Združenje za informatiko in telekomunikacije
Dimičeva 13 ■ 1504 Ljubljana ■ T: (01) 58 98 102 ■ F: (01) 58 98 100, (01) 58 98 200 ■ zit@gzs.si ■ www.gzs.si/zit

Agencija za komunikacijska omrežja in storitve RS
g. Marko Mišmaš, direktor
Stegne 7
1000 Ljubljana

Datum: 20. 5. 2024

Zadeva: **Informacijski sistem, namenjen zajemu podatkov obvestil in poročil operaterjev o dogodkih**

Spoštovani g. direktor,

V Sekciji operaterjev elektronskih komunikacij pri Združenju za informatiko in telekomunikacije, Gospodarska zbornica Slovenije (v nadaljevanju: SOEK) smo preučili informacijski sistem poročil operaterjev o dogodkih (Okvara/napaka (208. člen ZEKom-2), Napovedana dela (208. člen ZEKom-2), Varnostni incident (118. in 119. člen ZEKom-2) in Kršitev varnosti osebnih podatkov (227. člen ZEKom-2)). Preko informacijskega sistema bo operaterjem omogočeno poročanje ne več ročno preko obeh obrazcev, pač pa preko informacijskega sistema.

V zvezi z uvedbo sistema sta bili izvedeni 2 delavnici in sicer dne 13. 2. 2024 in dne 16. 4. 2024. Testni informacijski sistem je bil operaterjem dan na voljo za testiranje dne 17. 4. 2024. Sistem naj bi pričel delovati dne 1. 6. 2024.

Operaterji, člani SOEK uvodoma pozdravljamo vpeljavo informatiziranega načina za poročanje, ki ga pričakujemo že vrsto let, a opozarjamo na naslednje okoliščine, **zaradi katerih menimo, da je vpeljava informatiziranega sistema zelo preuranjena in bi bilo vpeljavo treba zadržati oz. informatiziran sistem vpeljati, ko bodo zagotovljeni vsi pogoji za njegovo vpeljavo**, **kar pa bi bilo lahko najprej 1. 1. 2025** – po točkah kot sledi:

1) Bodoči Zakon o informacijski varnosti (ZInfV)-poročanje o varnostnih incidentih.
2) (mnogo) Večja količina podatkov pri najbolj poročani kategoriji (208. člen ZEKom-2), ki se poročajo po novem (poročanje ni primerno strukturirano ter optimiziramo; poročanje je izjemno zamudno).
3) Rok za prilagoditev ter uporabo sistema je absolutno prekratek.
4) Način prijave

Ad1: Bodoči Zakon o informacijski varnosti (ZInfV)

Ena od kategorij o katerih smo operaterji zakonsko dolžni poročati je »Varnostni incidenti«, ki z novim Zakonom o informacijski varnosti (ki je sicer še v fazi priprave), prehaja iz AKOS na Urad Vlade RS za informacijsko varnost (v nadaljevanju: URSIV). Kot izhaja iz predloga ZInfV, bo 118. člen ZEKom-2 prenehal veljati in s tem se za operaterje neha obveza poročanja incidentov AKOSu. To pomeni, da se bodo nadzorno-varnostni centi operaterjev (NOC/SOC) morali v (pre)kratkem

času prilagoditi na to novo AKOSovovo poročanje, pri čemer prilagoditev pomeni, da moramo iz že vzpostavljenega delujočega sistema (ki smo ga vzpostavljali vrsto let), preiti na tega novega, nato pa bo poročanje po ZInfV najverjetneje spet drugačno, lahko celo popolnoma drugačno, najverjetneje tudi na ločenem informacijskem sistemu, drugačnemu kot je ta od AKOS. Kot operaterji spremljamo poročanje o varnostnih incidentih, to področje v EU ni enotno urejeno in ni standardizirano, je pa zaznati trend, da bi se to utegnilo spremeniti v bližnji prihodnosti (kar je dodaten razlog, da ne hitimo v prilagoditev sistema, ki bo tudi iz tega razloga lahko precej spremenjen oz. drugačen od AKOSovega).

