Nidec

Drives

Kybernetická bezpečnost v průmyslu

Obsah

Strategie „nekomplikovanosti“ chrání naše zákazníky

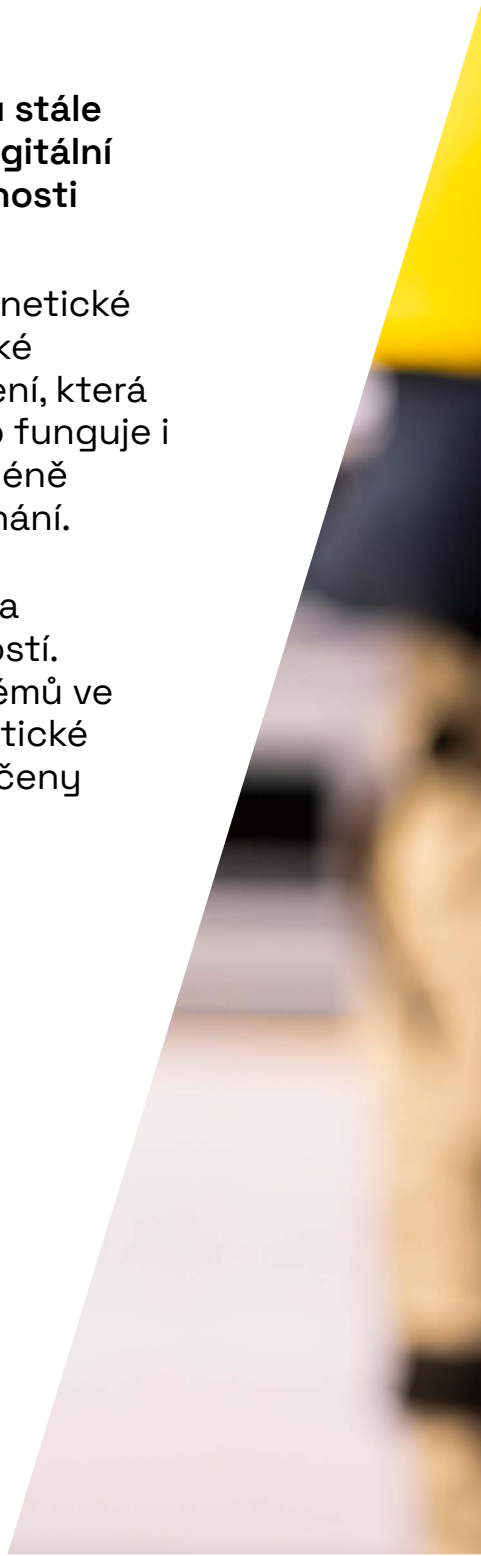
Kybernetická bezpečnost je nezbytnou součástí moderní výroby.

Kybernetická bezpečnost průmyslu je pro výrobce strojů stále důležitější prioritou, a to částečně kvůli množství nové digitální techniky zaváděné v průmyslovém prostředí a její schopnosti ovlivňovat způsoby práce.

Je to také reakce na nedávnou legislativu v oblasti kybernetické bezpečnosti, která má za cíl regulovat tyto nové technické prostředky. Ve společnosti Nidec navrhujeme chytrá řešení, která zjednodušují složité procesy; myslíme si, že tento přístup funguje i u složité legislativy. Chytrá řešení snižují riziko, protože méně pohyblivých částí znamená méně potenciálních míst selhání.

S tím, jak se firmy a stroje stávají stále sofistikovanějšími a propojenějšími, rostou rizika spojená s digitální zranitelností. Kyberkriminalita se stala jedním z nejnaléhavějších problémů ve všech odvětvích, přičemž útoky ransomwarem a kybernetické podvody byly v Global Cybersecurity Outlook 2025 označeny za dvě nejzávažnější kybernetická rizika. (Světové ekonomické fórum)

> Ve společnosti Nidec navrhujeme chytrá řešení, která zjednodušují složité procesy; myslíme si, že tento přístup funguje i u složité legislativy.



