Směrnice NIS2: Řešení na klíč

Od auditu a analýzy rizik, přes financování, až po integraci technologií

Více informací najdete na

www.is4security.cz/nis2

Od 16. ledna 2023 je v platnosti **směrnice NIS2**, která posiluje **kybernetickou bezpečnost v klíčových odvětvích Evropské unie**. Členské státy EU mají do 17. října 2024 povinnost ji implementovat do své národní legislativy.

§

IS4 security

Feel Real Trust

VENDOR REPRESENTATIVE COMPANY

Bitdefender

sectona

endian

KAPITOLA 01

NIS2: ŠIRŠÍ OCHRANA PRO KRITICKOU INFRASTRUKTURU V EU

PODLÉHÁ VAŠE ORGANIZACE REGULACI NIS2?

Směrnice NIS2 se zaměřuje na ochranu klíčových odvětví a služeb, které jsou nezbytné pro fungování společnosti. Jejich narušení by mohlo mít závažné dopady na chod ekonomiky, každodenní život občanů a bezpečnost státu. Rozděluje je do 2 kategorií: Základní subjekty a Důležité subjekty. Rozdělení umožňuje lépe zohlednit míru rizika a nastavit odpovídající dohledové mechanismy a požadavky na kybernetickou bezpečnost.

ZÁKLADNÍ SUBJEKTY

Mezní hodnoty

250+	50+	43+
zaměstnanců	obrat v mil. €	aktiva v mil. €

Sektory s vysokou kritičností

- Energetika
- Odpadní voda
- Doprava
- Zdravotnictví
- Bankovnictví
- Digitální infrastruktura
- Poskytovatelé řízených ICT služeb
- Veřejná správa
- Pitná voda
- Infrastruktura finančních trhů
- Vesmír

DŮLEŽITÉ SUBJEKTY

Mezní hodnoty

50-250	10-50	< 43
zaměstnanců	obrat v mil. €	aktiva v mil. €

Další kritické sektory

- Poštovní a kurýrní služby
- Odpadní hospodářství
- Chemický průmysl
- Potravinářství
- Výroba elektronických a optických přístrojů aj.
- Poskytovatelé digitálních služeb
- Výzkum

KAPITOLA 02

REGULOVANÉ SEKTORY

POŽADAVKY NA KYBERNETICKOU BEZPEČNOST SMĚRNICE NIS2?

Implementací směrnice členské státy EU zajistí, že **základní** a **důležité** subjekty přijmou vhodná a přiměřená technická, provozní a organizační opatření k řízení rizik. Tato opatření představují pro bezpečnost sítí a informačních systémů, jež tyto subjekty používají pro svůj provoz nebo pro poskytování svých služeb, prevenci nebo minimalizaci dopadu incidentů, a to jak na samotné subjekty, tak na příjemce jejich služeb. Opatření jsou založena na přístupu zohledňujícím všechna rizika, a jejich cílem je chránit síťové a informační systémy, a fyzická prostředí těchto systémů, před incidenty. Mezi tato opatření patří například:

1. Politiky týkající se **analýzy rizik** a bezpečnosti informačních systémů.
2. **Řešení incidentů.**
3. Zajištění **kontinuity provozu**, jako je správa zálohování, obnovení po havárii a krizové řízení.
4. **Bezpečnost dodavatelského řetězce**, včetně bezpečnostních aspektů, týkajících se vztahů mezi jednotlivými subjekty a jejich přímými dodavateli nebo poskytovateli služeb.
5. **Bezpečnost** při pořizování, vývoji a údržbě sítí a **informačních systémů**, včetně řešení a odhalování zranitelností.
6. Pravidla a postupy pro **hodnocení účinnosti opatření pro řízení rizik** v oblasti kybernetické bezpečnosti.
7. Základní postupy **kybernetické hygieny** a školení o kybernetické bezpečnosti.
8. Pravidla a postupy týkající se **používání kryptografie a šifrování.**
9. **Zabezpečení lidských zdrojů**, zásady řízení přístupu a správa aktiv; používání vícefaktorové autentizace nebo řešení průběžné autentizace, zabezpečené hlasové, video a textové komunikace, a popřípadě zabezpečené systémy nouzové komunikace v rámci subjektu.

