Doc. dr. sc. Robertina Zdjelar

Upravljanje incidentima u kontekstu NIS 2 Direktive

Sažetak

Svrha NIS 2 Direktive je uspostaviti okruženje i razviti kulturu o važnosti zaštite od kibernetičkih napada i sprečavanje nastanka kritičnih i rizičnih događaja koji mogu ugroziti povjerljivost, konzistentnost ili dostupnost informacija i imovine. Tema članka vezana je uz pripremu, prepoznavanje, izvješćivanje o incidentima, procjenu utjecaja incidenata i djelovanju na incidente. Sve navedene aktivnosti opisane su međunarodnim standardima i dobrom praksom pa će u skladu s tim biti navedeni ključni dokumenti kao i regulativa temeljem koje se postavlja obveza upravljanja kibersigurnosnim incidentima.

Ključne riječi: CSIRT, incident, incident velikih razmjera, kibernetička sigurnost, mjere upravljanja incidentima, NIS 2 Direktiva, postupanje s incidentima, tim za postupanje s incidentima, tim za upravljanje incidentima, standardizirana praksa, značajan incident

1. Uvod

Prema podacima EUROSTATA[1] u „2021. godini u Europskoj Uniji 22,2% poduzeća (s 10 ili više zaposlenih i samozaposlenih osoba) u poslovnoj ekonomiji (isključujući rudarstvo i vađenje kamena i financijski sektor) doživjelo je IKT sigurnosne incidente koji su rezultirali različitim vrstama posljedica kao što je nedostupnost IKT usluge, uništavanje ili oštećenje podataka ili otkrivanje povjerljivih podataka. “Temeljem rezultata službene europske statistike tema upravljanja sigurnosnim incidentima zaslužuje pozornost svih onih koji su obveznici primjene NIS 2 Direktive, jer će u skoroj budućnosti svi ključni i važni subjekti biti obvezni uskladiti svoje poslovanje s odredbama spomenute Direktive.

Sagledavajući multidisciplinarnost koja se zahtijeva u procesu prilagodbe poslovanja NIS 2 Direktivi gotovo sigurno je da su područja upravljanja rizicima i upravljanja incidentima najobuhvatnija, upravo zato jer oni čine srž problema s kojim se treba nositi i rješenja kada je riječ o kibernetičkoj sigurnosti.

U nastavku će biti opisana pravna regulativa upravljanja incidentima s aspekta NIS 2 Direktive, međunarodni standardi i dobre prakse koje se preporučuje primjenjivati i implementirati kod obveznika primjene NIS 2 Direktive i nastavno na njih biti će ukratko opisane aktivnosti upravljanja kibersigurnosnim incidentima.

[1] Preuzeto s https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1, pristupljeno 9. studenog 2024.

2. Pravna regulativa

Kada govorimo o upravljanju incidentima s aspekta kibernetičke sigurnosti i primjene NIS 2 Direktive (EK, 2022) pažnju treba usmjeriti na odredbe NIS 2 Direktive, kojima se na upravljačkoj razini propisuje svrha, obim, zaduženja, obveza postupanja na uočene kibersigurnosne incidente. Osim odredbi NIS 2 Direktive treba uvažavati i nacionalni Zakon o kibernetičkoj sigurnosti („Narodne novine“ 14/24) (dalje u tekstu: Zakon).

Člankom 6. NIS 2 Direktive definiran je pojam ***„incident”*** i on znači događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup.

Recitalom 69. NIS 2 Direktive definirano je da *„U skladu s Prilogom Preporuci (EU) 2017/1584,* ***kibersigurnosni incident velikih razmjera*** *trebao bi značiti incident koji uzrokuje razinu poremećaja koja premašuje sposobnost države članice da na njega odgovori ili koji ima znatan učinak na najmanje dvije države članice. Ovisno o svojem uzroku i utjecaju, kibersigurnosni incidenti velikih razmjera mogu se proširiti i pretvoriti u prave krize koje onemogućavaju pravilno funkcioniranje unutarnjeg tržišta ili predstavljaju ozbiljne rizike za javnu sigurnost i zaštitu za subjekte ili građane u nekoliko država članica ili u Uniji u cjelini. S obzirom na širok opseg i, u većini slučajeva, prekograničnu prirodu takvih incidenata, države članice i relevantne institucije, tijela, uredi i agencije Unije trebali bi surađivati na tehničkoj, operativnoj i političkoj razini kako bi pravilno koordinirali odgovor širom Unije.“*.

