



CYBER-ePAC - יכולות סייבר מובנות בבקרי התהליך

החשיבות הגוברת בהגנת סייבר עבור מערכות בקרה תעשייתיות (ICS), הופכת לממשית יותר ויותר בשנים האחרונות בעיקר בשל הדיווחים בתקשורת, המודעות לסכנות וההכרה ברצון לפגוע בתשתיות קריטיות. שלא כהתקפות הנפוצות בעולם ה IT, תשתיות התקשורת, והקמעונאות, התקפות בעולם הבקרה התעשייתית משפיעות באופן מידי גם על הסביבה המוחשית והתהליכית.

הקונפליקט בין הצורך ליישם סביבת בקרה מתקדמת, אמינה ופתוחה הנסמכת על תשתית תקשורת מפעלית, לבין הצורך לשמור על סביבת הייצור מבודדת ככל האפשר מפגיעות מהווה שיקול מרכזי בתכנון מערכות הבקרה התעשייתיות בעידן החדש.



אז כיצד ניתן לשמר את הנגישות והאמינות של מערכות הבקרה התעשייתיות בעידן החדש?

ההתפתחות הטכנולוגית המואצת בתחום המחשוב והתקשורת, דוחפת את יצרני ציוד הבקרה התעשייתית להשקיע מאמצים כבירים בפיתוח יכולות תקשורת וסייבר מתקדמות **כחלק אינטגרלי מבקרי התהליך** המחוברים לרשת התפעולית. הדרישה למוצרי בקרה מאובטחים יותר גדלה משנה לשנה ומהווה בסיס ליצירת פתרונות מגוונים לבקרה תעשייתית אמינה ומאובטחת יותר, אך עד לאחרונה הפתרונות מרכזיים היו חיצוניים לבקר התהליך, כמו חומות אש, הפרדת רשתות והגבלה בסביבת המחשוב. פתרונות אלו הצריכו לעיתים אינטגרציה מורכבת וידע נרחב תחום אבטחת המידע ורשתות התקשורת.

יישום טכנולוגיות אבטחת מידע חדשות המוטמעות **כחלק ממערכת ההפעלה של הבקר** הינם המילה האחרונה בתחום אבטחת המידע בבקרי התהליך. יישום זה הופך את בקרי התהליך ל"מודעים" יותר ויותר לסביבה בה הם מותקנים ומגיבים למגוון איומים בהתאם.

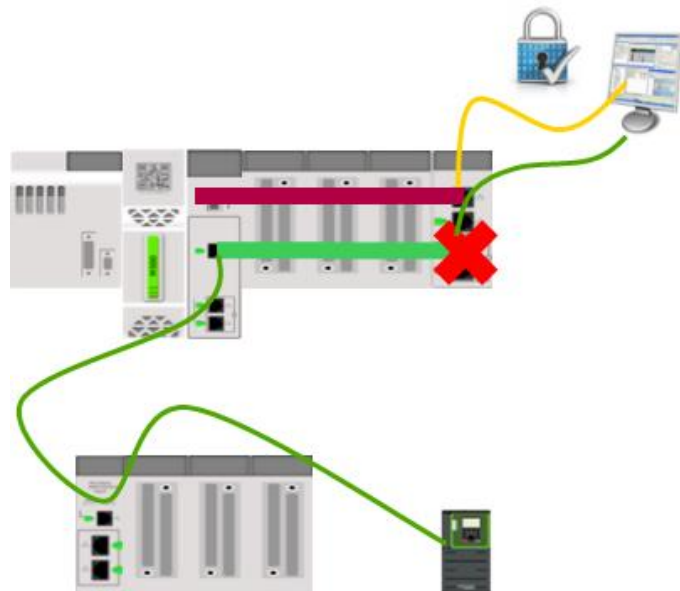
אם כך, מדוע זה יישום יכולות סייבר בבקרי התהליך לא הוטמעו עד היום?