KAPITOLA 02

SANKCE

Příslušné orgány mohou ukládat **vysoké správní pokuty** (viz níže) za porušení povinností, vyplývajících z vnitrostátních právních předpisů, kterými se provádí směrnice NIS2. Kromě pokut může dozorový orgán uložit i další sankce.

Základní subjekty

až 10 000 000 €

nebo **2 %** celosvětového ročního obratu

Důležité subjekty

až 7 000 000 €

nebo **1,4 %** celosvětového ročního obratu

KAPITOLA 04

PROČ SPOLUPRACOVAT S IS4 SECURITY

Ve spolupráci s našimi partnery zajistíme celý proces implementace kybernetické bezpečnosti do vaší společnosti, počínaje auditními a analytickými službami, přes návrh a plán implementace, zajištění financování, až po realizaci a následné monitorování.

PROCES ZAJIŠTĚNÍ SOULADU SE SMĚRNICÍ NIS2 A NOVÝM ZOKB:

AUDITNÍ A ANALYTICKÉ SLUŽBY

Než se pustíte do akce, je potřeba vědět, odkud vycházíte! Počáteční audity odhalí, jak daleko je vaše firma od shody s NIS2.

NÁVRH A PLÁN IMPLEMENTACE

Na základě analýzy vám navrhneme individuální řešení a plán implementace. Každé řešení je šité na míru vašim specifickým požadavkům a situaci.

ZAJIŠTĚNÍ FINANCOVÁNÍ

Zajistíme financování kybernetické bezpečnosti a digitální transformaci vaší firmy. Dotace až 60 % (průběžná i ex post).

REALIZACE A MONITOROVÁNÍ

Po schválení plánu kybernetické bezpečnosti nastává fáze realizace. V ní se navržená řešení převedou do praxe.

JAK ŘEŠENÍ Z PORTFOLIA IS4 SECURITY POMŮŽE SE SPLNĚNÍM POŽADAVKŮ NIS2?

Firemní koncept **„Vendor Representative Company“** umožňuje kombinovat nejlepší technologie jedním dodavatelem. Řešení kybernetické bezpečnosti tak můžete pokrýt řešeními, které se vzájemně doplňují.

Bitdefender endian sectona

Gartner Peer Insights Customers' Choice 2024 · AV comparatives 2023 · Forrester Wave Leader 2023 Endpoint Security · Gartner Peer Insights Customers' Choice 2024 · Gartner Peer Insights Customers' Choice 2024

ANALÝZA RIZIK A BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

Analýza rizik a zajištění bezpečnosti informačních systémů je kritické pro ochranu proti kybernetickým hrozbám. Identifikuje a hodnotí možné nebezpečí, zranitelnosti a jejich dopad. Na základě této analýzy lze navrhnout a implementovat opatření pro prevenci, detekci a reakci na útoky. To zabezpečuje ochranu dat, zachování důvěrnosti a nepřetržitou dostupnost systémů.

Bitdefender

Bitdefender® GravityZone Risk Management

Umožňuje bezpečnostním týmům vyhledávat a identifikovat rizika spojená s chybnou konfigurací operačních systémů, se zranitelnými aplikacemi a nebezpečným chováním uživatelů. Identifikace rizik je přímo šitá na míru odvětví dané organizace.

VÍCE INFORMACÍ →

Bitdefender

Bitdefender® GravityZone Patch Management

Posílení zabezpečení a snížení rizika potenciálních zranitelností softwaru, operačních systémů a aplikací, pomocí automatizované správy záplat. S modulem GravityZone Patch Management můžete udržovat své operační systémy a softwarové aplikace aktuální, a využívat komplexní přehled o stavu záplat v celé instalační základně systémů Windows, Linux a MacOS. Modul automatizované správy záplat poskytuje aktualizace pro celou síť pracovních stanic, fyzických serverů nebo virtuálních serverů organizace.

