Digital Security
Progress. Protected.

Smernica NIS2 - už v zákone

Buďte v súlade s novelizovaným zákonom o kybernetickej bezpečnosti, ktorý transponuje požiadavky smernice NIS2

Digital Security
Progress. Protected.

Novela zákona o kybernetickej bezpečnosti (ZoKB) platná od 1. 1. 2025, ktorá aktualizuje zákon o kybernetickej bezpečnosti č. 69/2018 Z. z. o požiadavky smernice NIS2, prináša nasledujúce kľúčové zmeny.

REGULOVANÉ SUBJEKTY

Novela zákona sa vzťahuje na novo regulované subjekty a tiež rozširuje rozsah pôsobnosti aj na ďalšie systémy a služby subjektov, ktoré boli regulované už pred novelou zákona o kybernetickej bezpečnosti.

POKUTY

Maximálna pokuta za porušenie povinností vyplývajúcich z novely zákona môže byť 10 mil. € alebo 2 % z celosvetového čistého ročného obratu.

KOORDINOVANÝ PRÍSTUP K ZRANITEĽNOSTIAM

Novela zákona podporuje koordinovaný prístup k zraniteľnostiam v IKT systémoch s cieľom minimalizovať riziko zneužitia.

BEZPEČNOSŤ DODÁVATEĽSKÉHO REŤAZCA

Novela zákona kladie väčší dôraz na bezpečnosť dodávateľského reťazca.

VZDELÁVANIE

Novela zákona zaviedla povinnosť prevádzkovateľov základných služieb zabezpečiť jasné určenie zodpovedností, vzdelávanie a budovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti, pričom podrobnosti stanoví úrad právnym predpisom.

AUDIT A SAMOHODNOTENIE

Regulované subjekty sú povinné pravidelne vykonávať audity a samohodnotenia na vyhodnotenie stavu svojej kybernetickej bezpečnosti.

HLÁSENIE INCIDENTOV

Novela zákona zaviedla podrobnejšiu úpravu povinnosti regulovaných subjektov hlásiť kybernetické incidenty. Táto úprava je obsiahnutá v § 24 zákona.

APLIKÁCIA BEZPEČNOSTNÝCH OPATRENÍ NA ZÁKLADE ANALÝZY RIZÍK

Novela zákona zaviedla podrobnejšie pravidlá pre všeobecné bezpečnostné opatrenia, ktoré budú stanovené vyhláškou, ich implementácia bude vychádzať z analýzy rizík (ktorú musí vypracovať odborník) alebo sektorových štandardov, pričom prevádzkovatelia základných služieb ich musia zaviesť do 12 mesiacov od zápisu do registra.

SYSTÉM CERTIFIKÁCIE KYBERNETICKEJ BEZPEČNOSTI

Novela zákona zavádza požiadavky na certifikáciu bezpečnosti IKT produktov, služieb a procesov, čím sa zvyšuje úroveň ochrany pred kybernetickými hrozbami.

Kedy a čo musia splniť regulované subjekty?

Novela zákona o kybernetickej bezpečnosti prináša nové povinnosti pre novo regulované subjekty a pre subjekty, ktoré boli regulované už pred novelou zákona o kybernetickej bezpečnosti.

ČASOVÁ OS PRE NOVÉ SUBJEKTY

Táto časová os zobrazuje povinnosti pre prevádzkovateľov základnej služby (PZS) podľa § 17 novelizovaného zákona a prevádzkovateľov kritickej základnej služby (PKZS) podľa § 18 ods. 1 a ods. 2 novelizovaného zákona.

1. 1. 2025
Účinnosť novely zákona

2. 3. 2025
Oznámenie úradu

MAREC 2025
Oznámenie úradu o zápise do registra PZS (§ 17 ods. 4 ZoKB) – pre toto oznámenie nemá úrad lehotu

APRÍL 2025
Vznik práv a povinností pre subjekt – 30 dní od zápisu do registra PZS

MAREC 2026
Povinnosť zaviesť bezpečnostné opatrenia

MAREC 2027
Prvý audit alebo samohodnotenie

INFORMÁCIE PRE EXISTUJÚCE SUBJEKTY

Od 1. januára 2025 sa prevádzkovatelia základných služieb podľa zákona platného do 31. decembra 2024 považujú za prevádzkovateľov kritických základných služieb podľa nových pravidiel. Rovnako, poskytovatelia digitálnych služieb, ktorí podliehajú pravidlám platným do konca roka 2024, sa od 1. januára 2025 považujú za prevádzkovateľov základných služieb podľa novelizovaného zákona.