O ***„kibersigurnosnom incidentu velikih razmjera“*** govori i članak 6. NIS 2 Direktive. U takvim slučajevima propisane su dodatne mjere i suradnja, te nadležnost mreže EU-CyCLONe, o čemu će više biti govora u nastavku.

Člankom 16. NIS 2 Direktive propisane su zadaće mreže EU-CyCLONe, a posebice treba istaknuti povećanje razine pripravnosti za upravljanje kibernetičkim sigurnosnim incidentima velikih razmjera i krizama; poboljšanje zajedničke informiranosti o kibersigurnosnim incidentima velikih razmjera i krizama; procjena posljedica i učinka relevantnih kibersigurnosnih incidenata velikih razmjera i kriza te predlaganje mogućih mjera ublažavanja; koordinacija upravljanja kibersigurnosnim incidentima velikih razmjera i krizama te pomoć pri odlučivanju na političkoj razini u pogledu takvih incidenata i kriza i tako dalje.

Recital 102. govori *„Kada ključni ili važni subjekti saznaju za* ***značajan incident****, trebali bi biti obvezni bez nepotrebne odgode, a u svakom slučaju* ***u roku od 24 sata, podnijeti rano upozorenje****. Nakon tog ranog upozorenja trebala bi uslijediti* ***obavijest o incidentu****. Dotični subjekti bi trebali podnijeti obavijest o incidentu bez nepotrebne odgode, a u svakom slučaju* ***u roku od 72 sata otkad saznaju za značajan incident****, u prvom redu kako bi ažurirali informacije podnesene u ranom upozorenju i naveli početnu procjenu značajnog incidenta, uključujući njegovu ozbiljnosti i učinak te, ako su dostupni, pokazatelje ugroženosti.* ***Završno izvješće trebalo bi podnijeti najkasnije jedan mjesec nakon obavijesti o incidentu****. Rano upozorenje trebalo bi sadržavati samo informacije koje su nužne kako bi Computer security incident response team (engl. CSIRT-ovi) ili, ako je to primjenjivo, nadležno tijelo bili*

upoznati s značajnim incidentom i kako bi se dotičnom subjektu, prema potrebi, omogućilo traženje pomoći. U takvom ranom upozoravanju, ako je to primjenjivo, trebalo bi navesti postoji li sumnja da je značajan incident uzrokovan nezakonitim ili zlonamjernim djelovanjem te postoji li vjerojatnost da će imati prekograničan učinak."

Incident je **„značajni incident"** ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga koje subjekt pruža odnosno djelatnosti koju obavlja ili financijske gubitke za subjekt i/ili ako je utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete (članak 37. Zakona).

Pojam **„izbjegnuti incident"** znači svaki događaj koji je mogao ugroziti dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup, ali je uspješno spriječen ili se nije ostvario. (NIS 2 Direktiva, članak 6.)

Zakonom su osnovni pojmovi definirani u članku 4.

Člankom 10. i člankom 11. NIS 2 Direktive definiran je pojam, uloga i djelokrug rada ***Computer Security Incident Response Team*** - CSIRT-ova, te se između ostaloga navodi da su oni zaduženi za praćenje i analiziranje kibernetičkih prijetnji, ranjivosti i incidenata na nacionalnoj razini i, na zahtjev, pružanje pomoći predmetnim ključnim i važnim subjektima u vezi s praćenjem njihovih mrežnih i informacijskih sustava u stvarnom ili gotovo stvarnom vremenu. CSIRT-ovi su zaduženi i za ostalu komunikaciju vezanu za incidente, pa je tako u njihovom djelokrugu rada i pružanje ranih upozorenja i najava te informiranje predmetnih ključnih i važnih subjekata, kao i nadležnih tijela i drugih relevantnih dionika o kibernetičkim prijetnjama, ranjivostima i incidentima, ako je moguće u gotovo stvarnom vremenu. Imaju propisanu obvezu i odgovarati na incidente i, ako je to primjenjivo, pružati pomoć predmetnim ključnim i važnim subjektima. U ostale propisane obveze CSIRT-ova spadaju:

„(d) prikupljanje i analiziranje forenzičkih podataka te osiguravanje dinamičke analize rizika i incidenata te informiranosti o stanju u pogledu kibernetičke sigurnosti;

(e) osiguravanje, na zahtjev predmetnog ključnog ili važnog subjekta, proaktivnog skeniranja mrežnih i informacijskih sustava predmetnog subjekta radi otkrivanja ranjivosti s potencijalno znatnim učinkom;

(f) sudjelovanje u mreži CSIRT-ova i pružanje uzajamne pomoći u skladu sa svojim kapacitetima i kompetencijama drugim članovima mreže CSIRT-ova na njihov zahtjev;

(g) ako je to primjenjivo, djelovanje u svojstvu koordinatora za potrebe postupka koordiniranog otkrivanja ranjivosti;

(h) doprinošenje korištenju alata za sigurnu razmjenu informacija" i slično.

