<u>תקנה 9(א) לתקנות הגנת הפרטיות (אבטחת מידע) - מהם "אמצעים מקובלים"</u>

טיוטה להערות הציבור

מבוא

תקנה 9(א) לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז- 2017 (להלן: **התקנות**) קובעת כי "בעל מאגר מידע ינקוט **אמצעים מקובלים** בנסיבות העניין ובהתאם לאופי מאגר המידע וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות". לפי תקנה 19 לתקנות חובה זו חלה גם על המחזיק במאגר המידע, ובהתאם לסעיף 23כו(ח) לחוק הגנת הפרטיות, תשמ"א – 1981 (להלן: **החוק**) ניתן להטיל עיצום כספי על בעל שליטה במאגר מידע או על מחזיק אשר מפר אותה, בשיעור הקבוע בפרט 16 לתוספת השלישית לחוק. תקנה 9(א) אינה מגדירה מהם אותם "אמצעים מקובלים".

מטרת מסמך זה היא לפרט מהם האמצעים המקובלים העיקריים לניהול הרשאות גישה, שיש בהם להבטיח שרק גורמים מורשים יוכלו לגשת למידע, ורק בהתאם לרמת הגישה הנדרשת, כנדרש בתקנה 9(א) לתקנות. זאת, בהסתמך על תקנים בינלאומיים, על המקובל בשוק, ובשים לב לסיכונים לאבטחת מידע ולחובות הקבועות לפי התקנות, בהתאם לסיווג המאגרים לרמות אבטחת מידע.

יובהר, כי עשויים להיות אמצעים נוספים לוודא הרשאת גישה מעבר למפורט במסמך זה, אולם הנטל להוכיח כי הם מקובלים ומספקים יהיה על בעל השליטה או המחזיק המבקשים לנקוט בהם לשם קיום דרישות תקנה 9(א). כמו כן, כיוון שהתחום הטכנולוגי הוא תחום שההתפתחויות בו רבות ומהירות, ייתכנו שינויים בנוגע לאמצעים המקובלים בשוק ובהתאם לכך הרשות עשויה לעדכן את המסמך מעת לעת. בכל מקרה, החובה לבחון ולקבוע את אמצעי הגישה למאגר ולמערכות המאגר בהתאם לתקנה 9(א) מוטלת על בעל השליטה במאגר והמחזיק במאגר, בהתאם לאמצעים המקובלים בנסיבות העניין הקונקרטיות ובהתאם לאופי מאגר המידע שבו מדובר וטיבו.

רקע

שיטות אימות זהות לשם גישה למאגר מידע

שיטות אימות זהות משמשות על מנת לוודא כי האדם המבקש גישה למאגר המידע הוא אכן בעל הרשאה כדין, אשר הוסמך על ידי בעל השליטה או המחזיק במאגר המידע לגשת למידע ולבצע בו פעולות. לצורך כך מקובל לחלק את שיטות האימות העיקריות לשלוש קבוצות:

1. **משהו בידיעתך (Something You Know)**: אימות המבוסס על מידע הידוע רק למשתמש. דוגמאות: סיסמה (Password), קוד גישה מספרי קצר PIN (Personal Identification Number). יודגש, כי מספר תעודת הזהות אינו מהווה גורם אימות מספק.
2. **משהו בבעלותך (Something You Have)**: אימות שמבוסס על רכיב פיזי או דיגיטלי מאובטח הנמצא ברשות המשתמש והוא מחזיק בו. דוגמאות: קוד חד-פעמי לטלפון נייד (One Time Password – OTP), אפליקציה לאימות. יש לתת עדיפות לשימוש בגורמי אימות מתקדמים כגון: Passkeys וגורמי אימות המשלבים קריפטוגרפיה, כרטיס חכם (Smart Card) או מכשיר פיזי לאימות גישה למערכות מחשוב.
3. **משהו שאתה (Something You Are)**: אימות שמבוסס על תכונות פיזיולוגיות או התנהגותיות המאפיינות את המשתמש. דוגמאות: טביעת אצבע (Finger Print), זיהוי קול (Voice Recognition), זיהוי דפוסי פעולה של המשתמש (Behavioral Biometrics) או זיהוי פנים (Facial Recognition).

אימות רב-גורמי (Multi-Factor Authentication - MFA)

שימוש במספר שיטות אימות במקביל, על ידי דרישה לאימות של שני גורמים בלתי תלויים לפחות בעת ביצוע גישה, מחזק את ההגנה על מערכות המאגר ועל מאגר המידע. כך תהליך הגישה הופך למסובך יותר עבור תוקפים, ובהתאם פוחת הסיכון לפריצה והשגת גישה לא מורשית למאגר המידע או למערכותיו.

רמות אימות

הרשות מסתמכת, לצורך קביעת רמות האימות הנדרשות לגישה למאגרי מידע, על העקרונות הקבועים בהנחיות המקצועיות של המכון הלאומי לתקנים וטכנולוגיה של ארה"ב (NIST)[1] בכפוף להתאמות הנדרשות לדין הישראלי, לרגישות המידע ולמאפייני הסיכון של מאגרי המידע.