Pre existujúce subjekty
je kľúčovým dátumom 31. december 2026.

Do tohto dátumu môže úrad rozhodnúť o výmaze zo zoznamu regulovaných subjektov a zároveň sa končí prechodné obdobie pre plnenie bezpečnostných opatrení a výkon auditu podľa starých pravidiel.

Koho sa týka novela zákona o kybernetickej bezpečnosti?

Novela zákona o kybernetickej bezpečnosti sa zameriava na subjekty, ktoré pôsobia v sektoroch s vysokou úrovňou kritickosti alebo v iných kritických sektoroch. Nové požiadavky podľa novely zákona zavádzajú zvýšené štandardy ochrany pre lepšiu odolnosť voči kybernetickým hrozbám.

NOVELA ZÁKONA ZARAĎUJE MEDZI REGULOVANÉ SUBJEKTY ORGANIZÁCIE SPADAJÚCE DO TÝCHTO SEKTOROV:

- Energetika
- Doprava
- Financie
- Zdravotníctvo
- Voda a atmosféra
- Digitálna infraštruktúra
- Riadenie služieb IKT (medzi podnikmi)
- Verejná správa
- Vesmír
- Poštové a kuriérske služby
- Odpadové hospodárstvo
- Výroba a distribúcia chemických látok
- Výroba, spracovanie a distribúcia potravín
- Výroba
- Poskytovatelia digitálnych služieb
- Výskum

Jedným z hlavných kritérií na určenie regulovaného subjektu je jeho veľkosť a obrat. Nová legislatíva sa vzťahuje na organizácie, ktoré majú viac ako 50 zamestnancov a obrat nad 10 miliónov eur. **Zákon však identifikuje aj subjekty, ktoré môžu byť zaradené medzi regulované bez ohľadu na ich veľkosť a obrat.**

Ak máte pochybnosti, či spadáte pod novelu, môžete použiť indikatívnu pomôcku na určenie subjektu, ktorú pripravil Národný bezpečnostný úrad.

AKÉ BEZPEČNOSTNÉ OPATRENIA POTREBUJETE SPĹŇAŤ?

Podľa novely zákona o kybernetickej bezpečnosti sú regulované subjekty povinné zaviesť prísnejšie bezpečnostné opatrenia, ako je **monitorovanie sietí, správu zraniteľností či včasné hlásenie kybernetických incidentov**. Mnohé z týchto požiadaviek môžu jednoducho splniť vďaka komplexným riešeniam a službám od spoločnosti ESET, ktoré im pomôžu posilniť ochranu a odolnosť voči hrozbám.

Požiadavky, s ktorými vám pomôžeme

ORGANIZÁCIA A RIADENIE INFORMAČNEJ BEZPEČNOSTI A KYBERNETICKEJ BEZPEČNOSTI

Firmy musia zaviesť systém riadenia kybernetickej bezpečnosti, ktorý určí zodpovednosti a procesy na ochranu ich údajov a systémov. To zahŕňa jasné určenie úloh pre jednotlivých zamestnancov, pravidlá správy prístupu a kontrolné mechanizmy. Cieľom je vytvoriť organizačnú štruktúru, ktorá zabezpečí dodržiavanie bezpečnostných opatrení na všetkých úrovniach.

Spoločnosť ESET poskytuje konzultačné služby pre zavedenie organizácie a riadenie informačnej bezpečnosti.

VIAC INFORMÁCIÍ

SPRÁVA ZRANITEĽNOSTÍ A KYBERNETICKÝCH HROZIEB

Každá organizácia musí aktívne monitorovať a aktualizovať svoje systémy na ochranu pred novými zraniteľnosťami a hrozbami. To znamená pravidelné skenovanie systémov, analýzu rizík a zabezpečenie aktualizácií softvéru. Firmy tým môžu predísť kybernetickým útokom využívajúcim zastarané systémy a softvérové chyby.

Funkcia Vulnerability and Patch Management na správu zraniteľností a záplat je súčasťou riešenia ESET PROTECT MDR.

