



תאריך: 10 בינואר 2010
כ"ד בטבת התש"ע

נייר עמדה בנושא תקנות אבטחת מידע להגנת פרטיות

והזמנה ליום עיון בנושא

הרשות למשפט טכנולוגיה ומידע (להלן - הרשות) מפרסמת בזאת להערות הציבור נייר עמדה מטעמה ובו הסדר מוצע בתחום חובות אבטחת מידע על בעל מאגר ומחזיק לפי חוק הגנת הפרטיות, התשמ"א-1981 (להלן - החוק), לקראת יום עיון בנושא "אבטחת מידע בהקשר של הגנת הפרטיות במאגרי מידע".

יום העיון נערך בשיתוף פעולה עם רשות הגנת המידע הספרדית (AEPD) במסגרת תוכנית ה-twinning המתקיימת עמה, ובו יוצגו גם הגישות של נציב הגנת המידע האישי הספרדי והבריטי בנושא זה. עוד תשתתף ביום העיון נציגה בכירה של איגוד מבקרי המידע הספרדי. ביום העיון יוצג גם נייר עמדה זה, וייערך בו דיון לאור דברי האורחים מחו"ל.

יום העיון ייערך בקריית הממשלה ב- 20.01.2010 בקריית הממשלה, רח' בגין 125, תל-אביב בחדר 101 בשעות 09:00-13:30. לרישום ליום העיון יש להרשם בשליחת דוא"ל עם פרטי הנרשם (שם), תואר תפקיד, ארגון) ל- twinning@justice.gov.il מספר המקומות מוגבל!

נייר העמדה מצ"ב, וניתן להורדה גם בכתובת הבאה –

<http://www.justice.gov.il/MOJHeb/RashutTech/TwinningProject/Iruim/takanot+avtachat+meida.htm>

הערות לנייר העמדה ניתן להעביר לרשות עד יום 15.2.2010 לדוא"ל -

ilita@justice.gov.il

אודות נייר העמדה

נייר העמדה מופץ לציבור בשלב זה על מנת להניע דיון בנושא זה, במסגרת תוכנית העבודה של הרשות, וכחלק ממהלך הסדרה מקיף יותר של תחום זה. הפצתו כעת נעשית לצורך קבלת הערות

Government Campus, 9th floor
125 Begin Road
P. O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קריית הממשלה, קומה 9
ד ר ך ב ג י ן 1 2 5
ת . ד . 7 3 6 0
ת ל א ב י ב 6 1 0 7 2
ט ל ' : 0 3 - 7 6 3 4 0 5 0
פ ק ס : 0 2 - 6 4 6 7 0 6 4



מקדמיות של בעלי עניין לקראת עיון ודיון מול מחלקת ייעוץ וחקיקה במשרד המשפטים, האמונה על החקיקה וחקיקת המשנה בתחום הגנת הפרטיות.

כידוע, הוראות בתחום אבטחת המידע משמשות אדן מרכזי עליו מבוססת ההסדרה בתחום פרטיות במאגרי המידע, משום שהוראות אלה מביאות לצמצום החשש מפני שימוש לרעה או פגיעה במידע.

מטרת נייר העמדה לפרט ולקבוע את עקרונות אבטחת המידע הקשורים בעיבוד מידע אישי במאגרי מידע, בהתבסס על תקנים מקובלים. מטרת יישום העקרונות בהקשר של מאגרי מידע נועד לסייע במימוש תכליות החוק - כלומר הגנה על זכויות נושאי המידע במאגר המידע, מפני שימוש לרעה הפוגע בפרטיותם. עם זאת, ניתן להניח כי עמידה בעקרונות המוצעים תבטיח כי התנהלות הארגון בתחום המידע באופן כללי תהיה תקינה.

נייר העמדה מציע מנגנונים וכלים פנים ארגונים, שמטרתם הפיכת אבטחת המידע במאגר, לחלק משגרת ניהול המידע בפרט וניהול הארגון בכלל. מטרת המנגנונים לכוון באופן מוחשי וברור יותר לחובותיהם ואחריותם בתחום אבטחת המידע. בשל כך נדרש כי הארגון יקבע נהלים בתחום אבטחת המידע, שיסדירו בצורה מפורטת וברורה יותר היבטים אלה. החובה לקבוע מסמכים המפרטים את הנהלים נגזרת מעקרונות יסוד של אבטחת מידע ושל ניהול תקין, ומאפשרות הנחלה של עקרונות ההתנהלות בתוך הארגון.

בנוסף, הנהלים יאפשרו לארגון גם להציג לצדדים שלישיים – לקוחותיו, ספקיו, בתי משפט ורשם מאגרי מידע את אופן פעולתו ואופן התמודדותו עם חובותיו לפי החוק. כך, בעת אירוע שמהווה פגיעה בפרטיות במאגר מידע, מצבו של ארגון שנקט באמצעים סבירים למנוע את התרחשות הפגיעה, יהיה שונה מארגון שלא נקט אמצעים סבירים כאלה.

בשל מגוון הארגונים המעבדים מידע אישי, נייר העמדה הוא מודלורי, בכך שהוא מחיל חובות ברמה עולה וגדלה ככל שהארגון הוא ארגון שפעילות עיבוד המידע שבו, בהקשר החוק, הינה משמעותית יותר. תפיסה זו, של חובות מודלוריות נגזרת ישירות מעקרונות יסוד של אבטחת מידע ומוצאת ביטוייה גם במסמכים דומים בעולם.

המסמך חובר על ידי עו"ד יצחק גורדון מהמחלקה המשפטית ברשות, בעזרתם של המתמחים מורן בר, אדם שלשבסקי ויוסי טהר ובהנחיית עו"ד עמית אשכנזי, היועץ המשפטי של הרשות.

בברכה,

יורם הכהן, עו"ד
ראש הרשות למשפט, טכנולוגיה ומידע

Ministry of Justice
The Israeli Law, Information &
Technology Authority (ILITA)



מדינת ישראל
State of Israel

משרד המשפטים
הרשות למשפט, טכנולוגיה ומידע

נייר עמדה בנושא

תקנות אבטחת מידע להגנת

פרטיות במאגרי מידע

כ"ד בטבת התש"ע
10 בינואר 2010

Government Campus, 9th floor
125 Begin Road
P. O. Box 7360
Tel Aviv 61072
Tel.: +972-3-7634050
Fax: +972-2-6467064

Email: ILITA@justice.gov.il
Web: ILITA.justice.gov.il

קרית הממשלה, קומה 9
דרך בגין 125
ת.ד. 7360
תל אביב 61072
טל': 03-7634050
פקס: 02-6467064

להערות הציבור

מבוא

חוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק), קובע הוראות שונות וחובות המוטלות על בעל מאגר, מחזיק במאגר ומנהל מאגר. אחת החובות המרכזיות היא חובת אבטחת המידע, שמטרתה צמצום החשש מפני שימוש לרעה או פגיעה במידע. סעיף 17 לחוק הגנת הפרטיות קובע כי:

"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע."

ואילו "אבטחת מידע" מוגדרת בסעיף 3 לחוק באופן הבא:

"הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין;"

מטרת התקנות המוצעות לפרט ולקבוע את עקרונות אבטחת המידע הקשורים בניהול ובשימוש במידע במאגרי מידע, בהתבסס על תקני אבטחת מידע מקובלים בעולם*. בשונה מאבטחת מידע באופן כללי, שמטרתה להגן על המידע של ארגון כנכס של אותו ארגון, המטרה של ההסדר המוצע הוא מימוש תכליות החוק - כלומר הגנה על זכויות נושאי המידע במאגר המידע, מפני שימוש לרעה במידע אודותיהם. יחד עם זאת, ניתן לומר כי עמידה בעקרונות המוצעים בתקנות אלה, תבטיח כי ניהול המידע בארגון באופן כללי - יהיה תקין. התקנות מבקשות לקבוע מנגנונים וכלים פנים-ארגוניים, שמטרתם הפיכת אבטחת המידע במאגר המידע, בהתאם למאפייני המאגר, לחלק משגרת ניהול המידע בפרט וניהול הארגון בכלל. מטרת המנגנונים להמחיש בצורה ברורה יותר את חובותיהם ואחריותם של ארגונים בתחום אבטחת המידע.

המנגנונים המוצעים נחלקים למספר רבדים: ברובד הראשון נדרש בעל המאגר לקבוע מהו המידע המוגן ומהם הסיכונים הקשורים אליו. ברובד השני, נדרש הארגון לייעד נושא משרה בארגון שאבטחת המידע היא חלק מתפקידו, ועליו להיות אחראי בתוך הארגון על כך. תובנה מקובלת בתחום אבטחת המידע הינה כי:

"מערכות מידע רבות לא נועדו מלכתחילה להיות בטוחות. האבטחה שניתן להשיג באמצעים טכניים היא מוגבלת, והיא זקוקה לתמיכה הולמת של ניהול ונהלים. זיהוי אמצעי הבקרה המתאימים דורש תכנון זהיר ושימת לב לפרטים. ניהול אבטחת המידע בארגון נזקק קודם כל לשיתוף פעולה של כל העובדים. לפעמים יש גם צורך בשיתוף פעולה של ספקים, לקוחות או בעלי מניות, ואף בייעוץ של מומחים שמחוץ לארגון. הכללת אמצעי הבקרה לאבטחת המידע בשלב הגדרות הדרישות והתוכן, תהיה באופן משמעותי זולה יותר ואפקטיבית יותר לעומת הכללתם בשלב מאוחר יותר." [ת"י 7799, מבוא, עמ' 2]

בשל כך נדרש כי הארגון יקבע נהלים בתחום אבטחת המידע, שיסדירו בצורה מפורטת וברורה יותר את ההיבטים האלה. החובה לקבוע מסמכים המפרטים את הנהלים נגזרת מעקרונות יסוד של אבטחת מידע ושל ניהול תקין, ומאפשרת הנחלה של עקרונות אלה בתוך הארגון.

* יצוין כי כיום קיימים כבר הסדרים בנושא אבטחת מידע בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו – 1986 (להלן – התקנות הקיימות), אך מדובר בהסדרים המחייבים עדכון. לפיכך, בהמשך הדרך, כאשר טיוטת התקנות הנוכחית תבשיל לקראת הפיכתה לתקנות פורמליות, יהיה צורך גם בעריכת תיקונים בתקנות הקיימות, ובכלל זה ביטול של הוראות שיוחלפו בהוראות חדשות במסגרת התקנות המוצעות. בנוסף לכך תידרש התאמה של הוראות תחילה לתקנות, שיאפשרו תקופת היערכות מתאימה להוראות השונות של התקנות.

