INFORMAČNÍ DOKUMENT

NIS 2

červen 2024

Obsah

1 Úvod

1.1 Co je NIS 2?

NIS 2 je směrnice EU, která musí být implementována do státní legislativy každé členské země EU nejpozději 17. října 2024. Cílem NIS 2 je dosáhnout vysoké úrovně kybernetické bezpečnosti v EU pro zajištění bezpečnosti a efektivního fungování ekonomiky a společnosti daného regionu. Vyžaduje, aby subjekty poskytující základní a důležité služby v klíčových sektorech společnosti budovaly systémy kybernetického zabezpečení, zmírňovaly hrozby síťových a informačních systémů, zajišťovaly plynulý chod služeb při řešení bezpečnostních incidentů a hlásily bezpečnostní incidenty příslušným úřadům. Nařizuje, aby členské státy přijaly strategie národní kybernetické bezpečnosti a zřizovaly úřady, mimo jiné také úřad pro krizového řízení kybernetických incidentů a akční týmy pro řešení incidentů zabezpečení počítačových systémů. Zevrubně popisuje opatření pro risk management kybernetické bezpečnosti, včetně postupů pro jejich zavedení. Nesplnění těchto požadavků subjekty poskytujícími základní a důležité služby může mít za následek vysoké pokuty a právní postihy manažerských týmů.

Pro více informací navštivte:
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 Koho se týká NIS 2?

NIS 2 zahrnuje všechny subjekty, které poskytují **základní** nebo **důležité** služby pro společnost a ekonomiku v Evropě. To znamená také společnosti a dodavatele.

1.2.1 Přímo zahrnuté subjekty

Základní subjekty – Energie, přeprava, bankovnictví/finance, zdravotnictví, dodávky pitné vody, odpadní vody a kanalizace, digitální infrastruktura, veřejná správa, vesmír

Důležité subjekty – Poštovní a doručovatelské služby, likvidace odpadu, chemické látky, potraviny, výroba (např. lékařská zařízení, elektrovýroba, přepravní výbava), poskytovatelé digitálních služeb (např. e-shopy, vyhledávače, sociální sítě), výzkumné organizace

Příslušné státní úřady – Ve členských státech EU byly stanoveny příslušné státní úřady dohlížející na zavádění a dodržování NIS 2 v příslušných zemích.

1.2.2 Nepřímo zahrnuté subjekty

Prodejci a dodavatelé – NIS 2 se nepřímo týká také prodejců, dodavatelů a poskytovatelů služeb z řad třetích stran, kteří zajišťují základní nebo digitální služby základním a důležitým subjektům. Tyto společnosti musí zajistit zabezpečení jejich produktů a služeb a mohou být vázáni smlouvami o požadavcích na kybernetické zabezpečení ze strany zákazníků.

Uživatelé základních a digitálních služeb – Ačkoli se na ně NIS 2 přímo nevztahuje, uživatelé základních a digitálních služeb získávají prospěch z vylepšených postupů kybernetické bezpečnosti a z akčních plánů reakce na incidenty, které tato směrnice vyžaduje. To nepřímo zvyšuje zabezpečení a spolehlivost služeb, které využívají.

2 Požadavky NIS 2

2.1 Pro subjekty poskytující základní a důležité služby

Bezpečnostní opatření – Zabudování vhodných bezpečnostních opatření pro řízení rizik a zajištění zabezpečení jejich sítě a informačních systémů. Tato opatření musí kopírovat výstupy z analýzy rizik a postupy nejlepší praxe.

Záznamy o incidentech – Hlášení významných incidentů, které by mohly mít výrazný dopad na zabezpečení sítě a informačních systémů, kompetentním úřadům. Včasné hlášení je zásadní pro koordinaci reakcí a zmírnění hrozících škod.

Risk management – Provádění analýzy rizik pro zjištění možných hrozeb a slabých míst a přijetí opatření k jejich zmírnění.

Spolupráce s příslušnými úřady – Spolupráce s úřady členských zemí EU. To zahrnuje poskytnutí nezbytných informací a přistupování k systémům za účelem pravidelného přehledu a reakcí na incidenty.

