**NIS 2 – Trend Article**

**Cesta k digitální bezpečnosti: co přináší nová směrnice EU NIS2?**

**Kybernetické hrozby a evropská odpověď**

Rostoucí digitalizace přináší nejen pokrok, ale i zvyšující se rizika spojená s kybernetickými útoky. Už v roce 2016 Evropská unie zavedla směrnici NIS (Network and Information Security) s cílem posílit kybernetickou bezpečnost ve strategicky důležitých odvětvích, které jsou pro fungování společnosti nezbytné. Konkrétně se jednalo o energetiku, dopravu, bankovnictví, finanční trhy, zdravotní péči, vodní hospodářství a digitální infrastrukturu.

Od té doby však došlo k zásadním změnám ve společnosti, přičemž jednu z hlavních rolí hrála pandemie COVID-19. Hromadné nasazení videokonferenčních nástrojů jako MS Teams, Zoom nebo Google Meet a zvýšená poptávka po e-commerce a doručovacích službách, zintenzivnily přechod do digitálního světa. McKinsey odhaduje, že pandemie urychlila digitalizaci o 3 až 4 roky. Tento vývoj ovšem přinesl i nové výzvy v oblasti kybernetické bezpečnosti a EU musela svou směrnici aktualizovat.

**NIS2: Přísnější pravidla pro bezpečnější svět**

V listopadu 2022 tak EU přijala novou směrnici NIS2, která výrazně rozšiřuje působnost původní legislativy a zpřísňuje bezpečnostní opatření. Kromě sedmi původních sektorů nyní NIS2 pokrývá i nové oblasti, jako jsou výrobní průmysl, poštovní a kurýrní služby, nebo věda, výzkum a vzdělávání.

NIS2 zavádí pro dotčené organizace v těchto sektorech povinnost identifikovat a řídit kybernetická rizika, zabezpečit informační systémy a pravidelně školit své zaměstnance. Jedním z nových nařízení je například i povinnost hlásit závažné bezpečnostní incidenty do 24 hodin od jejich zjištění, s podrobným reportem do 72 hodin a závěrečnou zprávou do 30 dnů.

Směrnice také rozděluje organizace do dvou kategorií – „zásadní“ a „důležité“ subjekty, přičemž každá kategorie má specifické povinnosti. Sankce za nedodržení povinností a pravidel mohou být velmi vysoké. Zásadním subjektům hrozí pokuta až 10 milionů EUR (cca 240 milionů Kč) nebo 2 % z celosvětového ročního obratu, podle toho, která částka je vyšší. Důležitým subjektům může být uložena pokuta až 7 milionů EUR (cca 170 milionů Kč) nebo 1,4 % z obratu.

NIS2 tedy hraje klíčovou roli v zajištění kybernetické bezpečnosti v celé EU. Organizace a firmy zavazuje k zavádění nových opatření a dodržování přísných pravidel, která mají chránit kritickou infrastrukturu, jako jsou energetické sítě, vodní hospodářství a zdravotnictví. Tím je zajištěno, že základní služby, na které se lidé spoléhají, zůstanou funkční a bezpečné i v případě kybernetických útoků.

**Jak se na NIS2 připravuje 2N?**

Jelikož má společnost 2N více než 250 zaměstnanců a roční obrat vyšší než 10 milionů EUR, veškerá nařízení a požadavky z této směrnice se ji bezprostředně týkají. Společnost zároveň spadá do několika regulovaných odvětví, jako je „výroba elektronických přístrojů a zařízení“, „poskytování veřejně dostupných služeb elektronických komunikací“ a také „poskytovatel služeb cloud computingu“.

Problematikou kybernetické bezpečnosti se 2N zabývá dlouhodobě a je držitelem certifikátu ISO 27001, který pravidelně a úspěšně obnovuje v rámci dozorových a recertifikačních auditů. V letošním roce navíc získala i bezpečnostní certifikaci IEC 62443-4-1, která se vztahuje na její výtahové produkty.

