת בשנים האחרונות גם בתחום של ניהול סיכוני מערכות מחשוב וסייבר. מטרתו של מאמר זה היא לספק לעושים במלאכה קווים מנחים ומתודולוגיה לביצוע תהליך של ניהול סיכונים במרחב הסייבר. תחילה תובא סקירה תיאורטית על תחום ניהול הסיכונים והיתרונות שהוא מספק לארגונים, ובהמשך תפורט הצעה לתהליך היישום בפועל.

תיאוריה של ניהול סיכונים

ניהול סיכונים הוא מתודה שהפכה לנושא ללמידה ומחקר לאחר מלחמת העולם השנייה. מקור הידע המודרני של תחום זה הם שני ספרים שעסקו בתיאוריה של ניהול סיכונים ויצאו לאור סמוך לאמצע שנות השישים של המאה העשרים.[4] התהליך החל סביב בחינת סיכוני שוק, במטרה להגן מפני הפסדים כספיים העלולים להיגרם כתוצאה מאירועים ותאונות. בשנות השבעים של המאה העשרים התפתח הנושא בשוק הביטוח ובמערכת הפיננסית, ככלי לניהול סיכונים פיננסיים של מוסדות בנקאיים, בנקים וחברות ביטוח. ניתוח הסיכונים התפעוליים וסיכוני הנזילות הופיע בתחילת שנות התשעים של המאה.[5] מאז הפך תחום זה לפרקטיקה מקובלת במגוון ארגונים, בהם חברות עיסקיות, חברות תעופה, רשויות מדינתיות וכדומה.

2 Steven Minsky, "Kmart Cyber Breach: Another Failure in Risk Management", *LogicManager*, July 26, 2017, https://www.logicmanager.com/erm-software/2017/07/26/kmart-cyber-breach.

3 שם.

4 R. I. Mehr, B. A. Hedges, *Risk Management in the Business Enterprise* (Homewood, Illinois: R. D. Irwin, 1963); A. Williams, M. H. Heins, *Risk Management and Insurance* (New York: McGraw Hill, 1964).

5 Georges Dionne, "Risk Management: History, Definition and Critique", *Risk Management and Insurance Review*, Vol. 16, no. 2, Fall 2013.

ניהול סיכונים בעולם העיסקי מתבצע בתחומים רבים, ובהם: ניהול סיכונים תפעוליים, כלומר, הבטחה שהתשתיות התפעוליות של הארגון ימשיכו לתפקד גם במקרה של תקלות במרכיבים מהותיים; ניהול סיכונים פיננסיים, בכלל זה סיכוני אשראי, סיכוני מטבע וסיכוני שוק; ניהול סיכונים של תאימות לרגולציה, לחוק או לאתיקה.

מטרתו של תהליך ניהול הסיכונים היא להפחית את השפעתם של אירועים חריגים על הארגון. התהליך כולל את ניסוח תרחישי הסיכון העשויים לפגוע בארגון, הערכת פוטנציאל הנזק בעת התממשותו, הערכת הסבירות להתממשות התרחיש, תעדוף בקרות לטיפול בתרחישים על פי עוצמתם, שהינו שילוב בין השפעת הסיכון ובין ההסתברות להתממשותו, ולבסוף ניסוח תוכנית להפחתת הסיכון. מחזור החיים של תהליך ניהול הסיכונים יכלול בדרך כלל כמה שלבים.

שלב א': הגדרת תיאבון הסיכון הארגוני

תיאבון הסיכון הוא כמות הסיכון ברמה כללית שהארגון מוכן לקבל כדי לקיים את מטרותיו.[6] זהו ביטוי לנכונות הארגון לסבול רמות חשיפה גבוהות/נמוכות לסיכון ולחוסר ודאות, כדי להשיג את יעדיו האסטרטגיים. מקובל שתיאבון הסיכון נקבע על ידי הדירקטוריון וההנהלה.

קביעת תיאבון הסיכון היא תהליך סובייקטיבי, שנועד לאזן בין התשואות הפוטנציאליות המתלוות לנטילת הסיכון ובין ההפסד הפוטנציאלי ממנו. מסגרות תיאבון הסיכון מספקות להנהלה תמונה ברורה באשר לרצון ליטול סיכון ופרספקטיבה לאיזון בין סיכון לתמורה. תיאבון הסיכון של הארגון אינו סטטי. ההנהלה עשויה לדרוש לשנות את שיעור הסיכון שהיא מוכנה ליטול, בהתאם לנסיבות המתפתחות על ציר הזמן.

