16 אוקטובר 2024

י"ד תשרי תשפ"ה

הנדון: מגמות ותובנות בממד הסייבר בקרב משרדי עו"ד

רקע

1. החל מחודש ינואר 2023 ועד עד השבוע הראשון לחודש אוקטובר 2024 (כולל), מערך הסייבר הלאומי טיפל במעל 45 אירועי סייבר במשרדי עורכי-דין[1].
2. מספרם היחסי הרב של האירועים לצד "הצלחות" של תוקפים אשר באות לידי ביטוי בהצפנת הרשת ובגניבת מידע רב, מצביעות על העובדה שסקטור זה מהווה 'מטרה קלה' ואטרקטיבית עבור תוקפים הפועלים במרחב הסייבר ממניעים שונים.
3. בסקירה זו יוצגו נתונים אודות אירועי סייבר אשר דווחו או טופלו על ידי מערך הסייבר הלאומי, לצד סקירת המלצות נקודתיות וזאת במטרה לסייע בצמצום היקף התופעה בקרב פלח זה.
4. המסמך מתייחס לאירועי סייבר שדווחו למערך הסייבר החל מחודש ינואר 2023 עד השבוע הראשון לחודש אוקטובר 2024 (כולל) (להלן – "**התקופה הרלוונטית**").

מוטיבציית תוקפים (מדינתי ופשיעתי) לבחירה בסקטור זה כיעד מועדף

1. מניתוח אירועי הסייבר במשרדי עורכי דין בתקופה הרלוונטית, מסתמן כי הבחירה במשרדים אלו כיעד לתקיפה מאפשר השגת מספר מטרות מבצעיות שונות עבור תוקפים, מאחר שמדובר ב- "מרחב מאפשר", בין היתר, מהנימוקים הבאים: במקרים שונים נמצא כי מדובר בעסקים שלא אימצו עקרונות מקובלים לבניית ארכיטקטורה מאובטחת, כמו גם חוסר במודעות ובשלות לעקרונות הגנת מידע וסייבר.
2. ככלל, אין במרבית המשרדים גורם האמון על הגנת מידע וסייבר (CISO) אשר בעל ניסיון, ידע ומשאבים מספקים להעלאת חוסן ובניית מערכת הגנה "אפקטיבית" מפני תקיפות סייבר.
3. לאור פערי הגנה, תוקפים מצליחים לבצע הוצאה לפועל של תקיפות בעלות נמוכה, ותוך זמן קצר יחסית.

[1] בהתאם למגמה העולמית ניתן להניח כי מספר האירועים שהתרחשו בפועל גבוה יותר. באופן נקודתי, המגמה של תקיפת משרדי עורכי-דין במדינת ישראל דומה לזו שקיימת בארה"ב. לפי דו"ח לשכת עורכי-הדין האמריקאית (ABA) , בשנת 2023 כ-29% ממשרדי עורכי-הדין בארה"ב סבלו מסוג כלשהו של פרצת אבטחה.

