Mojca Progar Vodja marketinga, Kolektor Sisteh

ZInfV 1 v praksi: od skladnosti do odpornosti v industriji in kritični infrastrukturi

Nov Zakon o informacijski varnosti (ZInfV 1) v slovenski prostor prinaša bistveno širši in zahtevnejši okvir kibernetske varnosti. Ne gre več le za nalogo IT oddelkov, temveč za odgovornost vodstva, upravljanje tveganj, neprekinjeno poslovanje, obvladovanje incidentov in varnost dobavne verige.
Za industrijska podjetja in upravljavce kritične infrastrukture to pomeni konkreten premik: varnostni ukrepi morajo biti dokumentirani, uvedeni, preverljivi in podvrženi rednim izboljšavam. Ker se s takšnimi projekti v Kolektor Sistehu srečujemo vsak dan, smo za pogled regulatorja vprašali mag. **Melito Šinkovec**, vodjo Sektorja za informacijsko in kibernetsko varnost v Uradu vlade Republike Slovenije za informacijsko varnost (URSIV).

Zakaj ta zakon ni “samo še ena regulativa”, ampak realna sprememba v načinu upravljanja kibernetske varnosti?
Zagotavljanje informacijske in kibernetske varnosti bi moralo biti v organizaciji, ki deluje in nudi storitve v digitaliziranem svetu, ena izmed prioritet njenega delovanja, saj zagotavljanje tovrstne varnosti vpliva na sam obstoj in delovanje organizacije. Kibernetske grožnje in incidenti so postali naša realnost. O njih že skoraj vsak dan beremo v dnevnih novicah. Zavedati se je treba, da lahko kibernetski incident ohromi dejavnost organizacije ali pa jo celo pahne v zaprtje ali stečaj. Gre za pomembno grožnjo, ki jo morajo organizacije upoštevati.

Tudi zato je ZInfV-1 v ospredje postavil pomembno vlogo najvišjega vodstva organizacije. Zagotavljanje informacijske in kibernetske varnosti ni več le tehnični ali operativni izziv oziroma naloga IT služb, temveč gre za proces, v katerega mora biti vpeto najvišje vodstvo organizacije. Slednje odloča in določa, katero področje znotraj organizacije bo deležno več ali manj finančnih, kadrovskih in drugih virov, in s tem daje poudarek in podlago za zagotavljanje tudi kibernetske varnosti. Bistvena novost novega zakona, ki ureja področje informacijske in kibernetske varnosti, je tudi v njegovem obsegu učinkovanja. Zajema namreč precej večje število zavezancev, kot jih je stari zakon. Število zavezancev se je povečalo z okoli 200 na 700, pri čemer seznam še ni zaključen. Pričakujemo, da bo status zavezancev potrdilo blizu 1000 subjektov.

Na uradu pa se trudimo, da omenjeni zakon ne postane le še ena regulativna ovira in obveznost, pač pa želimo zavezancem tudi olajšati delo in jim nuditi podporo in pomoč.

Kakšno podporo lahko zavezanci pri izpolnjevanju obveznosti po ZInfV-1 dobijo od URSIV?
Že v lanskem letu je bil pripravljen priročnik za kibernetsko varnost, ki je bil nato posodobljen zaradi sprejetja novega ZInfV-1. Namen priročnika je zavezancem podati osnovne informacije in napotke za pripravo varnostne dokumentacije. Pripravljen je bil tudi spletni obrazec, prek katerega organizacije preverijo, če so zavezanci po ZInfV-1. V primeru pozitivnega odgovora lahko prek obrazca tudi oddajo skladno z zakonom zahtevane podatke. Z namenom dodatnega pojasnjevanja vsebin novega zakona so bila pripravljena tudi pojasnila k ZInfV-1, kjer lahko organizacije pridobijo dodatne informacije glede določanja zavezancev, samoregistracije, rokov za izpolnjevanje zahtev, usposabljanja in drugih vsebin iz zakona.

