רשות ניירות ערך
Israel Securities Authority
سلطة الأوراق المالية

מחלקת ביקורת והערכה

כ״ח אדר א תשע״ט
5 במרץ 2019

לכבוד

<u>חברות ניהול תיקים</u>

באמצעות מערכת יעל

א.ג.נ.,

הנדון: <u>תובנות מניתוח מענה לשאלון בנושא סיכוני אבטחת מידע וסייבר שהופץ בקרב חברות ניהול תיקים בחודש יולי 2018</u> (להלן: ״**השאלון**״)

במהלך החודשים נובמבר 2022 – מרץ 2023, ביצעה מחלקת ביקורת והערכה ברשות בדיקה מדגמית של אופן יישום המלצות שפורטו במסגרת חוזר התובנות שלהלן, בקרב חברות ניהול תיקים. בעקבות הבדיקה הוחלט לעדכן את חוזר התובנות. העדכונים בוצעו ביחס לתובנות מס׳ 2, 14, 15 ו-17 להלן, והם משקפים ליקויים רוחביים אשר עלו בבדיקת יישום התובנות ועמדות הסגל לגביהם. העדכון נכון ליוני 2023.

1. סיכוני אבטחת מידע וסייבר הם סיכונים אסטרטגיים וסיסטמיים ברמה המשקית. תחכום האיום הקיברנטי, עוצמת הסיכון והשלכות התממשותו מחייבים התייחסות מיוחדת אליו, הן ברמה אסטרטגית והן ברמה יישומית. יודגש שהסיכון הקיברנטי אינו מהווה סוגיה טכנולוגית גרידא אלא גם סוגיה עסקית-אסטרטגית חוצה ארגון, וככזה מחייב, לשם ביסוס מערך בקרות אפקטיבי, שילוב חוצה ארגון של אנשים, טכנולוגיה, תהליכים ונהלים.

2. בחודש מאי 2018 נכנסו לתוקף תקנות הגנת הפרטיות (אבטחת מידע), התשע״ז-2017 (להלן: ״**תקנות אבטחת מידע**״ או ״**התקנות**״), אשר חלות **על כל הגופים בישראל המנהלים או מחזיקים מאגר מידע**, כהגדרתו בחוק הגנת הפרטיות, התשמ״א-1981. התקנות קובעות עקרונות לאבטחת מידע, לשם הגנה על מידע אישי מפני שימוש לרעה על ידי גורמים בתוך הארגון ומחוצה לו. אי-יישום הדרישות העולות מתקנות אבטחת מידע עלול להוות הפרה לא רק של התקנות האמורות, אלא גם של הוראות הדין הייחודיות החלות על בעל רישיון מכוח חוק הסדרת העיסוק בייעוץ השקעות, בשיווק השקעות ובניהול תיקי השקעות, התשנ״ה-1995 (להלן: ״**חוק הייעוץ**״). לפיכך, **על חברות ניהול תיקים לנקוט במכלול הפעולות הנדרשות על מנת להגן, בין היתר, על המידע הנוגע ללקוחותיהן (ובפרט, מאגר נתוני לקוחות)**. עמדת סגל הרשות היא כי **על חברות ניהול תיקים לתת ביטוי לפעולות האמורות, לרבות אלו שנעשות במסגרת יישום הדרישות העולות מתקנות אבטחת מידע, במסגרת נוהל אבטחת מידע** (הנדרש על פי ההוראה לתאגידים המורשים בדבר חובת קביעת נהלי עבודה בנוגע לדרכי פעולתם והתנהלותם (נוסח חדש – 2015)[1].

[1] http://www.isa.gov.il/גופים%20מפוקחים/IsaFile_3978.pdf/233/2315/Documents/Consultants_Marketers

