המלצות אבטחת מידע ופרטיות

⚔️ מלחמת חרבות ברזל ⚔️

תורמים לכתיבת המסמך:

- **יובל שגב** - יו"ר פורום הסייבר באיגוד הדירקטורים
- **דני אברמוביץ** - מנכ"ל טייטנס סקיוריטי ונשיא של הצ'אפטר הישראלי באיגוד העולמי לאבטחת מידע (ISSA)
- **יגאל אקרמן ואור ישראל לוי** - יועצי אבטחת מידע מחברת טייטנס סקיוריטי
- **קובי וידר** - מומחה סייבר
- **מיטל דהרי** - מומחית אבטחת מידע
- **ניר יהונתן פסי** CISO
- **איתמר שלו** - מומחה סייבר

להערות או המלצות לשיפור המסמך, ניתן לשלוח כל תגובה לכתובת: yuvalsegev80@gmail.com

תוכן עניינים:

חלק א – כללי 3
הנחות עבודה: 4
סיכונים ותרחישים לדוגמא: 5
חלק ב' – המלצות וטיפים בהיבטי אבטחת מידע והגנת הפרטיות 6
שלב ראשון – הכנה (Preparation) 7
שלב שני – זיהוי וניתוח (Detection and Analysis) 11
שלב שלישי – בידוד, השמדת האיום והתאוששות (Containment, Eradication and Recovery) 12
שלב רביעי – חזרה לשגרה (Post-Incident Activity) 13
שלב חמישי – שיפור מתמיד (Continuous Improvement) 13
נספח א' - מילון מונחים 14
נספח ב' – כיצד ניתן לזהות האם מדובר בלינק (קישור לאתר אינטרנט) זדוני? 16
נספח ג' – מקבץ הנחיות אבטחת מידע והגנת הפרטיות לארגונים 18
נספח ד' – חברות ייעוץ ומומחי סייבר והגנת הפרטיות שניתן להתייעץ איתם 19

חלק א – כללי

מבוא:

בעת מלחמה, ההגנה על המידע והפרטיות של האזרחים, ושמירה על בטיחות כוחות הביטחון, הופכת לקריטית עוד יותר. אנחנו נמצאים במלחמה עם אויב שלא יודע שובע, והמעשים בשבוע האחרון הוכיחו לנו את אכזריותו. בצער רב, לידיו נפלו מכשירי טלפון רבים של חיילינו ואזרחנו היקרים, וכעת לאויב יש גישה למכשירים אלו ולמידע שאגור בהם.

בנוסף, ברחבי העולם יש אנשים שפרו-פאלסטינאים, ומטרתם להפיץ פייק ניוז ברשתות החברתיות ולהוציא אותנו לא טוב מול העולם.

שמירה על המידע והפרטיות חשובה למניעת נזקים פוטנציאליים לאזרחים, לכוחות הביטחון ולבטחון הלאומי. מידע רגיש שנפל או יפול בידי האויב יכול לשמש לצרכים צבאיים נוספים או לגרום תעמולות בעולם.

בעידן הדיגיטלי, ארגונים רבים מהווים מטרה למתקפות סייבר רבות מצד האויב. עלינו לשפר את מערך הגנת הסייבר בארגון, להגביר את המודעות בקרב כלל העובדים, ולשמור על ערנות.

מסמך זה נכתב על ידי קבוצות עבודה מהשוק הפרטי, במטרה להנגיש מידע רלוונטי עבור מנהלי אבטחת המידע בארגונים השונים במשק.

תודה רבה לכל מי שתרם ליצירת המסמכים והמדריכים. להוספת תגובות והמלצות למסמך, ניתן לפנות ליובל שגב, במייל yuvalsegev80@gmail.com.

הנחות עבודה:

- לאויב יש אינטרס לייצר לחץ פסיכולוגי ותודעתי. פעולות הפחדה, סחיטה, הפצה של פייקניוז, עשויות להוות חלק מהמערכה.
- טלפונים סלולריים של כמה מאלו שאינם בין החיים או נפלו בשבי נלקחו, והאויב מתחבר לקבוצות הווטסאפ שלהם, לפרופיל הלינקדין ולרשתות חברתיות שלהם. דוגמא לכך, ראינו כאשר אחד המחבלים רצח קשישה, והעלה סרטון לפרופיל הפייסבוק של הנרצחת. אנו לרוב נוטים לסמוך על הודעות שמתקבלות ממקור איתו יש לנו היכרות אישית. בימים אלו, יש לבחון בזהירות הנחת מוצא זו, עד לחזרה לשגרה. כמו כן, על חלק ממכשירי הטלפון הניידים הותקנו תוכנות שונות שמאפשרות גישה לרשת הארגונית. אם יש תוכנות לשליטה מרחוק, חשוב לבטל את הגישה לאותם משתמשים, ולנטר כל גישה לרשת הארגון.
- בעת מצבי קיצון (כגון מלחמה), אנו נוטים לרוב לסמוך על אנשים אחרים וגופים שמפרסמים ומציעים תמיכה, תרומות, וסיוע לנזקקים. בימים אלו, יש לבחון בזהירות הנחת מוצא זו, ולהיות חשדנים יותר.
- רוב ההודעות ברשתות החברתיות הינן פייק. הפצתן אינה מסייעת, ואף גורמת לנזק.

