Direktiva NIS2 - že v zakonu

biti skladen s spremenjenim zakonom o kibernetski varnosti, ki prenaša zahteve direktive NIS2

Digital Security
Progress. Protected.

Sprememba Zakona o kibernetski varnosti (ZoKB), ki začne veljati 1. januarja 2025 in ki posodablja Zakon o kibernetski varnosti št. 69/2018

Zb. z zahtevami direktive NIS2, prinaša naslednje ključne spremembe.

REGULIRANI SUBJEKTI

Spremenjeni zakon se uporablja za nove regulirane subjekte, razširja pa tudi področje uporabe na druge sisteme in storitve subjektov, ki so bili
so bili regulirani že pred spremembo Zakona o kibernetski varnosti.

POVEZAVE

Najvišja globa za kršitev obveznosti iz spremenjenega zakona lahko znaša 10 milijonov EUR ali 2 % svetovnega letnega neto prometa.

USKLAJEN PRISTOP K RANLJIVOSTIM

Zakon o spremembi spodbuja usklajen pristop k ranljivostim v sistemih IKT, da bi se čim bolj zmanjšalo tveganje izkoriščanja.

VARNOST DOBAVNE VERIGE

Spremenjeni zakon daje večji poudarek varnosti dobavne verige.

IZOBRAŽEVANJE

S spremenjenim zakonom je bila uvedena obveznost izvajalcev bistvenih storitev, da zagotovijo jasno opredelitev odgovornosti, usposabljanje
in krepitev varnostne ozaveščenosti na področju kibernetske varnosti, podrobnosti pa bo določil organ z uredbo.

REVIZIJA IN SAMOOCENJEVANJE

Regulirani subjekti morajo izvajati redne revizije in samoocene, da bi ocenili stanje svoje kibernetske varnosti.

POROČANJE O INCIDENTIH

S spremenjenim zakonom je bila podrobneje urejena obveznost reguliranih subjektov, da poročajo o kibernetskih incidentih. Ta ureditev je vsebovana v 24. členu zakona.

UPORABA VARNOSTNIH UKREPOV NA PODLAGI ANALIZE TVEGANJA

Spremenjeni zakon je uvedel podrobnejšo ureditev splošnih varnostnih ukrepov, ki bodo določeni z odlokom, njihovo izvajanje bo temeljilo na analizi tveganja (ki jo mora pripraviti strokovnjak) ali sektorskih standardih, izvajalci bistvenih storitev pa jih morajo izvajati v 12 mesecih od vpisa v register.

SISTEM CERTIFICIRANJA KIBERNETSKE VARNOSTI

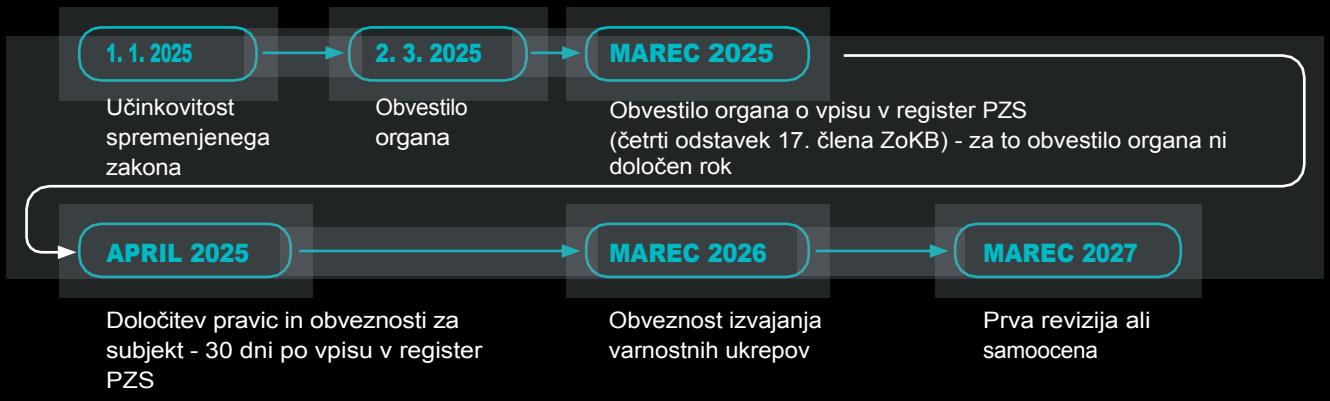
Spremenjeni zakon uvaja zahteve za certificiranje varnosti proizvodov, storitev in procesov IKT, s čimer se povečuje raven zaščite pred kibernetskimi grožnjami.

