19 ינואר 2025
סימוכין: חאמ-0014

התמודדות עם סיכוני סייבר במוצרי IoT - המלצות למדיניות

תקציר מנהלים

1. שילובם הגובר של מכשירי "האינטרנט של הדברים" (IoT) בחיי היומיום, החל ממוצרי צריכה, דרך בתים חכמים ועד להטמעתם בתשתיות מדינה קריטיות, מביא עמו סיכוני סייבר משמעותיים, אשר חלקם כבר מתממשים הלכה למעשה, וביתר שאת במהלך מלחמת "חרבות ברזל".
2. למרות נוכחותם ההולכת וגוברת, כשלי שוק מהותיים מובילים לכך שמרבית מוצרי IoT מתאפיינים ברמת אבטחה נמוכה, לצד העדר מודעות לסיכונים מצד המשתמש. כשלים אלו חושפים את הארגונים והמשתמשים בהם באופן סיסטמתי לסיכוני סייבר.
3. סיכונים אלה כוללים שיבוש והשבתת פעילות של מערכות חיוניות כגון רשתות חשמל, תקשורת ובריאות, גישה אסורה ושימוש במידע פרטי, מסחרי ומדינתי, סיכוני אבטחה פיזיים, ואף שימוש במוצרי IoT כפלטפורמת לתקיפת מערכות אחרות.
4. לאור זאת, מדינות רבות ברחבי העולם, ובראשן בריטניה והאיחוד האירופי, הכירו בצורך המתגבר בהתערבות ממשלתית, והחלו לנקוט בצעדים רגולטוריים שונים במטרה לצמצם את הסיכונים הנובעים ממכשירי IoT. מגמה זו מדגישה את החשיבות של נקיטת פעולה גם בישראל, על מנת להגן על המשתמשים ולמנוע את הפיכתה ל"חצר אחורית" החשופה לתקיפות סייבר.
5. **מסמך זה מניח המלצות באשר לצעדי המדיניות הרצויים לצמצום הסיכון הנשקף ממוצרי IoT בישראל. זאת, תוך הבחנה בין מגזרי המשק השונים ורמות הסיכון הנשקף לאינטרס הציבורי מתקיפתם בסייבר ובהתחשב בתשתית החוקית הנוכחית.**
6. עבור שכבות המשק החוסות תחת מסגרת נורמטיבית קיימת, קרי גופי הממשלה, תשתיות מדינה קריטיות (להלן: "תמ'ק") וארגונים חיוניים, ההמלצות ממוקדות באימוץ צעדים לצמצום משטח התקיפה, המתכתבות עם הנעשה בעולם. בממשלה ובתשתיות מדינה קריטיות - הצבת דרישות מחייבות ביחס למאפייני המוצר ולאופן השימוש בו בהתאם לתורה תחומית[1] מבוססת תקנים בין-לאומיים. בארגונים חיוניים - פרסום מדריכים מקצועיים ומתן הנחיות לצמצום משטח התקיפה לצד עדכון השאלון לאבטחת שרשרת האספקה שפיתח מערך הסייבר הלאומי.
7. באשר למגזר הפרטי (יתר המשק), המלצות המדיניות מחולקות לשני מישורי פעולה: הראשון, העלאת מודעות הציבור לסיכוני הסייבר הקיימים במוצרי IoT, בליווי המלצות להתגוננות. השני, חיזוק רמת האבטחה ואספקת מידע על תכונות האבטחה של המוצרים באמצעות הצבת דרישות מחייבות שיחולו על יצרנים, יבואנים ומשווקים. תהליך גיבוש הדרישות יכלול ביצוע הערכה להשפעות רגולציה (RIA), כולל הערכת עלויות למשק, אפקטיביות צפויה, וקיום תהליכי התייעצות ושיתוף ציבור.
8. **בנוסף, נוכח מצב החירום במדינה והצורך לפעול ללא דיחוי לצמצום הסיכונים ממוצרים המציבים פוטנציאל איום ברמה הלאומית, הוקם צוות בין-משרדי ליצירת מענה ממוקד למוצרים אלה, על בסיס התשתית הנורמטיבית ומבנה הסמכויות הקיים.**

[1] תורת סייבר תחומית (Disciplinary Methodology) - מסמך מתודולוגי שנועד להתמודד עם האתגרים הייחודיים סביב בעיה או טכנולוגיה מסוימת, האוגד לתוכו סקירת איומים ספציפיים, מסגרת עבודה שיטתית לזיהוי והערכת סיכונים בתחום, תפיסות התמודדות עם הסיכונים, קווים מנחים להגנה ורשימת בקרות לריסון הסיכונים. התורה התחומית מתבססת על מקורות ידע מהימנים, תקנים ורגולציות בינלאומיים.

