הריגול בסייבר והשפעתו על שיקולי חברות עסקיות

גבי סיבוני ודוד ישראל

מרחב הסייבר הופך לכלי העיקרי והיעיל לריגול עסקי ולגניבת מידע וקניין רוחני. הוא מאפשר לתוקף קיצור דרך טכנולוגי, ההופך ליתרון תחרותי ועסקי בשוק בכלל ומול הנתקף בפרט. מאמר זה בוחן את מידת ההשפעה של הצורך להתמודד עם סיכוני הסייבר בכלל ועם אבטחת המידע הארגוני בפרט על השיקולים של מקבלי ההחלטות בחברות עסקיות. מדובר בהחלטות הקשורות לשיקולים של כדאיות הכניסה לפיתוח, תשומות ההגנה על המידע, אורך חיי המוצר ועצם הכדאיות העסקית בכניסה לתחומים חדשים. המאמר גם מעלה מספר רעיונות לסיוע בתחומים אלה ברמה הלאומית.

מילות מפתח: סייבר, ריגול, ריגול עסקי, אבטחת מידע, קניין רוחני, פשיעת סייבר, גניבת סייבר, טכנולוגיה.

רקע

ריגול עסקי אינו דבר חדש, וקיים בגלגולים שונים מאז שחר ההיסטוריה. ידועות מהפכות תעשייתיות היסטוריות אשר התבססו על העתקת ידע. כך, למשל, מכונות תעשייתיות מבריטניה מצאו את דרכן לארצות הברית וסייעו בהפיכתה למעצמה תעשייתית על חשבון פטנטים בריטיים.[1] בעולם העסקי, ריגול תעשייתי נחשב בדרך כלל כאחד האיומים הגדולים על היכולת של ארגון להתקיים בתוך השוק התחרותי בו הוא מתמודד. הנחת היסוד בעולם זה הייתה שהסיכון של גניבת מידע ואובדן מידע המשמש כקניין רוחני יכול להתממש בעיקר כתוצאה מאיום פנימי, כמו עובד ממורמר, סוכן מושתל או אף שיטוי של עובד נאמן. איום

ד"ר גבי סיבוני הוא ראש התוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי.
דוד ישראל הוא מומחה לאבטחת מידע בחברת "מוטורולה ישראל" ומתמחה בתוכנית לביטחון סייבר במכון למחקרי ביטחון לאומי.

זה יכול להתממש גם כתוצאה מהעתקת מוצר ו"הנדסה לאחור" שלו (Reverse Engineering).

ההתגוננות מפני ריגול תעשייתי התמקדה עד לפני כעשור בהגנת המרחב הפיזי, למשל באמצעות מתחמים ממודרים, בקרות כניסה ומצלמות אבטחה. זאת, לצד בחינת המהימנות של עובדים וגורמים בשרשרת הפיתוח והייצור, ובכלל זה תחקירים ביטחוניים, בדיקות אמינות של עובדים, בחינת ספקים ועוד. ההגנה התבססה בעיקר על מניעת גישה למידע ולקניין רוחני הנמצאים בתוך המתחם הפיזי של הארגון ועל צעדים למניעת האפשרות להדליף מידע זה על ידי גורם פנימי מורשה או על ידי גורם זר שחדר את מעטפת ההגנה הפיזית.

ההגנה על המידע הארגוני ועל הקניין הרוחני נשענה וממשיכה להישען גם על רישום פטנטים והסכמים משפטיים, דוגמת הסכמי סודיות בין חברות וספקים, וזאת בהנחה שארגון יוכל לתבוע את זכויותיו מגופים שיפגעו בקניינו הרוחני. המידע הרגיש כולל לא רק קניין רוחני, אלא גם מידע העלול לפגוע בארגון במגוון דרכים, כמו פרטי חוזים, מרכיבי שכר (לצורך ציד של כישרונות מיוחדים), מידע לגבי מכרזים והצעות מחיר, תוכניות אסטרטגיות, תוכניות שיווק, רשימת לקוחות וספקים ועוד.

התפתחות השימוש במרחב הקיברנטי לצורכי פיתוח טכנולוגי ולצורכי ייצור[2] חושפת מרחב סיכון משמעותי לדליפת מידע רגיש וקניין רוחני. למעשה, התפתחות זאת שינתה את כללי המשחק בתהליכי אבטחת המידע והקניין הרוחני והפכה את ההגנה עליהם למורכבת יותר, עתירת משאבים ובעלת השפעה משמעותית על תהליכי העבודה וזרימת המידע בארגון. ההבנה הקיימת בקרב הנהלות בכירות בארגונים היא כי ידו של התוקף הינה על העליונה וכי סיכויי ההצלחה שלו גבוהים. זאת, לעומת המגבלות של המתגונן במרחב הקיברנטי. באחד המחקרים של חברת ייעוץ גדולה אף נטען כי כשישים אחוזים מהמנהלים הבכירים מאמינים שהתקפות הסייבר יגברו ויהפכו למתוחכמות ובעלות קצב מהיר יותר מאשר יכולת הארגונים להתמודד איתן.[3]

על רקע דברים אלה, מתחולל כיום שינוי עמוק בתהליכי קבלת ההחלטות הקשורות במחקר ופיתוח ובשיקולים שארגונים עסקיים ומסחריים נדרשים לשקלל בכל הקשור להשקעות בתחומים אלה. עוצמת האיום לגניבת מידע וקניין רוחני מחייבת את הארגונים להתייחס בצורה רצינית לנושא ההגנה עליהם. הגנה כזאת מחייבת הקצאה של משאבים לא מעטים, ובכלל זה משאבים טכנולוגיים, כמו גם יישום תקנים ונוהלי עבודה מתאימים. אלה מעמיסים על המשאבים האנושיים ועל עלויות הפיתוח, ובכך מצמצמים למעשה את ההשקעות בפועל בפיתוח עצמו. בהקשר זה על הארגון לשאול מספר שאלות יסודיות, כמו: מהן החולשות הקריטיות בתהליך העסקי ואיך יש להגן מפניהן? מה צפויה להיות העלות הנוספת

הכרוכה בהגנה על המידע ובמערך האבטחה שיידרשו בתהליך המחקר והפיתוח? האם ניתן יהיה להקים את מערך האבטחה הנדרש קודם להתנעת הפיתוח, והאם כתוצאה מכך גדל הסיכון העסקי של כניסה מאוחרת לשוק? מכיוון שברור שכל הגנה עלולה להיפרץ, יש גם לשאול מה תהייה היכולת להתאושש מפגיעה בתהליך העבודה במהלך הפיתוח ומה תהייה ההשפעה של הפריצה על ההשקעה הכוללת, וכן אילו עיכובים צפויים בתהליכי הפיתוח כתוצאה ממגבלות שיתוף מידע ומה תהיה השפעתם? כל תהליך פיתוח מחייב שותפות של גורמים חיצוניים, ולעיתים מיקור חוץ. בהקשר זה יש לשאול באיזו מידה נדרש יהיה להשקיע משאבים בהגנה במצבים כאלה, או לחייב ספקים חיצוניים לממש הגנות נוספות, דבר שעשוי לייקר את השירות?