3. על רקע האמור, התבקשו חברות ניהול תיקים להשיב לשאלון שמטרותיו העיקריות היו: (א) לעורר מודעות של בעלי הרישיון לנושא של סיכוני אבטחת מידע ואיומי סייבר בכלל, ולדרישת תקנות אבטחת מידע בפרט; (ב) למפות את המצב הקיים בנוגע להתמודדות עם הסיכונים והאיומים האמורים; (ג) להפיק, באמצעות ניתוח המענה לשאלון, תובנות אשר פרסומן עשוי לסייע להתמודדות טובה יותר של חברות ניהול תיקים עם סיכוני אבטחת מידע ואיומי סייבר.
4. מסמך זה בא לרכז את תובנות סגל הרשות מניתוח המענה לשאלון, ולזרקר מספר סיכונים שמודעות בעלי הרישיון אליהם ואופן ההתמודדות עמם טעונים שיפור (להלן: "**ריכוז התובנות**").
5. לנוחיותכם, מצורף בנספח **מילון מושגים** הכולל פירוט של מונחים מקצועיים הנזכרים בריכוז התובנות.
6. בכוונת סגל הרשות להמשיך לפעול להגברת מודעות מנהלי התיקים לסיכוני אבטחת מידע ואיומי סייבר ולשיפור אופן ההתמודדות עמם, בין היתר, באמצעים הבאים:
   א. בדיקת נוהל אבטחת מידע של חברות ניהול תיקים בכלל, ושל חברות שהעריכו שהנוהל שלהן אינו מקיף מספיק בפרט.
   ב. קיום דו-שיח בנושא סיכוני אבטחת מידע ואיומי סייבר עם חברות ניהול תיקים בכלל, ועם חברות שתשובותיהן לשאלון מיקמו אותן בקצה ההתפלגות בפרט.
   ג. הכללת הנושא של התמודדות חברות ניהול תיקים עם סיכוני אבטחת מידע ואיומי סייבר במפרטי ביקורות שעורך סגל הרשות.
7. בשאלות והבהרות ניתן לפנות באמצעות דוא"ל MaratS@isa.gov.il.

ריכוז התובנות

ניהול סיכונים

1. **תעדוף הטיפול בסיכוני אבטחת מידע וסייבר** – מפת איומי הסייבר העומדים בפני הארגונים השונים היא מגוונת ודינמית, מה שמקשה מאוד על יכולתם לתת מענה מלא לכל איום אפשרי. לאור זאת, חשוב כי חברות יבצעו הערכת סבירות להתממשות הסיכונים השונים וכן של מידת השפעתם על הפעילות העסקית של החברה. בהתאמה, ככל שהסבירות להתממשות סיכון גבוהה יותר והשפעתו על פעילות החברה מהותית יותר, ראוי כי בתכנית להפחתת הסיכונים ייקבע הטיפול בסיכון זה בסדר עדיפות גבוה.

2. **התאמת תכנית הרציפות העסקית** – העלייה בתחכום ועצימות איומי סייבר מביאה לכך שהסבירות לפגיעה בתפקוד החברה כתוצאה מהתממשות של אירוע סייבר, עלולה להיות גבוהה משמעותית מהסבירות לפגיעה בתפקוד החברה כתוצאה מהתממשות של איום "מסורתי". בהתאם, ארגונים נדרשים להתאים את תכניות הרציפות העסקית שלהם, כך שיספקו מענה גם למאפיינים הייחודיים הכרוכים בהתממשות של סיכוני אבטחת מידע וסייבר. מומלץ כי התכניות יותאמו באופן בו תהיה כלולה בהן התייחסות לא רק להיבטים הנוגעים להשבתה, אלא גם **לכלל ההיבטים** המאפיינים אירוע מסוג זה, לרבות טיפול בדליפת מידע רגיש, עדכון לקוחות וכדומה.

נהלים ותיעוד

3. **ניהול רשימה מעודכנת של מערכות מידע, תשתיות ונכסי מידע אחרים בחברה** – השימוש במערכות מידע וכלים טכנולוגיים בארגונים הולך וגובר במשך השנים, ומהווה כיום חלק בלתי נפרד מהפעילות העסקית השוטפת. יחד עם זאת, כל שימוש באמצעים אלו עלול לחשוף את החברה לאיומי סייבר חדשים. לפיכך, חשוב כי החברה תנהל רשימה מקיפה ומעודכנת של מערכות המידע, התשתיות ונכסי מידע אחרים הקיימים בחברה, אשר תסייע לחברה, בין היתר, לקיים תהליך הערכת סיכונים אפקטיבי וכן לטובת תחזוקתם השוטפת.

