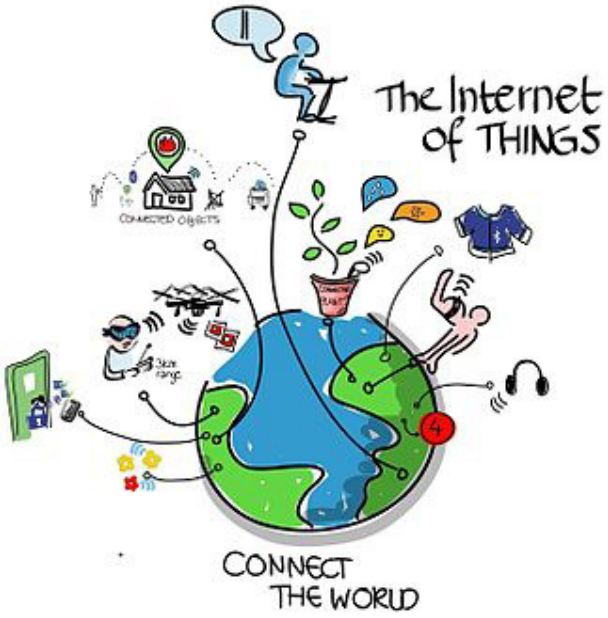
סיכוני סייבר – והפעם זרקור על תשתיות לאומיות
האם נערכת לחפירות הרכבת הקלה בתל-אביב?

רו"ח דורון רונן, MA, LLM, CIA, CRMA, CRISC, CFE
סגן נשיא ויו"ר הוועדה המקצועית-IIA ישראל איגוד מבקרים פנימיים בישראל,
נשיא שקדם וחבר הנהלה ISACA ישראל-האיגוד הישראלי לביקורת ואבטחת מערכות מידע

הקדמה

מאז שנות השמונים של המאה העשרים, הפכו מחשבים מאמצעי טכנולוגי חדשני לאחד מגורמי הייצור ואמצעי התקשורת החשובים והנפוצים ביותר בכלכלה של ימינו. אם בעבר בוצעו רוב האינטראקציות העסקיות בין בני האדם בטלפון, בדואר או שיחה, כיום המגמה השתנתה לחלוטין. רוב התקשורת והאינטראקציה בין בני אדם מבוצעות באמצעות מחשבים ורשתות מחשב. יתרה מזאת, חלק ניכר מהכלכלה, תשתיות המדינה ואפילו תשתיות הביטחון מושתת כיום על מחשבים.
עם הרחבת השימוש באינטרנט, החלו להתרבות ולהשתכלל מעשי החדירה למחשבים ואבטחת המידע באינטרנט הפכה מאמצעי טקטי לקונספט אסטרטגי.
ככל שהתרחבו והתפתחו המחשבים, החומרות, התוכנות, היישומים (האפליקציות), הרשתות, התקשוב, הציוד הפריפריאלי, הטלפונים החכמים, הטאבלטים, כל עולם הסייבר (האקדמיה ללשון העברית חידשה מונח זה בעברית ל- **סב"ר** = סביבת רשת), כך גם התרחבה הסכנה של זליגת וְדֶלֶף מידע והאמצעים הישנים ששימשו נגדה, חייבים היו להשתכלל. השכלולים מתבטאים בתוכנות חדשות להגנת מידע, לחסימת דואר זבל, להגנה בפני וירוסים, בשכלולים פיזיים ולוגיים וכן באמצעי הגנה חדשים לאבטחת מידע.
כיום, חברות הכבלים והלוויין משנות לנו את השעון במֵמִיר בעת החלפת שעון חורף לשעון קיץ ובחזרה. גישה דומה יש גם לחברות המעניקות לנו שירות אינטרנט. בעת הזזת השעון, מתעדכן המחשב שלנו אוטומטית על ידי נותני השירות. במילים אחרות, גופים זרים נמצאים במחשבים שלנו.

למעשה, כל ארגון/מפעל/עסק חשוף לחדירה למחשביו. הבעיה, שחדירה למחשבינו, מתגלית רק לאחר שהנזק כבר נגרם. אנחנו צריכים למנוע מראש את הנזקים ואת החדירה למחשבינו.
ישנם מנהלי ארגונים החוששים להוציא סכומי כסף נאותים לאבטחת מידע, או שאינם מודעים לחשיבות הנושא. החיסכון הכספי שהם חוסכים עלול לגרום לארגון נזק שאין לתארו. אבדן נתונים, שיבושם, פגיעה בתפעול, חוסר אפשרות גביה מחוסר ידע ממי וכמה לגבות, פורמולות ייצור שאבדו, כמויות מלאי קיים או חוסר, גילוי סודות מקצועיים למתחרים.