א. זוהי רשימת שאלות חלקית, אולם היא מבהירה עד כמה השתנה תהליך קבלת ההחלטות בעידן איומי הסייבר ועד כמה משמעותית ההשקעה בתהליכי האבטחה שנועדו להתמודד איתם. שיקולים של איומי סייבר, המתווספים כנדבך רב־משמעות לכלל השיקולים העסקיים, עשויים להביא ארגון לקבל החלטה להימנע מכניסה לפיתוח טכנולוגי בתחומים המועדים להיות מטרה אטרקטיבית לריגול מסחרי. רגיש במיוחד בהקשר זה הוא מצבה של תעשיית חברות ההזנק. אלו נמצאות בדרך כלל במצוקת משאבים ומשקיעות את כל הונן בפיתוח הטכנולוגי, כך שיתקשו מאוד להשקיע את המשאבים הנדרשים כדי להגן בצורה מספקת על נכסי הקניין הרוחני שלהן. כתוצאה מכך, תעשיית החדשנות הינה התעשייה החשופה ביותר לאיומי סייבר הנוגעים לגניבת קניין רוחני.

ב. ישראל הינה מדינה בעלת תשתית טכנולוגית ענפה הכוללת, בין השאר, חברות הזנק רבות המפתחות מוצרים ופתרונות חדשניים. על רקע זה ראוי לבחון את תפקידה של המדינה בסיוע לאבטחת הקניין הרוחני המפותח בה, במיוחד זה המפותח כתוצאה מהשקעות הממומנות על ידי המדען הראשי של משרד הכלכלה.

ג. חברות חשופות לפגיעה במרחב הסייבר לא רק בהקשרי ריגול מסחרי, אלא גם בהקשרים של תקיפות סייבר הנעשות לצורך פגיעה, השבתה וגרימת נזק. גם התקפות כאלו מחייבות התייחסות והגנה. עם זאת, לצורך המיקוד, מאמר זה מבקש לבחון את משמעות הצורך להשקיע באבטחה והגנה על מידע קניין רוחני ועל תהליכי הפיתוח והמחקר, וכיצד שיקולי אבטחה אלה עשויים להשפיע על היקף ההשקעות במו"פ בכלל. כמו כן, המאמר מבקש לבחון כלים שיסייעו לחברות לעמוד בצורכי ההגנה שלהן על ידי מאמצים משותפים ויוזמות בין חברות עסקיות שונות. לצד זאת בוחן המאמר את תפקיד המדינה ביצירת

תשתית אבטחה שתוכל לסייע לחברות קטנות וגדולות לשפר את ההגנה על מידע קניין רוחני ואת מוכנותן להתמודד עם איומי הסייבר.

מורכבות ההגנה על תהליכי יצירת קניין רוחני

אחד ממוקדי המידע הרגישים ביותר להגנה הינו הקניין הרוחני, המהווה את הנכס העיקרי של חברות טכנולוגיות וחברות הזנק. כדי להבין את מורכבות ההגנה על תהליכי יצירתו של קניין רוחני – הווה אומר מורכבות אבטחתו של חוד החנית העסקי ושמירה על היתרון התחרותי הקריטי לקיומו של ארגון – נדרש לנתח את מחזור חייו של המידע. לצורך זה נתייחס למחזור חייו של פיתוח מוצר בחברת היי־טק.

פיתוח מוצר טכנולוגי מתאפיין בשלבים העיקריים הבאים: ייזום הרעיון, אפיון, יצירת אב טיפוס, בדיקות מעבדה ומעבר לייצור. מיותר לציין שכל השלבים המלווים את ייזום ופיתוח הרעיון, עד הבשלתו כמוצר סופי וייצורו, הינם תהליכים דיגיטליים מבוססי מערכות מידע שונות ומגוונות, הנותנים מענה לכל אחד משלבי הפיתוח והיצירה של הקניין הרוחני. כפועל יוצא מכך, כל אחד מהשלבים בתהליך יוצר מוטיבציה לתוקף והינו רלוונטי למתקפת סייבר אפשרית, אם באמצעות רשת האינטרנט ואם באמצעות גורם פנימי הפועל בשוגג או בזדון.

עקרונית, ובצורה מופשטת ביותר, מטרת הארגון היא לאתר את הנקודות הרגישות בתהליך ולמקד את הגנות הסייבר באזורים אלה. בפועל, ניתוח הסיכונים, המתבסס על תהליכי זרימת המידע וחשיבותו בתהליך הפיתוח, הופך מהר מאוד לתמנון רב־זרועות המצריך התייחסות אבטחתית מעמיקה. הזנחתו של ערוץ מסוים, או הערכת חסר של חשיבותו, עלולות להיות נקודות התורפה של מערך ההגנה בכללותו. המורכבות של ההגנה על כל אחד משלבי הפיתוח מושפעת מהעובדה כי כל אחד מהתהליכים מתאפיין בשימוש בכלים ובטכנולוגיות מגוונים ובעבודה בסביבה שונה ומצריך תמיד יכולות של שיתוף מידע. בכל אחד מהשלבים נדרש הארגון להעריך את הצורך במתן מענה לסיכונים הנוגעים לסודיות המידע, לאמינותו ולזמינותו (Confidentiality, Integrity, Availability).

נבחן לדוגמה את מורכבות ההגנה על מידע רגיש של ארגון המעוניין לפתח מוצר טכנולוגי המוגדר כפרויקט אסטרטגי ואשר עלול להוות מטרה למתקפות סייבר. כבר בשלב ייזום המהלך נוצרים מסמכים המוגדרים כחסויים ומוגבלים לעיניהם של מורשים בלבד: סיכומי פגישות, מצגות, ניתוחים טכנולוגיים, תרחישי שוק, קביעת מפת דרכים טכנולוגית וכדומה. אלה נשמרים בצורה דיגיטלית, המצריכה מעטפת הגנה אשר תבטיח גישה למורשים בלבד. משמעות הדבר היא בדרך כלל יישום מערכות למניעת זליגה של מידע,[4] שהן יקרות ומורכבות לתפעול. מורכבות ההגנה על מידע ארגוני רגיש דורשת ניתוח תהליכי יצירתו של המידע

בארגון, מיפוי המערכות, הבנת מחזור החיים, איתור המידע המסווג בבסיסי נתונים, בשרתי קבצים ובמחשבי קצה, וקביעות מדיניות ארגונית להגדרות סיווג. כל זאת, עוד בטרם נבחרו הכלים הטכנולוגיים אשר יאכפו את המדיניות אותה יש להטמיע, להדריך בהם את המשתמשים ולתמוך בהם לאורך כל חיי הפרויקט.