Jedna od uloga CSIRT-ova je promicanje donošenja i primjene zajedničkih ili ***standardiziranih praksi, planova za klasifikaciju i taksonomija*** u odnosu na postupke za postupanje s incidentima.

U rješavanju prekograničnih incidenata pomoć osigurava mreža CSIRTova (članak 15. NIS 2 Direktive i članak 4. Zakona).*CSIRT mreža je „mreža nacionalnih CSIRT-ova osnovana u svrhu razvoja povjerenja i pouzdanja te promicanja brze i učinkovite operativne suradnje*

među državama članicama Europske unije (u daljnjem tekstu: države članice), koju uz predstavnike nacionalnih CSIRT-ova čine i predstavnici nadležnog tijela za prevenciju i zaštitu od kibernetičkih incidenata Europske unije (CERT-EU)".

Značajan incident o kojem ključni i važni subjekti moraju izvještavati, je onaj koji uzrokuje ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili financijske gubitke za predmetni subjekt. Također ako je incident utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete onda se smatra značajnim. (NIS 2 Direktiva, članak 23.)

Člankom 23. NIS 2 Direktive propisano je da ključni i važni subjekti moraju izvijestiti (u propisanim rokovima) o značajnom incidentu. Ako dotični subjekti obavijeste nadležno tijelo o značajnom incidentu, država članica osigurava da to nadležno tijelo obavijest po primitku proslijedi CSIRT-u. U slučaju prekograničnog ili međusektorskog značajnog incidenta, države članice osiguravaju da njihove jedinstvene kontaktne točke pravodobno dobiju relevantne informacije.

3. Međunarodni standardi i dobre prakse

Već je spomenuto u tekstu da su CSIRT-ovi zaduženi za promicanje donošenja i primjene zajedničkih ili ***standardiziranih praksi, planova za klasifikaciju i taksonomija*** kada je riječ o kibernetičkoj sigurnosti.

Međunarodna organizacija za standarde (engl. International Standard Organization ISO) izdala je:

- Temeljne principe i procese upravljanja incidentima pod nazivom ISO/IEC 27035-1:2023 Information technology — Information security incident management, Part 1: Principlesandprocess i
- Vodič za plan i pripremu postupanja s incidentima pod nazivom ISO/IEC 27035-2:2023 Information technology — Informations ecurity incident management Part 2: Guidelines to plan andprepare for incident response.

ISO/IEC 27035-1:2023 (odredba 1. Obuhvat) je temelj serije ISO/IEC 27035 i prikazuje osnovne koncepte, načela i proces s ključnim aktivnostima upravljanja incidentima u informacijskoj sigurnosti, koji pružaju strukturirani pristup pripremi, otkrivanju, izvješćivanju, procjeni i odgovoru na incidente te primjeni naučenog na osnovi vlastitog iskustva.

ISO/IEC 27035-2:2023 (odredba 1. Obuhvat) daje smjernice za planiranje i pripremu odgovora na incidente i izvlačenje lekcija iz odgovora na incidente. Smjernice su date kao detaljnija pojašnjenja specifičnih točki ISO/IEC 27035-1:2023. Glavne točke u fazi "planiranja i pripreme" uključuju:

- politike upravljanja incidentima informacijske sigurnosti i predanost najvišeg rukovodstva;
- politike informacijske sigurnosti, uključujući one koje se odnose na upravljanje rizikom, ažurirane i na organizacijskoj razini i na razini sustava, usluge i mreže;
- plan upravljanja incidentima informacijske sigurnosti;

- uspostavljanje tima za upravljanje incidentima (IMT);
- uspostavljanje odnosa i veza s unutarnjim i vanjskim organizacijama;
- tehnička i druga podrška (uključujući organizacijsku i operativnu podršku);
- brifinge i obuku o upravljanju incidentima u informacijskoj sigurnosti.

Faza učenja iz prakse (engl. Lessons learned) uključuje:
- utvrđivanje područja za poboljšanje;
- utvrđivanje i uvođenje potrebnih poboljšanja;
- evaluaciju tima za postupanje s incidentima (IRT).