כשאנו מדברים על טכנולוגיות המידע, אנו מתייחסים לחומרה, לתוכנה, למערכת ההפעלה, לתקשורת, לרשתות, לנתונים ולאחסונם, לעיבודם, לתפעולם, להעברתם ולפלטי נתונים.

נתונים סטטיסטיים לפתיח

לפי דיווחי האינטרפול, על מדינת ישראל 10,000 מתקפות בדקה. לפי סקר של סימנטק (24 מדינות, 20 אלף משתמשי רשת): 14 איש בעולם חווים מתקפת סייבר מידי שניה, יותר ממיליון מידי יום. הסיכוי לגולש לחוות מתקפה מקוונת עומד על 1 ל- 2.27 (להבדיל, תאונת מטוס 1 ל 10.7 מיליון, מוות בתאונת דרכים 1 ל- 6,279). עלות פשעי הסייבר (שנת 2011) – 388 מיליארד דולר. פרק הזמן למותקף לטפל בבעיית אבטחת מידע - 10 ימים בממוצע. 54% ניזוקו ממתקפות משולבות, נוזקות או וירוסים. 10% חוו מתקפות בטלפונים החכמים, כולל Smishing (כלומר Phishing באמצעות SMS – מסרונים).

מרחב הסייבר הולך וצובר תאוצה

תחום הסייבר הולך וצובר תאוצה בזירה הממוחשבת. יותר ויותר ארגונים נוכחים לדעת כי יש צורך בכלים ובנהלים על מנת להתמודד עם אירועי אבטחת מידע, העלולים להגיע ולשתק את הארגון וסביבתו הקרובה. היכולת להגיב בזמן אמת למתקפות סייבר, היא קריטית להתנהלותו העסקית של הארגון.

כחלק ממלחמה בהרחבת מעשי הפריצות, גופים גדולים או עסקים עם סניפים רבים, מקימים מרכז להפעלת אבטחת מידע שמטרתו להוות מרכז לניהול ותגובה לאירועי אבטחת מידע המתבסס על נתונים מדויקים ומהימנים. בעסקים שהמידע בהם קריטי, קיימים כבר בארץ ארגונים בהם מרכז זה עובד 24 שעות ביממה, 7 ימים בשבוע. לעומתם, ישנם ארגונים המפעילים את המרכז רק בשעות העבודה.
מרחב הסייבר, גאדג'טים רבים שנוספו, הרחבת האינטרנט, הפייסבוק, הטוויטר, הווטסאפ וכדומה, מעלים לאוויר נתונים רבים. מכאן שיש להרחיב ולהגביר את אבטחת המידע להגנה על הארגון מבחוץ ומבפנים.

השפעת סיכוני התשתיות הלאומיות על סיכוני סייבר

רובנו מודעים כיום לסיכוני הסייבר, מי יותר, מי פחות. ברם, האם אנו מודעים באותה מידה לגבי השפעת סיכוני התשתיות הלאומיות על סיכוני הסייבר?

המשל - אפרט במספר דוגמאות:

1. **<u>ארה"ב נ' ברה"מ: צינור הגז הטרנס סיבירי (אפריל 1982)</u>**: במסגרת המלחמה הקרה ברה"מ-ארה"ב, סוכן כפול של ה- CIA שתל תוכנה עם וירוס, וגרם לפיצוץ הכי גדול מבין הלא-גרעיניים שנראה מהחלל. הפסד ישיר של מיליארדים לברה"מ, וברה"מ גם הפסידה את השוק האירופאי שרכש ממנה גז.[1]
2. **<u>רוסיה נ' אסטוניה: אינטרנט (2007)</u>**: ברה"מ שחררה את אסטוניה מהנאצים במלחמת העולם השניה. לאחר המלחמה נשארו מאות אלפי רוסים באסטוניה, והם התיישבו שם. ב- 1991, הייתה אסטוניה הראשונה שהתנתקה עקב נפילת ברה"מ. עם השנים, הפכה אסטוניה למדינה המתקדמת ביותר מבין מדינות סקנדינביה והבלטיות בנושא אינטרנט; למעשה – מדינת אוטומציה. רישות של מעל 95%. כל פעילות הבנקים באינטרנט. ב- 2007 אסטוניה הסירה את פסל החייל הרוסי ממרכז העיר טאלין, והעבירה אותו לבית הקברות. מיידית, החלה מתקפה על אתרי האינטרנט של אסטוניה. כל הפעילות שותקה ע"י Bot-Net (רובוטים נשלטים – שקיבלו פקודה "להפציץ בדואל" וכד'), שגרמו ל- DOS (Denial of Service).[2]

