VODNIK

Odklepanje kibernetske varnosti

Vse, kar morate že danes vedeti o direktivi NIS2

EVERSHEDS SUTHERLAND & ESET Digital Security Progress. Protected.

VSEBINA

Uvod

Zahvaljujemo se vam za prebiranje naše bele knjige o direktivi NIS2. V njej bomo obravnavali najpomembnejše vidike direktive NIS2 ter njeno uporabo pri poslovanju organizacij v EU.

Direktiva NIS2, znana tudi kot nova različica direktive o varnosti omrežij in informacij, je evropska direktiva za krepitev kibernetske varnosti v Evropski uniji (EU). Njen namen je je pomagati organizacijam, da se zaščitijo pred kibernetskimi grožnjami, ter zagotoviti, da bo kibernetska infrastruktura EU varnejša in zanesljivejša. Države članice imajo do 17. oktobra 2024 čas za prenos direktive v nacionalno zakonodajo.

V tej beli knjigi bomo podali pregled najpomembnejših določb direktive NIS2 in njihove uporabe za organizacije v EU. Obravnavali bomo tudi obveznosti, ki jih imajo organizacije pri izpolnjevanju zahtev direktive, in kako lahko pri tem pomagamo v ESET-u.

Upamo, da bo ta bela knjiga koristna za organizacije, ki želijo izvedeti več o tem, kako se zaščititi pred kibernetskimi grožnjami in kako ravnati v skladu z direktivo NIS2 - še preden bo na voljo nacionalna zakonodaja o kibernetski varnosti.

Kaj je direktiva NIS2?

Je vaša organizacija srednja ali velika in deluje v enem od kritičnih sektorjev, kot so energetika, promet, zdravstvo in digitalna infrastruktura? Potem bo nova zakonodaja EU močno vplivala na zahteve glede kibernetske varnosti v vaši organizaciji.

"Ta evropska direktiva bo približno 160.000 subjektom pomagala okrepiti varnostno držo in poskrbela, da bo Evropa postala varen kraj za življenje in delo. Zakon mora omogočiti tudi izmenjavo informacij z zasebnim sektorjem in partnerji po vsem svetu. Če nas napadajo v industrijskem obsegu, se moramo odzvati v industrijskem obsegu," je dejal Bart Groothuis, poslanec v Evropskem parlamentu.

Ker je kibernetska varnost izjemno pomembna za zaščito naše družbe, je Evropska unija (EU) leta 2016 uvedla prvo direktivo o varnosti omrežij in informacij (direktiva NIS). Čeprav je ta zagotovila večjo usklajenost znotraj EU na področju varnosti omrežij in informacij, je bilo treba po mnenju Evropskega parlamenta kibernetsko odpornost za zaščito družbe še povečati. Zaradi vse večje digitalizacije in velikega števila kibernetskih napadov je bila direktiva NIS zdaj revidirana in izboljšana. Direktiva NIS2 bo zato imela širši doseg in se bo osredotočila na več sektorjev. Tako bo izenačila in povečala kibernetsko odpornost organizacij s sedežem v državah članicah EU.

"Ta evropska direktiva bo približno 160.000 subjektom pomagala okrepiti varnost in poskrbela, da bo Evropa postala varno mesto za življenje in delo."

Upravljanje tveganj in sodelovanje:

Kako bo ta revidirana direktiva zagotovila boljšo kibernetsko odpornost? NIS2 poskuša izboljšati raven kibernetske varnosti v državah članicah EU na različne načine. Direktiva povečuje varnostne zahteve, osredotoča se na obravnavo varnosti dobavne verige (proizvodne ali dobavne verige), prinaša enotne obveznosti glede poročanja, zaostruje nadzorne ukrepe in uvaja izvršilne zahteve z usklajenimi sankcijami v vseh državah članicah. Obravnava tudi izmenjavo informacij in (med)državno sodelovanje pri kriznem vodenju.