מעֵבר לצורך לאבטח שיתוף מידע פנים ארגוני, קיים צורך לנהל ולאבטח גם את המידע היוצא מהארגון. כמעט בכל ארגון מתקיים שיתוף מידע עם גורמים חיצוניים, כגון יועצים, ספקים ונותני שירותים למיניהם, וכמעט כל גורם בארגון נדרש לשתף מידע עם גורמים חיצוניים כדי לקדם את התהליכים העסקיים: החל ממהנדס הפיתוח המשתף במידע את קבלן המשנה החיצוני המומחה לתחום ספציפי ורגיש בפרויקט, דרך עורכי הדין הנדרשים לקבל ולשלוח חוזים עסקיים סודיים לשותפים, לספקים או ללקוחות פוטנציאליים, וכלה בעובדי הלוגיסטיקה והייצור המקבלים ושולחים מידע לנותני שירותים חיצוניים כחלק מניהול שרשרת האספקה.[5]

שמירה על אבטחת המידע הרגיש היוצא מתוך הארגון היא אחד האתגרים המורכבים ביותר ליישום, מאחר ומגוון הערוצים הדיגיטליים האפשריים להוצאה והכנסה של מידע הוא כמעט אינסופי. עובד עלול להוציא מידע על ידי שליחתו בדואר האלקטרוני הארגוני, דרך הדואר האלקטרוני הפרטי שלו, באמצעות העתקתו לרכיב זיכרון נייד כגון Disk on Key, צריבתו על כונן תקליטורים, שימוש בשירותי ענן לשיתוף קבצים חינמיים,[6] והגרוע מכל – באמצעות שירותי Peer-to-Peer, בהם המשתמש מתקין על מחשב בארגון תוכנה המקשרת אותו ישירות לרשת מחשבים המשתפים קבצים. כל אחד מאמצעים אלה מהווה סיכון משמעותי לקניין הרוחני של החברה. כל אחד מערוצי המידע מחייב ליישם טכנולוגיה אשר תגביל, תמנע, תחסום ותנטר את כל המידע העובר בה.

ארגונים רבים השקיעו משאבים רבים בחסימת התקנים חיצוניים אוגרי זיכרון, כגון Disk On Key ודומיהם, במניעת גלישה באינטרנט לשרתי שיתוף קבצים ועוד. אולם הצורך העסקי ביעילות, ושיתוף מידע בצורה מהירה וזמינה מתוך המשרד ומחוצה לו, מאלצים את הארגון ליצור ולאפשר ערוצי שיתוף מידע מאובטחים ומבוקרים מתקדמים. אחת האופציות הינה אימוץ של טכנולוגיות ענן, המאפשרות לארגונים להתייעל ולהנגיש את המידע מכל מקום באמצעות טלפונים סלולריים, מחשבי לוח ומחשבים ביתיים. שירותי הענן הם פתרון מצוין לארגון, אולם רמת האבטחה המובנית בהם לא מסַפקת לפי שעה תשובות לדרישות המחמירות להגנה על מידע וקניין רוחני.

תוצאות מחקר של חברת הייעוץ האסטרטגי "מקינזי"[7] מצביעות על כך שהדאגה מפני התקפות סייבר גורמת להאטה משמעותית באימוץ טכנולוגיות ענן ושירותי מובייל. כשבעים אחוזים מהנשאלים במחקר דיווחו כי דחו אימוץ

טכנולוגיות ענן בשנה ויותר מסיבות של אבטחת מידע, וארבעים אחוזים דיווחו כי דחו שימוש בשירותי מובייל בשנה ויותר מאותה סיבה. בתחום ההיי־טק, חמישים אחוזים מהנשאלים דיווחו כי יידרשו לבצע שינויים בתהליכי המחקר והפיתוח שלהם. עובדה נוספת המשקפת את השפעתן של הגנות סייבר על תפקודם של ארגונים היא שחמישים אחוזים מהמנהלים הבכירים מתחום ההיי־טק שהשתתפו במחקר דיווחו כי הנושא מהווה "נקודה כואבת", המגבילה את יכולת העובדים לשתף מידע.

מתברר, אפוא, כי טכנולוגיות המבטיחות התייעלות עסקית, כגון שירותי ענן יעילים וזולים, וכן טכנולוגיות שיתוף מידע וניידות, נתפסות כסיכון עסקי גבוה, עד כדי כך שהארגון מעדיף למעשה לספוג עלויות תפעול גבוהות ולא להסתכן ולהמתין עד אשר מערכות אלו יבטיחו לו בשלות ואבטחה איתנה. במצב כזה, ארגונים עלולים להתעלם מסיכוני סייבר בשל העדפתם יעילות תהליכים וקיצור זמן להשלמת המוצר על פני יישום בקרות והשלמה עם ההגבלות הנובעות מתהליכי האבטחה.

נקודת חולשה נוספת הקשורה לצורך של ארגונים לנתח וליישם מדיניות אבטחת מידע כאשר מדובר בגישה למידע וקניין רוחני, הינו הצורך לתת לגורמים חיצוניים גישה לרשת החברה. במקרים רבים מוצא הארגון לנכון לאפשר לספקים חיצוניים גישה מרחוק לרשת שלו, ובכך הוא נחשף למעשה לסיכונים המגיעים מכיוון הספק ומרמת אבטחת המידע הנהוגה אצלו.[8]

בין הגורמים שעשויה להיות להם גישה אל לב מערכות המידע והרשת הארגונית ניתן למצוא חברות המספקות תמיכה מרחוק למערכות מחשוב פנים ארגוניות, ספקים הנדרשים לעדכן מערכות מידע לוגיסטיות פנים ארגוניות וספקי משנה ושותפים עסקיים המתחברים מרחוק כדי לבצע פעילות במערכות החברה. גורמים אלה מחייבים את הארגון להקים, לתחזק ולנהל תשתית תקשורת מאובטחת ומוצפנת, בעלת הזדהות חזקה מול הארגון המקבל גישה. בנוסף, הארגון נדרש להגביל את הגישה הרשתית של הגורם החיצוני אך ורק למשאבים החיוניים לביצוע עבודתו, ולמנוע מצב בו גורם חיצוני יוכל לשוטט בצורה חופשית בתוך רשת החברה ולהיחשף למידע רגיש המצוי בשרתיה ובבסיסי הנתונים שלה. כל גישה של גורם חיצוני מצריכה ניתוח תהליכי, כגון: שם השרת אליו נדרשת הגישה, אילו תוכנות ופרוטוקולים יהיה עליו להפעיל, יצירת שם משתמש ייעודי, הפעלת מערכת ניטור ובקרה על כל תהליך ההתחברות והפעילות המתבצעת ברשת, יישום חוקי Firewall, וכמובן מעקב שוטף אחר הצורך בקישור החיצוני וטיפול בתקלות.

יש לתת מענה גם לרמת אבטחת המידע המיושמת אצל הגורם החיצוני ולסיכון האבטחתי הנובע מחולשה אפשרית בתחנת הקצה של נותן השירות. בין השאר יש לבחון האם המחשב שלו הוא בעל תוכנת אנטי־וירוס מעודכנת? האם קיבל

את עדכוני האבטחה האחרונים? האם הוא נגוע ב"סוס טרויאני" או בכל קוד עוין אחר? מחשב של ספק המתחבר לרשת הארגון הופך לחלק אינטגרלי ממנה. במקרים רבים הוא החוליה החלשה במערכת, אשר דרכה ניתנת האפשרות לגורם עוין לקבל אחיזה ברשת לצורך התקפת סייבר. במצב זה, לא משנה אם מדובר בארגון מסודר בעל מדיניות אבטחה עדכנית, המנהל את אבטחת תחנות הקצה בתאימות למדיניות הארגון בכל האמור לעדכוני אבטחה שוטפים, אנטי־וירוס ומניעת תוכנות בעלות סיכון אבטחתי; ברגע שניתנה גישה לגורם חיצוני בעל מדיניות אבטחה נחותה מזו של הארגון, הרי שהוא הופך לסיכון ממשי ומיידי.

