ní přesnost, se může aplikovat jiná, levnější technologie. Podstatné je, aby všechny části umožňovaly pořizovat, přenášet a analyzovat digitální data. Navíc lze díky škálovatelnosti a modularitě těchto technologií ekosystémy nasazené u zákazníka i jejich konfiguraci průběžně modernizovat či doplňovat podle měnících se potřeb a požadavků a nahrazovat postupně jednodušší systémy vyspělejšími variantami. Příkladem inovace je RF600 UHF RFID (*obr. 1*), jenž umožňuje data z nástrojů, produktů, beden, palet a kontejnerů přenést s využitím protokolu OPC UA a MindSphere do cloudu a zde je využít pro analýzy v reálném čase, které podporují rychlé a informované rozhodování při řízení výrobních procesů (*obr. 2*).

Digitální dvojče: reálná optimalizace skladů ve virtuálním světě

Software Tecnomatix Plant Simulation umožňuje simulaci, analýzu a optimalizaci sekvencí a procesů díky schopnosti vizualizovat veškeré skladovací provozy. Digitální dvojče skladového provozu usnadňuje digitální návrh, simulaci, ověření a optimalizaci všech intralogistických procesů ještě před jejich uvedením do praxe (*obr. 3*). Digitální dvojče manipulační techniky umožňuje virtuální plánování, simulaci, odhady a optimalizaci těchto systémů jak pro manuální či automatické stroje, tak i pro kombinaci obou. Díky tomu je možné verifikovat a optimalizovat výrobní kapacity a efektivitu již v rané fázi konceptu. Dále je také možné simulovat provoz mechanických a elektrických přístrojů a automatizaci systémů pro přepravu materiálu současně s automatickým generováním programů pro PLC. To je výchozím bod pro virtuální zprovoznění.

Digitální dvojče reálného provozu skladu

Při provozu manipulační techniky vzniká velké množství hodnotných dat. Sběr a analýza těchto dat jsou zcela zásadní, aby bylo možné získat informace ze zařízení a poznatky z konkrétních aplikací. Příklady:
- stav strojů v decentralizovaných systémech,
- spotřeba energie,
- informace o údržbě,
- analýza provozních podmínek,
- porovnání reálných a plánovaných provozních podmínek pro uzavření zpětné vazby ve fázi plánování.

Společnost Siemens dodává techniku pro kompletní řízení skladového hospodářství od návrhu a simulace skladu a provozu v něm přes technické prostředky až po služby spojené s dlouhodobým a úspěšným provozem skladového hospodářství, intralogistiku a řízení celého dodavatelského řetězce.

Více informací lze nalézt na stránkách siemens.cz/rfid.

Radim Adam

Hlavními motivy přechodu na MSP jsou vážnější kybernetické hrozby a potřeba vyšší produktivity

Společnost Zebra Systems, distributor řešení N-able na českém a slovenském trhu, uvedla, že hlavními důvody přechodu tradičních dodavatelů informačních systémů na model řízených služeb (MSP – *Managed Service Provider*) je potřeba dosáhnout vyšší produktivity a automatizace při řešení stále náročnějších požadavků zákazníků. V loňském roce se také objevily rozsáhlejší bezpečnostní hrozby, které již nelze s tradičním reaktivním přístupem efektivně eliminovat.

K nejvážnějším incidentům se z pohledu poskytovatelů IT služeb zařadily zejména tzv. útoky *supply chain*, umožňující získat přístup k datům klientů prostřednictvím nezabezpečené infrastruktury poskytovatelů. Útok *supply chain* je útok vedený s použitím softwaru důvěryhodného dodavatele, který se vlastně za útočníka postará o masivní distribuci malwaru. Vektorem je např. infikovaná aktualizace softwaru.

Ke konci roku 2021 byla odhalena zranitelnost v knihovně Log4j, logovacího aplikačního rámce pro jazyk Java od Apache, která naráz ohrozila stovky softwarových systémů využívaných různými organizacemi po celém světě. Protože jazyk Java se dříve široce používal a dosud používá i v průmyslové automatizaci, odhalení zranitelnosti velmi vyděsilo i mnohé dodavatele v našem oboru. Nemluvě o tom, že zranitelnost ohrozila také informační systémy mnoha úřadů, nemocnic, bezpečnostních služeb a armádních složek.

Rozsah takovýchto útoků je již nad síly těch dodavatelů IT služeb, kteří se spoléhají hlavně na reaktivní přístup k incidentům.

Mnoho z nich proto přechází na řízené služby (MSP) či jimi svou nabídku alespoň doplňuje. Model MSP využívá ověřené platformy pro vzdálenou správu a monitorování (RMM – *Remote Monitoring and Management*) s integrovanými nástroji kybernetické bezpečnosti. K hlavním přínosům integrovaných řešení s RMM patří:
- automatizace rutinních činností – podle některých údajů umožňuje ušetřit až 240 h ročně na jednoho pracovníka,
- automatizovaná správa aktualizací (*patch management*), která dovoluje zvládnout aktualizace velkého množství softwarových systémů a minimalizovat rizika napadení,
- inteligentní ochrana koncových zařízení – umožňuje lépe reagovat na hrozby typu *zero-day*, jež nejsou zjistitelné běžnými antivirovými programy,
- rychlý a bezpečný vzdálený přístup – nutný zejména u velmi distribuovaných systémů, např. pracuje-li velké množství uživatelů z domova,
- vyšší produktivita – s moderními nástroji MSP dokáže jeden technik spravovat až tisíc koncových bodů u zákazníků,
- transparentní vztahy se zákazníky – s konzistentní tvorbou nabídek, reportů a fakturací poskytovaných služeb.

N-able je již více než dvacet let dodavatelem nástrojů pro poskytovatele řízených služeb (MSP), kteří je využívají ke správě, monitorování a zabezpečení infrastruktur informačních systémů svých zákazníků. Nástroje N-able využívá přes 22 000 dodavatelů MSP pro správu více než 500 000 firemních sítí a 7 milionů koncových bodů. Více informací zájemci naleznou na http://www.n-able.com.

(*Zebra Systems*)