Obseg direktive NIS2:

Direktiva NIS2 vpliva na veliko več sektorjev kot prvotna direktiva NIS. V direktivi NIS so bili kot bistveni sektorji določeni le zdravstvo, promet, bančna infrastruktura in infrastruktura finančnih trgov, digitalna infrastruktura, oskrba z vodo, energetika in ponudniki digitalnih storitev, države članice pa so lahko same določile, katere organizacije se še štejejo za bistvene. Direktiva NIS2 uvaja enotna pravila za srednje velike in velike organizacije, ki delujejo v ključnih sektorjih, kot so energetika, promet, zdravstvo in digitalna infrastruktura. To zdaj vključuje tudi "zelo kritične sektorje", vključno z energetiko, prometom, bančništvom, infrastrukturo finančnih trgov, zdravstvom, pitno vodo, odpadno vodo, digitalno infrastrukturo, upravljanjem IKT (B2B), javno upravo in vesoljem, ter "kritične sektorje", kot so poštne in kurirske storitve, ravnanje z odpadki, kemikalije, živila, proizvodnja, ponudniki digitalnih storitev in raziskave. Nova zakonodaja bo veljala za vsa srednja in velika podjetja v teh sektorjih, pri čemer bodo lahko države z nacionalno zakonodajo še dodatno razširile krog zavezancev.

Je vaša organizacija bistvena ali pomembna?

Način izvrševanja direktive je odvisen od kategorije, v katero spada organizacija. NIS2 razvršča organizacije v dve kategoriji: med bistvene in pomembne. Ali je organizacija uvrščena med bistvene ali pomembne, je odvisno od tega, ali spada v kritični ali zelo kritični sektor, in od njene velikosti.

V KATEREM SEKTORJU DELUJE VAŠA ORGANIZACIJA?

- ENERGIJA
- TRANSPORT
- BANČNIŠTVO
- ZDRAVSTVO
- PITNA VODA
- ODPADNA VODA
- DIGITALNA INFRASTRUKTURA
- UPRAVLJANJE STORITEV IKT (MED PODJETJI)
- JAVNA UPRAVA
- VESOLJE
- INFRASTRUKTURA FINANČNIH TRGOV
- POŠTNE IN KURIRSKE STORITVE
- RAVNANJE Z ODPADKI
- PROIZVODNJA
- DIGITALNI PONUDNIKI
- RAZISKAVE
- IZDELAVA, PROIZVODNJA IN DISTRIBUCIJA KEMIKALIJ
- PRIDELAVA, PROIZVODNJA IN DISTRIBUCIJA ŽIVIL

*** Velika:**
več kot 250 zaposlenih in letni promet najmanj 50 milijonov evrov (ali bilančna vsota najmanj 43 milijonov evrov).

*** Srednja:**
več kot 50 in manj kot 250 zaposlenih ter letni promet, ki ne presega 50 milijonov evrov (ali bilančno vsoto, ki ne presega 43 milijonov evrov).

KAKO VELIKA JE VAŠA ORGANIZACIJA?

*** VELIKE ORGANIZACIJE**

*** SREDNJE VELIKE ORGANIZACIJE**

VELIKE ORGANIZACIJE

SREDNJE VELIKE ORGANIZACIJE

BISTVENA *

POMEMBNA

* Pri tem pravilu obstajajo nekatere izjeme, saj so lahko subjekti, kot so na primer ponudniki kvalificiranih storitev zaupanja, registratorji domen najvišje ravni in ponudniki storitev DNS, ne glede na velikost njihove organizacije, opredeljeni kot bistveni. Za vse izjeme glej člen 3(1).

Srednje velike organizacije z manj kot 250 zaposlenimi in letnim prometom do 50 milijonov evrov (ali bilančno vsoto do 43 milijonov evrov), ki delujejo v zelo kritičnih sektorjih, se štejejo za pomembne, skupaj z drugimi velikimi in srednje velikimi organizacijami v kritičnih sektorjih. Za bistvene se štejejo le velike organizacije, ki presegajo zgornjo mejo za srednje velike organizacije in spadajo v zelo kritične sektorje. Nekatere organizacije se samodejno štejejo za bistvene, ne glede na njihovo velikost, če bi imel izpad storitev resne posledice za družbo ali če so izključni nacionalni ponudnik. Sem spadajo recimo organizacije, ki zagotavljajo javna komunikacijska omrežja in storitve, ponudniki storitev zaupanja ter ponudniki storitev registracije domen najvišje ravni.