מבוא

1. השימוש במוצרי IoT (Internet of Things) עולה בהתמדה במרחב הפרטי והציבורי כאחד. לצד היתרונות הרבים של השימוש במוצרים אלו, גורמי תקיפה מזהים אותם כחוליה חלשה, לרוב בשל רמת אבטחה נמוכה לצד העדר מודעות לסיכונים מצד המשתמש, והלכה למעשה הם נתונים יותר ויותר לתקיפות סייבר מוצלחות.
2. הסיכונים מתקיפות אלה כוללים שיבוש והשבתת פעילות של מערכות חיוניות כגון רשתות חשמל, תקשורת ובריאות, גישה אסורה ושימוש במידע פרטי, מסחרי ומדינתי, סיכוני אבטחה פיזיים, ואף שימוש במוצרי IoT כפלטפורמת לתקיפת מערכות אחרות.
3. תוצאות התממשות הסיכון הומחשו במלחמת "חרבות ברזל", כאשר מצלמות אבטחה ורשת בחזקת אזרחים פרטיים היוו יעד אטרקטיבי לתקיפה. זאת, בין היתר, מתוך מטרה לאסוף מודיעין לריגול ולפגוע במאמצי הלחימה. בתגובה, הממשלה קבעה תקנות שעת חירום, ובהמשך הוראת שעה, המסמיכות את צה"ל ושב"כ לחדור למחשבים המשמשים להפעלת מצלמות נייחות לצורך ביצוע פעולה לסיכול או מניעה של גישה למידע חזותי, שיש בה כדי לסכן את ביטחון המדינה או הרציפות התפקודית של צה"ל.
4. התפתחויות משמעותיות חלו גם ברגולציה הבין-לאומית, בדגש על אירופה, המקדמת חקיקה להחלת דרישות אבטחה רחבות על מוצרי חומרה ותוכנה, וכניסה לתוקף של החוק למוצרי IoT בבריטניה. על רקע הסיכונים ונוכח השינויים במאפייני הרגולציה במרחב הבין-לאומי – התחדד הצורך במענה לאומי בישראל לסיכוני האבטחה במוצרי IoT.
5. **מטרת מסמך זה הינה להניח המלצות באשר לצעדי המדיניות הרצויים לצמצום הסיכון הנשקף ממוצרי IoT בישראל.** ההמלצות נגזרות ממסגרת ניתוח המבחין בין מגזרי המשק השונים ורמות הסיכון הנשקף לאינטרס הציבורי מתקיפתם בסייבר, ועל רקע ניתוח כשלי השוק, התשתית הנורמטיבית וממצאי השוואה בין-לאומית כפי שיפורט להלן.

רקע

מהו IoT?

1. המונח "האינטרנט של הדברים" (Internet of Things - IoT) מתאר טכנולוגיה שבמסגרתה מכשירים פיזיים, משובצי מחשב, מסוגלים לאסוף מידע מהסביבה בה הם נמצאים ולהעבירו למכשיר אחר למטרות שונות בעלות השפעה בעולם הפיזי[2]. מכשירים אלו מקושרים לרשת האינטרנט או למוצרי IoT נוספים בטכנולוגיות חיבור שונות (Bluetooth, Wi-Fi, Zigbee ועוד), באופן המאפשר העברת ועיבוד מידע באופן מקומי או מרוחק (למשל עיבוד בענן).
2. מוצרים אלו כוללים, בין היתר, מוצרים ביתיים "חכמים" - טלוויזיות, מצלמות אבטחה ומערכות אזעקה, צעצועים חכמים ומוניטורים לתינוקות, רכזות בית חכם (hubs) ועוזרות מופעלות קול, מקררים ומכונות כביסה; מכשור לביש (כולל שעונים חכמים); מערכות עירוניות (ניטור זרימת התנועה, פסולת, בטיחות הציבור וכו'); כלי רכב; ציוד תעשייתי ומכשור רפואי.

[2] איגוד האינטרנט הישראלי "האינטרנט של הדברים (IoT) בישראל תועלות, אתגרים והמלצות מדיניות"(2022), בעמוד 11.
https://www.isoc.org.il/files/docs/IOT-Policy-2022.pdf

גידול בהיקף השימוש במוצרי IoT

3. לפי הערכות, מספר מוצרי ה-IoT ברחבי העולם צפוי להכפיל את עצמו מכ-15 מיליארד בשנת 2023 ליותר מ-29 מיליארד בשנת 2030[3]. ברקע למגמה זו, התפתחותן של טכנולוגיות להעברת מידע מהיר באמצעות רשתות האינטרנט והסלולר (5G), מחשוב ענן (Cloud Computing) וטכנולוגיית הבינה המלאכותית (AI) - המאפשרות אחסון, שיתוף ועיבוד מידע בהיקף עצום. מוערך שמגפת ה-COVID-19 שפרצה ב-2020 האיצה גם כן את צריכת המוצרים, ככל הנראה בשל עלייה במתכונת העבודה מרחוק.

ניתוח הבעיה

התופעה הבלתי-רצויה: רמת אבטחת סייבר נמוכה והבנה לא מספקת מצד המשתמשים

מוצרי IoT מתאפיינים בשתי בעיות עיקריות החושפות את המשתמשים בהם לסיכוני סייבר באופן סיסטמתי:

1. **רמה נמוכה של אבטחת סייבר** - המשתקפת בחולשות אבטחה נרחבות ואספקה חלקית ולא עקבית של עדכוני אבטחה לטיפול בהן. המוצרים מתוכננים לעתים קרובות תוך התמקדות בנוחות המשתמש אך על חשבון תכונות אבטחה בסיסיות. כך, במכשירי IoT רבים אין אפשרות להתקין עדכוני אבטחה או לבצעם באופן אוטומטי, פעמים רבות המוצרים מגיעים עם סיסמת ברירת-מחדל ללא הכרח בשינויה. יתרה מכך, לעתים כלל לא קיים ממשק משתמש (מסך, לוח מקשים) במכשיר, דבר המקשה על המשתמש לשנות את הסיסמא, ההגדרות ועדכוני אבטחה, והופך אותו לפחות מאובטח[4].
2. **הבנה לא מספקת בקרב המשתמשים על סיכוני הסייבר של המוצרים –** היעדר הבנה ומודעות לסיכוני לשימוש לא-מאובטח במוצרים. מחקרים מצביעים על כך שיש מחסור משמעותי במידע על תכונות האבטחה המובנות במוצרים[5], וכתוצאה מכך, צרכנים רבים מניחים שהמוצר שרכשו נושא מאפייני אבטחה כלשהם[6].