להערות הציבור

בנוסף, הנהלים מאפשרים לארגון גם להציג לצדדים שלישיים – לקוחותיו, ספקיו, בתי משפט, רשם מאגרי המידע ורגולטורים אחרים, את אופן פעולתו ואופן התמודדותו עם חובותיו לפי החוק. כך, בעת אירוע שמהווה פגיעה בפרטיות במאגר מידע, מצבו של ארגון שנקט באמצעים סבירים למנוע את התרחשות הפגיעה, יהיה שונה מארגון שלא נקט אמצעים סבירים כאלה.

בשל מגוון הארגונים המעבדים מידע אישי, התקנות המוצעות הן מודולריות, בכך שהן מחילות חובות ברמה הולכת וגדלה ככל שהארגון הוא ארגון שפעילות עיבוד המידע שבו, בהקשר של חוק הגנת הפרטיות, היא משמעותית יותר. תפיסה זו, של חובות מודולריות נגזרת ישירות מעקרון היסוד של אבטחת מידע שלפיה התמודדות עם סיכוני האבטחה נבחנת בהתאם לפעילות של המאגר, והיא מוצאת ביטויה גם במסמכים דומים בעולם.

נוסח מוצע לתקנות מכוח חוק הגנת הפרטיות, התשמ"א-1981

לעניין אבטחת מידע במאגרי מידע

הגדרות

1. בתקנות אלה -

"אחראי האבטחה" – מנהל המאגר כהגדרתו בסעיף 7 לחוק הגנת הפרטיות,

התשמ"א-1981¹ (להלן – החוק), ואם מונה ממונה על אבטחת מידע כאמור בסעיף 17 לחוק – גם הממונה;

"חומר מחשב", "מחשב" ו"פלט" – כהגדרתם בחוק המחשבים, התשנ"ה-1995².

"עובד" -

(1) ביחס לבעל מאגר - לרבות יחיד המבצע פעולות בקשר למאגר מטעמו של בעל המאגר ועל פי הרשאתו, ולמעט עובד של מחזיק;

(2) ביחס למחזיק - לרבות יחיד המבצע פעולות בקשר למאגר מטעמו של המחזיק ועל פי הרשאתו;

"התקן נייד" - מחשב נייד או התקן נתיק המשמש לאחסון חומר מחשב;

"מאגרים שחלה עליהם רמת האבטחה הבינונית" - מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה;

"מאגרים שחלה עליהם רמת האבטחה הגבוהה" - מאגרי מידע מן הסוגים המפורטים בתוספת השנייה;

¹ ס"ח התשמ"א, עמ' 128.

² ס"ח התשנ"ה, עמ' 366.

להערות הציבור

"תקן ישראלי" - כמשמעותו בחוק התקנים, התשי"ג-1953.³

2. אחריות כוללת
לאבטחת המידע
במאגר
- (א) בעל מאגר יגדיר במסמך המחייב גם את עובדי המאגר (להלן – הגדרות המאגר), לכל הפחות, את כל העניינים האלה:

(1) תיאור של סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 1(3) לתוספת הראשונה, וכן הערכת הרגישות של כל סוג מידע;

(2) המטרות המותרות של השימוש במידע שבמאגר;

(3) פירוט לעניין העברת מידע מהמאגר מחוץ לגבולות המדינה-ארץ היעד, מטרת ההעברה וזהות הנעבר;

(4) פירוט לעניין ביצוע פעולות עיבוד מידע באמצעות מחזיק;

(5) הסיכונים המרכזיים לפגיעה בשלמות המידע, חשיפתו או שימוש בו שלא כדין, ואופן ההתמודדות איתם.

(ב) בעל מאגר -

(1) יעדכן את הגדרות המאגר בכל שינוי שחל במאגר, הנוגע לעניינים המנויים בתקנת משנה (א) או לעניינים אחרים שהוא כבר כלל בהגדרות המאגר;

(2) יבחן אחת לשנה לפחות, אם יש צורך בעדכון הגדרות המאגר, כאמור בפסקה (1).

(ג) על מנת להפחית את סיכוני אבטחת המידע למידע שבמאגר, יבחן בעל המאגר לפני הקמת מאגר המידע ולכל אורך פעילותו של מאגר המידע, כי המידע הנאסף והנשמר על ידו אינו מעבר לנדרש לצורך מימוש מטרות המאגר.

(ד) בעל מאגר יתכנן, ככל הניתן מראש, את פעילות המאגר ואת מערכותיו באופן שיפחית את סיכוני אבטחת המידע למידע שבמאגר.

3. ממונה על אבטחת
מידע
- (א) בלי לגרוע מהוראות תקנה 2, מונה ממונה על אבטחת מידע במאגר המידע (להלן – ממונה על אבטחה), יהיה הממונה אחראי על אבטחת המידע במאגר.

³ ס"ח התשי"ג, עמ' 30.

להערות הציבור

(ב) זהות הממונה על אבטחה, סמכויותיו ותפקידיו יוגדרו בצורה ברורה על ידי בעל המאגר.

(ג) הממונה על אבטחה יהיה כפוף ישירות לבעל המאגר.

(ד) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה.

נוהל אבטחה 4. (א) אחראי האבטחה יערוך נוהל אבטחת מידע (להלן – נוהל האבטחה) בהתאם לתקנות אלה ובהתאם להגדרות המאגר, ועל בסיס סקר הסיכונים השנתי, ככל שנערך כזה.

(ב) נוהל האבטחה יחייב את כל העובדים שיש להם גישה למערכות המחשוב של המאגר, או לכל מידע או רכיב הנדרש לצורך הפעלת המאגר או לצורך גישה אליו כאמור בתקנה 5(א)(5).

(ג) נוהל האבטחה יכלול, בין היתר, התייחסות לכל אלה:

(1) תיאור של רכיבי המערכות כאמור בתקנה 5(א) ותיאור מבנה הרשת שבה פועל המאגר;

(2) קביעת הרשאות גישה למידע במאגר בהתאם לתקנה 8;

(3) הוראות למורשי הגישה למאגר המידע לצורך שמירה על אבטחת המידע במאגר בעת השימוש בו.

(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול נוהל האבטחה, בנוסף לאמור בתקנת משנה (ג), התייחסות גם לכל אלה:

(1) הוראות בעניין האבטחה הפיזית והסביבתית של מתקני המאגר כאמור בתקנה 6;

(2) אופן הבקרה על השימוש במאגר המידע, ובכלל זה רישום של הגישה למערכות המחשוב של המאגר;

(3) הוראות לעניין אבטחת מערכות התקשורת אל מערכות המאגר וממנו;

(4) הוראות לעניין ניהול והעברה של אמצעי אחסון והתקנים ניידים;

(5) הוראות לעניין אופן גיבוי המידע ושחזורו;

להערות הציבור

(6) הוראות לעניין ביצוע ביקורות תקופתיות כדי לוודא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה.

(ה) נוהל האבטחה יהיה עדכני בכל עת, וייבחן מחדש בכל פעם שמתבצעים שינויים מהותיים במערכות המאגר או ככל שיש בכך צורך כתוצאה מהביקורת התקופתית.

(א) בעל מאגר יערוך רשימת מצאי של מכלול רכיבי המערכות המשמשות את המאגר (להלן – מערכות המאגר), ובכלל זה -

מיפוי וביצוע סקר .5
סיכונים

(1) מערכות חומרה, רכיבי תקשורת, לרבות ציון של מיקומם הפיזי;

(2) התקנים ניידים, לרבות ציון זהות האדם העושה בהם שימוש;

(3) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ותחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;

(4) תוכנות המשמשות לתקשורת אל מערכות המאגר ומהן;

(5) כל מידע או רכיב אחר הנדרש לצורך הפעלת המאגר או לצורך גישה אליו, ושיש לו חשיבות מבחינת אבטחת מידע.

(ב) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכונים אבטחת מידע (להלן - סקר סיכונים); תוצאות סקר הסיכונים יועבר לאחראי האבטחה ולבעל המאגר, אשר ידונו בהם ויבחנו את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעלו לתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו.

(ג) רשימת מצאי וסקר סיכונים כאמור בתקנה זו, לפי העניין, ייערכו מדי שנה עד יום 31 בדצמבר.

(א) אחראי האבטחה יבטיח כי המערכות המפורטות בתקנה 5(א) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו.

אבטחה פיזית
וסביבתית .6

(ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - ינקוט אחראי האבטחה אמצעים סבירים לבקרה ולתיעוד של הגישה לאתרים שבהם מצויות מערכות המאגר (בתקנות אלה – מתקני המאגר), של הגישות שבוצעו בפועל, ושל הכנסה והוצאה של ציוד אל מתקני המאגר ומהם.

להערות הציבור

7. אבטחת מידע
בניהול כח אדם

(א) קליטת עובדים למשרות המחייבות שימוש במידע ממאגר המידע, תיעשה תוך נקיטת אמצעים סבירים לבירור כי אין חשש להתאמתם לגישה למידע; אמצעים אלה יינקטו בשים לב לרגישות המידע שבמאגר ולהיקף הרשאות הגישה לתפקידים שאליהם מיועדים העובדים הנוגעים בדבר, כאמור בתקנה 8.

(ב) בעל מאגר יפעל להדרכת עובדים כאמור בתקנת משנה (א), לקיום החובות לפי תקנות אלה, בטרם יקבלו גישה למידע ממאגר המידע.

(ג) עובדים כאמור בתקנת משנה (א) יחתמו בטרם קבלת גישה למידע ממאגר המידע על התחייבות לשמור על סודיות בנוגע למידע שבמאגר בהתאם להוראות סעיף 16 לחוק, ועל התחייבות לקיים את החובות לפי תקנות אלה.

(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - יקיים בעל המאגר פעילות הדרכה תקופתית, בדבר הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, ובדבר חובות העובדים לפיהם.

8. ניהול הרשאות
גישה

(א) הרשאות הגישה של עובדים למאגר המידע ייקבעו על בסיס הגדרת תפקיד; הרשאת הגישה לכל תפקיד תהיה בהיקף ובמידה הנדרשים לביצוע התפקיד בלבד.

(ב) אחראי האבטחה ינהל רישום מעודכן של תפקידים, הרשאות הגישה שנקבעו להם, ועובדים הממלאים תפקידים אלה (להלן – רשימת ההרשאות התקפות).