Direktiva NIS2 načeloma ni namenjena majhnim in mikropodjetjem, ki imajo manj kot 50 zaposlenih in letni promet manj kot 7 milijonov EUR (ali bilančno vsoto manj kot 5 milijonov EUR). Če pa imajo ključno vlogo za družbo, gospodarstvo, sektorje ali storitve, morajo države članice posebej določiti, katera od njih zajema ta direktiva.

Glavna razlika med bistvenimi in pomembnimi subjekti je v spremljanju skladnosti s pravili. Pri bistvenih subjektih, predvsem organizacijah iz ključnih sektorjev, bo nadzor proaktiven. To pomeni, da se bo pri teh organizacijah aktivno spremljalo, ali se zakonodaja upošteva. Pri pomembnih subjektih bo nadzor potekal naknadno, če bodo obstajali znaki, da je prišlo do incidenta. Če se po incidentu izkaže, da organizacija ni sprejela zahtevanih ukrepov, bodo te organizacije morda morale obravnavati tudi morebitne posledice neupoštevanja te zakonodaje.

Kaj lahko pričakujemo od NIS2?

To vam bomo razložili na osnovi dveh uporabniških primerov.

Energetsko podjetje BrightEnergies s 500 zaposlenimi se je z varnostnimi obveznostmi soočilo že ob uvedbi prve direktive o varnosti omrežij in informacij. V nacionalni zakonodaji o varnosti omrežij in informacijskih sistemov (na Nizozemskem, od koder prihaja podjetje, je vključena v Zakon o varnosti omrežij in informacijskih sistemov) je bil sektor, ki mu je pripadalo (energetika), uvrščen med vitalne ponudnike. Sedanji direktor Lennard tedaj še ni delal v podjetju BrightEnergies, vendar obstaja dokumentacija o tem, kateri ukrepi in procesi so bili takrat prilagojeni ali obnovljeni. Leta 2022 je izvedel, da bo sprejeta nova zakonodaja na področju varnosti omrežij in informacij. V tej novi zakonodaji je njegovo energetsko podjetje bistveni subjekt. Z uvedbo zakonodaje NIS je bilo sicer že izvedenih kar nekaj sprememb. Vendar, ker so hekerji v drugih državah, na primer v Luksemburgu, Italiji in na Portugalskem že večkrat napadli energetska podjetja, želi Lennard storiti vse, kar je v njegovi moči, da podjetje BrightEnergies ne bi bilo prizadeto. Zakonodaja NIS2 ima zato zanj že zdaj visoko prioriteto.

Podjetje za predelavo in recikliranje odpadkov Waste2Resource doslej ni bilo vključeno v sistem NIS ali drugo zakonodajo o kibernetski varnosti. V zadnjih letih pa je postalo bolj jasno, da se lahko s kibernetskim napadom sooči tudi predelovalec odpadkov: leta 2021 je bil konkurent več dni zaprt zaradi izsiljevalske programske opreme, ki je preprečila vožnjo smetarskih tovornjakov. Ekipa IT v podjetju Waste2Resource je zadovoljna, da podjetje spada pod direktivo NIS2, čeprav jo zato čaka veliko dela. Ekipa, ki jo vodi na novo zaposlena direktorica informacijske varnosti (CISO) Kayleigh, se trenutno ukvarja s pripravami, kot je izdelava analize tveganja. Vsekakor pa ona in njena ekipa že vedo, da so v skladu z direktivo NIS2 obravnavani kot pomemben subjekt, zato se morajo spoprijeti z dolžnostjo skrbnega ravnanja in obveznostjo odzivnega poročanja.

