



ועדת הסייבר והגנת הפרטיות

הנחיות לעצמאים – דף מידע

המלצות אבטחת מידע – מלחמת חרבות ברזל

לאור השלב בו אנו נמצאים, בהתעצמות מתקפות סייבר על ארגונים ועסקים בישראל, שההערכה היא כי ילכו ויתעצמו, פנה עו"ד רועי כהן – נשיא לה"ב - בבקשה שאושרה, להתקנת חבילות הגנת סייבר ואבטחת מידע מבית סיסקו. הפתרונות יינתנו למשך תקופת המלחמה ללא תמורה. לבקשת התקנה **לחצו כאן**

דף מידע זה מרכז עבורכם מידע והמלצות בנושא אבטחת מידע החשובים מאוד בימים אלה. בתקופת הלחימה צפויות תקיפות סייבר שונות על ידי האויב כנגד ארגונים ואזרחים במדינת ישראל. ביצוע ההמלצות המצורפות עשוי לסייע במניעת אירועי סייבר. יש לבצען בהקדם האפשרי.

1. הקטינו ככל האפשר את אפשרויות הגישה מרשת האינטרנט לשרתים ושירותים שאינם חיוניים בארגון.
2. אפשרו גישה רק לשירותים המיועדים לגישה מרחוק מרשת האינטרנט כגון שרתי Web, מערכות VPN, שרתי דוא"ל וכדומה.
3. אפשרו גישה מרחוק לרשת הארגון רק באמצעות שירותים ייעודיים כגון VPN או מערכות עם הצפנה והזדהות חזקה (אישור רב שלבי) מתאימה.
4. ארגונים העושים שימוש במערכות ענן שונות, אפשרו גישה למערכות רק עם הזדהות חזקה (אישור רב שלבי) בפרט למשתמשים בעלי הרשאות ניהול.
5. בצעו בהקדם עדכוני גרסה לכל תוכנות האבטחה. יש להוריד עדכוני אבטחה אך ורק מהאתר הרשמי של היצרן.
6. בצעו עדכוני סיסמה לכל משתמשי הארגון. ודאו כי הסיסמה ארוכה, מורכבת וקשה לניחוש.
7. הגבילו את סוגי הקבצים הניתנים לשליחה בדוא"ל לארגון למינימום הנדרש לצורך תפקוד תקין.
8. התריעו בפני המשתמשים על הצורך להגביר ערנות בפתחת קבצים מצורפים או קישורים המגיעים בדוא"ל, וברשתות החברתיות, גם ממקורות מוכרים.
9. עבור גישה מרחוק, הגבילו הגישה של כל משתמש למערכות להם הוא זקוק לצורך ביצוע עבודתו, ומינעו גישה חופשית לכל הרשת הארגונית.
10. אם אפשרי מבחינה עסקית, חיסמו גישה למערכות הארגון מחוץ למדינת ישראל.

11. וודאו כי ברשותכם לפחות 2 גיבויים תקינים של כל המערכות והמידע החיוני לארגונכם. שימרו גיבוי אחד באופן שאינו מקוון למניעת פגיעה בכל הגיבויים על ידי תוקפים.
12. היערכו למתקפות מניעת שירות. ראו פרסום מערך הסייבר הלאומי בקישור https://www.gov.il/he/departments/publications/reports/alert_1550.
13. אל תזינו נתונים רגישים לתוך מאגרי מידע לא מנוהלים ולא מוכרים.
14. שימו לב לניסיונות מניפולציה ריגשית, להודעות בעל נוסח מאיים, מאיץ, מפחיד או מפתה.
15. הגדירו אימות רב שלבי לכל החשבונות שלכם, פרטיים ועסקיים (GMAIL, WHATSAPP, וכו')
16. אל תשתפו יוזמות שאתם לא מכירים מי עומד מאחוריהן (יש המון פייק ניזוז ומלחמת תודעה + לוחמה פסיכולוגית).
17. נתבקשתם לבצע פעולה "חריגה/משמעותית" כגון העברה כספית, שינוי פרטים רשמיים, מסירת מידע רגיש וכו'? וודאו בערוץ נפרד את נכונות ההודעה ואימות הבקשה

כתבו את המסמך:

- עו"ד יעקב עוז - יו"ר ועדת סייבר ופרטיות
- עו"ד מיכל ברטוב - DPO

לפרטים נוספים: עו"ד יעקב עוז 052-7700359

בדף הבא – פעולות ישראליות ביוזמות פרטיות ו(לא בפעילות המבוצעת על ידי גורמי צבא).

המידע אינו מאומת ומאושר



- ✓ השגת גישה למערכות דואר ממשלתיות, מכללות במימון חמאס, מערכות ענן, שרתי מידע, חשבונות ווטסאפ, ארגונים גדולים בעזה ואזורים נוספים ועוד - איסוף מודיעין והעברתו לגורמים רלוונטיים.
- ✓ פריצה לרשת החנויות Badri & Hania, גניבה ופרסום של כל מאגרי המידע והשחתת האתר הראשי
- ✓ פריצה ל-13 מרפאות בעזה - גניבה ופרסום של כל מאגרי המידע והשחתת האתר הפנימי המיועד לעובדים ומטופלים.
- ✓ השגת גישה למאגרי מידע של חברות המספקות שירותי תקשורת בעזה - איסוף מודיעין.
- ✓ פריצה לטלפונים וחשבונות וואטסאפ של עיתונאים, מחבלים ובכירים מהחמאס.
- ✓ השבתת אתרי אינטרנט ששימשו למימון פעולות טרור.
- ✓ גניבת מאגרי מידע מתוך משרד הבריאות בעזה, בנקים ועוד.
- ✓ השתלטות מלאה על אוניברסיטה בעזה, שרתים, מצלמות, חשבונות אדמין ועוד.
- ✓ גניבת מידע מחברות איראניות, כולל השגת גישה לרשתות, השחתה והשבחה של אתרים ועוד.
- ✓ מתקפות דיכוס והשחתת אתרים, סתם בשביל הכיף, כנגד מספר אתרים של חמאס וגורמי טרור אחרים.
- ✓ עשרות יוזמות פרטיות לחסימה של חשבונות לגיוס כספי טרור בשיתוף פעולה עם חברות הטכנולוגיה, ובמקביל פעולה לשחרור חשבונות לגיוס כספים עבור חיילי צה"ל שנחסמו בגלל אנומליות שונות
- ✓ ברגעים אלו ממש יש קבוצות ישראליות הנמצאות בתוך רשתות שונות, פועלות בשקט כדי לבצע תנועה רוחבית, להשיג מידע ולבסוף, גם להשבית ו/או לגרום נזק אחר.

באדיבות ישראל אמון - סמנכ"ל אבטחת מידע Cisco ישראל.