(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יתקיימו גם כל אלה:

(1) מידור הגישה לחלקים רגישים של מערכות המאגר, ובכלל זה מערכות האחסון של המידע ומנגנוני התיעוד לפי תקנות 10 ו-11, כך שלעובד יחיד לא תהא גישה לכל החלקים הרגישים, אלא אם כן הדבר חיוני לפעילותו של בעל המאגר;

(2) ביצוע פעולות חיוניות לא יהא בשליטתו של עובד אחד בלבד; לעניין זה, קביעת ההרשאות כאמור בתקנת משנה (א) ואפשרות העתקתו של כלל מאגר המידע או חלק מהותי ממנו, ייחשבו כפעולה חיונית.

להערות הציבור

9. זיהוי ואימות (א) במאגר המידע יופעלו אמצעים לוידוא כי הגישה למידע במאגר המידע נעשית רק בידי עובד המורשה לכך ובהתאם לרשימת ההרשאות התקפות.
- (ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, אם האמצעים כאמור בתקנת משנה (א) מבוססים על שימוש בסיסמאות, יקבע נוהל האבטחה הוראות לעניין אורך הסיסמה, מספר הניסיונות השגויים, אופן הטיפול בתקלות ובאימות זהות, ותדירות החלפת הסיסמאות שתיקבע בהתאם לתפקיד של מורשה הגישה, ובכל מקרה לא תעלה על ששה חודשים.
- (ג) אחראי האבטחה ידאג לביטול ההרשאות של עובד שסיים את תפקידו ולשינוי ססמאות וקודי גישה למאגר, שהעובד עשוי היה לדעת, מיד עם סיום תפקידו של העובד.
10. תיעוד גישה (א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה ינוהל מנגנון תיעוד אוטומטי שיתעד כל ניסיון גישה למערכות המאגר (בתקנה זו – מנגנון התיעוד), ובכלל זה את כל הנתונים האלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה והאם הגישה אושרה או נדחתה; אם הגישה אושרה, יישמרו הנתונים המאפשרים זיהוי רכיב המערכת שאליו בוצעה הגישה.
- (ב) מנגנון התיעוד לא יאפשר ביטול או שינוי של הפעלתו.
- (ג) מנגנון התיעוד יהיה נתון לשליטתו הישירה של אחראי האבטחה, והוא יבחן פעם בחודש לפחות את נתוני התיעוד, ויערוך דו"ח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.
- (ד) נתוני הרישום של מנגנון התיעוד יישמרו למשך 24 חודשים לפחות.
- (ה) אחראי האבטחה יידע את העובדים במאגר בדבר קיומו של מנגנון תיעוד המתעד את ניסיונות הגישה למערכות המאגר.
11. תיעוד של אירועי אבטחה (א) אחראי האבטחה אחראי לתיעוד אירועים המעלים חשש לפגיעה בשלמות המידע או לשימוש בו בלא הרשאה (להלן - אירועי אבטחה); ככל הניתן יבוסס התיעוד האמור על רישום אוטומטי.
- (ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יוגדרו בנוהל האבטחה הוראות לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

להערות הציבור

(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ידון בעל המאגר באירועי האבטחה ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהם.

(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור בתקנת משנה (ג) אחת לרבעון לפחות.

(א) העתקה של מידע מהמאגר על גבי התקנים ניידים תיעשה באופן המונע שימוש לרעה בהם, ותוך נקיטת אמצעי הגנה סבירים ומקובלים; לעניין זה, שימוש תקין בשיטות הצפנה מקובלות ייחשב כנקיטת אמצעים סבירים.

12. ניהול והעברה של מסמכים והתקנים ניידים

(ב) התקנים ניידים שמאוחסן בהם מידע מהמאגר, יישאו על גביהם כתובת בולטת לעין: "מידע מוגן לפי חוק הגנת הפרטיות".

(ג) פלט של מידע מהמאגר יופק בלווית כתובת בולטת לעין בכל עמוד: "מכיל מידע מוגן לפי חוק הגנת הפרטיות".

(ד) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יערוך אחראי האבטחה רשימת מצאי של התקנים ניידים המכילים מידע ממאגר המידע, באופן שיאפשר מעקב אחר מיקומם בכל עת, ויקיים מנגנון לתיעוד ולמעקב אחר משלוחים נכנסים ויוצאים של התקנים ניידים; חשש לגישה לא מורשית להתקן נייד או לפגיעה בו, לרבות אובדנו, ייחשב אירוע אבטחה ויחולו לגביו הוראות תקנה 11.

(ה) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, שמירת מידע בהתקנים ניידים, הוצאת התקנים ניידים המכילים מידע מחוץ למתקני המאגר, או עיבוד מידע מחוץ למתקני המאגר, ייעשו רק באישור מראש של אחראי האבטחה, אשר יקבע את רמת האבטחה הנדרשת במצבים אלו.

(ו) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יתויג המידע שבמאגר באמצעים טכנולוגיים המאפשרים מעקב אחר העתקה של מידע מהמאגר ואחר השימוש שנעשה בו.

(א) בעל המאגר יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר.

13. אבטחת תקשורת וניהול מאובטח של מערכות המאגר

להערות הציבור

(ב) מערכות המאגר לא יחוברו לרשת האינטרנט או לרשת ציבורית אחרת ללא התקנת אמצעי הגנה סבירים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

(ג) העברת מידע ממאגר המידע ברשת תקשורת אלחוטית, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש באמצעי הצפנה.

(ד) במאגר מידע שניתן לגשת אליו מרחוק באמצעות רשת תקשורת, בנוסף לאמצעי אבטחה כאמור בתקנות משנה (ב) ו-(ג), יש לעשות שימוש באמצעי זיהוי ואימות המאפשרים לזהות באופן סביר את זהות המתקשר ולאמת את ההרשאה שלו לביצוע הפעילות מרחוק ואת היקף ההרשאה.

(ה) אחראי האבטחה ידאג לכך שיתבצעו עדכונים שוטפים של המערכות והתוכנות המשמשות להגנה על המידע במאגר המידע, לרבות חומר המחשב הנדרש לפעולתן.

(א) בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירותי עיבוד של המידע שבמאגר המידע, כולו או חלקו, או שירות אחר הכרוך במתן גישה למאגר המידע (להלן - השירות) -

מיקור חוץ

.14

(1) יבחן לפני ביצוע ההתקשרות כאמור, בשים לב לסיכוני אבטחת המידע הכרוכים בהתקשרות, האם מוצדק לבצע את השירות באמצעות גורם חיצוני בכלל ובאמצעות הגורם המסוים בפרט;

(2) יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה:

(א) המידע שרשאי הגורם החיצוני לעבד;

(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;

(ג) סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;

(ד) משך תוקפה של ההתקשרות;

(ה) החובות בתחום אבטחת המידע החלות על הגורם החיצוני לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל המאגר, ככל שקבע;

להערות הציבור

(ו) חובתו של הגורם החיצוני להחתים את עובדיו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לצורך העיבוד המותר בחוזה וליישם את אמצעי האבטחה הקבועים בהסכם, כאמור בפסקת משנה (ה);

(ז) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - סמכותו של בעל המאגר לפקח על פעילותו של הגורם החיצוני כאמור בפסקה (4).

(3) ירשום בנוהל האבטחה של המאגר את העניינים המנויים בפסקה (2)(א) עד (ה), וכן יפנה בצורה מפורשת להסכם ולנוהל האבטחה של הגורם החיצוני כאמור בתקנת משנה (ב).

(4) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה - ינקוט אמצעי בקרה ופיקוח כדי לוודא את עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה.

(ב) גורם חיצוני שהתקשר עם בעל מאגר כאמור בתקנת משנה (א), יחולו עליו הוראות תקנות אלה והוא יערוך נוהל אבטחה כאמור בתקנה 4, בשינויים המחויבים, וירשום בו גם את עניינים המנויים בתקנת משנה (א)(2)(א) עד (ז) ואת זהותו של בעל המאגר.

15. מחיקת מידע מהמאגר (א) מידע המצוי במאגר מידע שכבר אין בו צורך לתפעולו השוטף של המאגר, יימחק אלא אם קיים צורך על פי דין לשומרו לצרכי גיבוי; גיבוי כאמור יישמר בנפרד באופן שיפחית את סיכוני אבטחת המידע לשימוש לא מורשה בו.

(ב) כל אמצעי אחסון המכיל מידע המיועד למחיקה - יושמד או יימחק על ידי נקיטת אמצעים שנועדו למנוע גישה למידע הכלול בו או שחזור שלו בשלב מאוחר יותר.

16. ביקורות תקופתיות (א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, תיערך פעם בשנתיים לפחות, ביקורת פנימית או חיצונית, שתוודא את עמידתו בהוראות תקנות אלה.

(ב) אם נערכת ביקורת פנימית, לא יהיה המבקר מי שנושא בתפקיד ממונה אבטחה של המאגר.

להערות הציבור

(ג) דו"ח הביקורת ידווח על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, יזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב, ויסתמך גם על ממצאים ממערכות המחשוב של בעל המאגר.

(ד) דוחות הביקורת יועברו לאחראי האבטחה וכן לבעל המאגר, אשר ידון בהם ויבחן את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהם.

(א) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע אחראי האבטחה -

17. גיבוי, שחזור והתאוששות

(1) נהלי עבודה לביצוע גיבויים מדי שבוע, לכל הפחות, אלא אם המידע לא עודכן במהלך אותו זמן;

(2) נהלי התאוששות, כדי להבטיח שבכל עת ניתן יהיה לשחזר את המידע למצבו המקורי ברגע שיתרחש אובדן או הרס.

(ב) אחראי האבטחה יבטיח כי מדי שישה חודשים ייערך אימות של נכונות ההגדרות, הפעולות והיישום של הנהלים עבור יצירת גיבויים ושחזור של המידע, כאמור בתקנת משנה (א).

(ג) במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11, יתועדו גם הליכי שחזור המידע לפי תקנה זו, ובכלל זה יתועדו זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר.

(ד) לשם ביצוע נהלי ההתאוששות כאמור בתקנת משנה (א)(2), נדרש אישור של אחראי האבטחה.

(ה) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יישמר עותק גיבוי של המידע ושל נהלי ההתאוששות כאמור בתקנת משנה (א)(2), אשר מתקיימות גם לגבי דרישות אבטחת המידע לפי תקנות אלה, מחוץ למתקני המאגר, או שיעשה שימוש באמצעים שיבטיחו את שלמות המידע ואת אפשרות השחזור של המידע במקרה של אובדן או הרס.

(א) הרשם רשאי לתת הוראות או הנחיות לגבי כלל מאגרי המידע, בכל עניין הנוגע לאבטחת מידע וליישום תקנות אלה, לרבות פירוט של אמצעי האבטחה שיש לנקוט במצבים ובמקרים שונים, תקנים ושיטות אבטחה מקובלים שיש להשתמש בהם.