Kdaj in kaj morajo regulirani subjekti izpolnjevati?

Sprememba Zakona o kibernetski varnosti uvaja nove obveznosti za novo regulirane subjekte in za subjekte, ki so bili regulirani že pred spremembo Zakona o kibernetski varnosti.

ČASOVNI OKVIR ZA NOVE SUBJEKTE

Ta časovnica prikazuje obveznosti za operaterje bistvenih storitev (ESO) iz 17. člena spremenjenega zakona in operaterje ključnih storitev (CESO) iz prvega in drugega odstavka 18. člena spremenjenega zakona.



INFORMACIJE ZA OBSTOJEČE IZVAJALCE

Od 1. januarja 2025 se izvajalci bistvenih storitev po zakonu, ki je veljal do 31. decembra 2024, štejejo za izvajalce bistvenih storitev po novih pravilih. Prav tako se ponudniki digitalnih storitev, za katere veljajo pravila, veljavna do konca leta 2024, od 1. januarja 2025 štejejo za izvajalce bistvenih storitev v skladu s spremenjenim zakonom.

Za obstoječe subjekte je ključni datum 31. december 2026.

Do tega datuma se lahko Organ odloči, da bo regulirane subjekte črtal s seznama reguliranih subjektov, hkrati pa se bo končalo prehodno obdobje za izvajanje varnostnih ukrepov in revizije v skladu s starimi pravili

Na koga vpliva sprememba zakona o kibernetski varnosti?

Sprememba zakona o kibernetski varnosti je namenjena subjektom, ki delujejo v sektorjih z visoko stopnjo kritičnosti ali drugih kritičnih sektorjih. Nove zahteve iz spremenjenega zakona uvajajo višje standarde zaščite za boljšo odpornost na kibernetske grožnje.

SPREMENJENI ZAKON MED REGULIRANE SUBJEKTE VKLJUČUJE ORGANIZACIJE, KI SPADAJO V TE SEKTORJE:

- Energetika
- Transport
- Finance
- Zdravstveno varstvo
- Voda in ozračje
- Digitalna infrastruktura
- Upravljanje storitev IKT (med podjetji)
- Javna uprava
- Prostor
- Poštne in kurirske storitve
- Ravnanje z odpadki
- Proizvodnja in distribucija kemikalij
- Proizvodnja, predelava in distribucija živil
- Proizvodnja
- Ponudniki digitalnih storitev
- Raziskave

Eno od glavnih meril za opredelitev reguliranega subjekta je njegova velikost in promet. Nova zakonodaja se uporablja za organizacije z več kot 50 zaposlenimi in prometom, ki presega 10 milijonov EUR. Vendar pa zakon opredeljuje tudi subjekte, ki se lahko uvrstijo med regulirane ne glede na njihovo velikost in promet.

