26 מרץ 2019
י"ט אדר ב תשע"ט
סימוכין: ב-ס-875

המלצות הגנה בסייבר לקראת פעילות "OpIsrael"

רקע

בתאריך 7 לאפריל 2019, ובימים שלפניו ואחריו (ככל הנראה החל מ- 4/4/2019), צפויה פעילות התקפית אנטי ישראלית מתוכננת במרחב הסייבר, פעילות המוכרת בשם "OpIsrael". פעילות זו מתבצעת מזה מספר שנים על ידי קבוצות האקטיביסטים מרחבי העולם ובעיקר ממדינות ערב ומדינות אסלאמיות נוספות, אשר חרטו על דגלם פגיעה בגופים ישראלים כתגובה לסכסוך הישראלי-פלשתיני.

קבוצות אלו מזהות עצמן עם קהילת האקטיביסטים המוכרת כ- Anonymous ועל פי רוב, פשעי הסייבר שהן יוזמות במהלך פעילותן מיועדים ליצירת הד תקשורתי, ניסיון להפחדת הציבור והעברת מסרים פוליטיים.

עיקר ההתקפות מתאפיינות בהשחתות אתרים, מתקפות מניעת שירות, חדירה למאגרי נתונים והדלפת מידע, גניבת מידע אודות משתמשים, הדלפת נתונים חוזרים מתקיפות קודמות, תקיפות כופר, ניצול חולשות ברכיבי IOT לתקיפות מניעת שירות מבוזרות ועוד.

השנה יתקיימו בחירות לכנסת ה-21 בתאריך ה-9/4, והאירועים עשויים להמשיך ולהתרחש סביב מועד זה ולאחריו. על פי רוב, ולאור ניסיון העבר, פעילויות אלו מתחילות בטרם המועד הרשמי המתוזמן, כאשר האירוע המרכזי מתרחש סביב ה- 7 באפריל ומתמשך מספר ימים לפני / אחרי מועד זה.

כפי שלמדנו בשנים האחרונות, ביצוע פעולות מניעה פשוטות ובסיסיות שיפורטו בהמשך, בשילוב פעילות שמבצע מערך הסייבר הלאומי, יכולות למזער למינימום את פוטנציאל הנזק מיריבים אלו. אנו ממליצים להיות ערוכים למתקפות שונות במסגרת קמפיין זה, ובפרט למתקפות מניעת שירות, לכל הפחות החל מ- 3/4/19 ועד 11/4/19.

מסמך זה מפרט המלצות הגנה לשם הערכות לקראת קמפיין OpIsrael והעלאת חוסן הגופים מפני איומי סייבר. חלק מההמלצות הינן טכניות, לכן אנו ממליצים לפנות לגורם מקצועי ומוסמך, אשר יוכל לסייע בהטמעתן.

נספחים א' וב' של המסמך מפרטים את ההמלצות וניתן להיעזר בהם להטמעת הבלים, עצמאית או בסיוע גורם מקצועי.

במקרה חירום, ניתן לפנות ל- CERT הלאומי במספר 119.

בברכה,

מערך הסייבר הלאומי

נספח א' - המלצות הגנה

1. הגנה על אתר האינטרנט

1.1. הגנה מפני תקיפת DOS/DDOS על אתר האינטרנט

1.1.1. כחלק מהגנה על אתר האינטרנט יש לוודא כי בוצעו במערכת ה-WAF הגדרות מתאימות ובכלל זה הפעלת BOT Mitigation, זיהוי חתימה ייחודית של התקיפה, חסימתה וכד'.

1.1.2. בהיעדר יכולת ארגונית מתאימה, מומלץ לבחון שימוש בשירותים מנוהלים Anti DDOS, WAF ע"י ספק התקשורת.

1.1.3. על מנת להתמודד עם תקיפת DDOS ניתן לשקול ביצוע פעולות נוספות:

1.1.3.1. חסימה של תעבורה ממדינות עוינות (ע"פ Geo Location) .

