ביצוע סקר סיכונים ומבדק חדירות למערכות מידע

נוסח מעודכן בעקבות תיקון 13

1. מבוא

מטרת מסמך זה היא להציג את עמדת הרשות להגנת הפרטיות (להלן: "**הרשות**") בנוגע לביצוע סקר סיכונים ומבדקי חדירות, ולעמוד על חשיבותם להגנת הפרטיות ולאבטחת המידע בארגון, במיוחד לנוכח ריבוי מתקפות הסייבר על ארגונים.

החובה לבצע סקר סיכונים ומבדק חדירות למערכת קבועה בתקנות 5(ג) ו-5(ד) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "**התקנות**"), ביחס למאגרי מידע שחלה עליהם רמת אבטחה גבוהה. עם זאת, סקר סיכונים ומבדקי חדירות הם פרקטיקות רצויות לביצוע בכל ארגון וביחס לכל מאגר מידע אישי, ותרומתן לפעילות הארגון ולאבטחת המידע בו היא רבה.

המסמך יתמקד בשתי החובות הללו, בדגש על מתן המלצות לביצוען, הסבר אודות העיתוי הראוי למלאן, והפרקטיקה המקובלת בנושא.

2. סקר סיכונים

סקר לאיתור סיכוני אבטחת מידע (להלן: "**סקר סיכונים**") נועד להעריך את רמת הבשלות הארגונית, להתמודדות עם איום לפגיעה בשלמות, סודיות וזמינות המידע בארגון. על מנת שסקר סיכונים ישקף נאמנה את אופן ניהול הסיכונים בארגון, על הארגון לזהות, לנתח ולהעריך את כלל התרחישים האפשריים להתרחשות אירוע אבטחה, ואת סבירותם להתממש.

סקר סיכונים הוא הליך מורכב, הכולל שלבים רבים, שניתן לביצוע במתודולוגיות שונות, וביחס למערכות שונות. סקר הסיכונים מתבסס, בין היתר, על הגדרת נכסי הארגון על ידי ההנהלה הבכירה, מיפוי האיומים על המידע הארגוני, והפעילות העסקית של הארגון. סקר הסיכונים אמור לשמש את הארגון כדי להבין אילו בקרות עליו ליישם על מנת שניתן יהיה לבנות תכנית עבודה ממוקדת לנושא זה ובמסגרתה ייקבע סדר העדיפויות לטיפול בסיכונים שונים. זאת בהתאם לחומרת חולשות האבטחה ולסבירות התקיימות התרחישים השונים, כפי שיפורט בהמשך

יש לבצע סקר סיכונים במאגר מידע באופן פרטני, בתהליך עסקי מסוים או בשניהם גם יחד. כמו כן, סקר סיכונים עשוי להידרש גם כאשר נעשים שינויים טכנולוגיים משמעותיים במערכות המידע של הארגון, או שינויים משמעותיים ברכיבי מסמך הגדרות המאגר, שנדרש מכוח תקנה 2(ב) לתקנות.
כמו כן, יש לערוך את סקר הסיכונים מיד בסמוך לאחר הפעלת המאגר והקמת מערכות המאגר, שכן במועד זה נוצרים ומתגבשים הסיכונים עימם אמור הארגון להתמודד.

תקנה 5(ג) לתקנות קובעת **חובת** ביצוע סקר הסיכונים, כדלקמן:

1. החובה חלה על מאגר מידע ברמת אבטחה גבוהה, כפי שמוגדרת בתוספת השנייה לתקנות[1].
2. יש לבצע את סקר הסיכונים אחת ל-18 חודשים לפחות.
3. בעל המאגר נדרש לבחון את תוצאות סקר הסיכונים, את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיו, וכן לפעול לתיקון הליקויים שנמצאו במסגרת הסקר.