Smjernice o procesu upravljanja incidentima informacijske sigurnosti i njegovim ključnim aktivnostima kao i dodane upute za plan i pripremu odgovora na incidente opće primjenjive su na svaki oblik i veličinu organizacije.

Osim ISO smjernica na raspolaganju za primjenu su i Upute za postupanje s incidentima kod računalne sigurnosti (NIST SP 800-61, 2012) koje je izdao National Institute of Standards and Technology (NIST). Kako se navodi u uvodu spomenutog dokumenta (NIST SP 800-61, 2012) svrha publikacije je pomoći organizacijama u ublažavanju rizika od incidenata računalne sigurnosti putem praktičnih smjernica o djelotvornom i učinkovitom odgovoru na incidente. „*Primarni fokus dokumenta je* ***otkrivanje, analiziranje, određivanje prioriteta i rukovanje incidentima****. Organizacije se potiču da prilagode preporučene smjernice i rješenja za ispunjavanje njihovih specifičnih zahtjeva za sigurnost i misiju"* (NIST SP 800-61, 2012).

NIST SP 800-61 razlikuje pojmove: kibersigurnosni događaj i kibersigurnosni incident. Razlika u terminima je upravo u činjenici da je kod incidenta već došlo do štete, dok događaj samo ukazuje na ranjivost, ali šteta nije nastala.

4. Preporučene aktivnosti upravljanja incidentima

Standardna metodologija upravljanja incidentima prema ISO/IEC 27035-1:2023i ISO/IEC 27035-1:2023 uključuje:

- definiranje ciljeva upravljanja kibernetičkim sigurnosnim incidentima
- planiranje i pripreme
- otkrivanje i izvješćivanje
- procjene i odlučivanje
- postupanje s incidentima
- nove spoznaje i učenje iz grešaka i propusta
- zapisi o kibernetičkim sigurnosnim incidentima
- komuniciranje o incidentima
- mjerenje i pregled aktivnosti upravljanja kibernetičkim sigurnosnim incidentima.

Sažeti opis svake od aktivnosti temeljen na preporukama ISO i NIST relevantnim dokumentima o kibernetičkim incidentima nalazi se u nastavku članka.

4.1. Utvrđivanje ciljeva upravljanja kibersigurnosnim incidentima

U ovoj aktivnosti korisno je pratiti preporuke iz ISO/IEC 27035-1 (točke 4.2.) koje govore o ciljevima upravljanja incidentima. Prije svega, potrebno je pratiti događaje povezane s informacijskom/kibernetičkom sigurnosti te ih klasificirati. Osnovno je utvrditi koje su to osobine zapaženih događaja zbog kojih ih se treba klasificirati kao incidente informacijske sigurnosti. Također, ključan cilj upravljanja incidentima je definiranje kako postupiti u slučaju da je neki događaj klasificiran kao incident te u kojem vremenskom roku treba sanirati situaciju. Klasifikacija događaja i incidenata važna je i radi prepoznavanja mogućih posljedica koje oni imaju na informacijsku sigurnost i na dionike. Klasifikacija po utjecaju na informacijsku sigurnost osim događaja i incidenta uključuje i pojam krize, što znači da u slučajevima kada incident poprimi šire razmjere da u tom slučaju treba postupati prema pravilima za krizna stanja. O kibernetičkim krizama već je bilo govora u uvodu, a o načinu postupanja i ostalim ključnim informacijama biti će govora u sljedećim izdanjima.

U situaciji kibernetičkog incidenta neophodno je biti svjestan ranjivosti sustava koja je omogućila da napad onesposobi ili ošteti imovinu i učini ključnog ili važnog subjekta nesposobnim ispuniti svoje ciljeve. Da bi upravljanje incidentima bilo učinkovito potrebno je razviti svijest odgovornih osoba, ali i ostalih zaposlenika, o obuhvatu aktivnosti koje je potrebno poduzeti za uspostavu i dosljednu primjenu propisanih mjera zaštite.

Svaka ranjivost sustava, predviđena u postupku analize kod same uskladbe poslovanja s NIS 2 Direktivom ili ranjivost koja je utvrđena nastankom nekog incidenta treba biti obrađena u cjelini, kako bi se uvele mjere za sprečavanje nastanka novih incidenata.