18. סמכויות הרשם

להערות הציבור

(ב) הרשם רשאי לפטור סוגי מאגרי מידע או מאגרים מסוימים מחובות אבטחת מידע לפי תקנות אלה, בין היתר בהתחשב בגודל המאגר, סוג המידע שנמצא בו, היקף הפעילות של המאגר, או מספר העובדים במאגר.

(ג) הרשם רשאי להורות כי עמידה בהוראות תקן מקובל או בהנחיות של רשות מוסמכת בעניין אבטחת מידע, תפטור מתחולת תקנות אלה כולן או חלקן; לעניין זה -

"רשות מוסמכת" - רשות בישראל המוסמכת על פי דין לתת הנחיות בעניין אבטחת מידע;

"תקן מקובל" - תקן אבטחת מידע שהוא תקן ישראלי או תקן של גוף מוכר שאיננו ישראלי, שהרשם אישר לעניין זה.

19. תחולה (א) על מאגרי מידע שאינם מאגרים שחלה עליהם רמת האבטחה הבינונית או רמת האבטחה הגבוהה - יחולו הוראות תקנות אלה, למעט תקנות 4(ד), 5(ב), 6(ב), 7(ד), 8(ג), 9(ב), 10(א), 11(ב) עד (ד), 12(ד) עד (ו), 14(א)(2)(ז) ו-4(א), 16(א) ו-17(א) ו-ה).

(ב) על מאגרים שחלה עליהם רמת האבטחה הבינונית - יחולו הוראות תקנות אלה, למעט תקנות 5(ב), 8(ג), 11(ד), 12(ו) ו-17(ה).

(ג) על מאגרים שחלה עליהם רמת האבטחה הגבוהה - יחולו בנוסף להוראות התקנות החלות על מאגרים שחלה עליהם רמת האבטחה הבינונית - גם הוראות תקנות 5(ב), 8(ג), 11(ד), 12(ו) ו-17(ה).

(ד) הוראות תקנות אלה יחולו גם על מחזיק של מאגר, בשינויים המחויבים, ובכל מקום שכתוב "בעל המאגר" יראו כאילו כתוב "המחזיק של מאגר".

20. פטור מתחולה על אף הוראות תקנות אלה, על מאגר מידע אשר בבעלות יחיד שאינו תאגיד אשר רק לו יש גישה אל המאגר, יחולו הוראות תקנות 2(ג) ו-4(א), 5(א), 6(א), 9(א), 12(א), 13 ו-15 בלבד.

תוספת ראשונה

(תקנה 1)

1. מאגרי מידע שחלה עליהם רמת האבטחה הבינונית:

(1) מאגר מידע המשמש לשרותי דיוור ישיר או למכירה של מידע באופן אחר;

להערות הציבור

- (2) מאגר מידע שבבעלות גוף ציבורי כמשמעותו בסעיף 23 לחוק ;
- (3) מאגר מידע הכולל מידע שהוא אחד מאלה :
- (א) מידע על צנעת חייו האישים של אדם ;
- (ב) מידע רפואי או נפשי ;
- (ג) מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א-2000⁴ ;
- (ד) מידע כלכלי, לרבות מידע אודות הרגלי הצריכה של אדם ;
- (ה) מידע אודות דעות פוליטיות ואמונות דתיות ;
- (ו) מידע אודות נטיות, הרגלים ומעשים מיניים ;
- (ז) מידע אודות עברו הפלילי של אדם ;
- (ח) נתוני תקשורת כהגדרתם בחוק סדר הדין הפלילי (סמכויות אכיפה – נתוני תקשורת), התשס"ח – 2007⁵ ;
- (ט) מידע שהוא מאפיין אנושי פיזיולוגי, ייחודי, הניתן למדידה ממוחשבת – ומשמש לזיהוי.
2. על אף האמור בפרט 1(3) לתוספת זו, מאגר מידע המקיים אחד מאלו, יראו אותו כאילו אינו מאגר שחלה עליו רמת האבטחה הבינונית, ויחולו לגביו הוראות תקנה 19(א) :
- (1) המאגר כולל מידע מן הסוגים המפורטים בפרט 1(3)(ב), (ד), (ז), (ח) או (ט) לתוספת זו, אך ורק אודות העובדים או הספקים של בעל מאגר המידע, ובלבד שהמידע נדרש למטרות ניהול העסק בלבד ;
- (2) מאגר המידע מפורסם לכלל הציבור לפי סמכות כדן ;
- (3) מספר המועסקים אצל בעל המאגר אינו עולה על 10.
3. מחזיק במאגרי מידע השייכים לחמישה בעלים שונים לפחות, יחולו לגביו הוראות תקנה 19(ב) ויראו אותו כמחזיק במאגר שחלה עליו רמת האבטחה הבינונית, אף אם מאגרי המידע שבהחזקתו אינם מאגרים כאמור בפרט 1 לתוספת זו ; הוראות פרט זה לא יחולו לגבי מאגרי מידע שמתקיים בהם האמור בפרט 1(2) או 2 לתוספת זו.

⁴ ס"ח התשס"א, עמ' 62
⁵ ס"ח התשס"ח, עמ' 72.

להערות הציבור

תוספת שניה

(תקנה 1)

מאגרי מידע שחלה עליהם רמת האבטחה הגבוהה:

- (1) מאגר מידע כאמור בפרט (1) לתוספת הראשונה, שיש בו מידע אודות 100,000 אנשים ומעלה.

דברי הסבר

תקנה 1 – הגדרות

ההגדרות העיקריות בתקנות המוצעות הן אלה:

אחראי האבטחה – חובות אבטחת המידע השוטפות, מוטלות על מנהל המאגר כהגדרתו בסעיף 7 לחוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק), ואם מונה ממונה על אבטחת מידע כאמור בסעיף 17 לחוק – גם על הממונה.

"עובד" – מטרת ההגדרה להתמקד בחובות של מי שיש לו גישה למידע במסגרת פעילותו בארגון, ולצורך כך המבחן הוא פונקציונאלי וגמיש. משום כך המוקד אינו דיני העבודה, אלא מכלול בעלי ההרשאות לגישה למאגר שגישתם למידע נקבעת בידי הארגון בעל המאגר, ובכלל זה עובד שמתקיימים ביחס אליו יחסי עובד-מעביד וגם עובד קבלן. מאחר שתקנות אלה חלות גם על מחזיק במאגר שקיבל את המאגר לעיבוד מבעל המאגר (כאמור בתקנה 19(ד) המוצעת), לכן גם ביחס למחזיק יחולו ההוראות האמורות של ההגדרה "עובד", בשינויים המחויבים, לעניין "עובד" של המחזיק.

"מאגרים שחלה עליהם רמת האבטחה הבינונית" – מאגרי מידע מן הסוגים המפורטים בתוספת הראשונה. מאגרים אלה הינם מאגרים בעלי רגישות בינונית, שנקבעה בהתאם לשילוב של פרמטר כמותי (היקף המועסקים) ופרמטר מהותי (סוג המידע המעובד). הפרמטר הארגוני נבחר כפרמטר כמותי מוביל משום שהיקף מורשי הגישה הלגיטימיים למידע בארגון, הם שקובעים במידה רבה את היקף החשיפה של המידע, ובהתאם לכך מהווים אינדיקציה למידת הסיכון שבתפעול המאגר, ולצורך בהתמודדות עם סיכון זה באמצעות כלים בתחום אבטחת המידע.

"מאגרים שחלה עליהם רמת האבטחה הגבוהה" – אלה הם מאגרים שרגישותם נקבעה בהתאם לשילוב של פרמטרים כמותיים (היקף המועסקים והיקף המידע במאגר), מהותי (סוג המידע המעובד) וכמותי (היקף המידע). ההנחה היא כי סיכונים מערכתיים, לאוכלוסיות גדולות, ממוקדים במאגרים מסוג זה;

תקנה 2 – אחריות כוללת לאבטחת המידע במאגר

תקנות משנה (א) ו-(ב)

מטרת התקנה לקבוע כי בעל מאגר המידע צריך להכיר את פעילות עיבוד המידע המבוצעת על ידו, האפיון של המידע המצוי במאגר, דרגות הרגישות שלו, ולבחון את הסיכונים השונים לפעילות זו ואופן ההתמודדות איתם. הגדרה ברורה של הנהלת הארגון בנושא זה משמשת נקודת מוצא חיונית לקבלת החלטות ומימוש האחריות הניהולית של בעל המאגר. לצורך כך על בעל המאגר להגדיר מהם האיומים על המידע, ומהם הנוזקים והפגיעות שיגרמו לנושאי המידע, בשל תקלה או פריצת אבטחת מידע.

להערות הציבור

על הארגון להגדיר את הדברים במסמך אחיד גם על מנת לוודא תיאום בין נושאי המשרה השונים בתוך הארגון, בהקשר לחובותיהם השונות לפי תקנות אלה (כגון מנהל מערכות המידע, מנהל משאבי אנוש, קב"ט וכדומה).

בהתאם לסעיף 9 לחוק, נדרש כיום בעל מאגר לכלול חלק מפרטים אלה בבקשת רישום המאגר, ובכלל זה בהתאם להוראות סעיף 9(ב) לחוק:

”

- (1) זהות בעל מאגר המידע, המחזיק במאגר ומנהל המאגר, ומעניהם בישראל;
- (2) מטרות הקמת מאגר המידע והמטרות שלהן נועד המידע;
- (3) סוגי המידע שיכללו במאגר;
- (4) פרטים בדבר העברת מידע מחוץ לגבולות המדינה.”

ולפי הוראת 9(ד) לחוק, על בעל מאגר ומחזיק לעדכן את רשם מאגרי המידע (להלן – הרשם) בדבר שינויים בפרטים אלה.

תקנות משנה (ג) ו-ד)

מטרת הוראות אלה לקבוע כי יש לנקוט אמצעים סבירים בכל השלבים של תפעול מערכות מאגר המידע, ובכלל זה בשלב המקדמי של עיצובן, להפחית את סיכויי אבטחת המידע. בהקשר זה התקנה נועדה לבטא גם תובנה מקובלת, שעדיף להטמיע את שיקולי אבטחת המידע בעת עיצוב המערכת. במסגרת זו על בעל המאגר, בין היתר, לבחון האם המידע הנאסף והנשמר על ידו אינו מעבר לנדרש לצורך מימוש מטרות המאגר, וכן לשקול אם מטרות המאגר מאפשרות שימוש במידע בדרך שתאפשר שמירה על האנונימיות של נושא המידע (אנונימיזציה).