נדבך נוסף שיש להתייחס אליו מבחינה אבטחתית הוא תהליך היצירה של אב טיפוס ושלב ביצוע הניסויים. זהו נדבך רגיש, שכן כאן נחשפים למעשה לראשונה הטכנולוגיה החדשנית, המוצר והיכולות החדשות העתידות לאפשר לארגון את פריצת הדרך העסקית. כאן מתגבש הקניין הרוחני לכדי ישות מגובשת, שאם גורם עוין ישים עליה את ידו, הוא יוכל לזכות ביתרון משמעותי. לפיכך, הצורך האבטחתי מכתיב ברוב המקרים הקמת מעבדות ואזורי פיתוח ממודרים על ידי בניית רשתות נפרדות, ניתוק מוחלט מרשת האינטרנט ויישומם של מוצרי אבטחה ותשתית נוספים המקבילים לאלה הנמצאים ברשת הארגונית. מיותר לציין את העלות הכלכלית הגבוהה של בניית רשתות נפרדות מסוג זה, כמו גם את הקשיים התפעוליים המתעוררים כתוצאה מכך בכל הקשור להוצאת מידע מתוך הרשתות המסווגות והכנסתו אליהן.

אחד ממעגלי האבטחה המשמעותיים ביותר הוא מערך הניטור והבקרה של אירועי אבטחה. ללא מערך ניטור אין לארגון יכולת לזהות אירועי אבטחה במערכותיו, אי־עמידה במדיניות האבטחה ואירועי סייבר פוטנציאליים, לא כל שכן יכולת להגיב לאירועים כאלה ולפעול במהירות להקטנת הסיכון. מערכות לניטור אירועי אבטחת מידע (SEIM)[9] הן בדרך כלל מערכות יקרות, המצריכות תחזוקה ועדכון שוטפים כדי להתאימן לאיומים חדשים, לתהליכים עסקיים ולמערכות אבטחה מדווחות חדשות. מערכת לניטור אירועי אבטחת מידע יודעת לקבל התרעות אבטחת מידע שמקורן בדרך כלל ברישומי אירועים מתוך המערכות הפנים ארגוניות (Audit Log / Security Log), כגון שרתים, ציוד תקשורת, מערכות Firewall, שרתי הזדהות, מערכות גישה מרחוק, בסיסי נתונים, שרתי קבצים ועוד. בנוסף לכלים הטכנולוגיים נדרש כוח אדם מיומן, המבין את משמעות האירועים המתקבלים במערכת ויכול לנתח את הפעילות ולקבל החלטה לגבי דרכי התגובה. יתרה מזו, שימוש במערכות לניטור אירועי אבטחת מידע מאפשר שילוב של מידע מודיעין סייבר חיצוני, המספק מידע עדכני על אופיין של התקפות סייבר ידועות, מקורות התקיפה וכלים הנמצאים בשימוש התוקפים. מידע מודיעיני זה מוצלב עם מידע הקיים ברשת הארגון ומאפשר זיהוי מוקדם ותגובה מהירה לאירוע.

החשיבות של יישום מערכות לניטור אירועי אבטחת מידע בתהליך ההגנה מפני התקפות סייבר עולה גם מתוך תוצאות מחקר של PoneMon Institute.[10] לפי מחקר זה, חברות שיישמו מערכות כאלו היו יעילות יותר בזיהוי והכלה של התקפות סייבר. כתוצאה מכך, אותן חברות חסכו כארבעה מיליון דולר של נזק, בהשוואה לחברות שלא יישמו מערכות לניטור אירועי אבטחת מידע.

הצעד החשוב ביותר בהתגוננות מפני איומי סייבר הוא השקעה בחינוך ובמודעות העובדים לסיכוני סייבר. אירועים של התקפות קיברנטיות מוצלחות על ארגונים התאפיינו, בין השאר, בחדירה לארגון דרך נקודת התורפה שלו – העובד, ולו הזוטר ביותר, שבאמצעותו ניתן להגיע לנקודת אחיזה ברשת הארגון הקורבן, וממנה להתחיל במתקפה. בהקשר זה יש עניין מיוחד בדוח מחקר על התקפות ממוקדות מבוססות דיוג (phishing) שנעשו על עובדי חברות.[11]

בכך לא מסתיימות הפעילויות שהארגון נדרש לבצע כדי להגן על קניינו הרוחני. לא די בהגדרת הנקודות הרגישות בתהליך ובהגנה עליהן; על הארגון להשקיע ולפתח לעצמו גם יכולות הגנה רשתית ולהקים מערכות ניטור ובקרה, שמצידן מצריכות רכישה, הטמעה ותחזוקה שוטפת, וכל זאת כדי לזהות אירועי אבטחה והתקפות סייבר בזמן אמת.

נוכח כל הנאמר לעיל, ברור כי הגנה על הקניין הרוחני הינה תהליך טכנולוגי, ארגוני ומינהלי מורכב ומשמעותי עבור הארגון. לתהליך זה ולעלותו הכספית השפעות עסקיות שליליות, כפי שינותח להלן.

השפעות כלכליות שליליות

החשש הכבד מפני התקפות סייבר ופוטנציאל הנזק הגבוה שיש בהן גורמים להשפעות כלכליות שליליות על ההתייעלות התפעולית של הארגון, על קיצור תהליכי הפיתוח והייצור ועל ההגעה לשוק לפני המתחרים. לפי הערכות המחקר של חברת "מקינזי",[12] כל עוד איומי הסייבר ימשיכו להתגבר והיכולת ההגנתית לא תסַפק את המענה ההולם, ההשפעות הכלכליות השליליות הנובעות מסיכוני סייבר יגרמו בחמש עד שבע השנים הבאות נזק למשק העולמי שיתבטא בפגיעה ביצירת ערך לחברות בסכומים שבין תשעה ל־21 טריליון דולר. משמעות הדבר היא כי תשומות ההגנה מפני סיכוני סייבר, וכן אובדן מידע וקניין רוחני כתוצאה מריגול מסחרי מבוסס סייבר, יגרמו לפגיעה משמעותית בכלכלה העולמית. המספרים דלעיל מושפעים כמובן מהתפתחות חוסנן של מערכות ההגנה. לצד זאת קיימת השפעה כלכלית ספציפית על כל חברה, בעיקר בשל הצורך שלה להגדיל את תקציב אבטחת הסייבר על חשבון תקציב המחקר והפיתוח, וכתוצאה מכך גם הקטנת הרווחיות התפעולית.

מעֵבר לעובדה שסיכוני הסייבר גורמים להשפעות כלכליות שליליות המתבטאות בהאטה עולמית ובצורך של חברות להשקיע בצורה מוגברת בתקציבי הגנת הסייבר, הסיכון המשמעותי לארגונים הוא של פגיעה ממשית בקניין הרוחני, על כל ההשלכות הכלכליות של הדבר. פגיעה בקניין רוחני עלולה להשפיע על שינוי מאזן הכוחות המסחריים בעולם, ליצור תחרויות לא הוגנות ולפגוע כלכלית ברווחיות חברות עד כדי חדלות קיומן. חברות רבות שחוו פגיעה בקניין הרוחני שלהן דיווחו על אובדן מכירות, רישיונות ותמלוגים, ירידה ברווחים ופגיעה במוניטין המותג והמוצר.