VIAC INFORMÁCIÍ

RIADENIE UDALOSTÍ A KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

Firmy musia mať zavedené postupy na detekciu, reakciu a riešenie kybernetických bezpečnostných incidentov. To zahŕňa nastavenie procesov pre riešenie incidentov, ktoré umožnia minimalizovať ich vplyv a rýchlo obnoviť bežnú prevádzku.

Nástroj rozšírenej detekcie a reakcie (XDR) ESET Inspect, ktorý rýchlo zachytáva a reaguje na incidenty, je súčasťou riešenia ESET PROTECT MDR.

VIAC INFORMÁCIÍ

RIADENIE KONTINUITY, ČINNOSTÍ, ZÁLOHOVANIE, OBNOVA SYSTÉMOV PO HAVÁRII A KRÍZOVÉ RIADENIE

Organizácie musia zabezpečiť, aby ich systémy zostali funkčné aj počas krízových situácií, napríklad vďaka zálohovaniu dát a testovaniu obnovy systémov. Tento proces umožňuje rýchly návrat k bežnej činnosti a minimalizáciu strát pri výpadkoch či haváriách.

Na zavedenie procesov pre zabezpečenie kontinuity môžete využiť ESET konzultačné služby.

VIAC INFORMÁCIÍ

SPRÁVA AKTÍV A RIADENIE KYBERNETICKÝCH HROZIEB A RIZÍK

Správa aktív vyžaduje, aby firmy presne vedeli, čo má pre nich hodnotu a je aktívum, ktoré treba spravovať. Identifikácia a riadenie rizík zabezpečuje, že spoločnosť vie, kde sú potenciálne slabiny, a vie ich včas eliminovať alebo minimalizovať ich vplyv na prevádzku.

S vytvorením katalógu aktív a manažmentom rizík vám pomôže ESET konzultačnými službami v oblasti riadenia informačnej bezpečnosti.

VIAC INFORMÁCIÍ

BEZPEČNOSŤ PRI NADOBÚDANÍ, VÝVOJI A ÚDRŽBE SIETE, INFORMAČNÝCH SYSTÉMOV, APLIKÁCIÍ A KONFIGURÁCIÍ

Každá nová aplikácia, sieť alebo informačný systém musí spĺňať bezpečnostné kritériá už počas vývoja a testovania. Firmy musia zabezpečiť, že softvéry a siete prejdú bezpečnostnými auditmi pred uvedením do prevádzky, čím sa minimalizuje riziko kybernetických hrozieb.

Spoločnosť ESET poskytuje organizáciám možnosti penetračného testovania vyvíjaných informačných systémov a aplikácií.

VIAC INFORMÁCIÍ

POSTUPY POSUDZOVANIA ÚČINNOSTI OPATRENÍ, RIADENIE SÚLADU A KONTROLNÉ ČINNOSTI

Organizácie musia pravidelne hodnotiť účinnosť svojich bezpečnostných opatrení, napríklad prostredníctvom auditov či kontrol. Zabezpečia tak súlad s normami a identifikujú oblasti, kde treba zlepšiť ochranu, čím predchádzajú vzniku bezpečnostných slabín.

Spoločnosť ESET poskytuje organizáciám možnosti penetračného testovania, technických auditov auditu kybernetickej bezpečnosti podľa požiadaviek NBÚ.

VIAC INFORMÁCIÍ

SPRÁVA IDENTÍT A PRÍSTUPOV

Firmy musia zaviesť systém správy identít a prístupov, ktorý určí, kto môže pristupovať k jednotlivým systémom a údajom, a pod akými podmienkami. To zahŕňa aj silné overovanie prístupu pomocou viacfaktorovej autentifikácie a pravidelné revízie prístupových práv, aby sa zabezpečilo, že iba oprávnení používatelia majú prístup k citlivým informáciám.

Nástroj na dvojfaktorovú autentifikáciu ESET Secure Authentication je súčasťou riešenia ESET PROTECT MDR.

VIAC INFORMÁCIÍ

KRYPTOGRAFICKÉ OPATRENIA A ZÁSADY POUŽÍVANIA KRYPTOGRAFIE

Na ochranu citlivých údajov musia firmy používať šifrovacie technológie, ktoré zabraňujú neoprávnenému prístupu. Kryptografia je základným nástrojom na zabezpečenie dôvernosti a integrity dát pri ich ukladaní a prenose medzi systémami.

Šifrovanie celého disku ESET Full Disk Encryption je súčasťou riešenia ESET PROTECT MDR.

