ירושלים, י״ז אב תשפ״ב
14 באוגוסט, 2022

<u>הנחיה: חובת גילוי לגבי סיכוני מוצרי IoT ״האינטרנט של הדברים״</u>

הנחיה זו נכתבה בשיתוף עם מערך הסייבר הלאומי במשרד ראש הממשלה.[1]

האינטרנט של הדברים – Internet of Things (או בקיצור IoT)[2] – מתייחס למוצרים המסוגלים לבצע את אחד או את כל הדברים הבאים: לאסוף מידע מהסביבה, לאחסן ולעבד מידע, לתקשר עם מוצרים אחרים באמצעות רשת תקשורת ולבצע פעולות בעולם הפיזי.[3] פעמים רבות מוצרים אלה מכונים בלשון הדיבור מוצרים ״חכמים״.

עם ההתפתחות הטכנולוגית ניתן לראות עלייה בהיקף השימוש במוצרי IoT. מוצרי IoT יכולים להיות מוצרים כדוגמת טלוויזיות חכמות, מזגנים, סטרימרים, בית חכם, דודים חשמליים, מוניטורים של תינוקות, מצלמות אבטחה ביתיות ועוד.

לצד התועלת שנובעת מחיבור מוצרי IoT שונים לאינטרנט קיימים גם סיכונים, שכן מוצרי IoT המקושרים לאינטרנט חשופים לסיכוני סייבר ואבטחת מידע שונים. סיכונים אלו יכולים לפגוע במשתמש במספר דרכים, החל מפגיעה בפרטיות ודליפת מידע אישי ועד נזק פיזי למוצר או לאדם. דברים אלה מקבלים משנה תוקף במקרים שבהם המשתמש אינו נדרש להחליף את הסיסמה הראשונית של מוצר IoT, ופעמים רבות הוא כלל לא מודע לאפשרות לעשות כן, ובנסיבות אלה ניתן להוציא לפועל בקלות רבה יותר תקיפת סייבר נגד המוצר.

---

[1] גוף ממשלתי המופקד על קידום הגנת הסייבר והתמודדות עם תקיפות סייבר במשק הישראלי.

[2] לפי האקדמיה ללשון עברית, המונח IoT מכונה בעברית מִרְשָׁתֶת הַדְּבָרִים. להרחבה, ראו: https://hebrew-academy.org.il/2016/04/13/%D7%9E%D7%9C%D7%99%D7%90%D7%AA-%D7%94%D7%90%D7%A7%D7%93%D7%9E%D7%99%D7%94-%D7%9C%D7%9C%D7%A9%D7%95%D7%9F-%D7%94%D7%A2%D7%91%D7%A8%D7%99%D7%AA-%D7%90%D7%99%D7%A9%D7%A8%D7%94-%D7%9E%D7%95%D7%A0%D7%97/.

[3] ההגדרה של המונח IoT לפי המכון הלאומי לתקנים וטכנולוגיה (NIST) היא ״user or industrial devices that are connected to the internet. IoT devices include sensors, controllers, and household appliances״, ובתרגום חופשי ״התקנים אישיים או תעשייתיים המחוברים לאינטרנט, ובכלל זה חיישנים, בקרים ומכשירי חשמל ביתיים״. להרחבה, ראו: https://csrc.nist.gov/glossary/term/internet_of_things_IoT

לשכת הממונה |
בית עופר, נחום חפצדי 5, קומה 1, גבעת שאול, ירושלים 954840 | טלפון: 073-3717700 | פקס: 073-3717740
nurits@fta.gov.il

הגנת סייבר על מוצרי IoT היא מאתגרת במיוחד, מאחר שבמקרים רבים מדובר במוצרים עם חומרה ותוכנה חלשים ופשוטים משיקולי צורך ועלות ולא ניתן להתקין עליהם אמצעי אבטחה מתקדמים, ומצד שני מוצרים אלה מחוברים לאובייקטים בעולם הפיזי שעליהם הם שולטים.

במקביל, קיימת עלייה מתמדת במספר תקיפות סייבר ברחבי העולם ובפרט בישראל. גורם זדוני יכול להוציא לפועל תקיפות סייבר בקלות יחסית, ובה בעת עלול להיות להן פוטנציאל נזק גדול. בנוסף, ריחוק גיאוגרפי בין התוקף לנתקף, אנונימיות שממנה נהנה התוקף במרחב הסייבר והקושי באכיפה כנגד התוקפים מפחיתים בצורה משמעותית את ההרתעה מפני ביצוע תקיפות סייבר. נוסף על כך, בניגוד לתקיפות קינטיות, שמוגבלות ליעדים שנמצאים בסמוך למקום הימצאותו של התוקף, תקיפות סייבר יכולות להתבצע הלכה למעשה מכל מקום בעולם כנגד כל מקום. לכל אלה צריך להוסיף את העובדה כי התוקף פועל "מעל חוק", עובדה שמקנה לו גמישות רבה, בעוד הנתקפים כפופים למגבלותיו של החוק, עובדה שמקשה עליהם להגן על הרשתות שבשליטתם.

חוק הגנת הצרכן, התשמ"א-1981 (להלן – **החוק**) קובע את האיסור להטעות צרכן, במעשה או במחדל, בפרט מהותי בעסקה, כאשר אחד מהפרטים המהותיים הקבועים בסעיף 2 לחוק הוא "(4) השימוש שניתן לעשות בנכס או בשירות, התועלת שניתן להפיק מהם והסיכונים הכרוכים בהם".