1.1.3.2. במקרים חריגים של תקיפה מחו"ל - חסימה גורפת של פניות מחו"ל.

1.1.3.3. חסימה של מקורות הידועים כבעלי מוניטין בעייתי/עוין (ב-FW) (IP Reputation).

1.1.3.4. זיהוי וחסימת מקורות כמו Anonymizer, TOR המאפשרים גלישה אנונימית.

1.2. הגנה מפני השחתת אתר

1.2.1. יש לעדכן גרסת CMS (Content Management Systems) כגון WordPress, Drupal, Joomla, וכו', ובפרט גרסאות התוספים (Plugins), בהם מצויות רוב החולשות, ולבצע עדכון לגרסת האפליקציה האחרונה שהופצה ועדכוני אבטחת מידע.

1.2.2. יש להקשיח חיבור ל-CMS - יעשה רק באמצעות חיבור TLS מאובטח והזדהות באמצעות שני אמצעי זיהוי (2FA).

1.2.3. יש להגביל גישה לשרת ומערכת ניהול התוכן למספר כתובות ה-IP המינימליות הנדרשות.

1.2.4. יש לבדוק את תקינותם של שדות הקלט באתר ולוודא כי אינם מאפשרים הכנסת תווים שאינם נדרשים או תואמים את הערכים הצפויים.

1.2.5. יש להפעיל ניטור אבטחתי ללוגים (Logs) על שרת ה-WEB לאיתור פניות חריגות, ובבדי לאפשר יכולת זיהוי תקיפות בדיעבד. יש להפעיל ניטור לוגים (Logs) במערכת ההפעלה לאיתור וזיהוי פעילות חריגה.

1.2.6. יש להקשיח את חוקי ה-Firewall כך שתתאפשר גישה רק בפרוטוקולים לגיטימיים.

1.2.7. במידת האפשר, יש לבצע סריקת אבטחה תקופתית לאיתור פעילות זדונית של גורמים חיצוניים, כגון Waterhole.

1.2.8. מומלץ להכין מראש דף אינטרנט חליפי אשר ישמש להחלפת האתר הנתקף בעת הצורך.

1.2.9. מומלץ לשקול אפשרות ניתוב התעבורה דרך מסננים מובנים של חברת האחסון או ספקית התקשורת.

1.3. **<u>הגנה על שמות מתחם</u>**

1.3.1. על מנת לעשות שימוש בשם מתחם, יש להגדיר בNS) Name Server) שלו את כתובת ה-IP שבה פועל שם המתחם וכן לבצע את הפעולות הבאות:

1.3.1.1. מומלץ לבצע סקר למיפוי שרתי ושירותי ה-NS בהם נעשה שימוש.

1.3.1.2. מומלץ לוודא כי נעשה שימוש בלפחות שני שרתי NS נפרדים על תשתיות נפרדות.

1.3.1.3. מומלץ להגדיר התרעה על שינויים בהגדרות רשומת הDNS אצל הרשם ולבחון אפשרות לנעילת הרשומה הארגונית אצל הרשם.

1.3.1.4. בנוסף, יש לנטר את השינויים אשר נעשים בשרת הDNS באמצעות ממשק הניהול. הניטור יבוצע בהתאם לאופן ניהול השרת (מקומי בארגון או ספק האחסון).

1.3.1.5. יש לבצע בחינה עיתית של רשומות הDNS -הארגוניות הרלוונטיות לצורך זיהוי שינויים בלתי מורשים בהן.

2. <u>גיבוי ויכולת התאוששות</u>

2.1. יש לוודא ביצוע יומיומי של גיבוי חומרים בעלי חשיבות כגון: אתר האינטרנט, בסיסי נתונים, שרת הקבצים וכיו"ב. ביצוע הגיבוי נועד לאפשר שחזור מהיר של מידע במידת הצורך (אם המידע ימחק/יוצפן או ישובש).

2.2. יש לוודא שמירה של הגיבוי על מדיה נפרדת, במיקום נפרד ומאובטח. ככלל, מומלץ לבצע גיבוי במספר ערוצים במקביל (שירותי ענן, שרתי גיבוי, קלטות וכד').