Kategorizacija, procjene, utvrđivanje prioriteta i razmjena iskustva osnovne su radnje u procedurama za pripremu sustava zaštite od kibernetičkih napada, čiji rezultati su osnova za donošenje strateških odluka i investiranje u kontrole informacijske sigurnosti. Razmjena iskustava ima značajnu ulogu u kontekstu primjene NIS 2 Direktive jer upravo to se i preporuča za jačanje mjera zaštite od kibernetičkih napada.

4.2. Planiranje postupanja i pripreme

Uobičajeno postupanje u uređenim sustavima je da prva aktivnost bude planiranje, pa je stoga i kod upravljanja incidentima tako. Prije svega potrebno je postaviti ključne ***politike upravljanja kibernetičkim sigurnosnim incidentima*** koje donosi i odobrava odgovorna osoba ključnog i važnog subjekta. Politike upravljanja kibersigurnosnim incidentima trebaju osigurati okvir koji opisuje jasan obuhvat promatranja, definicije što se smatra kibersigurnosnim incidentima, opis događaja koji se obavezno moraju analizirati, definiranje uloga i odgovornosti, opis zakonodavnog okvira i ostale bitne informacije za izradu plana.

Izrada plana postupanja s incidentima zahtijeva kompetentne ljudske resurse i vrijeme. Ukoliko se u fazi testiranja pokaže da plan postupanja s incidentima nije efikasan potrebno je uložiti dodatne napore za ažuriranje i uskladbu, a sve kako bi u situacijama kada incident nastane postupanje bilo učinkovito i u zadanom vremenu. Treba imati na umu da incidenti nastupaju nenajavljeno pa je postupanje s incidentima prilično stresna situacija koja zahtijeva

fokusiranu, brzu reakciju na način koji maksimalno anulira posljedice i vraća sustav u stanje prije incidenta.

Za usvajanje ***plana postupanja s incidentima*** potrebno je provesti pripremne aktivnosti kao podršku upravljanju incidentima. Prije svega valja reći da plan postupanja treba biti pisani dokument, koji mora biti odobren od odgovornih osoba ključnog i važnog subjekta. Osim toga, planom treba opisati svrhu, ciljeve i obuhvat politike, kategorije i kriterije za postavljanje prioriteta među incidentima, organizacijsku strukturu i definiranje uloga i odgovornosti te nadležnosti za upravljanje incidentima, kao i mjere za postupanje, procedure za izvješćivanje i komunikaciju.

Planiranje postupanja s incidentima podrazumijeva i uspostavu tima za postupanje s incidentima, ali i radnje poput treninga, uključivanja unutarnjih i vanjskih dionika u upravljanje incidentima kao i vježbe odnosno testiranje plana postupanja s incidentima. Tim za postupanje s incidentima (engl. Incident response team) treba imati jasno propisana pravila postupanja, odgovornosti i aktivnosti za koje je zadužen unutar ključnog ili važnog subjekta. Tim, odnosno njegovi članovi moraju znati što činiti, koje resurse imaju na raspolaganju u kojem vremenskom periodu. Svi članovi tima trebaju biti pripremljeni, istrenirani za postupanje u stresnim i izvanrednim situacijama, što incidenti svakako jesu. Članovi tima, moraju smireno i sabrano djelovati, poduzimati korake propisane procedurom, ako je situacija predviđena planom. U slučaju da je riječ o novoj i nedefiniranoj situaciji, koja planom nije predviđena važno je osvijestiti tu činjenicu, držati se koordinacije s jednog mjesta i pratiti upute voditelja tima.

Plan postupanja treba biti testiran u praksi te ukoliko se uoče neki nedostaci i nelogičnosti treba biti ažuriran.

4.3. Otkrivanje događaja i izvješćivanje

Otkrivanje i izvješćivanje o ***kibersigurnosnim događajima*** podrazumijeva izradu popisa događaja koji mogu naštetiti imovini (ne znači nužno da se to već dogodilo ili da će se dogoditi). Događaj nije nužno i incident. Iz inicijalno sačinjenog popisa prepoznatih i zabilježenih štetnih događaja radi se kategorizacija i utvrđuju se prioritetni ovisno o tome kakav rizik predstavljaju po sigurnost imovine.

Edukativne i informativne akcije podižu svijest o potrebi da se štetni događaji bilježe te da se s njima postupa s dužnom pažnjom u cilju zašite imovine, u ovom kontekstu posebno informacijske imovine. U fazi otkrivanja još se ne govori o incidentu, jer štetni događaji tek trebaju proći procjenu (vjerojatnost nastanka i učinak koji mogu imati ako se dogode) kako bi se moglo utvrditi radi li se o incidentu, o događaju koji je potencijalno bio rizičan, ali nije nastala šteta na imovini ili je pak šteta u takvim razmjerima da se događaj treba kategorizirati kao kriza.