אחת הדוגמאות המשמעותיות בתחום גניבת קניין רוחני הוא מטוס החמקן הסיני J–31, הדומה בצורה מפתיעה למטוס החמקן F–35 של חברת "לוקהיד מרטין" האמריקאית. החברה האמריקאית נפלה בעבר קורבן להתקפת סייבר סינית, במהלכה נגנבה ממנה טכנולוגיית החמקן האמריקאי.[13] מטוס החמקן F–35 נחשב למטוס המתקדם ביותר בעולם, וכיום נמצאים בידי הסינים מידע טכנולוגי יקר ערך הקשור למטוס זה, כגון תרשימי מנוע מפורטים, מערכות מכ"ם וטכנולוגיות ייצור מתקדמות. קניין רוחני שהושקעו בו מיליארדי דולרים הפך במקרה זה למידע החשוף לגורם מתחרה, שעשה בו שימוש מיידי ויצר את המטוס J–31, הדומה להפליא לחמקן המקורי. מידע טכנולוגי מתקדם, הנופל לידי גורם מתחרה, מעניק לו קפיצת דרך טכנולוגית והופך אותו לשחקן משמעותי בשוק שנשלט בעבר על ידי מספר מצומצם של חברות.

הבעיה העיקרית בגניבת מידע וקניין רוחני היא העובדה שהארגון הנפגע מתקשה לזהות שנפל קורבן למתקפת סייבר שמטרתה גניבת מידע וקניין רוחני, שהרי מידע זה ממשיך להיות קיים בשרתים שלו והוא ממשיך לתפקד לכאורה כאילו לא קרה דבר. למעשה, הארגון כבר אינו שולט במידע, ועליו להתמודד עם מתחרה חדש שיפתיע אותו עם טכנולוגיה דומה או משופרת מזו שלו ויזכה ליתרון יחסי יקר ערך. מחקרים מראים כי הזמן שלוקח לחברה לגלות שהיא קורבן להתקפת סייבר הוא כ־230 ימים בממוצע.[14] משמעות הדבר היא כי במשך זמן זה התוקף שוהה בתוך מערכות הארגון, ותקופה זו ארוכה מספיק כדי לחקור את המידע המגיע לידיו, לנתחו מבחינת הרלוונטיות שלו לצרכיו, להסיק מסקנות ואף לשפר את התקיפה. המידע הנאגר אצל התוקף מאפשר לו להבין את מבנה הרשת של הארגון, להכיר שמות של מערכות הנמצאות בשימושו, לזהות שרתי קבצים ובסיסי נתונים, לפצח סיסמאות של עובדים בעלי הרשאות בסיווג גבוה ולחדור למאגרי המידע המעניינים אותו. מעבר לכך, המידע המועתק מהארגון מאפשר לתוקף להבין את המבנה הארגוני, להכיר את אנשי המפתח, את בעלי התפקידים ואת מקבלי ההחלטות, ולהמשיך להתקפה ממוקדת יותר במטרה לשלוף את המידע הספציפי בו הוא מעוניין.

כאמור, הארגון המותקף כלל אינו מודע לעצם קיומה של ההתקפה עליו וגם לא למשך השהייה של התוקף ברשת שלו. גם אם יש לו חשדות, יעבור זמן רב עד שהוא יידע פרטים מדויקים לגבי עומק ההתקפה ואיכות המידע שנגנב ממנו. פרק הזמן הארוך בטרם זיהוי ההתקפה הינו אחד היתרונות המשמעותיים ביותר של התוקף, וקיצור זמן הגילוי הוא אחד האתגרים המשמעותיים ביותר בהגנה מפני מתקפות סייבר. יכולת זיהוי של התקפת סייבר ותגובה עליה תלויות בצורה ישירה ברמת ההשקעה של הארגון במערכות מתקדמות לזיהוי והתרעה על פעילויות חריגות, בהגנה על עמדות קצה ומאגרי מידע, ביישום תקני אבטחה ובמודעות עובדים.

יש לזכור שהתקפת סייבר הממוקדת בגניבת מידע אינה דומה להתקפת סייבר שמטרתה מניעת שירות (DoS). במקרה האחרון, חברה מאורגנת תוכל להפעיל את תהליכי ההתאוששות עם סיום ההתקפה ולחזור לפעילות רגילה, תוך כדי הסקת מסקנות לגבי תיקון הפרצות. לעומת זאת, התקפה שבמהלכה נגנב מידע וקניין רוחני מצריכה מהקורבן לבצע תהליך מורכב של קבלת החלטות לגבי האסטרטגיה של המשך פעילותו העסקית, כמו למשל: איך לאמוד את מידת הנזק שנגרם לחברה כתוצאה מגניבת הקניין הרוחני? האם להמשיך לפתח מוצר שהמידע הטכנולוגי לפיתוחו וייצורו כבר אינו בשליטת החברה? האם להמשיך את האסטרטגיה העסקית בהתאם לתוכניות המקוריות, או שמא לשנות אותה מהקצה לקצה?

לפי הערכות ממקורות שונים,[15] הנזק לכלכלה העולמית הנובע מהתקפות סייבר הממוקדות בריגול תעשייתי הוא בסדר גודל של מיליארדי דולרים כל שנה. האפקט הכלכלי של גניבת מידע וקניין רוחני מתבטא במספר פרמטרים הנוגעים ישירות לארגון עצמו, ובצורה עקיפה גם למצב הכלכלי במדינה. בכל מקרה, היכולת להעריך מספרית את הנזק הכלכלי מהווה אתגר בפני עצמו, שקיים קושי אמיתי להעריכו בצורה כמותית, ועל כן הוא בגדר השערה.

את המשמעות הכלכלית המצטברת כתוצאה מגניבת מידע קניין רוחני ניתן לסכם במספר מאפיינים, ובראשם היכולת של התוקף לצבור יתרון טכנולוגי, באמצעותו הוא יוכל להציע מוצר זהה במחיר זול יותר, וזאת מאחר ולא השקיע בפיתוח ולפעמים גם עלויות הייצור שלו הן נמוכות. התוצאה לגבי הקורבן יכולה להיות ירידה במכירות, ירידת מחירים, ירידה ברווחים, ירידה בערך המניות שלו ואף סגירת החברה. בכל מקרה, קיימות עלויות גבוהות לחברה, הנובעות מהצורך לטפל באירוע התקיפה והשקעה בשיפור מערכות ההגנה שלה. דוגמה מפורסמת לחברה שחדלה להתקיים בשל גניבת מידע היא חברת DigiNotar ההולנדית, שפשטה את הרגל אחרי שמידע קריטי נגנב ממנה.[16]

הנזקים במישור הלאומי מהתקפות סייבר לצורך גניבת מידע קניין רוחני עלולים להתבטא בירידה בתוצר ובאובדן מקומות עבודה, במיוחד במדינה בה הכלכלה מוּטת טכנולוגיה ומו"פ. השקעות בטכנולוגיה מתקדמת עלולות לרדת לטמיון

ולהניב רווח כלכלי דווקא לתוקף. זאת ועוד, מידע טכנולוגי ביטחוני רגיש עלול לזלוג לאויבים ולהשפיע על מאזן הכוחות מול אויבים ויריבים. הערכה כמותית של השפעה כזו יכולה להישען על תחזיות כלכליות שונות, אולם בכל מקרה ברור כי האפקט הכלכלי הנוצר מהתקפות סייבר, הן ברמת החברה הפרטית והן ברמה הלאומית, דורש התייחסות אסטרטגית מעמיקה.