מומלץ לפעול בהתאם להמלצות פיקוד העורף בנושא:

- ✅ האם המידע הגיע ממקור מהימן?
- ✅ האם שיתופו עלול לפגוע במישהו?
- ✅ האם הפצת המידע יכולה לסייע איכשהו?

סיכונים ותרחישים לדוגמא:

סחיטה – מצב שבו מישהו זדוני (במקרה הזה האויב) איים על אדם אחר (במקרה הזה, בני המשפחה או חברים) אם אותו אדם לא יעשה מה שמבקשים ממנו.

- **תרחיש אפשרי**: האויב רואה ברשתות החברתיות את התמונה של האדם שנעדר, מתקשר למשפחה ומנסה לסחוט אותה בתמורה לקבלת מידע.

זליגת מידע רגיש – הגעתו של מידע רגיש (כגון נתוני מיקום, טלפונים, כתובות, וכדומה), בידי אדם זר (במקרה הזה האויב), שינצל אותו לביצוע פעילויות זדוניות.

- **תרחיש אפשרי**: האויב ינסה להתחבר לקבוצות ווטסאפ במטרה לשאוב משם מאגרי מידע רגישים שנבנים מתוך מטרה טובה (דוגמא למאגר עם מידע רגיש וניהול הרשאות לא מיטבי) או יקים קבוצה כזו, אשר בהתחלה תפעל בצורה לגיטימית (דוגמא לקבוצה שמציעה לאנשים שמחפשים טרמפ דרומה).
- **תרחיש אפשרי**: האויב יישאב מידע רגיש ויקבל תמונת מצב מתוך פרסומים וריכוזי נתונים שנבנים בצורה "פתוחה" ללא בקרה (ראו לדוגמא מאגר איתור נעדרים, בו ניתן לשאוב את כל המאגר בקלות באמצעות הקשת כל ה א-ב).
- **תרחיש אפשרי**: האויב יקים אתר אשר מתיימר לסייע (נניח, איתור נעדרים) במטרה לקבל מידע רגיש כגון מיקום, תפקיד בצבא וכו' מקהל יעד מטורגט. זה יאפשר לו לאסוף מידע רגיש אודות כוחות הביטחון.
- **תרחיש אפשרי:** האויב ינסה להוציא מידע ממכשירים סלולריים ו/או לבצע פעולות בשמם של החטופים/נרצחים (העברה כספית, הוצאת מידע רגיש, יצירת קשר עם קרובים או קולגות וכו').

התחזות והפחדה – מצב שבו גורם זר (במקרה הזה האויב) יתחזה לאדם אחר (במקרה הזה לאחד החטופים או נעדרים), וינסה לבצע פעולות בשמו (כגון ביצוע עסקאות מקוונות), או פעולות הסתה והפחדה (לפרסם בשמו תמונות וסרטונים בקבוצות דיון שונות וברשתות החברתיות).

- **תרחיש אפשרי**: האויב ייכנס דרך מכשירי טלפון של אנשים שנחטפו לרשתות חברתיות וישלח הודעות בשמם, או יכריח אותם להקליט הודעות (פייק ניוז) במטרה לייצר בהלה ולהעביר מסרים וכו'.

חלק ב' – המלצות וטיפים בהיבטי אבטחת מידע והגנת הפרטיות

כללי

במסגרת הכנתם של ארגונים להתמודדות עם איומי סייבר, אנחנו ממליצים לאמץ את המסגרת של NIST 800-61 לתגובה וניהול אירועי אבטחת מידע וסייבר.
המסגרת מכילה בתוכה 5 שלבים עיקריים:

1. שלב ראשון – הכנה (Preparation)
2. שלב שני – זיהוי וניתוח (Detection and Analysis)
3. שלב שלישי – בידוד, השמדת האיום והתאוששות (Containment, Eradication and Recovery)
4. שלב רביעי – חזרה לשגרה (Post-Incident Activity)
5. שלב 5 – שיפור מתמיד (Continuous Improvement)

כמובן, שזה רק המלצה של מומחי אבטחת מידע שעמלו וגיבשו את המסמך עמדה, וזה לא חובה או המלצה רשמית של מערך הסייבר. על הארגונים לאמץ ולהתאים את ההנחיות לפי הצורך.