Poročanje o incidentih je že danes, ko operaterji izpolnjujemo obrazce zelo kompleksno, a smo operaterji izpolnjevanje obrazcev uspešno avtomatizirali (in v to vložili kar nekaj truda in seveda sredstev), na predstavitvi pa je postalo jasno, da se bo v novem režimu zahtevalo ogromno podatkov, ki večino do sedaj niso bili del obrazca, pa tudi API namerava AKOS vzpostaviti šele konec leta, kar pomeni dvojno delo za operaterje. Na to je vezana tudi naša nadaljnja ugotovitev (ki jo podrobneje utemeljimo v naslednji točki), da bi moral AKOS v splošnem aktu opredeliti podatke, ki naj jih operaterji poročamo, sicer se bo lahko avtomatiziran sistem spreminjal, pač po potrebah AKOS. Kot smo opozorili operaterji na delavnicah in kot je AKOSu znano (ali pa bi mu moralo biti), prilagoditev ni tako lahko izvesti, ker so sistemi operaterjev kompleksni in medsebojno različni. Operaterji smo tudi na različnih stopnjah poročanj (nekateri verjetno ne poročajo varnostnih incidentov ali jih poročajo poredkoma) in ko pride do incidenta so prizadevanja operaterja usmerjena v identifikacijo incidenta in odpravo, ne pa v več urno izpolnjevanje poročil (operaterji, ki danes redno poročamo smo preizkusili sistem in ugotovili, da se je čas izpolnjevanja povečal iz nekaj sekund kot smo rabili do sedaj za izpolnitev obrazca na več kot 10 minut!).

Ad2) (mnogo) Večja količina podatkov pri najbolj poročani kategoriji (208. člen ZEKom-2), ki se poročajo po novem (poročanje ni primerno strukturirano ter optimiziramo; poročanje je izjemno zamudno)

Bolj kot prilagoditev poročanja varnostnih incidentov, postaja poročanje dogodkov po 208. členu ZEKom-2 z novim informacijskim sistemom mnogo kompleksnejše. AKOS je takorekoč podeseteril količino podatkov, ki jih moramo poročati operaterji (če primerjamo planirani sistem s sedaj veljavnim obrazcem), pri čemer je teh poročanj daleč največ (nekaj na dan). Na to smo opozarjali že na delavnici, enake ugotovitve ostajajo in se celo krepijo s preizkušanjem sistema. Vsekakor se nam poraja tudi pomislek zakaj je potrebnih toliko novih podatkov, ki do sedaj niso bili potrebni ne iz vidika AKOS, ne iz vidika končnega uporabnika, pri čemer kot smo na več mestih poudarili, prilagoditev temu novemu sistemu terja čas (sistemska prilagoditev na ravni podjetja je zahteven proces).

Znotraj obrazca je ravno tako naveden način obveščanja nacionalnega CSIRT, za kar imamo vzpostavljene interne postopke, ki so do sedaj delovali uspešno ter z dodanim nivojem zaščite (vsaka korespondenca je bila ravno tako vodena v svojem ITSM-incidentu). Terminologija znotraj posredovane dokumentacije omenja metodologijo obveščanja, ki je za CKVO presplošna in jo je v praksi težje izvajati, le-ta se pa na nivoju obveščanja ISP-jev ravno tako najverjetneje močno razlikuje.

Menimo, da je v javnem interesu, da se podaljša preizkušanje informacijskega sistema, omogoči povratne informacije in tako omogočit temeljit pregled in premislek ne samo o obsegu potrebnih podatkov pač pa tudi načinu poročanja in optimizaciji poročanja. Pristop, da pričnemo s prilagoditvijo po 1. 6. 2024, ko naj bi bil uraden začetek uporabe sistema, ni najprimernejši, tudi ne

iz vidika prevelikega obremenjevanja operativnih ekip. V skrajnem primeru naj se omogoči prehodni rok do 1. 1. 2025, v katerem operaterji preidemo na avtomatizirano poročanje, preizkušamo sistem in omogočimo AKOSu prilagoditve sistema, ki naj uradno zaživi 1. 1. 2025.

Za lažjo predstavo, prilagamo analizo poročanja po obstoječem sistemu (z obrazci) ter predvidenim novim informacijskim sistemom, ki ga je naredil enega od članov:

	Nov AKOS inf. vmesnik	**Stari AKOS obrazec**	
Checkboxi [Nr.]	50	6 do 7	/na dogodek
Freestyle polja [Nr.]	15	2	/na dogodek
Potreben čas za izvedbo [min]	17	0,5 do 1 (z avtomatizacijo)	/na dogodek

Največji problemi so dodatne sekcije, kjer se zahtevajo podatki, ki jih do sedaj ni bilo treba poročati:

- število afektiranih uporabnikov,
- predviden čas motenega delovanja in še dodatno trajanje celotne akcije oz. časovni okvir,
- potrebno javljati na kak način je bila javnost obveščena in posredovati to vsebino,
- definirati regijo, kraje, občino in je potrebno vse to ročno dodajati,
- definirati vplive dogodkov na kritično infrastrukturo, varnost podatkov, čezmejni vpliv dogodka, druge operaterje, druge ključne sisteme države in ostale podatke,
- ostalo.