בבואנו לבדוק את השפעת הריגול המסחרי בעולם הסייבר על קבלת החלטות עסקיות של ארגונים, נדרש לבחון תחילה שלושה היבטים בסיסיים: הראשון נוגע לרמת המודעות של מקבלי ההחלטות לסיכוני ריגול סייבר; השני נוגע לשאלה האם יש בחברות השונות כלים להערכת הסיכונים ולקבלת החלטות בנושא; השלישי נוגע לאופן שבו החלטות שהתקבלו כמענה לאיומי הסייבר מיושמות בארגון. מחקרים[17] מראים כי רוב החברות מִתקשות להעריך את הסיכון, וכתוצאה מכך מתקשות לגבש תוכניות להקטנתו. קיימת תמימות דעים כי איומי הסייבר וההתקפות המתוחכמות ילכו ויתגברו, מבלי שלארגונים תהיה יכולת אפקטיבית להתגונן מפניהם.

דליפת מידע שהוא קניין רוחני הינה אחת הדאגות המרכזיות בחברות היי־טק, והיא נתפסת כחמורה ביותר יחסית לדליפת סודות של מִפרטי המוצרים. לעומת זאת, חברות שירותים מודאגות בעיקר מדליפת מידע המזהה את לקוחות החברה ומפגיעה בשירות אותו הן מספקות. סקירת בשלותן של חברות לנתח סיכוני סייבר (cyber risk-maturity) מצביעה על כך שגם בארגונים גדולים קיימים פערים ניכרים ביכולתם לבצע ניהול סיכונים. תשעים אחוזים מהחברות דורגו כבעלות תהליך ניהול סיכונים "מתפתח" או "בתחילת דרכו", ורק חמישה אחוזים מהחברות שהשתתפו בסקר הוגדרו ככאלו שבהן מתקיים תהליך ניהול סיכונים "בוגר".[18]

מעניין לציין כי לא נמצאה קורלציה בין ההוצאה הכספית על ניהול סיכונים לבין בשלות התהליך של ניהול אותם סיכונים. נמצאו חברות שהשקיעו מעט משאבים בתחום זה, אך ביצעו תהליך ניהול סיכונים אפקטיבי, בעוד שאחרות השקיעו משאבים רבים בתהליך ניהול הסיכונים, אולם ללא תִחכום, דבר שהשאיר מקום רב לשיפורים. מנהלים בכירים בתחום הפיננסי, שלא היה להם ידע טכני, התקשו לשלב סיכוני סייבר בתהליך ניהול הסיכונים ולקבל החלטות מושכלות בשל חוסר מידע. זאת ועוד, למרות העיסוק של ארגונים גדולים בהגנה על המידע ובהשקעות כספיות בתחום זה לאורך שנים, הנתונים משקפים את גודל הפער הקיים בין האיומים המתוחכמים בעולם הסייבר ובין יכולתן של חברות להגן על עצמן.

למעשה, ניתן להסיק כי הבעיה העיקרית אותה חווה העולם בהיבט של סיכוני סייבר היא היכולת להעריך את הסיכון, וכפועל יוצא מכך הקושי לתת לו מענה אבטחתי הולם. הקושי להתמודד עם איומי סייבר מורכבים, ומבחן התוצאה העגום

נכון להיום, הובילו למסקנה כי יש צורך בהגברת המומחיות בתחום הסייבר בתוך הארגונים עצמם. כיום ישנה מגמה[19] גוברת בחברות אמריקאיות גדולות למנות מומחי סייבר לתפקידים בכירים בארגון. חברות הנמנות על רשימת Fortune–500 ממנות מומחי סייבר המדווחים ישירות למנכ"ל, לעומת המבנה הנפוץ בו ממונה אבטחת המידע הארגוני (CISO) היה כפוף לסמנכ"ל מערכות המידע הארגוני (CIO). יתר על כן, הדרישות ממי שממלא את תפקיד מומחה הסייבר נוגעות כיום לא רק להבנה טכנית בתחום אבטחת המידע, אלא גם להיכרות מעמיקה עם התהליכים העסקיים והבנה בניהול סיכונים.

בעוד שחברות גדולות מקבלות החלטות אסטרטגיות בנושא אבטחת סייבר ומקימות גופים בעלי ידע וטכנולוגיות שנועדו לנתח את הסיכונים ולשפר את רמת האבטחה סביב נכסי המידע, חברות בינוניות וקטנות מתקשות לעשות זאת בכוחות עצמן. הסיבה לכך היא שאין להן את הגודל והמשאבים ליישם את כלל התהליכים, הטכנולוגיות וההתאמות התכופות הנדרשות בתחום הגנת הסייבר. חברות בעלות משאבים מוגבלים עומדות בפני מספר אפשרויות: יישום הגנות סייבר מינימליות, כמיטב הבנתן ויכולתן התקציבית, וכתוצאה מכך חשיפה לאיומים של גניבת מידע וקניין רוחני, שהרי הן יהיו ככל הנראה חדירות לתוקף נחוש, בין אם במודע ובין אם לא במודע. חברות קטנות רבות, המצומצמות במשאבים, ימנו ברוב המקרים את איש המערכת (System) כגורם המקצועי האמון על אבטחת המידע. טיפולו של אדם כזה יתמקד, במקרים רבים, בנושאים הנמצאים בתחום אחריותו הטכנית, כגון אבטחה של שרתים ותחנות קצה, ניהול משתמשים, אבטחת שרת הדואר ותשתית הרשת. אדם זה לא יקים מערך של אבטחת מידע התואם ניתוח מקצועי של סיכוני הסייבר הרלוונטיים לארגון.

אפשרות אחרת היא שהארגון יגדיל את תקציב הגנת הסייבר שלו כדי לתת מענה הולם לרמת האיומים, ובהתאם לכך גם לניהול הסיכונים. ניתן להניח שהדבר יחייב השקעות משמעותיות בתשתית אבטחת הסייבר, רכישת מוצרים רלוונטיים, הקמת צוות מומחים, הכשרה מקצועית, עמידה בתקנים ועוד. השקעות בתחום זה יקרינו על הרווחיות של הארגון ועל יכולתו להתמודד בשוק תחרותי, תוך ציפייה שלו שהן יחזירו את עצמן. זאת, בראש ובראשונה בהקטנת ההסתברות להיפגע מהתקפות סייבר וביכולת שהן יקנו לארגון לפתח תהליכים עסקיים בסביבה שתהייה מאובטחת כנדרש.

אפשרות נוספת היא להסתמך על שירותי אבטחה מנוהלים. פירוש הדבר הוא לקבל שירותי אבטחה נקודתיים מחברות מיקור חוץ, שבמקרים רבים אינן רואות את התמונה הכוללת של הארגון ואינן נמצאות בתוך התהליכים הקריטיים שנסקרו לעיל. שיטה זו טומנת בחובה יתרון, בעיקר בכך שהיא מאפשרת קבלת שירותים מקצועיים בתחום שלארגון אין ידע או יכולת טכנולוגית וכלכלית להטמיע או

לנהל בעצמו. זאת ועוד, גם העלויות יהיו נמוכות יחסית, מכיוון שנותן השירות מפזר את העלויות על פני מספר רב של לקוחות. מצד שני, גורם חיצוני, שאינו חי את הארגון בצורה יומיומית ואינו שותף לתהליכים העסקיים שלו המשתנים מדי יום, הוא בעל יכולת נמוכה לספק מענה אינטגרטיבי התפור בדיוק לצורכי הארגון. יתר על כן, מיקור חוץ מספק בדרך כלל מגוון שירותים מתומחר, מוגדר, סגור ובדרך כלל גנרי, כך שיתאים לרוב לקוחותיו, דבר היוצר קושי לקבל שירותי אבטחה ספציפיים לצורכי הארגון ובצורה דינמית. שירותי אבטחה מנוהלים יכולים להוות קפיצת מדרגה אבטחתית משמעותית לארגונים קטנים בעלי צרכים ברורים, אולם רק עד גבול מסוים, שבו התהליכים העסקיים הופכים למורכבים.