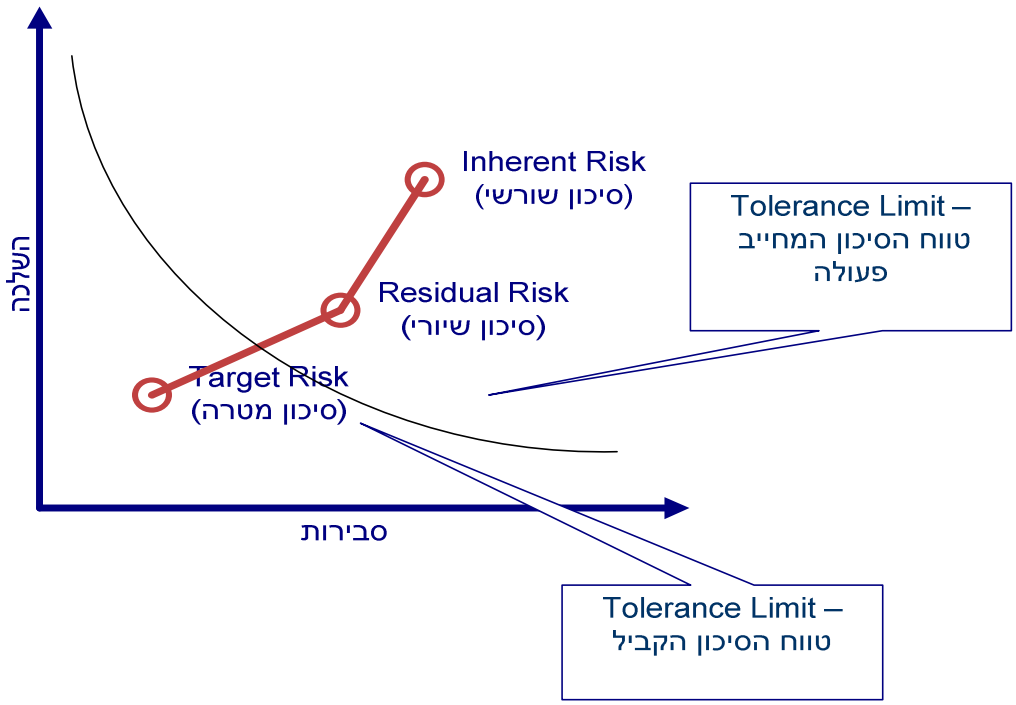
3. **<u>ארה"ב וישראל (?) נ' אירן: כור גרעיני - פרשת Stuxnet (יוני 2010)</u>**: חברה אלמונית מבלרוס דיווחה על וירוס סוס טרויאני או תולעת שמצאה אצל לקוח שלה באירן, שככל הנראה הוחדר לתחנת כוח מקומית באמצעות הֶתְקֵן USB נייד, תָקַף מערכות שליטה ובקרה של מערכות חשמל והכור הגרעיני (לרבות מערכות ההפעלה של הצנטריפוגות בכורים האטומיים באירן). קוד הנוזקה בגודל MB0.5. מקורות זרים (מומחה גרמני והניו-יורק טיימס) טענו שהעקבות מובילים לארה"ב וישראל (יח' 8200) ששיתפו ביניהם פעולה. ארה"ב וישראל הכחישו קשר לכך. נפגע מפעל העשרת דלק ב-נתאנז (אירן), וכתוצאה, עוכבה התפתחות הגרעין באירן.[3]
4. **<u>(?) נ' ישראל: מנהרות הכרמל (ספטמבר 2013)</u>**: סוס טרויאני חדר למערך ה-IT או למערכת המצלמות. מתקפת סייבר זו גרמה לשיתוק מנהרות הכרמל לשעות רבות במשך יומיים.[4]
5. **<u>סין נ' ארה"ב: חשיפת זהות עובדים בשירות הממשל (מאי 2015)</u>**: הסינים פרצו למאגר עובדים בשירות הממשל האמריקני, וחשפו את זהותם של 4 מיליון עובדים בשירות הממשל. חוקרים סבורים כי סין אוספת מידע כדי לגייס מרגלים.[5]
6. **<u>רוסיה (?) נ' ארה"ב: מתקפת סייבר רחבת היקף על הפנטגון (יולי 2015)</u>**: המתקפה הגדולה בהיסטוריה נגד הפנטגון. חדירה לרשת הדואלים (מיילים) הלא מסווגת של הכוחות המשולבים. הרשת הושבתה והורדה מהאוויר לשבועיים. פריצת הסייבר המתוחכמת השפיעה על 4,000 חיילים ואזרחים שעובדים במטות המשולבים. כפי הנראה בוצעה המתקפה באמצעות מערכת אוטומטית כלשהי, שמשיגה נתונים עצומים תוך זמן קצר, ושבתוך דקה בלבד מעבירה את כל המידע לאלפי חשבונות באינטרנט.[6]

