Kibernetska varnost NIS2 in osnutek ZInfV-1

Naj nas v ukrepanje ne sili regulativa,
pač pa želja po povečevanju odpornosti!

maj 2024

BDO

Anketa

1. Ali zaposlene redno opozarjate na njihovo obveznost poznavanja in spoštovanja notranjih aktov?
2. Ste zadnje šolanje zaposlenih o kibernetskih tveganjih in odgovornem rokovanji z IKT sredstvi izvedli pred manj kot šestimi meseci?
3. Imate uvedeno dvofaktorsko avtentikacijo na vseh ključnih področjih?
4. Ste uvedli kazalnike / indikatorje učinkovitosti / stanja na področju kibernetske varnosti?
5. Pripravljate celovito poročilo za upravo in organ upravljanja o stanju na področju kibernetske varnosti?
6. Imate uveden proces preverjanja zunanjih pogodbenih izvajalcev?
7. Ali aktivno spremljate aktivnosti v vašem medmrežju in interakcije z zunanjim omrežjem?
8. Ste testirali:
   - „scenarije ukrepanja ob nastopu incidenta“
   - „omejeno poslovanje v razmerah incidenta“
   - „normaliziranje poslovanja s pomočjo varnostnih kopij“
9. Ste v zadnjih šestih mesecih zaznali in obravnavali kibernetski incident?

Razvoj

- 6. julij 2016: Sprejeta je bila direktiva NIS1 (Network and Information Security Directive).
- 9. maj 2018: Rok za prenos direktive NIS1 v nacionalne zakonodaje držav članic EU.
- 16. december 2020: Evropska komisija je predlagala direktivo NIS2.
- 28. november 2022: Sprejeta je bila direktiva NIS2 (Direktiva (EU) 2022/2555).
- 17. oktober 2024: Predvideni rok za prenos direktive NIS2 v nacionalne zakonodaje (Slo: ZInfV-1).
- 18. oktober 2024: Direktiva o varnosti omrežij in informacijskih sistemov 1 se razveljavi s takojšnjim učinkom.
- 17. april 2025: Države članice pripravijo seznam bistvenih in pomembnih subjektov.
- 17. oktober 2027: Komisija vsakih 36 mesecev pregleda delovanje Direktive o varnosti omrežij in informacijskih sistemov (NIS2).

