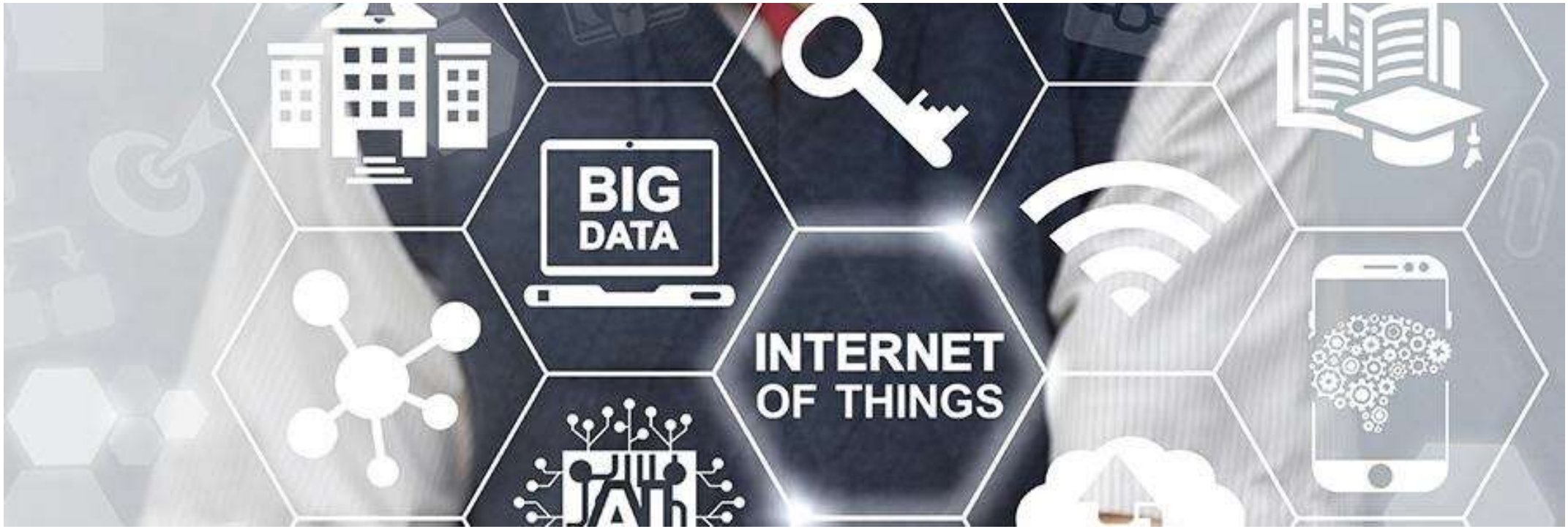


Kibernetska varnost v javni upravi

Tevž Delak, CISA, CDPSE

18 september 2024

forvis mazars

Izhodišče
Kibernetska varnost

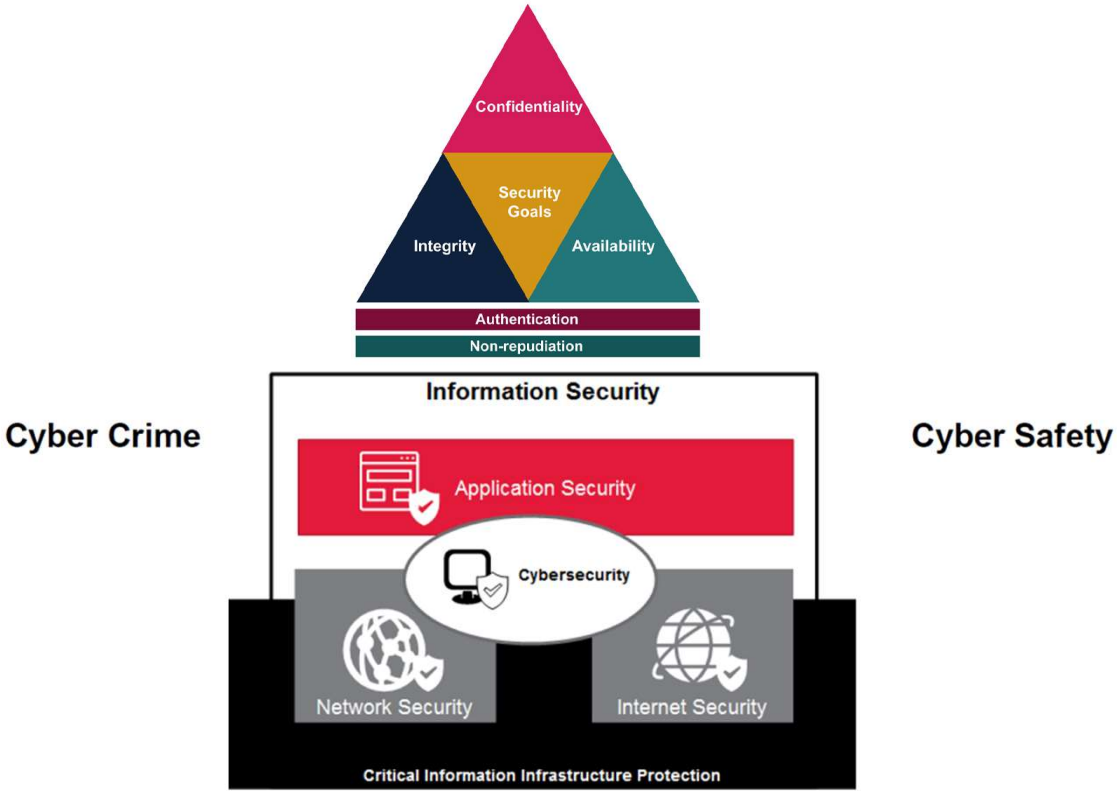
NIST slovar

Preprečevanje škode, zaščita in obnova računalnikov, elektronskih komunikacijskih sistemov, elektronskih komunikacijskih storitev, žičnih komunikacij, elektronskih komunikacij, vključno z informacijami, ki jih vsebujejo, z namenom, da se zagotovi njihova razpoložljivost, celovitost, avtentičnost, zaupnost in nepreklicnost.

ISO/IEC 270832 Cybersecurity standard

„Cybersecurity“ ali „Cyberspace security,“ ki je opredeljena kot zaščita zasebnosti, celovitosti in razpoložljivosti informacij v kibernetskem prostoru.

„Cyberspace“ kot kompleksno okolje, ki je posledica interakcije ljudi, programske opreme in storitev na internetu s pomočjo tehnoloških naprav in z njim povezanega omrežja, ki ne obstaja v fizični obliki.



Izhodišče
Pomen tehnologije v današnjem poslovnem okolju

Zakaj je tako pomemben?

- Podjetja se vedno bolj zanašajo na tehnologijo.
- Tehnologija predstavlja konkurenčno prednost:
  - izboljšano sprejemanje odločitev