שלב ב': זיהוי תרחישי סיכון

איתור סיכונים, באמצעות עבודת מחקר הכוללת ניסוח של תרחישי סיכון על בסיס ההיסטוריה של התממשות סיכונים בארגון ומחוצה לו. תהליך זה מתבצע באמצעות סקירת התהליכים העיסקיים הקריטיים של הארגון, שמטרתה היא להבין את התהליכים המשמעותיים ביותר לתפקודו. אלה כוללים לרוב תהליכים מעולמות הייצור, התפעול והמכירות; סקירת נכסי הארגון התומכים בתהליכים אלה (כגון, כוח אדם, תשתית מחשוב, מכונות וכדומה); ניתוח החשיפה של הארגון לסיכונים שיכולים להשליך על התנהלותו, כמו ניתוח סיכונים משקיים (האטה משקית) והאופן שבו הם יכולים להשפיע על היקף המכירות בחברה, או ניתוח

6 "Principles for An Effective Risk Appetite Framework", *Financial Stability Board*, November 18, 2013.

סיכונים מגזריים, כגון השפעה של מצבה הביטחוני של מדינת ישראל על מגזר תיירות החוץ; ולבסוף, בחינת דרישות החוק והרגולציה, כמו, למשל, השפעת חוקי בטיחות, חוקי בנייה ועוד.

שלב ג': ניתוח תרחישי סיכון

סיכון מוגדר כהסתברות של התרחשות מזיקה מוגדרת, בשילוב עם התוצאה הנובעת מאותה התרחשות. סיכון הינו, לפיכך, מכפלה של שני פרמטרים: הסבירות שיתרחש תרחיש כלשהו, והשפעת הנזק הצפוי במידה והוא יתממש. התוצאה של מכפלת שני המדדים האלה קרויה הסיכון השורשי. זיהוי תרחישי הסיכון יתבסס על עבודת מחקר שתכלול ניתוח אירועים דומים בהיסטוריה של הארגון ומחוצה לו, קבלת חוות דעת ממומחים, דוחות ניהול/סקרי סיכונים קודמים, דוחות כספיים, הליכים משפטיים, נתונים על תביעות ביטוח ועוד.

עוצמת הנזק נבחנת בפרמטרים של נזק ישיר ונזק עקיף כתוצאה מתרחיש של פגיעה בארגון. נזק ישיר יכול להיגרם, למשל, כתוצאה מפגיעה ברציפות התפקודית של הארגון על רקע השבתת מערכות ואי־יכולת לייצר כמתוכנן. נזק עקיף יכול להיות, לדוגמה, פגיעה במוניטין של הארגון כתוצאה מאי־יכולת לעמוד בהתחייבויות, מתביעות משפטיות ועוד.

שלב ד': גיבוש תוכנית להפחתת הסיכון

חלק גדול ממערך הפעולות, הכלים והתהליכים בהם משתמשים ארגונים לצורך הפחתת הסיכון נקרא בקרות. מערך הבקרות בארגון כולל את כל הכלים הקיימים בתהליכי העבודה המתקיימים באותו ארגון בהקשר למושאי הסיכון. לא ניתן להפעיל ארגון באופן אפקטיבי ללא מערכת בקרות שיטתית ותקינה.

ניתן לחלק את סוגי הבקרות המופעלות בארגון למספר משפחות:

- **נקיטת פעולות לצורך מניעה** – כלומר, נקיטת צעדים למניעת הסיבה לכשל, ובכלל זה על ידי שינוי אופן הפעילות של הארגון. למשל, יתכן ותהליך ייצור מסוים נמצא מסוכן מדי, ועל כן תחליט ההנהלה להימנע ממנו.
- **נקיטת פעולות הסטה** – העברה של השפעת הכשל לגורם חיצוני, כגון קבלן משנה או חברת ביטוח.
- **בקרה מונעת** – בקרה שמטרתה למנוע מבעוד מועד התרחשותה של פעולה שאינה רצויה. לדוגמה, הגבלת הרשאות ממוחשבות בתחנות מחשב קריטיות.
- **בקרה מגלה** – בקרה שמטרתה לגלות פעולות לא רצויות שהתרחשו, כך שיתאפשר לארגון לתקן אותן לאחר מעשה. לדוגמה, הפקת דוח חריגים לניתוח וניטור פעולות חריגות.

- **בקרה מתקנת** – בקרה שמטרתה לתקן פעולות לא רצויות לאחר מעשה. לדוגמה, שחזור אוטומטי של נתונים לאחר קריסה של מערכת המחשב.
- **בקרה מפצה** – בקרה שמטרתה לתת מענה במקום שבו הבקרות הקיימות אינן חזקות מספיק.

שלב ה': ניתוח הסיכון השיורי

הסיכון השיורי הינו הסיכון שנשאר לאחר הטמעת התוכנית להפחתת הסיכון. המצב הרצוי הוא שלאחר יישום הבקרות, רמת הסיכון השיורי תהיה נמוכה יותר מרמת הסיכון השורשי של התרחיש המנותח. כמו כן נדרש שרמת הסיכון השיורי תהיה בגבולות התיאבון לסיכון שנקבע. אם הסיכון השיורי אינו קביל (גבוה מדי), יש ליישם בקרות נוספות שיורידו את הסיכון השיורי לרמה קבילה, כפי שנקבע על ידי ההנהלה בהגדרת תיאבון הסיכון.