Urad je decembra lani pričel z izvajanjem brezplačnih usposabljanj odgovornih oseb na področju obvladovanja tveganj informacijske in kibernetske varnosti, kjer so vodstvu predstavljene obveznosti zakona in druge vsebine, pomembne za razumevanje zagotavljanja kibernetske varnosti v organizaciji.

Na spletni strani je na voljo tudi vprašalnik za samooceno zagotavljanja kibernetske varnosti v Excel obliki, ki temelji na CIS kontrolah. Datoteko lahko naložite lokalno, jo izpolnite in pridobite oceno zagotavljanja informacijske in kibernetske varnosti v organizaciji. Ocenjuje se 19 segmentov, poleg skupne ocene varnosti pa pridobite tudi oceno zrelosti varnostnih postopkov in politik. Poleg tega je na voljo vzorčna dokumentacija, ki je subjektom v pomoč pri pripravi varnostne dokumentacije.

Zavedati se je treba, da lahko kibernetski incident ohromi dejavnost organizacije ali pa jo celo pahne v zaprtje ali stečaj. Gre za pomembno grožnjo, ki jo morajo organizacije upoštevati.

Od januarja do marca 2026 so potekale tudi delavnice na temo treh vsebin, in sicer skladnost z ZInfV-1, v okviru katere se je prikazalo praktične korake priprave varnostne dokumentacije. Druga delavnica je bila na temo storitev varnostno-operativnega centra, tretja pa glede odzivanja na kibernetske incidente. Posnetki delavnic in gradiva so na voljo na spletu (Gradiva in posnetki delavnic o izpolnjevanju zakonskih obveznosti na področju kibernetske varnosti | GOV.SI). Urad pripravlja tudi digitalno platformo za priglasitev incidentov in obveščanje. Načrtuje se tudi okrepitev aktivnosti za dvig odpornosti vključno s sistemom finančnih spodbud. Za slednje je v postopku priprave področni zakon, ki bo vplival na mehkejši prehod v višji nivo kibernetske varnosti.

Pri tem želimo opozoriti tudi na preventivne aktivnosti na področju kibernetske varnosti. V skladu z ZInfV-1 morajo vodstva zagotoviti letna izobraževanja zaposlenih. Z namenom blaženja finančnih posledic ter doseganja čim višje odpornosti organizacije predlagamo, da se za dvig osveščenosti zaposleni poslužujejo

brezplačnih tečajev, ki jih nudi skupina CSIRT SI-CERT pri Arnesu. URSIV prek svojega proračuna financira delovanje skupin CSIRT.

Kdo je zavezanec in kje se danes dela največ napak?
Največ težav pri samoregistraciji subjektov smo zaznali pri identifikaciji storitev, ki jih opravlja organizacija, in tistih, ki jih ZInfV-1 določa v prilogah 1 in 2 in posledično pomenijo, da subjekt izpolnjuje prvega od treh kriterijev za zavezanca po ZInfV-1. Veliko vprašanj je bilo tudi glede pomena velikosti organizacije, kar predstavlja drugi dve merili, da subjekt postane zavezanec.

Večina omenjenih težav je bila naslovljena lansko leto, ko je potekel prvi rok za samoregistracijo. Prejeli smo precej vprašanj na to temo in tudi uspeli na vse podati odgovor. V primeru, da smo zaznali napačne samoregistracije, smo subjekt na to opozorili. Skladno z zakonom pa ni predvidenega postopka ugotavljanja, ali je subjekt zavezanec ali ne. Omenjen postopek izvedemo le pri določenih izjemah, kot jih predvideva zakon.

Za namen pojasnjevanja smo na uradu pripravili Pojasnila k ZInfV-1, ki so lahko organizacijam v pomoč pri prepoznavanju, ali so zavezanci in tudi glede drugih zahtev iz zakona.