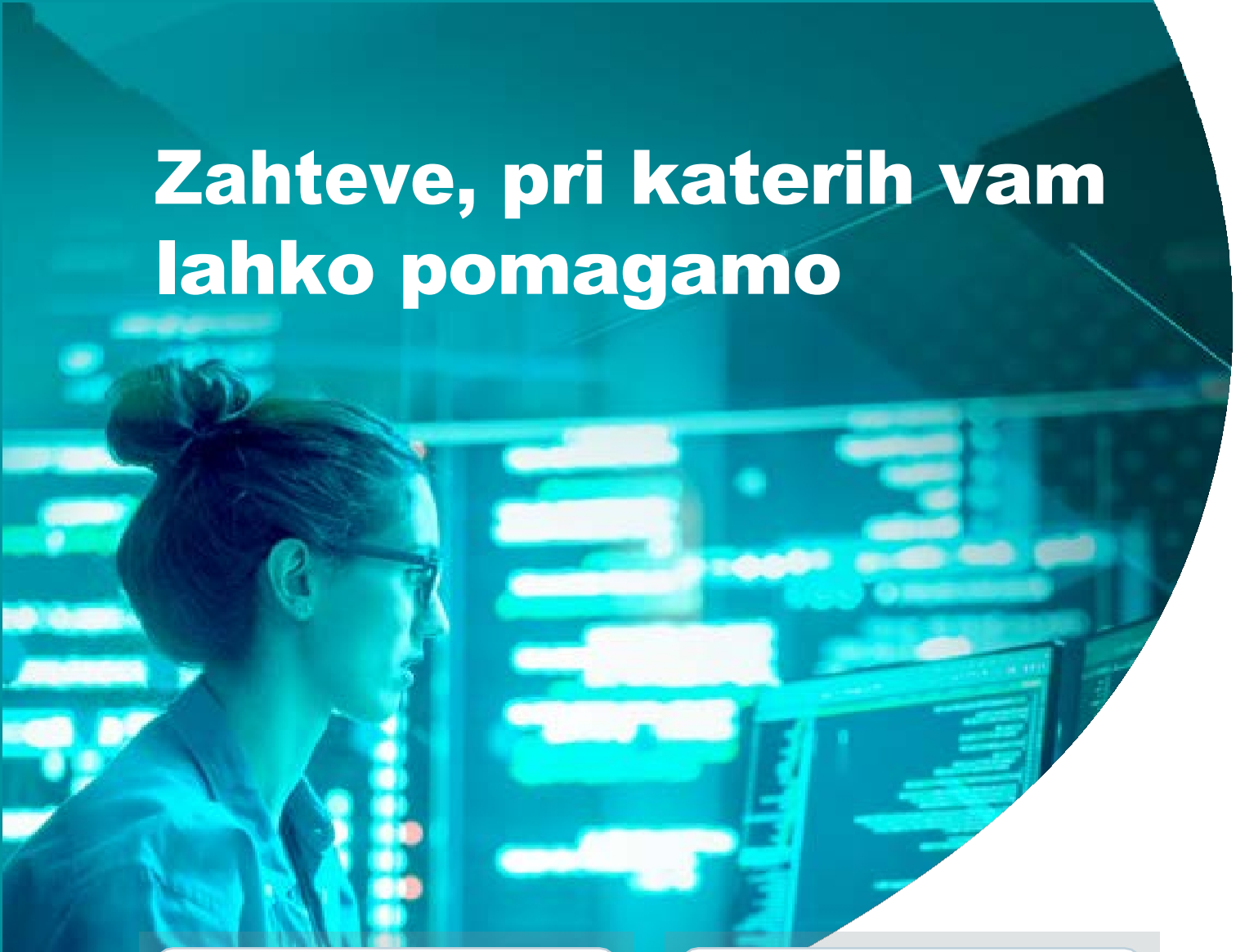
Če ste v dvomih, ali spadate v okvir spremembe, lahko uporabite okvirni pripomoček za določitev subjekta, ki ga je pripravil nacionalni varnostni organ.

KATERE VARNOSTNE UKREPE MORATE UPOŠTEVATI?

V skladu s spremenjenim zakonom o kibernetski varnosti morajo regulirani subjekti izvajati strožje varnostne ukrepe, kot so spremljanje omrežja, upravljanje ranljivosti in pravočasno poročanje o kibernetskih incidentih. Številne od teh zahtev lahko preprosto izpolnijo s celovitimi rešitvami in storitvami iz ESET-ovih celovitih rešitev, ki jim pomagajo okrepiti zaščito in odpornost na grožnje.

eset Digital Security
Progress. Protected.