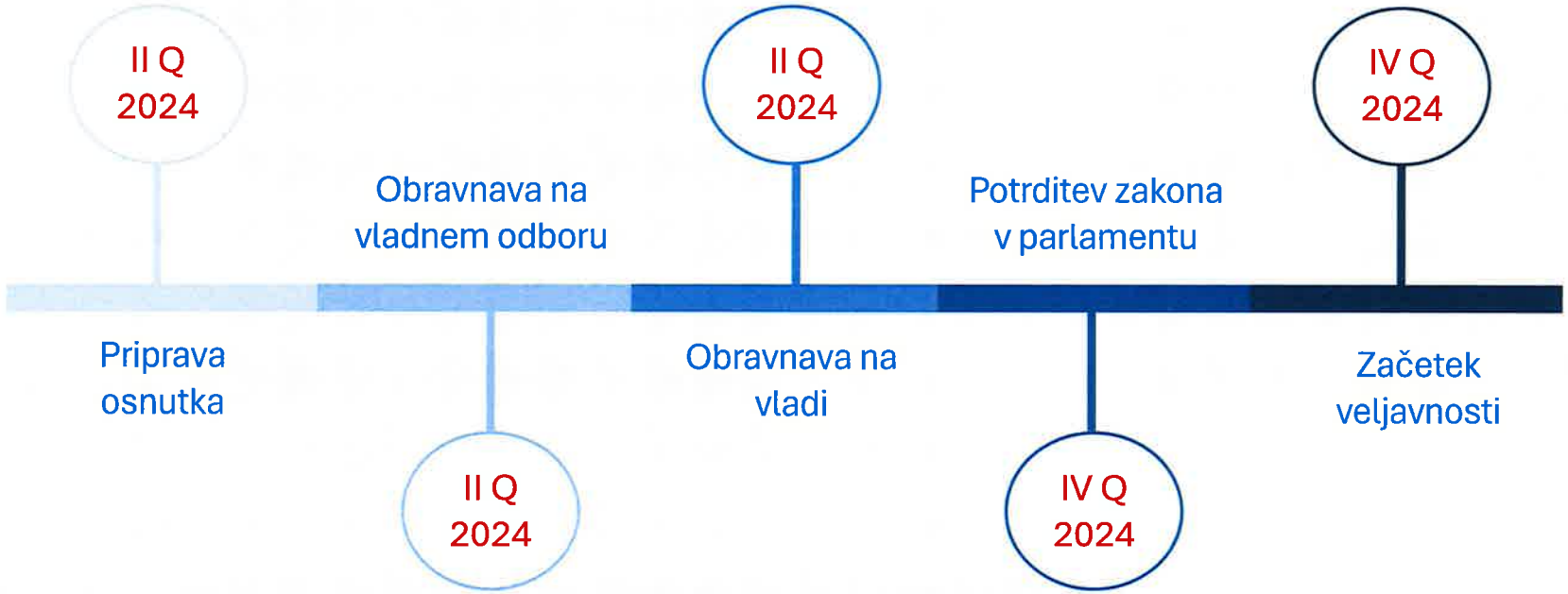
Ključni cilji Direktive NIS2

1. Postaviti merila za ukrepe kibernetske varnosti v kritičnih industrijah, ki so ključne za sodobno družbo (znatna širitev obsega industrij in organizacij v primerjavi z NIS1).

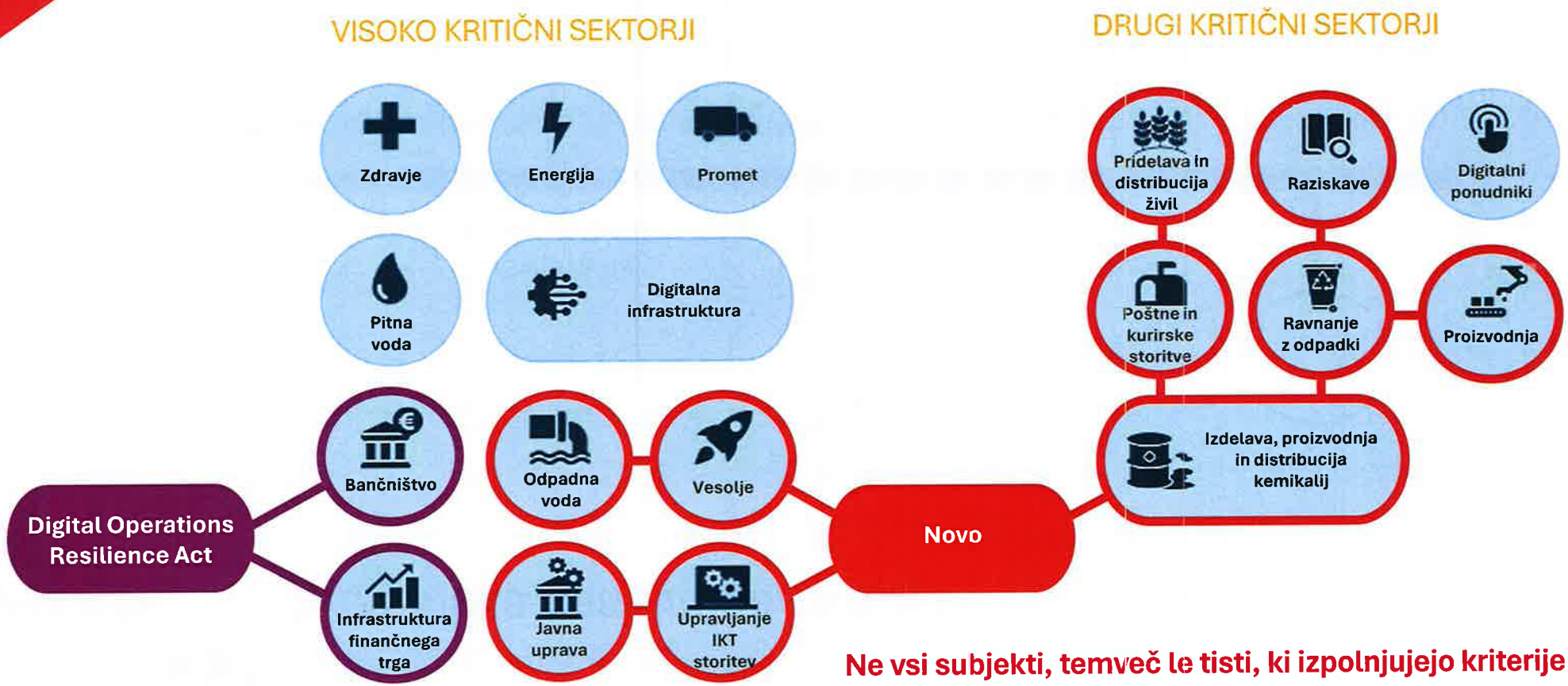
2. Zagotoviti, da se položaj kibernetske varnosti v različnih državah članicah EU znatno izboljša in v največji možni meri poenoti.

