תקיפת בקרים נגישים מרשת האינטרנט

28/07/2026
י"ד אב תשפ"ו

[תקציר]

1. לאחרונה עדכנה CISA כי איתרו פעילות של גורמים הקשורים לאיראן כנגד בקרים תעשייתיים הנגישים מרשת האינטרנט, בעיקר במגזר המים והביוב.
2. מערך הסייבר הלאומי הפיץ בעבר מספר התרעות בנושא זה.

[פעולות מידיות לביצוע]

- וודאו כי הבקרים ושאר הרכיבים ברשת התפעולית (OT), כגון Historian, עמדה הנדסית (Engineering Workstation) וכד', אינם נגישים ישירות מרשת האינטרנט.
- אם נדרשת גישה לרכיבים אלו מרשת זו, מומלץ ליישמה באמצעות שירות כגון VPN או ZTNA, עם הצפנה והזדהות חזקה מתאימה, או להגבילה לכתובות ספציפיות וידועות מראש.
- וודאו כי סיסמת ברירת המחדל בציוד הוחלפה לסיסמה ארוכה ומורכבת הקשה לניחוש. הפעילו הזדהות חזקה אם נתמכת בציוד.
- בחנו והתקינו באופן עיתי את עדכוני האבטחה של היצרנים לרכיבים השונים ברשת ה-OT.

[פרטים]

1. התוקפים פעלו כנגד בקרים תעשייתיים (PLC) המנהלים את הפעילות במערכות OT.
2. ממשק הניהול של הבקרים היה נגיש ישירות מרשת האינטרנט.
3. התוקפים השתמשו בסיסמאות ברירת מחדל או בסיסמאות קלות לניחוש.
4. לאחר השגת הגישה לבקרים, התוקפים שינו רכיב קוד אשר נעשה בו שימוש חוזר בתכנות הבקר, באופן שהפעלתו ביצעה שינויים בפעילות הבקר, ואף מנעה דיווח על השינויים למערכת הניהול.
5. הפעלת הקוד ששונה על ידי התוקפים גרמה במכוון להפעלת המערכת באופן חריג ולא שגרתי.
6. הותקפו בעיקר בקרים מתוצרת רוקוול אוטומציה, אך גם אלו של סימנס, שניידר אלקטריק ויצרנים נוספים.

[דרכי התמודדות]

1. יש לוודא שבקרים אינם נגישים ישירות מרשת האינטרנט. מומלץ להגביל גישה לציוד זה לכתובות ארגוניות ספציפיות על פי צורך בלבד. אם מסיבה עסקית נדרשת גישה לבקר מרשת האינטרנט, יש לבצעה משירות כגון VPN או ZTNA, עם הצפנה והזדהות חזקה מתאימה, ולהגביל באופן אקטיבי בבקר או ב-Router/Firewall רשתי, את הגישה לכתובת זו בלבד.
2. אין לאפשר גישה חופשית לבקר מכל רשת האינטרנט, בין ברמת צפייה בלבד ובין בהרשאות מנהלן. אין לאפשר גישה חופשית לבקר החוצה מרשת הבקרה אל כל רשת האינטרנט או הרשת הארגונית. יש להגביל הגישה לכתובות המחויבות לשם פעולה תקינה של הבקר.
3. ארגונים המשתמשים ברשת סלולרית לגישה לבקר, יש לבחון שימוש ב-APN להגדרת רשת פרטית בין הבקר לשאר המערכות הארגוניות, ללא גישה אל רשת האינטרנט וממנה.
4. יש לנהל את הבקר באמצעות פרוטוקולים מוצפנים בלבד.
5. יש לבחון האפשרות לניהול הבקרים ממחשבים ייעודיים שזהו השימוש היחיד בהם, על מנת למנוע תקיפה של מחשבי הניהול ומהם מעבר לתקיפת הבקרים עצמם.

6. אם הבקר תומך במנגנוני הזדהות חזקה, מומלץ להפעילם.
7. אם הבקר ניתן להפעלה במצב RUN, מומלץ לבחון הפעלתו באופן זה.
8. אם קיימים בבקר מנגנוני רישום אירועים (לוגים) מומלץ להפעילם ולייצא את הלוגים למחשב ייעודי. יש לבחון לוגים אלו באופן עיתי לזיהוי אנומליות או להיעזר במערכות ייעודיות כגון מערכות SIEM.
9. אם נדרשת תמיכת היצרן/הספק בבקר מרחוק, יש להגבילה לכתובות הרלוונטיות ברשת היצרן. יש לחייב יידוע של הארגון בפרטי הגישה הנדרשת, ואישורה טרם ביצועה בפועל.
10. יש להתעדכן באופן עיתי בפרסומי יצרן הבקרים, ולבחון ולהתקין את הגרסה העדכנית ביותר של תוכנת ההפעלה שלהם. יצרנים שונים מאפשרים רישום לרשימות דיוור על מנת לקבל עדכונים סדירים בנושאי אבטחה הנוגעים לבקרים.
11. **הנאמר בסעיפים לעיל רלוונטי גם לשאר הרכיבים ברשת התפעולית, ואותן הגנות צריכות לחול גם עליהם.**

[מקורות]

1. https://www.gov.il/BlobFolder/reports/alert_1969/he/ALERT-CERT-IL-W-1969.pdf
2. https://www.gov.il/he/pages/alert_1631
3. https://www.gov.il/he/pages/alert_1588