גורמי השורש (כשלי השוק)

1. **החצנות שליליות -** היעדר תמריץ ליצרנים להתייחס להיבטי אבטחה במוצר משום שהם אינם נושאים בנזקים הנובעים מתקיפות סייבר. רק לעתים נדירות יצרנים שהושפעו מאירועי סייבר משמעותיים סבלו מהשלכות שליליות משמעותיות בטווח הארוך[7]. מחקר מהולנד על אבטחה של מכשירי IoT מצא כי "העלויות של כשלי אבטחה מוטלות לרוב על בעלי עניין אחרים מלבד בעלי המכשיר או היצרנים"[8]. כלומר, העלויות מתגלגלות לצדדים שלישיים.

---

[3] https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/#statisticContainer
[4] Impact Assessment: Regulation of consumer connectable product cyber security, Department for Science, Innovation and Technology (DSIT), 10 July 2023,p.13 https://www.legislation.gov.uk/ukia/2023/80/pdfs/ukia_20230080_en.pdf
[5] Blythe, J. M., Sombatruang, N., & Johnson, S., 2018. 'What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?' https://osf.io/preprints/socarxiv/63zkt/
[6] Harris Interactive, Consumer Internet of Things Security Labelling Survey Research Findings Report, February 2019
[7] Morgner and Benenson (2018): "Exploring Security Economics in IoT Standardization Efforts", Workshop on Decentralized IoT Security and Standards (DISS) 2018, p. 3.
[8] Rodríguez et al (2021): "Superspreaders: Quantifying the Role of IoT Manufacturers in Device Infections", 20th Annual Workshop on the Economics of Information Security (WEIS 2021), p. 13.

2. **Time to Market** - בשל האופי המהיר של שוק המוצרים הטכנולוגיים, יצרנים שואפים להביא לשוק מוצרים או מאפיינים חדשים במהירות (יתרון למוביל ראשון[9]). מאחר ולרוב אין ליצרנים ניסיון או מומחיות בתחום אבטחת הסייבר, היבטי אבטחה מהווים חסם פוטנציאלי לכניסה מהירה לשוק.
3. **אסימטריה במידע בין צרכנים ליצרנים בנוגע למאפייני האבטחה של המוצרים -** משתמשים לרוב אינם יכולים להעריך את רמת האבטחה של מוצר שהם רוכשים. סקר שנערך בקרב יצרני מכשירי IoT ברחבי העולם גילה שרק 43% מהיצרנים מספקים מידע למשתמשים לשינוי סיסמאות ברירת מחדל ורק 26% מהיצרנים מספקים מידע הנוגע להגנה על המוצרים שלהם מפני התקפות[10]. במצב זה, המכונה בספרות "שוק לימונים" — שוק שבו הצרכנים אינם יודעים להעריך את ההבדל בין מוצרים שונים בהיבטי אבטחת סייבר[11], נבצר מהם לתמרץ את היצרנים למימוש שיטות אבטחה טובות יותר באמצעות כוחות השוק.
4. כשלי השוק המתוארים לעיל מובילים למציאות שבה אין ליצרנים תמריץ לשפר את רמת האבטחה של המוצרים. **במאפייני השוק הנוכחיים אין לצפות לשינוי המצב הקיים ללא התערבות מדינתית.** גישה זו רווחת גם במדינות המובילות בעולם המערבי, כפי שיוצג בהמשך המסמך.

סיכונים

סוגי סיכונים מרכזיים ביחס לאבטחת הסייבר של מוצרי IoT

1. **גישה ושימוש במידע על ידי מי שאינו מורשה לכך** - מוצרי IoT במרחב הפרטי והציבורי מייצרים מטרות אטרקטיביות לתקיפה בשל עושר המידע שהמכשירים צוברים על המשתמשים וסביבתם, כולל מידע אישי ורגיש (פרטים מזהים, מידע פיננסי, ביומטרי, סיסמאות, צילומים והקלטות ועוד). גישה לא מורשית למידע עלולה לגרום לפגיעה בפרטיות ובמוניטין, לגניבת זהות ורכוש, ואף לשמש גורמים עוינים לביצוע פעילויות מעקב וריגול ביטחוני ותעשייתי.
2. **ניצול חולשות במערכות IoT לגרימת נזקים בעולם הפיזי** - מתקפת סייבר כגון פריצה לרכבים ומכשירי בריאות, כגון קוצבי לב, עשויה לסכן את חיי המשתמשים. תיתכן גם השפעה על הציבור הרחב, כאשר מתקפה על מערכות נתמכות IoT עשויה להביא לפגיעה בפעילותן עד כדי שיתוקן של מערכות חיוניות – למשל רשת החשמל, מערכות לטיפול במי שתייה, מערכות פיננסיות, בתי חולים, מתקני כימיקלים וכו'.
3. **שימוש במוצרי IOT לתקיפת מערכות אחרות**[12] - תוקפים יכולים להשתמש במוצרי IoT כדי להסתנן לרשתות פנימיות ולהשתמש בהם כבסיס לתקיפה נרחבת על מערכות אחרות, ובכלל זה מתקפות מניעת שירות מבוזרת (DDOS – Distributed Denial of Service). לרוב, התוכנה התוקפת לא משפיעה על פעילות המכשיר כך שהבעלים אפילו לא מודע לתקיפה.