החשיבות של ניהול סיכוני סייבר

הקצב המהיר של השינויים הטכנולוגיים, הגידול בכמות השירותים הדיגיטליים וזמינותם, ההתממשקות עם מערכות ותיקות והצורך ההולך וגדל בקווי תקשורת עם ספקים, יוצרים כר נרחב להתפתחותם של איומי סייבר ולחשיפתם של ארגונים רבים לסיכוני סייבר משמעותיים. בד בבד, חלה בעשור האחרון עלייה מתמדת במספרם של גורמי איום, בהיבטים של יכולות, זמינות, כלי תקיפה וקבוצות תקיפה. כתוצאה מכך, היה זה אך טבעי לעבור לניהול סיכוני סייבר בשיטות של ניהול סיכונים. ואף על פי כן, הדרך עדיין ארוכה עד להטמעה מלאה של מתודות אלו כדבר של שגרה.[7]

לאחר פירוט הגישה הכללית והמקורות התיאורטיים, ראוי לבחון את יתרונותיו של תהליך ניהול הסיכונים במרחב הסייבר. ניהול סיכוני סייבר הינו חלק מניהול הסיכונים התפעוליים ומניהול הסיכונים הכולל של הארגון. על פי סקר של Deloitte ישראל, שנערך בשנת 2017, יש עלייה משמעותית במספר הארגונים המנהלים סיכוני סייבר.[8] כשישים אחוזים מהחברות הגדולות בישראל אוספות ומנתחות מידע לצורך קבלת תמונה עדכנית של איומי סייבר. עוד עולה מהסקר כי יותר מחמישים אחוזים מהחברות הגדולות במשק מקיימות מסגרת לניהול סיכונים ומפעילות מדיניות הגנת סייבר תאגידית, וכי מספר דומה של חברות גדולות ערכו סקר סיכוני סייבר רוחבי בשנה שקדמה לדוח. נתונים אלה גבוהים מהממוצע בקרב כלל המשק בישראל, ועם זאת, יש עדיין מקום לשיפור רב במצב.

7 "השוק הישראלי ואיומי סייבר – תמונת מצב 2017", **דלויט ישראל**, 2017, https://www2.deloitte.com/content/dam/Deloitte/il/Documents/risk/Deloitte_Cyber_Infographic1.2.pdf

8 שם.

אימוץ גישה של ניהול סיכונים בתחום ביטחון הסייבר כולל שורה של יתרונות:

- **יתרונות פיננסים –** הטמעה מיטבית של מערך הגנות סייבר ופיתוח מדיניות אבטחת מידע נאותה מונעים הפסדים ישירים, כגון גניבת כסף, וכן הפסדים עקיפים, כגון פגיעה במוניטין, ובנוסף לכך קנסות בגין אי־עמידה בדרישות החוק והרגולציה. לדוגמה, הפרת הוראות התקנה הבין־לאומית של האיחוד האירופי להגנה על נתונים (General Data Protection Regulation) גוררת קנסות מינהליים של עד עשרים מיליון אירו, או עד ארבעה אחוזים מסך המחזור השנתי – הגבוה מבין השניים.[9] מתקפת סייבר גם עלולה להשפיע על מחיר המניה של החברה, כתוצאה מפגיעה חמורה באמון הלקוחות ו/או פגיעה במוניטין ובמותג שלה.
- **יתרונות אסטרטגיים –** התמודדות נאותה עם אתגר הסייבר באמצעות מערך הגנות אופטימלי מספקת לארגון תמונה בהירה של החשיפה לסיכוני סייבר. הדבר משפיע על מידת האמון שרוחשים בעלי העניין והמשקיעים בארגון וביכולותיו להשיג את מטרותיו.
- **יתרונות משפטיים –** שמירה על המידע שהארגון מחזיק, כמו גם שמירה על יתר הנכסים הדיגיטליים שלו, מוגדרות במדינות רבות בעולם על פי חוק כאחריות של המנהלים וחברי הדירקטוריון.
- **יתרונות תפעוליים –** אירוע סייבר עשוי להיות בעל השפעה על מגוון היבטים תפעוליים, ובהם שרשרת האספקה, תמחור הייצור, כוח אדם ועוד. לדוגמה, אירוע סייבר, שבמסגרתו נפגעו קווי התקשורת עם ספקי החברה, עשוי לגרור שיבושים משמעותיים בתהליך הייצור.
- **המשכיות עיסקית** – שכלול יכולות ההתמודדות עם אירועי סייבר ישפיע ישירות על יכולת הארגון לממש המשכיות עיסקית, או לפחות להקטין את משך הזמן עד לשובו לעבודה.

