



ניהול הגנת Cyber עבור גישה מרחוק לבקרים המלצות לניהול הגנת Cyber עבור בקרי סדרת UniStream™ של יוניטרוניקס

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 ועוד. בעקבות כך, הגנת סייבר הינה בלב דרישות המשתמש עבור פרויקטי אוטומציה תעשייתית.

הצורך בקישוריות חיצונית, המאפשרת גישה מרחוק, מייצרת אתגרים חדשים בתחום אבטחת המידע היות והיא מגבירה את פוטנציאל החשיפה והסיכון.

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 ימנוע פרצות אבטחה כאלו או אחרות.

מסמך זה מפרט את עיקרי הכלים והשלבים השונים המומלצים בכדי לשפר את רמת הגנת הפרויקט/המכונה אשר משתמשת בבקרי יוניטרוניקס מסדרת UniStream™.

1. רמת הציוד

בסיס

א. יוניטרוניקס מפתחת ומשפרת את מוצריה לאורך כל חיי המוצר. החברה מפרסמת באתר החברה את גרסאות התוכנה ומערכת ההפעלה העדכניות ביותר, אשר כוללות גם שיפורים בנושא הגנת ה-Cyber. את גרסאות התוכנה העדכניות ניתן למצוא תחת קישור זה. יש לעקוב אחר מסמכי ה-Release Notes המפורסמים באתר www.unitronicsplc.com בכל עדכון גרסה ולעדכן את מוצרי החברה בגרסאות העדכניות בהתאם לרלוונטיות. **יוניטרוניקס ממליצה לעדכן את הבקרים וכלי הפיתוח לגירסה 1.32 ומעלה.**

ב. יש לוודא כי הרשאות הגישה לבקר והציוד הנלווה מנוהלות ומבוקרות וכי סיסמאות ברירת המחדל שונו ונשמרו בהתאם למקובל. שינוי ססמאת ברירת המחדל וקביעת ססמת גישה חדשה לבקר **תמנע אפשרות ממשתמש מזדמן** להתחבר לבקר באמצעות UniLogic.

ג. מוצרי UniStream™ תומכים במספר רבדי אבטחה והגנה. על המפתח והמשתמש לוודא הפעלת הפונקציונאליות הבאה בהתאם לצרכי המערכת:

- קביעת סיסמאות ל VNC באמצעות VNC Server Management.
- קביעת הרשאות ל UniApps באמצעות Password Management.
- קביעת משתמשים והרשאות למסכי המשתמש באמצעות User Access Control.
- הגדרת משתמשים והרשאות עבור מסכי ה Web Server.

עבור מערכות בהן הורדת אפליקציית המשתמש נעשית באמצעות Flash Drive או באמצעות SD Card, יש לדאוג להגדרת הסיסמאות השונות במקומות המיועדים לכך.

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 התעשייתיים 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.

נשמח לעמוד לרשותך, לסיוע בתכנון ויישום מערכות האבטחה של מערכות האוטומציה שלך. פנה אלינו לקבלת מסמך הנחיות שיסייע לך להגן על המערכות שלך: info-automation@rdt.co.il | support@unitronics.com

ייחוד ראיוני
לא גלפוס