- **דוגמאות הממחישות את הסיכונים מפורטות בנספח א.**

---

[9] שם, עמ' 11
[10] ה"ש 7, עמ' 9
https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-rodriguez.pdf
[11] הרשקוביץ, שוורץ אלטשולר, סיון סבליה, **מהו סייבר? חלק א: על מרחב הסייבר, תקיפות סייבר והגנת סייבר**, המכון הישראלי לדמוקרטיה (2021), עמ' 9 https://www.idi.org.il/media/16859/what-is-cyber-security-part-one-cyberspace-cyber-attacks-and-cyber-protection.pdf
[12] ה"ש 1, עמ' 42

פוטנציאל הנזק

1. קיים קושי מתודולוגי להעריך בצורה מדויקת את פוטנציאל הנזק כתוצאה מתקיפת סייבר על מוצרי IoT בישראל. לצורך הערכה בקירוב של הסיכונים, נתבסס על ניתוח דיפרנציאלי של משטח התקיפה. ניתוח זה מתמקד במשמעויות השונות העלולות להתרחש בעת תקיפות סייבר והנזקים האפשריים כתוצאה מתקיפות אלו, תוך הבחנה בין יעדי התקיפה השונים:

1) **גופי ממשלה** - המערכות הממשלתיות כוללות מידע אישי של האזרחים ומידע על פעולות המדינה וגופיה השונים, ובו בזמן מאפשרות למשק לתפקד באופן שוטף. פגיעה במערכות הממשלה עלולה להסב נזק משמעותי **לתפקודה, לריבונותה ולביטחונה של מדינת ישראל ואזרחיה**. ברבים מגופי הממשל עושים שימוש במצלמות, נתבי Wifi (ראוטרים), ומערכות ניהול מבנה Building Management Systems, המאפשרות שליטה ובקרה על מערכות המבנה השונות כגון מערכות חשמל, תאורה, מיזוג אוויר, בטיחות, אבטחה, מעליות ועוד.

2) **תשתיות מדינה קריטיות** - אלו משמעותיות להמשך תפקודו התקין של המשק (לדוג' חברת החשמל, בנק ישראל, חברת המים מקורות וכו'). ברבים מגופי התמ"ק ניתן למצוא מצלמות, בקרים (קירור, השקיה, פסולת), סנסורים (חיישנים), ומערכות כריזה. לעתים מדובר בפריסה רחבת היקף של מכשירים מחוברים, המייצרת קושי לניטור קבוע ורציף. פגיעה במערכות בתשתיות אלה עלולה לגרום **לפגיעה בביטחון הציבור, באספקת שירותים ומוצרי צריכה חיוניים לאזרח, או חלילה סיכון חיי אדם**[13]. קיים גם סיכון לריגול, אשר ביחס לתעשיות רגישות, כתעשיות ביטחוניות עלול להוות סיכון ביטחוני[14].

3) **ארגונים חיוניים** - שכבה המורכבת מהגופים שפגיעה בהם עלולה להוביל לפגיעה בתפקוד התקין של המשק ובכלכלה הישראלית (לדוג' בתי חולים, רשויות מקומיות) גם בשכבה זו פגיעה במערכות עלולה להוביל **לפגיעה בביטחון הציבור, באספקת שירותים חיוניים לאזרח, ולסיכון חיי אדם**. למשל השבתת מכשור רפואי מקוון מציל חיים או חבלה בציוד מערכות בריאות שמוביל להרס תרופות או ציוד רפואי.

4) **יתר המשק** - פגיעה במוצרי IOT בחזקת עסקים ואזרחים טומנת פוטנציאל לפגיעה בפרטיות (פרטים מזהים, מידע פיננסי, ביומטרי, סיסמאות, צילומים והקלטות ועוד), הזלגת מידע עסקי, פגיעה פיזית בציוד ועוד.

5) מעבר לכך, לתקיפות סייבר השפעות כלכליות נרחבות ביותר, כאשר אלו רלוונטיות לכלל הסיכונים שהוצגו לעיל. ממצאי דו"ח הערכת עלויות כלכליות שבוצע במערך הסייבר הלאומי מראים כי **עלות תקיפות סייבר בישראל מוערכת בסכום של כ־12 מיליארד ₪ בשנה**[15]. הגם שחלקם של תקיפות של מוצרי IoT מסך העלויות אינו ידוע, מוסכם כי, ללא מענה הגנתי הולם, עלויות אלו צפויות לגדול מדי שנה עם ההתפתחות הטכנולוגית בכל תחומי החיים והגידול הצפוי בכמות המתקפות ובאיכותן.

---

[13] ה"ש 10, עמודים 42-43.
[14] שם.
[15] מערך הסייבר הלאומי, "הערכת העלות הכלכלית בגין תקיפות סייבר בישראל" (2024), עמ' 3.

מצב קיים

התשתית הנורמטיבית בישראל

1. מערך הסייבר הלאומי אמון על קידום יכולת ההגנה על מרחב הסייבר בישראל מכוח החלטות הממשלה מס' 3611 (2011), 2443 (2015), 2444 (2015) ו-3270 (2017). **החוק להסדרת הביטחון בגופים ציבוריים**[16] מטיל על המערך את האחריות לטיפול ב"באבטחת מערכות ממוחשבות" בגופי תמ"ק המונחים על ידו (רשימת הגופים מנויה בתוספת החמישית לחוק).

2. מכוח החלטת ממשלה 2443, המערך מנחה מקצועית את **היחידות המגזריות** שהוקמו בתוך משרדי הממשלה ויחידות הסמך השונות, האחראיות על קידום הגנת הסייבר בענפים שונים, ואת **יה"ב** (היחידה להגנת הסייבר בממשלה) במערך הדיגיטל, האמונה על הגנת הסייבר במשרדי הממשלה וביחידות הסמך.

סקירה השוואתית

1. במטרה ללמוד ממדינות מתקדמות אחרות כיצד בחרו להתמודד עם סיכוני הסייבר ממוצרי IoT, נסקרו דברי חקיקה בשלוש מדינות השוואה: בריטניה, האיחוד האירופי וארה"ב.

