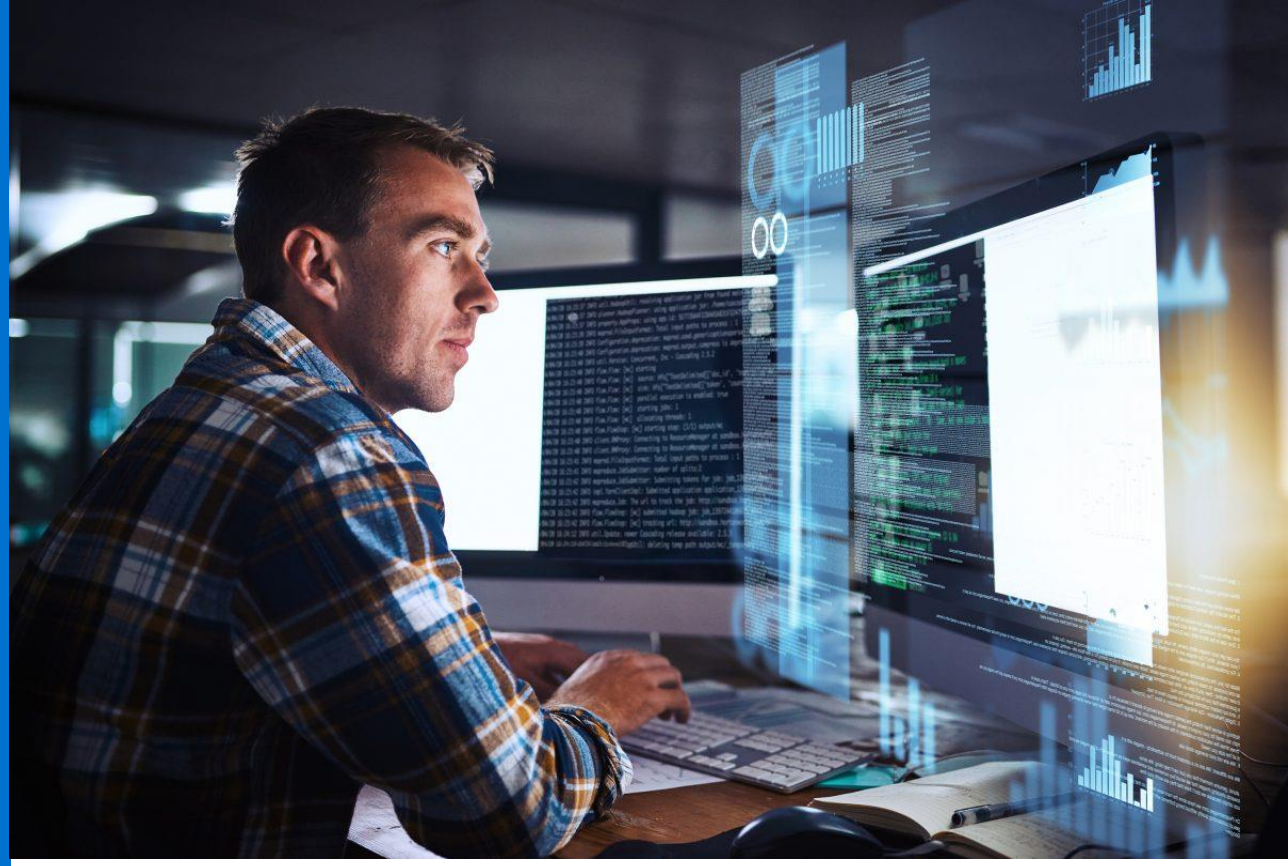
Revizijski pogled: Priprava na skladnost z evropsko direktivo NIS 2 in obvladovanje IKT izzivov v organizacijah



Uroš Žust, CISA, aPRIS, CISM, CISSP, PMP

Partner, Mazars IT

22. 5. 2024

Gospodarska zbornica Slovenije

zit Združenje za informatiko in telekomunikacije

mazars

Uvod
Ključne informacije (1/2)

Roki NIS 2 direktive:

- 16 Januar 2023 – Direktiva v veljavi
- 17 Oktober 2024 – Uvedba ukrepov, potrebnih za uskladitev z direktivo (Člen 41.1)
- 18 Oktober 2024 – Predpisi veljajo za vse zavezance (Člen 41.2)
- 17 April 2025 – Definiran obseg zavezancev (Člen 3.3)

Direktiva se navezuje na ostale direktive in uredbe:

- Direktiva Critical Entities Resilience (CER)
  (Fizična varnosti & varnost pomembnih procesov)
- Uredba Digital Operational Resilience Act (DORA)

Zahteve NIS 2
Povzetek pomembnih navedb za organizacije

Preambula (83) – Zunanje izvajanje

Zahteve **glede ukrepov za obvladovanje tveganj za kibernetsko varnost in obveznosti poročanja**, določene v tej direktivi, bi se morale uporabljati za ustrezne bistvene in pomembne subjekte **ne glede na to, ali ti subjekti svoje omrežne in informacijske sisteme vzdržujejo sami ali pa njihovo vzdrževanje oddajajo zunanjim izvajalcem**.

Člen 4 – Sektorski pravni akti Unije

1. Kadar se s sektorskimi pravnimi akti Unije zahteva, da bistveni ali pomembni subjekti bodisi sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost bodisi priglasijo pomembne incidente, in **kadar so takšne zahteve po učinku vsaj enakovredne obveznostim iz te direktive**, se ustrezne določbe te direktive, vključno z določbami o nadzoru in izvrševanju iz poglavja VII, **za take subjekte ne uporabljajo**. **Kadar** sektorski pravni akti Unije **ne zajemajo vseh subjektov v določenem sektorju**, ki spadajo na področje uporabe te direktive, **se** ustrezne določbe te direktive **še naprej uporabljajo** za subjekte, ki niso zajeti v sektorskih pravnih aktih Unije.
2. Zahteve iz odstavka 1 tega člena se štejejo za enakovredne obveznostim iz te direktive, kadar:
   a) imajo **ukrepi za obvladovanje tveganj za kibernetsko varnost vsaj enakovreden učinek** kot ukrepi iz člena 21(1) in (2) ali
   b) sektorski pravni akt Unije določa takojšen, po potrebi samodejen in neposreden, dostop do priglasitev incidentov za skupine CSIRT, pristojne organe ali enotne kontaktne točke iz te direktive, in kadar so zahteve za priglasitev pomembnih incidentov po učinku vsaj enakovredne tistim iz člena 23(1) do (6) te direktive.

Omenjene zahteve so izpostavljene tudi v 3. členu Osnutka predloga novega ZInfV-1.

Zahteve NIS 2
Povzetek pomembnih navedb za organizacije

Člen 20 – Upravljanje

1. Države članice zagotovijo, **da upravljalni organi bistvenih in pomembnih subjektov odobrijo ukrepe za obvladovanje tveganj za kibernetsko varnost**, ki jih sprejmejo zadevni subjekti, ...
2. Države članice zagotovijo, da **se morajo člani upravljalnega organa bistvenih in pomembnih subjektov usposabljati**, in spodbujajo bistvene in pomembne subjekte, da podobno usposabljanje redno ponujajo svojim zaposlenim, da pridobijo dovolj znanja in spretnosti, ki jih usposobi za prepoznavanje in ocenjevanje tveganj in za oceno praks obvladovanja tveganj za kibernetsko varnosti ter njihovega vpliva na storitve, ki jih opravlja subjekt.

Omenjene zahteve so izpostavljene tudi v 19. členu Osnutka predloga novega ZInfV-1.

Zahteve NIS 2
Povzetek pomembnih navedb za organizacije

Člen 21 – Ukrepi za obvladovanje tveganj za kibernetsko varnost

1. Države članice zagotovijo, da bistveni in pomembni subjekti sprejmejo ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, …
   … morajo ukrepi iz prvega pododstavka **zagotavljati raven varnosti omrežnih in informacijskih sistemov, ki ustreza obstoječim tveganjem**. Pri ocenjevanju sorazmernosti teh ukrepov **je treba ustrezno upoštevati stopnjo izpostavljenosti subjekta tveganjem, velikost subjekta in verjetnost pojava incidentov ter njihovo resnost**, vključno z njihovim družbenim in gospodarskim vplivom.

Omenjene zahteve so izpostavljene tudi v 21. členu Osnutka predloga novega ZInfV-1.