תקנה 3 – ממונה על אבטחת מידע

לפי סעיף 17 לחוק נדרשים גופים מסוימים, בנוסף לאחריותם לפי סעיף 17 למנות גם "ממונה אבטחה" שהינו בעל הכשרה מתאימה. ביחס לגופים אלה, נקבע כי החובות המנויות בתקנות למנהל מאגר, יחולו בנוסף על הממונה.

נקודה משמעותית שיש לתת עליה את הדעת היא להגדיר מהם הכלים והסמכויות לממונה על אבטחה בתוך הארגון על מנת שיוכל לממש את חובות הארגון בתחום זה. דברים אלה נכונים גם לגבי ממונה על אבטחה שמונה בידי בעל מאגר, אפילו אם חלה עליו חובה למנות ממונה לפי סעיף 17 לחוק.

תקנה 4 – נוהל אבטחה

התקנה מחייבת את אחראי האבטחה לערוך נוהל אבטחה ארגוני. מטרתו של הנוהל היא לייצר מדיניות אבטחה ארגונית, לקבוע כללים ונהלים המחייבים את כל עובדי הארגון, וליצור מודעות לסוגיית אבטחת המידע במאגרי הארגון ולחשיבות העמידה בכללים שנקבעו. קיום של נוהל אחיד ומחייב מאפשר אחידות בסדרי העבודה מול מאגרי המידע, נגישות להוראות במקרה של ספק, ומאפשר קיום תשתית להתחייבות כל עובד לעמוד בתנאיה.

נוהל האבטחה ייערך ברמת פירוט ובהיקף משתנה בהתאם לסוג הארגון. ברמה הבסיסית נדרש נוהל זה לכלול מיפוי של מערכות המידע של הארגון, פירוט ההרשאות למערכות המידע ואופן השמירה על הוראות אלה. במאגרי מידע שחלה עליהם רמת האבטחה הבינונית

להערות הציבור

או הגבוהה, ובהתאם לחובות המהותיים החלים לעניין רמות אלה, יידרש הנוהל לכלול הוראות נוספות.

על הנוהל להיות מעודכן ותואם בכל עת, הן את מצב המערכת והן את התקנות.

תקנה 5 – מיפוי וביצוע סקר סיכונים

תקנת משנה (א)

גוף המבקש לגשת לאבטחת המידע המצוי במאגר המידע שלו, צריך קודם כל למפות את רכיבי מערכות המידע שלו, כדי שניתן יהיה להגן עליהם בצורה יעילה בעזרת אמצעי אבטחה מתאימים.

לכן בשלב הראשון נדרש בעל מאגר לערוך רשימה מסודרת של כל רכיבי מערכות המחשב המשמשות להפעלת מאגר המידע או הקשורות אליו, לרבות ציוד מחשב וציוד תקשורת (רכיבי החומרה), ותוכנות מחשב (רכיבי התוכנה), כמפורט להלן:

- מערכות החומרה כוללות בין היתר: מחשבי שולחן, שרתי מחשב, תחנות עבודה, מדפסות, אמצעי מיתוג ובקרה כגון - התקני חומת-אש פיזיים, ראוטרים, מתגים, ומודמים, התקנים ניידים המתחברים לרשת כמו מחשבים ניידים, מחשבי כף יד, ואמצעי זיכרון ניידים.
- מערכות התוכנה כוללות בין היתר: מערכות הפעלה של המחשבים, יישומים (אפליקציות) לגישה לנתונים שבבסיסי הנתונים במאגר, יישומים לעיבוד נתונים, יישומי תקשורת נתונים ומערכות הגנה כגון: אנטי-וירוס, חומת-אש (פירוול) ותוכנות אנטי-רוגלות.

קיומה של רשימה מסודרת של רכיבי החומרה ורכיבי התוכנה, מסייעת לאחראי על האבטחה במאגר, לבצע מעקב מתמיד אחר מצאי רכיבי המערכת, ללא החמצת התייחסות לאף אחד מהרכיבים. התמונה הכללית המתקבלת מהרשימה המלאה מעניקה לאחראי "מבט על" המאפשר זיהוי נקודות תורפה וסיכונים ונקיטת אמצעים אבטחה הולמים לטיפול בהם.

מעבר לעריכת רשימת רכיבי מערכות המחשב, יש צורך לציין את מיקומם הפיזי של כל אחד מרכיבי החומרה. למיפוי של מיקום הרכיבים השונים יש חשיבות רבה, מאחר שהוא מדגיש את מקומו של כל רכיב בתוך המערכת הכללית, ואת היחס בינו לבין הרכיבים האחרים. מיפוי זה מאפשר זיהוי של תהליכי העבודה במערכת, ובמקרה של ליקוי אבטחה, מאפשר לזהות את מקורו ואת תחומי השפעתו.

תקנת משנה (ב)

התקנה קובעת כי במאגרי מידע שחלה עליהם רמת האבטחה הגבוהה, אין להסתפק בדרישות תקנת משנה (א), אלא יש לבסס את אבטחת המידע על מסמך מקיף ומעמיק יותר – "סקר הסיכונים". הכוונה בביטוי "סקר סיכונים" לסקר הנערך בידי בעל מקצוע בעל הכשרה מתאימה במטרה לזהות ולדרג את רמת הסיכון הקיימת בכל אחת ממערכות המחשוב שבמאגר המידע, על סמך מאפייני סיכון שייקבעו.

תוצאות סקר הסיכונים יועבר לאחראי האבטחה ולבעל המאגר, אשר ידונו בהם ויבחנו את הצורך בעדכון הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעלו לתיקון הליקויים שנתגלו במסגרת הסקר, ככל שנתגלו.

להערות הציבור

תקנת משנה (ג)

התקנה קובעת כי המיפוי והסקר האמורים בתקנות משנה (א) ו-(ב) יבוצעו בתדירות של פעם בשנה קלנדרית לפחות. מערכות תוכנה וחומרה נתונים באופן מתמיד לאפשרויות שדרוג, עדכון, ושינוי רכיבים. כל שינוי כזה במערכת החומרה או התוכנה, משפיע באופן ישיר על רכיבים אחרים במערכת בהיותם תלויים ברכיב שהשתנה או שהוא תלוי בהם. ההשפעה של כל שינוי עלולה לייצר סיכוני אבטחה חדשים, או ליצור שינוי במבנה המערכת, המחייב התייחסות בראי אבטחת המידע.

בנוסף, איומי אבטחה נוצרים חדשות לבקרים, עם גילוי פרצות או חשיפות במערכות נפוצות. לכן, יש צורך לקיים בחינה חוזרת של מבנה המערכת ורכיביה, כדי להפיק תמונת מצב עדכנית ונאמנה למקור. ובמאגרי מידע המחויבים בסקר סיכונים, קיים צורך לעדכן את סקירת הסיכונים במערכת בהתאם לשינויים שנעשו. קביעת תדירות החובה לביצוע הבדיקות נותנת מענה למעקב אחר השינויים שחלו במערכת בזמן שחלף מאז הבדיקה האחרונה.

תקנה 6 – אבטחה פיזית וסביבתית

התקנה מחייבת שמירה על מידור פיזי של מערכות החומרה הקשורות לניהול מאגרי המידע. המערכות ימצאו במקום מוגן, שכניסה אליו מתאפשרת רק לעובדים בעלי הרשאה מתאימה, בהתאם לסיווג הביטחוני.

הקפדה על אבטחה פיזית של המערכות מונעת גישה של גורמים לא מורשים אל מערכות המידע. מניעת גישה זו חשובה מאוד לאור העובדה כי הגדרות הליבה של המערכת ואמצעי ההגנה הלוגיים שלה ניתנים לשינוי ועדכון בשיטות שונות המתאפשרות על ידי הגישה הפיזית. גישה פיזית אף עלולה לאפשר גניבת אמצעי האחסון הפיזיים ובכך שימוש לא מורשה במידע.

במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יש לתעד את הכניסות והיציאות של העובדים אל מתקני המאגר, וכן לתעד הכנסת ציוד אל המתקנים, והוצאת ציוד מהם. תיעוד מלא מאפשר מעקב ובקרה במקרה של כשל אבטחתי. באמצעות התיעוד ניתן להצביע על גורם הכשל, ולנקוט באמצעי פתרון מתאימים.

תקנה 7 – אבטחת מידע בניהול כח אדם

הגורם האנושי הינו גורם סיכון משמעותי בתחום אבטחת מידע. תובנה מקובלת המבוססת על לימוד של אירועי אבטחה, מלמדת כי שיעור גבוה של אירועי אבטחה נובע מהתנהלות כוח האדם בארגון.

כחלק ממערך הצעדים הננקטים על מנת לשמור על אבטחת המידע שבמאגר, יש לוודא כי ייקלטו לעבודה הקשורה למאגר המידע, עובדים המתאימים לעבודה זו, מבחינת אמינותם ויושרם. את רמת הסיווג הנדרש יש להתאים לרגישות המידע במאגרים, ולאופי הארגון שבו מתעתד המועמד לעבוד.

בשלב הבא, לאחר שהוחלט כי המועמד אכן מתאים לעבודה הנוגעת למאגרי המידע, יש להבהיר לעובד החדש, בטרם יקבל גישה למאגרים, את חובותיו לפי חוק הגנת הפרטיות, ולפי התקנות. את הבהרת חובותיו ניתן לממש בצורה של הדרכה מובנית לעובדים חדשים, שתועבר על ידי אחראי אבטחת המידע, או על ידי גורם מתאים אחר, ורצוי אף באמצעות חוברת מידע בסיסית המבהירה נושא זה. מובן כי היקף העיסוק בנושא משתנה בין ארגונים בהתאם לתפקיד.

להערות הציבור

טרם קבלת הגישה למאגר, ולאחר הבהרת החובות לפי חוק לעובד החדש, יחתום העובד על התחייבות לשמירת סודיות בקשר למידע אליו הוא נחשף במסגרת עבודתו עם מאגרי המידע של הארגון, התחייבות זו תואמת להוראות סעיף 16 לחוק.

בנוסף על האמור לעיל, על מנת לרענן את חשיבות אבטחת המידע ואת החובות הנובעות ממנה, מוצע כי במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יחוייב בעל המאגר לערוך פעילויות הדרכה תקופתיות. פעילויות ההדרכה יכללו סקירה של מסמכי האבטחה המחייבים בארגון: הגדרות המאגר, נוהל האבטחה, והחובות לפי התקנות.