אתגר ביטחון הסייבר נתפס לעיתים כבעיה הנוגעת לאנשי מערכות מידע, שבידיהם גם מצויים הפתרונות לה, אולם ברור כיום שהבעיה נוגעת לא רק לכלים טכנולוגיים. אתגר ביטחון הסייבר הינו רחב היקף וכולל אנשים, תהליכים ארגוניים, טכנולוגיה ומדיניות ארגונית. כל אלה ועוד מהווים נדבכים חשובים ביותר בביטחון הכולל של הארגון ובאיתנותו.

ניהול סיכוני סייבר

התממשותם של סיכוני סייבר עלולה לשבש את פעילותם התקינה והמאובטחת של ארגונים ולגרום, בין היתר, למניעת שירות, לחשיפת מידע עיסקי או מידע

9 סעיף 83 לתקנה 2016/679 (EU) של הפרלמנט האירופי: Regulation (EU) 2016/679 of the European Parliament and of the European Council, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

על לקוחות, למחיקה ושיבוש נתונים ועוד. מאפיין מהותי בניהול סיכונים הוא פוטנציאל הפגיעה. פוטנציאל הפגיעה בסייבר מתבטא לא רק בנזק למידע בהקשר של משולש הסודיות, השלמות והזמינות, אלא גם בהיבטים הנוגעים לסיכונים אחרים, כגון: מוניטין, חוק ורגולציה והמשכיות עיסקית.

בשנים האחרונות הופצו מספר הוראות רגולציה בנושא ניהול סיכוני סייבר, כמו, למשל, הוראה לניהול בנקאי תקין 361 של בנק ישראל בנושא ניהול הגנת הסייבר.[10] ההוראה דורשת מהבנקים בישראל לנהל את סיכוני הסייבר שלהם כדי לצמצם את הסבירות להתממשותם. במסגרת קביעת המתודולוגיה לניהול סיכוני סייבר, נדרשים ארגונים להעריך את תרחישי הסיכון ולבחון את מערך ההגנות שלהם.

הנחיית משרד האוצר[11] קובעת כי גוף מוסדי בישראל יעריך את סיכוני הסייבר שלו באמצעות נקיטת הצעדים הבאים: זיהוי תהליכים, מערכות ונכסי מידע; מיפוי הסיכונים לתהליכים, למערכות ולנכסי המידע; מיפוי סיכונים שורשיים; מיפוי והערכת הבקרות למזעור סיכונים אלה, לרבות בחינה של מידת ההשפעה של הבקרות עליהם; ולבסוף הערכת סיכון שיורי בהתאם להשפעת הבקרות שיושמו.

כדי ליישם עקרונות אלה, מוצע לפעול לאור תרחישי סיכון הנגזרים מהתהליכים בארגון ומנכסי המידע המיועדים להגנה, ולהמשיך בהגדרת התרחישים של סיכוני הסייבר אליהם חשוף הארגון. משם מוצע לעבור להערכת הסיכון השורשי במצב של התממשות התרחיש, לניתוח בשלותו של מערך בקרות הסייבר באמצעות ניתוח רמת ההטמעה שלו, ולאחר מכן לעבור לניתוח מידת היעילות של בקרות הסייבר הזמינות בארגון. לבסוף מוצע לנתח את הסיכון השיורי ואת הפערים בהגנה, וכנגזרת מכך לתעדף את הטיפול באותם פערים על ידי גיבוש תוכנית עבודה.

הגדרת תרחישי הסיכון

ראשיתו של תהליך הגדרתם של תרחישי הסיכון היא בניתוח התהליכים העיסקיים הקריטיים של הארגון, ולצידם ניתוח המערכות והנכסים הדיגיטליים התומכים בתהליכים אלה. המשכו של התהליך הוא בניסוח תרחישי התקיפה האפשריים בסייבר. שלב זה מבוסס על איסוף וניתוח מודיעיני, ובכלל זה ניתוח מגמות תקיפה וניתוח תוקפים פוטנציאליים, כאשר התרחיש כולל פעולה של תוקף. כאשר התרחיש הינו אירוע לא מכוון במרחב הטכנולוגי, יש לנתח תרחישי תקלות. את תרחישי התקיפה שנוסחו יש למפות לתהליכים קריטיים ולמערכות התומכות בתהליכים אלה.

---

10 "הוראה 361, ניהול הגנת הסייבר", *המפקח על הבנקים, בנק ישראל*, https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/361.pdf.

11 "ניהול סיכוני סייבר בגופים מוסדיים", *מדינת ישראל, משרד האוצר – אגף שוק ההון, ביטוח וחיסכון*, 31 באוגוסט 2016.