אין לכך סיבה אחת ברורה אך עם זאת ניתן לציין מספר גורמים מרכזיים אשר יצרו את הצורך וסייעו להתפתחות היכולות הנ"ל בבקרי התהליך וביניהם:

1. התפתחות טכנולוגית משמעותית במעבדי הבקר והזיכרון – שימוש במעבדים מהירים וכמות זיכרון של עשרות MB, מאפשרת כיום לבקרי התהליך לבצע מספר משימות במקביל, ניהול תקשורת חכם ומורכב, והקשחה של מערכת ההפעלה בפני איומים. כל זאת ללא פגיעה בביצועי הבקר מבחינה תהליכית
2. מודעות הולכת וגוברת לאיומי סייבר ולפגיעה האפשרית בתשתיות ובתהליכי הייצור מכל מקום ובכל זמן
3. התפתחות מכשור חכם אשר מצריך חיבורי תקשורת ותמיכה במגוון פרוטוקולים על גבי בקר יחיד, ברשת בקרה מפעלית מבוססת ETHERNET
4. הצורך בסביבת בקרה פתוחה וחכמה יותר אשר מתקשרת עם מכלולי הבקרה והניטור בתקשורת רשתית ולא ב I/O פיזי

כיצד זה מיושם הלכה למעשה ?

בקרים בעלי יכולות סייבר, כוללים מגוון מנגנוני הגנה פנימיים וחיצוניים, אשר מגיעים **כחלק אינטגרלי** מחומרת/מערכת ההפעלה בבקר וסביבת הפיתוח. מנגנונים אלו מאפשרים לבקר להתמודד מפני התקפות ברשת הבקרה, לנהל בקרת גישה חכמה, להשתמש ביכולות הצפנה ואף לדווח על ניסיונות פריצה ושיבוש בזמן אמת.



לצורך כך יצרני ציוד הבקרה משקיעים מאמצים כבירים בשילוב טכנולוגיות IP והצפנה בחומרת ציוד הבקרה, ובנוסף מבצעים התאמות של טכנולוגיות הגנה בפני סייבר קיימות לעולם זה.

יש לציין כי חדשנות זו בתחום הסייבר לוקחת בחשבון כי משתמש הקצה אינו מומחה IT ברוב המקרים אלא מהנדס בקרה.

בקרים המובנים ביכולות סייבר, כוללים כיום מגוון יכולות מתקדמות המאפשרות לבקר עצמו להתגונן מפני מתקפות סייבר כגון:



- Achilles Level 2 – הבקר ורכיבי התקשורת נבדקו ואושרו כעומדות מפני פגיעויות נפוצות בתחום אבטחת מידע וסייבר בצידוד בקרה תעשייתית.
- תקשורת מוצפנת בין הבקר ל-SCADA מבוססת IPSEC
- מנגנון הזדהות מבוסס סיסמא לצורך גישה לאפליקציה בבקר התהליך ומחוצה לו.
- ניהול גישה לסביבת הפיתוח ולשינויים בבקר התהליך עד לרמת הרגיסטר – כל גישה ופעולה כפופה להזדהות ומתועדת בקובץ לוג אותו ניתן לתחקר.
- הגבלת גישה לעדכון קושחת הבקר (FIREWARE) – הגנה בפני עדכון לא מורשה של קושחת הבקר או ניסיונות לטעינת קושחה שאינה חתומה על ידי יצרן הציוד.
- חיבור ל-SYSLOG חיצוני לדיווח על הפרות אבטחה וניסיונות גישה שאינם מורשים
- חסימת פרוטוקולים, פורטים, כתובות רשת באמצעות רשימת גישה (Access control list) המנוהל במערכת ההפעלה של הבקר
- חתימת זמן לתעבורת התקשורת מול הבקר – כל מסר חתום בחותמת זמן אמת המסונכרנת לשעון הזמן בבקר.
- בדיקת מקוריות רכיבי הבקר וסביבת הפיתוח (קבצים, DLL, זיכרון ...) אשר חתומים על ידי יצרן החומרה (Integrity check)

בשנים האחרונות אנו רואים מגמה שבה יצרני ציוד הבקרה עוקבים אחר התפתחות טכנולוגיות ההגנה במרחב הסייבר הנפוצים בעולם ה-IT, ומיישמים טכנולוגיות אלו בסביבת הבקרה התהליכית.

ניסים חי

שניידר אלקטריק ישראל

054-6798775

Nissim.hai@schneider-electric.com