Zahteve NIS 2
Povzetek pomembnih navedb za organizacije

Člen 21 – Ukrepi za obvladovanje tveganj za kibernetsko varnost

2. Ukrepi iz odstavka 1 morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščititi omrežne in informacijske sisteme ter njihovo fizično okolje pred incidenti, in vključujejo vsaj naslednje:
   a) politike o analizi tveganja in varnosti informacijskih sistemov;
   b) obvladovanje incidentov;
   c) neprekinjeno poslovanje, kot je upravljanje varnostnih kopij in vnovična vzpostavitev delovanja po nepredvidljivih dogodkih, ter obvladovanje kriz;
   d) **varnost dobavne verige**, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;
   e) varnost pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov, **vključno z obravnavanjem in razkrivanjem ranljivosti**;
   f) politike in postopke za **oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost**;
   g) osnovne prakse kibernetske higiene in usposabljanje na področju kibernetske varnosti;
   h) politike in postopke v zvezi z **uporabo kriptografije** in po potrebi šifriranjem;
   i) varnost človeških virov, politike nadzora dostopa in upravljanje sredstev;
   j) **uporaba večfaktorske avtentikacije** ali rešitev neprekinjene avtentikacije, **varovanih glasovnih, video in besedilnih komunikacij** in varnih sistemov za komunikacije v sili znotraj subjekta, kadar je to primerno.

Omenjene zahteve so izpostavljene tudi v 21. členu Osnutka predloga novega ZInfV-1.

Zahteve NIS 2
Povzetek pomembnih navedb za organizacije

Člen 23 – Obveznosti poročanja

1. Vsaka država članica zagotovi, da bistveni in pomembni subjekti njeni skupini CSIRT ali, kadar je to potrebno, njenemu pristojnemu organu brez nepotrebnega odlašanja v skladu z odstavkom 4 priglasijo vse incidente, ki pomembno vplivajo na zagotavljanje njihovih storitev, kot je navedeno v odstavku 3 (pomemben incident).

4. Države članice zagotovijo, da zadevni subjekti za namen priglasitve iz odstavka 1 skupini CSIRT ali po potrebi pristojnemu organu predložijo:

   a) brez nepotrebnega odlašanja, **v vsakem primeru pa v 24 urah po seznanitvi z incidentom, zgodnje opozorilo**, iz katerega je po potrebi razvidno, ali je bil pomemben incident domnevno povzročen z nezakonitim ali zlonamernim dejanjem ali bi lahko imel čezmejni vpliv;

   b) brez nepotrebnega odlašanja, **v vsakem primeru pa v 72 urah po seznanitvi s pomembnim incidentom, priglasitev incidenta**, s katero se po potrebi posodobijo informacije iz točke (a) in navede začetna ocena pomembnega incidenta, vključno z njegovo resnostjo in vplivom ter, kadar so na voljo, kazalniki ogroženosti;

   c) na zahtevo skupine CSIRT ali po potrebi pristojnega organa vmesno poročilo o ustreznih posodobitvah stanja;

   d) končno poročilo, najpozneje v enem mesecu po predložitvi priglasitve incidenta iz točke (b), ki vključuje naslednje:

      i. podroben opis incidenta, vključno z njegovo resnostjo in vplivom;

      ii. vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil incident;

      iii. izvedene blažilne ukrepe in take ukrepe v teku;

      iv. po potrebi čezmejni vpliv incidenta;

Omenjene zahteve so izpostavljene tudi v 25. in 26. členu Osnutka predloga novega ZInfV-1.

Zahteve ZInfV-1 (Osnutek)
Kaj predpisuje predlagani novi zakon

Člen 4 – obdelava podatkov in informacij

1. … **Obdelava osebnih podatkov** v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežij, informacijskih sistemov in informacij **pomeni zakoniti interes zadevnega upravljavca podatkov**.

Člen 20 – varnostna dokumentacija bistvenih in pomembnih subjektov

1. Bistveni in pomembni subjekti **za zagotavljanje visoke ravni informacijske in kibernetske varnosti in odpornosti svojih omrežnih in informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja**, ki temeljita na pristopu upoštevanja vseh nevarnosti in morata obsegati najmanj:
   - natančen in posodobljen popis informacijskih in drugih sredstev ter podatkov, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter določitev njihovih upravljavcev;
   - analizo obvladovanja tveganj, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;
   - politiko in načrt neprekinjenega poslovanja, vključno z oceno vpliva na poslovanje, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij in določitvijo vlog ter odgovornosti;
   - načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;
   - načrt odzivanja na incidente s protokolom obveščanja pristojnega CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente informacijske varnosti ter opisom vlog in odgovornosti za odzivanje na incidente;
   - načrt varnostnih ukrepov za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost, ki upoštevajo in področne posebnosti bistvenega ali pomembnega subjekta;
   - politiko s postopki za oceno učinkovitosti varnostnih ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

2. Bistveni in pomembni subjekti določijo obseg sistema upravljanja in varovanja informacij ter neprekinjenega poslovanja ob upoštevanju rezultatov analize vpliva na poslovanje, kateri mora obsegati najmanj tista informacijska, komunikacijska in druga sredstva, podatke ter procese, ki so potrebni za njihovo delovanje ali opravljanje storitev; .