  - večja produktivnost in učinkovitost
  - izboljšana izkušnja strank
  - globalni doseg
- Tehnologija vpliva na vse poslovne procese, vključno z računovodstvom in financami.
- Trend digitalizacije se ne bo le nadaljeval, temveč se bo v prihodnosti tudi povečeval.
- Nove tehnologije prinašajo nove grožnje, predvsem kibernetske grožnje.

forvis mazars

Uvod
Situacija v EU

Situacija na področju EU

- Število kibernetskih incidentov narašča.
- EU se zaveda vpliva digitalizacije na celoten ekosistem organizacij in potrebe po vzpostavitvi jasnih pravil na področju upravljanja kibernetskih tveganj – EU Cybersecurity Strategy (2020).
- EU se fokusira na razvoj skupinskih zmogljivosti odzivanja na večje kibernetske napade in doseganja kibernetske varnosti in stabilnosti v kibernetskem prostoru.
- Namen je zagotoviti učinkovit odziv na kibernetska tveganja z uporabo skupnih sredstev in znanj po članicah EU.
- ENISA (European Union Agency for Cybersecurity) – krovni organ za upravljanje s kibernetskimi tveganji.
- EU CyCLONe (The European cyber crisis liaison organisation network) - mreža za sodelovanje nacionalnih organov držav članic, pristojnih za obvladovanje kibernetskih kriz.