Kaj ZInfV-1 pomeni za vodstva podjetij?
1. Preveriti status zavezanca in obveznost samoregistracije.
2. Imenovati odgovorne osebe in zagotoviti usposabljanje.
3. Izvesti oceno tveganj in določiti prioritetne ukrepe.
4. Urediti dokumentiransistem upravljanja varovanja informacij in neprekinjenega poslovanja.
5. V pogodbe z dobavitelji vključiti minimalne varnostne zahteve.
6. Vzpostaviti postopke za zaznavanje, obravnavo in prijavo incidentov.

Kako stroga je časovnica za vzpostavitev skladnosti in kdaj lahko zavezanci pričakujejo prvi resen nadzor inšpekcije ter sankcije za neskladnost?
Časovnica za skladnost je kar stroga. Zavezanci, ki so ob uveljavitvi ZInfV-1 izpolnjevali merila iz 6. in 7. člena ZInfV-1, so morali opraviti prvo registracijo po mehanizmu za samoregistracijo v šestih mesecih od uveljavitve zakona, to je bilo do 19. decembra 2025. Nadalje morajo ti zavezanci, ki se delijo na bistvene in pomembne, sprejeti ukrepe za obvladovanje tveganj za informacijsko in kibernetsko varnost iz 21. in 22. člena ZInfV-1 v roku osemnajstih mesecev, in sicer do 19. decembra 2026. Ob tem so določene izjeme, ki se nanašajo na zavezance po starem zakonu o informacijski varnosti, in sicer morajo nekdanji izvajalci bistvenih storitev (IBS), nekdanji organi državne uprave (ODU) in operaterji po ZEKom-2 skladnost glede omenjenih ukrepov doseči v roku enega leta od uveljavitve ZInfV-1, in sicer do 19. junija 2026. Prvi nadzori skladnosti z ZInfV-1 se bodo pričeli izvajati v januarju 2027.

Treba se je zavedati, da je vzpostavljanje informacijske in kibernetske varnosti proces, ki se dejansko nikoli ne konča, zato je vedno čas in priložnost za napredek in izboljšave.

Če gledamo z vidika uprav, kam bi morala podjetja najprej vlagati, da bi se približala skladnosti z ZInfV-1?
Podjetja bi morala dati poudarek na kadrovske vire v najširšem smislu, torej je treba identificirati ustrezne kadrovske vire, jih ustrezno usposobiti in zagotoviti kontinuirano ohranjanje in nadgrajevanje znanja. Ustrezno usposobljen kader bo znal pripraviti zahtevano varnostno dokumentacijo in izbrati primerne tehnološke rešitve, ki bodo zagotavljale ustrezen nivo kibernetske varnosti in obvladovanje tveganj.

Treba se je zavedati, da je vzpostavljanje informacijske in kibernetske varnosti proces, ki se dejansko nikoli ne konča, zato je vedno čas in priložnost za napredek in izboljšave.

Kaj naj zavezanci, ki želijo slediti zahtevam ZInfV 1, naredijo najprej?
Pristop organizacije k izpolnjevanju obveznosti po ZInfV-1 je seveda odvisen od njene dosedanje vpetosti v obveznosti po ZInfV-1 oziroma od sledenja dobrim praksam zagotavljanja informacijske varnosti v skladu s standardi iz družine ISO/IEC 27000. Če se organizacija prvič srečuje z obveznostmi, je treba pričeti na začetku. Ta začetek pa so kadrovski viri. Najprej je treba identificirati osebo, morda ekipo, ki bo pričela z delom na tem področju. Primeren korak je lahko ugotavljanje vrzeli, če je organizacija že bila v stiku z zagotavljanjem informacijske varnosti. Predvsem pa bi izpostavila pripravo in izvedbo celovitega programa usposabljanj za zagotavljanje informacijske in kibernetske varnosti za vse kategorije in vloge zaposlenih (CISO, skrbnik informacijskih sistemov, vodstvo, računovodstvo, kadroviki itd.), priprava realistične ocene informacijskih tveganj, priprava realnih in primernih ukrepov in njihova implementacija glede na ugotovljena tveganja ter zagotavljanje ustreznih postopkov za vpeljavo sprememb (ang. change management).

