Doc. dr. sc. Robertina Zdjelar

Upravljanje imovinom u kontekstu kibernetičke sigurnosti

Sažetak

Nastavno na uvodni članak o ključnim poglavljima vezanim uz kibernetičku sigurnost autorica u ovom članku daje pregled ključnih aktivnosti vezano za upravljanje imovinom (asset management) s aspekta osiguranja kibernetičke sigurnosti prema NIS 2[1] direktivi (EK, 2022).

Područje upravljanja imovinom (asset management) sagledavano je se s različitih perspektiva, posebice računovodstvene, financijske i perspektive kontrolinga, ali i s perspektive investiranja. S razvojem svijesti o važnosti kibernetičke sigurnosti razvila se i svijest o potrebi da se vodi računa o sigurnosti imovine.

Svakoj organizaciji raspolaganje imovinom je nužan preduvjet za ostvarenje vizije, misije i strategije. Što se smatra imovinom ovisi o konkretnom slučaju. Sagledavanje imovine s aspekta kibernetičke sigurnosti ima za svrhu osvijestiti koja imovina je ključna za sigurno poslovanje, koja imovina je kritična i ranjiva s aspekta kibernetičkih napada te što je potrebno poduzeti da se rizici od napada spriječe te da ako se već desi kibernetički incident i bude eventualno nastane šteta na imovini da ona bude svedena na minimum.

U ovom radu biti će u kratkim crtama opisana metodologija koju se može primijeniti na upravljanje imovinom, koje su koristi od upravljanja imovinom, koji su to ključni elementi sustava upravljanja imovinom. Također, autorica će u radu dati prikaz programa kibernetičke sigurnosti upravljanja imovinom te koje je korake preporučeno provesti za implementaciju programa. Od posebne važnosti, za određene kategorije imovine, može biti pravo pristupa do podataka o imovini. Kako postupati s imovinom u trenutku kada zaduženi korisnik više nema osnovano pravo koristiti neku imovinu (umirovljenje, promjena poslodavca…)?

Ključne riječi: kibernetička sigurnost, kontinuitet poslovanja, kontrole, NIS 2 direktiva, upravljanje imovinom, upravljanje krizama, upravljanje rizicima

Uvod

U uvodnom tekstu „Uskladba poslovanja s NIS 2 Direktivom – ključna područja“ autorica je navela između ostaloga da je kod pripreme i provedbe projekta uskladbe poslovanja s Direktivom NIS 2 u fazi planiranja potrebno obratiti pažnju na praksu koja se primjenjuje pri ***upravljanju imovinom***. Uspostavljene procedure u nekoj organizaciji trebaju biti sagledane i ažurirane s ciljem da se kroz već postojeću praksu napravi poboljšanje koje će jamčiti kibernetičku sigurnost u poslovanju.

Nastavno na postojeću praksu i preporuke koje su se tijekom zadnja dva desetljeća razvijale, temeljem čega su razvijeni standardi svakako treba pažnju obratiti na ***ISO/IEC 55000:2024 Asset management — Vocabulary, overview and principles***. Standard ***ISO 31000:2018 - Risk Management*** nije certifikacijski, no u njemu su navedene praktične upute oko uspostave upravljanja rizicima, a obuhvaćen je i segment rizika vezanih uz imovinu. Prema navedenom standardu preporuča se kod utvrđivanja rizika sagledati oblik i vrijednost imovine i resursa. Standard ***ISO/IEC 27005:2022 Manage Information***

[1] NIS 2 (EK, 2022) DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Security Risk dijeli imovinu na primarnu/poslovnu imovinu i potpornu imovinu koja predstavlja komponente informacijskog sustava na kojima se vode podaci o imovini.

Što se smatra imovinom?

Prema ISO/IEC 27005:2022 imovina je sve što ima vrijednost za organizaciju i što je potrebno zaštititi jer je neophodno za postizanje organizacijske misije. Informacijski sustav sastoji se od opreme, programa, procesa, informacija koje je potrebno prepoznati i zaštititi, ali i od korisnika čije znanje, kompetencije i digitalne vještine su posebno važne kada je riječ o kibernetičkoj sigurnosti. Imovina koja sadrži informacije od ekonomske, administrativne ili pravne vrijednosti također treba biti uključena pod upravljanje imovinom u kontekstu kibernetičke sigurnosti.

Recitalom 8. Uredbe (EU) 2019/881 (EK, 2019), definiran je pojam „Kibersigurnost“ što je preuzeto i u NIS 2 (EK, 2022). Prema navedenom izvoru kibernetička sigurnost *„nije samo problem povezan s tehnologijom, već je za njega od jednake važnosti ljudsko ponašanje. Stoga bi trebalo snažno promicati „kiberhigijenu”, odnosno jednostavne, rutinske mjere kojima se, ako ih građani, organizacije i poduzeća redovito provode, na najmanju moguću mjeru smanjuje njihova izloženost rizicima od kiberprijetnji.“*

Kibernetička sigurnost kao pojam definiran je člankom 2. Uredbe (EU) 2019/881 (EK, 2019) u točki 1. kao : „kibersigurnost znači sve aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu“ .