שלב ראשון – הכנה (Preparation)

מדובר בשלב הראשון אך אחד החשובים, היות והכנה טובה, יכולה למנוע או להקטין את מידת הנזק הפוטנציאלית ממתקפות סייבר עתידיות.

תוכנית לתגובה וניהול אירועי סייבר

בשלב ההכנות, מכינים את התשתית עליה מתבססת יכולתו של הארגון להתמודד ולנהל אירוע סייבר עתידי, או אירוע קיצון, באמצעות נוהל תגובה וניהול אירועי סייבר, תוכניות להמשכיות עסקית והתאוששות מאסון, נהלים תפעוליים, נהלי אבטחת מידע, הדרכות והכשרות, ותרגולים.

אחד הדברים החשובים בשלב ההכנה, הוא לגבש תוכנית תגובה וניהול אירועי סייבר (IRP). התוכנית צריכה לכלול בין היתר את הצוות תגובה, תפקידים ואחריות, ואת נהלי התגובה (פלייבוקים) למגוון האירועים הפוטנציאליים (כגון פישינג, דלף מידע, נוזקת כופר, מתקפות מניעת שירות (DoS), מתקפות מניעת שירות מבוזרות (DDoS), ועוד.

התוכנית צריכה להיות מותאמת לצרכים הייחודיים והיכולות של הארגון, בהתייחס למרכיבים הבאים:

- המגזר אליו משתייך הארגון (פיננסי, בטחוני, רפואי, טלקום, מפעלים, וכדומה)
- גודל הארגון (כמות העובדים ופריסה גיאוגרפית)
- סוג הנכסים (נכסי מידע ונכסים מוחשיים כגון מפעלי ייצור)

תוכנית להמשכיות עסקית (BCP) והתאוששות מאסון (DRP)

כמו כן, זהו גם שלב כל ההכנות מבחינת נהלים ותוכניות לניהול המשכיות עסקית (BCP) והתאוששות מאסון (DRP).

- **תהליך BIA והערכת סיכונים (בהיבט העסקי)**
  השלב הראשון (אם לא נעשה כבר), הוא לבצע תהליך של ניתוח השלכות עסקיות או BIA (ר"ת של Business Impact Analysis). בשלב זה, על הארגון למפות את כל התהליכים העסקיים הקריטיים בארגון, כולל מערכות מידע תומכות, וגם להתייחס לספקים.

- **תהליך הערכת וניהול סיכונים (בהיבטי הסייבר)**
  לאחר סיום תהליך ה-BIA, על הארגון לזהות את הסיכונים, לבצע הערכת סיכונים, ולנהל את הסיכונים בהתאם למדיניות ניהול הסיכונים של הארגון (שנקבעת לפי סוג המגזר אליו משתייך הארגון, דרישות רגולציה, איומי ייחוס וכדומה).

- **גיבוש אסטרטגיה לניהול המשכיות עסקית והתאוששות מאסון**
לאחר סיום תהליך ה-BIA, וסקר הסיכונים, הארגון יוכל לקבוע את האסטרטגיה לניהול המשכיות עסקית והתאוששות מאסון.
כחלק מהאסטרטגיה, צריכים לוודא שיש גיבוי שוטף לכל המידע הקריטי, היות וזה ישפיע על היכולת של הארגון בשלב ההתאוששות מאירוע סייבר.
על סמך האסטרטגיה, ייקבעו תוכניות להמשכיות עסקית והתאוששות מאסון. התוכניות הללו צריכות להיות בהלימה מלאה עם דרישות העסקיות והרגולטוריות של הארגון, ובהתאם לתרחישי האיום שנקבעו (מלחמה, שריפה, הצפה, כשל טכנולוגי, וכדומה).

ספקים ושרשרת האספקה

ארגונים רבים לא מתייחס לספקים שלהם בתהליכי הערכת וניהול סיכונים ו/או המשכיות עסקית של הארגון. כחלק מתוכנית ניהול סיכוני בשרשרת האספקה, על הארגון להתייחס לכל שרשרת האספקה, ולזהות נקודות חולשה ולנקוט צעדים לסגירת הפערים. חשוב לזכור שחוזק השרשרת היא כחוזק החוליה החלשה שבה, ולעתים, פגיעויות אבטחת מידע נוצרות בשרשרת האספקה של הארגון.