Glede omenjenih korakov si lahko subjekti pomagajo s pripomočki, ki sem jih že omenila, torej z vprašalnikom za samooceno skladnosti v Excel obliki, vzorčno dokumentacijo, gradivom delavnic, priročnikom kibernetske varnosti.

Kaj se bo z uveljavitvijo ZInfV 1 po vašem mnenju moralo spremeniti v odnosih med zavezanci in njihovimi dobavitelji tehnologije in storitev?
ZInfV-1 na področju varnosti dobavnih verig jasno opredeljuje odnose oziroma zahteve med zavezanci in njihovimi dobavitelji. Omenjeno je opredeljeno v 10. točki 22. člena med ukrepi za obvladovanje tveganj povezano še s četrtim odstavkom istega člena. Pomembno je vedeti, da je organizacija, ki sicer ni zavezanec po ZInfV-1, lahko soočena z zahtevami iz zakona, če je dobavitelj zavezancu po ZInfV-1. Te zahteve se dejansko prenašajo naprej po celotni verigi, zato je pomembno, da se s tem seznanijo tako dobavitelji kot tudi kupci, tudi če sami niso neposredni zavezanci po zakonu. Zavezanec v razmerju do dobavitelja določi ustrezne minimalne zahteve, povezane z informacijsko in kibernetsko varnostjo, ki pa morajo biti opredeljene v pogodbi ali drugem pisnem dogovoru med njima. Dolžnost zavezanca je tudi, da preverja izvajanje tovrstnih zahtev. Pregled dosedanjih incidentov kaže, da pri zelo veliko zabeleženih kibernetskih incidentih vzrok izvira pri dobavitelju. Primer: zlonamerni akter ukrade poverilnice dobavitelja in z njimi vstopi v informacijski sistem zavezanca. Kaj bi v tem primeru moral narediti zavezanec, da bi poskusil preprečiti incident? Dobavitelju predpiše ukrep uporabe večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije za tiste informacijske sisteme, prek katerih dobavitelj vstopa v okolje zavezanca, in izvedbo omenjenega ukrepa tudi preverja.

ZInfV-1 na področju varnosti dobavnih verig jasno opredeljuje odnose oziroma zahteve med zavezanci in njihovimi dobavitelji.

19. 6. 2025	Uveljavitev ZInfV-1
19. 12. 2025	Prva registracija zavezancev po mehanizmu za samoregistracijo
19. 6. 2026	Skladnost z ukrepi za obvladovanje tveganj za informacijsko in kibernetsko varnost (21. in 22. člen) za izjeme – IBS, ODU in operaterji po ZEKom-2
19. 12. 2026	Sprejetje ukrepov za obvladovanje tveganj za informacijsko in kibernetsko varnost (21. in 22. člen ZInfV-1) za ostale zavezance
Januar 2027	Začetek prvih nadzorov skladnosti z ZInfV-1

Katere vrste kibernetskih groženj danes najbolj skrbijo državo, ko govorimo o kritični infrastrukturi in industriji, in kako se to odraža v zahtevah ZInfV-1?

Med najpogostejše grožnje trenutno uvrščamo spletno ribarjenje in socialni inženiring, prek katerega se poskuša pridobiti poverilnice in druge osebne podatke ali pa namestiti zlonamerno programsko opremo. V teh primerih so velikokrat tarča manj varni dobavitelji. Pogosto se izkorišča ranljivosti v programskih rešitvah. Predvsem so izpostavljeni tudi stari industrijski operativni sistemi, ki imajo vrsto ranljivosti, saj se jih običajno ne posodablja, ker bi ta korak lahko povzročil prekinitev delovanja sistema. V teh primerih je treba poskrbeti za drugačno vrsto zaščite. Zelo pogosta grožnja so tudi porazdeljeni napadi onemogočanja storitev oziroma t. i. DDoS napadi, ki onemogočijo delovanje spletne strani, kar predstavlja še posebej veliko grožnjo, če spletna stran ponuja storitev. Vse omenjene grožnje so naslovljene prek ukrepov za obvladovanje tveganj informacijske varnosti v 22. členu ZInfV-1, ki v 17. točkah zajamejo vse najpomembnejše ukrepe.