Koje su koristi od upravljanja imovinom?

Upravljanje kao aktivnost ima za svrhu usmjeravanje predmeta upravljanja iz postojećeg stanja prema željenom stanju. Cilj upravljanja imovinom je da imovina bude adekvatna, da bude dostatna u kvaliteti i količini radi ostvarenja zadanih ciljeva organizacije, da bude zaštićena od uništenja i otuđenja ili onesposobljene funkcionalnosti. Također, kod odlučivanja o investiciji, upravljanje imovinom treba osigurati potrebne informacije za investiranje, planirati i osigurati povrat uloženih sredstava u investiciju.

Imovinu je potrebno kategorizirati prema izloženosti rizicima, prema vjerojatnosti nastanka rizika i utjecaju koji rizik može imati po imovinu. Dobro upravljanje imovinom osigurava uvjete za pravovremeno pružanje usluga i proizvodnju, prema kvaliteti i dinamici očekivanoj od strane korisnika/kupaca.

Implementacija društvene odgovornosti organizacije podrazumijeva brigu o smanjenju štetnih utjecaja na okoliš, očuvanje resursa i prilagodbu klimatskim promjenama, što ukazuje na društveno odgovornu i etičnu poslovnu praksu. Povezano s očuvanjem okoliša potrebno je voditi brigu o usklađenosti procesa upravljanja imovinom s pravnim, statutarnim i regulatornim zahtjevima, što zajedno s prihvaćanjem društvene odgovornosti osigurava bolju reputaciju organizacije s perspektive kupaca/korisnika i svijesti i pouzdanosti od strane vlasnika.

Člankom 7. Direktive NIS 2 (EK, 2022) definirano je da svaka država članica donosi nacionalnu strategiju za kibersigurnost u kojoj se utvrđuju strateški ciljevi, resursi potrebni za postizanje tih ciljeva i odgovarajuće mjere politike i regulatorne mjere radi postizanja i održavanja visoke razine kibersigurnosti. Nacionalna strategija za kibersigurnost uključuje između ostaloga i mehanizam za utvrđivanje relevantne imovine i procjenu rizika u toj državi članici.

Člankom 21. Direktive NIS 2 (EK, 2022) definirano je da države članice osiguravaju da ključni i važni subjekti poduzimaju odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izloženi mrežni i informacijski sustavi kojima se ti subjekti služe u svom poslovanju ili u pružanju svojih usluga te za sprečavanje ili smanjivanje na najmanju moguću mjeru učinka incidenata na primatelje njihovih usluga i na druge usluge. Spomenute mjere temelje se na pristupu

kojim se uzimaju u obzir sve opasnosti i čiji je cilj zaštita mrežnih i informacijskih sustava i fizičkog okruženja tih sustava od incidenata, a između ostalog uključuju sigurnost ljudskih resursa, politike kontrole pristupa i upravljanje imovinom.

Upravljanje imovinom u kontekstu upravljanja organizacijom predstavlja koordinirane aktivnosti kojima se ostvaruje nova vrijednost. Sustav upravljanja imovinom sastoji se od politike, ciljeva i procesa za postizanje tih ciljeva, a primjenjuje se na portfolio imovine koja udovoljava postavljenim kriterijima važnosti, neophodnosti, podložnosti rizicima.

U sljedećem poglavlju biti će opisani koraci koje posebno treba predvidjeti planom upravljanja imovinom, planirati tko ih je odgovoran provoditi.

Program upravljanja imovinom

Program upravljanja imovinom predviđa sljedeće korake:

1. identifikaciju sve digitalne imovine u organizaciji, poput strojeva (hardware), programa (software), mrežne infrastrukture (network infrastructure) i drugih uređaja (za pohranu), procesa ili prijenosa podataka
2. kategorizaciju imovine prema kritičnosti, vrijednosti i osjetljivosti što ima za cilj utvrđivanje prioriteta za uspostavu sigurnosnih mjera i pravilno alociranje resursa vezanih uz zaštitu.
3. kreiranje i ažuriranje popisa utvrđene imovine, koji između ostaloga treba sadržavati lokaciju, IP adresu. Popis također mora sadržavati podatke o vlasniku/korisniku, o sigurnosnoj kopiji podataka (vezano uz tu imovinu, npr. gdje se čuvaju postavke nekog uređaja) i podatak o vrijednosti za organizaciju. Popis mora biti točan, ažuriran, konzistentan.
4. procjena rizika kroz koju se treba osvijestiti vjerojatnost događanja sigurnosnog incidenta i intenzitet utjecaja koji on može imati na imovinu
5. implementacija sigurnosnih kontrola koje moraju biti primjerene kategorizaciji imovine i izloženosti iste rizicima, a najčešće podrazumijevaju kontrolu pristupa, enkripciju, instaliranje vatrozida, prepoznavanje upada u sustav i mjere prevencije.
6. nadzor provođenja zadanih sigurnosnih kontrola, praćenje njihove učinkovitosti te revidiranje i održavanje istih prema potrebi
7. kontinuirano poboljšanje treba osigurati da upravljanje imovinom bude efikasno i značajno. Kontinuirano poboljšanje podrazumijeva ažuriranje programa upravljanja imovinom na osnovu informacija do kojih se dolazi tijekom ranijih faza. Svakako valja obratiti pažnju na okruženje koje je dinamičko, razvoj tehnologije koji sa sobom nosi nove rizike, promjene u organizaciji i promjene u samom programu kibernetičke sigurnosti.

Kako bi se osigurala sigurnost imovine, a u kontekstu prethodno opisanih koraka postupanja, važno je utvrditi i sljedeće:

- ograničiti pristup imovini ovisno o kategorizaciji iste
- održavati zapise o korisnicima koji imaju ovlaštenja za korištenje
- čuvati informacije o imovini na način da se osigurava vjerodostojna sigurnosna kopija
- jasno obilježiti imovinu i podatke o imovini kako bi se dodatno usmjerila pažnja autoriziranih korisnika na važnost iste
- autorizirati pristup ključnim informacijama o imovini.

O sigurnosti imovine treba voditi računa i kod njezinog stavljanja izvan funkcije iz bilo kojeg razloga, a posebice je ovo važno za kibernetičku sigurnost jer se odnosi na računala, fizičke primjerke kopija podataka, uređaja za pohranu podataka i druge IKT opreme. Imovina koja više nije u upotrebi, a nije s njom postupano na propisan i siguran način može potencijalno biti iskorištena za krađu podataka, za pristup do ključnih drugih resursa neophodnih za poslovanje organizacije, a što može uzrokovati značajne štete, kako materijalne tako i reputacijske (npr. krađa podataka, identiteta i sl).

Kibernetički rizici, kibernetički incidenti i kibernetičke krize, a naročito posljedice koje oni uzrokuju po kontinuitet poslovanja dovoljan su poticaj da se upravljanje imovinom prihvati kao nezaobilazan korak u osiguranju kibernetičke sigurnosti.

Zaključak

Ako ponovo sagledamo što je to kibernetička sigurnost, tada ukratko možemo ponoviti da upravljanje imovinom treba imati za cilj da imovina bez koje organizacija ne može poslovati mora biti zaštićena od svih prepoznatih rizika, a posebice od rizika koje donosi digitalizacija poslovanja i ponašanje korisnika u takvom okruženju.

Kakva je praksa u Republici Hrvatskoj tek će s vremenom biti utvrđena trenutna razina zrelosti u području upravljanja imovinom s aspekta kibernetičke sigurnosti. Pretpostavka je da će u narednom kratkoročnom razdoblju (do jedne godine) zasigurno kroz procese prilagodbe poslovanja zahtjevima Direktive NIS 2 (EK, 2022) biti komunicirane dobre prakse što će uvelike pomoći obveznicima primjene NIS 2 da svoje sustave prilagode i time osiguraju ne samo kibernetičku sigurnost vlastitog sustava, nego i u širem okruženju mogu dati doprinos širenju dobre prakse i stvaranju sigurnog okruženja.

Reference

1. Europska Komisija, (2019), **REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)**
2. Europska Komisija, (2022), DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), preuzeto https://eur-lex.europa.eu/eli/dir/2022/2555/oj, pristupljeno 10. svibnja 2024.
3. ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks, preuzeto https://www.iso.org/standard/80585.html, pristupljeno 13. svibnja 2024
4. ISO 31000:2018, Risk management, A practical guide, preuzeto https://www.iso.org/publication/PUB100464.html, pristupljeno 10. srpnja 2024.
5. ISO 55000:2024, Asset management — Overview, principles and terminology, preuzeto https://www.iso.org/standard/55088.html, pristupljeno 20. srpnja 2024.
6. „Narodne novine“ br. 14/24, Zakon o kibernetičkoj sigurnosti, preuzeto https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html, pristupljeno 12. lipnja 2024.

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 dvadesetgodišnje 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 ISO 27001 interni auditor, ISO 9001 interni auditor, ESG akademija, voditelj financijskog kontrolinga, voditelj pripreme i provedbe EU projekata. U postupku je stjecanja certifikata za vodećeg implementera NIS 2 direktive. Svoje radno iskustvo koristi kao izvor ideja za znanstvene i stručne radove.