Obveznosti in posledice

NIS2 zahteva, da dodatne panoge sprejmejo obsežnejše zahteve glede kibernetske varnosti, pomembni in bistveni subjekti pa morajo sprejeti ukrepe za obvladovanje varnostnih tveganj. Med drugim morajo izdelovati varnostne kopije, izvajati analize tveganja in poročati o incidentih z velikim vplivom na storitev. Da bi bilo administrativno breme čim manjše, bo za skladnost z določbami direktive NIS2 odgovorno neposredno vodstvo organizacije.

Ta nova politika predstavlja velik korak za mnoge organizacije – velike ali majhne. Tako vlada kot organizacije bodo morale prevzeti večjo odgovornost. To bo imelo tudi finančne posledice: pričakuje se, da se bo proračun za IKT v podjetjih, za katera direktiva še ne velja, povečal za do 22 %, v podjetjih, za katera direktiva že velja, pa za največ 12 %. Povečalo se bo tudi administrativno breme. Ali se bodo ti dodatni izdatki za IKT izplačali in bodo podjetjem zaradi višje ravni kibernetske varnosti prinesli konkurenčno prednost, bomo še videli.

Pričakuje se, da direktiva NIS2 ne bo privedla le do strožjega izvrševanja kibernetske varnosti in s tem povezanih obveznosti, temveč tudi do varnejšega digitalnega gospodarstva v Evropski uniji in zaščite pred kibernetskimi napadi.

Kaj bo NIS2 pomenila za vašo organizacijo

Kot je bilo že omenjeno, bo direktiva NIS2 razlikovala med dvema kategorijama: bistvenimi in pomembnimi subjekti, medtem ko se je prej razlikovalo le med vitalnimi organizacijami, ki so bile vključene v NIS, in nevitalnimi organizacijami. Vsi sektorji in organizacije, ki bodo zajeti v NIS2, so za družbo zelo pomembni. Če te organizacije ne bi več mogle opravljati svoje vloge, bi to družbi povzročilo velike težave.

Kibernetski napadi imajo torej lahko velik vpliv ne le na organizacije, temveč tudi na družbo.

Tukaj je nekaj primerov večjih napadov:

NotPetya

Širjenje izsiljevalske programske opreme NotPetya v letu 2017 je povzročilo motnje, vključno z zaprtjem pristanišča v Rotterdamu.

2017

Mandemakers gr. & VDL

Med napadi z izsiljevalsko programsko opremo na podjetji Mandemakers Groep in VDL je bilo njuno poslovanje resno moteno.

2021

Bakker Logistiek

Zaradi napada na podjetje Bakker Logistiek je v nizozemskih supermarketih več dni primanjkovalo sira na policah.

2021

Kaseya

Napad na ponudnika programske opreme Kaseya je kibernetskim kriminalcem omogočil dostop do sistemov več tisoč podjetij.

2021

Ti dve kategoriji sta bili oblikovani zato, ker v primeru incidenta podjetja iz vseh sektorjev na isti lestvici nimajo enakega vpliva na družbo. V nadaljevanju pojasnjujemo razliko med obema skupinama - bistveno in pomembno - in kako bo takšno ločevanje vplivalo na spremembe, ki jih bo organizacijam prinesla direktiva NIS2.

Dolžnost skrbnega ravnanja in poročanja

Vse organizacije, ki spadajo v NIS2 - bistvene ali pomembne - bodo morale izpolnjevati svojo dolžnost skrbnega ravnanja. Direktiva vsebuje seznam več vrst ukrepov, ki jih morajo minimalno izpolnjevati ponudniki:

- politike o analizi tveganja in informacijske varnosti sistemov
- skrb za krizno upravljanje in neprekinjeno delovanje v primeru večjega kibernetskega incidenta
- zagotavljanje varnosti dobavne verige
- dolžnost zagotavljanja varnosti omrežja in informacijskih sistemov
- uporaba kriptografije in šifriranja
- politike in postopki za ocenjevanje učinkovitosti ukrepov za obvladovanje tveganj

Evropska komisija si pridržuje pravico, da z delegiranimi in izvedbenimi sklepi podrobneje določi ukrepe in jih razširi z dodatnimi ukrepi. Države članice lahko nato določijo posebne ukrepe ob upoštevanju nacionalnih in sektorskih okoliščin.