4. נמצא כי לאחר חדירה לרשת משרד, התוקפים מצליחים בקלות להרחיב את היקף התקיפה תוך הגעה ל'יעד הזהב' (דוגמת תיבת דוא"ל, תיקיית קבצים רגישים או מסד נתונים בעל גישה לתיקי לקוחות).
5. מטבע הדברים, משרדי עורכי-דין מחזיקים מידע בעל עניין רב לתוקפים, דבר אשר מקנה להם יכולת להגיע להישגים הבאים:
   א. כלכלי - לשם סחיטה כספית או מכירת מידע שנגנב, דוגמת אירועי כופרה.
   ב. ריגול תעשייתי, דוגמת מידע אודות קניין רוחני או צפי להתממשות עסקת מיזוג גדולה אשר עשויה להשפיע על שווי מנייה.
   ג. מדיני, דוגמת איסוף מידע רגיש אודות יעדים לפעולה וגופים ביטחוניים.
6. בהתפלגות לפי וקטור החדירה באירועי הסייבר המדוברים, נמצא כי הרוב המוחלט של האירועים החל מהתחברות לתשתית ה-VPN\SSL VPN של המשרד. ההתחברות צלחה בשל מספר סיבות אפשריות:
   א. פרטי התחברות "חלשים" שניתן לפצח באמצעות ניחוש סיסמאות או שימוש במילון סיסמאות.
   ב. שימוש בתשתית VPN\SSL VPN בעלת פגיעות ידועה. כאשר התוקף הצליח להשמיש את הפגיעות, בין אם לשם תשאול מרחוק של סיסמת המשתמש וקבלתה באופן גולמי (Plaintext) או באמצעות שיטה אחרת.
   ג. רכישת פרטי התחברות שדלפו בעבר ונמכרו לגורמים שונים ברשת האפילה (Darknet). פעמים רבות הדלפת הסיסמה של המשתמש נבעה מתקיפה קודמת של מחשב עובד המשרד באמצעות כלי לקצירת נתוני גישה (Infostealer).
7. ניתן לראות מספר וקטורי תקיפה נוספים בסקטור זה:
   א. קיימת מגמה כללית על פיה כאשר חולשות מפורסמות באופן פומבי, ניסיונות ההשמשה שלהן בנכסים בהם קיימות אותן חולשות עולים.
   ב. ממשק RDP ומדפסת ושרת דוא"ל Exchange מוחצנים לעולם ללא יישום מנגנוני אבטחה מקובלים.
   ג. תוכנות לשליטה-וניהול מרחוק (RMM), דוגמת AnyDesk או TeamViewer, היו מותקנות בחלק ניכר מהמשרדים שהותקפו. דבר אשר הקל על המשתמש בביצוע פעולות המשך דוגמת תנועה רוחבית (Lateral Movement) ברשת המשרד, והדלפת מידע.
8. שכיח כי 'יעד הזהב' עבור תוקפים בעת חדירה לרשת הארגונית של משרדי עו"ד הינו שרת הדוא"ל של החברה (דוגמת שרת Exchange). ביחס לעצי התיקיות (Dirlist) בהן עושה החברה שימוש, תיבת המייל חושפת אפיקי אפשרות פעולה רבים, לרבות – גילוי ומיפוי לקוחות ועסקאות עתידיות, אפשרות להונאת מנכ"לים, שהייה מודיעינית ולמידת היעד.

פוטנציאל הנזק למשרדים בסקטור

1. פוטנציאל הנזק הנובע מחשיפת המידע הנשמר במשרדים מסוג זה, מהווה סיכון גדול מאוד לא רק למשרדים עצמם אלא גם ללקוחות המשרדים ובמקרים מסוימים גם לביטחון הלאומי. עבור גורמים עוינים משרדי עריכת דין מהווים

מושאי תקיפה נחשקים, בין היתר, מקום שמדובר במידע ערכי כגון – מידע מסחרי, קניין רוחני, מידע אישי ומידע אחר, הנשמר במשרד וחוסה תחת חיסיון עו"ד-לקוח.

2. במקרה שגורם עוין קיבל גישה לנכסים של המשרד, ההשלכות עשויות לכלול בין היתר:
   א. פגיעה במוניטין, אמון הציבור ולקוחות המשרד.
   ב. הליכים משפטים נגד המשרד ובעלי השליטה, לרבות תביעות צד-שלישי.
   ג. אכיפה מינהלתית ו/או פלילית.
   ד. שיבוש או מניעת אפשרות לקיומה של פעילות עסקית תקינה, לרבות אובדן הכנסות.
   ה. הליכים משמעתיים מצד ועדת האתיקה של לשכת עורכי-הדין.

גילוי הדעת של לשכת עורכי דין וקידום העלאת חוסן בסקטור זה על ידי מערך הסייבר הלאומי