א. **בריטניה** – בשנת 2022 עבר חוק אבטחת מוצרים ותשתיות טלקומוניקציה (**Product Security and Telecommunications Infrastructure Act 2022**), והתקנות מכוחו נכנסו לתוקף באפריל 2024. החוק מחייב יצרנים, יבואנים ומפיצים לעמוד בדרישות אבטחה עבור מוצרים IoT, המבוססות על הוראות תקן ETSI EN 303 645 ועל תקן ISO/IEC 29147:2018. החוק מגדיר קנסות כספיים גבוהים על הפרת הדרישות, שיכולים להגיע עד ל-10 מיליון או 4% מהכנסה שנתית (הגדול מבניהם).

ב. **האיחוד האירופי** – בשנת 2024 אושר חוק חוסן הסייבר (**Cyber resilience Act**), על ידי מועצת האיחוד האירופי והפרלמנט, תחולת יישומו בפועל נקבעה לשנת 2027. החוק מטיל חובה על יצרנים, יבואנים ומשווקים של מוצרים עם אלמנטים דיגיטליים, כולל תוכנה וחומרה, לעמוד בדרישות אבטחה בתכנון, פיתוח, ייצור, אספקה ותחזוקה של המוצר וניהול הטיפול בחולשות. החוק מייצר הבחנה בין המוצרים בחלוקה לשלוש קטגוריות סיכון (רגילה, חשובה, וקריטית), המתבטאת בדרישה לאופן יישום הערכת התאמה (conformity assessment) עצמית או על ידי צד שלישי. הקנס בחוק יכול להגיע עד 15,000,000 אירו או עד 2.5% מסך המחזור השנתי, לפי הגבוה מבניהם.

ג. **ארה"ב** – בשנת 2020 נחקק בארה"ב חוק "שיפור אבטחת הסייבר באינטרנט של הדברים" (**Internet of Things Cybersecurity Improvement Act**, PUBLIC LAW 116–207). החוק מחייב את סוכנויות הממשל הפדראלי, לעמוד בהנחיות אבטחת סייבר שקבע המכון הלאומי לתקנים וטכנולוגיה (NIST) בתקן **SP 800-213**, וכן קטלוג **SP 800-213A** המפרט בקרות טכניות ולא טכניות בנוגע לאופן השימוש והניהול המתאימים למכשירי IoT בבעלות או בשליטת של הממשל.

[16] חוק להסדרת הבטחון בגופים ציבוריים, תשנ"ח-1998, https://www.nevo.co.il/law_html/law01/111m1_001.htm

1) **קליפורניה** - חוק אבטחת מכשירים מחוברים (Security of Connected Devices, SB-327) משנת 2020, מחייב "תכונות אבטחה סבירות". החוק לא מספק שיטות קונקרטיות להגנה, מלבד התייחסות ספציפית לסיסמה (סיסמה דיפולטיבית ייחודית, לחילופין- יצירת אמצעי אימות חדש בשימוש ראשון).

2) **אורגון** - בשנת 2020 נכנס לתוקף חוק (**HB- 2395**) עם נוסח כמעט זהה לזה של קליפורניה, במטרה להגן על מכשירים והמידע שבהם מפני גישה בלתי מורשית, השמדה, שימוש, חשיפה או שינוי.

- **הרחבה על החקיקה לעיל בנספח ב.**

המלצות למדיניות

השילוב שבין חשיבות מערכות IoT בעולם המודרני לבין פגיעותן למתקפות סייבר, על רקע כשלי השוק שתוארו, **מחדד את הצורך בהתערבות מדינתית**, כפי שכבר נעשה במדינות מפותחות. המלצות המדיניות מחולקות בהתאם להבחנה שנערכה בפרק הערכת הסיכון ובהתחשב בתשתית החוקית הנוכחית.

כך, עבור שכבות המשק החוסות תחת מסגרת נורמטיבית קיימת – ההמלצות ממוקדות באימוץ צעדים לצמצום משטח התקיפה המתכתבים עם הנעשה בעולם. באשר לשכבת המשק שאינה מוסדרת – עיצוב אופן ההתערבות המדינתית בנושא כולל תהליך בחינה של מספר חלופות מדיניות, החל מכלים "רכים" דוגמת פרסום מדריכים והמלצות, דרך תמריצים כלכליים, ועד להחלת דרישות באמצעות רגולציה מחייבת. לאחר בחינת החלופות המלצת המדיניות הינה להחיל דרישות אבטחה מחייבות עבור המוצרים, כפי שיפורט להלן.

1. **גופי ממשלה – הצבת דרישות מחייבות** ביחס למאפייני המוצר ולאופן השימוש בו במשרדי הממשלה ויחידות הסמך. הדרישות יגזרו מתורה תחומית להגנה על מוצרי IoT מבוססת תקנים בין-לאומים, בדומה למודל בארה"ב, הנשען על תקן NIST SP 800-213; **הטמעת דרישות אבטחה כתנאי בחוזים ובמכרזים ממשלתיים** במסגרת הליכי רכש מרכזיים או של משרדי הממשלה ויחידות הסמך, לרכש של מוצרי IoT.

2. **תשתיות מדינה קריטיות – הצבת דרישות מחייבות** המתייחסות למאפייני המוצר ולאופן השימוש בו בגופי התמ"ק, אשר יגזרו מתורה תחומית להגנה על מוצרי IoT (ר' לעיל).