3. Okrepiti sodelovanje med različnimi nadzornimi organi na področju kibernetske varnosti v EU.

Slovenska časovnica ZInfV-1



NIS2 in ZInfV-1: sektorji v prilogah I in II



Ne vsi subjekti, temveč le tisti, ki izpolnjujejo kriterije (promet, število zaposlenih, bilančna vsota).

Odgovornost vodstva in organov nadzora

- Potrjuje ukrepe za obvladovanje tveganj kibernetske varnosti v organizaciji.
- Usmerja in nadzoruje vpeljavo ukrepov za obvladovanje tveganj.
- Se redno udeležuje usposabljanj, ter skrbi za zasnovo in izvedbo usposabljanj vseh zaposlenih s ciljem pridobitve zadostnih znanj in spretnosti za prepoznavanje in ocenjevanje tveganj kibernetske varnosti, kot tudi njihovih vplivov na ključne poslovne proces organizacije, posledično pa tudi na proizvode in storitve organizacije.
- Nadzoruje učinkovitost zasnovanih in vpeljanih ukrepov.
- Potrjuje nadgradnje in prilagoditve ukrepov.
- Je lahko odgovorno za zakonsko neskladnost ali kršitve.

ODGOVORNOST ORGANIZACIJE!

- Odgovornost najvišjega vodstva za skladnost in izpolnjevanje zahtev
- Varnostne obveze subjektov
- Dolžnost obveščanja o incidentih

Varnostni ukrepi

Organizacije morajo sprejeti ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za obvladovanje tveganj za varnost omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter za preprečevanje ali zmanjšanje vpliva incidentov na prejemnike storitev in druge storitve.

Ukrepi morajo ob upoštevanju najsodobnejših in po potrebi ustreznih evropskih in mednarodnih standardov ter stroškov izvajanja zagotavljati raven varnosti omrežnih in informacijskih sistemov, ki ustreza obstoječim tveganjem.

ODGOVORNOST ORGANIZACIJE!

- Odgovornost najvišjega vodstva za skladnost in izpolnjevanje zahtev
- Varnostne obveze subjektov
- Dolžnost obveščanja o incidentih

Varnostni ukrepi

ODGOVORNOST ORGANIZACIJE!

- Odgovornost najvišjega vodstva za skladnost in izpolnjevanje zahtev
- Varnostne obveze subjektov
- Dolžnost obveščanja o incidentih

Pri ocenjevanju sorazmernosti varnostnih ukrepov je potrebno smiselno upoštevati:

- stopnjo izpostavljenosti tveganjem,
- velikost subjekta,
- verjetnost pojava incidentov,
- resnost morebitnih incidentov, vključno z njihovim družbenim in gospodarskim vplivom.

Evropska komisija vzpodbuja prednostno uporabo IKT proizvodov, IKT storitev in postopkov IKT, ki so jih razvili bistveni ali pomembni subjekti ali ki so bili kupljeni pri tretjih straneh in so certificirani na podlagi evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi člena 49 Uredbe (EU) 2019/881 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti.