VÍCE INFORMACÍ →

ŘEŠENÍ INCIDENTŮ A ZAJIŠTĚNÍ KONTINUITY PROVOZU

Efektivní správa strukturovaných incidentů má potenciál minimalizovat následky kybernetických útoků a zabezpečit integritu dat a systémů ve vaší organizaci. Klíčovým faktorem pro úspěšnou manipulaci s incidenty je rozpoznání samotného útoku.

Bitdefender

Bitdefender® GravityZone Business Security Enterprise

Dosahujte bezkonkurenční rychlosti a efektivity detekce a reakce napříč koncovými body, identitami, sítěmi, produktivními aplikacemi, cloudy a mobilními zařízeními. Přináší pokročilou ochrana před hrozbami, potlačení útoku prostřednictvím automatické, a lidmi řízené, reakce. Sjednocuje technologie EDR/XDR, Risk Analytics a Hardening do jedné konzole s jediným agentem, a využívá 30 vrstev pokročilých technik k úspěšnému zastavení útoků v celém životním cyklu hrozeb, od prvního kontaktu, přes případné proniknutí, persistenci, až po škodlivé aktivity. Funkce Bitdefender Ransomware Remediation blokuje útoky ransomwaru a automaticky obnovuje obsah zašifrovaných souborů bez nutnosti platit výkupné.

VÍCE INFORMACÍ →

endian

Endian® UTM & Bezpečnostní gatewaye Endian IoT

Bezpečnostní gatewaye Endian IoT jsou vybaveny několika bezpečnostními funkcemi, které dokáží odhalit a zastavit kybernetické útoky: Hloubková kontrola paketů (DPI) analyzuje datové pakety, odesílané přes síť. Na rozdíl od tradičních metod analýzy, které se zaměřují pouze na metadata, DPI provádí analýzu až na uživatelskou úroveň a identifikuje více než 300 protokolů IT/OT. a 2000 aplikací. To umožňuje zjistit běžný stav sítě. Pokud se v síti vyskytne anomálie provozu, je odhalena pomocí systému detekce narušení (IDS). Pokud se jedná o útok, použije se systém prevence narušení (IPS - Intrusion Prevention System) zasáhne, aby jej zastavil.

VÍCE INFORMACÍ →

POLITIKY PRO KRYPTOGRAFII A ŠIFROVÁNÍ

Politiky pro kryptografii a šifrování jsou základem pro silnou kybernetickou bezpečnost. Definují, jaká data a komunikace budou šifrovány a jakými metodami. Zajišťují ochranu citlivých informací před neoprávněným přístupem a snižují riziko úniku dat. Kvalitní politiky řídí správné používání šifrování napříč organizací, a tím posilují celkovou odolnost vůči hrozbám.

Bitdefender

Bitdefender® GravityZone Full Disk Encryption

Nativní, osvědčený šifrovací modul, který zajistí, aby vaše firemní data byla v bezpečí a snížilo se riziko jejich ztráty nebo krádeže. GravityZone Full Disk Encryption lze přidat k jakémukoli řešení zabezpečení koncových bodů Bitdefender. Používá osvědčené nativní šifrování pro Windows (BitLocker) a Mac (FileVault), není potřeba žádný nový agent. Zároveň poskytuje centrální správu a obnovu klíčů, které pomáhají chránit před neoprávněným přístupem k datům, prostřednictvím vynucení ověřování před spuštěním systému. Tím je zaručeno bezpečné prostředí, odolné proti neoprávněné manipulaci mimo operační systém. Navíc generuje zprávy specifické pro šifrování, které pomáhají organizacím splnit požadavky na zajištění souladu s legislativou.