נראה כי חברות קטנות, המתבססות על הקניין רוחני שלהן, יתקשו להגן על המידע הקנייני ועל תהליכי העבודה שלהן מפני התקפות סייבר מתוחכמות. אותן חברות יסתפקו בפתרון אבטחתי חלקי, מתוך הנחה כי הן לא מהוות מטרה מועדפת לתקיפות מתוחכמות כאלו. פתרון מסוג זה יציב אותן על הקצה העליון של סולם החברות הנמצאות בסיכון גבוה להיפגע מאיומי סייבר, וכן מריגול עסקי ומגניבת מידע וקניין רוחני.

המצב קשה במיוחד במקרה של חברות ההזנק הישראליות. תעשיית המחקר והפיתוח בישראל הינה תעשייה ענפה. מאות חברות נסמכות על תקציב המו"פ של המדען הראשי במשרד הכלכלה ועל גיוסי הון מקרנות למיניהן כדי לפתח ידע, טכנולוגיה ומוצרים. חברות ההזנק הישראליות מאופיינות בכך שהקניין הרוחני שלהן הינו המנוע החשוב ביותר לקיומן ולהתפתחותן. חברות אלו יידרשו לבחור באחת משלוש החלופות שתוארו לעיל. ניתן להניח כי בשל מצוקה תקציבית, ואולי גם מתוך חוסר מודעות, הן יבחרו ליישם הגנות סייבר מינימליות. משמעות הדבר היא שנכסי המידע המתקדמים ביותר ומנוע הצמיחה הפוטנציאלי לכלכלה הישראלית יקבלו הגנות סייבר ברמה הנמוכה ביותר במשק. אפשרות כזאת מהווה נתון מטריד הדורש התייחסות מעמיקה ברמת הלאומית.

נקודה נוספת התומכת בצורך לגבש התייחסות ואסטרטגיה לאומית בתחום הגנת הסייבר של חברות הזנק בישראל היא העובדה כי אחת מדרכי המימון הנפוצות למחקר ופיתוח הינה קבלתו ממשרדו של המדען הראשי במשרד הכלכלה. המדען הראשי מאפשר הקמה של חממות טכנולוגיות על ידי חברות יזמיות ומימון של עד 85 אחוזים מתקציבן, בסכום כולל שנתי של 1.5 מיליארד שקל. הציפייה היא שפירעון המימון הממשלתי יתממש על ידי תשלום תמלוגים למדינה מכל הכנסה הנובעת מהמוצר שפותח במסגרת פרויקט החממה, או ממוצר הנובע ממנו, לרבות שירותים הנלווים למוצר או כרוכים בו. השקעתו של המדען הראשי במחקר ופיתוח מונחת למעשה על קרן הצבי בשל החשיפה העצומה של הטכנולוגיות המפותחות לגניבת הקניין הרוחני. הנזק הצפוי במקרה זה הוא בלתי ישוער: החברות מסַכנות

את יכולתן לממש את תוצרי המחקר והפיתוח, וכפועל יוצא מכך גם את יכולתן לשלם תמלוגים למדינה בגין המימון הממשלתי לאותו מחקר.

תובנות מסכמות

הגנה על מידע וקניין רוחני היא צורך קריטי של כל ארגון עסקי, אזרחי או לאומי. תהליך ההגנה על מידע קניין רוחני הינו מורכב מבחינה טכנולוגית ותהליכית ובעל השפעה משמעותית על תקציבי הפיתוח של הארגון. יישום מוצלח של מעטפת הגנה אפקטיבית על מידע ועל קניין רוחני תלוי בעיקר במודעות הארגון לסיכונים וליכולתו ליישם את מעטפת ההגנה בצורה מיטבית. כל זאת, כפועל יוצא של יכולותיו הכלכליות של הארגון, בשלות התרבות הארגונית בנושא אבטחת מידע, קיומן של פונקציות ארגוניות וכוח אדם מיומן. נדמה שהיכולת הכלכלית לממש פתרונות הגנה מתקדמים מהווה את אחת המגבלות העיקריות בהתמודדות של חברות קטנות ובינוניות עם סיכוני הגניבה של מידע קניין רוחני. עם זאת, קיומה של יכולת כלכלית הינו תנאי הכרחי אולם לא מספיק להתמודדות יעילה עם סיכוני מתקפות סייבר.

מתברר כי לארגונים קשה להעריך את סיכוני הסייבר, וזאת בשל חוסר ידע עדכני, מורכבות הנושא, היעדר משאבים כלכליים, חוסר במיומנויות או מבנה ארגוני לא מתאים (כגון חסרונה של פונקציה האמונה על תחום ניהול הסיכונים והגנת סייבר). מצב זה משפיע על עצם המודעות לסיכוני סייבר ועל המוכנות לפעול נגדם. גם ארגונים עתירי משאבים וכוח אדם מקצועי לא תמיד מצליחים ליישם הגנות מיטביות מול איומי סייבר, המסוגלות לתת מענה אפקטיבי באמצעים השונים של אבטחת המידע. חמור במיוחד הוא מצבן של חברות הזנק, המאופיינות מצד אחד כבעלות קניין רוחני פורץ דרך ובעל פוטנציאל כלכלי אדיר, ומצד שני כבעלות יכולות תקציביות מוגבלות המונעות מהן להקים מערכי הגנה אפקטיביים על הקניין הרוחני יקר הערך שלהן. יתר על כן, חברות הזנק, מעצם טבען, ממוקדות בפיתוח הטכנולוגי ואינן נוטות להקים גופי טכנולוגיית מידע (IT) ואבטחת מידע משמעותיים.

גופים ביטחוניים ותשתיות אזרחיות קריטיות בישראל מוגדרים כגופים מונחים על ידי הרשות לאבטחת מידע (רא"ם) ועל ידי הממונה על הביטחון במשרד הביטחון (מלמ"ב). לעומתם, המרחב האזרחי במדינת ישראל נותר ללא הכוונה או סיוע ברמה הלאומית, ולמעשה אמור להתנהל לפי הבנתו ויכולתו. מטה הסייבר הלאומי אמנם נדרש להתוויית מדיניות כוללת להגנה על מערכות ממוחשבות בישראל ("מדיניות קיברנטית לאומית") ולפיתוח תפיסת הפעלה מדינתית שלה בשגרה,[20] אך הגנה על מידע וקניין רוחני בגופים אזרחיים שאינם מוגדרים כתשתית קריטית אינה חלק עיקרי בפעילותו של מטה זה.

חובה על מדינת ישראל לפעול לשיפור תפקודה בהגנה על ידע שהיא מממנת באמצעות כספי מו"פ, וכן לקדם מהלכים להגנה על מידע וקניין רוחני של המגזר הטכנולוגי והעסקי, שהרי פגיעה בו תקרין ישירות על הכלכלה והתחרותיות של המשק הישראלי כולו. בנוסף לאמור לעיל, יש מקום להקים גוף מייעץ בתחום ההגנה על הידע והקניין הרוחני למגזר האזרחי בכלל ולחברות טכנולוגיות, כגון חברות הזנק, בפרט. יתכן וניתן לעשות זאת באמצעות מטה הסייבר הלאומי.