Rezultati rada ove faze su izvještaji o uočenim štetnim događajima koji se dostavljaju timu za upravljanje incidentima (to nije tim koji postupa s incidentima, to je tim koji upravlja

procesom). U ovoj fazi tim za upravljanje incidentima zaprima popis potencijalnih opasnosti po sigurnost imovine.

O tome što i kako provjeravati u kontekstu kibernetičke sigurnosti sustava posebno je obrađeno poglavlje u okviru tema uskladbe poslovanja s NIS 2 Direktivom.

4.4. Procjene i odlučivanje

Procjena kibersigurnosnog događaja i kategorizacija provodi se temeljem raspoloživih informacija o događaju, koje su zapisane u izvještaju koji je dostavljen timu za upravljanje incidentima. U svakom slučaju važno je procijeniti ima li konkretan događaj utjecaj na povjerljivost, integritet i dostupnost informacijske imovine. Ako ima, onda je riječ o kibersigurnosnom incidentu. U toj situaciji ***tim za upravljanje incidentima*** angažira ***tim za postupanje s incidentima***.

Za procjene je potrebno koristiti sve dostupne bilješke o procesima, korisnicima, događajima kako bi se otkrilo koje su ranjivosti sustava iskorištene i na koji način te kakva šteta će nastati na informacijskoj i ostaloj imovini.

4.5. Postupanje s incidentima

Tim za postupanje s incidentom treba utvrditi koji podaci su preko kojeg sustava dohvaćeni bez zadane autorizacije, odnosno treba utvrditi koji je cilj napada. Pravovremeno otkrivanje incidenta i djelovanje na posljedice incidenta ima značajnu ulogu na štetu koju incident može izazvati.

Informiranost i upućenost zaposlenika o tome na koji način moraju prijaviti štetne događaje koji mogu biti kategorizirani kao incidenti od posebne je važnosti. Ključan resurs je vrijeme i brzina reakcije na nastalu situaciju. Nakon što je incident potvrđen, tim za postupanje s incidentima treba prepoznati koje su ključne radnje koje treba poduzeti da bi se utvrdio tip i opseg napada te u kratkom roku definirati način kako će se djelovati na posljedice i kako vratiti sustav u stanje prije nastalog incidenta. Neki scenariji napada su opisani u ENISA materijalu „THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS" iz srpnja 2021 (EINISA, 2021) (o čemu je više govora u poglavlju o kibernetičkoj sigurnosti u opskrbnom lancu). Poznati scenariji mogu biti predviđeni planom postupanja s incidentima, pa je procedura za postupanje unaprijed zadana, što znatno štedi vrijeme i čime se postiže brzi učinak.

Dodatan napor kojeg tim za postupanje s incidentima treba podnijeti je povratak sustava u stanje u kojem je bio prije napada. Koordinacija aktivnosti povratka u prvobitno stanje odnosno oporavka (engl. recovery) sustava je neophodna jer nerijetko postupak podrazumijeva aktivnosti u više različitih smjerova (oporavak sekundarne informacijske imovine i oporavak primarne informacijske imovine).

Razlika između postupanja s uobičajenim događajem i incidentom je ta što se događaj rješava uobičajenom poslovnom procedurom i ne zahtijeva razinu hitnosti kao što je to slučaj kod incidenta.

Procedura za postupanje s incidentom trebala bi sadržavati između ostalog: jasno definiran incident kojim treba upravljati; popis nužnih resursa za djelovanje uključujući i ljudske potencijale s propisanim kompetencijama; redoslijed koraka koje treba poduzeti; vremenski plan postupanja i rok; popis kontaktnih točaka i kanala komuniciranja.

Sve informacije o postupanju s incidentom trebaju biti zapisane i o postupanju se treba sačiniti izvještaj te isti dostaviti u registar sigurnosnih incidenata kojim upravlja tima za upravljanje incidentima. Svrha takvih zapisa je da se dodatnim analizama, nakon što je na incident odgovoreno, izvedu pouke i da se temeljem takvih zaključaka unaprijede kontrolne mjere.

Sam proces postupanja s konkretnim incidentima može biti rutinska radnja, ali može biti i složen proces koji zahtijeva angažman forenzičara kako bi se suštinski proanalizirao incident na koji treba odgovoriti.