4. **עדכון נוהל אבטחת מידע** – נוהל אבטחת מידע מהווה כלי מרכזי בבנייה ושמירה על חוסנה של החברה מפני סיכוני אבטחת מידע וסייבר. לפיכך, כאמור לעיל, מצופה כי חברות ניהול תיקים יתנו ביטוי במסגרת נוהל זה גם לפעולות הננקטות לטובת יישום הדרישות שנקבעו בתקנות אבטחת מידע.

סיכוני הגורם האנושי

5. **הגברת מודעות העובדים לסיכוני אבטחת מידע וסייבר** – הגורם האנושי מהווה גורם חשוב ביותר בבניית מערך אבטחת מידע אפקטיבי בחברה, אך בו בזמן הוא גם החוליה החלשה ביותר במערך זה. לכן, קיימת חשיבות רבה בהגברת המודעות בקרב עובדי החברה לסיכוני אבטחת מידע וסייבר, לרבות עדכון שוטף של העובדים בדבר איומי סייבר חדשים. הגברת המודעות בקרב העובדים עשויה לסייע לחברה להקטין את ההסתברות להתממשות אירוע סייבר, בדגש על חדירת פוגענים וכופרות דרך ערוצים לגיטימיים לכאורה בהם עושים העובדים שימוש במהלך הפעילות השוטפת. כחלק מהגברת המודעות, מומלץ לבצע הדרכות לעובדים המתמקדות בסיכונים ובמצופה מהעובדים במקרה והם חושדים באירוע סייבר.

6. **הגבלת השימוש במחשבים וציוד טכנולוגי של החברה לצרכים עסקיים בלבד** – בעידן המודרני, לאור ההתקדמות הטכנולוגית, טושטשו הגבולות בין התחום העסקי והתחום הפרטי, והשימוש של עובדים במחשבים או בציוד טכנולוגי אחר הוא גמיש הרבה יותר ופעמים רבות אינו תלוי מקום. לצד זאת, חשוב לשים לב כי העדר

הקפדה על כך שהשימוש במחשבים או בציוד החברה נעשה לצרכים העסקיים בלבד, מגביר את הסיכון לדליפת מידע או לפגיעה בו, לרבות בדרך של הצפנתו, באמצעות חשיפת המחשב או הציוד לפוגען, כופרה וכיו"ב.

כלים טכנולוגיים

7. **עדכוני תוכנה ורכיבי אבטחת מידע במערכות הפעלה ויישומים שונים** – מערכות הגנה בתחום אבטחת מידע וסייבר הן כלי הכרחי בבניית מערך אבטחת המידע של החברה. היות שגורמים עוינים מפתחים כלי התקפה חדשים באופן תדיר, מומלץ להקפיד על עדכון שוטף של מערכות ההגנה כאמור. היעדר עדכון שוטף של תוכנות ורכיבי אבטחת מידע, מגביר את הסיכון לניצול חולשות אבטחה במערכות אלו, אשר ידועות לגורמים עוינים, וכתוצאה מכך לאפשרות של דליפת מידע ואף השבתת מערכות אלו.

8. **התקנת מערכות סינון אתרים ותכנים** – כיום, חלק ניכר מהתקפות הסייבר נערך במהלך גלישה של משתמש במרחב האינטרנטי. על מנת לצמצם סיכון זה, קיימת חשיבות בהתקנתן של מערכות שמטרתן סינון אתרים ותכנים אשר עלולים לכלול למשל קוד זדוני, וכן קיימת חשיבות בעדכונן ותחזוקתן השוטפת של מערכות אלו בכדי לשמור על האפקטיביות שלהן.

9. **התקנת מערכות הגנה נוספות מפני גישה לא מורשית לרשת הפנימית של החברה** – התקפות סייבר שונות מבוצעות באמצעות חדירה לרשת הפנימית של החברה. לפיכך, קיימת חשיבות בהטמעת אמצעים טכנולוגיים שונים, כגון: נתבי אבטחה (firewall), מערכות IPS וכדומה, כאמצעי הגנה אפקטיביים מפני גישה לא מורשית מרשת ציבורית, למשל האינטרנט, לרשת הפנימית של החברה.

