Two Towers Technologies
High standards for high goals

Bezpečnost a LabVIEW

„ostrovní systém“ není řešení

Počet cílených útoků na průmyslové systémy (OT) roste o desítky procent ročně. Globální finanční riziko spojené s těmito incidenty podle odhadů přesahuje **300 mld. USD** a v Evropě cílí téměř pětina všech kybernetických hrozeb právě na ICS a OT prostředí.

Předpoklad, že „stroj je odpojený od sítě“, je dnes iluzí. Útočníci jako bránu dokážou využít servisní notebooky, USB média nebo i IoT komponenty. Důsledkem pak nemusí být jen únik dat, ale reálná fyzická škoda: **zastavení výroby**, **poškození technologie** nebo i **ohrožení života a zdraví**.

Směrnice NIS2 a nařízení CRA mění pravidla pro kybernetickou bezpečnost v EU. I když vaše firma nespadá přímo pod kritickou infrastrukturu, vaši zákazníci podléhající NIS2 budou vyžadovat bezpečnostní garance ve smlouvách.

Provádíme audit a úpravu LabVIEW aplikací tak, aby splňovaly technické i legislativní požadavky na odolnost.



BEZPEČNĚJŠÍ LABVIEW • BEZPEČNĚJŠÍ PROVOZ

two-towers.tech/labview-security

7 pilířů bezpečnosti

1 Migrace na podporovanou verzi LabVIEW

Bezpečnost začíná podporovaným softwarem. Verze LabVIEW starší než čtyři roky již nemají aktivní podporu výrobce a chybí jim kritické bezpečnostní záplaty. Migrace na aktuální verzi technicky usnadňuje implementaci všech následujících bezpečnostních opatření, která starší verze často neumožňují.

2 Správa verzí (Git)

Ruční správa souborů je u malých projektů pohodlná, ale s rostoucí složitostí kódu přestává stačit. Hrozí ztráta historie a vzájemné přepisování změn. Git tento problém řeší: umožňuje mimo jiné přesné sledování úprav, rychlý návrat k poslední funkční verzi a bezpečnou spolupráci více vývojářů. Zároveň otevírá cestu k automatizaci.

3 Monitoring zranitelností

Jen díky aktuálnímu seznamu závislostí (SBOM) lze efektivně porovnávat váš kód s katalogy zranitelností (CVE). Detekce ohrožené součásti vyžaduje okamžitou aplikaci záplaty nebo vlastní opravu kódu. U vlastních komerčních produktů tento proces přikazuje nařízení CRA, včetně povinnosti bezodkladně notifikovat zákazníky o nově zjištěné zranitelnosti.

4 Automatizace vývojového cyklu (CI/CD)

Opakované úkony ve vývoji mohou běžet automaticky. Při každé změně kódu se spustí statická analýza kódu, hromadný překlad (MassCompile), unit testy, sestavení aplikace (Build) a generování SBOM. Statická analýza kódu navíc nemusí kontrolovat jen dodržování stylistických pravidel, ale může i detekovat známé bezpečnostní slabiny (CWE) dříve, než se kód dostane do produkce.

5 Autentizace a autorizace

Systém nesmí důvěřovat každému příkazu jen proto, že přišel z lokální sítě. Je nutné zavést řízení přístupu pro uživatele i stroje. Řešením je napojení na firemní Identity Server nebo vytvoření bezpečné lokální správy s vynucenou politikou hesel. Používání sdílených účtů typu „Operator1“ s heslem „1234“ není v souladu se současnými bezpečnostními standardy.

6 Šifrování komunikace

Veškerá síťová komunikace musí být šifrována. Nešifrovaná data jsou zranitelná vůči průmyslové špionáži (odposlech naměřených hodnot) nebo podvržení dat (spoofing). Útočník může změnit naměřené hodnoty tak, že systém spustí proces, který být spuštěn nemá. V extrémním případě hrozí převzetí řízení stroje s přímým rizikem pro zdraví obsluhy.

7 Evidence a sběr bezpečnostních událostí

Aplikace musí zaznamenávat nečekané stavy, neúspěšné pokusy o přihlášení a změny konfigurace. Tyto záznamy je vhodné odesílat do centrálního dohledového systému. Bez centralizovaných logů nelze zpětně dohledat příčinu incidentu ani prokázat shodu s předpisy.

Začněte auditem

Zkontrolujeme vaše současné LabVIEW aplikace proti těmto sedmi bodům a navrhneme konkrétní postup úprav.

Kontakty
jan.prochazka@two-towers.tech
+420 739 242 034
https://two-towers.tech

Integration Partner CONSULTANT