ניתוח התהליכים הקריטיים וניתוח המערכות והנכסים הדיגיטליים התומכים בתהליכים אלה מתבצעים באמצעות תהליך הנקרא Business Impact Analysis (BIA). תהליך זה הינו חלק ממערך כלים רחב המיועד לתרום להמשכיות העיסקית ולעזור לארגון להתאושש במהירות האפשרית לאחר אירוע. BIA מהווה חלק מתוכנית ההתאוששות, בכך שהוא עוזר לאמוד את הנזקים השונים שנגרמו ואת חשיבותם היחסית של חלקי הארגון השונים. מסמך BIA ארגוני חסר לעיתים התייחסות להיבטים השונים של הסייבר, כגון סודיות ושלמות המידע. אם חסרה בו התייחסות כזאת, יש לעדכנה בהיבטי הסייבר הרלוונטיים. ניתוח BIA ומסמך אסטרטגיית הגנת הסייבר הארגונית צריכים לגזור רשימה מתועדפת של הנכסים הדיגיטליים המיועדים להגנה. במסגרת זו יש להגדיר את עקרונות ההגנה ויעדיה, כפי שהם מוכתבים על ידי דירקטוריון הארגון, הרגולטורים ובעלי עניין נוספים.

כדי להתמודד עם תרחישי התקיפה האפשריים במרחב הסייבר, נדרש לבצע הערכה של מרחב סיכוני הסייבר הארגוניים באופן שמתייחס למספר נקודות, ובהן: מיהם בעלי האינטרס לתקוף את הארגון? מהם יכולותיהם והכלים העומדים לרשותם? את מי הם תקפו בעבר וכיצד? הערכה זו אמורה להישען על תהליך מקדים של איסוף מודיעיני, הכולל ניתוח מגמות תקיפה, תוקפים פוטנציאליים וניתוח יכולותיהם.

איסוף מודיעיני הממוקד בצורכי הארגון מחייב להגדיר את רכיבי המידע הרלוונטיים לאיסוף. לעיתים מקובל לכנות פעולה זו צי"ח (ציון ידיעות חשובות). הצי"ח מגדיר את מגוון מקורות המידע הרלוונטיים ואת אזורי המיקוד לאיסוף מידע. למשל, ארגון בנקאי במדינת ישראל ראוי שימקד את איסוף המודיעין באיומים על התעשייה הבנקאית מצידם של ארגוני פשיעה, איומים שמקורם באויבים, ואף איומים שמקורם בארגונים אקטיביסטיים העשויים לפעול נגד מדיניות כלכלית מסוימת או נגד "קפיטליזם גלובלי".

תוצרי איסוף המידע משמשים לשתי מטרות עיקריות. הראשונה היא עדכון מתמשך של האיומים, שישמש את הפעילות הארגונית בהערכת המצב ובתגובה מהירה וממוקדת לאיומים חדשים; השנייה היא ניסוח תרחישי הסיכון איתם עשוי להתמודד הארגון, תוך ציון פרמטרים רלוונטיים לכימות האיום, ובהם סבירות הארוע, מידת הנזק ועוד. מקורות המידע לאיסוף המודיעין יכללו: מקורות מסחריים המספקים שירותי מידע (לאור צי"ח), מקורות זמינים חינמיים, שיתופי פעולה והחלפת מידע עם גורמים רלוונטיים, דוגמת מרכזי שיתוף מגזריים, גורמי CERT ואחרים, ולבסוף – מידע שמקורו במידע שהארגון מקבל מגורמי הנחיה.

הערכת הסיכון השורשי

תהליך הערכת הסיכון השורשי מבוצע בשני שלבים: הערכת פוטנציאל הנזק בהינתן התממשות התרחיש, והערכת הסבירות להתממשותו של התרחיש. הערכת פוטנציאל הנזק צריכה להתבצע תוך היוועצות עם הגורמים העיסקיים. אלה נדרשים להעריך את רמת הנזק הכספי בכל תרחיש, תוך ניתוח הסיכונים לנכסים העיסקיים האסטרטגיים, כפי שהוגדרו על ידי הארגון, ועליהם חשוב להגן. בנוסף, נדרש להעריך את הנזק הפוטנציאלי בכל תרחיש. לצד הנזקים הישירים, נדרש להעריך גם היבטים של נזק עקיף, כגון חשיפה לתביעות, חשיפה לעיצומים, פגיעה במוניטין ופגיעה ברציפות התפקודית.