VIAC INFORMÁCIÍ

BEZPEČNOSŤ PRI PREVÁDZKE SIETÍ A INFORMAČNÝCH SYSTÉMOV

Na zaistenie bezpečnosti siete a systémov je potrebné pravidelné monitorovanie, zabezpečenie dátových prenosov a ochrana proti neoprávneným prístupom. Firmy musia tiež implementovať opatrenia na minimalizáciu rizika, ako sú firewallové systémy a nástroje na ochranu proti útokom.

Nástroj rozšírenej detekcie a reakcie (XDR) ESET Inspect monitoruje v reálnom čase všetku podozrivú aktivitu v celej sieti a je súčasťou riešenia ESET PROTECT MDR.

VIAC INFORMÁCIÍ

BEZPEČNOSŤ A SPÔSOBILOSTI ĽUDSKÝCH ZDROJOV

Firmy musia školením a vzdelávaním svojich zamestnancov zabezpečiť, aby rozumeli kybernetickým hrozbám a dodržiavali bezpečnostné zásady. Dôležité je pravidelné vzdelávanie a podpora v oblasti informačnej bezpečnosti, pretože ľudský faktor môže byť významným rizikom.

Spoločnosť ESET ponúka e-learningové aj prezenčné školenie kybernetickej bezpečnosti pre zamestnancov.

VIAC INFORMÁCIÍ

OCHRANA PROTI ŠKODLIVÉMU KÓDU A NEŽIADUCEMU OBSAHU

Organizácie sú povinné používať antivírusové programy a riešenia na detekciu a blokovanie škodlivého softvéru, aby zabránili infikovaniu systémov. Kontrolou a filtrovaním obsahu sa zabezpečí, že sa do systémov nedostanú nežiaduce súbory alebo odkazy, ktoré by mohli predstavovať bezpečnostné riziko.

Ochrana koncových zariadení ESET Endpoint Security poskytuje spoľahlivé zabezpečenie proti škodlivému kódu a je súčasťou riešenia ESET PROTECT MDR.

VIAC INFORMÁCIÍ ESET ENDPOINT SECURITY

VIAC INFORMÁCIÍ ESET MOBILE THREAT DEFENSE

SYSTÉMOVÁ BEZPEČNOSŤ, SIEŤOVÁ BEZPEČNOSŤ A KOMUNIKAČNÁ BEZPEČNOSŤ

Tento bod zahŕňa ochranu pred útokmi na rôznych úrovniach infraštruktúry, od systémových až po komunikačné kanály. Implementáciou bezpečnostných protokolov na úrovni hardvéru, softvéru a sietí sa minimalizuje riziko neoprávneného prístupu a zneužitia údajov počas ich prenosu.

Nástroj rozšírenej detekcie a reakcie (XDR) ESET Inspect neustále monitoruje infraštruktúru, identifikuje a blokuje hrozby v reálnom čase a chráni dáta pri prenose aj v úložisku. Je súčasťou riešenia ESET PROTECT MDR.

VIAC INFORMÁCIÍ

MONITOROVANIE, ZAZNAMENÁVANIE A HLÁSENIE UDALOSTÍ

Organizácie musia zabezpečiť, aby všetky dôležité udalosti a incidenty v ich systémoch boli sledované, zaznamenávané a vyhodnocované. Tento proces tiež zahŕňa povinnosť hlásenia kybernetických incidentov kompetentným orgánom, čo zvyšuje transparentnosť a umožňuje efektívnu reakciu.

Nástroj rozšírenej detekcie a reakcie (XDR) ESET Inspect zaznamenáva incidenty a experti spoločnosti ESET v rámci služby ESET PROTECT MDR zabezpečia, aby organizácie mali potrebné informácie na včasné a správne hlásenie.

VIAC INFORMÁCIÍ

OCHRANA ZÁZNAMOV, SÚKROMIA A OZNAČOVANIE INFORMÁCIÍ

Organizácie musia chrániť citlivé informácie, zabezpečiť súkromie svojich používateľov a označovať údaje podľa ich citlivosti. Implementácia ochrany údajov pri ukladaní a správe záznamov pomáha predchádzať únikom a neoprávnenému prístupu k dôležitým dátam.

Šifrovanie celého disku ESET Full Disk Encryption chráni citlivé údaje a je dostupné v riešení ESET PROTECT MDR.