Varnostni ukrepi

Vključujejo **najmanj**:

- politike o analizi tveganja in varnosti informacijskih sistemov;
- obvladovanje incidentov;
- neprekinjeno poslovanje, vključno z upravljanjem varnostnih kopij in vnovično vzpostavitvijo delovanja po nepredvidljivih dogodkih ter za obvladovanje kriz;
- varnost dobavne verige, vključno z vidiki, povezanimi z varnostjo, ki se nanašajo na odnose med posameznim subjektom in njegovimi neposrednimi dobavitelji ali ponudniki storitev;
- varnost pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem ranljivosti;
- politike in postopke za oceno učinkovitosti ukrepov za obvladovanje tveganj za kibernetsko varnost;
- osnovne prakse kibernetske higiene in usposabljanje na področju kibernetske varnosti;
- politike in postopke v zvezi z uporabo kriptografije / šifriranjem;
- varnost človeških virov, politike nadzora dostopa in upravljanje sredstev;
- 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.

ODGOVORNOST ORGANIZACIJE!

- Odgovornost najvišjega vodstva za skladnost in izpolnjevanje zahtev
- Varnostne obveze subjektov
- Dolžnost obveščanja o incidentih

Dnevniški zapisi

Organizacije zagotovijo ohranjanje dnevniških zapisov o delovanju svojih ključnih, krmilnih in nadzornih informacijskih sistemov ali delov omrežja, za obdobje šestih mesecev, lahko pa tudi za daljše obdobje, kadar iz analize obvladovanja tveganj in ocene sprejemljive ravni tveganj izhaja, da bi bilo tveganja možno ustrezno obvladovati z daljšo hrambo dnevniških zapisov.

Dnevniški zapisi o delovanju ključnih, krmilnih in nadzornih informacijskih sistemov ali delov omrežja morajo biti hranjeni na način, ki zagotavlja njihovo avtentičnost, celovitost in razpoložljivost v primeru incidentov.

ODGOVORNOST ORGANIZACIJE!

- Odgovornost najvišjega vodstva za skladnost in izpolnjevanje zahtev
- Varnostne obveze subjektov
- Dolžnost obveščanja o incidentih

Obveznost priglašanja in obveščanja

Pristojni skupini pri CSIRT brez nepotrebnega odlašanja naj organizacije priglasijo vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev.

Pri tem se incident šteje za pomembnega, če:

- je zadevnemu subjektu povzročil ali bi mu lahko povzročil znatne operativne motnje pri opravljanju storitev ali finančne izgube;
- je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

ODGOVORNOST ORGANIZACIJE!

- Odgovornost najvišjega vodstva za skladnost in izpolnjevanje zahtev
- Varnostne obveze subjektov
- Dolžnost obveščanja o incidentih

Primerjava okvirjev - NIST

IDENTIFIKACIJA

- Upravljanje sredstev (ID.AM): Podatki, osebje, naprave, sistemi in objekti, ki organizaciji omogočajo doseganje poslovnih namenov, naj bodo opredeljeni in upravljani v skladu z njihovim relativnim pomenom za organizacijske cilje in strategijo organizacije glede tveganj.
- Poslovno okolje (ID.BE): Informacije se uporabljajo za informiranje o vlogah, odgovornostih in odločitvah glede kibernetske varnosti.
- Upravljanje (ID.GV): Politike, postopki in procesi za upravljanje in spremljanje regulativnih, pravnih, okoljskih in operativnih zahtev organizacije so razumljivi in se uporabljajo pri upravljanju tveganja kibernetske varnosti.
- Ocena tveganja (ID.RA): Organizacija mora razumeti tveganja kibernetske varnosti za delovanje organizacije, ter vplivi na sredstva organizacije in posameznike.
- Strategija upravljanja tveganj (ID.RM): Prednostne naloge, omejitve, tolerance tveganja in predpostavke organizacije so določene in se uporabljajo za podporo odločitvam o operativnem tveganju.
- Upravljanje tveganj v dobavni verigi (ID.SC): Organizacija je vzpostavila in izvaja postopke za prepoznavanje, ocenjevanje in obvladovanje tveganj dobavne verige.