1. על רקע אירועי סייבר שונים שהתרחשו בארץ ובחו"ל שכללו זליגת מידע אישי, בשנת 2022 פרסמה ועדת האתיקה הארצית של לשכת עורכי הדין גילוי דעת (את/22/1) בנושא אבטחת מידע המצוי בידי עורכי הדין, אשר גובש, בין היתר, בסיוע מערך הסייבר הלאומי. גילוי הדעת מציג המלצות לרף מינימלי של חובת אבטחת מידע על ידי עורך דין וקובע כי הפרתו עשויה בנסיבות מסוימות להוות הפרה של חובתו האתית של עורך הדין בקשר עם חובת הסודיות וחיסיון עו"ד -לקוח [2].
2. מערך הסייבר רואה חשיבות ביישום האמור בגילוי הדעת כאמצעי חשוב בהעלאת רמת הגנת הסייבר במשרדי עו"ד,
3. ניסיונו של מערך הסייבר בטיפול באירועי סייבר במשרדי עו"ד מלמד על כך שתוקפים מיעדים את תקיפותיהם למשרדי עורכי דין בהיקפים שונים ובעלי התמחויות שונות.
4. גודל המשרד אשר נמדד לפי כמות עורכי הדין המועסקים בו, בדרך כלל משליך ישירות על כמות לקוחותיו ועל היקף המידע הרגיש המצוי ברשתות המחשוב של המשרד. עם זאת, ייתכן בהחלט שמידע רגיש ואף מידע בעל רגישות מיוחדת ובהיקפים גדולים יוחזק גם במשרדים בעלי היקף בינוני וקטן.
5. הניסיון כי מלמד משרדים קטנים ובינונים נוטים לעשות שימוש רווח יותר בגורמי מיקור-חוץ לשם קבלת שירותי IT והגנת מידע וסייבר. בד ובד, התגלה כי אין אחידות בדרישות הגנת מידע וסייבר מצד במשרדים מול גורמים אלו.
6. בעקבות עלייה בכמות תקיפות הסייבר נגד משרדי עורכי-דין, מערך הסייבר הלאומי מקדם מערך הסייבר הלאומי פעילות להעלאת חוסן בקרב סקטור זה, לרבות באמצעות קיום פגישות וקידום פעילות משותפת בנושא עם לשכת עורכי הדין.

[2] את/1/22, "גילוי דעת מקדים בדבר אבטחת המידע המצוי בידי עורכי הדין" (להלן – **גילוי הדעת**). https://www.israelbar.org.il/UpLoadFiles/ethics_committee_opinion_1-22_full.pdf.

7. בין היתר, תואם כי הלשכה תהווה גורם באמצעותו יפיץ מערך הסייבר תוצרים ותובנות מקצועיות (דוגמת התרעות) לכלל עורכי הדין המאוגדים תחתיה. .
8. כן דובר על החשיבות בריענון ויישום גילוי הדעת בנושא אבטחת מידע והגנת סייבר על-ידי כל הנוגעים בדבר.
9.

דרכי התמודדות מומלצות

להלן המלצות מרכזיות למשרדים בהיבטי אבטחת מידע והגנת סייבר, על רקע תובנות מניתוח אירועי הסייבר אשר לוו על ידי מערך הסייבר.

כידוע, גילוי הדעת שפורסם על ידי ועדת האתיקה הארצית , הציג את החובות החלות על עורך דין ביחס לשמירת סודיות המידע המצוי בידיו בראי העידן הטכנולוגי המודרני. [3]

בפרק זה נסקור מספר המלצות הגנה, כאשר לשם הנוחות, לצד כל המלצה יוצג הסעיף הרלוונטי מגילוי הדעת.

ככלל, מומלץ לתעדף תחילה את אימוץ ההמלצות תחת סעיף "ד(6).3. עבודה מרחוק – הגנה על חיבור מרחוק אל רשת המשרד (לעובדים, לספקים ולצורך שירות תמיכה מרחוק).[4]

שימוש באמצעים טכנולוגים מקובלים להגנה על מחשבים, מכשירים ניידים ושרתים [סעיף ד.(3). בגילוי הדעת].

1) מומלץ לוודא כי המשרד עושה שימוש בפתרון XDR, הכולל שירותי ניטור חיצוניים (MDR) על בסיס 24/7. בכלל זה, מומלץ לבצע באופן תקופתי סימולציה ב"הפתעה" של אירוע סייבר במשרד, ולבחון את אפקטיביות המענה מצד ספק שירותי הניטור.
2) מומלץ לוודא כי נעשה שימוש בתוכנות שריישיון השימוש בהן בתוקף. החשיבות של תוכנות ברישוי היא שהן מקבלות עדכוני אבטחה באופן שוטף. תוכנות ללא רישוי (או "פרוצות") אינן מקבלות עדכונים בכלל ועדכוני אבטחה בפרט. בתוכנות בהן יש אפשרות כזו, יש לקבוע "עדכוני אבטחה אוטומטיים". בדגש על מערכות הפעלה, אמצעי אבטחה (דוגמת אנטי-וירוס) וכלי אופיס.
3) מומלץ לבצע הקשחה בהתאם לעקרונות מקובלים, דוגמת הסרת רכיבי תוכנה שאינם נדרשים, ביטול פונקציונאליות שאינה נדרשת בשגרה (דוגמת פרוטוקול SMB v1.0), חסימת גישה ל-CMD, Windows Script Host (WSH) וה-PowerShell. כמו כן מומלץ להיעזר במתודולוגיות מקובלות להקשחה דוגמת CIS (רמה 2 כמינימום מומלץ)[5] ו-DISA STIG (רמה 2 כמינימום מומלץ).[6]

---

[3] את/1/22, "גילוי דעת מקדים בדבר אבטחת המידע המצוי בידי עורכי הדין" https://www.israelbar.org.il/UpLoadFiles/ethics_committee_opinion_1-22_full.pdf.