הערכת סבירות התממשותו של התרחיש מתבצעת על פי רוב באמצעות מספר מדדים. הראשון שבהם נוגע לשכיחות התממשותו מבחינה היסטורית של תרחיש דומה בארגון דומה. יחד עם זאת, השוני בין אירועים בעולם התוכן של מתקפות סייבר והעובדה שקיים מגוון רחב מאד של תרחישי תקיפה ואירועים, גורמים לכך שלא ניתן להסתמך אך ורק על מדד זה, ונדרשים כלים נוספים כדי לאמוד את הסבירות להתממשות הסיכון. ניתן, לכן, לעשות שימוש בשני מדדים נוספים: הראשון הוא מדד המתאר את ההערכה הסובייקטיבית של צוות מודיעין הסייבר באשר לסבירות התממשותו של הסיכון, וזאת על בסיס הערכת המודיעין. הערכה זו מוצגת במדרג של 1־5, כאשר 5 מציין סבירות גבוהה להתממשות. המדד השני הוא רמת החשיפה המובנית, כלומר, עד כמה קל לתקוף את הנכסים המתוארים בתרחיש. החשיפה המובנת נקבעת לפי מאפיינים שונים של הסביבה הטכנולוגית הקיימת בארגון, כמו, למשל, כמות הממשקים, מספר המשתמשים, גישה לאינטרנט, ציוד תקשורת, קישוריות בין תחנות ועוד. לכל מאפיין קיימים מספר ערכים, המדַרגים את רמת החשיפה של הסביבה הטכנולוגית לתקיפות סייבר. גם הערכות אלו מתבצעות במדרג של 1־5, כאשר 5 מציין יכולת תקיפה בקלות מרובה. לדוגמה, ככל שיש לארגון יותר נקודות גישה לאינטרנט, כך קל יותר לתקוף אותו. ארגון בעל נקודת גישה אחת לאינטרנט יקבל, אפוא, ציון 1, וארגון בעל עשרות או מאות נקודות גישה לאינטרנט יקבל ציון 5. הערכה דומה מתבצעת לכל אחד מהמאפיינים. לצורך חישוב רמת החשיפה המובנית מבוצע שקלול של ממוצע הציונים בפרמטרים השונים.

חישוב מידת הסבירות להתממשות הסיכון מתבצע באמצעות הצבת מדד הערכת חוקר המודיעין (Analyst Score) ומדד החשיפה המובנית (Risk Exposure) במשוואה שלהלן, והערכת הסבירות תתבצע באמצעות הנוסחה הבאה:[12]

12 כל הערכים במדרג שבין 1–5.

$$RL\ (Risk\ Likelihood) = \frac{RE\ (Risk\ Exposure) \times AS\ (Analyst\ Score)}{5}$$

משוואה 1

RL הינה הסבירות להתממשות הסיכון, *RE* הינו ציון החשיפה המובנית, *AS* הינו ציון הניתן על ידי חוקר המודיעין לסבירות התממשותו של הסיכון. מטרת החלוקה ב־5 היא לאפשר לדרג את הסבירות בין 1־5.
הסיכון השורשי מחושב באופן הבא:

$$IR\ (Inherent\ Risk) = \frac{RL\ (Risk\ Likelihood) \times RI\ (Risk\ Impact)}{5}$$

משוואה 2

IR הינו הסיכון השורשי (Inherent Risk), *RL* הינה סבירות הסיכון (Likelihood) ו־*RI* הינו השפעת הסיכון (Impact).[13] מטרת החלוקה ב־5 היא לאפשר לדָרג את הסבירות בין 1־5.
תהליך הניתוח של המערכות התומכות בתהליכים הקריטיים בארגון, תהליך איסוף המודיעין וניתוחו לכדי איומים, והשלמת ניתוח הסיכון, מאפשרים להעריך את סיכוני הסייבר הקריטיים לארגון. להלן דוגמה:

שם האיום	שם האיום לצורך שפה משותפת
גורם האיום	גורם האיום מתוך המידע המודיעיני שנאסף
נתיב התקיפה	נתיב מימוש התקיפה מתוך המודיעין והמידע הטכנולוגי של הארגון
מערכת קריטית מושפעת	מתוך רשימת המערכות התומכות בתהליכים הקריטיים
סבירות	הערכת הסבירות להתממשות התרחיש
נזק	הערכת פוטנציאל הנזק בהתממשות התרחיש
הסיכון השורשי	מדד הסיכון השורשי, כפי שחושב בעזרת נוסחת הסיכון השורשי

13 הגישה המוצגת במאמר זה לחישוב הסיכון השורשי הינה אחת ממספר גישות קיימות, והיא מובאת כאן לצורך הדגמה.

הערכת בשלותן של הגנות הסייבר

מקובל לסווג את הבקרות בתחום הסייבר לשלוש משפחות עיקריות:

- הראשונה – בקרות מונעות (Preventives controls), המיועדות לסייע בניטור ובפיקוח על נתונים ופעילויות, במניעת שגיאות, מחדלים או נזק מכוון. דוגמאות לבקרות מסוג זה הן הפרדת תפקידים והרשאות, בקרת כניסה, איסוף וניתוח מודיעין סייבר.
- השנייה – בקרות מגלות (Detective controls), המסייעות באיתור חריגים. דוגמאות לבקרות מסוג זה הן מערכות לגילוי אנומליות בהתנהגות משתמשים, כגון משתמש העובד בשעות לא סבירות ומבצע פעולות שאינן בשגרת עבודתו ותפקידו.
- השלישית – בקרות מתקנות (Corrective Controls), המסייעות בעיקר להחזיר את המצב לקדמותו או לסייע בהשבת השגרה (לדוגמה, תהליך גיבויים ושחזורים), ואף לשפר את ההגנה.