בהתאם למתודולוגיית NIST קיימות שלוש רמות עיקריות של אימות:

1. **רמת אימות 1** (Authenticator Assurance Level 1): רמה זו מספקת **ביטחון בסיסי** לכך שמבקש האימות הוא אכן בעל אמצעי האימות השייך לחשבון המבוקש. רמה זו דורשת אימות חד-שלבי, כאשר הצלחת האימות מחייבת ממבקש האימות להוכיח בעלות ושליטה באמצעי האימות.

[1] NIST SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management, https://csrc.nist.gov/pubs/sp/800/63/b/4/final

עם זאת, במקרים שבהם רגישות המידע במאגר או רמת הסיכון מצדיקים זאת, ניתן ליישם גם ברמה זו אמצעי אימות נוספים, ובכלל זה שימוש באימות רב-שלבי המבוסס על פרוטוקול אימות מאובטח, אף שאינם נדרשים לפי מתודולוגיית NIST ברמת אימות זו.

2. **רמת אימות 2** (Authenticator Assurance Level 2): רמה זו מספקת **ביטחון גבוה** בכך שמבקש האימות הוא אכן בעל אמצעי אימות אחד או יותר השייך לחשבון המבוקש. על מבקש האימות להוכיח בעלות ושליטה בשני גורמי אימות שונים (אימות רב- גורמי) בנוסף כדי לעמוד בדרישות רמה זו, אמצעי האימות חייב להיות מוגן מפני התחזות (Phishing-Resistant Authentication).

יובהר, כי אימות מוגן מפני התחזות הוא תנאי נוסף לרמה זו, ומשמעותו שחיבור אמצעי האימות לחשבון מבוצע באמצעות פרוטוקול מאובטח שאינו מאפשר לתוקף להשתמש בתוצר האימות (Authenticator output) באתר מתחזה, או להעבירו לשימוש צד שלישי.

3. **רמת אימות 3** (Authenticator Assurance Level 3): רמה זו מספקת **ביטחון גבוה מאוד** בכך שמבקש האימות הוא אכן בעל אמצעי אימות אחד או יותר השייך לחשבון המבוקש. על מבקש האימות להוכיח בעלות **ושליטה בשני גורמי אימות** שונים (אימות רב- גורמי), באמצעות פרוטוקול קריפטוגרפי מבוסס מפתח ציבורי שאינו ניתן לייצוא. אמצעי האימות חייב להיות מוגן מפני התחזות (Phishing-Resistant Authentication), כלומר האימות יבוצע באמצעות אמצעי קריפטוגרפי שאינו ניתן לייצוא ואינו מאפשר עקיפת הזיהוי או שימוש בידי גורם מתחזה במסגרת מתקפת Phishing לרבות בזמן אמת.

הדרישות לפי רמת אימות

עוד מגדיר המכון הלאומי לתקנים וטכנולוגיה של ארה״ב (NIST) את הדרישות לאופן האימות, ולפרק הזמן לאימות מחדש, בחלוקה לפי רמת אימות. מצורפת טבלת הדרישות האמורות.
דרישות נוספות לרמות אימות (ביניהן חסינות לתקיפות מסוגים שונים, תיעוד ובקרה) – מפורטות בתקן NIST. כמו כן, פירוט של אופני האימות (כגון רכיבי תוכנה, OTP ורכיבים מוצפנים) – מפורטים בתקן NIST.

רמת אימות	רמת אימות 1	רמת אימות 2	רמת אימות 3
אופן האימות	1. סיסמה 2. סוד נבדק (Look-up secret)[2] 3. רכיב מחוץ לרשת 4. רכיב OTP חד שלבי 5. תוכנה או רכיב קריפטוגרפי מוצפן חד שלבי[3]	1. רכיב OTP רב- גורמי 2. תוכנה או רכיב קריפטוגרפי מוצפן רב- גורמי 3. רכיב חוץ רשתי רב- גורמי 4. סיסמה או השוואה ביומטרית[4] **בצירוף אחד מתוך:** • סוד נבדק (Look-up secret) • רכיב מחוץ לרשת • רכיב OTP חד שלבי • תוכנה או רכיב קריפטוגרפי מוצפן חד שלבי	1. רכיב קריפטוגרפי מוצפן רב- גורמי 2. רכיב קריפטוגרפי מוצפן חד שלבי **בצירוף אחד מהשניים:** • סיסמה • השוואה ביומטרית
אימות מחדש	30 יום	12 שעות או שעה של חוסר פעולה; ניתן להזין אמצעי אימות אחד	12 שעות או 15 דקות של חוסר פעולה
הגנה מפני התחזות (Phishing Resistance)	לא נדרש	אין חובה ליישם, אך צריכה להיות אפשרות להפעיל במידת הצורך	חובה

[2] מנגנון אימות שבו השרת שומר רק ערך גיבוב (Hash) חד-כיווני של הסיסמה, והמשתמש מוכיח החזקה בסיסמה מבלי לחשוף אותה.