10. **אבטחת ההתחברות מרחוק לרשת הפנימית של החברה** – שימוש בהתחברות מרחוק לרשת הפנימית של החברה הוא הכרחי בחברות רבות ונעשה על בסיס שוטף. לאור זאת, חשוב להבין את הסיכונים הטמונים באמצעי זה ולתת לכך מענה הולם. חיבור מחשבים זרים לרשת הפנימית של החברה עלול להוביל להדבקת מחשבי הרשת בנוזקה, להביא לדליפת מידע וכיו"ב. לכן יש לוודא, בין היתר, כי החיבור מרחוק מבוצע תוך שימוש במנגנון "הזדהות חזקה", כי תווך התקשורת מוצפן וכי נאכפות דרישות סף שונות עבור חיבור באמצעות מחשב מרחוק (למשל, קיומו של אנטי-וירוס פעיל ועדכני).

בקרת גישה פיזית לחברה

11. **בקרת גישה פיזית למתקני החברה** – לצד התמודדות עם סיכוני אבטחת מידע מודרניים, כדוגמת אירוע סייבר, על החברות לתת מענה גם לסיכוני אבטחת מידע קלאסיים העומדים בפניהן, למשל גישה לא מבוקרת למתקני החברה. בהתאם, חשוב לפעול להגבלת גישה פיזית של גורמים לא מורשים למתקני החברה ולמערכות המידע שלה, שכן הגבלה לא מספקת מגבירה את הסיכון לפגיעה בשוגג או בזדון במערכות המידע, עד כדי אי זמינותן וכן לדליפת מידע וכיו"ב.

12. **בקרת גישה למסמכים פיזיים של החברה** – חברות רבות ממשיכות לעשות שימוש במסמכי נייר גם כיום, ועליהן לתת את הדעת להגבלת גישה ולסיכון דליפת מידע רגיש גם ביחס למסמכים כאמור. בהקשר זה, מומלץ לגלות ערנות גם לסיכון הקיים באובדן לצמיתות של מידע חיוני, השמור במסמכי נייר שאינם מגובים אלקטרונית.

13. **בקרת גישה פיזית לרשת הפנימית של החברה** – מרבית המאמצים המושקעים על ידי חברות כיום בהיבטי הגנת הרשת, מופנים להתמודדות עם איומים הבאים מרשת האינטרנט, אך לצד זאת יש לוודא כי הגישה הפיזית לרשת הפנימית של החברה מבוקרת גם היא בצורה מיטבית. חשוב לזכור כי היעדר יישום של בקרות גישה

בטכנולוגיות שונות, אשר מונעות התחברות פיזית לרשת הפנימית של החברה, דרך מחשב או התקן נייד שאינו מורשה, מעלה את הסיכון לדליפת מידע, להדבקת מחשבי הרשת בנוזקה וכיו״ב, ואף להשבתת הרשת.

<u>העברת מידע מהחברה</u>

14. **הגנה על מידע רגיש המועבר באמצעות דוא״ל או התקן נייד** – בחברות רבות נעשה שימוש שוטף לצורך העברת מידע הן באמצעות התקנים ניידים, כדוגמת דיסק און קי, והן באמצעות שימוש בתכתובות מייל. לפיכך, קיימת חשיבות רבה בהטמעת אמצעים טכנולוגיים שמטרתם למנוע דליפת מידע רגיש מהחברה החוצה, כגון חסימת התקנים ניידים לא מורשים בתחנות העבודה, מניעה או קבלת התראה בדבר שליחת מידע רגיש באמצעות דוא״ל או העברת קבצים באמצעי תקשורת שונים. יודגש כי חברות המעוניינות להמשיך ולהשתמש בהתקנים ניידים לצרכיהן, יכולות להסתייע בכלים טכנולוגיים המאפשרים לעשות כן <u>תוך ביצוע בקרה אפקטיבית</u> המצמצמת סיכון לדליפת מידע.