Zahteve, pri katerih vam lahko pomagamo



ORGANIZACIJA IN UPRAVLJANJE INFORMACIJSKE VARNOSTI IN KIBERNETSKE VARNOSTI

Podjetja morajo uvesti sistem upravljanja kibernetske varnosti, ki določa odgovornosti in postopke za zaščito podatkov in sistemov. To vključuje jasno opredelitev vlog za posamezne zaposlene, pravila za upravljanje dostopa in nadzorne mehanizme. Cilj je ustvariti organizacijsko strukturo, ki zagotavlja upoštevanje varnostnih ukrepov na vseh ravneh.

Družba ESET zagotavlja svetovalne storitve za uvajanje organizacije in upravljanje informacijske varnosti.

PREBERITE VEČ

UPRAVLJANJE RANLJIVOSTI IN KIBERNETSKE GROŽNJE

Vsaka organizacija mora dejavno spremljati in posodabljati svoje sisteme za zaščito pred novimi ranljivostmi in grožnjami. To pomeni redno pregledovanje sistemov, analizo tveganj in zagotavljanje posodobitev programske opreme. S tem lahko podjetja preprečijo kibernetske napade, ki izkoriščajo zastarele sisteme in ranljivosti programske opreme.

Upravljanje za upravljanje ranljivosti ranljivosti in popravkov in popravkov je del rešitve ESET PROTECT MDR.

VEČ INFORMACIJ

UPRAVLJANJE DOGODKOV IN KIBERNETSKIH TVEGANJ VARNOSTNI INCIDENTI

Podjetja morajo imeti vzpostavljene postopke za odkrivanje, odzivanje in reševanje kibernetskih varnostnih incidentov. To vključuje vzpostavitev postopkov za obravnavanje incidentov, ki
zmanjšajo njihov vpliv in hitro vzpostavijo normalno delovanje.

ESET Inspect,(XDR) orodje za izboljšano odkrivanje in odzivanje , ki hitro zajame in se odzove na incidente, je del rešitve ESET PROTECT MDR.

VEČ INFORMACIJ

UPRAVLJANJE NEPREKINJENEGA DELOVANJA, OPERACIJE, VARNOSTNO KOPIRANJE, OBNOVITEV PO NESREČI IN KRIZNO UPRAVLJANJE

Organizacije morajo zagotoviti, da njihovi sistemi v kriznih razmerah delujejo, na primer s testiranjem varnostnega kopiranja in obnovitve podatkov.
sistemov. Ta postopek omogoča hitro vrnitev k običajnemu poslovanju in zmanjšuje izgube med izpadi ali nesrečami.

Za uporabite ESET-ove svetovalne storitve.uvedbo postopkov neprekinjenega delovanja lahko

PREBERITE VEČ

UPRAVLJANJE SREDSTEV TER UPRAVLJANJE KIBERNETSKIH GROŽENJ IN TVEGANJ.

Upravljanje sredstev zahteva, da podjetja natančno vedo, kaj je zanje vredno i n kaj je sredstvo, ki ga je treba upravljati. Prepoznavanje in upravljanje tveganj zagotavlja, da podjetje ve, kje so morebitne ranljivosti, in jih lahko zgodaj odpravi ali čim bolj zmanjša njihov vpliv na poslovanje.

Z oblikovanjem kataloga sredstev in upravljanjem tveganj lahko pomaga s družba ESET svetovalnimi storitvami za upravljanje informacijske varnosti.

PREBERITE VEČ

VARNOST PRI PRIDOBIVANJU, RAZVOJU IN VZDRŽEVANJU OMREŽIJ, INFORMACIJSKIH SISTEMOV, APLIKACIJ IN KONFIGURACIJ

Vsaka nova aplikacija, omrežje ali informacijski sistem mora med razvojem in testiranjem izpolnjevati varnostna merila. Podjetja morajo zagotoviti, da programska oprema in omrežja prestanejo
revizije varnosti pred začetkom obratovanja, kar zmanjšuje tveganje kibernetskih groženj.