ניתן לאמץ גישה פשוטה של 5 שלבים עיקריים לניהול הסיכונים בשרשרת האספקה:

<u>שלב 1 – מיפוי הסביבה הארגונית</u>

בשלב הראשון על הארגון למפות את כל הפעילות העסקית שלו:

1. תהליכי עבודה בארגון
2. תהליך זרימת המידע (פנימה והחוצה)
3. מיהם הספקים הרלוונטיים
4. מהו תהליך העבודה מול אותם ספקים
5. לסווג את הספקים (בהתאם למידת הרגישות של המידע שיש להם גישה, או רמת הקריטיות של השירות שהם מספקים ללקוח)

<u>שלב 2 – הערכת וניהול סיכונים</u>

בשלב השני הארגון צריך לקבוע לעצמו תוכנית להערכת וניהול סיכונים לשרשרת האספקה (בהתאם לדרישות העסקיות, רגולציה, איומי הייחוס, וכדומה).
לאחר מכן, על הארגון לבצע סקרי ספקים ולוודא סגירת הפערים (חלק מניהול הסיכונים).

<u>שלב 3 – תוכנית המשכיות עסקית והתאוששות מאסון לספקים</u>

בשלב השלישי, על הארגון להתייחס לכלל הספקים בתוכניות המשכיות עסקית והתאוששות מאסון שלו, או לקבוע תוכנית נפרדת לכל ספק, בהתאם לרמת הקריטיות והפעילות העסקית שלו.

<u>שלב 4 – הדרכות ותרגולים</u>

בשלב הרביעי, על הארגון לבצע הדרכות והכשרות לעובדים ולספקים, לוודא שכל הגורמים שמעורבים בתהליך, אכן מכירים היטב את תהליכי העבודה בשגרה ובחירום, ולבחון את מידת האפקטיביות של ההדרכות והתוכניות, באמצעות תרגולים שוטפים.
בתום התרגולים, צריכים לבצע תהליך מוסדר של הפקת לקחים, ולממש את כל ההערות לשיפור.

שלב 5 – ניטור ושיפור מתמיד
בשלב החמישי, על הארגון לנהל תהליך מוסדר של מעקב שוטף וניטור הפעילות של הספק, לאיתור פגיעויות ובעיות אבטחה נוספות שעלולות לצוץ בהמשך הדרך.

שירותי מודיעין סייבר

כחלק מההכנות להתמודדות מול איומי סייבר, מומלץ לצרוך שירותי מודיעין סייבר מחברות סייבר שמתמחות במתן שירותים מסוג זה.

חשוב להתייחס למרכיב חשוב בשירותי המודיעין, וזה הטלפונים של הנעדרים, חטופים והקורבנות שנפלו במתקפה המחרידה של ה-7.10.2023.

האויב השיג הרבה מכשירים ניידים, ובהם מידע אישי רב, ואף מידע עסקי. חשוב להתייחס למרכיב הזה בעת תהליך הניטור השוטף, ולוודא שאין ניסיונות שימוש לרעה במידע שהושג מהטלפונים הללו.

כמו כן, לארגונים בהם הייתה גישה לעובדים מרחוק, חשוב למחוק את הנתונים ולנתק את המכשירים מהרשת הארגונית. במידת הישימות, צריך גם לנטר את כל ניסיונות הגישה מהמכשירים הללו, או שימוש במידע שהושג מהם.

הדרכות

חובה לבצע מגוון הדרכות להגברת המודעות בנושא איומי אבטחת מידע והגנת הפרטיות לכלל העובדים בחברה.

כמו כן, חובה גם לבצע הדרכות והכשרות ממוקדות לכל הדרגים השונים (הנהלה, צוותי IT, צוותי תגובה), לשפר את המוכנות שלהם להבנת והתמודדות עם אירועי סייבר, ניתוח ההשלכות העסקיות, ותגובה וניהול האירוע.

תרגולים

תרגולים לבדיקת מוכנות הארגון מבחינת עמידה באירועי קיצון שונים. התרגולים צריכים לבחון את המוכנות הטכנולוגית לצד המוכנות הלוגיסטית ושל האנשים, מבחינת היכולת שלהם להתמודד עם מגוון אירועי קיצון שונים.

להלן דוגמאות של תרגולים אפשריים:

1. **תרגולי סייבר לחברי הנהלה**
   המטרה: שיפור היכולת של חברי הנהלת הארגון לזהות את ההשפעה של אירועי הסייבר על הפעילות העסקית (Situational Awareness), ולשפר את היכולת של הארגון להתמודד עם אירועי קיצון.

2. **תרגולי סייבר לעובדים**
   המטרה: לשפר את היכולת של העובדים לזהות ולדווח על אירועי סייבר שונים (כגון ניסיונות פישינג).