15. **הגנה על מידע אישי שמועבר ללקוחות** – לא פעם עולה צורך להעביר מידע אישי ללקוחות החברה אשר מוגדר כמידע רגיש בחוק הגנת הפרטיות. על מנת לוודא את שלמות המידע ומניעת דליפתו לגורם לא מורשה, כתוצאה משימוש ברשת האינטרנט או רשתות תקשורת ציבוריות אחרות, מומלץ לקיים בקרות כמו הצפנה של המידע המועבר או מסירת המידע ללקוחות באמצעות אתר אינטרנט מאובטח. יודגש כי חברות רבות אמנם מיישמות פתרון במסגרתו ספקי שירות חיצוניים מצפינים עבורם את קבצי הדיווח ללקוחות, אך תופעת העברת מידע לא מוצפן, כדוגמת דיווחים רבעוניים, עדיין קיימת. מומלץ לחברות למצוא פתרונות הצפנה, גם אם אלו אינם כלולים בחבילת השירות המתקבלת מטעם ספקי שירותים חיצוניים.

16. **מניעת דליפת מידע המצוי בהתקן נייד** – ההתפתחות הטכנולוגית, בין היתר, בתחום ההתקנים הניידים, כגון: טלפונים חכמים, טאבלטים ומחשבים ניידים, מאפשרת גמישות טכנולוגית רבה לפעילות העסקית של החברה. עם זאת, מקום בו החברה מאפשרת שימוש בהתקנים ניידים לצורכי עבודה, חשוב כי תבחן דרכים להפחתת הסיכון לדליפת מידע וכן לחשיפת מחשבי החברה לפוגענים כתוצאה משימוש זה. יודגש, כי בעת שימוש בהתקן נייד קיים סיכון מוגבר לדליפת מידע כתוצאה, למשל, מאובדנו של ההתקן או גניבתו.

<u>חשבונות משתמשים</u>

17. **צמצום השימוש בחשבון משתמש משותף** – מטעמי נוחות, חברות מאפשרות התחברות למערכות המידע שלהן באמצעות חשבון משתמש אחד המשותף למספר עובדים. לצד היתרונות שבכך, יש לזכור כי העדר הקצאה של חשבון משתמש ייחודי עבור כל עובד בחברה, אינו מאפשר לשייך את הפעולות שבוצעו בחשבון לגורם מסוים, ובכך מגביר את הסיכון לשימוש לא נאות בחשבון המשתמש. יודגש כי לעמדת הרשות, כל עוד מועסק בחברה יותר מעובד אחד, קיימת בעייתיות בשימוש בחשבון משותף, כמתואר לעיל.

18. **הגבלת הרשאות גישה של משתמשים** – בכדי לאפשר גמישות מרבית, מגדירות חלק מהחברות לעובדיהן הרשאות גישה רחבות, ולעיתים כלל לא מוגבלות, למערכות המידע ולמאגרי המידע של החברה. לצד היתרונות הטמונים בגמישות זו, ישנה חשיבות רבה בהגבלת הרשאות הגישה והתאמתן לצרכי התפקיד של כל עובד ועובד, לפי העניין, וזאת על מנת לצמצם את הסיכון לדליפת מידע. יצוין כי מתן הרשאות יתר כאמור למערכות המידע של החברה, מגביר במיוחד את הסיכון לביצוע מעילות והונאות.

19. **מנגנון אוטומטי לנעילת חשבון משתמש** – ישנם מצבים בהם במהלך יום עבודה נותר מחשבו של עובד פתוח, על אף שהעובד אינו מצוי פיזית בקרבתו. מצב זה מאפשר ניסיונות פריצה לחשבונות על ידי גורמים לא מורשים, ולכן קיימת חשיבות ליישם מנגנון אוטומטי לנעילת חשבונות המשתמשים.

20. **שימוש בסיסמת התחברות חזקה** – לרוב, על מנת להתחבר למערכות המידע אשר נמצאות בשימוש החברות, נדרש להכניס פרטי הזדהות וסיסמה. הלכה למעשה, כיוון שעל העובד לזכור מספר לא מבוטל של סיסמאות, קיימת נטייה טבעית לבחור סיסמה פשוטה וקלה לזיכרון. בהקשר זה חשוב להבין כי השימוש בסיסמאות חלשות וקלות לפיצוח, מעלה את הסיכון לחדירה למערכות המידע של החברה, וכתוצאה מכך לדליפת מידע ו/או לפגיעה בהן.

21. **ניהול יומן רישום פעולות משתמשים (LOG)** – בהתרחש אירוע סייבר בחברה, ניהול שוטף של יומן רישום פעולות משתמשים, שהוגדר מראש במערכות המידע של החברה, מעלה את הסיכוי לאתר מתקפות סייבר בהתהוותן, וכן מאפשר לבצע תחקור אפקטיבי בדיעבד.