[4] יצוין כי מסמך זה אינו בא להחליף את הנחיית ועדת האתיקה הארצית את/1/22, וכי במקרה של סתירה או צורך בפרשנות, החלטת ועדת האתיקה הארצית היא זו שמחייבת.

[5] CIS Benchmarks List
https://www.cisecurity.org/cis-benchmarks

[6] DISA STIG

4) מומלץ לנטרל באופן גורף את השימוש בפקדי MACRO בכלי האופיס. במקרה של ניסיון צרופה/קובץ להפעיל את הפקדים יש להדריך את המשתמשים להימנע מלעשות כן, ולדווח מידית לגורם האבטחה במשרד.
5) מומלץ לוודא כי מסמכים המגיעים מחוץ למשרד נפתחים במצב PROTECTED MODE. יש לחשוד בכל מסמך או הודעה המנסים לשכנע את המשתמש להסיר אמצעי הגנה אלו.
6) מומלץ להפעיל את מנגנון Pop-Up Blocker המובנה בדפדפן. פעולה זו מצמצמת באופן ניכר קפיצת חלונות אשר עשויים להיות נגועים בפוגענים.
7) מומלץ לנטרל הפעלת קוד JAVASCRIPT בקורא קבצי PDF.
8) מומלץ להפעיל את מנגנוני האבטחה המובנים במערכת ההפעלה דוגמת המנגנונים הבאים הקיימים במערכת הפעלה Windows 10 ומעלה: Attack Surface Reduction (ASR) Rules, Credential Guard, Secure Bot, AppLock, Windows Firewall, Defender Application Guard.

הגנה על הרשת הארגונית [סעיף ד.(4).1. בגילוי הדעת].

1) מומלץ לוודא כי במבואות רשת המשרד מותקן רכיב אבטחה מסוג NGFW, אשר מנגנוני האבטחה הבאים מופעלים ומוגדרים בהתאם להמלצות היצרן:
2) IPS, Anti-Virus, Sandbox, DLP, URL Filtering, Threat Intelligence (TI)
3) מומלץ לוודא סגמנטציה של רשת המשרד (Network Segmentation), כאשר לטובת שליטה ובקרה מומלץ לוודא כי התעבורה בין הסגמנטים תעבור דרך ה-NGFW. כמו כן, מומלץ לוודא כי כל נכס בעל פונקציונליות עסקית מסוימת ממוקדם בסגמנט ייעודי.
4) מומלץ לבצע טיוב עתי של חוקת הגישה בהתאם לעקרון Least Access Privilege.
5) מומלץ שלא לחשוף ממשקים דוגמת RDP, Exchange, מדפסות וכדומה ישירות לעולם. כחלופה ניתן לעשות שימוש ב-VPN\SSL-VPN.
6) מומלץ לוודא כי ברשות המשרד ניטור רציף לאיתור אירועי סייבר. ניתן לעשות שימוש בשירות SOC\MDR חיצוני, העומד בדרישות מתודת SOC-CMM[7] רמה ארבע ומעלה.

ניהול הרשאות גישה וחשבונות משתמשים [סעיף ד.(5).1. בגילוי הדעת].

1) מומלץ לוודא כי כברירת מחדל המשתמשים עושים שימוש בהרשאות נמוכות (Least Privilege). כלומר, לא יעשה שימוש בהרשאות מנהל מערכת בעמדות הקצה וכדומה.
2) מומלץ לוודא כי היקף הגישה למידע למשתמשים יהיה בהתאם לצרכים העסקיים (Need to Know). סוגיה זו חשובה ביתר שאת בעת התמודדות עם כופרה (Ransomware), כאשר צמצום הגישה למידע משמעותו הישירה צמצום אפקט הנזק הפוטנציאלי.

https://public.cyber.mil/stigs/
[7] SOC-CMM
https://www.soc-cmm.com/

3) מומלץ לוודא כי לא נעשה שימוש בסיסמאות ברירת מחדל ו/או סיסמאות שדלפו בעבר (Credentials Stuffing) ו/או סיסמאות חלשות. כמו כן, יש להנחות את המשתמשים להימנע משימוש בסיסמאות הנסמכות על מידע אישי (דוגמת שם הילד/ה). כאשר ההמלצה היא לעשות שימוש בסיסמה של לפחות 11 תווים עבור חשבון משתמש רגיל ו 16 תווים לחשבון מנהל מערכת, כאשר אין חובה כיום לממש סיבוכיות לסיסמה. לשם שיפור יכולת המשתמשים לזכור את הסיסמה מומלץ להציע להם לעשות שימוש באנלוגיות משירים וספרים שהם אוהבים.