יש לוודא כי עובדים מודעים לסיכון שגורמים שונים ינסו לרמות או להונות אותם על מנת לגרום להם להוציא מידע מהמאגר בדרכי מרמה, ואת חובתם לבדוק כי מידע המופק מהמאגר ניתן למי שזכאי לכך.

תקנה 8 – ניהול הרשאות גישה

התקנה מחייבת לוודא כי הגישה למידע במאגר תתאפשר רק לאותו עובד אשר קיים צורך לאפשר את גישתו למידע בהתאם להגדרת תפקידו. פעולה זו מתבצעת על ידי ניהול הרשאות גישה. לכל עובד מוצמדת רמת הרשאה המתאימה לתפקידו, והמאפשרת לו את היקף הגישה למידע על פי רמת הרשאתו. הקצאת הרשאות תבוסס על גישת "צריך לדעת" שמשמעותה: אם העובד לא צריך גישה למידע מסוים לצורך עבודתו, אזי לא נאפשר לו את הגישה לאותו מידע.

לרוב, כאשר עובד מבצע כניסה למחשב האישי שלו, הוא נדרש להקיש שם משתמש וסיסמא, או לספק אמצעי זיהוי אחר. באמצעות המערכת מזהה אותו, ומאפשרת לו את הגישה בהתאם לרמת ההרשאה שנקבעה לו מראש.

בנוסף, במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, יש ליישם תובנות מתקדמות יותר בתחום אבטחת המידע, הדורשות פיצול הסמכות לבצע פעולות קריטיות במערכות רגישות או חיוניות בין שני אנשים, באופן שמפחית את איומי האבטחה.

תקנה 9 – זיהוי ואימות

תקנת משנה (א)

כדי לאמת שמי שניגש למידע במאגר המידע הינו אכן עובד מורשה, יש לוודא כי תשוך זהות פיזית להרשאה כפי שהוגדרה במערכות המחשב של המאגר. זאת כדי למנוע גישה של גורמים עוינים מחוץ לארגון או שימוש לרעה מתוך הארגון.

קיימים מספר מנגנונים המאפשרים אימות זהות של משתמש: שם משתמש וסיסמה, אמצעי חומרה פיזי (כגון כרטיס חכם), זיהוי ביומטרי, או שילוב של שניים או יותר מהאמצעים הללו.

תקנת משנה (ב)

במאגרי מידע שחלה עליהם רמת אבטחת המידע הבינונית או הגבוהה, על הארגון לקבוע נוהל אבטחה לעניין השימוש בסיסמאות, בהתאם לרגישות התפקידים וההרשאות.

הנוהל יקבע קריטריונים ל"חוזק" סיסמאות. סיסמה "חזקה" היא סיסמא שקשה לפרוץ אותה, הואיל והיא ארוכה, מורכבת ממחרוזת תווים אקראית, ומשלבת סוגים שונים של תווים. לעומתה, סיסמה חלשה תהיה לרוב קצרה, בעלת היגיון פנימי (כמו רצף מספרים), או קשורה לבעלים שלה (כמו מספר הטלפון, תאריך לידה או מספר תעודת זהות). הקריטריונים יחייבו את העובדים ליצור סיסמה מספיק חזקה לצרכי הגישה שלהם למידע.

להערות הציבור

כמו כן, יקבע הנוהל את מספר הניסיונות להזנת סיסמה שגויה לפני שהמערכת חוסמת את אותו משתמש מגישה למערכת. חסימה זו מיועדת למנוע מצב של פיצוח הסיסמה על ידי ניסיונות חוזרים ונשנים של צירופים שונים.

כדי למנוע התחזות לעובד ועקיפת מנגנוני ההגנה, וכן במקרה של משתמש שנחסם, הנוהל יקבע מי אחראי לברר ולאפשר גישה העוקפת את מנגנוני ההגנה.

בנוסף נדרש שהנוהל יקבע מדיניות החלפת סיסמאות. התקנה מחייבת כי החלפת הסיסמאות תתבצע לפחות פעם בשנה. בעת גישה למידע רגיש, החלפת הסיסמה היא אמצעי חיוני לשימוש לא נאות בסיסמה, שהרי גם במקרה שהסיסמה תיחשף באופן כלשהו, טווח הנזק יצומצם לזמן שיחלוף עד להחלפתה בלבד.

במערכות רבות קיימות סיסמאות ברירת מחדל לכניסה להגדרות המערכת. (דוגמא נפוצה לכך היא ראוטר אלחוטי ביתי, שבו סיסמת ברירת היא "Admin", וכך גם שם המשתמש). על אחראי האבטחה לוודא את עדכון הסיסמאות, על מנת למנוע ממי שאינו מורשה גישה להגדרות רכיבי המערכת.

תקנת משנה (ג)

במקרה של עזיבת עובד את מקום העבודה, או שינוי בתפקידו, התקנה מחייבת את אחראי האבטחה לעדכן את רשימת הרשאות הגישה בארגון. במקרה של עזיבת העובד יש לבטל את ההרשאות המוקצות לו, וכן לשנות את הסיסמאות הכלליות שהשתמש בהם. במידה וחל שינוי בתפקידו של העובד, יש לעדכן את הרשאותיו בהתאם להרשאות המוקצות לאותו תפקיד חדש, ולבטל את הרשאותיו הקודמות. בהתאם לעדכונים הללו, אחראי האבטחה יעדכן גם את רשימת הרשאות שערך לפי תקנה 8(ב), על מנת לקבל תמונה עדכנית של מצב ההרשאות בארגון.

תקנה 10 – תיעוד גישה

תקנת משנה (א)

במאגרי מידע שחלה עליהם רמת אבטחת המידע הבינונית או הגבוהה, מחייבת התקנה את אחראי האבטחה להפעיל מנגנון המתעד את הכניסות למערכת, את ניסיונות הכניסה למערכת, ואת הפעולות שבוצעו לאחר הכניסה למערכת. כל פעולה שכזאת תתועד בצמוד לזהותו של מבצע הפעולה, לזמן של ביצוע הפעולה, והמשאב הספציפי כלפיו כוונה הפעולה.

תקנת משנה (ב)

על המנגנון להיות עצמאי, לפעול באופן רציף, ללא אפשרות התערבות חיצונית, כולל התערבות של מפעילו. באופן כזה, תישמר אמינותו של המנגנון, ואמינות התיעוד. בהתקני Firewall פיזיים למשל, משולב מנגנון כזה במערך הניהול של ההתקן.

תקנת משנה (ג)

התקנה מחייבת את אחראי האבטחה לבחון את נתוני התיעוד שהפיק המנגנון מדי חודש. על אחראי האבטחה מוטלת החובה לבחון את התיעוד באופן מקצועי ומעמיק. עליו להתייחס לא רק לניסיונות כניסה שהמערכת דחתה, אלא אף לניסיונות כניסה שאושרו – תוך בחינת הלגיטימיות של האישור בניסיון למצוא כניסות לא מורשות למערכת. במידה והבחינה אכן גילתה ליקויים, על אחראי האבטחה לערוך דו"ח מסודר המפרט את הליקויים שנמצאו, ואת הצעדים שנקטו.

להערות הציבור

תקנת משנה (ד)

התקנה מחייבת לשמור את נתוני התיעוד האמור לפחות שנתיים. באופן כזה תתאפשר בחינה מדוקדקת של התיעוד במקרה של אירוע נקודתי שהתגלה בטווח של עד שנתיים מאוחר יותר.

תקנת משנה (ה)

התקנה מחייבת את אחראי האבטחה ליידע את עובדיו בדבר קיום התיעוד של פעולות הגישה שלהם למערכת. יידוע זה נועד להבטיח את מודעותו של העובד למעקב אחר פעולותיו, וממילא בעל גישה למערכת לא יבצע פעולות שאינן מורשות בידועו כי פעולתו מתועדת.

תקנה 11 – תיעוד של אירועי אבטחה

תקנת משנה (א)

מטרת תקנה זו ליצור "זיכרון ארגוני" ביחסי לאירועי אבטחה, על מנת להפיק מהם לקחים. מוצע ככלל מנחה שנועד להקל על תחקור כאמור, להתבסס ככל הניתן על רישומים אוטומטיים במערכות המידע של הארגון. מוצע כי אחראי האבטחה או צוותו יעשו שימוש ברישומים סטנדרטיים, ובמידת הצורך ובהתאם לארגון, גם יוטמעו בארגון מנגנונים ייעודיים המנהלים רישום אוטומטי אודות פעילות ברשת הארגון.

תקנת משנה (ב)

במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, ייקבעו נהלי דיווח מסודרים אודות אירועי אבטחה לגורמים המוסמכים.

תקנות משנה (ג) ו-(ד)

במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה, מחייבת התקנה את אחראי האבטחה לדווח לבעל המאגר על אירועי האבטחה שזוהו על פי הוראות התקנות הקודמות. בעל המאגר ידון בדיווחי אחראי האבטחה, ועל פיהם יבחן האם יש צורך לעדכן את הגדרות המאגר או נוהל האבטחה. במאגרי מידע שחלה עליהם רמת האבטחה הגבוהה ייערך דיון כאמור אחת לרבעון.

במקרים בהם נתוני אירועי האבטחה (כגון: כניסה בלתי מורשית למאגר, ניסיונות חדירה חיצוניים חוזרים ונשנים, שימוש חריג של עובד בהרשאתו לצורך גישה למשאבים יחודיים) מצביעים על כמות גדולה של אירועים, או על חומרתם המיוחדת, מתעורר הצורך לבחון את נהלי האבטחה, ובהתאם, לעדכן את המסמכים המיישמים את המדיניות. לכן, מטילה התקנה את החובה על בעל המאגר, לשקול את עדכון המסמכים בדונו על ממצאי אחראי אבטחת המידע מידי רבעון.

תקנה 12 – ניהול והעברה של מסמכים והתקנים ניידים

כללי

התקנים ניידים, כוללים לעניין תקנות אלה: מחשבים ניידים ומחשבי כף-יד, ואמצעי אחסון נתונים כגון: תקליטורים, כונני פלאש למיניהם, כונני גיבוי ניידים וכיו"ב. התקנים אלה, מעצם טבעם כניידים, דורשים התייחסות מיוחדת, מאחר שככלל מדובר בהתקנים קטנים יחסית, הניתנים להעברה ממקום למקום, ולפיכך קיים סיכון כי מידע עלול לדלוף החוצה באופן לא מורשה על ידי שימוש בהם. כדי למנוע מצב כזה, יש לנקוט במספר צעדים לפי הוראת התקנה:

להערות הציבור

תקנת משנה (א)

מוצע לחייב נקיטה באמצעי הגנה סבירים על המידע המצוי על ההתקן הנייד, על מנת להקשות על שימוש בידי מי שאינו מורשה במקרה של אובדן ההתקן או גניבתו. קיימים שיטות שונות להגן על מידע בהתקנים ניידים. התקנה קובעת, כי הצפנת המידע על ההתקן הנייד, על ידי שימוש נכון בשיטות הצפנה מקובלות (לדוגמה, שימוש בתוכנה המשתמש בשיטות הצפנה כמו: PGP), תיחשב נקיטת אמצעים סבירים.