Uvod
Situacija v Sloveniji

SI-CERT Poročilo o kibernetski varnosti

Uvod
Standardi, okvirji

Svetovno priznani in uveljavljeni standardi in okvirji na področju kibernetske varnosti

- NIST CSF verzija 2.0 (februar 2024)
- CIS Controls verzija 8 (maj 2021)
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (oktober 2022)
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls (februar 2022)
- ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity (julij 2012)
- COBIT 2019 (2018)

Uvod
Zakonodaja

Akti povezani s kibernetsko varnostjo na področju EU

- **The Cyber Resilience Act** – regulativa o zahtevah glede kibernetske varnosti naprav z digitalnimi elementi (bolj varna strojna in programska oprema)
- **Cybersecurity Act** – predvsem fokusirana na okrepitev vloge ENISE kot centralnega organa za operativno sodelovanje in krizno upravljanje v EU ter certifikacije IKT produktov, procesov in storitev
- **Cyber Solidarity Act** – skupni napori za izboljšanje odziva na kibernetska tveganja v sklopu EU. Fokus je na European Cybersecurity Shield in Cyber Emergency Mechanism, vse z namenom zagotavljanja boljših metod obrambe pred kibernetskimi tveganji
- **NIS 2 Directive** – usmerjena v zagotavljanje skupnega visokega nivoja zagotavljanja kibernetske odpornosti
- **Digital Operational Resilience Act (DORA)** – specifična uredba za finančni sektor, namenjena dvigu odpornosti finančnih sistemov proti kibernetskim grožnjam. Fokusirana je na izboljšanje upravljanja tveganja IKT, poročanja o incidentih, izboljšanja operativnega testiranja odpornosti ter vključevanje zunanjih izvajalcev
- **General Data Protection Regulation (GDPR)** – fokusirana na zaščito podatkov in informacij
- **Critical Entities Resilience (CER) Directive** – fokusirana predvsem na fizični aspekt varovanja
- **Zakon o informacijski varnosti (ZInfV)** - ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji

forvis mazars

NIS 2
Namen

Kaj je spodbudilo razvoj NIS 2 Direktive

- Pomanjkljivosti NIS 1 Direktive (2016)
  - Nezadostna raven kibernetske odpornosti
  - Izvajanje se je med državami članicami zelo razlikovalo
  - Nekateri ključni sektorji so bili izpuščeni
  - Ni skupnega odzivanja na incidente
  - Nejasna odgovornost
- Večja jasnost odvisnosti od zunanjih izvajalcev
- Digitalni incidenti vplivajo na celoten ekosistem organizacij
- EU se fokusira na digitalna sistemska tveganja
- Število kibernetskih incidentov narašča

NIS 2
Ključne informacije

NIS 2 v Sloveniji

- Ključni datumi:
  - 16 Januar 2023 – 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)
  - 18 Oktober 2025 - Subjekti sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost (iz osnutka ZInfV-1 JO2)
- Zavezanci:
  - Velike organizacije (več kot 250 zaposlenih in več kot 50 milijonov prihodkov) – Bistveni subjekti
  - Srednje organizacije (več kot 50 zaposlenih in več kot 10 milijonov prihodkov) – Pomembni subjekti
  - Majhne in mikro organizacije (odločitev države) – Odvisno od storitev, ki jih izvajajo
  - Javna uprava (z izjemami) – Bistveni subjekti
- Razlog za pripravo novega Zakona o informacijski varnosti (ZInfV-1)

NIS 2
Zavezanci

Visoko kritični sektorji / bistveni subjekti (Priloga I)

- Energija (elektrika, **daljinsko ogrevanje in hlajenje**, nafta, plin, **vodik**)
- Promet (zračni, železniški, vodni, cestni)
- Bančništvo
- Infrastruktura finančnega trga
- Zdravje
- Pitna voda
- **Odpadna voda**
- Digitalna infrastruktura
- **Upravljanje storitev IKT (med podjetji)**
- **Javna uprava**
- **Vesolje**

Ostali kritični sektorji / pomembni subjekti (Priloga II)

- **Poštne in kurirske storitve**
- **Ravnanje z odpadki**
- **Izdelava, proizvodnja in distribucija kemikalij**
- **Pridelava, predelava in distribucija živil**
- **Proizvodnja (proizvodnja medicinskih pripomočkov ter in vitro diagnostičnih medicinskih pripomočkov; proizvodnja računalnikov, elektronskih in optičnih izdelkov; proizvodnja električnih naprav; proizvodnja drugih strojev in naprav; proizvodnja motornih vozil, prikolic in polprikolic; proizvodnja drugih vozil in plovil)**
- Digitalni ponudniki
- **Raziskave**

***Zeleno odebeljeni** sektorji so v NIS 2 novi glede na NIS.

forvis mazars

NIS 2
Povzetek pomembnih navedb za organizacije

Direktiva - Preambule

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**.