2.3. במידה ואחסון הגיבוי המבוסס ענן מבוצע באמצעות שירותים מקוונים המאחסנים את הקבצים ע"ב האינטרנט, חשוב לוודא כי השרות מספק הצפנת הנתונים ואימות דו שלבי.

2.4. יש לבצע גיבויי תצורה לרכיבי תשתית ותקשורת (דוגמת: נתבים, FW, מערכות אבטחה ועוד).

2.5. יש לוודא קיום וריענון של תכנית אירגונית להתאוששות מאירוע סייבר.

2.6. יש לוודא עדכניות נוהל התאוששות ושחזור לגרסה תקינה בעת הצורך, במידת האפשר מומלץ לבצע בדיקה ולוודא שהשחזור עובד.

3. תהליכי מודעות ועבודה

3.1. תהליכי מודעות

מרחב הסייבר האישי מוכר לכולנו היטב. אתר אינטרנט אישי, דואר אלקטרוני פרטי ודואר אלקטרוני ארגוני, טלפון סלולרי, רשתות חברתיות – כל אלו כלים יומיומיים המשמשים אותנו לטובת העבודה ומהווים חלק חשוב בשמירת קשרים מקצועיים, אישיים וחברתיים.

העובד משתמש לטובת עבודתו באפיקים אלו, ומהווה לעיתים שלא במכוון אפיק כניסה מרכזי של התוקף לארגון. לכן, מומלץ להנחות את העובדים לשים לב לפעולות הבאות על מנת להישמר מפני גורמים עוינים:

3.1.1. אין להכניס התקנים חיצוניים למחשבים הניידים/נייחים.

3.1.2. יש להימנע מלהעביר פרטים אישיים או כל מידע אחר למקור לא ידוע.

3.1.3. יש לבדוק את פרטי השולח בדקדקנות, ייתכן ויש זיוף בשם השולח שיראה לגיטימי אך יפנה לאתר מתחזה.

3.1.4. יש להימנע מפתיחת צרופות (Attachments) מגורם שאיננו מוכר.

3.1.5. יש להימנע מכניסה לפרסומות שנראות חשודות כמו הצעה עסקית קוסמת, מוצר נחשק במחיר מפתיע או זכייה בפרס כספי. המודעה יכולה לשמש כפלטפורמה לדיוג (פישינג) ובלחיצה על המודעה להוביל למשל לאתר מתחזה.

3.1.6. יש ללמד את העובדים להיות חשדניים לסימנים חשודים העשויים להעיד על תקיפת סייבר.

3.1.7. יש לתדרך את העובדים כי במידה ונפלו קורבן למתקפה, עליהם לדווח באופן מיידי למנהל אבטחת המידע או לגורם ממחלקת ה-IT אשר יבצע בדיקה מקיפה ככל שניתן.

3.1.8. יש לחדד נהלים וערנות נותני שירותים ארגוניים, כגון מרכז התמיכה, SOC, IT וכיו"ב למתן תשומת לב לתקלות ואירועים חריגים ו/או חשודים.

3.2. היערכות ארגונית ותהליכי עבודה

3.2.1. יש לצמצם את רמת החשיפה של הארגון לאינטרנט למינימום הנדרש:

3.2.1.1. הגבלת גישה חיצונית לספקים, נותני שירותים ומשתמשים אשר אינם זקוקים לכך.

3.2.1.2. כיבוי תחנות עבודה אשר אינן בשימוש.

3.2.2. יש לחדד נהלי תגובה והיערכות לכלל הגורמים הרלוונטיים לתגובה לאירועי סייבר בארגון לטיפול מהיר ומיטבי.

3.2.3. אירועי OpIsrael הקרובים עתידים להתקיים סביב הבחירות לכנסת ה-21, ביום הבחירות יש להיערך לצוותי כוננות והיערכות ארגונית בהתאם לכל המשתמע מתזמון זה, לרבות עבודה ביום שבתון.