Med najpogostejše grožnje uvrščamo spletno ribarjenje in socialni inženiring, prek katerega se poskuša pridobiti poverilnice in druge osebne podatke ali namestiti zlonamerno programsko opremo.

Z izobraževanjem in usposabljanjem zaposlenih se naslavlja skrb pred spletnim ribarjenjem. Ni sicer dobro, da je omenjen ukrep tudi edini, saj je klik s strani ene osebe dovolj za okužbo informacijskega sistema, zato je dobro imeti tudi tehnično rešitev, ki bo reševala poskuse spletnega ribarjenja. Ranljivost programske opreme se na primer naslavlja z upoštevanjem varnostnih mehanizmov pri pridobivanju, razvoju in vzdrževanju programske opreme. Z uporabo večfaktorske avtentikacije in tehnične rešitve segmentacije omrežja se poskušamo ubraniti oziroma zmanjšati učinek nameščene zlonamerne programske opreme z zaklepanjem ali izsiljevanjem. Pri tovrstnem incidentu lahko izgubljene podatke hitreje povrnemo z ustreznim izvajanjem in upravljanjem varnostnih kopij podatkov.

Začetni finančni vložki v kibernetsko varnost se bodo z izpolnjevanjem določb ZInfV-1 dolgoročno prelili v prihranke.

Katere konkretne smernice in priporočen minimalni nabor ukrepov pripravljate na URSIV za zavezance v teh sektorjih?

Urad vlade RS za informacijsko varnost je, kot že predstavljeno, pripravil kar nekaj pripomočkov za zavezance in tudi druge organizacije, ki bi želele biti skladne z ZInfV-1. Pripravljajo pa se še priporočila za obvladovanje tveganj dobavne verige, ki jih lahko pričakujemo v kratkem. Vse omenjeno je dosegljivo na spletni strani urada: O Uradu vlade za informacijsko varnost | GOV.SI.

Ali se strinjate z oceno, da lahko podjetja, ki ZInfV 1 obravnavajo strateško, to izkoristijo kot konkurenčno prednost?

Absolutno se lahko strinjam, da lahko podjetja skladnost z ZInfV-1 oziroma zagotavljanje informacijske in kibernetske varnosti izkoristijo kot konkurenčno prednost. Kibernetski incidenti ovirajo gospodarske dejavnosti, ustvarjajo finančno izgubo, slabijo zaupanje uporabnikov ter povzročajo veliko škodo gospodarstvu in družbi. Zato na uradu ocenjujemo, da bo skladnost z zakonom izboljšala kibernetsko varnost, odpornost in konkurenčnost organizacije, spodbudila področje inovacij, tehnološkega razvoja in razvoja sektorja kibernetske varnosti. Skupna evropska pravila bodo olajšala poslovanje podjetij, ki so izvozno naravnana. Zmanjšale se bodo gospodarske izgube in se kazale v manj številčnih izpadih poslovanja. Pri tem pa seveda ne smemo pozabiti na škodo, ki nastane zaradi izgube ugleda. Začetni finančni vložki v kibernetsko varnost se bodo z izpolnjevanjem določb ZInfV-1 dolgoročno prelili v prihranke.

Ocenjujemo, da bo skladnost z zakonom izboljšala kibernetsko varnost, odpornost in konkurenčnost organizacije, spodbudila področje inovacij, tehnološkega razvoja in razvoja sektorja kibernetske varnosti.