3. **ארגונים חיוניים – פרסום מדריכים מקצועיים ומתן הנחיות** לארגונים לצמצום משטח התקיפה בהתאם למאפייני הסיכון בענפי המשק השונים**; עדכון שאלון אבטחת שרשרת אספקה שפרסם מערך הסייבר הלאומי** להוספת מודול IoT, אשר יתבסס על תורה תחומית להגנה על מוצרי IoT ויתורגם לבקרות מדורגות המותאמות לרמת הסיכון של הספק, הנגשתם בשאלון הספקים המקוון ובמערכת יוב"ל[17] בהתאם.

[17] מערכת יוב"ל – מערכת יעדים ובקרות לארגון https://grc.cyber.gov.il/scripts/manage/login.aspx

4. **המגזר הפרטי** – שכבת משק זו כוללת את העסקים שאינם מוגדרים תשתיות חיוניות או קריטיות ואת כלל האזרחים. כיום, שכבה זו אינה מוסדרת, ואינה מקבלת מענה באמצעות התשתית הקיימת. כאמור, **בשל הכשלים המהותיים, אין לצפות לתיקון המצב ללא התערבות המדינה**. אדרבא, הצפי הוא שהפער יחריף, ולכן חלופה של היעדר התערבות (חלופת ה-0) אינה פותרת את הבעיה.

חלופות נוספות אשר נבחנו בתהליך גיבוש המדיניות: קמפיין ציבורי להעלאת מודעות לסיכוני סייבר; תכנית תיוג (Labeling) וולונטארית המאפשרת ליצרנים לסמן מוצרים כעומדים בדרישות אבטחה בסיסיות; תכנית תיוג מנדטורית שתחייב יצרנים לגלות מידע על היבטי אבטחה של המוצר; דרישות מחייבות ליצרנים לעמידה בדרישות אבטחה. באשר לחלופות הנוגעות לתכניות לסימון מוצרים תיוג, מחקרים מראים כי אלו בעלות אפקטיביות מוגבלת לשינוי התנהגות צרכנית, בין אם באופן וולונטארי או מנדטורי, ועל כן מביאים לתועלת נמוכה ביחס לחלופה המחייבת לעמוד בדרישות אבטחה.

משכך, המלצת המדיניות ביחס לשכבת משק זו מתמקדת בשני מישורי פעולה:

1) **מודעות והסברה** - גיבוש וניהול קמפיין מתמשך להעלאת מודעות הציבור לסיכוני הסייבר הקיימים במוצרי IoT, בחלוקה לקהלי יעד ומאפייני השימוש הבולטים, ובליווי המלצות להתגוננות.

2) **חיזוק רמת האבטחה ואספקת מידע על תכונות האבטחה של המוצרים** – באמצעות הצבת דרישות מחייבות ליצרנים, יבואנים ומשווקים. אלו, יכולות להגיע בדמות תקינה, הנחיות או חקיקה ייעודית, ובהיקף תכולה הנע במנעד שבין מצומצם לרחב (מודל החוק בקליפורניה ואורגון/ בריטניה/ האיחוד האירופי).

יודגש, כי תהליך גיבוש הדרישות המחייבות מצריך ביצוע הערכה להשפעות רגולציה (RIA) ובכלל זאת הערכת עלויות למשק (ציות, יידוע, הפסדי סחורה פסולה, מערך פיקוח ואכיפה), אפקטיביות צפויה (התמודדות עם ייבוא אישי, מתן זמן הטמעה וכו'), וקיום תהליכי התייעצות ושיתוף ציבור.

בנוסף, נוכח מצב החירום במדינה המתקיים נכון למועד כתיבת מסמך זה, והעלייה בעוצמה ובחומרת תקיפות הסייבר, **קיים צורך לפעול ללא דיחוי לצמצום הסיכונים ממוצרים המציבים פוטנציאל איום ברמה הלאומית,** בהתחשב בהיקף הפריסה ופוטנציאל הנזק הטמון בהם. לשם כך, **הוקם צוות בין-משרדי להנעת מאמץ משולב ליצירת מענה ממוקד לסיכונים ממוצרים אלה**, על בסיס התשתית הנורמטיבית הקיימת, בהובלת מערך הסייבר הלאומי ובשיתוף בעלי העניין הרלוונטיים בממשלה.

נספח א – דוגמאות לסוגי סיכוני סייבר ממוצרי IoT

1. קיימות דוגמאות רבות להשפעה של מתקפות על מערכות IoT על הממד הפיזי, אחת מהן היא באירוע משנת 2014 שבו חוקרים הדגימו את יכולתם לפרוץ מרחוק למערכות מחשב של מכוניות ולסכן את חייהם של נוסעי המכונית ועוברי אורח. החוקרים הוכיחו כי ניתן להתחזות לנהג הרכב, ללא צורך בגישה פיזית, אלא באמצעות ניצול פרצת אבטחה במערכת מולטימדיה בשם Uconnect מתוצרת פיאט- קרייזלר שהותקנה ברכב כדי להשתלט על מערכת הבידור שלו. לאחר ההשתלטות ביצעו החוקרים שינויים בתוכנת ההפעלה של מערכת המחשוב, וזו אפשרה להם לשלוח פקודות להגה, בעקבות הניסוי הפיצה חברת פיאט-קרייזלר עדכון מערכות וביצעה החזרה (Recall) של 1.4 מיליון כלי רכב[18]. דוגמאות רלוונטיות נוספות הודגמו במחקר משנת 2016 שבוצע על ידי חוקרים מקנדה וממכון ויצמן ובו הצליחו לתקוף נורות "חכמות", להפיץ את הווירוס התוקף מנורה לנורה ולשלוט על כיבוין והדלקתן. מחקר נוסף משנת 2020, שנערך על ידי קבוצת צרכנים ויועצי אבטחה, מצא כי תקעים חכמים בשוק מכילים חולשות שעלולות להוביל לשריפה.