3.2.4. מערך הסייבר הלאומי מבצע הערכת מצב רציפה, לאורה יתכן ויבוצעו שינויים בהיערכות ו/או העלאת מצבי כוננות. הנכם מתבקשים להיות זמינים ולעמוד בקשר שוטף עם המערך.

3.2.5. מומלץ שלא להטמיע שינויים משמעותיים בסביבת הייצור סביב תקופה זו, על-מנת לצמצם את הסיכון לתקלות תפעוליות.

4. הגנה על תחנות קצה ושרתים

4.1. גלישה אינטרנטית מהווה אחד מאפיקי הכניסה המרכזיים של התוקף לארגון. על מנת להגן על תחנת קצה מפני האיומים הנ"ל, נדרש לשמור על היערכות תשתיתית והיגיינת רשת כמפורט בסעיפים שלהלן:

4.1.1. יש לוודא שעל כלל תחנות הקצה ו/או השרתים מותקן Anti-Malware \Anti-Virus. כמו כן יש לוודא כי ה-Anti-Malware \Anti-Virus מעודכן לגרסה האחרונה שהופצה על ידי הספק.

4.1.2. יש להתקין חומת אש (FireWall) אישית מעודכנת על תחנות הקצה.

4.1.3. יש לוודא כי מערכת ההפעלה המותקנת על כל תחנות העבודה /השרתים/ציוד קצה אחר מעודכנת בעדכוני האבטחה האחרונים של חברת Microsoft. מומלץ שלא להשתמש בגרסאות ישנות של מערכת הפעלה אשר אינן נתמכות ואינן מכילות את עדכוני האבטחה.

4.1.4. מומלץ לוודא שאפליקציות ותוכנות מדף מעודכנות בגרסה העדכנית ביותר של הספק. יש להקפיד על ביצוע עדכון מיידי של טלאי אבטחה אשר מופץ ע"י הספק. ככלל, מומלץ בהגדרות להגדיר עדכונים אוטומטיים.

4.1.5. יש לוודא כי העדכונים למערכת הפעלה, מוצרי אבטחה ו/או אפליקציות, מורדים מהאתר הרשמי של הספק. כמו כן, במידה וקיימת חתימה דיגיטלית של הספק יש לאמתה (SSL, המנעול בכתובת ה- URL המציין את תיקוף החתימה).

4.1.6. מומלץ לנטרל הרצת Power Shell בתחנות של משתמשי קצה, שאינם משתמשים בו באופן יומיומי ואינם זקוקים לו לביצוע עבודתם.

4.1.7. יש להקשיח את מערכות ההפעלה של תחנות העבודה, השרתים וציוד התקשורת לפי הנחיות יצרן, מומלץ לוודא שלא הופעלו שירותים (Services) שאינם נחוצים.

4.1.8. מומלץ ליישם פתרונות מתקדמים בתחנות קצה של משתמשים בעלי סיכון גבוה להתממשות חדירה, כגון קיבוע תצורה, הרצת קוד חתום בלבד, עבודה בתצורת Read Only בלבד וכיו"ב.

5. הגנה רשתית

5.1. ברשתות ארגוניות יש להסיר הרשאות עודפות במערכות הפעלה ואפליקציות, במסגרת זו:

5.1.1. יש למפות גורמים בעלי הרשאות אדמיניסטרטיביות ולצמצם היקף בעלי הרשאות אלו למינימום הנדרש.

5.1.2. יש לזהות האם ישנם חשבונות ברירת מחדל (Default accounts), לבחון את נחיצותם ולהסיר חשבונות שאינם נחוצים.

5.1.3. מומלץ לבצע סקירת הרשאות במערכות הליבה בארגון ולוודא כי הרשאות העובדים תואמות את הצרכים העסקיים. יש להסיר הרשאות-יתר.

5.2. מומלץ להטמיע פתרון LAPS – Local Administration Password Solution, לצמצום סיכון אסקלציית הרשאות של Local Admin.