נדגיש, כי על אף שהחובה מכוח התקנות חלה רק על מאגר ברמת אבטחה גבוהה, מומלץ לבצע סקר סיכונים גם בארגון שהוא בעליו של מאגר מידע ברמת אבטחה בינונית או ברמת אבטחה בסיסית לעניין התקנות, זאת בהתאם לאופי המידע, רגישותו, היקפו, וחשיבותו לארגון וללקוחותיו.
סקר הסיכונים אותו חובה לבצע לפי תקנה 5(ג) הוא סקר מקיף וכולל, השונה מהחובות השונות החלות על בעל מאגר[2] לבחון ולהתייחס לסיכוני אבטחה ספציפיים המופיעות בתקנות (כגון החובה לבחון את הצורך בעדכון נוהל האבטחה לפי תקנה 4(ה), והחובה לקיים דיון אחת לשנה באירועי האבטחה ולבחון את הצורך בעדכונו של נוהל האבטחה לפי תקנה 11(ג)).

יש לערוך את סקר הסיכונים המקיף מיד בסמוך לאחר הפעלת המאגר והקמת מערכות המאגר, שכן במועד זה נוצרים ומתגבשים הסיכונים עימם אמור הארגון להתמודד. סיכונים אלה נדרשים לבחינה כל 18 חודשים לפחות, על פי התקנות.

יובהר כי על אף האמור לעיל, חלה חובה על ארגון אשר התוודע לסיכוני אבטחה או לשינויים במיפוי סיכוניו (כגון לאור תיעוד אירועי אבטחה לפי תקנה 11(א) או דיון בהם לפי תקנה 11(ג), או במסגרת בחינת הצורך בעדכון נוהל אבטחת מידע כנדרש בתקנה 4(ה)), לפעול מיידית למזעורם ולא להמתין עד לחלוף תקופה של 18 חודשים. עוד יובהר כי טיפול בסיכוני אבטחת מידע, לאחר שנודע לארגון על קיומם, אינה תלויה בעריכת סקר סיכונים.

<u>להלן יפורטו המלצות הרשות בהתייחס להיבטים שונים הרלוונטיים לעריכתו של סקר הסיכונים בארגון:</u>

2.1 מיפוי מערכות

המידע הנאגר במאגר ניתן לעיבוד באמצעות מערכות מידע שונות. לכל מערכת, תוכנה או אפליקציה מאפיינים שונים, ולפיכך גם סיכוני אבטחת המידע משתנים בהתאם למאפיינים אלו.

---

[1] רמת אבטחת המידע נקבעת בהתאם להוראות התוספת הראשונה והשנייה לתקנות, ובכלל זה בשים לב לסוג המידע הקיים במאגר והאם הוא כולל מידע מסוגי המידע המפורטים בסעיף 1(3) לתוספת הראשונה, כמו גם כמות נושאי המידע במאגר. יובהר בעניין זה, כי ההגדרות של רמות האבטחה בתוספת השלישית לחוק הגנת הפרטיות, התשמ"א-1981, רלוונטיות אמנם לעניין גובה העיצום הכספי שניתן להטיל בגין הפרת התקנות, לפי הוראות התוספת השלישית לחוק, אולם הגדרות אלו אינן קובעות את רמת האבטחה החלה על המאגר לעניין התקנות עצמן, ולעניין החובות החלות על המאגר לפי התקנות.

[2] בחוק הגנת הפרטיות הוא מוגדר כ"בעל שליטה במאגר מידע". למען הסר ספק, מדובר באותו הגורם.

שלב מיפוי מערכות המאגר הינו שלב משמעותי שתכליתו הכרת המידע הארגוני והשליטה בו, ובהתאם, הוא מהווה חלק חשוב בסקר הסיכונים של הארגון.

מטרת מיפוי מערכות המאגר היא לשקף ולהציג את מאפייני מערכות המידע המעבדות מידע מן המאגר, לרבות מערך אמצעי האבטחה האמון על הגנתן ובקרתן. מסמך מיפוי מערכות המאגר עשוי לסייע רבות בהבנת תהליכים, ממשקים ויעילות מערכות בסביבת המחשוב. מכאן גם חשיבות המיפוי לצרכי סקירת הסיכונים וההתמודדות עמם.