Plán reakce na incidenty – Rozvíjení a udržování akčních plánů pro účinné řešení incidentů kybernetické bezpečnosti. Tyto plány musí obsahovat zevrubný popis postupů detekce, reportování a zmírňování dopadů incidentů.

Zabezpečené dodavatelské řetězce – Zabezpečení dodavatelských řetězců, včetně prodejců a dodavatelů třetích stran, s cílem zajistit celkovou odolnost sítě a informačních systémů.

Průběžné monitorování – Zajištění průběžného monitorování a kontrol sítě a informačních systémů pro detekci a reakci na hrozby a slabiny v reálném čase.

3 Dopad na dodavatele

Dodavatelé mohou subjekty NIS 2 podpořit splněním následujících požadavků:

Zabezpečení ve fázi návrhu – Výrobci zařízení IoT musí do svých zařízení zabudovat bezpečnostní funkce již ve fázi vývoje, a tím zajistit, že zabezpečení bude nedílnou koncepční součástí produktu.

Pravidelné aktualizace a opravy – Výrobci musí poskytovat pravidelné aktualizace a záplaty pro opravu slabých míst jejich zařízení IoT.

Ověřování a povolování – Zařízení IoT musí využívat silné kontrolní mechanismy ověřování pro zamezení neoprávněnému přístupu.

Šifrování dat – Přenos a uchovávání dat v zařízeních IoT musí být šifrovány pro ochranu citlivých informací před zpřístupněním nebo zobrazením stranou bez oprávnění.

Záznamy o incidentech – Výrobci musí hlásit veškeré významné bezpečnostní incidenty nebo prolomení zabezpečení jejich zařízení IoT příslušným úřadům a potenciálně také zákazníkům nebo uživatelům.

Ochrana soukromí – Zařízení IoT, která pracují s osobními daty, musí krom NIS 2 splňovat směrnice, jako je ONOOÚ (Obecné nařízení o ochraně osobních údajů, anglicky GDPR).

Zabezpečení dodavatelského řetězce – V zájmu ochrany před zaváděním bezpečnostních slabin v průběhu procesu výroby by mělo být požadováno zajištění zabezpečení celého dodavatelského řetězce, od dodavatelů součástí až po zákazníky

4 Reakce Axis

Následující text popisuje, jak Axis coby dodavatel splňuje požadavky směrnice NIS 2:

4.1 Zabezpečení ve fázi návrhu

Zabezpečení ve fázi návrhu představuje přístup, který chápe požadavky na zabezpečení a bezpečnostní aktivity jako nedílnou součást návrhu a vývoje produktu. Snižuje riziko slabých míst a zajišťuje systematickou robustní konfiguraci přispívající k zabezpečení produktu. Zásady zabezpečení ve fázi návrhu v Axis uplatňujeme pro software i hardware a pokrývají následující hlavní oblasti:

- *Axis Security Development Model (ASDM)*: ASDM je soubor konkrétních procesů a nástrojů zajišťujících, že zohlednění bezpečnosti je nedílnou součástí koncepční fáze vývoje softwaru. Tyto aktivity zahrnují posuzování rizik, modelování hrozeb, testování prolomení bezpečnostních zábran, vyhledávání slabých míst, řízení incidentů a program odměň za vyhledání chyb. Softwaroví vývojáři Axis využívají ASDM k tomu, aby zabezpečení bylo do softwaru zabudováno již ve fázi vývoje, s cílem vydávat software obsahující co nejnižší počet slabých míst.
- *Program odměňování za nalezené chyby*: Axis podporuje privátní program odměňování za nalezené chyby, který posiluje úsilí společnosti o proaktivní vyhledávání, opravy a zveřejňování informací o slabých místech linuxového operačního systému AXIS OS, který je instalován na většině produktů Axis. Posiluje závazek Axis budovat profesionální vztahy s externími odborníky na bezpečnost a etickými hackery.
- *Seznam komponent softwaru (Software Bill of Materials, SBOM)*: Axis poskytuje SBOM pro AXIS OS, linuxový operační systém používaný na většině zařízení Axis. Ten zajišťuje bezpečnostním analytikům, úřadům i zákazníkům přehled softwarových komponent, které obsahuje AXIS OS. Jedná se o obzvlášť přínosnou pomůcku pro každého, kdo se specializuje na vyhodnocování slabých míst a analýzu hrozeb. Axis tak dostává svému závazku budování transparentního přístupu v kybernetické bezpečnosti.
- *Výchozí bezpečnostní nastavení AXIS OS*: Zařízení běžící na nejnovější verzi AXIS OS jsou již ve výrobním závodě konfigurována do následujícího výchozího nastavení: nepoužívají výchozí nastavené heslo; HTTP a HTTPS jsou aktivovány; bezpečnost a komunikace vyhovující standardu IEEE 802.1X/802.1AR/802.1AE jsou aktivovány; protokoly s nižším zabezpečením jsou deaktivovány. Více informací o výchozím nastavení ochrany najdete *tady*.
- *Axis Edge Vault*: Axis Edge Vault je hardwarová bezpečnostní platforma zabudovaná do zařízení Axis, která obsahuje funkce ochrany proti vniknutí do síťových produktů Axis a umožňuje provádění bezpečnostních operací pomocí kryptografických klíčů. Zajišťuje ochranu celého řetězce pomocí funkce Secure boot a podepsaného OS; ověřování identity zařízení pomocí vestavěných unikátních ID zařízení Axis potvrzujících jeho původ; zabezpečení úložiště klíče pro ukládání kryptografických informací s ochranou proti neoprávněné manipulaci; detekce falšování videozáznamu pomocí podepsaného videa.

4.2 Pravidelné aktualizace a opravy

Axis vydává aktualizace softwaru, které mimo jiné obsahují opravy nově zjištěných slabých míst v zabezpečení hardwarových a softwarových produktů. Společně se svými zařízeními poskytuje Axis také nástroje, které zákazníkům usnadní jejich správu a zajistí udržování jejich softwaru v aktuálním stavu. Nově vydané verze AXIS OS pro připojená zařízení jsou v AXIS Companion, v AXIS Camera Station a v partnerském softwaru pro správu videa, jako je Milestone XProtect® a Genetec™ Security Center, stejně tak jako v nástrojích pro správu zařízení Axis, zvýrazněny. Kromě toho Axis nabízí službu zasílání bezpečnostních oznámení každému, kdo se k odběru přihlásí. Podrobnější informace najdete níže.

- *AXIS OS*: Axis nabízí dvě hlavní alternativy k udržování softwaru zařízení v aktuálním stavu: aktivní program a program dlouhodobé podpory (LTS). Účastníci aktivního programu získají přístup k nejnovějším službám a funkcím, k opravám chyb a k bezpečnostním záplatám. Dlouhodobá podpora (LTS) využívá dobře integrovaný systém třetí strany, který zajišťuje maximalizaci stability softwaru poskytováním pouze oprav chyb a bezpečnostních záplat.
- Nástroje pro správu zařízení: *AXIS Device Manager* a *AXIS Device Manager Extend* usnadňují zákazníkům udržovat zařízení Axis v aktuálním stavu pomocí nejnovějších bezpečnostních záplat a oprav chyb.

  Pro účinnou místní konfiguraci a správu zařízení Axis zajišťuje hromadné zpracování bezpečnostních úkonů, jako je správa přihlašovacích údajů k zařízení, zavádění certifikátů, deaktivace nepoužívaných služeb a upgrade OS AXIS, aplikace AXIS Device Manager.

  AXIS Device Manager Extend je jednoduchá a snadno použitelná aplikace, která umožňuje centrální správu a obsahuje souhrnné informace o všech vašich zařízeních. Budete získávat informace o upgradech softwaru zařízení. Upgrade i další úlohy můžete provádět hromadně pro mnoho zařízení současně. Také budete dostávat návrhy na výměnu produktů. Veškerá aktivita je zaznamenávána a plně dohledatelná. Všechny informace o zařízeních systému lze exportovat za účelem reportování nebo auditu.
- *Služba bezpečnostních oznámení Axis*: Tato služba, ke které Axis všem doporučuje se zaregistrovat, vám zajistí včasná oznámení o bezpečnostních incidentech a slabých místech.