5.3. מומלץ לוודא איסוף וניתוח לוגים בשרתים ובאפליקציות לטובת איתור ממצאים חשודים, העברת הלוגים למערכת הניטור המרכזית (SIEM, שו"ב וכיו"ב) וחידוד חוקים והתרעות במערכות אלו.

5.4. מומלץ לוודא עדכניות החוקים והחתימות במערכות האבטחה הארגוניות (FW, IDS, IPS, AV וכיו"ב).

5.5. מומלץ לטייב חוקי FW, במסגרת זו למחוק חוקים זמניים או לא רלוונטיים. כמו כן, לבחון Shadowing Rules וסדר כרונולוגי של חוקים על מנת לוודא את ההרשאות בפועל.

5.6. מומלץ למפות את כלל הקישורים והממשקים הקיימים בין הרשת הארגונית לרשתות חיצוניות ולוודא ניטור ומנגנוני הגנה מתאימים.

5.7. מומלץ לחסום פורטים ושרתים שאינם נדרשים לגישה לאינטרנט ולהגביל קצב תעבורה של פורטים ובפרט UDP.

5.8. מומלץ ליישם Ingress Traffic Filtering בתשתיות למניעת תקיפות DoS ולתקיפות זיוף כתובת המקור (IP spoofing).

5.9. מומלץ לתקף הגדרות נכונות של ה-Device Manager ולוודא כי לא מתאפשר חיבורם של:

5.9.1. כונן CD

5.9.2. תווך אוגר מידע (DOK)

5.9.3. רכיבים משדרים כגון Netstick, WiFi, Bluetooth

6. הגנה על מסדי נתונים ומאגרי מידע

6.1. מומלץ להצפין נתונים רגישים במסדי הנתונים.

6.2. מומלץ ליישם בקרות ואיתור אנומליות במסדי נתונים.

6.3. יש ליישם מדיניות גישה מחמירה למסדי הנתונים ובכלל זה:

6.3.1. מניעת שימוש בחשבונות אדמיניסטרטיביים ראשוניים כגון Root / SA.

6.3.2. ניהול תהליך שוטף לשינוי סיסמאות לחשבונות אדמיניסטרטיביים ראשוניים כגון Root / SA.

6.3.3. יישום הרשאות מינימאליות נדרשות עבור יישומים המשתמשים במסדי נתונים.

6.3.4. יישום הרשאות מינימאליות נדרשות עבור משתמשים אדמיניסטרטיביים המפתחים, מתחזקים ותומכים במסדי הנתונים.

7. סיסמאות ובקרת גישה

7.1. יש להפעיל מדיניות סיסמאות מורכבות בתחנות, שרתים וציוד רשת:

7.1.1. על הסיסמה להיות בת שמונה תווים לפחות ולכלול שימוש בתווים מיוחדים (כגון #$(@)!), דבר שיקשה על ניחושה.

7.1.2. יש לשמור את הסיסמה באופן מאובטח, אין לשמור במכשיר הסלולר, במחשב האישי או בפתק במשרד. ניתן לשנן או להצפין את הסיסמאות הנבחרות.

7.1.3. יש להקפיד שלא להשתמש בסיסמה אחידה או דומה לכל האפליקציות השונות.

7.1.4. יש לוודא שהסיסמה לא מרמזת או מקשרת לשם המשתמש, לתפקידו או לפרטים מזהים אחרים כגון שמות ילדים, תאריכי לידה, טלפונים, חיות מחמד, אשר ניתן למצוא בקלות ברשתות החברתיות.

7.1.5. בכל מקום המאפשר זאת – הן עבור הגישה לרשת וביצוע ה-login למכשיר, והן באפליקציות שמאפשרות זאת (כדוגמת Gmail, Whatsapp, Facebook) חובה להשתמש באימות דו שלבי (Two Factor Authentication).

7.1.6. יש להפעיל מנגנון הזדהות דו שלבית עבור לקוחות בתהליך ניהול הדומיינים, שינוי ועדכון פרטים.

7.1.7. כחלק מההערכות יש לבצע החלפת סיסמאות אדמיניסטרטיביות בשרתים חיצוניים ובשרתים רגישים.