מענה, ולו חלקי, לאתגרים שתוארו לעיל יוכל להינתן על ידי דרישה של המדינה להגן על ההשקעות שלה מכספי מו"פ. דרישה כזו תוכל לייצר יוזמות אזרחיות עסקיות לאספקת מענה ברמה של מומחיות, ובעלות סבירה, לחברות הממומנות על ידי המדען הראשי של משרד הכלכלה, ולכן טוב יהיה אם יינתן סיוע מדינתי מסוים לבניית תשתית אבטחה שתיועד לחברות הנזקקות. דוגמה לסיוע כזה יכולה להיות בניית יכולות פיתוח ופעולה בענן מאובטח, בסטנדרטים של המערכת הביטחונית או קרובים אליה.

חברה עסקית שתיקח על עצמה לספק פתרונות אבטחה ויכולות פיתוח בתשתית מאובטחת תוכל לעשות זאת רק אם תעריך שיהיו לה מספיק לקוחות וכי המודל העסקי שלה יהיה רווחי. דבר זה יקרה אם חברות הממומנות על ידי המדען הראשי של משרד הכלכלה יונחו לאבטח את הקניין הרוחני שלהן ברמה מספקת, כפי שתיקבע על ידי הגורמים המקצועיים. הפעולה הנדרשת תיצור שילוב בין הדרישה מצד הגורם המממן לפעול בסביבה מאובטחת ובין מתן מענה על ידי חברות אזרחיות, שיספקו סביבה כזאת לשוק מאובטח.

הקמת תשתית ענן מאובטח תיצור "מרחב מוגן" שייתן מענה לצורכי הפיתוח הטכנולוגי של חברות טכנולוגיות, ובהן חברות הזנק. תשתית כזאת תתבסס על מערכות אבטחה שיתמקדו בהגנה על מידע וקניין רוחני ותאפשר לאותן חברות לנהל את המידע הרגיש תחת מעטפת אבטחתית גבוהה בהרבה מזו שיכלו ליצור לעצמן. לשכת המדען הראשי, המתקצבת חממות טכנולוגיות במיליוני שקלים, היא מנוע ההאצה לשימוש בתשתית הענן המאובטח. לשכת המדען הראשי גם שותפה לתוכנית קידמ"ה (קידום מו"פ הגנת הסייבר),[21] יחד עם מטה הסייבר הלאומי, ומתעדפת בתקצוב משופר מחקר ופיתוח בתחום הסייבר במטרה לקדם ולמצב את ישראל כמובילה עולמית בתחום זה. קבלת תקציבים מהמדען הראשי אינה מותנית כיום בהצגת תוכנית הגנה על המידע והקניין הרוחני הנוצר, והחברות המתוקצבות במיליונים ומפתחות טכנולוגיות האמורות להיות מנוע הצמיחה הכלכלי של מדינת ישראל חשופות למעשה להתקפות סייבר, שהנזק הגלום בהן הינו עצום.

בעולם בו התקפות סייבר מתוחכמות ממוקדות בגניבת מידע שמטרתה היא לקצר תהליכים טכנולוגיים, נראה כי הקמת גוף מייעץ מקצועי לחברות טכנולוגיות

אזרחיות, וכן פיתוח תשתית ענן ייעודית מאובטחת ברמה גבוהה, ישנו בצורה דרמטית את סיכוייהן של חברות ההזנק לשרוד ולהגן בהצלחה על הקניין הרוחני שלהן. מדינת ישראל תוכל, באמצעות מהלך כזה, לקיים מנגנון אבטחה מחייב ולוודא החזר ההשקעה שלה במחקר ופיתוח.

הערות

1 Doron S. Ben-Atar, Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power (New Haven: Yale University Press, 2004).

2 במקרים רבים מועברות תוכניות ייצור של מכלולים במוצר (מארזים, מעגלים מודפסים, רכיבים אלקטרוניים ועוד) לגורמי הייצור הקבלניים באמצעות מדיה מגנטית. הדבר נעשה אם בהעברה פיזית של מדיה כזאת ואם באמצעות תקשורת מחשבים.

3 Tucker Bailey, Andrea Del Miglio, Wolf Richter, "The rising strategic risks of cyberattacks," *McKinsey Quarterly*, May 2014, http://www.mckinsey.com/insights/business_technology.

4 מערכות כאלו מכונות בשם: Data Leakage Prevention

5 שרשרת האספקה בארגון מנהלת את תהליכי הרכש, הייצור, האחסון, ההפצה והתובלה, ותפקידה הוא לקשר בין היצרנים, הספקים ולקוחות הקצה. ניהול שרשרת האספקה מצריך גמישות ותיאום גבוהים מול גורמים חיצוניים ומהווה מרכיב חשוב ביצירת הערך לחברה.

6 שירותי ענן דוגמת: Jambo Mail, Google Drive, DropBox ודומיהם.

7 Bailey, Del Miglio, Richter, "The rising strategic risks of cyberattacks."

8 ההתקפה על רשת Target האמריקאית, שבמהלכה נגנבו מיליוני כרטיסי אשראי, החלה בגניבת הרשאות הגישה של ספק מערכות תחזוקה שנתן שירותים לרשת זו. ראו: Brian Krebs, "Target Hackers Broke in Via HVAC Company," Krebs on Security, February 14, 2015, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

9 SEIM - Security Event Information Management

10 "2013 Cost of Cyber Crime Study: United States," Ponemon Institute, October 2013.

11 "APT1 Exposing One of China's Cyber Espionage Units," Mandiant Report, February 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

12 Bailey, Del Miglio, Richter, "The rising strategic risks of cyberattacks."

13 Franz-Stefan Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack," *The Diplomat*, January 27, 2015, http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack./

14 "Mtrends: Beyond the Breach," Mandiant 2014 Threat Report, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

15 McAfee, "The Economic Impact of Cybercrime and Cyber Espionage," Center for Strategic and International Studies, July 2013, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

16 ראו ניתוח מפורט של מתקפה זו בתוך: גבי סיבוני וסמי קרוננפלד, "לוחמת הסייבר של איראן", **צבא ואסטרטגיה**, כרך 4, גיליון 3, דצמבר 2012, http://media.wix.com/ugd/d48d94_1f8bd495a0554e44967b99e25e931eae.pdf

17 Bailey, Del Miglio, Richter, "The rising strategic risks of cyberattacks."

18 שם.

19 Nadia Damouni, "U.S. companies seek cyber experts for top jobs, board seats," Reuters, May 30, 2014, http://www.reuters.com/article/2014/05/30/us-usa-companies-cybersecurity-exclusive-idUSKBN0EA0BX20140530.

20 מתוך דף הבית של מטה הסייבר הלאומי באתר נציבות שירות המדינה: http://www.csc.gov.il/DataBases/NewsLetters/NewsLetters3/Pages/CyberHeadquarters.aspx

21 ראו חוזר המדען הראשי במשרד הכלכלה: "תוכנית קידמ"ה (קידום מו"פ הגנת הסייבר (לקידום יכולות התעשייה הישראלית בתחום הגנת הסייבר", 21 בנובמבר 2012, http://www.moital.gov.il/NR/rdonlyres/89646959-5455-4A5A-99FD-C4B07D07E8E5/0/syber122012_3.pdf