3. **תרגולי סייבר לצוותי ה-IT**

המטרה: לבחון ולשפר את היכולת של צוותי ה-IT להתמודד עם מגוון אירועי סייבר, ולתת מענה מהיר בהיבטים הטכנולוגיים (כגון התאוששות מנוזקת כופר, התאוששות ממתקפת מניעת שירות, התאוששות מכשל טכנולוגי, וכדומה)

4. **תרגולי סייבר לצוות SOC**

המטרה: בחינת האפקטיביות של מערכות הניטור והיכולת של הצוותים להתמודד עם מגוון רחב של אירועי סייבר

שלב שני – זיהוי וניתוח
(Detection and Analysis)

השלב השני במסגרת של NIST מתחלק לשני חלקים: חלק של זיהוי האירוע וחלק של ניתוח האירוע. לנוחיותכם, אנחנו נתייחס לכל חלק בנפרד.

חלק של זיהוי האירוע (Detection)

שלב זיהוי האירוע הינו אחד מהשלבים החשובים, היות וזה משפיע באופן ישיר על יכולתו של הארגון להגיב לאירוע. ככל שהארגון מזהה את האירוע בזמן אמת (או קרוב לזמן אמת), זה יכול להקטין את מידת הנזק הפוטנציאלי על הפעילות העסקית של הארגון.

לצורך שיפור יכולות הזיהוי של אירועי ותקריות סייבר, על הארגון לשפר את היכולות של זיהוי, באמצעות הטמעת ו/או טיוב פתרונות טכנולוגיים כגון SIEM, XDR/EDR, UBA/NBA ועוד.

בין אם לארגון יש SOC פנימי, או שהוא צורך שירותי SOC חיצוניים (MSSP), צריכים לטייב את החוקים ב-SIEM, ולשפר את מערך אבטחת המידע הארגוני במטרה לשפר את היכולת של הארגון לזהות אירועי ותקריות סייבר מהר ככל האפשר.

דיווח על זיהוי אירועים יכול להגיע גם מעובדי החברה.
הגבירו את המודעות של העובדים, לדווח למחלקת אבטחת מידע על כל אירוע חשוד (כגון ניסיון פישינג).

חלק של ניתוח האירוע (Analysis)

בחלק הזה, ישנה מעורבות של צוותי ה-SOC, ופתרונות סייבר (כגון SIEM, XDR/EDR וכדומה). חשוב לשפר את היכולות הטכנולוגיות באמצעות טיוב חוקים קיימים ויצירת חוקים ישימים חדשים, וגם את היכולות של צוותי התגובה, באמצעות הכשרות והדרכות ממוקדות (כגון ביצוע תחקור דיגיטלי, ביצוע תחקור נוזקות, ועוד).

שלב שלישי – בידוד, השמדת האיום והתאוששות (Containment, Eradication and Recovery)

השלב השלישי של NIST, מתחלק לשלושה חלקים: שלב בידוד האירוע, שלב השמדת האיום, ושלב ההתאוששות מהאירוע.

חלק של בידוד האירוע

לאחר זיהוי וניתוח האירוע, חשוב לבודד את האיום (ניתוק התחנה מרשת הארגון, או ניתוק הרשת או סגמנט הרשת). המטרה של בידוד האיום הוא במטרה למנוע התפשטות של הנזק הפוטנציאלי בארגון (למשל במקרה של הידבקות בנוזקה או מתקפת מניעת שירות).

חלק של השמדת האיום

לאחר שצוות התגובה תחקר והצליח לבודד את האירוע, חשוב לנקוט בכל הצעדים לוודא שהצליחו לנקות את המחשבים הנגועים, ואת הרשת, לפני שעובדים לשלב הבא.
מומלץ להתקין את המחשבים ואת המערכות מחדש, ולהשקיע זמן בבדיקות לאיתור נוזקות והתנהגות חשודה אחרת.

חלק של ההתאוששות מהאירוע

בחלק הזה, הארגון עובד על תהליך ההתאוששות מהאירוע, ונוקט בכל האמצעים על מנת להחזיר את הפעילות העסקית של הארגון לשגרה. ישנה חשיבות רבה לתהליך גיבוי ושחזור של הארגון.

שלב רביעי – חזרה לשגרה
(Post-Incident Activity)

לפני שחוזרים לשגרה, חשוב לוודא שצוותי התגובה וה-IT הצליחו לנקות את הרשת הארגונים מנוזקות או פעילות זדונית, המערכות הותקנות מחדש בצורה נקייה, הוקשחו והובטחו כראוי.
בנוסף, צריכים להגדיר תהליכי ניטור ובקרה לוודא שאין פרצות או נוזקות נוספות ברשת הארגון, ולזהות כל ניסיון נוסף לפעילות חשודה ברשת.
חשוב לשתף פעולה עם שירותי מודיעין סייבר, ולקבל עדכונים שוטפים על כל ניסיון פגיעה נוסף במערכות הארגון.