8. הגנה על דואר אלקטרוני

8.1. הדוא"ל מהווה אפיק כניסה מרכזי של התוקף לארגון. על מנת להגן על הארגון מפני איום זה מומלץ לבצע את הפעולות המפורטות להלן:

8.1.1. מומלץ להטמיע הגנה על שרתי / תיבות מייל באמצעות אנטי וירוס ו/או מערכת SandBox ארגוני. כמו כן, מומלץ להשתמש בסנן דואר זבל (Spam). ניתן לרכוש שירותים אלו מספק האינטרנט.

8.1.2. מומלץ לחסום במערכות סינון הדואר כניסת קבצי הרצה כגון סיומות EXE, MSI, CAB, CSR, BAT ,RAR, VBS, SXR וכדומה. כמו כן, מומלץ לשקול חסימה של קבצים המכילים פקודות מאקרו או פתיחתם תחת נטרול מאקרו וב-Protected View.

8.1.3. מומלץ להפעיל בדיקת מדיניות DMARC בשרתי הארגון עבור הדואר הנכנס. כמו כן, לצורך מניעת התחזות התוקף בשם הארגון/העובד, מומלץ להטמיע מדיניות DMARC.

8.1.4. יש לנטר אנומאליות בהזדהות לתיבת דוא"ל הארגונית ובכלל זה ניסיונות הזדהות כושלים, מדינות מהן בוצעה ההזדהות, מספר עמדות קצה/מכשירים מחוברים, שעות התחברות וכד'.

9. הגנה על מרכזיות טלפוניה

9.1. בטלפוניה נייחת קיים סיכון TDoS. במקרים אלה ההתקפה מבוססת על העמסת הקווים של המרכזיות עד כדי הפלתם, או שיחות חוזרות ונשנות למספר/י טלפון באופן רציף, דבר המונע מהם להוציא ולקבל שיחות. התקיפות יגיעו בדרך כלל משיחות VOIP (Voice over IP) באמצעות פרוטוקול SIP – (Session Initiation Protocol) שאחראי על חיבור, ניטור וניתוק השיחה בשיחות VOIP. על מנת להיערך למקרים אלה יש:

9.1.1. לבדוק מול ספק הטלפוניה האם ניתן לרכוש שירות הגנה במידה והחיבור הוא באמצעות SIP-Trunk.

9.1.2. להתקין רכיב הגנה על מרכזיות – SBC – (session border controller) – זהו רכיב רשתי המשמש כ- FW עבור תשתית VOIP.

9.2. מומלץ לוודא כי מערכת הטלפוניה מוקשחת על פי המלצות היצרן.

9.3. מומלץ לוודא כי תהליך קבלת שירות התמיכה מרחוק מותנה בקבלת גישה מגורם הארגון וכן נעשה שימוש בתשתית מתאימה כדוגמת VPN והזדהות חזקה.

9.4. מומלץ שלא להסתמך על המספר המוצג על גבי המסך (Caller ID) לצורך ביצוע פעילויות רגישות כדוגמת מתן היתר גישה למערכות או חשיפת מידע רגיש עסקית. מומלץ לחזור לפונה למספר שהוסכם מראש במידה ואינך מכיר אותו, וכן לבחון אפשרות להוסיף פריט הזדהות נוסף כדוגמת סיסמה משותפת.