Preambula (125) – Usposobljenost nadzornikov

Pristojni organi bi morali zagotoviti, da njihove nadzorne naloge v zvezi z bistvenimi in pomembnimi subjekti izvajajo usposobljeni strokovnjaki, ki bi morali imeti potrebna znanja in spretnosti za izvajanje teh nalog, … , **vključno s prepoznavanjem pomanjkljivosti v podatkovnih zbirkah, strojni opremi, požarnih zidovih, šifriranju in omrežjih**.

NIS 2
Povzetek pomembnih navedb za organizacije

Direktiva - Členi

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, 9. in 10. odstavku Osnutka predloga novega ZInfV-1.

NIS 2
Povzetek pomembnih navedb za organizacije

Direktiva - Členi

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, da izpolnijo člen 21, nadzorujejo njihovo izvajanje in **lahko odgovarjajo za kršitve tega člena s strani subjektov**.
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, odstavki 1 - 5 Osnutka predloga novega ZInfV-1.

NIS 2
Povzetek pomembnih navedb za organizacije

Direktiva - Členi

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**, ki jih ti subjekti uporabljajo za njihovo delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike svojih storitev in druge storitve.

   Ob upoštevanju najsodobnejših in po potrebi ustreznih evropskih in mednarodnih standardov ter stroškov izvajanja 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, 1. in 3. odstavku Osnutka predloga novega ZInfV-1.

NIS 2
Povzetek pomembnih navedb za organizacije

Direktiva - Členi

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 bolj podrobno izpostavljene tudi v 20. členu, 1. odstavku ter 21. členu, 2. odstavku Osnutka predloga novega ZInfV-1.

forvis mazars

NIS 2
Povzetek pomembnih navedb za organizacije

Direktiva - Členi

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) **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;
   d) V primeru **incidenta, ki je ob predložitvi končnega poročila** iz točke (d) **še vedno v teku**, bi morale države članice poskrbeti, da subjekti **takrat predložijo poročilo o napredku, končno poročilo pa najpozneje en mesec po razrešitvi incidenta**.

Omenjene zahteve so izpostavljene tudi 25. členu, 1. odstavku ter 26. členu, 1. in 2. odstavku Osnutka predloga novega ZInfV-1.

forvis mazars

ZInfV-1 JO2
Povzetek pomembnih navedb za organizacije

Zakon (ZInfV-1) - Členi

Člen 4 – obdelava podatkov in informacij

1. Obdelava osebnih podatkov na podlagi tega zakona se izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov, ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev pa tudi v skladu s predpisom, ki ureja zasebnost na področju elektronskih komunikacij. **Obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežij, informacijskih sistemov in informacij pomeni zakoniti interes zadevnega upravljavca podatkov**.

Člen 9 – pristojni nacionalni organ

1. **Pristojni nacionalni organ je Urad Vlade Republike Slovenije za informacijsko varnost (URSIV)**

ZInfV-1 JO2
Povzetek pomembnih navedb za organizacije

Zakon (ZInfV-1) - Členi

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:
    1. **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;
    2. **analizo obvladovanja tveganj**, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;
    3. **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;
    4. **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;
    5. **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;
    6. **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;
    7. **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.

forvis mazars

ZInfV-1 JO2
Povzetek pomembnih navedb za organizacije

Zakon (ZInfV-1) - Členi

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:

1. podporo vodstva subjekta pri zagotavljanju informacijske in kibernetske varnosti in **vključitvijo področja informacijske in kibernetske varnosti v letni načrt poslovanja** oziroma letni program dela;
2. **zagotavljanje integritete kadrov v povezavi z informacijsko varnostjo** pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve;
3. **osnovne prakse kibernetske higiene in usposabljanje** na področju informacijske in kibernetske varnosti;
4. **varnost človeških virov, preverjanje identitete** uporabnikov, zagotavljanje **ravni dostopnosti informacij in upravljanje pooblastil za dostop**;
5. **izvajanje in upravljanje varnostnih kopij podatkov**;
6. **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**, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja ustrezno obvladovati z daljšo hrambo dnevniških zapisov. **Ohranjanje dnevniških zapisov se zagotavlja primarno na ozemlju Republike Slovenije**, sekundarno pa se lahko zagotavlja na ozemlju Evropske unije, razen subjektov s področja digitalne infrastrukture, bančništva in infrastrukture finančnega trga, kateri lahko ohranjanje dnevniških zapisov v celoti zagotavlja na ozemlju Evropske unije;
7. upravljanje **omrežnih in informacijskih sistemov**, ki jih uporabljajo za svoje delovanje ali opravljanje storitev z določitvijo ustrezne odgovornosti za njihovo zaščito;
8. **politike in postopke v zvezi z uporabo kriptografije** in po potrebi šifriranjem;
9. **upravljanje prometa in komunikacij**;

ZInfV-1 JO2
Povzetek pomembnih navedb za organizacije

Zakon (ZInfV-1) - Členi

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

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 (nadaljevanje):
   10. **varnost dobavne verige** z določitvijo ustreznih minimalnih zahtev povezanih s kibernetsko varnostjo za **ključne dobavitelje ali ponudnike storitev**, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;
   11. **fizično in tehnično varovanje** prostorov in dostopov do prostorov, kjer so ključni deli omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev;
   12. **varnostne mehanizme v posamezni aplikativni programski opremi** za izvajanje dejavnosti, vključno z varnostjo pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov ter obravnavanjem in razkrivanjem ranljivosti;
   13. **upravljanje in preprečevanje izrab tehničnih ranljivosti**;
   14. **zaščita pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov**;
   15. **uporabo večfaktorske avtentikacije** ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj za kibernetsko varnost in
   16. **uporabo varovanih glasovnih, video in besedilnih komunikacij** in varnih sistemov za komunikacije v sili znotraj subjekta, kadar je glede na dejavnost subjekta to primerno.
4. **Dnevniški zapisi** morajo biti hranjeni na način, ki zagotavlja njihovo **celovitost, avtentičnost, razpoložljivost in zaupnost v primeru incidentov**.
5. Bistveni ali pomembni subjekti **najmanj enkrat letno oziroma v rednih časovnih obdobjih**, ki jih opredelijo v politiki in postopkih za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost in ob zaznanih ranljivostih, **preverjati izpolnjevanje varnostnih ukrepov** iz tretjega odstavka tega člena. **V primeru ugotovljenega pomanjkljivega ali neustreznega izvajanja varnostnih ukrepov morajo brez nepotrebnega odlašanja sprejeti vse potrebne, ustrezne in sorazmerne popravne ukrepe**.

forvis mazars

ZInfV-1 JO2
Povzetek pomembnih navedb za organizacije

Zakon (ZInfV-1) - Členi

Člen 45 – ocena skladnosti

1. **Odgovorne osebe zagotovijo**, da **bistveni subjekti izvajajo oceno skladnosti sprejetih ukrepov za obvladovanje tveganj kibernetske varnosti** iz tega zakona in da **pomembni subjekti izvajajo oceno skladnosti takšnih ukrepov**.
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 revizija 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 iz tega zakona in na podlagi tega zakona izdanih podzakonskih predpisov ali izvedbenih aktov Evropske komisije. Oceno skladnosti v okviru notranje revizije poleg preizkušenih revizorjev lahko izvajajo tudi notranji revizorji v sodelovanju z veščakom za informacijsko tehnologijo.
3. Pomembni subjekti morajo izvesti oceno skladnosti na zahtevo inšpektorja ali v primeru pojava pomembnega incidenta.
4. Preizkušeni revizor za bistvenega ali pomembnega subjekta pripravi poročilo o izvedeni oceni skladnosti.
5. Bistveni in pomembni subjekti morajo **poročilo** iz prejšnjega odstavka tega člena **posredovati inšpektorju v osmih dneh po njegovem prejemu**.
6. Ne glede na določbe prejšnjega odstavka tega člena, kadar se ugotavljanje skladnosti izvaja na zahtevo inšpektorja, na podlagi drugega ali tretjega tega člena mora subjekt, kjer se je ocena skladnosti opravila, poročilo iz prejšnjega odstavka predloži inšpektorju nemudoma po prejemu.
7. Stroške izvedbe ocene skladnosti nosijo bistveni in pomembni subjekti, če ta zakon ne določa drugače.