כמו כן, קובע החוק בסעיף 4 חובות גילוי ספציפיות, למשל בסעיף 4(א)(2) –

"כל תכונה בנכס המחייבת החזקה או שימוש בדרך מיוחדת כדי למנוע פגיעה למשתמש בו או לאדם אחר או לנכס תוך שימוש רגיל או טיפול רגיל".

יוער כי הוראות הסעיף חלות גם על שירות ולא רק על נכס.

לעמדת הרשות להגנת הצרכן ולסחר הוגן (להלן – **הרשות**) ומערך הסייבר הלאומי (להלן – **המערך**), לנוכח הסיכונים הממשיים שעלולים להיגרם בשל תקיפות סייבר נגד מוצרי IoT, ניתן לומר כי מדובר בתכונה במוצר המחייבת החזקה או שימוש בדרך מיוחדת. ההחזקה והשימוש כאמור נדרשים כדי למנוע פגיעה בצרכן או במוצר עצמו כפי שפורט לעיל.

סיכוני הסייבר הכרוכים בשימוש במוצרי IoT מתגברים בצורה משמעותית אם הצרכן אינו מחליף את שם המשתמש והסיסמה הגנריים המסופקים עם המוצר כברירת מחדל, וכן אם היצרן אינו מפרסם עדכוני אבטחה מעת לעת (במישרין או על ידי היבואן). לפיכך, ככל שהמוצר אינו כולל אפשרות מנדטורית מובנית לשנות סיסמה או שהיצרן אינו צפוי לפרסם עדכוני אבטחה למוצר, לעמדת הרשות והמערך מדובר בפגם או איכות נחותה בנכס או בשירות וגם זאת יש לגלות לצרכן במפורש בטרם עשיית העסקה כאמור בסעיף 4(א)(1) – "כל פגם או איכות נחותה או תכונה אחרת הידועים לו, המפחיתים באופן משמעותי מערכו של הנכס".

לשכת הממונה |
בית עופר, נחום חפצדי 5, קומה 1, גבעת שאול, ירושלים 954840 | טלפון: 073-3717700 | פקס: 073-3717740
nurits@fta.gov.il

אשר על כן קמה חובה לגלות לצרכן בטרם הרכישה של מוצר IoT כי מדובר במוצר שעלול להיות מנוצל לרעה על ידי גורם זדוני לצורך ביצוע תקיפת סייבר. ככל שיש במוצר IoT מנגנון מנדטורי מובנה להחלפת סיסמה, מתגבשת החובה לגלות לצרכן את החשיבות של החלפת סיסמה ראשונית וכן לגלות איך ניתן להחליף את הסיסמה באופן ברור ומפורט. כמו כן קמה חובה לציין בפני הצרכן אם היצרן צפוי לפרסם עדכוני אבטחה לגבי המוצר, משך הזמן שבו היצרן צפוי לפרסם עדכוני אבטחה למוצר (מה שמכונה בשפה המקצועית End of life), ואם עדכוני האבטחה לא מתעדכנים בצורה אוטומטית – יש לציין איך ניתן להתקין את עדכוני האבטחה באופן ברור ומפורט.

למותר לציין כי האמור לעיל אינו ממצה את כלל אמצעי האבטחה הראויים במוצר IoT, והיצרן והיבואן רשאים להוסיף אמצעים נוספים בהתאם לאופי המוצר ורמת הסיכון הנגזרת מהשימוש בו, ובכלל זה להצפין את תעבורת התקשורת אל המוצר וממנו, לפרסם מדיניות גילוי חדשות ולפרסם פרטי איש קשר שאליו ניתן לדווח על חולשות במוצר, לאחסן שמות משתמש וסיסמאות בצורה מאובטחת, שמירת מידע פרטי בצורה מאובטחת, ליישם עקרונות של הנדסת אבטחה (Security by Design) וליישם Best Practices כגון "Princple of least priviliege", הטמעת מנגנון התראה במוצר על שימוש או שינוי ללא הרשאה, ועוד.[4]

יודגש כי הגילוי חייב להיות להיעשות בטרם עשיית העסקה ובכל שלבי העסקה כגון בשלב השיווק ואף בשלב הפרסום. כמו כן הגילוי חייב להיות ברור ומובן לצרכן וכן באופן מובלט ככל שהוא ניתן בפרסום או בכתב אחר או בעל פה.

אני מנחה את מפקחי הרשות לטפל בכל תלונה לפיה לא היה גילוי נאות כאמור בהנחיה זו כהפרה של הטעיית הצרכן לפי סעיפים 2 ו – 4 לחוק.

בברכה,

מיכאל אטלן, עו"ד
הממונה על הרשות להגנת הצרכן ולסחר הוגן

[4] איגוד האינטרנט הישראלי **האינטרנט של הדברים (IoT) בישראל – תועלות, אתגרים והמלצות מדיניות** (2022); Department for Digital, Culture, Media & Sport in the UK **Code of Practice for Consumer IoT Security** (2018).

לשכת הממונה |
בית עופר, נחום חפצדי 5, קומה 1, גבעת שאול, ירושלים 954840 | טלפון: 073-3717700 | פקס: 073-3717740
nurits@fta.gov.il