מדריך פעולה ליישום תקנה 10(ד) לתקנות הגנת הפרטיות (אבטחת מידע) לשמירת קבצי תיעוד ולוגים

נוסח מעודכן בעקבות תיקון 13

1. **מבוא**

יישום החובות המוטלות בתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן - "**התקנות**") במאגרים ברמת אבטחה בינונית או גבוהה לפי התקנות[1], מחייב שמירת נתוני תיעוד של מנגנוני ניטור, שליטה ובקרה, כגון נתוני בקרה על כניסה ויציאה של עובדים במקום העבודה או ברשת הארגונית, ונתוני פעילות במסדי נתונים, מאגרי מידע, מערכות הגנה ועוד.

תקנה 10 לתקנות היא הרלוונטית למאגרי מידע שחלה עליהם רמת אבטחה בינונית או גבוהה, ומכילה הוראות בדבר בקרה ותיעוד גישה. התקנה קובעת כדלקמן:

א. במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (בתקנה זו – מנגנון הבקרה), ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.

ב. מנגנון הבקרה לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו; מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.

ג. בעל מאגר מידע[2] יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

ד. **נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.**

ה. בעל מאגר מידע יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

קבצי תיעוד הם אלה המשמשים לתיעוד הנתונים והפעילות במערכות מאגר המידע, בהתאם לתקנה 10(ד) (להלן – "**לוג**" או "**לוגים**").

במסמך זה הרשות להגנת הפרטיות (להלן – "**הרשות**") מבקשת להבהיר את האופן בו יש ליישם את החובה בצורה פרקטית. מטרתה, מצד אחד, ליישם את התכלית של בדיקה בדיעבד של אירועי אבטחה או ליקויים אחרים, תוך הבטחת זמינותם של נתונים אלה, ומניעת זליגתם (שעלולה לסכן את אבטחת

[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.

המידע); ומצד שני לסייע לארגון לנהל את התיעוד ושמירת הלוגים בצורה יעילה, נגישה וזמינה, ולהציג מנגנון יישום פרקטי לחובה הקבועה בתקנה.

2. **תכלית התקנות שעניינן בקרה ותיעוד גישה**

לחובת תיעוד האוטומטי הקבועה בתקנה 10(א) ישנן מספר תכליות:

2.1. ניטור מערכות המאגר – צפייה במערכות ודגימתן באופן רציף. הכוונה לניטור מערכות כגון, השרת שהמאגר מותקן בו, מערכת ההפעלה על השרת, חומת האש שמגנה עליו, ההגנה על יחידות הקצה שניגשות למאגר ועוד.

2.2. ביצוע בקרה על פעילות מערכות המאגר – הניטור הרציף מאפשר לבחון את נתוני הפעילות ולדגום נתונים חריגים.

2.3. הצורך לאחסן את כלל הנתונים במערכות המאגר – כך, ניתן יהיה לשחזר את שאירע בעת אירוע אבטחה. למשל, אם גורם זדוני חדר למערכות המאגר, נוכל לדעת כיצד הדבר התאפשר, מה הייתה תצורת הרשת הארגונית בעת האירוע, אילו רכיבים נפגעו ועוד. זאת, על מנת לתקן את הליקויים שנמצאו ולבצע פעולות לאי הישנות אירועים מסוג זה.

3. **סוגי גישה למערכות המאגר**

כפי שהוצג לעיל, תקנה 10(א) קובעת, כי יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר, המשמשות את המאגר ואשר יש להן חשיבות בהיבטי אבטחת מידע.

3.1. גישה המתבצעת בידי משתמש: כאשר מדובר בגישה המתבצעת בידי משתמש אנושי, לשרת המכיל מאגר מידע או לשרת אשר מספק שירותים המבוססים על מאגר מידע, אזי הכוונה לתחנת קצה (endpoint) מרוחקת של לקוח (client), שבאמצעותה המשתמש ניגש לצד השרת (server), עליו רץ היישום (האפליקציה), במטרה לאחזר מידע מן המאגר.

3.2. גישה המתבצעת באמצעות רכיב קוד: כאשר מדובר בגישה שמתבצעת בידי רכיב קוד כלשהו, אזי הכוונה לממשק פנימי שמקשר בין צד השרת שעליו היישום רץ, לבין מאגר המידע שהיישום ניגש אליו. ייתכן גם שמדובר בממשק חיצוני שמקשר בין היישום החיצוני לבין השרת, במטרה לאחזר מידע מן המאגר. לבסוף, ייתכן מצב בו היישום החיצוני ייגש ישירות למאגר המידע.

4. **מערכות המאגר ולוגים**

ככלל, החובה הקבועה בהוראות תקנה 10(ד) לשמור לוגים של כל מערכות המאגר, משמעה, אחסון כל קובץ שמתעד את הפעולה ונתוני הפעולה, של כל אחת ממערכות האבטחה של המאגר והמערכות המשמשות את המאגר. זאת, תוך הקפדה על זמינותם ונגישותם של הלוגים השמורים לפרק זמן של שנתיים לפחות.

יחד עם זאת, קיימות מערכות קריטיות לתפעול מאגר המידע ולאבטחתו, שחובה לנטר ולתעד את פעילותן באופן רציף, והלוגים שלהן חיוניים ביותר בעת חקירה של אירוע אבטחת מידע. בהן לדוגמה, לוגים של מערכת ההפעלה, חומת-אש או WAF. את נתוני התיעוד של מערכות אלה, יש לשמור נגישים, זמינים ומאובטחים במערכות אחסון מקומיות למשך כל התקופה הקבועה בתקנה 10(ד), קרי שנתיים.