הגנה על ערוץ הדואר האלקטרוני [סעיף ד.(6).1. בגילוי הדעת].

1) מומלץ לוודא כי ברשות המשרד מערכת או שירות חיצוני לסינון דוא"ל ספאם.
2) מומלץ לוודא כי המשרד הגדיר רשימת סוגי צרופות מותרים לכניסה בערוץ דוא"ל, תוך חסימה של צרופות בעלות רמת סיכון גבוה (דוגמת קבצי אופיס עם מאקרו, סקריפטים, קבצים בינאריים, צרופה עם נוזקות, צרופות מוצפנות, צרופות בעלות גודל חריג).
3) מומלץ לוודא ברשות המשרד מערכת או שירות חיצוני המסוגל לאתר ולהסיר או לחסום קישורים (Links) לאתרים בעלי מוניטין נמוך (דוגמת אתרים המשויכים לקמפייני תקיפה מוכרים, ספאמרים).
4) מומלץ לוודא כי בעת קבלת דוא"ל מחוץ למשרד מתווסף להודעה סימון בולט כי מדובר בהודעה ממקור חיצוני, וכי כברירת מחדל אין לבטוח בשולח ובמהימנות ההודעה.

הגנה על ערוץ שירותי גלישה [סעיף ד.(6).2. בגילוי הדעת].

1) מומלץ לוודא כי ברשות המשרד מערכת או שירות חיצוני לסינון גלישה (URL Filtering), תוך חסימה של גישה לאתרים בעלי מוניטין נמוך (דוגמת אתרים המשויכים לקמפייני תקיפה מוכרים, ספאמרים).
2) מומלץ לוודא כי המערכת או השירות חיצוני כוללים יכולת הרצת תכנים מרחוק (שלא על הדפדפן הפעיל בעמדת הקצה). טכנולוגיה המוכרת גם כ-RBI. וזאת במטרה לוודא שבמקרה של התפרצות נוזקה היא לא תפגע במערכות המחשוב במשרד.
3) מומלץ להגדיר קבלת התראה במקרה של חריגות בגלישה, דוגמת נפחי תעבורה חריגים, גלישה שלא בשעות העבודה, מספר פעילויות (Sessions) ממחשב יחיד החורג את הממוצע המקובל, שימוש באפליקציות לא שגרתיות לאופי הפעילות במשרד.
4) מומלץ לוודא כי המשרד הגדיר רשימת סוגי קבצים מותרים לכניסה בערוץ שירת הגלישה, תוך חסימה של קבצים בעלי רמת סיכון גבוה (דוגמת קבצי אופיס עם מאקרו, סקריפטים, קבצים בינאריים, צרופה עם נוזקות, צרופות מוצפנות, צרופות בעלות גודל חריג).

עבודה מרחוק – הגנה על חיבור מרחוק אל רשת המשרד (לעובדים, לספקים ולצורך שירות תמיכה מרחוק) [סעיף ד.(6).3. בגילוי הדעת].

1) מומלץ לוודא כי התקנת עדכוני אבטחה (פאצ'ים) ברכיב ה-VPN\SSL-VPN תתבצע עד 24 שעות קלנדריות מפרסום. במקרה של ימים ללא פעילות במשרד ו/או בגוף התמיכה החיצוני, מומלץ לנתק את רכיב ה-VPN\SSL-VPN מרשת האינטרנט עד להשלמת התקנת עדכון האבטחה בהצלחה.
2) מומלץ לוודא אכיפה כי התחברות מרחוק תאופשר רק בכפוף להשלמת אימות רב-גורמי (MFA) בהצלחה.
3) מומלץ לוודא כי לא הנעשה שימוש במשרד בפלטפורמות ניטור ושליטה מרחוק (RMM) העוקפות את רכיב ה-VPN\SSL VPN . במקרה של אילוץ תפעולי, יש לוודא כי נעשה שימוש בפלטפורמות תמיכה מרחוק בעלת רישיון רשמי, התוכנה מורדת מאתר היצרן הרשמי בלבד, וכי בסיום קבלת התמיכה מרחוק פעילותה מנותקת בצד המשרד.
4) מומלץ להגביל גישה לרכיב ה- VPN\SSL VPN לכתובות IP המשויכות למדינת ישראל (GEO Location).
5) מומלץ לבצע סקירה עיתית של רשימת חשבונות המשתמשים המורשים לגשת מרחוק, ולהסיר או לכל הפחות לנטרל חשבונות והרשאות שאין צורך עסקי בהם (דוגמת עובדים שעזבו או עובדים בחופשה ממושכת).