Izvješćivanje nadležnih tijela o nastalom incidentu potrebno je provoditi kada je riječ o značajnom incidentu, ali neovisno o tome svaki ključni i važni subjekt može dobrovoljno informirati i izvještavati o uočenim događajima i incidentima nadležna tijela. Člankom 23. NIS 2 Direktive propisani su rokovi i obveze izvješćivanja.

4.6. Nove spoznaje i učenje iz grešaka i propusta

Postupanje s incidentom može se smatrati korektivnom radnjom, a osvježavanje i aktualizacija kontrolnih mjera na temelju novog iskustva može se smatrati unapređenjem preventivnih mjera. Iz iskustva treba izvući pouke i zaključke, iz uočenih ranjivosti i slabosti sustava kontrolnih i sigurnosnih mjera treba prepoznati koje sigurnosne mjere trebaju biti unaprijeđene.

Suradnja i razmjena informacija o nastalim kibersigurnosnim događajima, incidentima ili značajnim incidentima te incidentima velikih razmjera uvelike može doprinijeti kvaliteti mjera, kvaliteti planiranog djelovanja i postupanja te unaprijediti aktualne mjere kibernetičke sigurnosti.

4.7. Zapisi o kibersigurnosnim incidentima

U smislu upravljanja kvalitetom svaki zapis koji služi dokumentiranju o nastalom događaju treba sadržavati jedinstveni identifikator ili broj zapisa koji označava događaj na koji se zapis odnosi, datum i vrijeme nastanka događaja, kategoriju i stupanj prioriteta, podatke o korisniku koji je događaj prijavio, opis događaja, opis imovine koja je potencijalno ugrožena ili može biti ugrožena i slično.

Sve navedeno osigurava mogućnost praćenja te slijedivost informacija važnih za donošenje zaključaka i utvrđivanje mjera za postupanje.

Bez materijalnih dokaza niti jedan argument nije prihvatljiv niti se može smatrati objektivno utvrđenim.

4.8. Komuniciranje o incidentima

Vrlo osjetljivo područje u postupanju s incidentima je i komuniciranje o događajima koji su kategorizirani kao incidenti (bilo kojeg stupnja). Za komuniciranje s okolinom o incidentima zadužen je tim za postupanje s incidentima na način da o istome obavještava tim za upravljanje incidentima, službu za odnose s javnošću, pravni odjel i upravu prije nego informacije o incidentima budu dostupne javnosti.

Treba razlikovati komuniciranje za vrijeme postupanja s incidentom te komuniciranje prema okruženju u kojem djeluje ključan i važan subjekt. Također, način prezentiranja odnosno iznošenja informacija treba biti primjeren primatelju i svrsi informiranja, a s ciljem da primatelj dobije razumljivu, jasnu i objektivnu informaciju o nastalom incidentu.

Koliko god nije poželjno o ranjivostima vlastitog sustava govoriti javno, ipak postoji potreba podizanja svijesti da takva komunikacija i proaktivna razmjena informacija o prepoznatim incidentima može u značajnoj mjeri doprinijeti sprečavanju nastanka incidenata širih razmjera (krize).

4.9. Mjerenje i pregled aktivnosti upravljanja kibersigurnosnim incidentima

Što mjeriti kada su tema kibersigurnosni incidenti odnosno učinkovitost kibernetičkih sigurnosnih mjera? Kontinuirano poboljšanje stanja kibernetičke sigurnosti zasebno je poglavlje odnosno tema u kojoj je prezentirano kako se postiže kontinuirano poboljšanje. Ukratko, kontinuirano poboljšanje postiže se poboljšanjem vrijednosti mjerenih pokazatelja za ključne faktore, što bi u kontekstu kibersigurnosnih incidenata podrazumijevalo:

- povećanje učinkovitosti primijenjenih kibersigurnosnih mjera jer se povećava otpornost sustava na kibernetičke napade i
- smanjenje ili uklanjanje ranjivosti sustava
- jesu li procedure za djelovanje na incidente učinkovite
- jesu li procedure za oporavak od incidenta učinkovite (optimalni resursi, zadano vrijeme)
- je li predviđeni komunikacijski kanal efikasan za sve zainteresirane strane
- jesu li zadovoljene obveze izvješćivanja prema NIS 2 Direktivi?

Kada se utvrdi što od navedenog možda nije prema očekivanju ili nije u skladu s propisima potrebno je temeljem dobivenih rezultata djelovati otklanjanje nepravilnosti u postupanju s incidentima.

5. Zaključak

Za kraj, moglo bi se reći nakon opisane metodologije upravljanja incidentima da je glavni moto „bolje spriječiti nego liječiti“.