Nato je dodatno treba še izpolniti poročilo, ki poleg 12 min vpisovanja za poročilo zahteva še dodatnih 5 min za poročilo. Pri tem poudarjamo, da velja to samo za planirana dela, za incidente in varnostne incidente pa še več.

Ad3) Rok za prilagoditev ter uporabo sistema je absolutno prekratek.

Glede roka za prilagoditev, ki je bil od začetka testiranja do sedaj prekratek za učinkovito testiranje, je bila glavnina problematike opisana v zgornjih dveh točkah. Operaterji sicer preizkušamo poročanje, zbiramo tudi opažanja, ki bodo posredovana AKOSu, a za resno testiranje, ki vodi v opredelitev končnega uporabnega sistema, je vendarle potrebno več časa.

Ad4) Način prijave

Ne strinjamo se s predlogom, kjer je bil izpostavljen način prijave v produkciji prek digitalnega certifikata z rabo lastnega SI PASS, saj je ta certifikat namenjen za osebne in ne službene zadeve. Menimo, da bi delo močno olajšali, če bi se identifikacija opravljala z digitalnim certifikatom podjetja kot individualnim SI PASS vsakega zaposlenega.

PREDLOG

Rok 1.6.2024 ko naj bi operaterji prešli na nov sistem poročanja je opredeljen s strani AKOS, zaradi česar bi ga AKOS lahko brez težav zamaknil na primernejše obdobje. Po našem mnenju sta sprejem novega ZInfV ter dejstvo, da sistem še zdaleč ni uporabniku prijazen (preveč kategorij, nepotrebne kategorije, poročanje še ni optimizirano itd) zadostna razloga za zamik. Namreč

operaterji imamo že tako ali tako vzpostavljene kanale za poročanje (kar pomeni, da bi se poročalo nemoteno še naprej). Po našem mnenju bi se bilo treba tudi dogovoriti, da se sistem, ko bo ustrezno prilagojen in preizkušen ne bo spreminjal, kar bi se lahko doseglo na tak način, da bi bili podatki, ki se morajo poročati, opredeljeni v prilogi splošnega akta o obveščanju in vrednotenju varnostnih incidentov ter o najavi omejitev ali prekinitev. Ugotavljamo namreč, da je AKOS zelo spremenil kategorije poročanja glede na danes veljaven sistem ter informacijski sistem ne sledi veljavnemu obrazcu (ki je bil do sedaj povesem zadosten tako za AKOS kot predvsem za uporabnike, ki jim je poročanje namenjeno).

Operaterji, člani SOEK predlagamo, da se v celoti zamakne vpeljava sistema in se načrtuje ne prej kot s 1. 1. 2025, ko bo najverjetneje že sprejet novi ZInfV, in ko bomo imeli operaterji tudi zadosti časa za testiranje, AKOS pa za optimizacijo poročanih podatkov (ki so še potrebni, da je končnim uporabnikom omogočen transparenten pregled nad vplivi na delovanje storitev). Delna uporaba sistema bo zgolj zapletla delo operativcem, ki izvajajo poročanja (npr. najavo del)., Zakasnitev vpeljave, glede na to, da operaterji že danes izvajamo poročanja, ne pomeni poslabšanja razmer, zamik, ki bi omogočil ustrezno vsebinsko presojo pa ima lahko zgolj pozitiven vpliv.

Za pojasnila ostajamo na voljo, po potrebi predlagamo čimprejšnje ponovno snidenje, na katerem bi se lahko pogovorili o postopni vpeljavi informatiziranega sistema, ki ga kot rečeno, operaterji pozdravljamo, a mora biti izvedeno na način, ki omogoča ustrezno vpeljavo.

S spoštovanjem,

Martina Ferjančič
Predsednica SOEK

Nenad Šutanovac, direktor
Združenje za informatiko in telekomunikacije pri GZS