שלב חמישי – שיפור מתמיד
(Continuous Improvement)

במסגרת תהליך שיפור מתמיד, על הארגון לנהל תהליכים מוסדרים של הפקת לקחים, ולנקוט בכל הצעדים הנדרשים לשיפור מתמיד.
שיפור מתמיד יכול לבוא לידי ביטוי בהטמעת כלי הגנה נוספים, טיוב כלי הגנה קיימים, הוספת חוקים חדשים במערכות ההגנה הקיימות (כגון SIEM, פירוול וכדומה), גיבוש נהלים חדשים או טיוב נהלים קיימים, טיוב ועדכון תוכניות קיימות להמשכיות עסקית והתאוששות מאסון, עדכון/טיוב נהלי תגובה לאירוע וכתיבת פלייבוקים חדשים, הדרכות מודעות לכלל העובדים וספקים, הכשרות מקצועיות לכל הצוותים הרלוונטיים.

נספח א' - מילון מונחים

"טרול" – טרולים הם אנשים שמטרתם להציק, לזעזע או להרגיז משתמשים אחרים ברשתות החברתיות. עם עשויים לכתוב הודעות מעציבות, מעליבות או מתקיפות בפורומים, תגובות, אתרי אינטרנט, רשתות חברתיות, ועוד, על מנת לגרום למשתמשים אחרים להגיב בצורה רגשית או להיכנס לוויכוחים.

"בוטים" – בוטים הם תוכנות אוטומטיות שמתוכנתות לבצע משימות מסוימות ברשת באופן עצמאי. הם יכולים לבצע מגוון רחב של פעולות, כמו לסרוק דפים באינטרנט, לשלוט בחשבונות ברשתות חברתיות, לשלוח הודעות אוטומטיות, ועוד. בוטים יכולים לשמש למגוון מטרות, כמו ניתוח נתונים, שיווק, ואף פעילות זדונית כמו הפצת דואר זבל, איסוף מידע, הסתה ועוד.

"לינק" – מילה לועזית להפנייה או קישור לאתר אינטרנט. זה מאפשר למשתמשים לנווט בין דפים ומשאבים שונים ברשת האינטרנט.

"אימות דו-שלבי" – מדובר בשיטת זיהוי ואימות חזקה, שידועה גם בשם **2FA** (ר"ת של 2 **Factors Authentication**), שיטה שבה נדרשים שני מקדמי זיהוי על מנת לאמת את זהותו של משתמש בעת הגישה לחשבון או לשירות מסוים ברשת. דוגמאות לשני מקדמי זיהוי הינם "משהו שרק המשתמש יודע" (כגון קוד או סיסמה), ו"משהו שנמצא רק בבעלותו של המשתמש" (כגון טלפון נייד או טוקן – שזה אמצעי אבטחה פיזי). למעשה, שיטת אימות דו-שלבי עובדת בצורה כזאת:

- שלב ראשון – המשתמש מזין את שמו ואת סיסמתו באתר או באפליקציה.
- שלב שני – המשתמש מקבל הודעה לטלפון הנייד שלו עם קוד אימות זמני שנשלח בהודעת טקסט (**SMS**), והוא נדרש להזין את קוד האימות הזמני באתר או באפליקציה כדי להשלים את תהליך הזיהוי ואימות, וכניסה לאתר או לאפליקציה.

"מנגנון CAPTCHA" – ר"ת של **Completely Automated Public Turing Test to Tell Computers and Humans Apart**). מדובר במנגנון הגנה שמטרתו לוודא שהמשתמש הוא אדם ולא בוט (תוכנה אוטומטית). המנגנון משמש למניעת הונאות ופעילות זדונית באתרים ובשירותים ע"י בוטים שמבצעים פעולות אוטומטיות, כמו שלית דואר אלקטורני, יצירת חשבונות באופן אוטומטי, הפצת תוכן פרסומי, ואף פעולות זדוניות כגון הפצת מידע כוזב, איסוף נתונים רגישים, ועוד.

אימות רב-גורמי (MFA)" – ר"ת של **Multi-Factor Authentication**. זהו תהליך של אימות זהותו של אדם, שמתבסס על לפחות שני אמצעי זיהוי ואימות, השייכים לקטגוריות הבאות:

- ידע (משהו שרק המשתמש יודע – למשל סיסמה), חזקה (חפץ ייחודי שנמצא בחזקתו של המשתמש – למשל מכשיר הטלפון הנייד שלו), וטבועה (משהו שהוא חלק מטבעו הביולוגי וייחודי רק לו – למשל אמצעי ביומטרי כגון אצבע, כף יד, קול, זיהוי פנים, ועוד). אימות דו-שלבי (**2FA**) הינו דוגמה לאימות רב-גורמי.