VÍCE INFORMACÍ →

endian

Endian® UTM & Bezpečnostní brány průmyslového IoT

Používáním virtuální privátní sítě (VPN) je komunikace v sítích šifrovaná. Díky použití moderních kryptografických algoritmů je datová komunikace vždy zabezpečena. Zařízení Endian podporují vytváření sítí VPN buď na základě protokolu IPsec, který je podporován většinou operačních systémů a síťových zařízení, nebo na základě služby OpenVPN. Navíc portál umožňuje vzdáleným uživatelům připojit se k vybraným místním hostitelům bez nutnosti připojení VPN protokolu IPsec.

VÍCE INFORMACÍ →

BEZPEČNOST V SÍTI & ZPRACOVÁNÍ ZRANITELNOSTÍ

Detekce kybernetických bezpečnostních událostí hraje klíčovou roli v moderním digitálním světě. Rychlé odhalení anomálií a útoků umožňuje okamžitou reakci a minimalizaci škod. Aktivní monitoring zabezpečuje ochranu dat, sítí a systémů, a posiluje schopnost organizace čelit neustále se vyvíjejícím hrozbám.

Bitdefender

Bitdefender® GravityZone Business Security Enterprise

Přináší pokročilou ochranu před hrozbami, potlačení útoku prostřednictvím automatické, a lidmi řízené, reakce. Odhaluje a zabraňuje útokům na zranitelná místa sítě, včetně útoků hrubou silou, krádeží hesel a laterálního pohybu dříve, než mohou být provedeny. Obrana proti síťovým útokům slouží také jako důležitý zdroj informací pro korelaci incidentů EDR. GravityZone Business Security Enterprise sjednocuje technologie EDR/XDR, Risk Analytics a Hardening do jedné konzole s jediným agentem, a využívá 30 vrstev pokročilých technik k úspěšnému zastavení útoků v celém životním cyklu hrozeb, od prvního kontaktu, přes případné proniknutí, persistenci, až po škodlivé aktivity. Dosahuje bezkonkurenční rychlosti a efektivity detekce a reakce napříč sítěmi, koncovými body, identitami, produktivními aplikacemi, cloudy a mobilními zařízeními. Funkce Bitdefender Ransomware Remediation navíc blokuje útoky ransomwaru a automaticky obnovuje obsah zašifrovaných souborů bez nutnosti platit výkupné.

VÍCE INFORMACÍ →

OCHRANA LIDSKÝCH ZDROJŮ, POLITIKY ŘÍZENÍ PŘÍSTUPŮ A SPRÁVA MAJETKU

Analýza rizik a zajištění bezpečnosti informačních systémů je kritické pro ochranu proti kybernetickým hrozbám. Identifikuje a hodnotí možné nebezpečí, zranitelnosti a jejich dopad. Na základě této analýzy lze navrhnout a implementovat opatření pro prevenci, detekci a reakci na útoky. To zabezpečuje ochranu dat, zachování důvěrnosti a nepřetržitou dostupnost systémů.

sectona

Sectona® Security Platform

Sectona poskytuje řešení pro správu přístupu uživatelů a zabezpečení, která firmám umožňuje vyhodnocovat chování uživatelů, implementovat vícefaktorové ověřování a zabezpečit kritická aktiva pomocí kryptografie a šifrování. Cílem tohoto přístupu, zaměřeného především na bezpečnostní aspekty, je chránit podniková prostředí rozprostřená mezi koncovými body, lokálními zařízeními a cloudem. Správa oprávněného přístupu (Privileged Access Management) Sectona, je snadno implementovatelné řešení, které vám pomůže splnit požadavky normy NIS2. Díky funkci PAM poskytujeme kompletní auditní stopu, která zjednodušuje zajištění dodržování legislativních požadavků. Sectona PAM také pomáhá zvýšit kybernetickou hygienu tím, že zefektivňuje přístup uživatelů pomocí přísných rámců, jako je přístup Just-in-Time a řízení přístupu na základě rolí.