Obveznost poročanja bo tudi veljala za vse organizacije, ki spadajo v sistem NIS2. Ta obveznost poročanja pomeni, da morajo prizadete organizacije o incidentu poročati imenovanemu organu v 24 urah po seznanitvi z incidentom, nato pa v enem mesecu predložiti končno poročilo.

Na kratko **o NIS2**

POMEMBNO

Kot v primeu podjetja **Waste2Resource**

Srednje organizacije, ki delujejo v enem od 11 "zelo kritičnih sektorjev", ali srednje in velike organizacije, ki delujejo v enem od 7 "kritičnih sektorjev".

BISTVENO

Kot v primeru podjetja **BrightEnergies**

Velike organizacije, ki delujejo v "zelo kritičnih sektorjih".

DUTY OF CARE

- vzdrževanje osnovne ravni digitalne higiene in izvajanje izobraževanja o kibernetski varnosti
- ocena tveganja za varnost informacijskih sistemov
- skrb za krizno upravljanje in neprekinjeno delovanje v primeru večjega kibernetskega incidenta
- zagotavljanje varnosti dobavne verige
- dolžnost skrbnega ravnanja za zagotavljanje varnosti omrežja in informacijskih sistemov, vključno z odzivanjem in obveščanje o ranljivostih

- zagotavljanje varnosti človeških virov, politike dostopanja in varovanje digitalnih sredstev
- uporaba kriptografije in šifriranja
- uporaba večfaktorske avtentikacije in/ali varno notranje komuniciranje
- politike in postopki za ocenjevanje učinkovitosti ukrepov za obvladovanje tveganj

Reaktivni nadzor **(po incidentu)**

Proaktivni monitoring **(tudi, če ni incidenta)**

OBVEZNOSTI POROČANJA (V TREH FAZAH)

- zgodnje opozarjanje v 24 urah
- obveščanje o incidentu v 72 urah
- končno poročilo po enem mesecu (ali poročilo o napredku v primeru trajajočega incidenta)

Upravna globa zaradi neizpolnjevanja obveznosti skrbnega ravnanja ali poročanja:

- globa v višini do **7.000.000 evrov**
- ali **do 1.4%** svetovnih letnih prihodkov v predhodnem poslovnem letu; odvisno kateri znesek je višji

Upravna globa zaradi neizpolnjevanja obveznosti skrbnega ravnanja ali poročanja:

- globa v višini do **10.000.000 evrov**
- ali **do 2%** svetovnih letnih prihodkov v preteklem poslovnem letu; odvisno od tega, kateri znesek je višji

Poleg tega se lahko začasno odvzamejo dovoljenja za obratovanje ali pa se začasno odvzame pooblastila fizični osebi, na primer generalnemu direktorju.

Nadzor

Obe kategoriji se razlikujeta v načinu nadzora izpolnjevanja predpisanih zahtev. Za sektorje in organizacije, ki so označeni kot bistveni, se bo izpolnjevanje zahtev nadziralo proaktivno. Nadzorovanje bo torej aktivno, zato bodo posledice slabega upravljanja odpravljene še preden bi prišlo do incidenta.

V drugi kategoriji, pri pomembnih subjektih, bo preverjanje skladnosti z zakonodajo potekalo reaktivno. To pomeni, da se bo skladnost teh organizacij z zakonodajo in zahtevami preverjala šele po incidentu. Če se pozneje izkaže, da ni bilo sprejetih dovolj ukrepov in zahteve niso bile izpolnjene, lahko sledijo enake sankcije kot za bistvene subjekte.