VIAC INFORMÁCIÍ

DODÁVATEĽSKÝ REŤAZEC

Firmy musia riadiť riziká spojené s dodávateľmi, ktorí môžu mať prístup k ich aktívam. Zahrnutie bezpečnostných požiadaviek do zmlúv a pravidelné audity dodávateľov zabezpečia, že tretie strany dodržiavajú bezpečnostné normy, ktoré chránia citlivé informácie organizácie.

Nástroj rozšírenej detekcie a reakcie ESET Inspect monitoruje prístupy a aktivity tretích strán v systéme, deteguje podozrivé správanie a minimalizuje riziká spojené s integráciou externých dodávateľov. Je dostupné v rámci riešenia ESET PROTECT MDR.

VIAC INFORMÁCIÍ

FYZICKÁ BEZPEČNOSŤ, BEZPEČNOSŤ PROSTREDIA A SPRÁVA KONCOVÝCH ZARIADENÍ

Zabezpečenie fyzického prístupu k citlivým zariadeniam a systémom je rovnako dôležité ako ochrana digitálneho priestoru. Firmy musia implementovať bezpečnostné opatrenia na ochranu priestorov a kontrolovať prístup k týmto priestorom, aby zabránili neoprávnenému fyzickému prístupu.

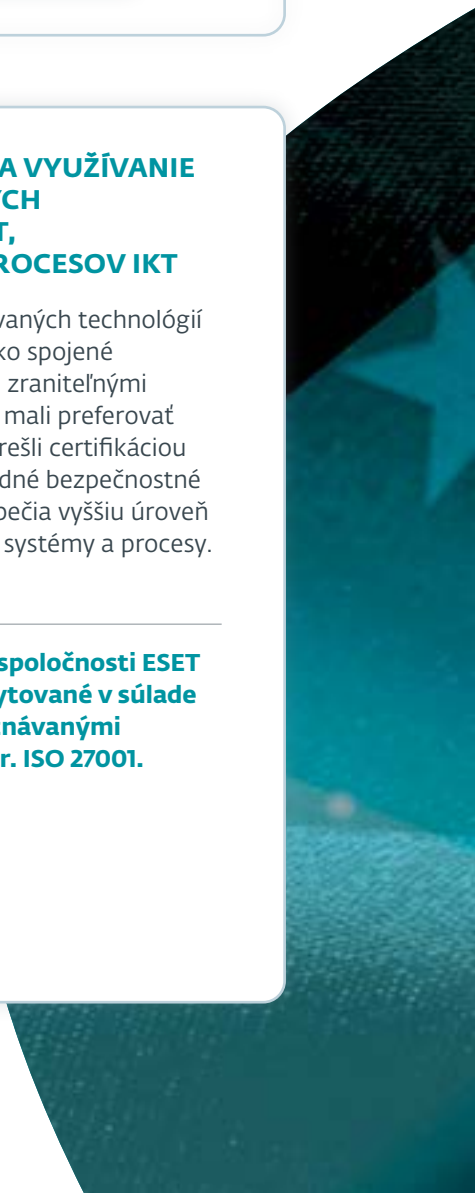
Auditné služby ESET pomôžu s identifikáciou nedostatkov a navrhnú opatrenia na ich odstránenie.

VIAC INFORMÁCIÍ

OBSTARÁVANIE A VYUŽÍVANIE CERTIFIKOVANÝCH PRODUKTOV IKT, SLUŽIEB IKT A PROCESOV IKT

Používanie certifikovaných technológií a služieb znižuje riziko spojené s nekvalitnými alebo zraniteľnými riešeniami. Firmy by mali preferovať technológie, ktoré prešli certifikáciou a spĺňajú medzinárodné bezpečnostné normy, čím si zabezpečia vyššiu úroveň ochrany pre svoje IT systémy a procesy.

Produkty a služby spoločnosti ESET sú vyvíjané a poskytované v súlade s medzinárodne uznávanými certifikáciami, napr. ISO 27001.



Viac informácií k **zákonu o kybernetickej bezpečnosti a požiadavkám NIS2** nájdete TU.

Viac informácií k **službám riadenej detekcie a reakcie MDR** od spoločnosti ESET nájdete TU.

Viac informácií ku **konzultačným a auditným službám** od spoločnosti ESET nájdete TU.

Digital Security
Progress. Protected.

www.eset.sk