נספח ב' - המלצות להטמעה והפעלת כלי הגנת סייבר

תחום הגנה		רלוונטי	רלוונטי לא	עצמאית	גורם מקצועי	תחזוקה שוטפת
תחנות קצה, מחשבים אישיים ושרתים						
	התקנת Anti Virus/Anti-Malware			√	√	√
	התקנת חומת אש (FireWall)			√	√	√
	עדכון מערכת הפעלה והגדרת עדכונים אוטומטיים			√	√	√
	עדכון תוכנות ואפליקציות מהאתר הרשמי והגדרת עדכונים אוטומטיים			√	√	√
	נטרול הרצת PowerShell בתחנות משתמשי קצה				√	
	הקשחת מערכות הפעלה של תחנות עבודה, שרתים, ציוד תקשורת לפי הנחיות יצר ; ביטול Services שאינם נחוצים				√	
	יישום פתרונות מתקדמים כגון קיבוע תצורה, הרצת קוד חתום בלבד, עבודה בתצורת Read Only וכד'				√	
הגנה רשתית						
	הסרת הרשאות עודפות במערכות הפעלה ואפליקציות				√	√
	הסרת חשבונות שאינם נחוצים				√	√
	הטמעת פתרון LAPS – Local Administration Password Solution, לצמצום סיכון אסקלציית הרשאות של Local Admin.				√	
	הגדרת פעילות לוגים בשרתים ואפליקציות לממצאים חשודים, העברתם למערכות הניטור הארגוניות ; חידוד חוקים והתרעות במערכות.				√	√
	עדכניות החוקים והחתימות במערכות האבטחה הארגוניות (FW, IDS, IPS, AV וכיו"ב).				√	√
	טיוב חוקי FW, מחיקת חוקים זמניים/לא רלוונטיים, בחינת Shadowing Rules לבדיקת הרשאות בפועל.				√	
	ביצוע סקירת הרשאות במערכות הליבה בארגון ; לוודא שהרשאות העובדים תואמות את צרכי הארגון ; הסרת הרשאות-יתר.				√	√
	מיפוי כלל הקישורים והממשקים הקיימים בין הרשת הארגונית לרשתות חיצוניות ולוודא ניטור ומנגנוני הגנה מתאימים.				√	√
	בחינה והקשחת תשתית חיצונית החשופה למתקפות.				√	
	חסימת פורטים ושרותים שאינם נדרשים לאינטרנט, הגבלת קצב תעבורת פורטים ובפרט UDP.				√	
	יישום Ingress traffic filtering בתשתיות למניעת תקיפות DoS ולתקיפות זיוף כתובת המקור (IP spoofing).				√	
	הגדרת Device Manager				√	√
הגנה על מסדי נתונים ומאגרי מידע						
	1. הצפנת נתונים רגישים במסדי הנתונים. 2. יישום בקרות ואיתור אנומליות במסדי נתונים. 3. יישום מדיניות גישה מחמירה למסדי הנתונים ובכלל זה : • מניעת שימוש בחשבונות אדמיניסטרטיביים ראשוניים • ניהול תהליך שוטף לשינוי סיסמאות לחשבונות אדמיניסטרטיביים ראשוניים				√	