Zahteve ZInfV-1 (Osnutek)
Kaj predpisuje predlagani novi zakon

Člen 21 – ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov

2. Varnostni ukrepi morajo temeljiti na pristopu upoštevanja vseh nevarnosti, katerega namen je zaščita omrežnih in informacijskih sistemov ter njihovega fizičnega okolja pred incidenti, in morajo obsegati najmanj:

- **podporo vodstva subjekta pri zagotavljanju informacijske in kibernetske varnosti** in vključitvijo področja informacijske in kibernetske varnosti v letni načrt poslovanja oziroma letni program dela;
- **zagotavljanje integritete kadrov v povezavi z informacijsko varnostjo** pred zaposlitvijo, med …;
- **osnovne prakse kibernetske higiene in usposabljanje na področju informacijske in kibernetske varnosti**;
- varnost človeških virov, preverjanje identitete uporabnikov, zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop;
- izvajanje in upravljanje varnostnih kopij podatkov;
- **zagotavljanje in ohranjanje dnevniških zapisov o delovanju omrežnih in informacijskih sistemov**, ki jih uporabljajo za svoje delovanje ali opravljanje storitev, njihovih uporabnikov in administratorjev **za obdobje najmanj šestih mesecev**, …;
- **upravljanje omrežnih in informacijskih sistemov**, ki jih uporabljajo …;
- politike in postopke v zvezi z uporabo kriptografije in po potrebi šifriranjem;
- upravljanje prometa in komunikacij;
- **varnost dobavne verige** z določitvijo ustreznih minimalnih zahtev povezanih s kibernetsko varnostjo za ključne dobavitelje …;
- **fizično in tehnično varovanje prostorov in dostopov do prostorov**, kjer so ključni deli omrežnih in informacijskih sistemov …;
- **varnostne mehanizme v posamezni aplikativni programski opremi** za izvajanje dejavnosti, …;
- upravljanje in preprečevanje izrab tehničnih ranljivosti;
- zaščita pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov;
- **uporabo večfaktorske avtentikacije** ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj za kibernetsko varnost in
- **uporabo varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili** znotraj subjekta, kadar je glede na dejavnost subjekta to primerno.

Zahteve ZInfV-1 (Osnutek)
Kaj predpisuje predlagani novi zakon

Člen 21 – ukrepi za obvladovanje tveganj za kibernetsko varnost bistvenih in pomembnih subjektov (nadaljevanje)

5. Bistveni in pomembni subjekti … , **morajo upoštevati ranljivosti, ki so specifične za posameznega neposrednega dobavitelja in ponudnika storitev ter splošno kakovost proizvodov ter praks svojih dobaviteljev in ponudnikov storitev na področju kibernetske varnosti**, vključno z njihovimi varnimi razvojnimi postopki. Bistveni in pomembni subjekti morajo ugotavljati tudi kateri ukrepi so ustrezni za zagotovitev varnosti dobavne verige … .

6. Bistveni ali pomembni subjekti **v rednih časovnih obdobjih**, ki jih opredeli v politiki … in ob zaznanih ranljivostih, **preverjajo izpolnjevanje ukrepov** iz … . Če pri tem ugotovijo, da ne izpolnjujejo vseh ukrepov … ali pa so ti neustrezno izvajani, morajo **brez nepotrebnega odlašanja sprejeti vse potrebne, ustrezne in sorazmerne popravne ukrepe**.

9. Bistveni in pomembni subjekti **ne smejo uporabljati informacijsko-komunikacijskih rešitev, ki imajo aktivno izkoriščane ranljivosti**, **brez dodatne izvedbe ocene tveganja** in kjer je to glede na oceno tveganja primerno, ustreznih popravljalnih ukrepov, ki znižajo stopnjo tveganja na sprejemljivo raven.