Úvod

S rostoucí popularitou zařízení internetu věcí rostou i obavy o jejich zabezpečení. Fyzická bezpečnost je součástí DNA většiny našich zákazníků: když například provozujete elektrárnu, musíte zajistit její bezpečnost.

Digitální technika má potenciál dále zvyšovat bezpečnost a zároveň zvyšovat produktivitu. Pokud však není správně implementována, může potenciálně otevřít nové cesty pro kybernetické zločince. Důsledky mohou sahat od ransomwaru až po hrozbu katastrofálního zastavení procesů a provozu zařízení.

Aby se tato rizika zmírnila, začaly aktualizované předpisy formovat kybernetickou bezpečnost strojů v celé EU i na dalších světových trzích. Nová pravidla je nejlépe interpretovat společně s normami řady IEC 62443. IEC 62443 (představena níže) není zakotvena v zákoně, ale nabízí řadu osvědčených strategií pro zajištění kybernetické bezpečnosti.

Nidec se specializuje na elektromotory a měničovou techniku. Ačkoli se tato zařízení mohou jevit jako nepravděpodobné cíle kybernetických zločinců, fungují v klíčových zařízeních po celém světě. S tímto vědomím jsme se co nejdříve vydali na cestu k dosažení souladu s předpisy. Je to opravdu tak jednoduché: bezpečnost a ochrana našich zákazníků je na prvním místě.

Účelem této bílé knihy je pro všechny zjednodušit pochopení souladu s předpisy. Naše odůvodnění pro zveřejnění vychází z toho, že jsme jedním z prvních výrobců průmyslové automatizace, kteří dosáhli souladu ještě před stanoveným termínem. Víme, že nové předpisy zvýší bezpečnost v našem odvětví. Vnímáme také zátěž, kterou mohou tato nařízení našim zákazníkům přinést, proto jsme považovali za nutné podělit se o své poznatky, vycházející z vlastního procesu a více než padesáti let zkušeností v oboru.

V komplikovaném prostředí regulací zachováváme jednoduchost tím, že identifikujeme místa, kde se legislativa překrývá a kde lze postupovat efektivněji. Doufáme, že se naši zákazníci budou cítit jistěji a budou mít větší sebevědomí při využívání našich strategií ve svém vlastním úsilí o dosažení souladu s předpisy. Všem ostatním čtenářům: jsme nadšeni automatizací, takže prosperující a předpisům vyhovující odvětví nám dokonale konvenuje.

Nová situace v oblasti kybernetické bezpečnosti

Prvním novým právním předpisem je evropské nařízení o strojních zařízeních (EU) 2023/1230. Tato směrnice upravuje bezpečnost a ochranu zdraví v souvislosti s používáním a výrobou strojů a byla navržena jako náhrada za předchozí směrnici EU o strojních zařízeních (2006/42/ES).

Směrnice o strojních zařízeních vyžadovala aktualizaci, protože byla vydána v roce 2006 a nemohla účinně upravovat technický vývoj následujících desetiletí.

Druhý právní předpis je zcela nový. Zákon o kybernetické odolnosti (CRA) je široce pojatý mandát, jehož cílem je napomoci realizaci posílené strategie EU v oblasti kybernetické bezpečnosti. Jeho požadavky jsou početnější než u nařízení o strojních zařízeních, ačkoli v mnoha bodech se oba předpisy překrývají. Může být užitečné uvažovat o CRA z hlediska zabezpečení a o nařízení o strojních zařízeních z hlediska bezpečnosti, i když v praxi není tento rozdíl tak jasný, protože kybernetická bezpečnost a bezpečnost jsou v mnoha průmyslových kontextech neoddělitelné.

