Potrebujeme projektovú dokumentáciu ku kybernetickej bezpečnosti?

Trendy v oblasti implementácie priemyselnej kybernetickej bezpečnosti sa v našich podmienkach pozitívne menia. Kým v minulosti bola problematika priemyselnej bezpečnosti nosnou témou a problematika priemyselnej kybernetickej bezpečnosti len okrajovou témou, v súčasnosti si spoločnosti budujú komplexné systémy riadenia kybernetickej bezpečnosti. Vrcholový manažment výrobných podnikov si uvedomuje dôležitosť riešenia nielen problematiky priemyselnej bezpečnosti, ale aj problematiky kybernetickej bezpečnosti a právom požaduje, aby bezpečnosť OT systémov (prevádzkové technológie) mala implementovanú rovnakú úroveň kybernetickej bezpečnosti, ako sú zaužívané bezpečnostné štandardy v IT prostredí (informačné technológie).

Podniky, ktoré sa rozhodli implementovať priemyselnú kybernetickú bezpečnosť, riešia problém, ako začať. Naša skúsenosť hovorí, že existujú v zásade dva základné prístupy, ktoré majú odlišné procesy implementácie, ale rovnaký cieľ – znížiť riziko kybernetického incidentu na akceptovateľnú úroveň. Prvý prístup je aplikovateľný na existujúce inštalácie OT systémov a druhý na novostavby. V tomto článku sa budeme podrobnejšie venovať druhému prístupu opisujúcemu novostavby.

Ak sa pripravuje stavba novej výrobnej technológie, je naším štandardom, že základná projektová dokumentácia priemyselnej kybernetickej bezpečnosti obsahujúca opis hlavných kybernetických požiadaviek je súčasťou komplexnej projektovej dokumentácie vo fáze basic design, resp. už v projektovej dokumentácii pre stavebné povolenie. Je vhodné, ak má podnik vytvorené interné smernice pre oblasť priemyselnej kybernetickej bezpečnosti, na ktoré možno odkazovať a zadefinovať tak spoločné základné kybernetické štandardy.

Postupne je projektová dokumentácia detailne rozpracovaná a vo fáze realizačného projektu už obsahuje všetky nevyhnutné schémy, postupy, opisy dátovej komunikácie a pod., pričom reflektuje potreby všetkých zainteresovaných profesií. Treba si uvedomiť, že projekt priemyselnej kybernetickej bezpečnosti sa tvorí paralelne s ostatnými projektovými dokumentáciami a pracovník zodpovedný za priemyselnú kybernetickú bezpečnosť, ktorý je súčasťou tímu vo všetkých fázach realizácie, disponuje kompetenciou spolurozhodovať o vhodnosti výberu zariadení IACS (Industrial Automation and Control Systems). Predstava, že kybernetickú bezpečnosť budeme riešiť až v neskorších fázach alebo po nábehu technológie (nakoľko sa riešia dôležitejšie problémy), je mylná. Finančné náklady za dodatočné riešenie kybernetickej bezpečnosti kvôli nevhodne navrhnutému IACS sú podstatne vyššie a implementácia je náročná. V podstate sa v tomto prípade aplikujú implementačné procesy ako pri existujúcich inštaláciách OT systémov. Inštalácia v existujúcich stavbách je náročnejšia, časovo a finančne nákladnejšia.

Aby bola implementácia kybernetickej bezpečnosti úspešná, treba si na začiatku stanoviť merateľné ciele. Tie sú definované v projektovej dokumentácii priemyselnej kybernetickej bezpečnosti. V našej praxi pri definícii cieľov vychádzame z požiadaviek normy IEC 62443 (definuje technické požiadavky, ktoré musí IACS spĺňať, aby vyhovoval jednej z úrovní bezpečnosti SL1 – SL4) s ohľadom na rôzne rizikové aspekty vychádzajúce napr. z projektovej dokumentácie funkčnej bezpečnosti či BPA (Business Process Analysis). Na základe definovaných cieľov je parametrizovaná a tvorená celá projektová dokumentácia priemyselnej kybernetickej bezpečnosti.

