Kybernetická bezpečnost – téma sílící s růstem digitalizace

Větší propojení průmyslových podniků s sebou přináší otázku jejich zabezpečení proti vnějším hrozbám. Množství kyberútoků roste a cílem jsou stále častěji i malé a střední podniky. Více než 80 % z nich uvedlo, že problémy s kybernetickou bezpečností by měly vážný negativní dopad na jejich podnikání. Z toho 57 % konstatuje, že by s největší pravděpodobností zkrachovaly nebo ukončily podnikání.

Jaké jsou současné a budoucí úkoly v oblasti kybernetické bezpečnosti, nastíní seminář, který se uskuteční jako součást doprovodného programu veletrhu Amper 2024. Organizátorem akce je CyberSecurityHub.cz ve spolupráci s Regionální hospodářskou komorou Brno.

V dnešní digitální éře jsou kybernetická napadení stále častější a závažnější hrozbou nejen pro jednotlivce, ale i pro organizace a firmy. Existuje několik důvodů, proč jsou tato napadení vůbec možná, a mnohé z nich souvisejí s různými aspekty současného digitálního světa. Jsou to:

– *Rostoucí digitalizace*. Jedním z hlavních důvodů, proč jsou kybernetická napadení stále častější, je rostoucí digitalizace. Většina činností podniku v současné době spadá pod IT (*Information Technology*) a informace o nich jsou mnohdy dostupné online. To dává kyberzločincům širší pole působnosti a větší možnosti pro útoky.
– *Nepředvídatelný vývoj nových technologií*. Vývoj nových technologií pro práci s daty a informacemi neustále pokračuje, což vytváří nové bezpečnostní hrozby a problémy. Obrana proti kybernetickým hrozbám musí být proto flexibilní a schopná rychle reagovat na nové útoky.
– *Nedostatek odborníků na kybernetickou bezpečnost*. Kvalifikovaných odborníků na kybernetickou bezpečnost je nedostatek, a přitom poptávka po nich stále roste. Tato situace vytváří mezeru, kterou kyberzločinci mohou využít. Nedostatek odborníků znamená, že organizace nemají dostatečné zdroje na ochranu před útoky.
– *Omezené finanční zdroje*. Kybernetická bezpečnost vyžaduje finanční investice do hardwaru, softwaru a školení personálu. Některé menší organizace a firmy nemusí mít dostatek finančních prostředků na zajištění řádné ochrany. To z nich dělá snazší cíle pro kybernetické útoky.
– *Nedostatečná osvěta a vědomosti*. Mnoha lidem a organizacím může chybět základní povědomí o kybernetických hrozbách a bezpečnostních opatřeních. To znamená, že jednotlivci mohou podcenit rizika a organizace nemusí využívat dostatečná bezpečnostní opatření.
– *Sociální inženýrství*. Kybernetičtí zločinci často využívají techniky sociálního inženýrství, aby získali přístup k citlivým informacím. Tato forma útoku závisí na manipulaci s lidským chováním a ne vždy je možné jí zcela zamezit technickými prostředky.
– *Neustále se měnící taktiky kyberzločinců*. Kyberzločinci jsou flexibilní a neustále mění své taktiky a strategie, což ztěžuje zachycení a odhalení jejich útoků.

Celkově lze říci, že kybernetická bezpečnost je komplexní a neustále se vyvíjející oblast, která vyžaduje pozornost a opatření na mnoha úrovních. Bez ohledu na důvody, proč jsou kybernetická napadení možná, je důležité, abychom byli ostražití, vzdělaní a aktivně se snažili chránit své aktivity a citlivé informace. Bezpečnostní vědomosti a opatření jsou pro zajištění naší digitální bezpečnosti zásadní.

Více informací o chystaném semináři zájemci najdou na www.ic40.cz.

Lukáš Smelík, Industry Cluster 4.0, z. s.

krátké zprávy

EtherCAT Technology Group roste v Asii i v Americe

Neustálý růst počtu členů asociace EtherCAT Technology Group (ETG) nevykazuje žádné známky zpomalení. Na veletrhu Hannover Messe sdružení ETG slavnostně přivítalo 7 000. člena: firmu Image Engineering z USA. Dvě třetiny členů jsou výrobci techniky s rozhraním EtherCAT, zbytek jsou uživatelé a univerzity (členy mohou být jen právnické osoby, nikoliv jednotlivci).

Silný růst vykazuje ETG nyní zvláště v regionech mimo Evropu. V současné době má organizace přes 3 000 členů v Asii a více než 1 000 v Americe. Již 42 % z celkového počtu členů pochází z Asie.

„Tento nárůst počtu členů odráží přijetí komunikačního systému EtherCAT na trhu," vysvětluje Martin Rostan, výkonný ředitel EtherCAT Technology Group. „V Asii se EtherCAT pevně etabloval v oblasti automatizační techniky – a to nejen v Čínské lidové republice. EtherCAT využívá většina asijských výrobců řídicích systémů. Díky tomu je přijímán i výrobci snímačů, I/O a pohonů." Kromě ČLR má ETG silnou pozici také v Čínské republice na Tchaj-wanu, v Jižní Koreji a Japonsku. Mezi novými členy jsou však rovněž společnosti z Blízkého východu, ze Saúdské Arábie a Ománu.

V Americe je absolutní růst tažen nejlidnatější zemí – Spojenými státy, ovšem Kanada se může pochlubit ještě vyšší hustotou počtu členských firem v poměru ke své populaci. K rozšíření komunikačního systému EtherCAT v regionu přispívají i členové z latinskoamerických zemí – mezi nimi převažují uživatelé, nikoliv výrobci automatizační techniky.

Sedmitisící člen, firma Image Engineering, je dokladem toho, že EtherCAT má stále silnější pozici i mimo tradiční průmyslovou automatizaci. Firma Image Engineering se totiž zabývá návrhy a realizací světelných, laserových, ohňových a pyrotechnických efektů pro koncerty, festivaly nebo sportovní utkání.

V České republice má ETG více než dvacet členů. Jsou mezi nimi nejen výrobci a uživatelé průmyslové automatizace, ale např. i automatizační techniky pro dopravu nebo energetiku a výzkumné instituce.

Více informací: https://www.ethercat.org/default.htm.

(*Bk*)