Ačkoli mají nové předpisy určité podobnosti, nejsou přímo propojené. Oba již vstoupily v platnost, ale z hlediska realizace bude dodržování nařízení o strojních zařízeních a CRA povinné od roku 2027. Strategie uvedené v této bílé knize nejsou zamýšleny jako komplexní návod k implementaci, ale představují náš pohled na osvědčené postupy.

Hnací síly legislativy

Stále nákladnější a narušující digitální útoky učinily z kybernetické bezpečnosti prioritu. To platí zejména pro společný trh EU, kde je pohyb zboží mezi členskými státy pro mnoho podniků životně důležitý.

Mnoho výrobců strojů se při montáži výrobků, které obsahují součásti od výrobců z různých států uvnitř i vně EU, spoléhá na tuto svobodu obchodu. Tato vrstvená struktura výrobků může znamenat vyšší efektivitu a nižší náklady, ale zároveň zvyšuje zranitelnost. Složitější dodavatelské řetězce vyžadují důkladnější bezpečnostní řešení.

Útoky na dodavatelský řetězec – kdy hackeři vkládají škodlivý kód do softwaru používaného více zákazníky – se dostaly na titulní stránky světových médií. Mediálně známý incident společnosti Kaseya získal v roce 2021 značnou pozornost, když hackeři zaútočili na její software a ovlivnili odhadem 2 000 podniků v 17 zemích.

Útoky na dodavatelský řetězec mohou způsobit výpadek životně důležitých služeb a kritických odvětví s katastrofálními dopady. Kyberkriminalita se vyvíjí rychleji než související legislativa, což znamená, že státní orgány musí reagovat rychle – a často zpětně – na nové hrozby. Složité dodavatelské řetězce jsou zranitelné vůči útokům, pokud zařízení obsahuje více součástí od různých výrobců a přitom na společné bezpečnosti nespolupracují všechny strany. Nové předpisy se snaží řešit otázku odpovědnosti tím, že podrobně určují, které strany jsou odpovědné za identifikaci zranitelností, které za identifikaci útoků a jak má každá strana reagovat.

Zpřísněná regulace má za cíl chránit spotřebitele a zmírnit škody, ale její rozsah a složitost znamenají značnou zátěž v oblasti souladu pro mnoho výrobců a vývojářů. Zejména rozsah CRA vyvolal u výrobců obavy ohledně toho, jak splnit požadavky. Účinné strategie identifikují podobnosti mezi novými předpisy, aby se snížila zátěž.

Přístup společnosti Nidec k jednoduchosti v oblasti kybernetické bezpečnosti využívá doporučení uvedená v normě IEC 62443 jako efektivní základ pro zajištění souladu při dodržování předpisů. Naši zákazníci očekávají od technických prostředků, které vytváříme, efektivní a vysoce kvalitní řešení, proto musí náš přístup k regulaci odpovídat těmto očekáváním.

Níže uvedená tabulka uvádí obecné požadavky nových předpisů spolu s normou IEC 62443.

	Právní požadavek	Typ	Požadováno pro označení CE
ISA/IEC 62443	Ne	Průmyslový standard	Ne
Nařízení o strojních zařízeních	Ano	Nařízení (uplatňované na úrovni EU)	Ano
CRA	Ano	Nařízení (uplatňované na úrovni EU)	Ano

V novém legislativním kontextu zůstává definice strojního zařízení v zásadě nezměněna oproti předchozímu výkladu ve směrnici o strojních zařízeních. Aktualizované nařízení o strojních zařízeních stanovuje šest konkrétních definic, které mohou být užitečnými vodítky při posuzování, zda se výrobek považuje za strojní zařízení. Jsou to:

1. **Položky s pohonným systémem a pohyblivými částmi, které plní určitou funkci.**
2. **Dle bodu 1 a vyžaduje zdroj energie.**
3. **Dle bodu 1 a 2 a vyžaduje montáž na vozidlo nebo instalaci do budovy.**
4. **Položky popsané v bodech 1–3 nebo části strojů, které fungují pouze při spojení dohromady.**
5. **Položky s pohyblivými částmi, které jsou spojeny za účelem umožnění zvedání jiných předmětů lidmi**
6. **Položky z bodů 1–5, které ke správné funkci vyžadují software.**

Přehled norem:

ISA/IEC 62443

Rodina norem ISA/IEC 62443 se skládá ze čtrnácti samostatných dokumentů. Jsou navrženy jako soubor doporučení, nikoliv právních požadavků, aby zajišťovaly kvalitu v prostředí průmyslové automatizace a řízení.

Poskytují pevný základ pro rozvoj strategií osvědčených postupů pro dosažení souladu s předpisy tam, kde je oficiální dokumentace teprve ve vývoji nebo kde rychlost změn činí stávající pokyny nedostatečnými či nepřesnými.

Poskytují pevný základ pro rozvoj strategií osvědčených postupů pro dosažení souladu s předpisy tam, kde je oficiální dokumentace teprve ve vývoji nebo kde rychlost změn činí stávající pokyny nedostatečnými či nepřesnými.

Tabulka: Stručně o IEC 62443
(Mezinárodní elektrotechnická komise)

Část 1: obecné	Část 2: zásady a postupy	Část 3: systém	Část 4: součást
Koncepce a modely	Požadavky na bezpečnostní program pro vlastníky IACS	Bezpečnostní prostředky pro IACS	Požadavky na bezpečný životní cyklus vývoje výrobku
Slovník pojmů a zkratek	Hodnocení úrovně ochrany	Hodnocení bezpečnostních rizik a návrh systému	Technické bezpečnostní požadavky na součásti IACS
Metriky shody systémové bezpečnosti	Správa aktualizací v prostředí IACS	Požadavky na bezpečnost systému a úrovně zabezpečení	
Bezpečnostní životní cyklus IACS a příklady použití	Požadavky na poskytovatele služeb IACS		
	Pokyny k implementaci pro vlastníky aktiv IACS		

Ne všechny části budou relevantní pro všechny systémy průmyslové automatizace a řízení (IACS), ale mnohé z nich jsou užitečné. Například úrovně zabezpečení stanovené v IEC 62443-3-3 jsou užitečné při navrhování hodnocení rizik a při provádění průběžných posouzení.

Jedním z prvních kroků v procesu hodnocení rizik je pochopení, jaká míra ochrany je při běžném provozu výrobku nezbytná. Protože mnoho pohonů Nidec je přesně přizpůsobeno svému použití, pochopení konkrétních požadavků každého z nich bylo vždy zásadním krokem. Například čerpadlo s digitálním tlakoměrem používané v domácím vodním systému pravděpodobně nebude vyžadovat takovou ochranu jako klíčové čerpadlo v čistírně odpadních vod; nadměrná ochrana může být ve skutečnosti na škodu, pokud zvyšuje zbytečné náklady nebo časové nároky, případně brání uživatelům v optimální práci.

> Protože mnoho pohonů Nidec je přesně přizpůsobeno svému použití, pochopení konkrétních požadavků každého z nich bylo vždy zásadním krokem.

Úrovně zabezpečení IEC 62443-3-3

Úroveň	Popis
SL 1	Ochrana proti náhodnému nebo neúmyslnému narušení
SL 2	Ochrana proti úmyslnému narušení pomocí jednoduchých prostředků, s nízkými zdroji, základními dovednostmi a nízkou motivací
SL 3	Ochrana proti úmyslnému narušení pomocí sofistikovaných prostředků, se středními zdroji, specifickými dovednostmi pro IACS a střední motivací
SL 4	Ochrana proti úmyslnému narušení pomocí sofistikovaných prostředků, s rozsáhlými zdroji, specifickými dovednostmi pro IACS a vysokou motivací