4.3 Ověřování a povolování

Pro zamezení neoprávněným přístupům a zvýšení celkového zabezpečení zařízení Axis společnost Axis podporuje:

- Správu přístupových práv k zařízení podle pracovního zařazení (správce/operátor/uživatel) a možnost centrálního přihlašování/ověřování připojením zařízení Axis ke standardizované centrální IT službě *Active Directory Federation Service* (ADFS) . (ADFS je softwarová komponenta vyvinutá společností Microsoft pro poskytování autorizační služby Single Sign-On (SSO) uživatelům využívajícím serverové operační systémy Windows Server. ADFS umožňuje uživatelům celého podniku přistupovat k aplikacím operačních systémů Windows Server pomocí stejných přihlašovacích údajů.)
- Technologie, které usnadňují *zero-trust networking*(sítě s nulovou důvěrou). U nejnovějších verzí AXIS OS tyto technologie zahrnují IEEE 802.1X, společně s ID zařízení Axis splňujícím požadavky standardu IEEE 802.1AR, pro automatizované a bezpečné připojování zařízení k síti IEEE 802.1X a IEEE 802.1AE (MACsec) pro automatické šifrování datového spojení.

4.4 Šifrování dat

Pro ochranu před zkopírováním nebo neoprávněným přístupem k citlivým informacím podporují produkty Axis:

- protokol HTTPS obsahující podporu přenosu dat TLS 1.2 nebo novější standardy. Přenos videa mezi serverem softwaru pro monitoring AXIS Camera Station a zákazníkem je šifrován standardem AES-256.
- *IEEE 802.1AE (MACsec)* pro automatické šifrování přenášených dat.
- Zabezpečený přenos videa pomocí RTP, označovaného také jako SRTP/RTSPS (od AXIS OS 7.40). SRTP/RTSPS využívá zabezpečenou a koncově zašifrovanou metodu přenosu pro záruku, že k videu ze zařízení Axis získají přístup pouze oprávnění uživatelé.
- *Šifrování lokálního úložiště* (SD karta)

- *Heslem chráněný export záznamu z koncového zařízení* (SD karta, sdílení pomocí sítě) od AXIS OS 10.10. To znamená, že lze vyexportovat záznam chráněný heslem, které posiluje zabezpečení sdílení video dat obsahujících citlivé údaje bez nutnosti ručního šifrování exportovaných záznamů.

4.5 Záznamy o incidentech

Axis poskytuje službu hlášení bezpečnostních incidentů nebo slabých míst zjištěných v našich produktech a službách.

- Axis se zapojila do procesu Common Vulnerability and Exposures (CVE) a získala status Numbering Authority (CNA). To znamená, že Axis uplatňuje při řízení postupy nejlepší praxe a transparentně reaguje na slabá místa zjištěná v našich produktech a službách pro minimalizaci rizika vystavení zákazníků rizikům. Axis také může přiřazovat čísla CVE nově zjištěným slabým místům a nahlásit je na webové stránce *www.cve.org*. *Zásady řízení slabých míst Axis* najdete na axis.com.
- *Tady* se může kdokoli zaregistrovat k odběru bezpečnostních oznámení společnosti Axis.
- Nové verze AXIS OS obsahují bezpečnostní záplaty i opravy chyb. Informace o dostupnosti aktualizovaného softwaru k zařízením jsou obsaženy také v AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend i ve VMS třetích stran, jako jsou Milestone XProtect a Genetec Security Center.
- Axis usiluje o transparentní přístup ke všem kybernetickým útokům na společnost a tyto incidenty se zavazuje hlásit v souladu s postupy vyžadovanými příslušnými švédskými úřady.

4.6 Ochrana soukromí

Axis zveřejňuje vlastní online *zásady ochrany soukromí* a oznámení o ochraně soukromí, ve kterých popisuje, jaká data jsou získávána (například u online účtů na My Axis) a jak se používají.

