

רב-מגן להגנה בסייבר

הגברת ההגנה כנגד תקיפות סייבר לספקים בחירום ("חרבות ברזל")

כללי

- א. יחידת "רב-מגן" במשרד הביטחון עוסקת בהנחיה והסמכת ספקים ביטחוניים של התעשיות הביטחוניות, משרד הביטחון וגופי הסמך שלו, בנושא ההגנה בסייבר.
- ב. להלן סט המלצות בסיסי לטובת השגת שיפור ברמת ההגנה הארגונית העשויות לסייע לארגונכם למנוע אירועי סייבר.
- ג. סט המלצות זה מיועד לחברות וארגונים אשר הינם ספקים ראשיים או ספקי משנה של מוצרים ושירותים המיועדים למשרד הביטחון, גופי הסמך, התעשיות הביטחוניות, ובאמצעותם גם מסופקים לצה"ל.
- ד. אנו ממליצים לטפל בנושאים אלו בדחיפות, וכן לדרוש יישום המלצות אלו מול ספקי המשנה הקריטיים שלך – החוסן שלהם הוא החוסן שלך.
- ה. בעת זו של חירום, אנו מבצעים באופן תדיר עדכונים והתאמות להמלצות אלו תוך שקלול מתווי האיומים וההתפתחויות בשטח, שקלול המלצות גופי הנחייה אחרים, עם הטמעת התובנות שלנו. בהתאם, מומלץ להתעדכן בכתובת האתר (URL) בקישור – <https://www.mod.gov.il/ravmagen>.
- ו. מומלץ להעביר מידע זה לנמענים אחרים תוך שימוש בקישור לעיל. המידע ניתן להפצה פומבית.
- ז. ההוראות הרשומות במסמכים אלו הינן במעמד של המלצה מיטבית ואינן בגדר של חובה למימוש. המידע נמסר "כפי שהוא" (AS-IS) ואופן השימוש הוא באחריות המשתמש. משרד הביטחון עצמו אינו מספק כיום תמיכה לספקים בנושאים אלו.
- ח. מומלץ להסתייע במומחי הגנת סייבר בכדי להוביל, לתכנן, ליישם, ולוודא מימוש הנושאים בצורה המיטבית בארגונך.

המלצות לשיפור רמת ההגנה

1. צמצמו והגבילו את הגישה לרשתות הארגון מרשת האינטרנט. נתקו גישה לשירותים שאינם חיוניים; מערכות חיצוניות, מערכות Online, תיקיות משותפות, וקישורים מול שותפים וספקים – צמצמו פורטים (Ports) ופרוטוקולים לנדרשים בלבד. צמצמו את טווח כתובות ה-IP לכתובות ישראליות, או כאלו לגיטימיות והנחוצות בלבד. טייבו חוקות Firewall.
2. סיגרו את הגישה המרוחקת לממשקי הניהול של מערכות ושירותים קריטיים ברשת מן החוץ.

