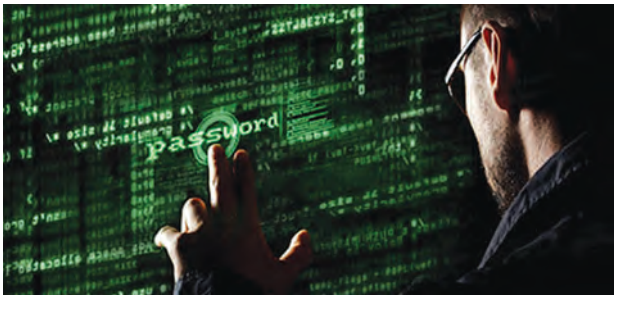
Cyberbezpieczeństwo w przemyśle

Sieci komunikacyjne stanowią swoisty kręgosłup nowoczesnych zakładów przemysłowych, w których prym wiedzie automatyka. Obecnie systemy komputerowe wykorzystują technologie informatyczne i urządzenia automatyki w celu efektywnego sterowania obiektami w czasie rzeczywistym, optymalizując proces produkcji. Wykorzystywanie możliwości szybkiego przesyłania danych w oparciu o struktury sieciowe wiąże się jednak z potrzebą wdrożenia zabezpieczeń przed zagrożeniami cybernetycznymi. Wyzwaniem dla wielu przedsiębiorców staje się ochrona maszyn, urządzeń oraz infrastruktury przed cyberatakami.

Ryzyko utraty produkcji staje się większe bez odpowiednich środków bezpieczeństwa chroniących przemysłowe systemy sterowania i sieci kontroli procesów. Są one podatne na zagrożenia wewnętrzne i zewnętrzne. Zagrożenia bezpieczeństwa systemów komputerowych wynikają często z przypadków i zaniedbań ludzkich, w tym nieumyślnego podłączenia zainfekowanego urządzenia do sieci. Możliwe jest również umyślne naruszenie bezpieczeństwa sieci przez pracowników, którzy niewłaściwe użytkują systemy pomagające w zapewnieniu stabilności, efektywności i produktywności procesu produkcyjnego. Zagrożenia zewnętrzne są różne – od uciążliwych wirusów komputerowych do cyberterroryzmu.

Często wiele firm nie zdaje sobie sprawy z zagrożeń związanych z cyberatakami. Na przestrzeni kilku lat, cyberataki za pomocą oprogramowania malware (oprogramowanie szpiegowskie) i ransomware (oprogramowanie szantażujące), jak Stuxnet, Petya, czy Wannacry, zainfekowały tysiące komputerów i systemów. Postęp technologiczny zarówno w strefie technicznej, jak i programowej powoduje, że skala zagrożenia rośnie. Każdego dnia wzrasta liczba prób ataków cybernetycznych na obiekty przemysłowe i infrastrukturę na całym świecie. Cyberataki mają różny charakter, od kradzieży wrażliwych danych, blokady dostępu do systemów komputerowych, po akta sabotażu z wyłączeniem całych instalacji i systemów w zakładzie. Przedsiębiorstwa dotknięte takimi atakami często ponoszą ogromne straty finansowe.



Warunkiem koniecznym do osiągnięcia najwyższego poziomu cyberbezpieczeństwa w przedsiębiorstwie jest m.in. specjalistyczna wiedza na temat przepływów w nim informacji. Jedną z dobrych praktyk poprawiających bezpieczeństwo sieci w przedsiębiorstwie są regularne audyty, w celu zidentyfikowania i wyeliminowania luk i zagrożeń w zabezpieczeniach. To luki w zabezpieczeniach są furtką dla cyberprzestępców. Najczęściej usuwane są poprzez instalowanie zapór i oprogramowania antywirusowego dostosowanego do obecnie używanego systemu.

Rozwiązania dotyczące bezpieczeństwa cybernetycznego powinny chronić dostępność, bezpieczeństwo i niezawodność obiektów przemysłowych oraz pomagać bezpiecznie wdrażać technologie IoT (*Internet of Things*).

Na przykład, linia biznesowa firmy Valmet w obszarze bezpieczeństwa systemów automatyki (Valmet Automation) od lat prowadzi systematyczne działania w zakresie bezpieczeństwa przemysłowego i rozwija usługę związaną z bezpieczeństwem cybernetycznym. Łączność sieciowa procesów i komunikacja między maszynami wymusza instalowanie szeregu zabezpieczeń w obszarze teleinformatycznym w systemach sterowania Valmet DNA. Firma wdraża metody i technologie w celu poprawy ogólnego poziomu bezpieczeństwa produktów oraz procesów przemysłowych. W obszarze bezpieczeństwa cybernetycznego stosuje także bezpieczne praktyki w oprogramowaniu inżynieryjnym, łącznie z modelowaniem stanu zagrożeń. Wprowadza odpowiednie standardy bezpieczeństwa, które pomagają utrzymać zasoby informacyjne w sposób bezpieczny dla użytkowników. Oferuje także usługę związaną z przechowywaniem jak i przywracaniem danych po udanym ataku cybernetycznym. Opracowuje również struktury bezpieczeństwa dla przyszłych i obecnych produktów automatyki.

Natomiast w firmie Voith rozwojem nowych metod i narzędzi do wykrywania i obrony przed cyberatakami zajmuje się Voith Digital Solution, dysponujący zintegrowanymi rozwią-