Primerjava okvirjev - NIST

ŠČITENJE

- Upravljanje identitete, avtentikacija in nadzor dostopa (PR.AC): Dostop do fizičnih in logičnih sredstev ter pripadajočih objektov je omejen na pooblaščene uporabnike, procese in naprave, ter se upravlja v skladu z ocenjenim tveganjem nepooblaščenega dostopa do pooblaščenih dejavnosti in transakcij.
- Ozaveščanje in usposabljanje (PR.AT): Osebje in partnerji organizacije so seznanjeni s kibernetsko varnostjo in so usposobljeni za opravljanje svojih nalog, ki so povezane s kibernetsko varnostjo, v skladu s politikami, postopki in pravilniki.
- Varnost podatkov (PR.DS): Informacije in zapisi (podatki) se upravljajo v skladu s strategijo organizacije za obvladovanje tveganj, s cilji zagotavljanja zaupnosti, celovitosti in razpoložljivosti informacij.
- Procesi in postopki za zaščito informacij (PR.IP): Varnostne politike (ki obravnavajo namen, obseg, vloge, odgovornosti, zavezanost vodstva in usklajevanje med organizacijskimi enotami), procesi in postopki se vzdržujejo in uporabljajo za upravljanje zaščite informacijskih sistemov in sredstev.
- Vzdrževanje (PR.MA): Vzdrževanje in popravila komponent nadzornega in informacijskega sistema se izvajajo v skladu s politikami in pravilniki.
- Zaščitna tehnologija (PR.PT): Tehnične varnostne rešitve se upravljajo za zagotavljanje varnosti in odpornosti sistemov in sredstev v skladu s povezanimi politikami, postopki in pravilniki.

Primerjava okvirjev - NIST

PREPOZNAVANJE

- **Anomalije in dogodki (DE.AE):** organizacija si prizadeva za odkrivanje nepravilnosti, njihov potencialni vpliv je prepoznan.
- **Stalno spremljanje varnosti (DE.CM):** Organizacija spremlja delovanje in upravljanje informacijskega sistema ter angažiranih sredstev. Cilj je zaznavanje kibernetskih incidentov ter preverjanje učinkovitosti zaščitnih ukrepov.
- **Procesi odkrivanja (DE.DP):** Procesi in postopki odkrivanja se vzdržujejo in preizkušajo, da se zagotovi zavedanje o neželenih dogodkih.

Primerjava okvirjev - NIST

ODGOVOR

- Načrtovanje odziva (RS.RP): Izvajajo in vzdržujejo se procesi in postopki odzivanja, da se zagotovi odziv na odkrite kibernetske incidente.
- Komunikacije (RS.CO): Odzivne dejavnosti se usklajujejo z notranjimi in zunanjimi zainteresiranimi deležniki (npr. zunanja podpora organov pregona).
- Analiza (RS.AN): Organizacija izvaja analize učinkovitosti odzivov v primeru incidentov in podporo dejavnostim obnove.
- Blažitev (RS.MI): Organizacija ima načrtovane dejavnosti za preprečevanje širjenja neželenega dogodka, ublažitev njegovih učinkov normalizacijo poslovanja.
- Izboljšave (RS.IM): Organizacija izboljšuje odzivne aktivnosti tudi s pomočjo upoštevanja izkušenj, pridobljenih pri sedanjih in prejšnjih aktivnostih odkrivanja/ukrepanja v primerih incidentov.

Primerjava okvirjev - NIST

OKREVANJE

- Načrtovanje okrevanja (RC.RP): Načrtovani in vzdrževani so procesi in postopki obnove, da se zagotovi ponovna vzpostavitev sistemov ali sredstev, ki so jih prizadeli kibernetski incidenti.
- Komunikacije (RC.CO): Koordinacija obnovitvenih dejavnosti z notranjimi in zunanjimi deležniki (npr. koordinacijskimi centri, ponudniki internetnih storitev, lastniki napadenih sistemov, žrtvami, drugimi skupinami CSIRT in prodajalci).

Primerjava okvirjev – ISO 27001

- Varnostne politike;
- Organizacija informacijske varnosti;
- Varnost na področju človeških resursov;
- Upravljanje sredstev;
- Nadzor nad sredstvi;
- Kriptografija;
- Fizična varnost in varnost v širšem okolju;
- Varnost dejavnosti;
- Varnost komunikacij;
- Pridobivanje, razvoj in vzdrževanje sistemov;
- Odnosi z dobavitelji;
- Upravljanje incidentov;
- Vidik varnosti informacij v okviru upravljanja neprekinjenega poslovanja;
- Skladnost.

DORA

Povezanost / odvisnost finančnih inštitucij od tretjih oseb. Prioriteta je ohranitev nadzora nad odnosi.