Společnost Axis rovněž zveřejnila *rámec a postupy kybernetické bezpečnosti* vycházející z tohoto Systému řízení informačního zabezpečení, který získal certifikaci ISO/IEC 27001. Rozsah certifikace Axis ISO/IEC 27001 pokrývá vývoj a chod interní IT infrastruktury a služeb. ISO 27001 je mezinárodně uznávaný standard, který poskytuje návod k ochraně a správě dat podniku formou účinného risk managementu.

Soulad s normou *ISO/IEC 27001* dokazuje, že společnost Axis používá mezinárodně uznávané procesy a osvědčené postupy pro správu své interní informační infrastruktury a systémů, které podporují a poskytují služby zákazníkům a partnerům.

Axis také pomáhá zákazníkům s řešením záležitostí souvisejících s ochranou soukromí během vykonávání dohledu s pořizováním video a audio záznamů. Tato řešení zahrnují:

- Statické privátní masky v kamerách Axis a dynamické privátní masky s aplikací *AXIS Live Privacy Shield*
- Koncová analytika, jako je aplikace *AXIS People Counter* nebo *AXIS P8815-2 3D People Counter*, které získávají a ukládají pouze statistická číselná data a nezpracovávají žádné informace vedoucí ke zjišťování totožnosti
- *Síťové termo kamery*
- *Radarové produkty*
- Nástroj pro úpravu videa v *AXIS Camera Station* pro zakrytí objektů nebo oblastí mimo rozsah zájmu
- *Audio funkce jsou ve výchozím nastavení vypnuté* v produktech videodohledu Axis

Více informací o ochraně soukromí najdete na *axis.com/solutions/privacy-in-surveillance*

4.7 Zabezpečení dodavatelského řetězce

Zabezpečení dodavatelského řetězce od dodavatelů součástí až po zákazníky je důležité pro prevenci vzniku slabých míst.

V rámci přístupu ke kybernetické bezpečnosti uplatňuje Axis *přístup zohledňující celý životní cyklus*. Usilujeme o zmírňování rizik, nejen v celém dodavatelském řetězci od výroby součástek až po hotový produkt, ale také během fází distribuce a implementace, včetně servisní fáze a fáze likvidace.

Mezi způsoby, jakými Axis přestupuje k zabezpečení dodavatelského řetězce, patří:

- Objednávání kritických komponent přímo od strategických dodavatelů. Úzce spolupracujeme s partnery z řad výrobců. Výrobní procesy jsou monitorovány a data jsou nepřetržitě (24/7) sdílena s Axis. Tím je zaručena analýza a transparence v reálném čase. Zjistit více o *zabezpečení dodavatelského řetězce Axis*.
- Vestavěná bezpečnostní výbava Axis Edge Vault, která chrání zařízení Axis před zneužitím následujícími způsoby:
  - **Podepsaný OS**: garantuje, že instalovaný AXIS OS skutečně pochází od značky Axis. Také kontroluje, že jakýkoli nový OS AXIS, který má být instalován na zařízení, rovněž obsahuje podpis Axis.
  - **Funkce Secure boot**: Umožňuje zkontrolovat, je-li operační systém opatřen podpisem Axis. Není-li OS autorizovaný, nebo pokud byl změněn, spuštění bude přerušeno a funkce zařízení zastavena. Ochranu před případnými změnami provedenými během fáze doručení zařízení zajišťuje kontrola podepsaného OS, funkce Secure boot a resetování do továrního nastavení.
  - **Axis ID zařízení** splňuje požadavky standardu IEEE 802.1AR a umožňuje identifikaci zařízení a připojení k síti. ID zařízení Axis je uloženo v zabezpečeném úložišti klíčů (zabezpečená položka, TPM, TEE).
  - **Šifrovaný systém souborů** chrání konfiguraci zákazníka a informace uložené v systému souborů před neoprávněným získáním nebo manipulací v době, kdy zařízení není používáno, například během přepravy od systémového integrátora ke koncovému zákazníkovi.
  - Kromě toho podpora **podepsaného videa** Axis umožňuje koncovým uživatelům ověřit, zda video vyexportované ze zařízení bylo falšováno, nebo ne To je obzvlášť důležité pro forenzní účely při vyšetřování nebo trestním stíhání. Více informací zjistíte na *axis.com/solutions/edge-vault*.
- Software stahovaný z axis.com podléhá kontrole a ověření neporušenosti souboru.
- Certifikace ETSI: Přes 150 produktů Axis používajících AXIS OS 11 nebo vyšší verzi mají certifikaci standardu kybernetické bezpečnosti *ETSI EN 303 645*. Zkratka ETSI znamená Evropský ústav pro telekomunikační normy (European Telecommunications Standards Institute). Požadavky se týkají samotných zařízení, včetně podpory hardwarových bezpečnostních funkcí, jako je bezpečné ukládání klíčů, a výchozích bezpečnostních prvků, jako je zapnutý protokol HTTPS a nepoužívání univerzálních výchozích hesel. Další aspekt zahrnuje správu životního cyklu, například definovanou dobu podpory pro bezpečnostní aktualizace zařízení. Další aspekty zahrnují metodiku pro snižování rizik slabých míst při vývoji softwaru, transparentní politiku správy slabých míst a podporu nejlepších postupů při zpracování osobních údajů. Tyto požadavky zohledňují nejlepší postupy v odvětví, které pomáhají zajistit, aby certifikované produkty měly minimální základní úroveň zabezpečení po celou dobu svého životního cyklu. Tento standard úzce kopíruje Zákon EU o kybernetické bezpečnosti, Směrnici EU o rádiových zařízeních a další standardy a právní předpisy platné na celém světě.

