Sekcija za kibernetsko varnost, Združenje za informatiko in telekomunikacije
Dimičeva 13 ■ 1504 Ljubljana ■ T: (01) 58 98 000, 58 98 474 ■ sekv@gzs.si, zit@gzs.si ■ www.gzs.si

SKUPAJ ZMOREMO VEČ

e-pošta: sekv@gzs.si
https://www.gzs.si/sekv

Vprašanja in odgovori s spletnega dogodka »Kaj morajo podjetja vedeti o NIS-2?«

VPR: Kako zgleda primer poročila, ki ga je potrebno oddati v 24/72 ur in 1 mesec po odprtju incidenta? Ali obstaja kakšen standardiziran template?

In predvsem komu je treba javiti da je prišlo do incidenta ? Sporocite link prosim.

ODG (ivana.zolgarolenik@telekom.si) : Pojasnila o priglasitvi kibernetskih incidentov in izmenjavi informacij so na voljo na https://www.cert.si/prijava-incidenta/ in na https://www.cert.si/obvezna-priglasitev-incidenta/, kjer so opredeljeni tudi

Obrazci za poročanje

1. Zavezanci, kot jih določa metodologija po ZInfV, pri sporočanju incidentov sledijo Nacionalnemu načrtu odzivanja na kibernetske incidente (NOKI), ki je vodilo zavezancev, komu, kdaj in kako priglasiti kibernetski incident znotraj svojih sistemov. Zavezanci lahko v komunikaciji s SI-CERT prostovoljno uporabijo **obrazec Priloga E iz NOKI.**
2. Operaterji elektronskih komunikacij v skladu z ZEKom-2 incident priglasijo prek obrazca, predpisanega s strani AKOS Poročilo o varnostnem incidentu
3. Upravljavci pri sporočanju kršitev varnosti osebnih podatkov na področju posebnih obdelav sledijo določbam po ZInfV in pri priglasitvi incidenta lahko uporabijo obrazec Priloga E iz NOKI.

Ob zaznanem varnostnem incidentu pošljite prijavo z elektronskim sporočilom na naslov cert@cert.si

Marko Zavadlav <Marko.Zavadlav@unistarpro.si>:
Vsi zavezanci, ki niso državni organi, priglasijo incidente na SI-CERT.
Na povezavi https://www.cert.si/obvezna-priglasitev-incidenta/ je za vse zavezance, ki niso državni organi, navodilo, kako priglasiti incident. Vključeno je navodilo, kako izpolniti obrazec, kako ga poslati, kdaj ga poslati, kako je z velikim, prilogami.

VPR: Kdo je pristojen za podajo mnenja, ali sodi določeno podjetje med zavezance po NIS-2? Še posebej, ko to ni jasno glede na definicije po REACH. Konkretna situacija, ko je podjetje z identično dejavnostjo v državi A zavezanec (madžarska), v državi B ni zavezanec (Nizozemska), v državi C (Francija) pa se lahko samo odloči, ali sodi med zavezance?

ODG (ivana.zolgarolenik@telekom.si): Pristojnost za določanje, ali podjetje sodi med zavezance po NIS 2, je v rokah nacionalnih pristojnih organov, ki jih vsaka država članica EU določi v skladu z ZInfV-1 ali lokalno zakonodajo, ki implementira NIS 2. Če podjetje po izvedeni samooceni glede na kriterije NIS 2 oz. nacionalne zakonodaje ne more ugotoviti ali je zavezanec, je smiselno, da se posvetuje s pristojnim organom v posamezni državi.
URSIV bo v 4 mesecih od uveljavitve zakona pripravil platformo za samoregistracijo, na kateri bodo subjekti pri registraciji dobili tudi odgovor ali so zavezanci ali ne.

Marko Zavadlav <Marko.Zavadlav@unistarpro.si>: V Sloveniji je trenutno predlog, da mora vsako podjetje samo ugotoviti, ali je zavezanec in mora izvesti samoprijavo. V trenutno veljavnem zakonu sicer velja še, da mora pristojni organ ugotoviti, ali je podjetje zavezanec in ga o tem obvestiti, a po novem naj bi se to spremenilo. Poleg tega lahko pristojni organ oziroma država mimo teh določil odloči, da je neko podjetje zavezanec.
Država lahko tudi v lokalni zakonodaji spremeni določila (zaostri pogoje) glede kriterijev za določitev zavezancev.

VPR: Koliko čas (termin) imamo proizvodna podjetja na voljo, da se uskladimo z zahtevami NIS-2?

ODG (ivana.zolgarolenik@telekom.si) : Prehodno obdobje za bistvene in pomembne subjekte (tudi proizvodna podjetja) bo osemnajst mesecev od uveljavitve Zakona o informacijski varnosti (ZinfV-1). Bistveni subjekti, ki so bili določeni kot izvajalci bistvenih storitev in določeni organi državne uprave na podlagi ZinfV bodo morali sprejeti ukrepe v enem letu od uveljavitve tega zakona. Enako velja za operaterje po Zakonu o elektronskih komunikacijah.

VPR: Ali zadošča za zavezance kot potrditev skladnosti z NIS-2, da imajo certifikat ISO 27001? Če ne, kje je razkorak. Hvala.