3. בצעו שינוי סיסמא רוחבי לכלל המשמשים והשירותים בארגון. שנו סיסמאות ברירת מחדל. הגדירו סיסמאות חזקות ומורכבות. וודאו חסימת חשבונות לפרק זמן ממושך לאחר 5 ניסיונות אימות לא מוצלחים.
4. הפעילו תהליכי אימות/הזדהות דו-שלבי (MFA) עבור כלל המשתמשים והנכסים.
5. וודאו כי כל המערכות אשר מחוברות לרשת האינטרנט מעודכנות ע"פ ההוראות והעדכונים (Patches) האחרונים אותם פרסמו יצרני המערכות. בעת פניה עצמאית לקבלת מידע ועדכונים יש לבצע זאת מול אתרי היצרנים.
6. בצעו שינוי סיסמא לכלל ממשקי השליטה וההפעלה של התקנים ממוחשבים; מצלמות אבטחה, שעוני נוכחות, התקני "בית חכם", מערכות בקרת מבנה, מערכות מתקניות, בקרי התקנים תעשייתיים וייצור (ICS / OT) והתקני IoT אחרים.
7. בצעו גיבוי מלא לנתוני הארגון. וודאו כי הגיבוי תקין ומכיל את כל הנדרש. העבירו את עותק הגיבוי למקום אחסנה המנותק מן הרשת, מקום מוגן ומרוחק גיאוגרפית. מומלץ לבצע לפחות שני גיבויים.
8. טייבו את רשימות המשתמשים וההרשאות המוקצות להן. זהו משתמשים או הרשאות מיותרות, בטלו או מחקו אותן.
9. הפעילו פונקציות אבטחה המובנות בהתקנים ומערכות קיימות.
10. בצעו למשתמשים ריענון אבטחת מידע וסייבר בנוגע לאירועי פישנינג, שימוש ברשתות חברתיות וטיפול באימיילים. וודאו כי המשתמשים מודעים לסיכונים הכרוכים בנושא פתיחת מיילים, פתיחת צרופות, הקשה על קישורים, ומענה להודעות המגיעות ברשתות חברתיות, כך שהודעות חשודות יועברו לטיפול הממונה על אבטחת המידע בארגון.
11. וודאו כי מערכות ההגנה והניטור הקיימות פועלות בצורה תקינה. כיילו את המערכות למצב הגנה מקסימאלי. ודאו כי המערכות שומרות על תיעוד אירועים (Log) לפחות 90 יום אחורה.
12. ודאו כי ערוצי החיבוריות קצה-לקצה בין שירותים ומערכות מיישמים VPN הכוללים הצפנה והזדהות חזקה. הגבילו גישה לכתובות IP ספציפיות. השתמשו ב- Private APN עבור חיבוריות התקנים מרוחקים על רשת סלולארית.
13. וודאו כי התקנים ורכיבים פרטיים (BYOD) כדוגמת טאבלטים, מכשירי טלפון חכם, מחשבים אישיים וכד' אינם מתחברים לרשת הארגונית ללא וידוא רמת התאמתם למדיניות ההגנה ברשת קודם לחיבור.
14. הפעילו שירותי סריקת חולשות מן האינטרנט (באמצעות שירות צד-שלישי) לצורך זיהוי פערים. סגרו את הפערים שהתגלו.
15. בצעו התקשרות עם ספק מומחה לשירותי התמודדות באירוע סייבר (IR) כך שניתן יהיה להפעילו במהירות עם זיהוי של אירוע.
16. לצורך שמירת המשכיות תפעולית של שירותים קריטיים המסופקים באמצעות האינטרנט ללקוחותיכם, הפעילו שירותי מניעת מתקפות מניעת שירות (DOS), ואתרו חלופות לרכיבים קריטיים.
17. מינוע גישה פיזית אל חדרי השרתים, מערכות המחשוב והתקשורת מפני גורמים לא מורשים.

בלמ"ס | CLEAR: TLP

מהדורה 3, מיום 16/10/2023

18. ככל שהתגלה אירוע סייבר בהקשר לתוצרים והשירותים הקריטיים, מבוקש לעדכן מהר ככל האפשר את הלקוח המזמין.

להלן טבלת הפניות להרחבות מידע עבור הסעיפים לעיל:

מס'	הרחבה / קישור	מס'	הרחבה / קישור
1	רב-מגן 2 סעיף 2.1.2, NIST SP 800-215	11	רב-מגן 2 סעיף 2.12.3 ו- 2.3.3
2	רב-מגן 2 סעיף 2.1.15, NIST SP 800-128	12	רב-מגן 2 סעיף 2.1.12-14, NIST SP 800-77
3	רב-מגן 2 סעיף 2.5.7 ו- 2.1.8, NIST 800-205	13	רב-מגן 2 סעיף 2.1.18, NIST SP 800-124, 800-46
4	רב-מגן 2 סעיף 2.5.3	14	רב-מגן 2 סעיף 2.11.2
5	רב-מגן 2 סעיף 2.14.1 ו- 2.12.2, NIST SP 800-40	15	רב-מגן 2 סעיף 2.6.1
6	רב-מגן 2 סעיף 2.5.7 ו- 2.5.9, NIST SP 800-213A	16	NIST SP 800-189
7	רב-מגן 2 סעיף 2.8.9, NIST SP 800-184	17	רב-מגן 2 סעיף 2.10.1
8	רב-מגן 2 סעיף 2.5.1 ו- 2.5.6	18	רב-מגן 2 סעיף 2.6.2
9	רב-מגן 2 סעיף 2.4.2		
10	רב-מגן 2 סעיף 2.2.1		

(*) תקן רב-מגן 2 מצורף באתר משרד הביטחון בכתובת הנ"ל. תקינת NIST ניתנת לאיתור והורדה פומבית באמצעות מנועי חיפוש באינטרנט.

בברכה,

צוות "רב-מגן"