VÍCE INFORMACÍ →

endian

Endian® Switchboard

Endian Switchboard je srdcem platformy Endian Secure Digital Platform, která bezpečně připojuje uživatele k zařízením (strojům, terénním zařízením atd.). Pomocí granulárních zásad oprávnění mohou podniky kompletně spravovat oprávnění mezi uživateli a branami, zařízeními a jejich příslušnými aplikacemi. Díky tomu mají firemní uživatelé, hosté a dodavatelé správný přístup na základě rolí pouze k zařízením, která potřebují k výkonu své pracovní funkce. Endian poskytuje také vícefaktorovou autentifikaci pro různé služby, a podporuje externí služby, jako je Microsoft Active Directory (AD) a Windows New Technology Lan Manager (NTLM). Uživatelé společnosti Microsoft se tak mohou snadno ověřovat v systémech Endian. Platforma Secure Digital Platform (Switchboard a 4i Edge X) je certifikována podle normy IEC 62443 pro úroveň zabezpečení 62443-3-3 („System Security“) a 62443-4-2 („Component Security“) na úrovni SL2. Tato certifikace zajišťuje, že zákazníci používající platformu Endian Secure Digital Platform jsou schopni splnit nebo překročit průmyslový standard pro průmyslovou a automatizační kybernetickou bezpečnost.

VÍCE INFORMACÍ →

ZABEZPEČENÍ DODAVATELSKÉHO ŘETĚZCE

NIS2 vyžaduje také zabezpečení dodavatelského řetězce a řešení vztahů s dodavateli, protože komplexní bezpečnost IT nelze zajistit bez bezpečných dodavatelů. Směrnice vyžaduje, aby se jednotlivé společnosti zabývaly bezpečnostními riziky IT v dodavatelských řetězcích a dodavatelských vztazích.

endian

Endian® UTM & Bezpečnostní brány průmyslového IoT

EndianOS chrání sítě před bezpečnostními hrozbami od externích dodavatelů. Brána Endian Firewall i DPI zabraňují průniku malwaru přes dodavatele, a mohou tak blokovat kybernetické útoky. Díky integrované antivirové ochraně jsou sítě chráněny i před dalším malwarem.

VÍCE INFORMACÍ →

sectona

Sectona® Security Platform

Správa privilegovaných přístupů Sectona přináší zabezpečení dodavatelsky řízených činnosti nad Vašimi aktivy. Díky možnosti definice přístupu externích uživatelů pomocí přísných rámců, jako je přístup Just-in-Time a řízení přístupu na základě rolí, můžete vyhodnocovat a řídit chování těchto uživatelů a zabezpečit tak svá kritická aktiva pomocí kryptografie a šifrování. Cílem tohoto přístupu, zaměřeného především na bezpečnostní aspekty, je chránit podniková prostředí rozprostřená mezi koncovými body, lokálními zařízeními a cloudem v rámci celého dodavatelského řetězce.

VÍCE INFORMACÍ →

„IS4 security patří mezi renomované dodavatele bezpečnostních řešení pro malé, středně velké i velké firmy a státní organizace. Prosazuje firemní koncept **„Vendor Representative Company“**, který umožňuje kombinovat nejlepší technologie jedním dodavatelem.

IS4 vždy vybírá do portfolia prioritně řešení, která mají jednoduchou správu a nižší provozní nároky, při zachování maximálních nároků na bezpečnost. Takto odladěné portfolio produktů následně přináší ovoce ve formě spokojených zákazníků a dlouhodobých vztahů.“

IS4 security
Feel Real Trust

VENDOR
REPRESENTATIVE
COMPANY

IS4 security s.r.o.

Jordánská 391
198 00 Praha 9

+ 420 245 501 800
info@is4security.cz
www.is4security.cz

IS4 security SK s.r.o.

Karadžičova 16
821 08 Bratislava

+421 907 727 354
info@is4security.sk
www.is4security.sk