"תקיפות סייבר למטרות השפעה ותודעה" – מה שידוע במונח המקצועי כ-**CNI** (ר"ת של **Computer Network Influence**). מדובר במתקפת סייבר שמטרתה לגרום להשפעה תודעתית למשל ע"י השחתת אתר אינטרנט, האלעת אתרים מזוייפים והפצת פייק ניוז, ועוד.

"גיבוי" – פעולה חד פעמית או שוטפת (אחת ליום, אחת לשבוע או לחודש), של העתקת מידע ממוחשב למקום אחר, לצורך מתן אפשרות לשחזורו במקרה שהוא נמחק או שובש. את הגיבוי ניתן לאחסן במחשב, התקן חיצוני נתיק (כגון דיסק קשיח נייד), סביבת ענן, ועוד. דוגמאות לגיבוי בענן, זה כאשר משתמש שומר את המידע שלו בענן (כגון תמונות).

"NIST" – ר"ת של **National Institute of Standards and Technology**. מדובר במכון התקנים האמריקאי שמספק מסגרות ותקנים שונים במגוון תחומים.

"BCP" – ר"ת של **Business Continuity Plan**. מדובר בתוכנית לניהול המשכיות עסקית, שמטרתה לוודא שהארגון ממשיך את עסקיו "כרגיל" גם בעת אירועי קיצון.

"DRP" – ר"ת של **Disaster Recovery Plan**. מדובר בתוכנית להתאוששות מאסון, שמטרתה לספק הנחיות להתאוששות מאירועי קיצון, שקשורים לפן הטכנולוגי (מערכות מידע ותשתיות).

"מתקפת מניעת שירות (DoS)" – מתקפת **DoS** (ר"ת של **Denial of Service**) הינה מתקפת סייבר שמטרתה למנוע שירות תקין של ארגון (כגון תקשורת, אתרי אינטרנט, אפליקציה, או שירות לוגיסטי שניתן במסגרת פעילות של ארגון).

"מתקפת מניעת שירות מבוזרת (DDoS)" – מתקפת **DDoS** (ר"ת של **Distributed Denial of Service**) הינה מתקפת סייבר (כגון **DoS**), שתמבצעת במקביל מכמה מקורות שונים, על מנת להקשות על הארגון להתמודד עם המתקפה.

נספח ב' – כיצד ניתן לזהות האם מדובר בלינק (קישור לאתר אינטרנט) זדוני?

זיהוי לינקים זדונים ברשתות חברתיות הוא קריטי למניעת הונאות או התפקות סייבר. להלן כמה דרכים לזהות ולהימנע מלינקים כאלה:

1. **תנסו לבחון את כתובת האתר (**URL**)** – תבדקו היטב את כתובת האתר של הלינק או ה-**URL** (ר"ת של **Uniform Resource Locator**). כתובת **URL** חשודה עשויה להכיל תווים מוזרים, טעויות כתיב, או להיראות כמו גרסה מעוותת של כתובת אתר אמיתית.

2. **תצוגה מקדימה** – רבות מן הרשתות החברתיות מציעות תצוגה מקדימה של הדף שאליו הלינק מפנה. הסתכלו על התצוגה המקדימה ובדקו אם היא נראית מקצועית ואמינה. אם יש חשש או ספק, ניתן להיעזר באיוגד הישראלי לאינטרנט (קו סיוע של איגוד האינטרנט – 054-8858911).

3. **תיאור הלינק** – תבדקו האם התיאור שמצוי ליד הלינק רלוונטי ומתאים לתוכן? לינקים זדוניים לעתים קרובות מצויידים בתיאורים מטעים או עם הרבה שגיאות כתיב.

4. **אמינות המפרסם** – תבדקו את המפרסם של הלינק. האם זה חשבון מוכר ומהימן, או חשבון חדש שאינכם מכירים? חיפוש קצר במנועי חיפוש (כגון גוגל) יכול גם לאתר האם מדובר בחשבונות פיקטיביים זדוניים.

5. **בדיקת הכתובת בכלים מקוונים** – ישנם כלים מקוונים שמאפשרים לבדוק את האמינות של כתובת אתר. כלים אלה יכולים להציע מידע על האתר והאם הוא נחשב למזיק או זדוני. אחד מהכלים המפורסמים הינו **VirusTotal**. ניתן להשתמש בלינק הבא:
https://www.virustotal.com/gui/home/url

6. **תגובות אחרות** – תקראו את התגובות של משתמשים אחרים ללינק. האם ישנן תגובות שמציינות שהלינק זדוני, או שאנשים לחצו ולא קרה כלום מה שיכול להעורר חשד.