forvis mazars

ZInfV-1 JO2
Povzetek pomembnih navedb za organizacije

Zakon (ZInfV-1) - Členi

Člen 46 – samoocena skladnosti

1. Izvajanje **samoocene skladnosti** morajo **pomembni subjekti opraviti najmanj enkrat na dve leti**.
2. Če je iz rezultatov opravljene samoocene skladnosti razvidno, da pomemben subjekt izpolnjuje zahteve, predpisane s tem zakonom, pomembni subjekti sestavijo izjavo o skladnosti, ki vsebuje potrebne elemente samoocenjevanja skladnosti.
3. Pomembni subjekti morajo **izjavo** iz prejšnjega odstavka tega člena **brez odlašanja predložiti inšpektorju, v osmih dneh od njene sestave**.
4. Stroške izvajanja samoocene skladnosti nosijo pomembni subjekti.

Člen 58 – sprejem ukrepov za obvladovanje tveganj

1. Bistveni in pomembni subjekti **sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost** iz 20. in 21 člena tega zakona **v roku dvanajstih mesecev od uveljavitve tega zakona**.
2. Ne glede na prejšnji odstavek **v roku šestih mesecev od uveljavitve tega zakona sprejmejo ukrepe za obvladovanje tveganj za kibernetsko varnost** iz 20. in 21 člena tega zakona tisti bistveni ali pomembni subjekti:
   - **če so bili pred 16. januarjem 2023 določeni** kot izvajalci bistvenih storitev, ponudniki bistvenih storitev ali organi državne uprave po Zakonu o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) ali
   - **operaterji** po Zakonu o elektronskih komunikacijah (Uradni list RS, št. 130/22 in 18/23 – ZDU-1O), ki in so vpisani v uradno evidenco, ki jo vodi Agencija za komunikacijska omrežja in storitve Republike Slovenije.

forvis mazars

NIS 2
Povzetek pomembnih navedb za organizacije

Zakon (ZInfV-1) - Členi

Ostali potencialni zanimivi členi

- Člen 23 - certificiranje
- Člen 26 - postopek priglasitve pomembnih incidentov
- Člen 27 - pristojnost in teritorialnost
- Člen 31 - prostovoljna priglasitev
- Člen 32 - vrednotenje incidenta in ukrepanje
- Člen 41 - splošne določbe (nadzora)
- Člen 42 - nadzor bistvenih subjektov
- Člen 43 - nadzor pomembnih subjektov
- Člen 53 - prekrški bistvenih subjektov
- Člen 54 - prekrški pomembnih subjektov

Povzetek
Ključne informacije

Osebni pogled predavatelja

- Nacionalna zakonodaja je ključna za razumevanje natančnega obsega obveznosti in odgovornosti.
- EU pozornost na vzpostavitve višje ravni kibernetske varnosti in odpornosti narašča.
- Izdelati samooceno stanja (https://www.gov.si/novice/2023-12-21-samoocena-informacijska-varnost/) oz. analizo vrzeli s prihajajočimi zakonodajnimi določili.
- Izbira ustreznega kontrolnega ogrodja (framework).
- Sinergije z obstoječimi in prihajajočimi predpisi.
- Redni pregledi.
- Nujno pravilno pristopiti k skladnosti (izdelava registra informacijskih sredstev - ocena kibernetskih tveganj - analiza poslovnih učinkov (BIA) - neprekinjeno poslovanje in okrevanje po katastrofi).
- Pričeti čim prej.

Kontakt

Forvis Mazars

Verovškova ulica 55A
1000 Ljubljana
Slovenia

info@mazars.si
+386 50 049 500

www.forvismazars.com/si

Tevž Delak

CISA, CDPSE
Senior Manager, IT Assurance & Advisory

040 454 616
tevz.delak@mazars.si

Sledite nam

LinkedIn:

www.linkedin.com/company/Forvis-Mazars-Slovenia
www.linkedin.com/company/ForvisMazarsGroup

X:
www.twitter.com/ForvisMazarsGroup

Facebook:

www.facebook.com/Forvis.Mazars.Slovenija
www.facebook.com/ForvisMazarsGroup

Instagram:

www.instagram.com/Forvis.Mazars.Slovenia
www.instagram.com/ForvisMazarsGroup

Več najdete na **www.forvismazars.com**