ניתן לשתף מידע המסווג "לבן" עם כל קבוצת נמענים, לרבות ערוצים פומביים

	• יישום הרשאות מינימאליות נדרשות עבור יישומים המשתמשים במסדי נתונים.						
סיסמאות ובקרת גישה							
הפעלת מדיניות סיסמאות מורכבת בתחנות, שרתים וציוד רשת	1. בחירת סיסמה המורכבת מאותיות, ספרות ותווים מיוחדים @#$%. 2. שמירה או הצפנה של סיסמאות במקום בטוח. 3. שימוש באימות דו שלבי (2FA). 4. שימוש בסיסמה שונה לכל אפליקציה/ תוכנה, שאינה מרמזת/מקושרת לפרט מזהה אישי.		√	√			
הגנה על דואר אלקטרוני							
	הטמעת Anti-Virus או Sandbox על שרתי/תיבות מייל. שימוש בסנן דואר זבל.					√	
	במערכות סינון דואר חסימת קבצי הרצה כגון: EXE, MSI, CAB, SXR, BAT, CSR וקבצים המכילים פקודות מאקרו					√	
	הגדרת רמת אבטחה גבוהה, כולל חשבונות Google, הכוללת קבלת התראות בעת התחברות לחשבון.				√	√	
	הטמעת מדיניות DMARC בשרתי הארגון					√	
	ניטור אנומאליות בהזדהות לתיבת הדואר של הארגון					√	
הגנה על מרכזיות טלפוניה מפני TDoS							
	בדיקה מול הספקית האם ניתן לרכוש שירות הגנה במידה והחיבור הוא באמצעות SIP-Trunk.				√	√	
	התקנת רכיב הגנה רישתי על מרכזיות - SBC.				√	√	
	הקשחת מערכת טלפוניה עפ"י המלצות היצרן.				√	√	
	קבלת שירות תמיכה מרחוק מותנה בקבלת גישה מגורם הארגון ושימוש בתשתית מתאימה כדוגמת: VPN והזדהות חזקה.				√		
	אין להסתמך על המספר המוצג על גבי המסך (Caller ID) לצורך פעילות רגישה. חייגו חזרה לפונה ובחנו אפשרות להוסיף פריט הזדהות נוסף (לדוגמה סיסמה משותפת).				√		
הגנה על אתר אינטרנט							
הגנה מפני תקיפת DOS/DDOS	1. הגדרות במערכת WAF והפעלת BOT Mitigation. 2. בחינת שימוש בשירותים מנוהלים Anti DDOS, WAF ע"י ספקית התקשורת. 3. לשקול חסימת תעבורה ממדינות עויינות או מקורות בעלות מוניטין עוין. 4. זיהוי וחסימת מקורות גלישה אנונימית כגון TOR, Anonymizer					√	
הגנה מפני השחתת אתר	1. עדכון גרסת CMS והתוספים (Plugin); עדכון גרסת אפליקציה ועדכוני אבטחה. 2. הקשחת חיבור ל CMS באמצעות חיבור TLS מאובטח והזדהות באימות דו שלבי (2FA). 3. הגבלת גישה לשרת ומערכת ניהול התוכן למינימום כתובות IP נדרשות. 4. בדיקת תקינות שדות הקלט באתר, שלא יאפשרו הכנסת תווים מעבר לערכים הצפויים. 5. הפעלת ניטור לוגים אבטחתי על שרת ה WEB ומערכת ההפעלה לאיתור פעילות חריגה ולזיהוי תקיפות בדיעבד. 6. הקשחת חוקי FW לאפשר גישה בפרוטוקולים לגיטימיים. 7. ביצוע סריקת אבטחה תקופתית לאיתור פעילות זדונית כגון Waterhole. 8. הכנת דף אינטרנט חלופי. 9. אפשרות לניתוב תעבורה דרך מסננים של חברת אחסון או ISP.					√	

הגנה על שמות מתחם	1. מיפוי שרתי ושירותי NS ווידוא שימוש בלפחות 2 שרתים נפרדים על תשתיות נפרדות. 2. הגדרת התרעה על שינויים בהגדרות רשומת ה-DNS אצל הרשם ובחינת אפשרות לנעילת הרשומה. 3. ניטור שינויים בשרת ה-DNS באמצעות ממשק הניהול. 4. ביצוע בחינה עיתית של רשומת ה-DNS לצורך זיהוי שינויים בלתי מורשים.				√	
גיבוי ויכולת התאוששות						
	ביצוע גיבוי יומי ואפשרות שחזור לחומרים חשובים (אתר, DB, קבצים אישיים).			√	√	√
	גיבוי במספר ערוצים במקביל: שרותי ענן, DOK, קלטות גיבוי וכד'			√	√	√
	גיבוי בשרותי ענן הכוללים הצפנת נתונים ואימות דו שלבי			√	√	√
	גיבוי במדיה נפרדת			√	√	√
	גיבויי תצורה לרכיבי תשתית ותקשורת כגון נתבים, FW, מערכות אבטחה ועוד.				√	
	קיום וריענון של תכנית אירגונית להתאוששות מאירוע סייבר. יש לוודא עדכניות נוהל התאוששות ושחזור לגרסה תקינה בעת הצורך.			√		√

שיתוף מידע עם הCERT הלאומי איננו מחליף חובת דיווח לגוף מנחה בלשהו, במידה שהתגלה צורך כזה

בברכה,
IL-CERT
119
Team@cyber.gov.il