7. **אם יש ספק אז אין ספק** – אם יש לכם ספק, עדיף להימנע מלחיצה על הלינק. במקרה של ספק, ניתן לחפש את הנושא באופן ישיר באמצעות מנועי חיפוש מקוונים (כגון גוגל או בינג).

8. הזהירות ובדיקה מיטבית של לינקים ברשתות חברתיות יכולות לעזור למנוע נזקים ולשמור על בטיחותכם ברשת.

נספח ג' – מקבץ הנחיות אבטחת מידע והגנת הפרטיות לארגונים

להלן רשימת תיוג של הנחיות אבטחת מידע והגנת הפרטיות שיכולה לסייע לארגונים ולחזק את חוסן הסייבר הארגוני והלאומי:

1. העלו את המודעות בנושא אבטחת מידע והגנת הפרטיות בקרב כלל עובדי החברה (ובמידת הישימות גם עבור הספקים והשותפים העסקיים שלכם).
2. תבחנו את מדיניות ניהול ההרשאות שלכם (תשימו דגש על עובדים/עובדות שיצאו למילואים). תשימו חוקי ניטור על אותם משתמשים (גם אם הם יכולים לגשת לרשת הארגון מרחוק).
3. הניחו כי בקבוצות ווטסאפ ישנם אנשים שאינכם מכירים, ואולי אף גורמים עוינים שהצליחו להתסנן. הקשיחו את מדיניות ניהול המשתמשים בקבוצה (כמות מנהלי הקבוצה, הרשאה להוסיף משתמשים, האם אפשר לפרסם הודעות, וכדומה).
4. העדיפו למסור מידע רגיש או לבצע פעולות רק בהתקשרות לא ישירה/מקוונת. בחנו יישום מנגנון **Call-Back** עבור תהליכים רגישים.
5. תקיימו דיון בנושא אם אנשי אבטחת המידע, הביטחון, ה-**IT**, הגנת הפרטיות, משאבי אנוש, ניהול סיכונים, המשכיות עסקית, שרשרת האספקה, ויתר בעלי העניין הרלוונטיים.
6. הגדירו לעובדים כיצד ניתן לדווח ו/או להתייעץ אתכם. ניתן לפרס הודעה בנוסח "בכל שאלה, ניתן לפנות אלינו בכתובת המייל הבאה: **security@mydomain.com**"
7. הגידרו לספקים ולשותפים העסקיים מיהם אנשי הקשר בנושא היבטי אבטחת מידע והגנת הפרטיות, ומהם דרכי ההתקשרות לדיווח על אירועים או חשד לאירועי סייבר.
8. תבצעו סקרי ספקים עבור הספקים הקריטיים שלכם, בייחוד כאלו שמחזיקים או יש להם גישה למאגרי מידע שלכם.
9. תבצעו סריקות פגיעויות שוטפות על מערכי המחשוב שלכם (כולל בענן), לצורך זיהוי פגיעויות וסגירת הפרצות מהר כלל הניתן.
10. תבצעו בדיקות חוסן על השירותים המונגשים שלכם, ועל האתרים החיצוניים, לוודא שאין חולשות שיאפשרו לאויב לנצל לרעה ולגרום נזקים.
11. תנחו את כל העובדים שלכם להשתמש במייל פרטי עבור כל היוזמות של התנדבות, תרומות, וכדומה.

נספח ד' – חברות ייעוץ ומומחי סייבר והגנת הפרטיות שניתן להתייעץ איתם

ישנם ערוצים רשמיים, דוגמת אתר מערך הסייבר הלאומי והרשות להגנת הפרטיות.
כמו"כ ישנו פורטל מבית איגוד האינטרנט הישראלי, אשר כולל מוקד ותמיכה באזרחים לצד גופים אלו, ישנן מספר חברות אשר התנדבו לסייע לגופים פרטיים ולאנשים פרטיים אשר מעוניינים לקבל סיוע בנושא.

בערוץ חדשות סייבר בטלגרם של ארז דאסה היקר, ניתן למצוא רשימה של כל החברות ייעוץ ומומחי סייבר שמוכנים לסייע לארגונים.

ניתן להגיע לרשימה בקישור הבא:
https://docs.google.com/spreadsheets/d/1Yq9gbYYW1-ogMzd7dEYrt1DfQ0TMSUmuxfELoTFKAJk/edit?usp=drivesdk