Štandardná projektová dokumentácia spoločnosti ProCS komplexne pokrýva problematiku priemyselnej kybernetickej bezpečnosti. Jej implementácia je rozdelená do troch základných fáz:

1. V prvej fáze je vytvorená projektová dokumentácia priemyselnej kybernetickej bezpečnosti, ktorá slúži ako základná metodická príručka na dosiahnutie cieľovej úrovne bezpečnosti.
2. V druhej fáze prebieha samotná implementácia cieľov a požiadaviek na aktívach na základe projektovej dokumentácie MaR, ASRTP, elektro a projektu kybernetickej bezpečnosti a ich overenie pomocou skenera zraniteľnosti.
3. V tretej fáze sú zdokumentované všetky dôležité nastavenia a konfigurácie aktív, porovnané cieľové bezpečnostné požiadavky s dosiahnutými požiadavkami a opísané základné odporúčania na správu priemyselnej kybernetickej bezpečnosti.

Projektová dokumentácia priemyselnej kybernetickej bezpečnosti pozostáva z viacerých na seba nadväzujúcich častí. V úvodných kapitolách vysvetľuje princípy normy IEC 62443 tak, aby bol obsah projektovanej dokumentácie zrozumiteľný pre koncového používateľa, implementátora či servisnú organizáciu. V ďalšej časti zameranej na identifikáciu posudzovaného systému exaktne definuje rozsah

aktív, ktorých sa projektová dokumentácia týka spolu s návrhom rozdelenia aktív do úrovní bezpečnosti, opisom dátovej komunikácie a diagramom dátových tokov. V časti zaoberajúcej sa úrovňami bezpečnosti rozdeľuje aktíva do bezpečnostných zón a prechodov a podrobne opisuje parametre komunikácie a bezpečnostné požiadavky podľa IEC 62443, ktoré sú neskôr predmetom vyhodnocovania dosiahnutej úrovne bezpečnosti. V ďalších častiach rieši problematiku fyzickej bezpečnosti, hardeningu, patch managementu, ochrany pred škodlivým softvérom, správy účtov, systému zálohovania a sieťovej bezpečnosti.

Požadované parametre opísané v projektovej dokumentácii priemyselnej kybernetickej bezpečnosti priebežne kontroluje aj zákazník počas realizácie FAT (Factory Acceptance Test) a SAT (System Acceptance Test).

Na záver je vypracovaná komplexná správa opisujúca identifikovateľné zraniteľnosti spolu s vyhodnotením cieľov. Správa je spoločným dielom implementátora, výrobcu IACS a zákazníka.

Myslíme si, že na úroveň implementácie priemyselnej kybernetickej bezpečnosti v podnikoch okrem legislatívnych požiadaviek zo strany štátu budú priamo vplývať aj vysoké bezpečnostné požiadavky zo strany poisťovní, ktoré budú vyžadovať deklaráciu súladu podniku s bezpečnostnými normami určenými pre OT, a preto sa kvalitne vypracovaná a udržiavaná projektová dokumentácia priemyselnej kybernetickej bezpečnosti stane nevyhnutnosťou.

Spoločnosť ProCS, s. r. o., sa od roku 2015 prezentuje pod značkou Actemium. V rámci medzinárodnej skupiny VINCI Energies. Actemium je medzinárodná sieť zameraná na priemyselné procesy. Actemium navrhuje, realizuje a udržuje výrobné zariadenia svojich zákazníkov s cieľom zlepšiť ich výkonnosť a konkurencieschopnosť.

ACTEMIUM

Ing. Štefan Kőrösi
vedúci skupiny IT

ProCS, s.r.o.
Kráľovská ulica 8/824
927 01 Šaľa
info@actemium.sk
www.actemium.sk