Naší strategií je zachovat jednoduchost, a proto náš postup začíná normou IEC 62443. Zbytečná složitost může být nebezpečná, zejména v průmyslovém prostředí. Totéž platí pro kybernetickou bezpečnost. Řada norem IEC 62443 představuje uživatelsky přívětivý přístup ke složitým požadavkům legislativy EU v oblasti kybernetické bezpečnosti. Jeho úrovně zabezpečení vyžadují, aby výrobci a provozovatelé sdíleli společné porozumění hrozbám, kterým čelí. Věříme, že tato srozumitelnost udržuje naše zákazníky v bezpečí.

Naší strategií je zachovat jednoduchost, proto náš proces začíná normou IEC 62443.

Přehled předpisů týkajících se strojních zařízení

Nařízení o strojních zařízeních funguje ve spojení s CRA s cílem posílit stávající bezpečnostní legislativu a zahrnout do jejího rozsahu nové a vznikající technické prostředky.

Stroje s digitálními součástmi musí splňovat bezpečnostní požadavky Nařízení o strojních zařízeních a požadavky na kybernetickou bezpečnost dle CRA. Nová pravidla vyžadují větší dohled nad vysoce rizikovými stroji, takže mnoho zařízení, která dříve mohla využívat samocertifikaci podle Směrnice o strojních zařízeních, nyní musí získat externí akreditaci.

Působnost Nařízení o strojních zařízeních zahrnuje software i fyzické, digitální nebo smíšené hardwarové součásti. Jednou z významných novinek oproti předchozí legislativě je požadavek na prevenci poškození dat. Jakýkoli typ připojení k digitálním platformám s sebou nese určitou míru rizika, proto bude pro splnění požadavků nutné provádět obdobná posouzení rizik jako u CRA. V praxi je nepravděpodobné, že jedno posouzení rizik zcela splní požadavky obou předpisů, ale společný rámec může být efektivním výchozím bodem.

Posouzení rizik podle Nařízení o strojních zařízeních se zaměří na dvě samostatné oblasti legislativy, které jsou podrobně popsány v tabulce níže.

Příloha III, oddíl 1.1.9 – Ochrana proti poškození dat	Příloha III, oddíl 1.2.1 – Bezpečnost a spolehlivost řídicích systémů
Připojení k jiným systémům a vzdálený přístup nesmí vytvářet nebezpečnou situaci	Řídicí systémy musí být navrženy tak, aby odolaly předvídatelným škodlivým pokusům třetích stran, které by mohly vést k nebezpečným situacím
Hardwarové komponenty, které přenášejí signály nebo data související s připojením či přístupem k softwaru používanému pro požadavky na bezpečnost a ochranu zdraví nebo pro zajištění shody, musí být chráněny před poškozením dat.	Samotný systém nesmí vytvářet nebezpečné situace ani být sám o sobě nebezpečný.
Software a data zapojená do bezpečnostních procesů musí být jako taková identifikována a chráněna před rizikem poškození.	Předvídatelná lidská chyba by neměla způsobit nebezpečné situace
Strojní zařízení musí identifikovat software nezbytný pro bezpečný provoz	Data vzniklá v souvislosti se zásahem musí být uchovávána po dobu pěti let.
Strojní zařízení musí shromažďovat důkazy o provedených zásazích	

Tyto požadavky budou tvořit základ harmonizovaných norem, které budou moci výrobci využít pro účely akreditace označení CE. Evropský výbor pro normalizaci v elektrotechnice (CENELEC) zahájil v létě 2024 vývoj harmonizované normy pokrývající výše uvedené oblasti, avšak její zveřejnění se neočekává před rokem 2027. Harmonizované normy zjednoduší proces zajištění shody, ale stroje vyrobené před jejich zveřejněním budou i tak muset být v souladu s požadavky.