2.2 המתודולוגיה לעריכת סקר הסיכונים בארגון

ניתן לערוך את סקר הסיכונים במתודולוגיות שונות בהתאם לגישות השונות הרווחות בתחום. על אף ריבוי הגישות, ניתן להגדיר מספר שלבים אלמנטריים והכרחיים המשותפים לכלל הגישות:

- ✓ הגדרת נכסי הארגון.
- ✓ זיהוי וניתוח האיומים על נכסים אלו.
- ✓ זיהוי חולשות ופגיעויות אפשריות, אשר עלולות לחשוף את הארגון לסיכונים.
- ✓ הערכת מידת השפעת התממשות סיכונים אלו על הארגון.
- ✓ מיפוי הפעולות והבקרות הקיימות בארגון, למול הפעולות והבקרות שראוי ליישם לצורך מזעור סבירות התממשות הסיכון.
- ✓ הערכת הסיכון השיורי, בהנחה שמירב הסיכונים מפוקחים ומנוהלים.

2.3 סקרי סיכונים בראי התקנות

ניהול סיכוני הארגון באמצעות עריכת סקר סיכונים הוא שלב מרכזי וחשוב מאוד באבטחת המידע של הארגון. על מנת לזהות ולהעריך את רמת הסיכון לפגיעה באבטחת מידע הקיימת בכל אחד מרכיבי מערכות המאגר, סקר הסיכונים יכלול, בין היתר, גם התייחסות לחובות המפורטות בתקנות הבאות:

- ✓ **תקנה 2(א)(6)** – תקנה זו קובעת כי על בעל מאגר להגדיר במסמך ההגדרות את הסיכונים העיקריים המהווים איום לפגיעה באבטחת המידע הארגוני ואופן ההתמודדות עימם.
  עמדת הרשות היא, שסקר סיכונים הוא דרך המלך למיפוי סיכוני אבטחת המידע, וקביעת דרכי ההתמודדות עימם.
- ✓ **תקנה 4(ג)(5)** - על בעל מאגר לקבוע נוהל אבטחת מידע, שיכלול התייחסות לסיכונים להם נחשף המידע במסגרת הפעילות השוטפת של בעל המאגר, כמו גם התייחסות לאופן קביעת הסיכונים והטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור

במאגר או במערכות המאגר. עמדת הרשות היא כי דרך המלך לביצוע חובה זו היא באמצעות ביצוע סקר סיכונים.

- ✓ **תקנה 4(ה)** – מחייבת בעל מאגר מידע לבחון, אחת לשנה, את הצורך בעדכון נוהל אבטחת מידע, ובנוסף קובעת את חובתו לבחון אם יש צורך בעדכונו של הנוהל במקרים של סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר, או לחלופין שינויים מהותיים במערכות המידע או בתהליכי עיבוד המידע.
- ✓ **תקנה 12** - תקנה זו מתייחסת לניהול התקנים ניידים, וקובעת, כי על בעל המאגר להגביל או למנוע אפשרות לחיבור התקנים ניידים למערכות המידע של המאגר, במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד, וקיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. ככל שקיימת לארגון חובה לבצע סקר סיכונים, ויש בבעלותו התקנים ניידים, הרי שסקר הסיכונים צריך לכלול התייחסות גם להוראות תקנה 12 ביחס לניהול התקנים ניידים.
- ✓ **תקנה 15(א)** [3]- בהתאם לתקנה זו, על בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע, לבחון לפני ביצוע ההתקשרות את סיכוני אבטחת המידע הכרוכים בהתקשרות, וכן לקבוע במפורש בהסכם עם הגורם החיצוני, בשים לב לסיכוני אבטחת המידע, בין היתר את המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו, מערכות המאגר שהגורם החיצוני יכול לגשת אליהן וסוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות.