Izmenjava informacij med bankami. Je ključnega pomena in se spodbuja. Izmenjava informacij na evropski ravni bi lahko bila koristna, vendar bi morale finančne institucije uravnotežiti prizadevanja s koristmi.

Priprava na skladnost z uredbo, opredelitev vrzeli, analiza procesov, zagotovitev zadostnih proračunov, oblikovanje in hramba dokazil, ki dokazujejo skladnost v daljših obdobjih.

Zbiranje relevantnih informacij o incidentih na področju IKT v standardiziranih formatih. Proces poročanja regulatorju naj bo izveden v predpisanih rokih.

Obnova je bila običajno osredotočena na operativne incidente / motnje. Pri odpornosti je potrebno dodati kibernetske in druge grožnje, povezane z IKT.

Kaj kažejo naše izkušnje?

1. Notranji akti so napisani, pomanjkljivo je njihovo ažuriranje, zaposleni jih slabo poznajo, jezik in posamezni uporabljeni izrazi so zaposlenim v delih nerazumljivi.
2. Organizacijski in tehnični ukrepi so večinoma določeni. Ustroj notranjih kontrol ni redno in sistematično preverjan in izboljševan, njihovo delovanje pogosto ni preverjano. Preveč pogosto je zanašanje na tehnične ukrepe.
3. Uvajalni paketi za nove zaposlene nezadostno poudarjajo odgovornost in pomembnost vsakega posameznika za krepitev kibernetske odpornosti.
4. Ozaveščanja in šolanja zaposlenih so redko izvajana in preverjana z IT orodji, povezava z nagrajevanjem ne obstaja.
5. Dvofaktorska avtentikacija je prisotna. Gesla so pogosto enostavna, zaposleni jih uporabljajo za več aplikacij, tudi za zasebne namene.
6. Pooblastila strokovnjakov pogodbenih partnerjev omogočajo operativne intervencije v produkcijskih okoljih brez dodatnih predhodnih odobritev ali kasnejših posebnih pojasnil.
7. Dnevniški zapisi o intervencijah v produkcijskih okoljih niso redno in ustrezno analizirani, popravljalni ukrepi so le redko sprejeti.
8. Spremljanje zapisov predhodnih odobritev in nadzor posegov (tudi nepooblaščenih poskusov) ni redno in sistematično.

Kaj kažejo naše izkušnje?
(nadaljevanje)

9. Upravljanje s spremembami pogosto odstopa od standardov in dobrih praks.
10. Kazalniki oz. indikatorji učinkovitosti / stanja na področju kibernetske varnosti niso vpeljani.
11. Celovita poročila za upravo in organe upravljanja o stanju na področju kibernetske varnosti so redka; večinoma so kibernetska tveganja le del širših poročil, v katerih prevladujejo druga tveganja.
12. Procesi preverjanj zunanjih pogodbenih izvajalcev niso standardizirani, pogodbena določila za revizijske vpoglede niso izkoriščena, pogodbeni izvajalci le redko dostavljajo poročila SOC 1, 2 ali 3 (v skladu z MSZ).
13. Velike organizacije se poslužujejo storitev izločenih varnostnih operativnih centrov, velika večina se jih zanaša na občasna in statična testiranja.
14. Scenariji ukrepanja ob nastopu različnih incidentov so določeni v politikah in pravilnikih, niso pa realno testirani.
15. Časi v katerih bi moral biti razpoložljiv določen obseg podatkov s katerim bi po incidentu lahko obnovili poslovanje (s ciljem minimiziranja vplivov in škod za stranke in druge deležnike) pogosto niso določeni.
16. Omejeno poslovanje v razmerah kibernetskega incidenta ni testirano.
17. Normaliziranje in obnavljanje poslovanja s pomočjo varnostnih kopij praktično ni testirano.
18. Incidenti se dogajajo pogosto, stranke o njih niso obveščene, razen če to nalaga zakon ali druga regulativa.

Česa se v organizacijah premalo zavedamo?