Přehledně:
Zákon o kybernetické odolnosti (CRA)

V říjnu 2024 vstoupily v platnost zákony o kybernetické bezpečnosti CRA. Tato legislativa se týká všech zařízení s datovým připojením nebo těch, která mohou být po sestavení připojena.

CRA reguluje všechny fáze životního cyklu výrobku nebo součásti, od výroby až po vyřazení z provozu, a zahrnuje – ale není omezena pouze na – téměř všechny IT systémy, zařízení internetu věcí (IoT), průmyslové řídicí systémy, strojní zařízení a velmi širokou škálu hardwaru a softwaru.

V roce 2027 musí po tříletém přechodném období všechny výrobky s digitálními součástmi splňovat požadavky CRA, pokud jsou prodávány na trhu EU, a splňující výrobky musí nést označení Conformité Européene (CE). Toto je požadováno různými právními předpisy již od roku 1993 pro mnoho výrobků prodávaných v Evropské unii (EU) jako důkaz splnění bezpečnostních požadavků. CRA vyžaduje označení CE na všech komponentách i na celých výrobcích, a to i v případě, že tyto části byly vyrobeny mimo EU.

Toto je jedna z nejdůležitějších částí nové legislativy pro provozovatele, protože dosud tomu tak nebylo. To může představovat významnou výzvu pro výrobce, kteří spoléhají na součásti od třetích stran.

Splnění tohoto požadavku pravděpodobně povede k výraznému nárůstu administrativy, ale zároveň pokryje společné požadavky napříč více právními předpisy. Seznam softwarových součástí (SBOM), který je vyžadován CRA, lze také využít pro splnění požadavků Nařízení o strojních zařízeních – čímž se předejde duplicitním procesům a zbytečné složitosti.

Kroky k dodržování předpisů CRA

1. **Pro každý pravděpodobný způsob použití výrobku proveďte posouzení rizik v oblasti kybernetické bezpečnosti. Různé způsoby použití mohou vyžadovat samostatná posouzení.**

2. **Zajistěte, aby návrh, vývoj a výrobní procesy obsahovaly integrované bezpečnostní prvky.**

3. **Vytvořte a udržujte procesy pro řešení zranitelností včetně zásad pro zveřejňování, distribučních protokolů a SBOM.**

Krok 1 může začít posouzením rizik vypracovaným v rámci standardních provozních postupů nebo v reakci na jinou nedávnou evropskou legislativu, například NIS2. Jelikož se však tato posouzení mohou zaměřovat na specifika odvětví a opomíjet klíčové technické aspekty CRA, měla by být považována spíše za výchozí bod než za náhradu. Pokud jsou rozdíly mezi stávající dokumentací a požadavky CRA příliš velké, nabízí norma IEC 62443-3-2 možný rámec s následující strukturou:

- Identifikujte systém, který je předmětem posouzení (SuC)
- Proveďte úvodní hodnocení kybernetických rizik na vysoké úrovni.
- Rozdělte SuC na jednotlivé součásti.
- Proveďte podrobné posouzení kybernetických rizik pro každou část.
- Zdokumentujte zjištění a požadavky.

Rozhodnutí v kroku 2 budou určena výsledky posouzení rizik. Jedna z možných strategií využije zjištění z kroku 1 ve spojení s procesy Secure Development Lifecycle (SDL) definovanými v normě IEC 62443-4-1.

- Řízení bezpečnosti
- Specifikace bezpečnostních požadavků
- Bezpečnost již při návrhu
- Bezpečná implementace
- Ověření bezpečnosti a validační testování
- Řízení bezpečnostních incidentů
- Správa bezpečnostních aktualizací
- Bezpečnostní pokyny

Průběžné hodnocení během celého životního cyklu výrobku podpoří soulad s předpisy a může představovat konkrétní přínos pro zákazníky z hlediska trvalé bezpečnosti na stále rizikovějším trhu. Spotřebitelé jsou stále informovanější o hrozbách pro svá data a bezpečnost a my věříme, že shoda s předpisy je pouze začátek. Víme, jak důležité jsou naše stroje v aplikacích našich zákazníků: To bylo hnací silou naší strategie kybernetické bezpečnosti.