<u>הנמשל:</u>
פרטתי מספר דוגמאות לגבי תשתיות לאומיות. השאלה היא – מה הקשר אלינו? מה הקשר לארגון שבו אנו עובדים ו/או נותנים לו שירותים? התשובה ברורה, אם תשובשנה תשתיות לאומיות (כגון: חשמל, תקשורת וכד'), לא נוכל לתפקד.
ואז נשאלת השאלה – מה אנו יכולים לעשות בנושא זה, הרי הטיפול בנושא אמור לכאורה להיות ברמת מדינה, ולא ברמת הארגון הבודד? התשובה היא – אנו חייבים להיערך: גיבויים, אתר חלופי, אל פסק ועוד. הדירקטוריון יקבע מדיניות בנושא (לרבות תיאבון הסיכון), ההנהלה תיישם את המדיניות הלכה למעשה, מנהל הסיכונים ייקח בחשבון נושא זה כחלק מניהול הסיכונים הכולל של הארגון, והמבקר הפנימי ישלב את הנושא בתוכנית העבודה שלו.

לדוגמה, הנושא העכשווי שמטריד את תושבי תל-אביב בפרט וגוש דן בכלל הינו עבודות החפירה של הרכבת הקלה. חלק מהסיכונים האפשריים הינם סיכונים תפעוליים כלליים, ולאו דווקא בתחום הסייבר; כגון: תנועה ותחבורה (פקקים, חוסר אפשרות להגיע ממקום למקום וכד'), מפגעים סביבתיים (אבק, רעש, חולדות, ואולי הצפות- "תעלת בלואמילך") ועוד. אבל, גם קיימים סיכונים שקשורים לתחום הסייבר ואבטחת המידע; כגון: עבודות חפירה עלולות לפגוע בקווי תקשורת וטלפוניה. לכך אנו חייבים להיערך (אין הכוונה, כמובן, שנחזור בזמן, ונתקין שובך יונים בכל ארגון/בית ונשתמש בתקשורת ע"י יוני דואר, או שנשתמש בקופסאות גבינה מחוברות ע"י חוטים...). לשם כך ראוי שמבקרים פנימיים ירכשו ידע מתאים בנושא זה, ובמידת הצורך יתייעצו במומחי ביקורת ואבטחת טכנולוגיות מידע. אין ספק, כי נושא הסייבר תופס ויתפוס חלק מהותי יותר ויותר בתוכנית העבודה של הארגונים השונים, ומכאן

גם של הביקורת הפנימית באותם ארגונים. ההשפעה על הביקורת הפנימית הינה גם לגבי עיתוי הביקורת; מעבר מביקורת בדיעבד, לביקורת תוך כדי תהליך, ביקורת בזמן אמת, ביקורת מתמשכת וכד'.

סיכום



מילת המפתח הינה מודעות. ככל שארגונים יהיו יותר מודעים, הם יוכלו לנהל את הסיכונים השונים באופן מושכל יותר. אין ספק שאנו והארגונים שלנו מודעים כיום לסיכוני הסייבר, וחשוב שכולנו נהיה מודעים באותה מידה גם להשפעת סיכוני התשתיות הלאומיות על סיכוני הסייבר. וחשוב מכל – שנדע להיערך לכך בהתאם, תוך התחשבות בתיאבון הסיכון (טווח הסיכון הקביל) של הארגון.[7]

---

[1] https://en.wikipedia.org/wiki/At_the_Abyss

"CIA plot led to huge blast in Siberian gas pipeline", Alec Russell, The Telegraph UK, 28.2.2004
http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html

[2]
https://he.wikipedia.org/wiki/%D7%97%D7%99%D7%99%D7%9C_%D7%94%D7%91%D7%A8%D7%95%D7%A0%D7%96%D7%94_%D7%A9%D7%9C_%D7%98%D7%90%D7%9C%D7%99%D7%9F

"חשד: רוסיה תוקפת וירטואלית את אסטוניה", הארץ, 17.5.2007 (http://news.walla.co.il/item/1108477)

"Russia accused of unleashing cyberwar to disable Estonia", Ian Traynor, the Guardian, 17.5.2007

[3] מאמר "Stuxnet - העתיד כבר כאן", בועז ארד, News1 מחלקה ראשונה, 8.10.2010

[4] "האם האקרים התקיפו את מצלמות האבטחה במנהרות הכרמל?", עומר כביר, כלכליסט, 27.10.2013

"דיווח: מנהרות הכרמל נסגרו בחודש שעבר בעקבות מתקפת סייבר", nana10, 27.10.2013

[5] "פריצת ענק למחשבי הממשל האמריקאי: נחשפו פרטי מיליוני עובדים", הארץ (אי-פי, ניו יורק טיימס), 5.6.2015 ו-13.6.2015

[6] "מתקפת סייבר עצומה: רוסיה פרצה לפנטגון", ynet, 7.8.2015

[7] תקן מקצועי 2600