Poročanje

Direktiva NIS2 določa "tristopenjski pristop" za poročanje o incidentih. Namen "zgodnjega opozarjanja" v 24 urah je omejiti morebitno širjenje incidentov in subjektom omogočiti, da poiščejo pomoč. "Prijava incidenta" v 72 urah mora vključevati začetno oceno pomembnega incidenta z navedbo njegove resnosti in vpliva ter kazalnikov kompromitiranosti. "Končno poročilo" – po enem mesecu – mora zagotoviti, da se je mogoče iz prejšnjih incidentov kaj naučiti. Cilj tega pristopa je postopno izboljšati odpornost posameznih subjektov in celotnih sektorjev na kibernetske grožnje. Poleg obvezne predložitve zgodnjega opozorila je pri obveščanju o incidentih poudarek na obravnavi incidentov.

1 **Zgodnje opozarjanje**

Brez nepotrebnega odlašanja in v vsakem primeru v 24 urah po seznanitvi s pomembnim incidentom je treba pristojnemu nadzornemu organu posredovati zgodnje opozorilo. V tem opozorilu je treba navesti, ali je incident nastal zaradi nezakonitega ali zlonamernega dejanja ali bi lahko imel čezmejni učinek. To so nujno potrebne informacije. V 24 urah po predložitvi tega opozorila mora subjekt, ki poroča, od pristojnega nadzornega organa ali skupine CSIRT prejeti odgovor z začetnimi povratnimi informacijami. Če subjekt to zahteva, lahko prejme smernice o izvajanju morebitnih omilitvenih ukrepov in po možnosti dodatno tehnično podporo. V primeru incidenta kriminalne narave subjekt prejme tudi smernice o tem, kako incident prijaviti organom pregona.

2 **Prijava incidenta**

V obvestilu o incidentu je treba brez nepotrebnega odlašanja in v vsakem primeru v 72 urah po seznanitvi s pomembnim incidentom posodobiti informacije iz zgodnjega opozorila ter navesti (i) začetno oceno pomembnega incidenta, (ii) vključno z njegovo resnostjo in vplivom ter, če so na voljo, (iii) kazalnike ogrožanja.

3 **Končno poročilo**

Nazadnje se v enem mesecu po predložitvi obvestila o incidentu predloži končno poročilo, ki vsebuje (i) podroben opis incidenta, njegovo resnost in vpliv, (ii) vrsto grožnje ali temeljni vzrok, ki je verjetno sprožil incident, (iii) uporabljene in tekoče omilitvene ukrepe ter (iv) čezmejni vpliv incidenta. V utemeljenih primerih in po posvetovanju s pristojnim nadzornim organom se lahko odstopi od 24-urnega roka za prijavo incidenta in enomesečnega roka za poročilo.

1

V družbi BrightEnergies je kriza. V omrežje je vstopil napadalec, nihče ne ve, kako je bilo to mogoče in kaj je treba storiti. Poleg tega direktor kibernetske varnosti ni dosegljiv! Vsi so zmedeni, vodenje pa kot nadomestni vodja prevzame strokovnjak za informacijsko tehnologijo Menno. V 24 urah pošlje zgodnje opozorilo RDI. Skupaj z zunanjim izvajalcem vestno išče varnostne kopije podjetja. Te so najdene in organizacija ve, da bo lahko preprečila hujše posledice, saj ima dostop do svojih pomembnih podatkov. Kljub temu podjetje že več dni ne deluje in se sooča z vsemi posledicami, ki jih to prinaša. Mesec dni po incidentu bodo v končnem poročilu navedeni podroben opis incidenta, omilitveni ukrepi in temeljni vzrok. Dejstvo, da na področju varnosti ni bilo organizirano vse tako dobro, kot bi bilo treba, je direktorju Lennardu odprlo oči. Ta kriza ima resne posledice za podjetje BrightEnergies.