ראוי שמערך הבקרות הכולל יותאם לארגון על פי צרכיו. קיימים כיום מספר תקנים והנחיות המתארים מבנה כללי של מערך בקרות. דוגמאות להם ניתן למצוא בהמלצות של מכון התקנים האמריקאי (NIST) המנחה ארגונים פדרליים,[14] ושל הגוף האמריקאי הפדרלי הקובע תקנים המיועדים למגזר הבנקאות בארצות הברית (FFIEC).[15] כמו כן, ניתן להסתייע בתורת ההגנה בסייבר שנכתבה על ידי מערך הסייבר הלאומי בישראל.[16] הערכת בשלות הבקרות מתבצעת עבור כל בקרה בנפרד, באמצעות ניתוח שני מדדים: מדד רמת ההטמעה של הבקרה ומדד מידת היעילות של הבקרה.

לצורך הערכת בשלות הבקרות יש לקיים ראיונות עם גורמים טכנולוגיים בארגון ועם גורמים נוספים, כגון היחידה לניהול סיכונים (אם יש כזאת). לכל בקרה יש לנסח טבלת דירוג ייחודית לה, שבמסגרתה יש להגדיר את סולם ההערכה של רמת הטמעת הבקרה בארגון. ניתוח זה מתבצע בהתאם לפרמטרים ייחודיים לכל בקרה. פרמטרים אלה מנוסחים במדרג של 1־5, כאשר 5 מבטא הטמעה מיטבית. בטבלה שלהלן ניתנת דוגמה להמחשת העניין. הדוגמה מנתחת את בקרת המודעות של העובדים לסיכוני סייבר:

---

14 "NIST Cybersecurity Framework", https://www.nist.gov/cyberframework;

15 "Cybersecurity Assessment Tool", *Federal Financial Institutions Examination Council (FFIEC)*, https://www.ffiec.gov/%5C/cyberassessmenttool.htm.

16 "תורת ההגנה בסייבר לארגון", *מערך הסייבר הלאומי, משרד ראש הממשלה*, https://www.gov.il/he/Departments/policies/cyber_security_methodology_for_organizations.

הערכת הטמעת הבקרה	ציון
לא קיים תהליך למודעות עובדים	1
תהליך בסיסי למודעות – הדרכות, עלונים, פורטל ארגוני	2
תהליך מתקדם למודעות – בסיסי, כולל תרגילים כלליים	3
קיים תהליך ארגוני מתקדם, כולל בקרה ומדידת ביצועים	4
קיים תהליך ארגוני מתקדם, לצד תהליך חיצוני, למודעות של שותפים עיסקיים לסיכוני סייבר	5

בנוסף, יש לקבוע לכל בקרה משקל המציין את חשיבותה למערך ההגנה הכולל של הארגון. המשקל נקבע במדרג של 1־5. ככל שהבקרה משמעותית יותר למערך ההגנה, כך משקלה מוערך כגבוה יותר. עם סיום תהליך הערכת המדדים הללו, ניתן לקבוע את ציון בשלות הבקרה באמצעות שימוש במטריצה שלהלן:

$CM =$

הטמעת הבקרה CA \ חשיבות הבקרה CI	1	2	3	4	5
1	5	3	2	1	1
2	5	3	2	2	2
3	5	4	3	3	3
4	5	4	4	4	4
5	5	5	5	5	5

בשלות הבקרה (CM) הינה פונקציה של חשיבות הבקרה (CI) ורמת הטמעת הבקרה בארגון (CA), ונקבעת בהתאם לערכי המטריצה.

ציוני בשלות הבקרות ייקבעו על פי הערכים המצוינים במטריצה. באופן זה ניתן לקבוע תוכנית מתועדפת לטיפול בבקרות. ככל שציון בשלות הבקרה נמוך יותר, כך הבקרה נמצאת בעדיפות גבוהה יותר לטיפול. משמעות הדבר היא שבקרות שנמצאות בראש הרשימה יתרמו באופן המיטבי לשיפור מערך ההגנות הכולל.

ערכי המטריצה מתייחסים למצבי קיצון, באופן הבא: אין צורך להשקיע משאבים בטיפול בבקרה בעלת חשיבות 1 (נמוכה). על כן, ערך בשלות הבקרה עבור כלל הבקרות בעלות חשיבות 1 הינו 5. בנוסף, אין רלוונטיות בהשקעת משאבים בטיפול בבקרה בעלת רמת הטמעה 5 (מרבית), ועל כן, ערך בשלות הבקרה עבור כלל הבקרות בעלות רמת הטמעה 5 הינו 5.

חשוב להתייחס גם לעלויות הטיפול בבקרה. כך, למשל, טיפול בבקרה שעלות התקנתה ותחזוקתה הינה יקרה באופן שיכֵלה חלק משמעותי מתקציב מערך ההגנה, אינו בהכרח אפקטיבי, גם אם ההגנה נמצאת בראש רשימת העדיפויות. במקרה כזה ניתן לבצע נרמול, באופן שישקף את העלות היחסית של הבקרות.