<u>שרשרת אספקה</u>

22. **עירנות לסיכונים הכרוכים בשרשרת האספקה** – קיום אינטראקציות עם ספקים במרחב הדיגיטלי הוא חלק מהשגרה השוטפת בפעילות העסקית של חברות כיום, ואנו עדים לגידול משמעותי בהתממשות איומי סייבר בעולם כתוצאה מניצול חולשות בתחום זה. לאור זאת, על כל חברה לגלות עירנות ביחס לסיכונים הנובעים משרשרת האספקה שלה, ולבחון כיצד היא יכולה להתמודד על מנת למזער אותם ככל הניתן.

23. **בקרות הגנת סייבר על שירותי מחשוב ענן** – חברות רבות עושות שימוש בשירותי מחשוב ענן על מנת לייעל את עבודתן בצורה מיטבית. יחד עם זאת, שירות זה חושף את החברות בפני מספר לא מבוטל של סיכוני סייבר. לכן, מומלץ לבחון יחד עם ספק שירותי מחשוב הענן של החברה, את בקרות הגנת הסייבר המופעלות על ידו לטובת הגנה על מידע השייך לחברה, או למצער לקבל מהספק סקירה על אודות בקרות אלו.

<u>תובנות אשר רלבנטיות בעיקר לחברות ניהול תיקים גדולות[2]</u>

24. **דיון תקופתי בדירקטוריון בנושא אבטחת מידע וסייבר** – תחום אבטחת מידע והגנת סייבר הוא תחום דינמי המתפתח בקצב מהיר ובהתאם לכך דורש רמת התעדכנות גבוהה ורציפה. לאור כל המפורט לעיל בדבר עוצמת הסיכונים והשלכות התממשותם, ישנה חשיבות רבה בקיומו של דיון תקופתי בדירקטוריון החברה בנושאים הקשורים לתחום זה, במסגרתו יינתנו דיווחים על ידי גורמים רלוונטיים. מצופה כי דירקטוריון החברה יקבע את התדירות הנדרשת לקיום דיונים כאמור, וכן הנחיות בדבר המידע אותו הוא מעוניין לקבל במסגרת דיווחים אלו.

25. **מינוי מומחה אבטחת מידע וסייבר** – לאור מורכבות הנושא, והרלבנטיות שלו כמעט לכל תחומי הליבה של החברה, מומלץ לחברות לבחון את הצורך במינוי גורם מקצועי המתמחה בתחום אבטחת מידע והגנת סייבר, אשר יוכל לספק מענה לצרכי החברה בתחום זה. עוד מומלץ כי גורם זה יהיה כפוף ארגונית לחבר הנהלה בכיר, על מנת להבטיח את מודעות והירתמות ההנהלה לצרכי הגנת הסייבר של החברה.

26. **מנגנוני מיון וסינון כח אדם** – כפי שצוין לעיל, לגורם האנושי מרכיב חשוב בבניית מערכי הגנת הסייבר אך הוא עלול להוות גם נקודת תורפה מבחינת החברה בכל הקשור לשמירה על המידע. לפיכך, יישום מנגנוני מיון וסינון

[2] כהגדרתן בתוספת ראשונה א' לחוק הייעוץ.

אפקטיביים בתהליכי גיוס כח אדם לחברה, עשויים לצמצם את הסיכון לפגיעה במערכות ומאגרי המידע של החברה על ידי עובדיה.

27. **עריכת סקר סיכונים וביקורות בתחום אבטחת מידע וסייבר** – עריכת סקרי סיכונים וביקורות בתחום אבטחת מידע וסייבר, מאפשרת לזהות ולמפות חולשות קיימות אשר עלולות לשמש גורמים עוינים במהלך מתקפת סייבר. על החברה לשאוף לטפל לאלתר בחולשות שאופיינו ברמת חומרה גבוהה בסקרי הסיכונים ובביקורות כאמור, וכן לטפל בהקדם האפשרי בחולשות ברמת חומרה בינונית.