NIS 2 Direktivom propisano je da države članice EU imaju obvezu osigurati da subjekti, ključni i važni, implementiraju upravljanje incidentima radi osiguranja stabilnosti poslovanja i sigurnosti ljudi i imovine od kibernetičkih napada i drugih štetnih događaja.

Incidentne situacije zahtijevaju visoku razinu spremnosti za postupanje u posebnim situacijama, stoga svi obveznici primjene NIS 2 Direktive svoje zaposlenike trebaju što prije informirati i trenirati za snalaženju u izvanrednim situacijama kao što je to kibernetički napad.

Informiranost i svijest o štetama na imovini i štetama na reputaciji ključnog ili važnog subjekta koje mogu prouzročiti napadači putem kibernetičkih napada trebale bi biti više naglašene u svakodnevnoj poslovnoj komunikaciji.

Prikazane i kratko opisane aktivnosti upravljanja incidentima tek su preporuke prema standardu ISO i NIST. Svaka organizacija može prilagoditi preporuke svojim potrebama, rukovodeći se ciljem da proces bude efikasan, procedure jasne i ljudski resursi informirani o važnosti upravljanja incidentima.

Reference

1. ENISA (2021), 'Threatlandscape for supplychainattacks', preuzeto https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, pristupljeno 2. kolovoza 2024.
2. Europska Komisija, (2022), DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a highcommonlevelofcybersecurityacrossthe Union, amendingRegulation (EU) No 910/2014 andDirective (EU) 2018/1972, andrepealingDirective (EU) 2016/1148 (NIS 2 Directive), preuzeto https://eur-lex.europa.eu/eli/dir/2022/2555/oj, pristupljeno 10. svibnja 2024.
3. ISO/IEC 27035-1:2023 Informationtechnology — Informationsecurity incident management, Part 1: Principlesandprocess, preuzeto https://www.iso.org/standard/78973.html, pristupljeno 31. kolovoza 2024.
4. ISO/IEC 27035-2:2023 Informationtechnology — Informationsecurity incident managementPart 2: Guidelines to plan andprepare for incident response, preuzeto https://www.iso.org/standard/78974.html, pristupljeno 31. kolovoza 2024.
5. National Institute ofStandardsand Technology, (2012). NIST SP 800-61 Rev Computer Security Incident HandlingGuide (August 2012), preuzeto https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, pristupljeno 20. kolovoza 2024.
6. Zakonom o kibernetičkoj sigurnosti („Narodne novine" br. 14/24)

O autorici

Doc. dr. sc. Robertina Zdjelar doktorirala je u području društvenih znanosti, polje informacijske i komunikacijske znanosti 2022. godine. Tijekom 2024. godine autorica je izabrana u znanstveno-nastavno zvanje naslovni docent. Bavi se istraživanjem u području informacijskih i komunikacijskih znanosti, stručnim radovima u području javnih politika, financija i računovodstva. Angažirana je kao vanjski suradnik na Sveučilištu u Zagrebu na Fakultetu organizacije i informatike Varaždin te na Pravnom fakultetu u Zagrebu te na Geotehničkom fakultetu u Varaždinu. Djelovanje na Fakultetu organizacije i informatike odnosi se na upravljanje kvalitetom u informatici, kvalitetu i mjerenja u informatici, upravljanje primjenom informacijske tehnologije u poslovanju, odgovornost, inkluzija i održivost u informatici. Na Pravom fakultetu u Zagrebu autorica je održala nekoliko predavanja na temu upravljanja projektima. Na Geotehničkom fakultetu u Varaždinu održala je tribinu pod naslovom "Umjetna inteligencija i gospodarenje otpadom".

U poslovnom okruženju autorica je zaposlenik Gradskog komunalnog poduzeća Komunalac d.o.o. kao direktorica Sektora financija, računovodstva i EU projekata, a u okviru kojega se nalaze i druge poslovne funkcije važne za poslovanje društva. Zadnjih osam godina zaposlena je u društvu Komunalac, čemu je prethodilo dvadeset godišnje radno iskustvo u Koprivničko-križevačkoj županiji na raznim pozicijama, od pripravnika, suradnika do pročelnice za financije, proračun i javnu nabavu.

Autorica posjeduje brojne stručne certifikate od kojih treba istaknuti ***NIS2 Directive Lead Implementer, ISO 27001 interni auditor, ISO 9001 Lead auditor***, ESG akademija, voditelj financijskog kontrolinga, voditelj pripreme i provedbe EU projekata.