2. דוגמא בולטת לשימוש במכשירי IoT לתקיפת מערכות אחרות היא מתקפת התוכנה הזדונית מיראי (Malware Mirai), ב-2016, שאפשרה לתוקפים להשתלט על אלפי מכשירי IoT, כמו מצלמות רשת ונתבי רשת, כצבא בוט־נטים (רשת של מערכות מחשב שנשלטות מרחוק על ידי האקרים) אשר יצרו יחד מתקפת מניעת שירות מבוזרת (DDoS) כדי לשבש את השירות של אתרים רבים כמו נטפליקס (Netflix), סי אן אן (CNN), וטוויטר (Twitter). המשתמשים במכשירים הנגועים לא ניזוקו כלל ואפילו לא היו מודעים כי המכשירים מעורבים במתקפה כלשהי, מאחר שהמכשירים תפקדו כהלכה . במקרה אחר משנת 2013, מתקפת סייבר בינלאומית על למעלה מ־100,000 מכשירי חשמל ביתיים חכמים, כגון טלוויזיות, רמקולים, מקררים ונתבי תקשורת עשתה בהם שימוש לשליחה של מעל 750,000 מסרי דואר אלקטרוני זדוניים.

3. דוגמא למתקפה שכללה גישה ושימוש במידע על ידי מי שאינו מורשה לכך אירעה בשנת 2017, שבה קזינו בצפון אמריקה חווה מתקפת סייבר שכללה אובדן של כמויות עצומות של נתונים עסקיים (10 GB), בשל חולשה שנמצאה בתוך מדחום חכם במיכל דגים. האקרים ניצלו חולשה זו כדי לפרוץ לרשת הרחבה יותר של הקזינו[19].

---

[18] חיים ויסמונסקי ומאי הר-שי, התמודדות משפטית עם איומי סייבר לכלי רכב "חכמים"(2020) עמ 208.
https://csrcl.huji.ac.il/sites/default/files/csrcl/files/hukim-13-197.pdf

[19] ה"ש 2, עמוד 20.

נספח ב – השוואה בין-לאומית

בריטניה

1. חוק אבטחת מוצרים ותשתיות טלקומוניקציה- **PSTI** (Product Security and Telecommunications Infrastructure Act 2022)[20], עבר בבריטניה ב-6 בדצמבר 2022, והתקנות מכוחו נכנסו לתוקף ב-29 באפריל 2024.
2. חלקו הראשון של החוק מחייב **יצרנים, יבואנים ומפיצים** לעמוד בדרישות אבטחה עבור "מוצרים מחוברים" (internet and network connectable products), תוך **הגדרת קנסות כספיים גבוהים על הפרת הדרישות, שיכולים להגיע עד ל-10 מיליון או 4% מהכנסה שנתית (הגדול מבניהם).**
3. **"מוצרים מחוברים" כוללים את כל המכשירים בעלי גישה לאינטרנט** (כמו מכשירי טלפון חכמים, טלוויזיות חכמות, קונסולות משחקים, מצלמות אבטחה ומערכות אזעקה, צעצועים חכמים ומוניטורים לתינוקות, רכזות בית חכם (Hubs) ועוזרות מופעלות קול ומכשירי בית חכם כגון מכונות כביסה ומקררים), **וכן מוצרים שיכולים להתחבר למספר מכשירים אחרים אך לא ישירות לאינטרנט** (נורות חכמות, תרמוסטטים חכמים ומעקבי כושר לבישים למשל).
4. החוק לא חל על מחשבים נייחים וניידים משום שמערכות ההפעלה בהם כבר כוללות תכונות אבטחה כך שאינם כפופים לאותם איומים וסיכונים.
5. דרישות האבטחה למוצרים קבועות בתקנות[21], ומבוססות על הוראות תקן ETSI EN 303 645 ועל תקן ISO/IEC 29147:2018. הדרישות כוללות:
   1) איסור על סיסמאות ברירת מחדל אוניברסאליות/ניתנות לניחוש בקלות
   2) פרסום אמצעי יצירת קשר (point of contact) לדיווח על בעיות אבטחה במוצר
   3) מידע על תקופת עדכוני אבטחה – תקופת הזמן המינימאלית שהמוצר יקבל עדכוני אבטחה.
6. בנוסף, יצרנים מחויבים:
   1) לחקור כל חשד לכשל בהתאמה ביחס למוצר.
   2) במקרה של כשל בהתאמה– על היצרן למנוע זמינות של המוצר ללקוחות בבריטניה; לתקן את כשל ההתאמה; להודיע על כשל ההתאמה בהקדם האפשרי.
   3) ניהול תיעוד של (א) כל חקירה שערך ביחס לכשל התאמה או חשד לכשל התאמה - ותוצאותיה (ב) כל כשלי התאמה הנוגעים למוצר- וכל צעד שנקט היצרן כדי לתקן את כשל ההתאמה בין אם הצעדים הללו הצליחו או לא. את התיעוד יש לשמור למשך 10 שנים מיום עריכתו.