Význam bezpečnosti jednotlivých komponent je obzvláště důležitý ve třetím kroku. SBOM je klíčový pro silnou strategii kybernetické bezpečnosti, protože podrobně uvádí jednotlivé komponenty a příslušné dodavatele. V kontextu útoku na dodavatelský řetězec umožní SBOM postiženým stranám mnohem rychleji informovat ostatní výrobce a dodavatele. Podrobný proces zacházení se zranitelností znamená efektivní prevenci a detekci hrozeb, která identifikuje a izoluje rizika, aniž by umožnila narušeným systémům zůstat bez povšimnutí.

Požadavky CRA musí být zveřejněny ve třech sadách dokumentů, které jsou aktualizovány po celou dobu životního cyklu výrobku. Dokumenty by měly odkazovat na základní požadavky CRA. Následující grafika podrobně uvádí požadavky a kde je v rámci CRA najít.

Přehled pilířů CRA

Cíl porozumění společné kybernetické bezpečnosti

Společnost Nidec je již více než padesát let předním výrobcem pohonů zaměřených na potřeby zákazníků. Zaměřujeme se na rozvoj automatizace. Nové zákony o kybernetické bezpečnosti vnímáme jako příležitost zamyslet se nad našimi postupy a ještě více zlepšit naši bezpečnost. Nebyl to rychlý proces, ale jsme hrdí na to, že zajišťujeme shodu se stejnou efektivitou a vysokými standardy, jaké uplatňujeme u naší techniky.

Chápeme, jak náročný je rozsah těchto změn, zejména pro malé výrobce a provozovatele, kteří čelí zvýšenému tlaku na rozpočet. Výrobky Nidec patří mezi první, které splňují nové předpisy, což znamená, že naši zákazníci mohou být v klidu. Neustále hledáme způsoby, jak se zlepšovat a inovovat, ať už to znamená dodržování předpisů nebo vývoj nové techniky. To máme na mysli, když říkáme, že je automatizace naší vášní.

Oblast kybernetické bezpečnosti se neustále vyvíjí a tempo změn se stále zrychluje. Ať už naše pohony pohánějí cokoli, víme, že jsou součástí robustní strategie kybernetické bezpečnosti, která chrání naše zákazníky. Vždy jsme vybírali správné pohony pro správná odvětví, a proto jsme stejně přistupovali i k oblasti kybernetické bezpečnosti. Myslíme si, že výsledek za to stojí.

Odkazy

Evropský parlament. „Nařízení (EU) 2023/1230 Evropského parlamentu a Rady ze dne 14. června 2023 o strojních zařízeních a o zrušení směrnice 2006/42/ES Evropského parlamentu a Rady a směrnice Rady 73/361/EHS, článek 3.“ (2023).

Mezinárodní elektrotechnická komise. https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards. 2021. Dokument. 17. Červenec 2025.

Komise pro bezpečnost práce a normalizaci. KAN. 2025. 15. Červenec 2025. <https://www.kan.de/en/publications/kanbrief/2/25/combating-vulnerabilities-with-standards-new-eu-cybersecurity-rules>.

„Směrnice NIS 2, konečné znění.“ 2022. Směrnice NIS 2. Směrnice. 16. Červenec 2025.

Světové ekonomické fórum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf. 2025. 23. 07 2025.

Nidec
All for dreams

Spojte se s námi

www.drivesfromnidec.com

Nidec Control Techniques Limited. Sídlo společnosti: The Gro, Newtown, Powys SY16 3BE.

Registrováno v Anglii a Walesu. IČO 01236886.

CONTROL TECHNIQUES KB CTD

WP_Industrial Cybersecurity_Iss01_EN 02/26