KYBERNETICKÁ BEZPEČNOSŤ RIADIACICH A INFORMAČNÝCH SYSTÉMOV V ZÁKLADNÝCH SLUŽBÁCH

Zákon o kybernetickej bezpečnosti priniesol množstvo opatrení a zmien pri projektoch zameraných na komunikačné a informačné technológie. Týka sa nielen štátnych zákaziek, ale zahŕňa aj prevádzkovateľov základných služieb, teda oblasť energetiky, plynárenstva či dopravy. Ako sa na tieto zmeny pripravili vývojári a výrobcovia riadiacich systémov, ktorí sem informačné systémy a služby dodávajú? Na to sme sa spýtali Pavla Kulika, riaditeľa útvaru Technického rozvoja spoločnosti ZAT, ktorá dodáva riadiace systémy a know-how pre energetiku a priemysel takmer do 70 štátov sveta.

Vaša spoločnosť nasadzuje riadiace systémy v strategických segmentoch z oblasti základných služieb. Aké opatrenia ste museli v súvislosti so zákonom prijať?

Ako dodávateľ riadiacich systémov do klasickej i jadrovej energetiky, plynárenstva aj železničnej dopravy sme tieto požiadavky samozrejme intenzívne riešili. Dodávame systémy do odborov s nárokmi na dlhú životnosť a bezporuchovosť riadiaceho systému. S príchodom tohto zákona k nim pribudli ďalšie na zabezpečenie proti úmyselnému kybernetickému napadnutiu. Implementovali sme niekoľko technických opatrení na zvýšenie odolnosti našich riadiacich systémov proti kybernetickým útokom a zároveň neustále pracujeme na zlepšovaní interných procesov. Z jadrovej energetiky máme dlhoročné skúsenosti s napĺňaním špecifických požiadaviek regulačných úradov v rôznych krajinách. Konkrétny spôsob zaistenia kybernetickej bezpečnosti vždy závisí od podmienok prevádzky riadiaceho systému. Zákazníci často špecifikujú svoje požiadavky, ktoré musia riadiace systémy spĺňať. Napríklad jadrová elektráreň má iné požiadavky ako klasická alebo zákazník z oblasti distribúcie plynu.

Ktoré odbory sú na tom z hľadiska bezpečnosti najlepšie?

Logicky najďalej v oblasti zabezpečenia bola jadrová energetika, kde sa požiadavky na kybernetickú bezpečnosť do značnej miery stretávajú s už skôr aplikovanými nárokmi na jadrovú bezpečnosť. Riadiace systémy sú tu veľmi štruktúrované. Často sa využívajú iba pri jednosmernej komunikácii špeciálnymi protokolmi. Tiež fyzická ochrana – zamedzenie neoprávnenej manipulácii so zariadením – je tu na veľmi vysokej úrovni. Špecifické požiadavky vrátane tých na kybernetickú bezpečnosť v súčasnosti riešime napríklad v elektrárni Loviisa vo Fínsku, kde dodávame riadiaci systém pre primárnu časť jadrovej elektrárne. V klasických elektrárňach bola situácia iná. Systémy riadiace jednotlivé časti technológie boli často pripojené do jednej komunikačnej siete. Dnes dochádza práve z dôvodu zvýšenia kybernetickej bezpečnosti k jej rozdeleniu na „komunikačné ostrovy“. Komunikácia medzi ostrovmi je potom striktne obmedzená a jednoznačne špecifikovaná. Tomu prispôsobujeme aj riešenie našich projektov.

V súčasnosti sa často skloňuje kybernetická bezpečnosť v distribúcii plynov. Ako to vyzerá v tomto segmente?

Hoci by sa laikovi mohol zdať opak, pre nás, výrobcu riadiacich systémov pre náročné priemyselné procesy, je realizácia kybernetickej bezpečnosti v oblasti distribúcie zemného plynu veľkou technickou výzvou. Na rozdiel od spomínaných jadrových a klasických elektrární, kde sú komunikačné siete aj samotné riadiace systémy umiestnené vnútri uzavretého stráženého objektu, v oblasti prepravy zemného plynu ide o rozsiahle siete s veľkým množstvom pripojených zariadení, často bezobslužných, navyše na rozľahlom území pokrývajúcom celú Českú republiku. Komunikačné siete môžu byť realizované mnohými spôsobmi. To kladie vysoké nároky na zabezpečenie nielen komunikačných sietí, ale najmä koncových riadiacich staníc.

Ako využívate technológie v rámci riešenia problematiky kybernetickej bezpečnosti?

V rámci kybernetickej bezpečnosti implementujeme technológie umožňujúce šifrovanie komunikácie, autorizáciu prístupov na servisné účely, blokovanie nepoužívaných služieb, kontrolu integrity softvérového vybavenia staníc atď. To platí aj pre inžinierske nástroje určené na tvorbu aplikačného softvéru. Vždy však záleží na charaktere konkrétnej aplikácie a koncepcii zaistenia kybernetickej bezpečnosti prevádzkovateľa, ktoré z opatrení je vhodné použiť.

V akých ďalších projektoch ste v poslednom čase riešili kybernetickú bezpečnosť?

Napríklad vodná elektráreň Lipno I je od minulého roka riadená bezobslužne zo 140 km vzdialeného dispečingu v Štěchoviciach v režime virtuálneho bloku až 120 MWe.

Pavel Kulik, riaditeľ útvaru Technického rozvoja v spoločnosti ZAT, a. s.

Ďalším prebiehajúcim projektom, kde nasadzujeme systémy s požiadavkami na kybernetickú bezpečnosť, je napríklad už spomínaná fínska jadrová elektráreň Loviisa.

Aké sú vaše ďalšie ciele v oblasti kybernetickej bezpečnosti?

Uznávaný americký odborník na informačnú bezpečnosť Bruce Schneier povedal: „Bezpečnosť nie je produkt, ale proces.“ Preto je aj naším cieľom nielen zvyšovať technickú odolnosť našich riadiacich systémov proti kybernetickým útokom, no najmä rozvíjať spoluprácu s našimi zákazníkmi na poli kybernetickej bezpečnosti. Jedine tak možno dosiahnuť funkčný výsledok. Naše vývojové oddelenie pracuje na zvyšovaní odolnosti riadiacich staníc proti kybernetickým útokom dlhodobo, čo nám umožňuje garantovať klientovi požadovanú bezpečnosť a spoľahlivosť. Navyše odolnosť inštalovaných riadiacich systémov proti kybernetickým útokom si štandardne testujú samotné firmy aj nezávislé audítorské spoločnosti.

Ďakujeme za rozhovor.

Denisa Ranochová