לצורך מילוי החובה הקבועה בתקנה, נדרש אם כן, בעל המאגר לבצע מיפוי של מערכות המאגר, הגדרת המאגר ומיפוי של סיכוני אבטחת המידע הכרוכים בהתקשרות מול ספק מיקור החוץ. ארגון שלא ערך סקר לבחינת הסיכונים המיוחדים להתקשרות עם גורם חיצוני כאמור (שאינו מחליף או גורע מביצוע סקר הסיכונים הכללי למאגר המידע), לא יוכל להבטיח שספקיו לא יסכנו אותו ואת לקוחותיו בהיבטי אבטחת מידע.

בנוסף לחובה לבצע סקר סיכונים, נדרשים בעלי מאגרים שחלה עליהם רמת אבטחה בינונית או גבוהה לבצע **גם ביקורת תקופתית מכוח תקנה 16.** מטרתה של הביקורת התקופתית לוודא, כי הארגון **מקיים את ההוראות החלות עליו,** כנדרש על פי התקנות, ובהתאם למאפיינים הייחודיים של מאגריו. במסגרת הביקורת יש לבחון, בין היתר, מהם אמצעי האבטחה המיושמים, תוך בדיקה האם הם עומדים בנוהל האבטחה ובתנאי התקנות. **יצוין כי בעל מאגר שחלה עליו רמת אבטחה גבוהה רשאי לקיים ביקורת תקופתית במסגרת עריכת סקר סיכונים, בהתאם להוראות תקנה 16(ד).**

[3] בנוסף, ניתן לעיין במדריך פעולה ליישום תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז- 2017 שפרסמה הרשות בשנת 2023: https://www.gov.il/he/pages/guide_section_15.

3. מבדק חדירות

כל ארגון מצוי באופן תמידי תחת איומים וסיכוני אבטחת מידע שעליו לזהות, לנתח ולהעריך. מבדק החדירות נועד לזהות ולנתח, הלכה למעשה, את נקודות החולשה באבטחת המידע הארגונית. באמצעות מבדק החדירות הארגון מדמה מתקפה על נכסי הארגון במטרה לזהות ולנצל נקודות חולשה ולבחון את יעילות הבקרות ומנגנוני הגנה הקיימים.

תקנה 5(ד) לתקנות מורה על ביצוע מבדק חדירות רק במאגרים שחלה עליהם רמת אבטחה גבוהה. התקנה מחייבת ביצוע מבדק חדירות אחת ל-18 חודשים לפחות. ביצוע המבדק לבדו אינו מספיק, ויש לדון ולנתח את ממצאיו במטרה לגבש תכנית עבודה לתיקון הליקויים, כמתחייב מתקנות 5(ג) ו-5(ד) לתקנות.

עוד יצוין, כי פרשנות הרשות ביחס למאגרים שחלה עליהם רמת האבטחה הגבוהה הינה, כי את מבדקי החדירות יש לערוך מיד בסמוך לאחר תחילת הפעלת המאגר, ועם התגבשותם של הסיכונים האמורים, וכן לפחות כל 18 חדשים.

3.1 רמות מבדק חדירות

כאמור, מבדק חדירות מדמה פעולות של תוקף המעוניין לגשת למידע הארגוני באופן בלתי חוקי. מכיוון שגורמים המבצעים את המבדק עשויים לדמות תוקפים בעלי מאפיינים שונים (תוקפים פנים-ארגוניים או חיצוניים לארגון, וכן תוקפים בעלי רמות שונות של ידיעה והיכרות עם הארגון, מערכותיו ובקרותיו), ניתן לבצע את מבדק החדירות ברמות שונות של ידע והכרות עם נכסי הארגון, כמפורט להלן:

- ✓ **מבדק "קופסה לבנה"** – למבצע המבדק נמסר מידע רב אודות הארגון, מערכות המידע שבו, בקרות אבטחת המידע וכיו"ב, על מנת שמבצע המבדק יוכל לתכנן ולעצב את פעולותיו להמשך.
- ✓ **מבדק "קופסה אפורה"** – למבצע המבדק נמסר מידע חלקי אודות הארגון, מערכותיו ובקרות אבטחת המידע. אופיו הדינאמי של מבדק זה, מאפשר לארגון להפעיל שיקול דעת רחב ביחס להיקף המבדק, מהירות ביצועו וביחס לאפשרות להתמקד בנושא ספציפי לבחינה ברשת הארגונית.
- ✓ **מבדק "קופסה שחורה"** – למבצע המבדק לא נמסר כלל מידע אודות הארגון, מערכותיו או בקרות אבטחת המידע. מדובר במבדק אשר מצריך זמן, השקעה ומשאבים רבים.

בהקשר זה יוער כי מבדק חדירות חייב להתבצע תחת הסכמה מוקדמת ומפורשת של האורגנים המוסמכים בארגון.[4] הסכמת הארגון נחוצה לשם אי ביצוע עבירות, בין היתר לפי חוק המחשבים, התשנ"ה-1995, ולשם הגדרת היקף המבדק בהתאם למטרה לשמה נדרש לבצעו.

רצוי לבצע סקרי סיכונים ומבדקי חדירות בתדירות ההולמת את הדינמיקה הטכנולוגית, העסקית והרגולטורית של הארגון, קרי, לאו דווקא אחת ל-18 חודשים, שהיא התדירות המינימאלית המתחייבת על פי התקנות. כך, במקרים בהם ארגון משנה אלמנטים משמעותיים בסביבת המחשוב שלו, מבצע שינוי בפעילות העסקית הכרוך בהטמעת טכנולוגיה חדשה וכיו"ב.

<u>היחס לתסקיר השפעה על הפרטיות</u>

לגישת הרשות, סקר סיכונים ומבדקי חדירות שבוצעו בהתאם לתקנה 5 לתקנות, מעניקים מענה מספק לזיהוי ולטיפול בסיכוני אבטחת המידע הנדרשים גם במסגרת תסקיר השפעה על פרטיות.[5]

4. <u>סיכום</u>

סקר הסיכונים ומבדק החדירות הם שלבים חיוניים ומשמעותיים מבחינה משפטית, עסקית וטכנולוגית לארגון. ביצוע סקר סיכונים ומבדק חדירות נדרשים לא רק מתוך החובה לקיימם על פי התקנות, אלא גם לצורך קידום ושגשוג פעילותו העסקית, ומתן מענה לצרכי לקוחות הארגון בצורה מיטבית.

לבסוף נזכיר כי אי ביצוע סקר סיכונים ומבדק חדירות במאגרי מידע כאשר חלה חובה לעשות כן מכוח תקנות 5(ג) ו-5(ד), מהווה הפרה של תקנות אלו, ועשויה להוביל לפתיחה בהליך אכיפה מנהלי, אשר עשוי להסתיים בהטלת עיצומים כספיים בסכומים משמעותיים (ראו סעיף (9) בטבלה שבתוספת השלישית לחוק הגנת הפרטיות, התשמ"א-1981).

---

[4] ביצוע מבדק חדירות שאינו יזום, ידוע, מוגדר ומוסכם מראש על ידי הארגון, לא יחשב כקיום חובת עריכת מבדק חדירות מצידו של הארגון, וביצועו עשוי להוות, בין היתר, עבירה פלילית ועוולה אזרחית לפי סעיף 4 לחוק המחשבים, התשנ"ה-1995.

[5] להרחבה ראו <u>מדריך לעריכת תסקיר השפעה על הפרטיות (2022)</u>, שפורסם על ידי הרשות להגנת הפרטיות.