נספח – מילון מושגים

1. **הגנת סייבר ואבטחת מידע** – תחום הגנת סייבר ואבטחת מידע מתייחס למכלול הפעולות הנוגעות להגנה ושמירה על חיסיון, שלמות וזמינות של מאגרי מידע, ושל הגדרות מערכת ונתונים אחרים.
2. **התקן נייד** – מחשב נייד, טאבלט, טלפון חכם, מסופון, דיסק או קי, וכיו"ב.
3. **יומן רישום פעולות (LOG)** – קובץ המכיל רישום של כל הפעולות שנעשו על ידי משתמש במחשב שלו או ברשת.
4. **כופרה** – קוד זדוני המוחדר לארגון על ידי תוקף, המצפין מאגרי מידע וקבצים אחרים השמורים במחשב ומונע את השימוש בהם. שחרור ההצפנה והחזרת הקבצים לשימוש מחייב במקרים רבים תשלום כופר לגורם התוקף.
5. **מאגר נתוני לקוחות** – אוסף נתוני מידע של לקוחות, כדוגמת יתרות, מדיניות השקעה ופרטי קשר, המוחזק בפורמט דיגיטלי והמיועד לעיבוד ממוחשב או אחר.
6. **מנגנון הזדהות חזקה** – מנגנון אימות משתמשים העושה שימוש בשילוב של רכיב המצוי בידי המשתמש ו/או פריט מידע הידוע למשתמש, ו/או רכיב ביומטרי, כגון: מחולל סיסמה חד פעמית (One Time Password – OTP), תעודה דיגיטלית (Digital Certificate), או קורא טביעת אצבע.
7. **מערכות מידע** – כלל המערכות והתשתיות הטכנולוגיות התומכות בפעילות הארגון, לרבות שרתים, ציוד תקשורת וציוד הגנת סייבר.
8. **מערכת IPS** – מערכת למניעת חדירות (Intrusion Prevention System) אשר חושפת, מתריעה וחוסמת פעולות חשודות, ניסיונות גישה בלתי מורשים, התקפות על הרשת וכל פעולה אשר מנוגדת לחוקים שהוגדרו מראש במערכת.
9. **נתב אבטחה (firewall)** – תוכנה או התקן חומרה, שמטרתו חסימת גישה לא מורשית מרשת ציבורית לרשת פנימית או למחשב בודד ברמת התקשורת.
10. **סיכון סייבר** – סיכון לשימוש לא מורשה בזהות, הפרעה לפעילות הארגון על ידי פגיעה בפעילות הרשת ו/או במערכות מידע, גניבה של מאגרי מידע, החדרה של קוד זדוני, חדירה למערכת מידע או חשיפת מידע.
11. **קוד זדוני/פוגען/נוזקה** – קוד המושתל על ידי גורם זדוני ועלול לגרום לפגיעה בשלמות ו/או בזמינות מאגרי מידע ומערכות מידע.
12. **רשת פנימית** – רשת תקשורת פנים ארגונית המופרדת מרשתות ציבוריות, ומשמשת לקישור בין תחנות קצה של עובדים לבין משאבי רשת דוגמת מאגרי מידע, שירותי הדפסה ועוד.
13. **רשת ציבורית** – רשת תקשורת חיצונית לארגון, כדוגמת רשת האינטרנט, אשר אינה נתונה לשליטת הארגון, ומשמשת, בין היתר, לתקשורת בין ארגונים.
14. **שרשרת אספקה** – מערך של ארגונים, אנשים, משאבים, תהליכים ומידע, המתקיים בין הארגון לבין ספקים חיצוניים. גורמים בשרשרת האספקה, להם גישה למאגרי המידע של הארגון, עלולים לגרום בשוגג או בזדון לפגיעה בחיסיון, שלמות וזמינות המידע של הארגון.
15. **תווך תקשורת** – נתיב להעברת נתונים, ללא צורך בהעברה פיזית, על גבי אמצעי אחסון נתונים.

16. **תקנות אבטחת מידע** – תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017. התקנות מפרטות את אופן יישומה של חובת אבטחת המידע, המוטלת בחוק הגנת הפרטיות הישראלי על כל בעל מאגר מידע או מחזיק במאגר של מידע אישי, כדוגמת אוסף נתונים ומידע של לקוחות.