ספקים ו – "שרשרת אספקה" [סעיף ד.(8). בגילוי הדעת].

1) מומלץ להחיל את הדרישות הבאות בהסכמי ההתקשרות מול הספקים:
א. התחברות למשאבי מחשוב בצד הספק, ובצד המשרד, תתבצע בכפוף להשלמת אימות רב-גורמי (MFA) בהצלחה.
ב. במקרים בהם משרד מאחסן מידע רגיש אצל צד שלישי, מומלץ לוודא כי: 1) לגורם המאחסן קיימת התקשרות מול חברת IR. 2) לוודא קיומו של מנגנון שיפוי מוסכם מול הגוף המאחסן.
ג. התקנת עדכוני אבטחה למערכות הספק החשופות לאינטרנט ישירות תתבצע בהקדם האפשרי או לכל המאוחר עד 24 שעות קלנדריות מפרסום.
2) מומלץ לוודא שמדובר בספק אשר עומד בדרישות מתודת שרשרת האספקה של מערך הסייבר הלאומי. https://www.gov.il/he/pages/supply_chain_guide

חשיבות הגיבוי למידע [סעיף ד.(9).1. בגילוי הדעת].

1) מומלץ לוודא מעבר לשיטת הגיבויים הקיימת במשרד, כי נעשה שימוש בנוסף בשירות גיבוי רציף של מידע לענן ציבורי (Continuous Backup), הכולל ניהול גרסאות (Version Control), יכולת מובנית להתמודדות עם כופרה, ושמירת מידע לתקופה קצובה בטרם מחיקה או שינוי.
2) מומלץ לוודא כי נעשה שימוש באסטרטגיית הגיבויים 1-2-3:
1 – אחסנו גיבוי אחד במקום מרוחק. בעדיפות לאחסון במערכת או שירות היוצרים נתק פיזי או לוגי (לכל הפחות) בין הגיבוי, לרשת האינטרנט.
2 – שמרו את המידע לפחות על שני סוגי מדיה שונים ונפרדים.
3 – ודאו קיומם של 3 עותקים של המידע; עותק ראשי ושני גיבויים.

3) מומלץ לוודא שחזור תקופתי ומדגמי של מידע, וזאת במטרה לוודא כי ניתן יהיה לעשות שימוש בגיבויים ביום פקודה.
4) מומלץ לוודא כי המידע המגובה מוצפן טרם ביצוע הגיבוי בפועל. את סיסמת הגיבויים יש לשמור בכספת או אמצעי אחר, תוך הימנעות משמירת הסיסמה במערכות המחשוב של המשרד.

היערכות לאירוע סייבר [סעיף ד.(9).2. בגילוי הדעת].

1) מומלץ לוודא כי ברשות המשרד הסכם תקף מול חברת IR (חברה העוסקת בתגובה לאירוע סייבר). בכל מקרה בו חווה הגוף אירוע סייבר מומלץ לפנות למערך הסייבר הלאומי, אשר בכוחו לסייע בטיפול באירוע ו/או להפנות לרשימת חברות IR אשר מרוכזת אצלו, בהתאם לנסיבות המקרה.

רשימת חברות IR לדוגמה:

https://www.gov.il/he/pages/forom_ir_final_list

2) מומלץ לוודא כי ברשות חברת ה-IR מיפוי עדכני של מערכות המחשוב של המשרד, לרבות ספקי שירותי מחשוב חיצוניים.
3) מומלץ לבחון לפחות אחת לחצי שנה במשותף עם חברת IR את רמת הכשירות והמוכנות של המשרד להתמודדות אירוע סייבר.

תורת ההגנה בסייבר - כללי

מומלץ גם להטמיע במשרד את תורת ההגנה מטעם מערך הסייבר הלאומי
https://www.gov.il/he/pages/cyber_security_methodology_2

*** סוף מסמך ***