ניתוח הסיכון השיורי

רמת הסיכון השיורי מתארת את פוטנציאל הנזק שעלול להיגרם לארגון כתוצאה מאירוע סייבר המתרחש לאחר יישום הבקרות הקיימות. כדי שהארגון יוכל להתמודד עם סיכוני הסייבר, עליו להעריך את רמת הסיכון השיורי עבור כל תרחיש בנפרד, כפי שהיא זוהתה בשלבים מוקדמים יותר בתהליך. חישוב הסיכון השיורי מבוצע בהתאם לנוסחה הבאה:

$$RR\ (Risidual\ Risk) = IR\ (Inherent\ Risk) - w \times CS\ (Control\ Score)$$

משוואה 3

כאשר: RR הינו הסיכון השיורי (Residual Risk), IR הינו הסיכון השורשי, CS איכות הבקרות הזמינות (Controls Score), ו־w הינו מקדם לאיכות הבקרות. לעיתים מקובל לקבוע מקדם עבור חישוב הסיכון השיורי, באופן שבו איכות הבקרות הזמינות מופחתת באחוז מסוים, כדי ליהנות מדרגת ביטחון גבוהה יותר בסיכון השיורי. למשל, קובעים כי ההתייחסות לאיכות הבקרות מופחתת בשלושים אחוזים. במצב כזה נדרש להציב בנוסחה $w=0.7$.

חישוב הסיכון השיורי מחייב להגדיר את הציון הכולל של מערך הגנות הסייבר בתרחיש הנדון, וזאת באמצעות הנוסחה הבאה:

$$OCM\ (Overall\ Control\ Maturity) = \frac{\sum_{i=1}^{n} CM_i\ (Control\ Maturity)}{n}$$

משוואה 4

ציון בשלות הבקרות הכולל (OCM) הינו ממוצע n ציוני בשלות הבקרות CM_i בתרחיש הנדון. חישוב הסיכון השיורי עבור כל תרחיש מתבצע באמצעות הנוסחה הבאה:

$$RR\ (Residual\ Risk) = IR\ (Inherent\ Risk) - w \times OCM\ (Overall\ Control\ Maturity)$$

משוואה 5

RR הינו הסיכון השיורי (Residual Risk), IR הינו הסיכון השורשי, CS היא איכות הבקרות הזמינות (Controls Score), ו־w הינו מקדם לאיכות הבקרות.

כעת יכול הארגון להעריך האם הסיכון השיורי תואם את תיאבון הסיכון, כפי שהוגדר על ידי הנהלת הארגון. אם מזוהים פערים, יש לשוב לפרק תעדוף הבקרות ולנסח תוכנית עבודה לשיפור מערך ההגנות, או לחילופין, להקטין פעילות מסוכנת בסייבר.

סיכום

מטרתו של מאמר זה היא לספק קווים מנחים לניהול סיכונים במרחב הסייבר, תוך הישענות על התיאוריה הבסיסית של דיסציפלינת ניהול הסיכונים שהתפתחה מאז שנות השישים של המאה העשרים. המאמר מציג גישה אחת לתהליך המוצע. קיימות גישות נוספות, אולם רובן ככולן נשענות על הבסיס התיאורטי של תורת ניהול הסיכונים.

ניהול סיכוני סייבר הינו מרכיב קריטי במסגרת ניהול מערך הגנות הסייבר הארגוני, לצד פעולות נוספות, דוגמת מבדקי חדירות. תהליך זה מאפשר לארגון להעריך את מידת הסיכון הניצבת מולו, מגדיר באופן מתודי את בחינת אמצעי ההגנה הארגוניים, ולבסוף מאפשר לארגון להעריך האם מידת החשיפה לסיכון תואמת את המוגדר והנדרש על ידי הדירקטוריון, הנהלת הארגון ובעלי העניין השונים.

מימוש הקווים המנחים שתוארו לעיל אינו ערובה למניעת אירועים במרחב הסייבר, אולם יש בו כדי להביא להבנה עמוקה יותר של הגורמים המטפלים במערך ההגנה נגד אותם סיכוני סייבר עימם הם נדרשים להתמודד. בכך הם יכולים לסייע רבות להקטנת הסיכונים מולם ניצב הארגון במסגרת צרכיו העיסקיים. לפי הערכת מומחים, הבעיה המערכתית שהתגלתה בחברת Kmart באירועי התקיפה שתוארו לעיל, הייתה מימוש גרוע של תהליכי ניהול הסיכונים.[17] מימוש תהליך ניהול סיכונים שיטתי וסדור יכול לסייע בצמצום החשיפה לסיכונים ובהקטנת הנזק התדמיתי והכספי העלול להיגרם באירועים מסוג זה.

17 Minsky, "Kmart Cyber Breach".