4.8 Školení a podpora

Axis poskytuje svým pracovníkům, partnerům a zákazníkům informace a školení týkající se nejlepší praxe v oblasti kybernetické bezpečnosti. Ta zahrnují:

- Zvyšování povědomí o zabezpečení a školení: Společnost Axis vyvinula informační program průběžného školení našich zaměstnanců pro zamezení a zmírnění bezpečnostních hrozeb našeho podniku. Toto informativní školení je povinné pro všechny pracovníky Axis. Podle pracovního zařazení je pak vývojářům systémů a zadavatelům doporučováno další školení na oblast zabezpečení.
- *Školení Axis Academy*: Tato školení jsou dostupná pro zákazníky a zahrnují online kurz o kybernetické bezpečnosti a *Přístup Axis ke kybernetické bezpečnosti*.
- Příručky *Hardening guide* dostupné online pro:
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Síťové switche Axis*
- *AXIS OS Security Scanner Guide*: Axis doporučuje provádět bezpečnostní kontroly zařízení Axis pro kontrolu, zda neobsahují slabá místa nebo chyby v konfiguraci. AXIS OS Security Scanner Guide nabízí doporučení, jak vyřešit určitá výsledky bezpečnostního skenu, a popisuje nejčastější „falešně pozitivní nálezy".
- *AXIS OS Forensic Guide*: Tento průvodce obsahuje rady technické povahy pro všechny pracovníky zajišťující forenzní analýzu zařízení Axis v případě kybernetického útoku na okolní síť a IT infrastrukturu kolem instalovaného zařízení Axis.

Pro více informací o společnosti Axis a kybernetické bezpečnosti prosím navštivte *Portál kybernetické bezpečnosti Axis*.

T10210486/CS/M3.3/2406

O společnosti Axis Communications

Axis vytváří chytřejší a bezpečnější svět díky řešením, která vedou ke zlepšení bezpečnosti a obchodních výsledků. Společnost Axis, lídr v oboru síťových technologií, nabízí řešení v oblasti videodohledu, řízení přístupu, interkomů a audiosystémů. Všechna tato řešení jsou rozšířena o inteligentní analytické aplikace a doplňuje je velmi kvalitní školení.

Axis má přibližně 4 000 zaměstnanců ve více než 50 zemích a při poskytování řešení zákazníkům spolupracuje s partnery v oblasti technologií a systémové integrace z celého světa. Společnost Axis byla založena v roce 1984 a sídlí ve švédském Lundu.