2

Družba Waste2Resource se tako kot njen konkurent sooča z napadom izsiljevalske programske opreme. Zahvaljujoč postopkom, ki jih je želela dokumentirati CISO Kayleigh, lahko ekipa IT hitro obnovi nedavno varnostno kopijo. Po manj kot 24 urah je organizacija ponovno vzpostavljena in deluje. Zahvaljujoč prizadevanjem za izpolnjevanje zahtev standarda NIS2 škoda ni prevelika. Kayleigh je pozabila le na eno stvar, na zgodnje opozarjanje. Na srečo jo eden od njenih sodelavcev v ekipi prav v zadnjem trenutku opozori, da je treba zgodnje opozarjanje izvesti v 24 urah. "Ne pozabi načrtovati posodobljenega in končnega obvestila," ji reče sodelavec, preden odide domov.

Pomembne kibernetske grožnje

V direktivi NIS2 so določena strožja pravila za poročanje o incidentih z večjimi posledicami. Organizacije morajo poročati tudi o vseh pomembnih kibernetskih grožnjah, na katere naletijo in ki bi lahko privedle do večjega incidenta. Kar zadeva koncept kibernetske varnosti, je direktiva NIS2 skladna z opredelitvijo kibernetske varnosti in certificiranjem informacijske tehnologije, ki jo je sprejela Evropska unija. Incident se šteje za pomemben, če povzroči znatne motnje v delovanju ali finančne izgube za organizacijo ali če bi lahko povzročil znatno materialno ali nematerialno škodo posameznikom ali organizacijam.

Prostovoljne prijave

Organizacije, ki ne spadajo na področje uporabe direktive NIS2, lahko prostovoljno poročajo o pomembnih incidentih, kibernetskih grožnjah ali skorajšnjih incidentih. Nadzorni organ pri tem upošteva postopek poročanja. V primeru prostovoljnih obvestil ne bi smele biti naložene nobene dodatne obveznosti.

Obseg obveznosti

Evropska komisija lahko zagotovi dodatne smernice glede informacij, oblike in postopka poročanja o incidentih z velikim učinkom in kibernetskih grožnjah. Področje uporabe obveznosti se zato lahko razširi.

Globe in kazni

Dolžnost skrbnega ravnanja in obveznost poročanja prinašata tudi obliko izvrševanja, da se zagotovi učinkovito spoštovanje pravil. Organi bodo imeli v ta namen na voljo različne nadzorne ukrepe in sredstva.

Kibernetska varnost in odpornost sta z NIS2 postali tema v upravnih odborih. Poleg skupnih načinov izvrševanja - vključno z globami, kaznimi in učinkom izgube ugleda - sta v igri tudi osebna odgovornost in suspenz direktorjev. Dnevov ignorance in prelaganja odgovornosti je konec.
// **Olaf van Haperen - Eversheds Sutherland**

Minimalne sankcije

Direktiva NIS2 vsebuje obvezen seznam sankcij, vključno s pregledi na kraju samem, varnostnimi revizijami, varnostnimi pregledi, zahtevami za informacije in zahtevami za dostop do podatkov. Nekatere sankcije so enake za vse države, druge pa ne, na primer sankcije za resne kršitve. V takih primerih morajo države same zagotoviti učinkovite, sorazmerne in odvračilne sankcije. Tudi vrsto sankcij (kazenske ali upravne) določi država sama. Sankcije morajo biti primerne resnosti in naravi kršitve ter morajo upoštevati dejavnike, kot so povzročena škoda, sodelovanje s pristojnim organom in druge okoliščine.

Upravne globe

Namesto ali poleg drugih ukrepov se lahko glede na okoliščine primera naložijo upravne globe. Pri izrekanju upravne globe je treba upoštevati enake elemente kot pri drugih sankcijah. Kršitve se lahko kaznujejo z upravnimi globami v višini do 10 milijonov EUR ali 2 % letnega svetovnega prihodka, kar je višje. Lokalni nadzorni organi morajo oblikovati lastne politike za nalaganje glob.

GLOBE

Direktiva NIS2 uvaja globe v višini do 10 milijonov EUR ali do 2% letnega svetovnega prihodka.