Zahteve ZInfV-1 (Osnutek)
Kaj predpisuje predlagani novi zakon

Člen 41 – splošne odločbe

4. **Inšpektor nadzira ali zavezanci izpolnjujejo svoje obveznosti** iz tega zakona predvsem **z neposrednim vpogledom v podatke, dokumentacijo ter v omrežne in informacijske sisteme; preverjanjem pogojev in načina izvajanja ukrepov za obvladovanje tveganj kibernetske varnosti; pregledom območij, objektov in prostorov zavezancev, kjer se nahajajo ključni, krmilni in nadzorni informacijski sistemi ter podatki, pregledom dokumentacije o izvrševanju predpisanih obveznosti obveščanja o kibernetskih incidentih** ter drugih obveznostih na podlagi zahtev pristojnih organov iz tega zakona; **pregledom poročil o izvedbi revizije informacijskih sistemov in varnostnih pregledov omrežja ter informacijskih sistemov** in pregledom druge dokumentacije, potrebne za izvedbo nadzora.

Zahteve ZInfV-1 (Osnutek)
Kaj predpisuje predlagani novi zakon

Člen 42 & 43 – Nadzor bistvenih / pomembnih subjektov

2. Inšpektor je pri izvajanju svojih nadzornih nalog pri bistvenih subjektih pooblaščen za to, da:
   1. opraviti inšpekcijske preglede na kraju samem in nadzor na daljavo, vključno z naključnimi pregledi, ki jih lahko izvede skupaj z usposobljenimi strokovnjaki; (vsi subjekti)
   2. **odrediti izvedbo redne in ciljno usmerjene revizije skladnosti s predpisi s področja informacijske in kibernetske varnosti,** ki jo izvede preizkušeni revizor informacijskih sistemov; (bistveni subjekti)
   3. **odrediti izvedbo izredne revizije skladnosti,** ki jo izvede preizkušeni revizor informacijskih sistemov, ko je to utemeljeno zaradi pomembnega incidenta ali očitne kršitve tega zakona s strani bistvenega subjekt; (bistveni subjekti)
   2. **odrediti izvedbo ciljno usmerjene revizije skladnosti s predpisi s področja informacijske in kibernetske varnosti**, ki jo izvede preizkušeni revizor informacijskih sistemov;

   4. / 3. opraviti varnostni pregled, ki temelji na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganj. (vsi subjekti)

Člen 45 – ocena skladnosti

2. **Izvajanje ocene skladnosti** morajo bistveni subjekti opraviti **najmanj enkrat na dve leti**, pred potekom roka pa, če to zahteva inšpektor ali v primeru pojava pomembnega incidenta. Ocena skladnosti se izvaja kot **skladnosti s predpisi s področja informacijske varnosti ali v okviru notranje revizije**, ki se izvaja na podlagi drugih predpisov in vključuje tudi področje informacijske varnosti na podlagi tega zakona … Oceno skladnosti v okviru notranje revizije poleg preizkušenih revizorjev lahko izvajajo tudi notranji revizorji v sodelovanju z veščakom za informacijsko tehnologijo

Člen 57 – sprejem ukrepov za obvladovanje tveganj

Bistveni in pomembni subjekti sprejmejo **ukrepe za obvladovanje tveganj za kibernetsko varnost** … **v roku 12 mesecev od uveljavitve tega zakona**.

NIS 2 v praksi
Kako zagotoviti skladnost

Osebni pogled

- Izvedba analize vrzeli (gap analysis), šele nato operativno delo (odprava odstopanj)
- Izbira ustreznega kontrolnega ogrodja (framework) – preveriti obstoječe zahteve in sinergije z obstoječimi in prihajajočimi predpisi.
- Izdelava registra informacijskih sredstev **->** ocena kibernetskih tveganj (metodologija) **->** analiza poslovnih učinkov - BIA **->** neprekinjeno poslovanje in okrevanje po katastrofi.
- Področja posebne pozornosti:
  - Upravljanje kibernetskih tveganj s strani upravljalnega organa
  - Ustrezno izobraževanje kadrov upravljalnega organa
  - Poročanje incidentov
  - Kriptografija in šifriranje
  - Varnost dobavne verige
  - Varnost komunikacij (sistemov za komuniciranje)
- Redni pregledi (glede na zakonske zahteve).

Vprašanja

Thank you for your attention.

Uroš Žust, CISA, aPRIS, CISM CISSP, PMP

Partner, IT Assurance & Advisory

+ 386 41 395 386

uros.zust@mazars.si

Mazars IT d.o.o.

Verovškova ulica 55a

1000 Ljubljana, Slovenia

www.mazars.si

mazars