תקנות משנה (ב) ו-(ג)

מוצע לחייב כי התקנים ניידים שמאוחסן בהם מידע מהמאגר, וכן פלט של מידע מהמאגר יישאו על גביהם כתובת בולטת לעין שתתריע כי המסמך או ההתקן הנייד מכילים מידע מוגן לפי חוק הגנת הפרטיות.

תקנת משנה (ד)

כדי לאפשר לאחראי אבטחת המידע לפקח על ההתקנים הניידים הנמצאים בשימוש העובדים, ועל השימוש בהם, מוצע לחייב את אחראי האבטחה לערוך רשימה של ההתקנים הניידים המשמשים לשמירת מידע שנשלף ממאגר המידע, ואת פרטי העובד המחזיק בהם. כמו כן מחויב אחראי האבטחה לקיים מנגנון לתיעוד ולמעקב אחר משלוחים נכנסים ויוצאים של התקנים ניידים. באופן כזה, מתאפשר מעקב אחר מיקומם של ההתקנים. כמוכן, שיש לאסור על שימוש בהתקנים ניידים שאינם מופיעים ברשימה שערך אחראי האבטחה, לצורך שמירת מידע ממאגרי המידע של הארגון, כאמור בתקנת משנה (ה).

במקרה של אבדן או גניבה של התקן נייד המופיע ברשימה, או פגיעה בו, על אחראי האבטחה להתייחס למקרה כמקרה של אירוע אבטחה, ומוטלת עליו החובה לנקוט באמצעים לפי תקנה 11. דהיינו, תיעוד מקרה האבטחה, ודיווח לבעל המאגר במסגרת שאר אירועי האבטחה המדווחים לו.

תקנת משנה (ה)

התקנה אוסרת על שימוש בהתקנים ניידים, לאחסון מידע ממאגר המידע, באופן עצמאי על ידי עובד, ללא שקיבל על כך אישור מראש מאחראי האבטחה. עובד המעוניין להשתמש בהתקן נייד לצרכים אלו, חייב לפנות אל אחראי האבטחה, שישקול את הסיכון שבשימוש מול הצורך, ויחליט האם לאשר את השימוש בהתקן. בנוסף יעדכן האחראי את הרשימה שהכין לפי תקנת משנה (ד).

תקנת משנה (ו)

במאגר מידע שחלה עליו רמת האבטחה הגבוהה, יתויג המידע שבמאגר באמצעים טכנולוגיים המאפשרים מעקב אחר העתקה של מידע מהמאגר ואחר השימוש שנעשה בו.

תקנה 13 – אבטחת תקשורת וניהול מאובטח של מערכות המאגר

תקנת משנה (א)

ברשת מחשבים ארגונית, ניתן לגשת מכל מחשב ברשת לכל מחשב אחר ברשת. גם אם מאגר המידע נמצא על מחשב אחד בלבד, הנעול בחדר מיוחד, אין זה אומר כי המאגר מוגן מפני גישה לא מורשית. העובדה כי המחשב מחובר ברשת לשאר המחשבים, גורמת סיכון של כניסה למחשב באמצעות הרשת.

התקנה מחייבת את בעל המאגר להפריד ככל האפשר בין המערכות המשמשות את מאגר המידע, כמו השרת שעליו מותקן המאגר, ותחנות הקצה בעלות גישה למאגר, משאר מערכות המחשבים הארגוניות. זאת, על מנת למנוע קישוריות בלתי רצויה, אל מחשבים או מערכות אשר לא נזקקים להשתמש במאגר המידע. קישוריות זו, עלולה לגרום שימוש לא נאות במאגר המידע.

להערות הציבור

קיימות מספר שיטות להפרדה זו, וביניהם: מערכת חומת אש פנימית, מערכת לחלוקת רשתות, ועוד.

תקנת משנה (ב)

בהמשך לסכנות שנמנו בתקנה הקודמת, במידה ומערכות המידע המשמשות את מאגר המידע מחוברות לרשת האינטרנט, נוצר סיכון של גישה חיצונית מתוך רשת האינטרנט – אל מערכות המידע של הארגון.

אכן, תובנה מקובלת היא כי:

"ארגונים ומערכות המידע ורשתות התקשורת שלהם עומדים יותר ויותר מול איומי אבטחה שמקורם בקשת רחבה של גורמים המסתייעים במחשבים, כגון איומי הונאה, ריגול, חבלה, ונדליזם, וכן מול איומי שרפה או הצפה, נזקים שמקורם בתקיפה של וירוסים, פריצה למחשבים ובמניעת שירות, הפכו להיות יותר שכיחים ויותר נועזים, והתחכום שלהם גדל כל העת.

...

קישור בין רשתות ציבוריות ופרטיות והשימוש המשותף במשאבי מידע, מקשה יותר ויותר על בקרת הגישה. המגמה לבזר את שירותי המחשוב החלישה את האפקטיביות של בקרה מרכזית מקצועית." [ת"י 7799, מהמבוא, עמ' 2].

על מנת להקטין את הסיכון למינימום, התקנה מחייבת, כי במידה והמערכות מתחברות לרשת האינטרנט, יש להתקין על גבי המערכות אמצעי הגנה סבירים מפני חדירה לא מורשית, או תוכנות מזיקות. אמצעי ההגנה הנפוצים היום כוללים: תוכנת אנטי-וירוס עדכנית, תוכנת אנטי-רוגלות עדכנית, תוכנת חומר אש, והתקן חומת אש פיזי.

מאחר שמערכות מידע רבות ביותר מתחברות לרשת האינטרנט, כולל בארגונים קטנים, חלה תקנה זו על מכלול מעבדי המידע, משום שבעידן הנוכחי חובה עליהם להגן על המידע המצוי ברשתותיהם מפני האיומים הכרוכים בחיבור לרשת האינטרנט.

תקנת משנה (ג)

העברת מידע באמצעות רשת האינטרנט עלולה להיות חשופה להתחקות ומעקב על ידי גורם זר המעוניין בהעתקת המידע ובשימוש בו. מידע הנשלח באמצעות רשת האינטרנט, עובר בדרכו, עד הגיעו ליעדו, תחנות רבות, אשר איננו מסוגלים להבטיח את רמת האבטחה בהן. לכן, התקנה מחייבת להצפין את המידע הנשלח באמצעות האינטרנט או רשת ציבורית אחרת.

תקנת משנה (ד)

מטרת תקנת משנה ד' לוודא כי הסיכונים שנוצרים בעת אפשרות של גישה מרחוק של עובדי הארגון, ספקיו ולקוחות, למערכות הארגון, ימצאו פתרון, ולא תהיה פגיעה ברמת האבטחה הכוללת בשל כך. לצורך כך נדרש הארגון לשמור על מנגונים שיבטיחו כי רק מורשים יגשו למידע.

תקנת משנה (ה)

מאחר שאיומי אבטחה נוצרים באופן שוטף, ומתגלות חולשות ופגימויות חדשות מעת לעת, יש צורך בניטור ועדכון שוטף של מערכות ההגנה.

תקנה 14 - מיקור חוץ

כללי

מטרת התקנה להבהיר את חובות בעל המאגר בעת ביצוע פעולות במיקור חוץ, באמצעות מחזיק. מאחר שפעולת מיקור חוץ יוצרת סיכונים מיוחדים משל עצמה, על בעל המאגר להתמודד עם סיכונים אלה בעת ביצוע פעולת מיקור חוץ. בהתאם לכך, על בעל המאגר

להערות הציבור

להגדיר את דרישות האבטחה בעת פעולת מיקור החוץ, כחלק בלתי נפרד מהגדרת שירות מיקור החוץ עצמו. על פי ההסדר המוצע, מעטפת אבטחת המידע של בעל המאגר תוחל גם על המחזיק, תוך יישום ושימוש בכלים משפטים מתאימים למימושה. על המחזיק תחול חובה לעמוד במסגרת זו.

בהקשר זה, הדעת נותנת כי קבלת שירות של מיקור חוץ מוסדרת בחוזה המסדיר את ההיבטים העסקיים והמסחריים של השירות – מטרת התקנה להבהיר כי במסגרת זו יש להתמודד עם הסיכונים לאבטחת המידע הקשורים במיקור החוץ, ולהסדירם בהסכם, כמפורט להלן:

תקנת משנה (א)

ראשית, מחויב בעל המאגר לבחון מראש את התועלת בהתקשרות עם הגורם החיצוני, מול הסיכונים של אבטחת המידע הכרוכים בהתקשרות זו. תוך שימת הדגש הראוי על זהות הגורם המועמד להתקשרות, והערכת מידת אמינותו.

אם התקבלה ההחלטה כי יש הצדקה להתקשרות זו, יש להתייחס במפורש בהסכם ההתקשרות בין הצדדים, לסוגיית אבטחת המידע. ההתייחסות תכלול את סוג המידע אליו רשאי הגורם החיצוני לגשת, ובאמצעות אילו מערכות; סוג העיבוד אותו הגורם החיצוני רשאי לבצע, ציון מפורש של משך תקופת ההתקשרות, חובות אבטחת המידע של הגורם החיצוני, והתחייבות עובדיו לעמוד בהן. כמו כן, במאגרי מידע שחלה עליהם רמת האבטחה הבינונית או הגבוהה יכלול ההסכם גם הסכמה בדבר סמכותו של בעל המאגר לפקח על פעילותו של הגורם החיצוני, על מנת לבחון שהוא אכן מקיים את דרישות האבטחה שנקבעו בהסכם.

לאחר עריכת ההסכם בין הצדדים, מחייבת התקנה את עדכון נוהל האבטחה של בעל המאגר, תוך ציון ההרשאות שניתנו לגורם החיצוני, והפניה למסמך שנחתם בין הצדדים. עדכון זה מעלה את מודעות אחראי האבטחה ושאר העובדים של בעל המאגר, למגבלות המוטלות על הגורם החיצוני, ובאופן זה, מאפשר פיקוח יעיל יותר על ביצוע פעילותו בתחום המוגדר לו, כפי שמחייבת התקנה.