ODSTAVITVE

Posamezniki z ustreznimi pooblastili ali vodstvenimi vlogami so lahko odstavljeni.

1

Podjetje **BrightEnergies** se po napadu z izsiljevalsko programsko opremo sooča s sankcijami. Kot pomemben subjekt mora zagotavljati najsodobnejšo kibernetsko varnost. CISO je suspendiran in podjetju sledi visoka globa. Direktor Lennard ugotavlja, da je varnost zdaj glavna prednostna naloga IT-ekipe in želi uvesti napredne varnostne rešitve za proaktivno preprečevanje napadov.

2

Na srečo se v **Waste2Resource** izognejo sankcijam. Incident je Kayleigh odprl oči, zato gre k izvršnemu direktorju in poudari, da bi lahko z nekaj več proračunskimi sredstvi organizacijo še bolje zavarovala. Čeprav se generalni direktor zaveda resnosti, je že precej zadovoljen: "Saj izpolnjujemo zahteve, kajne?" Kayleigh dobi nekoliko povečan proračun, da bi še bolj okrepila varnost.

Skupaj za odporno prihodnost

NIS2 vzpostavlja evropsko mrežo za povezavo v primeru kibernetskih kriz (EU-CyCLONe), ki bo zagotavljala podporo in usklajevanje v primeru obsežnega kibernetskega napada v EU. Strokovnjaki bodo tudi vztrajali pri sodelovanju in medsebojnem učenju med državami članicami, da bi si izmenjali nasvete in povečali medsebojno zaupanje.

Potrebujete pomoč pri implementaciji NIS2?

ESET Slovenija lahko za vašo organizacijo stori naslednje

Kot evropski ponudnik na področju digitalnih varnostnih rešitev z veseljem razmišljamo skupaj z vami in vam pomagamo pri vprašanjih, ki jih imate v zvezi z NIS2 ali njenim izvajanjem.

Možnosti, ki jih ponujamo na področju NIS2:

- izmenjava znanja prek naših kanalov, kot so Vodnik po digitalni varnosti ali naš korporativni blog
- interaktivna srečanja, kot so delavnice
- razmišljanje v zvezi s skladnostjo in izvajanjem ukrepov NIS2
- zagotavljanje varnostnih rešitev, ki prispevajo k skladnosti
- naši strokovnjaki so vedno na voljo za odgovore na vaša vprašanja

Vodilne rešitve za zakonsko skladnost z NIS2

ESET Slovenija nudi uvedbo, podporo ter vzdrževanje in upravljanje sistemov kibernetske varnosti, s katerimi bistveni in pomembni subjekti nenehno izboljšujejo oceno tveganja, poenostavijo varnostne procese ter skrajšajo čas za odkrivanje, preiskovanje in odzivanje na grožnje. ESET skupaj s partnerji iz njegovega strateškega zavezništva omogoča široko pokritost zahtev, ki jih bistvenim in pomembnim subjektom ne glede na velikost nalaga NIS2:

- obvladovanje tveganj kršitev varnosti podatkov
- upravljanje ranljivosti in varnostnega posodabljanja
- upravljanje varnostnih politik in poročanje o incidentih
- varnostno obveščanje
- usposabljanja za kibernetsko varnost
- avtomatizacija odkrivanja in odzivanja
- upravljanje storitve odkrivanja in odzivanja (SOC)
- več-faktorsko overjanje uporabnikov
- varnost omrežij in storitve zaščitenih komunikacij
- neprekinjeno poslovanje

Potrebujete več informacij? Prosimo, stopite v stik z nami!

Petra Veber
direktorica operacij

petra.veber@sisplet.com
Tel: (01) 428 94 66

Viri:

https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN

•

https://www.europarl.europa.eu/news/nl/press-room/20221107IPR49608/cyberbeveiliging-parlement-neemt-nieuwe-wet-aan-om-veerkracht-eu-te-versterken

EVERSHEDS SUTHERLAND & ESET®

Digital Security
Progress. Protected.