1. Zakonske zahteve so minimalni standard.
2. Ton z vrha je daje ključno sporočilo vsem zaposlenim.
3. Pravilniki, ki so jih napisale odlične odvetniške pisarne, vodstva in zaposleni pa ne poznajo njihove vsebine in njihovega vpliva na procese in postopke, so dokumenti z malo vrednosti, v praksi pa ne zagotavljajo kibernetske varnosti.
4. Ozaveščanje, šolanje in odgovornost zaposlenih so najmočnejši elementi kibernetske varnosti!
5. Standard oz. skladnost z njim nas ne varuje; podaja le informacijo o našem delovanju, če ga dosledno spoštujejo vsi v organizaciji.
6. Izločene storitve na področju kibernetske varnosti, ki jih izvaja „one man band“ organizacija po načelu „črne škatle“, pomenijo povečanje in ne zmanjšanje tveganj!
7. Izločanje funkcij na pogodbene izvajalce pomeni delegiranje aktivnosti, ne pa prenos odgovornosti.
8. Odgovornost za posledice kibernetskih incidentov primerih nosi poslovodstvo!
9. Samoocenjevanje ali objektivne zunanje presoje nam lahko pomagajo pri razumevanju našega stanja in potrebnih ukrepov.

Česa se v organizacijah premalo zavedamo?
(nadaljevanje)

9. Občasno testiranje odpornosti ni zadostno, bolj učinkovito je kontinuirano preverjanje.
10. Mnenja dobaviteljev parcialnih elementov s ciljem uvajanja predvsem tehničnih ukrepov niso nujno objektivna.
11. Varnostne kopije s katerimi nismo nikoli poskusili obnoviti poslovanja po „simuliranem incidentu“ so vprašljive vrednosti.
12. Kibernetska tveganja postajajo zaradi stopnje digitalizacije poslovanja in odvisnosti poslovnih modelov organizacij ključna.
13. Umetna inteligenca bo imela negativen vpliv na kibernetske grožnje.
14. Potencial umetne inteligence za povečevanje kibernetske odpornosti obstaja, a zaradi omejitev organizacij ostaja še neizkoriščen.
15. Ni vprašanje „če“, vprašanje je „kdaj“ in s kakšnimi posledicami bomo preživeli incident; zato je ključna priprava in uigranost za primere incidentov.

Povzetek - ocena možnih vplivov ZInfV-1

Vidik	Izzivi skladnosti	Priložnosti skladnosti
zahteve	okrepljeni varnostni ukrepi, strogo poročanje o incidentih in dobavna veriga	močnejša kibernetska varnost in zmanjšano tveganje zlorab podatkov
investicije v sredstva	potreba po naložbah v tehnologijo in strokovno znanje, zlasti za manjše subjekte	spodbuja operativno učinkovitost in inovativnost
revizije in ocene	redne revizije ali ad hoc revizije, ki jih izvajajo neodvisne organizacije	identificiranje področij za izboljšave, izboljšanje zanesljivosti in varnosti
vplivi na subjekte	morebitna obremenitev virov in njihovo prilagajanje novim standardom	povečan ugled, zaupanje in konkurenčna prednost
industrija kibernetske varnosti	prilagajanje razvijajočim se standardom skladnosti in njihovo vključevanje v ponudbo storitev	odpira nove trge za rešitve in storitve skladnosti

Kaj priporočamo?

- opredelitev in izvajanje okvirja za analizo tveganj in varnosti informacijskih sistemov;
- opredelitev in izvajanje postopkov za oceno učinkovitosti ukrepov za obvladovanje tveganj kibernetske varnosti;
- določitev ukrepov za obvladovanje incidentov in aktivnosti v primeru njihovega nastopa;
- definiranje neprekinjenega poslovanja, (upravljanje varnostnih kopij in vnovična vzpostavitev delovanja po neželenih dogodkih in za omejeno poslovanje v kriznih razmerah);
- postavitev in spoštovanje varnostnih standardov dobavne verige;
- opredelitev in spoštovanje pravil varnosti pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov;
- vzpostavitev dobrih praks kibernetske higiene in usposabljanj zaposlenih na področju kibernetske varnosti;
- opredelitev in spoštovanje postopkov v zvezi z uporabo kriptografije;
- določitev in izvajanje varnostnih pravil delovanja zaposlenih (nadzor dostopov in upravljanje sredstev);
- uporaba večfaktorske avtentikacije.

Hvala za pozornost!

info@bdo.si
andrej.baricic@bdo.si