בכל הנוגע ללוגים משאר מערכות המאגר, סבורה הרשות כי ניתן לשמור אותם במערכות אחסון מקומיות, למשך שישה חודשים לפחות, ובתום שישה חודשים ניתן להעבירם למשך הזמן שנותר, לאחסון במנגנון שימור ארוך טווח, דוגמת התקן אחסון המצוי מחוץ לחצרי הארגון (Off Site Backup).

להלן דוגמאות למערכות קריטיות, אשר את נתוני התיעוד הנוגעים להן יש לשמור במערכות מקומיות לאורך כל התקופה הקבועה בתקנה 10(ד), קרי שנתיים:

4.1. מערכת ההפעלה - מערכת הפעלה מעודכנת בכל עדכוני האבטחה חיונית לתפעול ולאבטחה של המאגר ומערכותיו. זו התוכנה שמנהלת את משאבי החומרה והתוכנה במחשב, מספקת את התשתית הנחוצה להרצה של מאגר המידע ויתר היישומים, ומנהלת את הגישה למעבד, לרכיבי הזיכרון השונים, להתקנים ולמשאבי המחשב והרשת.
כל אירועי הגישה הללו, כאמור לעיל, מתועדים בשלל לוגים שמערכת ההפעלה מנהלת, והוגדרו מלכתחילה בתצורה בידי הארגון.

4.2. מאגר המידע – לב ליבה של המערכת, אשר הבקרה והתיעוד בה חיוניים לצרכי בחינה וחקירה בכל אירוע. חובה לתעד את הגישה והפעולות המבוצעות במערכות מאגר המידע ולשמור את התיעוד. יש לוודא כי הלוגים נשמרים באופן מאובטח, שימנע השחתה או מחיקה, שגויה או מכוונת.
יש לתעד את הנתונים הבאים: זהות הניגש (משתמש אנושי או ממשק פנימי/חיצוני), התאריך והשעה של ניסיון הגישה, הרכיב שבאמצעותו התבצעה הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה (כלומר שם בסיס הנתונים, מערכת ניהול קבצים וכדומה), סוג הגישה (קריאה כתיבה או שליפה), היקפה, והאם הגישה אושרה או נדחתה.
מאחר שהמשמעות היא שמירת לוגים בהיקף נרחב, על הארגון לשקול שימוש בכלים ממוכנים לאיסוף וניתוח נוח של הלוגים.

4.3. AD – מדובר בחבילת Active Directory. זוהי חבילת כלי שירות שפותחה על ידי מיקרוסופט לניהול רשתות בארגונים. חבילת השירותים מאפשרת ניהול מרכזי של רשת המחשבים בארגונים.

4.4. EDR – רכיב חשוב לתיעוד פעולות שמתבצעות על תחנת קצה, ולכן הבקרה והתיעוד בו חיוניים. תחנת קצה עלולה להוות וקטור תקיפה, בעיקר לאור חולשות הנדסת אנוש.[3]

[3] להרחבה ראו: https://lifesci.tau.ac.il/it/guides/edrnac_faq

4.5. NAC – מנגנון שמנטר את נקודות הקצה והגישות לרשת הארגונית, מתוך הרשת הארגונית, ומהווה הגנה בסיסית באבטחת רשתות. תחנת קצה (מחשב, מדפסת וכדומה) עלולה להוות וקטור תקיפה, בעיקר לאור חולשות הנדסת אנוש, ולכן הבקרה והתיעוד בו חיוניים.[4]

4.6. חומת אש (firewall) – המחסום בין כל ממשק חיצוני לבין הרשת הארגונית ומאגר המידע, או בין ממשקים פנימיים. יש לתעד כל ניסיון להתחברות לרשת הארגונית ולמערכות המאגר. הבקרה והתיעוד הללו חיוניים.

4.7. WAF - חומת אש ייעודית לאפליקציות מקוונות, המסננת, מציגה וחוסמת תשדורת HTTP אל יישום אינטרנט וממנו. בארגון בו הותקנה הגנת WAF..

4.8. DBFW - חומת אש ייעודית להגנה על בסיס הנתונים, ויש לתעד ולשמור את כל הלוגים.

סיכום

מטרת המסמך הינה להבהיר את אופן יישום תקנה 10(ד) לתקנות לעניין שמירת נתוני התיעוד במערכות המאגר ולהציע קווים מנחים באמצעותם בעל המאגר והמחזיק יוכלו לוודא את עמידתם בהוראות התקנות. חשוב לציין, כי רשימת המערכות הקריטיות למאגר המידע המנויות לעיל, איננה רשימה סגורה. אם הותקנו בארגון מערכות ניטור והגנה נוספות, אזי יש לוודא כי גם הלוגים שלהם נשמרים.

הפרה של תקנה 10(ד) לתקנות עשויה להוביל לפתיחה בהליך אכיפה מינהלי אשר עשוי להסתיים בהטלת עיצומים כספיים בסכומים משמעותיים (ראו סעיף 18(ג) בטבלה שבתוספת השלישית לחוק הגנת הפרטיות, התשמ"א-1981).

[4] שם.