[3] אמצעי אימות המבוסס על הצפנה או חתימה קריפטוגרפית, שבו עצם ההחזקה ברכיב (ללא סיסמה או גורם נוסף) מספיקה לביצוע האימות.

[4] השוואה ביומטרית יכולה לכלול **טביעת אצבע, זיהוי פנים, זיהוי קול או כל מאפיין ביומטרי אחר,** אך **רק כאשר ההשוואה הביומטרית משמשת כגורם נוסף לאופן ביצוע האימות,** ולא כאמצעי יחיד.

יובהר כי המסמך הנוכחי מוסיף על האמור במסמכי ה"מדיניות הלאומית להזדהות בטוחה" שפורסמו על ידי היחידה להזדהות וליישומים ביומטריים במערך הסייבר הלאומי,[5] ואינו גורע מהם. מטרות המסמכים אינן זהות. מסמכי המדיניות הלאומית להזדהות בטוחה מתמקדים בקביעת קווים מנחים לביצוע הזדהות דיגיטלית של משתמש לצורך קבלת שירות מקוון, בהתאם לסיכון ולרגישות השירות. המסמך הנוכחי, לעומת זאת, עניינו באמצעים המקובלים שיש לנקוט לפי תקנה 9(א) לתקנות, כדי לוודא שגישה למאגר מידע ולמערכות המאגר תיעשה בידי בעל הרשאה המורשה לכך בלבד, בהתאם לרמת האבטחה החלה על המאגר לפי התקנות.

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017

התקנות מגדירות ארבע רמות אבטחה של מאגרי מידע: מאגר המנוהל בידי יחיד, מאגר מידע ברמת אבטחה בסיסית, מאגר מידע ברמת אבטחה בינונית, ומאגר מידע ברמת אבטחה גבוהה. בהתאם לכך, יש להתאים בין רמת האבטחה החלה על מאגר המידע לפי התקנות והסיכונים של פגיעה באבטחת המידע, לבין רמת האימות הנדרשת.

הטבלה מטה מציגה "אמצעים מקובלים" כדי לוודא כי הגישה למאגר המידע ולמערכות המאגר נעשית בידי בעל הרשאה מורשה, בשים לב לרמת האבטחה החלה על המאגר לפי התקנות, לסיכוני הפגיעה באבטחת המידע הקיים במאגר ובמערכות המאגר, ולסוג וזהות הגורם שניגש למאגר.
כמו כן, הטבלה לוקחת בחשבון את המעטפת הכוללת של אבטחת המידע החלה על כל מאגר מידע, אשר באה לידי ביטוי בתקנות החלות על כל רמת אבטחה.

להגברת ההגנה על מאגרי המידע, ניתן תמיד לקבוע אמצעים מחמירים יותר על המפורט בטבלה, גם כאשר מדובר במאגר מידע המנוהל בידי יחיד או במאגר מידע ברמת אבטחה בסיסית או בינונית.

רמת אבטחה	גורם	רמת אימות	אורך סיסמה	החלפת סיסמה	זיהוי רב-גורמי
מנוהל בידי יחיד	בעל הרשאה בארגון	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי
	בעל הרשאה	רמת	15 תווים או	6	אופציונלי

[5] https://www.gov.il/he/pages/national_policy_for_secure_identification

	בארגון בגישה מחוץ לארגון	אימות 1	8 תווים בצירוף אמצעי זיהוי נוסף	חודשים	
	לקוח בגישה מחוץ לארגון	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי
	מנהל מאגר/Admin	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי
רמת אבטחה בסיסית	בעל הרשאה בארגון	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי
	בעל הרשאה בארגון בגישה מחוץ לארגון	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי
	לקוח בגישה מחוץ לארגון	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי
	מנהל מאגר/Admin	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי

רמת אבטחה בינונית	בעל הרשאה בארגון	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי
	בעל הרשאה בארגון בגישה מחוץ לארגון	רמת אימות 2	בין 8 ל-15 תווים	6 חודשים	נדרש
	לקוח בגישה מחוץ לארגון	רמת אימות 2	בין 8 ל-15 תווים	6 חודשים	נדרש
	מנהל מאגר/Admin	רמת אימות 2	בין 8 ל-15 תווים	6 חודשים	נדרש
רמת אבטחה גבוהה	בעל הרשאה בארגון	רמת אימות 1	15 תווים או 8 תווים בצירוף אמצעי זיהוי נוסף	6 חודשים	אופציונלי
	בעל הרשאה בארגון בגישה מחוץ לארגון	רמת אימות 3	בין 8 ל-15 תווים	6 חודשים	נדרש
	לקוח בגישה מחוץ לארגון	רמת אימות 2	בין 8 ל-15 תווים	6 חודשים	נדרש
	מנהל מאגר/Admin	רמת אימות 3	בין 8 ל-15 תווים	6 חודשים	נדרש