במציאות של היום, בה עבודה מרחוק הינה חלק משגרת חיינו, יותר ויותר מכונות נדרשות לתמוך בגישה מרחוק על מנת לאפשר העברת נתונים למערכות מידע חיצוניות, שליטה מרחוק לצורכי תחזוקה, איסוף מידע ועוד. בעקבות כך, הגנת סייבר הינה בלב דרישות המשתמש עבור פרויקטי אוטומציה תעשייתית.

האחריות למניעת פירצות אבטחה בפרויקטי אוטומציה הינה של אנשי התפעול והבקרה, אשר מתכנתים ומחברים את הבקרים לרשת חיצונית. כדי לתמוך בנושא, יוניטרוניקס מציעה מגוון פתרונות וכלים המאפשרים בצורה פשוטה יישום אשר יגביר את ההגנה כנגד פרצות אבטחה.

מסמך זה מפרט את עיקרי הכלים עבור הגנות אלו בשימוש בבקרי יוניטרוניקס מסדרת Vision™ ו Samba™.

1. בסיס

רמת הציוד

א. יוניטרוניקס מפתחת ומשפרת את מוצריה לאורך כל חיי המוצר. החברה מפרסמת באתר החברה את גרסאות התוכנה ומערכות ההפעלה העדכניות, אשר כוללות גם שיפורים בנושא הגנת ה-Cyber.
את גרסאות התוכנה העדכניות ניתן למצוא תחת קישור זה.
יש לעקוב אחר מסמכי ה- Version Changes המפורסמים בכל עדכון גרסה ולעדכן את מוצרי החברה בגרסאות העדכניות בהתאם לרלוונטיות.

ב. יש לוודא כי הרשאות הגישה לבקר והציוד הנלווה מנוהלות ומבוקרות וכי סיסמאות ברירת המחדל שונו ונשמרו בהתאם למקובל.

ג. חשוב לנהל ולהגדיר את הרשאות הגישה מרחוק בהתאם לצרכי המערכת והמשתמש בכדי לצמצם חשיפה מיותרת.
למשל, פרוטוקול ה-PCOM (פרוטוקול התקשורת המובנה לטובת כלי הפיתוח והניהול) מאפשר הגנה במספר רמות:

- גישה חסומה - מומלץ לוודא כי הבקרים לא יאפשרו חיבור לפרוטוקול זה עד אשר עולה הצורך בכך
- צפיה בלבד
- מפעיל – צפייה ועדכון נתונים
- טכנאי - טיפול בתקלות, שינויי הגדרות בקר ועדכוני גרסאות

2. רמת הרשת

תקשורת מאובטחת

א. במקרים בהם הבקר נדרש לתקשורת מול רכיבים או שרתים ברשת האינטרנט, יש לדאוג כי הבקר יהיה ה- Client שיוזם את התקשורת.

ב. בכל חיבור ציוד האוטומציה לרשת האינטרנט, יש:

- לדאוג כי ציוד האוטומציה נמצא מאחורי Firewall וכי אין Firewall Rules החושפים את רשת ה-LAN לכניסה מרשת ה- WAN (בין אם זה נתב סלולארי או רשת קווית).
- לוודא כי אין הגדרות Port Forwarding החושפות את ציוד האוטומציה התעשייתית ישירות לרשת הציבורית.

ליישום פשוט ומהיר של הגנה ברמת הרשת מומלץ להשתמש במוצרי UCR, סדרת הראוטרים החדשה של יוניטרוניקס, המכילה פונקציונאליות מובנית של Firewall ו VPN. לחיבור מהיר יש לפעול לפי הצעדים הבאים:
הגדרת VPN במוצרי UCR בארבעה שלבים.

3. פתרון שלם

חיבור מאובטח מבוסס UniCloud

יוניטרוניקס מציעה פלטפורמת ענן בשם UniCloud, המאפשרת לכל לקוח חיבור מאובטח ללא צורך בשימוש בכתובות IP אינטרנטיות קבועות או ציבוריות, וללא צורך בידע מקדים בתחום הסייבר או ה-IT.
הפלטפורמה מכילה שכבות רבות של הצפנה והגנה מתקדמות המספקות יחד פתרון אבטחה שלם המאפשר, בין היתר, גם הגבלות גישה לפי רמת הרשאות וביצוע מעקב אחר מבצעי החיבור בפועל.