Co 2N čeká dál? Společnost musí nadále pravidelně a pečlivě revidovat svá stávající bezpečnostní opatření a současně s tím začíná plnit přísná pravidla směrnice NIS2. V rámci toho provádí rozdílovou analýzu, která určí, jaké povinnosti již splňuje díky certifikaci ISO 27001, a co je potřeba nově implementovat. Protože kybernetická bezpečnost patří mezi hlavní priority 2N, firma očekává, že zavedení zbývajících opatření proběhne hladce a v požadovaném termínu. Můžete si tak být jisti, že když se rozhodnete pro spolupráci se 2N, neriskujete nedodržení směrnic EU.

**Znalosti, důvěra a transparentnost jako klíčové hodnoty**

V oblasti kybernetické bezpečnosti 2N dlouhodobě staví na znalostech a zkušenostech své mateřské společnosti AXIS. Odborníci na téma cybersecurity z obou firem jsou v každodenním kontaktu a sdílejí spolu osvědčené postupy pro bezpečný vývoj.

Jedním z klíčových nástrojů, které 2N převzala od své mateřské společnosti, je Axis Security Development Model (ASDM), který do vývoje zavádí 13 procesů a postupů zaměřených na implementaci a následné ověřování bezpečnostních opatření v každé fázi vývoje. Tento přístup minimalizuje riziko bezpečnostních incidentů a posiluje důvěru a spokojenost zákazníků.

Právě důvěra a transparentnost mezi firmou a zákazníky jsou pro 2N klíčové hodnoty. Na webových stránkách společnosti (2n.com) tak naleznete veškeré materiály a informace týkající se kybernetické bezpečnosti. 2N touto transparentní komunikací nejen zdůrazňuje bezpečnost svých produktů a poskytovaných služeb, ale také posiluje důvěru v jejich spolehlivost.

**E-mail – 2N Hardening Guide**

**Předmět:** Posilte bezpečnost své sítě pomocí průvodce 2N Hardening Guide

**Preheader:** Ke stažení

Vážený [jméno příjemce],

v dnešním rychle se vyvíjejícím světě kybernetické bezpečnosti **již není zajištění bezpečnosti vašich zařízení založených na protokolu IP jen volnou - je to nezbytnost**. Vzhledem k tomu, že kybernetické hrozby jsou stále sofistikovanější, nebylo zabezpečení systémů nikdy naléhavější jako je nyní.

Abychom vám pomohli udržet si náskok, nabízíme 2N Hardening Guide **- komplexní zdroj, který vás provede touto problematikou a vysvětlí osvědčené postupy** pro zlepšení zabezpečení síťových zařízení 2N.

Ať už spravujete zařízení v prostředí s vysokým stupněm zabezpečení, jakými jsou např. zdravotnictví nebo státní správa, nebo jen chcete zabezpečit obytnou či multifunkční budovu, tato doporučení jsou navržena tak, aby minimalizovala zranitelnost a posílila vaši obranu.

Co se dozvíte

* **Nastavení silných hesel:** Zavedení spolehlivých pověření, která zabrání neoprávněnému přístupu.
* **Pravidelné aktualizace firmwaru:** Zajištění známých slabých míst, abyste měli náskok před hrozbami
* **Bezpečné komunikační protokoly:** Zajištění bezpečné komunikace mezi zařízeními
* **Povolení šifrování:** Ochrana citlivých dat během přenosu
* **Zakázání nepotřebných služeb:** Minimalizace potenciálních ploch pro útoky
* **Omezení přístupu k síti:** Snížení viditelnosti sítě omezením přístupu jen na důvěryhodné uživatele
* **Segmentace sítě:** Izolování kritických zařízení od širšího síťového provozu za účelem zvýšení bezpečnosti

Nečekejte, až dojde k narušení bezpečnosti. Vzdělávejte se a chraňte svůj systém okamžitě. Příručka 2N Hardening Guide je vaším základním zdrojem informací pro udržení robustní a bezpečné sítě.

[Stáhnout]

S pozdravem,

**Banner - trendový článek**

Pohled 2N na směrnici NIS2

Dostáváte stále více dotazů ohledně připravované směrnice EU NIS2 a jejího dopadu? V tomto článku se dozvíte, co NIS2 znamená, koho se týká a jak se na ni připravuje 2N, přední dodavatel řešení pro přístupové systémy.

>>Čtěte dál