20 https://www.legislation.gov.uk/ukpga/2022/46/part/1/enacted
21 https://www.legislation.gov.uk/uksi/2023/1007/schedule/1/made

האיחוד האירופי

1. החוק בנושא "דרישות אבטחת סייבר למוצרים עם אלמנטים דיגיטליים" **Cyber Resilience Act**[22] (horizontal cybersecurity requirements for products with digital elements), נכנס לתוקף ב-10 באוקטובר 2024. מועד תחולת היישום בפועל של מרבית הדרישות המנויות בחוק צפוי לשנת 2027.
2. החוק מציב דרישות אבטחה מחייבות עבור היקף רחב של מוצרים עם אלמנטים דיגיטליים. אלו, מוגדרים "כל מוצר, תוכנה או חומרה, בעל פתרונות עיבוד נתונים מרחוק, כולל תוכנה או רכיבי חומרה היוצאים לשוק בנפרד".
3. רכיבי החומרה אליהם מתייחס החוק כוללים, בין היתר, מחשבים ניידים, מכשירים חכמים (IoT), טלפונים חכמים, ציוד רשת או מעבדים. במוצרי תוכנה נכללים גם מערכות הפעלה, מעבדי תמלילים, משחקים או אפליקציות לנייד וכדומה.
4. החוק צפוי לחול על **יצרנים, יבואנים ומפיצים** (המוגדרים כולם "מפעילים כלכליים"), ומטיל חובה **לעמידה בדרישות אבטחה בתכנון, עיצוב, פיתוח, ייצור, אספקה ותחזוקה של המוצר והתייחסות ממוקדת לטיפול בחולשות** (זיהוי תיעוד, עדכוני אבטחה,יידוע).
5. החוק כולל גם דרישות פרוצדוראליות (ניהול תהליך סדור, ביצוע הערכת התאמה לדרישות החוק הטבעת סימון CE על המוצר, נשיאה באחריות למוצר במשך חיי המוצר או חמש שנים, המוקדם מביניהם).
6. החוק עורך הבחנה בין מוצרים בעלי רמות סיכון שונות, שעלולים להביא להשפעות שליליות בסדרי גודל שונים. זו, באה לידי ביטוי בעיקר בדרישות לאופן יישום הערכת התאמה (conformity assessment) באמצעות הערכה עצמית או על ידי צד שלישי.
7. במקרה של הפרה של דרישות החוק, **יתכנו קנסות מקסימליים של עד 15,000,000 אירו או עד 2.5% מסך המחזור השנתי העולמי לשנת הכספים הקודמת, לפי הגבוה מבניהם**. הסכום המדויק תלוי בסוג ובחומרתה של ההפרה.
8. החוק מסמיך את הרשויות להורות על החזרה (recall) של מוצרים שאינם עומדים בדרישות, ובמקרים חמורים, הרשויות עשויות להטיל איסור על מכירת מוצרים שאינם עומדים בדרישות באיחוד האירופי.

[2222]REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

ארה"ב

9. על רקע השימוש הגובר במכשירי IoT בממשל הפדראלי, נחקק בארה"ב חוק לשיפור אבטחת הסייבר באינטרנט של הדברים משנת 2020 (Internet of Things Cybersecurity Improvement Act, PUBLIC LAW 116–207).
10. החוק מחייב את המכון הלאומי לתקנים וטכנולוגיה (NIST) ואת המשרד לניהול ותקציב (OMB) לנקוט בצעדים להגברת אבטחת הסייבר עבור מכשירי IoT. החוק חייב את NIST לפתח ולפרסם תקנים והנחיות עבור הממשל הפדרלי, על השימוש והניהול המתאימים של מכשירי IoT בבעלות או בשליטת סוכנות פדראלית המחוברים למערכות מידע בבעלותה או בשליטתה, כולל דרישות אבטחת מידע מינימליות לניהול סיכוני אבטחת סייבר הקשורים למכשירים.
11. בנובמבר 2021 פרסם NIST את הנחיות אבטחת סייבר של מכשירי IoT לממשלה הפדראלית (SP 800-213), וכן קטלוג (SP 800-213A) המפרט בקרות טכניות ולא טכניות ליישום דרישות האבטחה של מכשירי IoT.
12. הצעת החוק מחייבת את ה-OMB לבחון את מדיניות ועקרונות אבטחת המידע של הסוכנות הפדראלית על בסיס התקנים שגיבש NIST. חל איסור על סוכנות פדראלית לרכוש, להשיג או להשתמש במכשיר IoT אם הסוכנות קובעת במהלך חתימת חוזה שהשימוש במכשיר מונע עמידה בתקנים ובהנחיות. בכפוף לוויתור במידת הצורך לביטחון המדינה, למטרות מחקר, או כאשר מכשיר מאובטח בשיטות יעילות חלופיות[23].

קליפורניה ואורגון

13. מדינת קליפורניה חוקקה כבר ב-2018 חוק (SB-327, Security of Connected Devices) לאבטחת IoT אשר נכנס לתוקף ב-1 בינואר 2020. מטרת החוק להגן על המכשיר ועל המידע הכלול בו מפני גישה בלתי מורשית, השמדה, שימוש, שינוי או חשיפה, כנדבך נוסף בהגנה על פרטיות המידע.
14. לצורך כך, החוק מגדיר כי התקני IoTהמסוגלים להתחבר לאינטרנט ישירות או בעקיפין, ושהוקצו לו כתובת פרוטוקול אינטרנט או כתובת Bluetooth, חייבים להיות מצוידים ב"תכונות אבטחה סבירות". הגדרה זו אינה מספקת שיטות קונקרטיות להגנה, מלבד התייחסות ספציפית למאפייני הסיסמאות: מכשירים שיוצרו/ייובאו יהיו בעלי סיסמאות ברירת מחדל ייחודיות, או: דרישה שמשתמש ייצור אמצעי אימות חדש בטרם קבלת גישה למכשיר בפעם הראשונה.
15. מדינת אורגון (HB-2395) הצטרפה לקליפורניה עם טקסט כמעט זהה שנכנס גם כן לתוקף ב-1 בינואר 2020.

[23] https://www.congress.gov/bill/116th-congress/house-bill/1668