תקנת משנה (ב)

התקנה מבהירה כי הוראות התקנות חלות על הגורם החיצוני עצמו, וכי הוא חייב לערוך נוהל אבטחה משלו, תוך מגבלותיו בגישה ובעיבוד של נתוני המאגר של מזמין השירות. מטרת התקנה היא, להבהיר את תחולת הסטנדרטים האמורים בתקנות, ומוחלים כבר על הארגון מזמין השירות (בעל המאגר), גם על הגורם החיצוני, נותן השירות. זאת, על מנת לשמור על רמת אבטחה מהימנה, ולמנוע זליגת המידע או חדירה אליו, דרך מערכות הגורם החיצוני.

תקנה 15 – מחיקת מידע מהמאגר

תקנת משנה (א)

בתקנה זו מוצע לחייב מחיקת מידע שכבר אין בו צורך לפי מטרות המאגר. מחיקה זו מסייעת מראש להקטנת הסיכון שבשימוש לרעה במידע, הן על ידי משתמש פנימי והן על ידי משתמש חיצוני. ככל שקיים צורך לגיטימי בשימור המידע לצרכי ארכיון, יש לשמרו בנפרד על מנת למזער את סיכוני האבטחה הנשקפים מגישה לא מורשית אליו.

תקנת משנה (ב)

התקנה קובעת שיש למחוק את המידע מאמצעי אחסון המיועד למחיקה, או להשמיד את אמצעי האחסון עצמו, באופן שלא יאפשר אחזור של המידע בעתיד.

מחיקה "רגילה" של מידע מחשב, לרוב אינה מחיקה אמיתית של המידע מאמצעי האחסון, אלא היא רק סימון של אותו מקום שהתפנה בעקבות ה"מחיקה" – כמקום הפנוי

להערות הציבור

לשימוש. על ידי שימוש בתוכנות ייעודיות, ניתן לאתר את המקום שבו אוחסן המידע מראש (שעתה מסומן כ"פנוי"), ולקרוא ממנו את המידע, כל עוד לא נכתב על גבי אותו מקום מידע חדש. מחיקה רגילה כזו, אינה מספיקה לעניין עמידה בהוראות התקנה. כאן יש דרישה למחיקה אקטיבית, שאינה מסתפקת בסימון המקום כמחוק, אלא בכתיבה של מידע אקראי לאותו מקום בנוסף לכך, באופן שלא יתאפשר שיחזור של המידע המקורי שנשמר שם. קיימות תוכנות רבות המאפשרות מחיקה כזו (wipe), ויש להשתמש בהן.

תקנה 16 – ביקורות תקופתיות

תקנת משנה (א)

במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, תחול חובת עריכת ביקורת, פעם בשנתיים, שבמסגרתה ייבחנו מדיניות האבטחה במאגר, קיומם של אמצעי אבטחה ומימושם – תוך בחינה האם מאגר המידע עומד בתנאי התקנות. הביקורת יכולה להיות פנימית – באמצעות עובדי הארגון, או חיצונית – באמצעות גורם חיצוני.

תקנת משנה (ב)

אם הביקורת היא ביקורת פנימית, חשוב לוודא כי עורך הביקורת אינו ממונה האבטחה בארגון, כדי לוודא כי הארגון מבצע בקרה בלתי תלויה. באופן כזה יוכל גם הארגון להציג תוצרים אלה, במידת הצורך, לבעלי מניותיו, לקוחותיו, בתי משפט והרשם.

תקנת משנה (ג)

דוח הביקורת יכלול את מסקנותיו לגבי יעילות אמצעי האבטחה והתאמתם לתקנות, וכן את מסקנותיו לגבי ליקויי אבטחה, אם נמצאו, והצעות לפתרונם. כמקובל, על דוח כאמור להסתמך על ממצאים ישירים ממערכות המידע.

תקנת משנה (ד)

התקנה קובעת, כי דוחות הביקורת יועברו למנהל המאגר, לאחראי האבטחה, ויידונו על ידי בעל המאגר. מטרת התקנה, לחייב את התייחסות הגורמים המחליטים לדו"ח שהופק. התקנה אף מחייבת את בעל המאגר לבחון את הצורך בעדכון הגדרות המאגר או נוהל האבטחה, בעקבות ממצאי הדו"ח.

תקנה 17 – גיבוי שחזור והתאוששות

מערכות מחשב, עלולות לקרוס באופן פתאומי בעטיים של גורמים שונים: התיישנות המערכת, תקלה טכנית, התקפה יזומה על ידי גורם זר, וירוס אלים ועוד. במקרה של אבדן המידע השמור במערכת, שחזור המידע כרוך בהשקעת משאבים רבים, ולעיתים אף אינו אפשרי. כמו כן, גם אם השחזור אפשרי, המערכת מושבתת עד לשחזור המידע מההתקנים שניזוקו.

לפיכך מוצע בתקנה זו כי במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה תהיה חובה לקבוע מדיניות של שמירת גיבויים למידע השמור במערכת, וקביעת נהלי התאוששות מתאימים במקרה של קריסת מאגר המידע, או מחיקתו.

תקנה זו מחייבת את אחראי האבטחה לקבוע נהלי גיבוי לביצוע גיבויים מדי שבוע ("גיבוי") משמעותו: יצירת עותק נוסף של המידע המגובה, עדכני לאותו זמן שבו נוצר הגיבוי). אם נמחק המאגר או שהמערכת קורסת, ניתן לגשת לאותו גיבוי, ולהפיק ("לשחזר") ממנו את המידע האבוד. כמו כן, על אחראי האבטחה לקבוע נהלים לשחזור המערכת במקרה של אבדן המידע.

ביצוע נהלי השחזור מצריך אישור מראש של אחראי האבטחה, והליך השחזור יתועד ברישום אירועי האבטחה לפי תקנה 11.

להערות הציבור

במאגר מידע שחלה עליו רמת האבטחה הגבוהה, חלה דרישה נוספת שלפיה עותק גיבוי של המידע ושל נהלי השחזור יישמר במיקום פיזי אחר מאשר מיקום המאגר עצמו. מטרת הוראה זו היא למנוע מצב של הרס נרחב אשר יפגע במאגר המידע ובגיבויים השמורים באותו מקום, כך שלא תהיה אפשרות שחזור. התקנה משאירה פתח ליישום פתרונות טכנולוגיים אחרים, במקום האחסון הפיזי המרוחק, ובלבד שהם יאפשרו את אותה רמת ביטחון בשחזור המידע במקרה הרס או אבדן.

תקנה 18 – סמכויות הרשם

תקנת משנה (א)

התקנות מציגות מסגרת בסיסית המכילה את העקרונות לאבטחת המידע במאגרי מידע. הרשם רשאי לפרט את העקרונות שהוצגו בתקנות, ולהתוות באופן מעשי את דרך המימוש המתאימה לעקרונות הללו, בהתאם לנסיבות המשתנות, להתפתחויות הטכנולוגיות ולתקני אבטחת המידע המשתנים. הרשם רשאי לתת הנחיות לגבי כלל מאגרי המידע, לגבי חלק מהם או לגבי מאגרים מסוימים, לפי הצורך.

תקנת משנה (ב)

לעיתים ישנם מאגרי מידע שבשל גודלם, היקף פעילותם, מספר העובדים המועסקים בהם או בשל סוג המידע הכלול בהם, יש מקום להקל את דרישות אבטחת המידע המוטלות עליהם לפי התקנות המוצעות. לפיכך מוצע לתת לרשם סמכות לפטור סוגי מאגרי מידע או מאגרים מסוימים מחובות אבטחת המידע לפי התקנות, על בסיס אמות המידה האמורות.

תקנת משנה (ג)

ישנם תקני אבטחת מידע שונים, בין שהם תקנים ישראליים ובין שהם תקנים זרים או הוראות של רשויות מוסמכות בתחום זה, אשר עמידה בתנאיהם מהווה החלה של רמת אבטחת מידע ראויה, שיש בה כדי להתמודד באופן ראוי עם הסיכונים הקשורים בתחום זה, אף אם אינם תואמים במדויק את הוראות תקנות אלה. לפיכך מוצע לתת לרשם סמכות להורות שעמידה בהוראות תקן מקובל או בהנחיות של רשות מוסמכת בעניין אבטחת מידע, תפטור מתחולת התקנות כולן או חלקן.

תקנה 19 – תחולה

כאמור לעיל במבוא לטיוטת התקנות, בשל מגוון הארגונים המעבדים מידע אישי, התקנות המוצעות הן מודולריות, בכך שהן מחילות חובות ברמה הולכת וגדלה, ככל שמאגר המידע הוא מאגר שפעילות עיבוד המידע שבו, בהקשר של חוק הגנת הפרטיות, היא משמעותית יותר. לפיכך רמות האבטחה לפי התקנות המוצעות מחולקות לשלוש קבוצות שונות של מאגרי מידע כאמור לעיל בדברי ההסבר לתקנה 1. תפיסה זו, של חובות מודולריות נגזרת כאמור ישירות מעקרון היסוד של אבטחת מידע, שלפיה התמודדות עם סיכוני האבטחה נבחנת בהתאם לפעילות של המאגר, והיא מוצאת ביטוי גם במסמכים דומים בעולם.

תקנה 20 – פטור מתחולה

מוצע כי מאגר מידע אשר רק לאדם אחד יש גישה אליו והוא בעל המאגר, אזי יהיה בעל המאגר פטור מהוראות התקנות, בשל הסיכון הנמוך יותר הנובע מכך שאין צורך לנהל ולפקח אחר המורשים למאגר. זאת למעט מספר הוראות בסיסיות של אבטחת מידע שיש להחיל על כל מאגר מידע שהוא, והן:

❖ אחריות כללית לאבטחת המידע במאגר מידע ולנקיטת אמצעים סבירים להפחית את סיכוני אבטחת המידע, ובין היתר, לבחון האם המידע הנאסף והנשמר במאגר אינו מעבר לנדרש לצורך מימוש מטרות המאגר.

להערות הציבור

- ❖ עריכת רשימת מצאי של רכיבי המערכת.
- ❖ אבטחה פיזית וסביבתית בסיסית (נעילת דלתות וכד'').
- ❖ קיום מנגנון זיהוי ואימות בכניסה למאגר (שם משתמש וסיסמה, וכד'').
- ❖ יישום אמצעי הגנה סבירים בעת העברת התקנים ניידים.
- ❖ אבטחת תקשורת, אינטרנט, דוא"ל וכ" (התקנת FIREWALL, אנטי-וירוס ועדכונים שוטפים וכיו"ב).
- ❖ מחיקת מידע מיותר, וכן שלאחר המחיקה לא ניתן יהיה לשחזרו מהמאגר או מאמצעי האחסון.