ESET zagotavlja organizacijam zmogljivosti penetracijskega testiranja informacijskih v razvoju.sistemov in aplikacij

PREBERITE VEČ

POSTOPKI ZA OCENJEVANJE UČINKOVITOSTI UKREPOV, UPRAVLJANJE SKLADNOSTI IN KONTROLNE DEJAVNOSTI

Organizacije morajo redno ocenjevati učinkovitost svojih varnostnih ukrepov, na primer z revizijami ali pregledi. S tem bo zagotovljena skladnost s standardi in odkrili področja, na katerih je treba izboljšati zaščito, ter tako preprečili nastanek varnostnih pomanjkljivosti.

Družba ESET zagotavlja organizacijam penetracijsko testiranje, tehnične revizije in revizije kibernetske varnosti, kot to zahteva agencija NSA.

VEČ INFORMACIJ

UPRAVLJANJE IDENTITET IN DOSTOPA

Podjetja morajo uvesti sistem za upravljanje identitete in dostopa, ki določa, kdo lahko dostopa do posameznih sistemov
in podatke ter pod kakšnimi pogoji. To vključuje močno preverjanje pristnosti dostopa z večfaktorsko avtentikacijo in redne preglede pravic dostopa, da se zagotovi, da imajo dostop do občutljivih podatkov samo pooblaščeni uporabniki.

Orodje za dvofaktorsko preverjanje pristnosti ESET Secure Authentication je del rešitve ESET PROTECT MDR.

VEČ INFORMACIJ

KRIPTOGRAFSKI UKREPI IN POLITIKA UPORABE KRIPTOGRAFIJE

Za zaščito občutljivih podatkov morajo podjetja uporabljati šifrirne tehnologije, ki preprečujejo nepooblaščen dostop. Kriptografija je bistveno orodje za zagotavljanje zaupnosti in celovitosti podatkov pri njihovem shranjevanju in prenosu med sistemi.

ESET Full Disk Encryption je del rešitve ESET PROTECT MDR.

VARNOST PRI DELOVANJU OMREŽIJ IN INFORMACIJSKIH SISTEMOV

Za zagotavljanje varnosti omrežij in sistemov je potrebno redno spremljanje in varovanje prenosa podatkov.
in zaščito pred nepooblaščenim dostopom. Podjetja morajo izvajati tudi ukrepe za zmanjšanje tveganja, kot so sistemi požarnih zidov in orodja za zaščito pred napadi.

Orodje za izboljšano odkrivanje in odzivanje (XDR) družbe ESET Inspect spremlja vse sumljive v realnem času dejavnosti v omrežju in je del rešitve ESET PROTECT MDR.

eset Digital Security
Progress. Protected.

VARNOSTNE IN KADROVSKE ZMOGLJIVOSTI

Podjetja morajo zagotoviti, da razumejo kibernetske grožnje z usposabljanjem in izobraževanjem svojih zaposlenih.
in upoštevati varnostne politike.
Pomembno je redno usposabljanje in podpora na področju informacijske varnosti
varnosti, saj je človeški dejavnik lahko pomembno tveganje.

ESET ponuja
E-učenje in osebno usposabljanje o kibernetski varnosti za zaposlene.

PREBERITE VEČ

ZAŠČITA PRED ZLONAMERNO KODO IN NEŽELENO VSEBINO

Organizacije morajo uporabljati protivirusne programe in rešitve za odkrivanje in blokiranje zlonameme programske opreme, da preprečijo okužbo sistemov.
Pregledovanje in filtriranje vsebine zagotavlja, da neželene datoteke ali povezave, ki bi lahko predstavljale varnostno tveganje, ne pridejo v sisteme.

ESET Endpoint Security zagotavlja zanesljivo zaščito pred zlonamerno kodo in je del rešitve ESET PROTECT MDR.

VEČ INFORMACIJ ESET ENDPOINT SECURITY

VEČ INFORMACIJ ESET MOBILE THREAT DEFENSE

VARNOST SISTEMA, VARNOST OMREŽJA IN KOMUNIKACIJSKA VARNOST.

Ta točka zajema zaščito pred napadi na različnih ravneh infrastrukture, od sistema do komunikacijskih kanalov.
Z izvajanjem varnostnih protokolov na ravni strojne in programske opreme ter na ravni omrežja se zmanjša tveganje nepooblaščenega dostopa in zlorabe podatkov med prenosom.