ODG (ivana.zolgarolenik@telekom.si) : ISO/IEC 27001 je vsekakor dobra osnova za izpolnjevanje zahtev direktive NIS 2, vendar sam po sebi ne zadošča za izpolnjevanje vseh zahtev direktive NIS 2. Za ustrezno skladnost je potrebno smiselno upoštevati še:

- ISO/IEC 27002: Kodeks ravnanja za nadzor informacijske varnosti (predvsem pomemben pri delu dokumentacije povezane z zagotavljanjem SUVI);
- ISO 22301: Standard za sisteme upravljanja neprekinjenega poslovanja (predvsem pomemben pri delu dokumentacije povezane z zagotavljanjem sistema upravljanja neprekinjenega poslovanja; v praksi se uporabljata kratici SUNP in BCMS);
- ISO 31000: Splošne smernice za obvladovanje tveganj (pomemben za oba dela SUVI in SUNP);
- ISO 31010: Tehnike ocenjevanja tveganj (pomemben za oba dela SUVI in SUNP);
- ISO 28000: Upravljanje varnosti dobavne verige;
- ISO 27035: Upravljanje varnostnih incidentov;
- IEC 62443: Kibernetska varnost industrijskih sistemov (IACS).

Pri uvajanju namreč ni smiselno kompliciratiz uvajanjem standardov iz različnih standardizacijskih okolij, temveč se je smiselno odločiti za en okvir in tega uveljaviti v celoti.

VPR: Priklenjenost na dobavitelja: kako se obravnavajo "dobavitelji" odprtokodnih rešitev? Ali bi morali sklepati pogodbe z Apache foundation in podobni?
ODG (ivana.zolgarolenik@telekom.si) : Odprtokodne skupnosti niso klasični dobavitelji, ne zagotavljajo podpore, SLA-jev ali varnostnih popravkov in sklepanje pogodb z njimi v večini verjetno niti ni možno. Se pa po direktivi NIS 2 štejejo kot del dobavne verige, če jih organizacija uporablja v svoji infrastrukturi. Zato morajo organizacije kljub odprtokodni naravi teh rešitev oceniti tveganja

njihove uporabe, spremljati varnostne popravke in ranljivosti, ter imeti vzpostavljene postopke za njihovo varno uporabo. Kjer je kritična odvisnost, se priporoča tudi vključitev tretjih ponudnikov, ki nudijo podporo in pogodbene zaveze za odprtokodne rešitve. To vse mora biti dokumentirano kot del celovitega upravljanja tveganj v dobavni verigi, skladno z zahtevami NIS 2.

Marko Zavadlav <Marko.Zavadlav@unistarpro.si>:

Vedno je potrebno izhajati iz ocene tveganja. V primeru odprtokodnih rešitev pač ne morete sklepati pogodb z dobaviteljem, torej je potrebno razmisliti o kompenzacijskih kontrolah. Seveda, če upo0raba odprtokodnih rešitev zadošča vašim zahtevam glede razpoložljivosti, zaupnosti in celovitosti in tveganjem, ki izhajajo iz uporabe le-teh.

VPR: Koliko podrobna naj bi bila izhodna strategija? Oz kaj se v njej lahko definira?

ODG(ivana.zolgarolenik@telekom.si): Namen strategije je zagotoviti nadzorovan, predvidljiv in varen izstop brez vpliva na poslovanje ali varnost. Zato mora biti izhodna strategija dovolj podrobna, da jasno določa pogoje, postopke in odgovornosti v primeru prenehanja sodelovanja s partnerjem ali dobaviteljem. V njej naj bi se opredelilo časovni okvir in način prenehanja pogodbenega razmerja, prenos podatkov in znanja, izbris ali vračilo informacij, odgovorne osebe, morebitne pogodbene obveznosti po zaključku sodelovanja ter načrt za nemoten prehod na novega ponudnika ali interno rešitev.

VPR: Koliko podrobna naj bi bila izhodna strategija? Oz kaj se v njej lahko definira?

Marko Zavadlav <Marko.Zavadlav@unistarpro.si>:

Najbrž se v svojih odgovorih prevečkrat ponavljam, ampak vedno izhajamo iz ocene tveganja. Pri izhodni strategiji najprej identificiramo grožnje, kot so na primer nejasnost pogodb, pristojnosti, odgovornosti, potem tehnične omejitve, kot so pasovne širine, različni formati, nadalje opredelimo kakšne časovne komponente, čas izpada, kompatibilnost in podobno. Ko vidimo, na kaj moram biti pozorni, pripravimo izhodno strategijo, kako je podrobna, je odvisno od primera. Načelno ne potrebujemo vseh podrobnosti, a moramo imeti opisane scenarije za izvedbo prekinitve.

VPR: Koliko razumem je ocenjevanje tveganj precej subjektivno. ali obstajajo kakšni objektivni kriteriji predvsem za področje IT sistemov in kibernetske varnosti?

Marko Zavadlav <Marko.Zavadlav@unistarpro.si>:

Najprej moramo zelo natančno opredeliti metodologijo. Če tega ni, potem je priložnost za subjektivnost ogromna. Nadalje je priporočljivo, da se oceno moderira, torej, da se sproti pojasnjuje, kaj pomenijo grožnje, kako se identificira ranljivosti, kako se ocenjuje vpliv.

VPR: Zavedam se da je strošek incidenta vsekakor neprimerljiv z investicijami. vseeno pa morda lahko delite oceno "čez palec" koliko eno srednje veliko podjetje s 50 zaposlenimi, dosti procesi na računalnikih rabi nameniti za SOC, ocene, dokumentacijo, kontrole,...

Marko Zavadlav <Marko.Zavadlav@unistarpro.si>:

Na to vprašanje je nemogoče odgovoriti. Ključno je, da imate v podjetju varnostno politiko, ki jo redno posodabljate in izvajate ter merite kontrole, ki iz nje izhajajo. Glede SOC pa je zopet odvisno od tega, katere storitve SOC želite. In pa zopet, izhajamo iz ocene tveganja. V tem primeru, kaj moramo varovati, kdo nam grozi, kakšno škodo nam lahko povzroči.