Orodje za izboljšano odkrivanje in odzivanje (XDR) družbe ESET Inspect nenehno spremlja infrastrukturo, prepoznava in blokira v realnem času grožnje ter ščiti podatke tako med prenosom kot v shrambi. Je del rešitve ESET PROTECT MDR.

SPREMLJANJE, BELEŽENJE IN POROČANJE O DOGODKIH

Organizacije morajo zagotoviti, da se vsi kritični dogodki in incidenti v njihovih spremljajo, beležijo in ocenjujejo. Ta postopek vključuje tudi obveznost poročanja o kibernetskih incidentih pristojnim organom,
kar povečuje preglednost in omogoča učinkovit odziv.

Orodje za izboljšano odkrivanje in odzivanje (XDR) družbe ESET Inspect beleži incidente, strokovnjaki podjetja pa ESET-ova storitev ESET PROTECT MDR zagotavlja, da imajo organizacije na voljo informacije, ki jih potrebujejo za pravočasno in natančno poročanje.

eset Digital Security
Progress. Protected.

ZAŠČITA ZAPISOV, ZASEBNOSTI IN OZNAČEVANJE INFORMACIJ

Organizacije morajo zaščititi občutljive podatke, zagotoviti zasebnost svojih uporabnikov in označiti podatke glede na njihovo občutljivost. Izvajanje zaščite podatkov pri shranjevanju in upravljanju zapisov pomaga preprečiti uhajanje in nepooblaščen dostop do pomembnih podatkov.

ESET Full Disk Encryption ščiti občutljive podatke in je na voljo v rešitvi ESET PROTECT MDR.

VEČ INFORMACIJ

DOBAVITELJSKA VERIGA

Podjetja morajo obvladovati tveganja, povezana z z dobavitelji, ki imajo lahko dostop do do njihovih sredstev. Vključitev varnostnih zahtev v pogodbe in redne revizije dobaviteljev bodo zagotovile, da tretje osebe spoštujejo varnostne standarde, ki ščitijo občutljive podatke organizacije.

Izboljšano orodje za odkrivanje in odzivanje ESET Inspect spremlja dostop in dejavnosti tretjih oseb v sistemu, odkriva sumljivo vedenje in zmanjšuje tveganja, povezana z povezana z vključevanjem zunanjih dobaviteljev. Na voljo je kot del rešitve ESET PROTECT MDR.

VEČ INFORMACIJ

FIZIČNA VARNOST, VARNOST OKOLJA IN UPRAVLJANJE KONČNIH TOČK

Varnost fizičnega dostopa do občutljivih naprav in sistemov je prav tako pomembna kot zaščita digitalnega prostora. Podjetja morajo izvajati varnostne ukrepe za zaščito prostorov in nadzorovati dostop do teh prostorov, da preprečijo nepooblaščen fizični dostop.

ESET-ove revizijske storitve vam bodo pomagale ugotoviti pomanjkljivosti in predlagati ukrepe za njihovo odpravo.

PREBERITE VEČ

NAROČANJE IN UPORABA IZDELKOV S CERTIFIKATOM IKT, STORITVE IKT IN PROCESI IKT

Uporaba certificiranih tehnologij in storitev zmanjšuje tveganje, povezano z povezanimi z nekakovostnimi ali ranljivimi rešitvami. Podjetja bi morala dati prednost tehnologijam, ki so bile certificirane in izpolnjujejo mednarodne varnostne standarde, s čimer zagotovijo višjo raven zaščite svojih sistemov in procesov IT.

ESET-ovi izdelki in storitve so razviti in dobavljeni v skladu z mednarodno priznanimi certifikati, kot je ISO 27001.

Več informacij o zakonu Kibernetska varnost in zahteve NIS2 lahko najdete TUKAJ.

Več informacij o storitvah družbe ESET za upravljano odkrivanje in odzivanje MDR najdete TUKAJ.

Več informacij o ESET-ovih storitvah svetovanja in revidiranja najdete TUKAJ.

Digital Security
Progress. Protected.

www.eset.sk