Vježbe za kibernetičke incidente u bankarskom sustavu

Jurčević, Mario

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Mario Jurčević

VJEŽBE ZA KIBERNETIČKE INCIDENTE U BANKARSKOM SUSTAVU

SPECIJALISTIČKI RAD

Zagreb, 2023.

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING
SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Mario Jurčević

CYBER INCIDENT EXERCISE FOR THE BANKING INDUSTRY

SPECIALIST THESIS
SPECIJALISTIČKI RAD

Zagreb, 2023.

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu poslijediplomskog specijalističkog studija Informacijska sigurnost.

Mentor: izv. prof. dr. sc. Stjepan Groš

Specijalistički rad ima: 57 stranica.

Specijalistički rad br.:_____.

Povjerenstvo za ocjenu u sastavu:

1. doc. dr. sc. Ante Đerek – predsjednik
2. izv. prof. dr. sc. Stjepan Groš – mentor
3. izv. prof. dr. sc. Toni Perković, Sveučilište u Splitu Fakultet elektrotehnike, strojarstva i brodogradnje – član

Povjerenstvo za obranu u sastavu:

1. doc. dr. sc. Ante Đerek – predsjednik
2. izv. prof. dr. sc. Stjepan Groš – mentor
3. izv. prof. dr. sc. Toni Perković, Sveučilište u Splitu Fakultet elektrotehnike, strojarstva i brodogradnje – član

Datum obrane: 28. rujna 2023.

Sažetak

Cilj ovog rada je definirati prijedlog procesa, scenarije i popratne materijale za provođenje vježbi odgovora na kibernetičke incidente u bankarskom sektoru. U okviru istraživanja za rad provedena je temeljita analiza postojećih praksi za vježbe odgovora na kibernetičke incidente, uključujući vrste vježbi, njihove ciljeve i metodologije.

Rezultati istraživanja ukazuju na to da su vježbe odgovora na incidente ključni alat za unapređenje pripravnosti financijskih institucija u suočavanju s raznovrsnim prijetnjama. Zaključak je da priprema i definiranje relevantnog i realnog scenarija koristeći dijelove TIBER-EU okvira omogućava dobru pripremu za odgovor na incidente, što pridonosi bržoj i učinkovitijoj reakciji u slučaju stvarnih incidenata, smanjujući potencijalne gubitke i štetu.

Ovaj će rad dati opće smjernice za planiranje, pripremu, razvoj i provođenje tih vježbi slijedeći važeće regulative i zakone kao i najbolje prakse u bankarskom sektoru, kako bi financijske institucije provođenjem vježbi unaprijedile proces odgovora na incidente. Također, u ovom su radu predloženi materijali koji se mogu koristiti prilikom pripreme i izvođenja vježbe, kao i konfiguracija vježbe u OpenEX simulatoru.

Ključne riječi: Odgovor na incidente, kibernetička sigurnost, vježba, potencijalni scenariji incident

Summary

The goal of this specialist thesis is to suggest a process, templates and scenarios that can be used for execution of cybersecurity incident response exercises in the financial sector. A thorough analysis of current practices in cybersecurity incident response exercises was conducted as a part of research for this thesis, including types of exercises, their goals and methodologies.

Results of this research clearly show that incident response exercises are a crucial process in the improvement of financial institution readiness to face various threats. Preparing and defining a relevant and realistic scenario based on TIBER-EU framework allows a well-rounded incident response, resulting in a faster and more efficient reaction with real incidents and reducing potential loss and damage.

This specialist thesis defines guidelines for planning, development and exercise preparation based on relevant regulations and laws in banking sector. Financial institutions can use the information from this specialist thesis to test and improve cybersecurity incident management process. In addition, this specialist thesis lists materials that could be used in preparation and execution of exercises, as well as an exercise scenario file for OpenEX simulator.

Keywords: Incident response, cybersecurity, exercise, incident scenario

SADRŽAJ

1. UVOD

Razvoj informacijskih tehnologija promijenio je način poslovanja i upravljanja u svim sektorima, pa tako i u financijskom sektoru. Kako bi ostvarile tržišnu prednost, financijske institucije implementacijom informacijskih sustava digitaliziraju procese i pronalaze tehnološka rješenja za odgovor na izazove visoko promjenjivog okruženja. Korištenje informacijskih tehnologija financijskim institucijama omogućava proširivanje opsega usluga i približavanje klijentima, no korištenje informacijskih tehnologija također stvara veliku ovisnost o informacijskoj tehnologiji. Prema tome, potrebno je pravilno upravljati informacijskim sustavima kao sastavnim djelom upravljanja bankom. Kako bi se to postiglo, potrebno je uvesti sustav upravljanja sigurnošću informacijskih sustava (engl. *Information Security Management System*, ISMS). ISMS je prema ISO/IEC 27001 standardu sustav upravljanja sigurnošću informacija koji se sastoji od politika, postupaka, smjernica, procesa i struktura organizacije. ISMS uključuje sustavno upravljanje rizicima i zaštitu informacija od neovlaštenog pristupa, korištenja, otkrivanja, uništavanja, poremećaja, zloupotrebe, prijetnji ili krađe [1].

Bez obzira na zrelost sustava za upravljanje informacijskom sigurnošću, svaki sustav podložan je incidentima te je ključno znati kako odgovoriti na njih. Incident je neplanirani i neželjeni događaj čija je posljedica povreda (ili koji neposredno prijeti povredom) važećih propisa RH, politike sigurnosti informacijskog sustava, ostalih internih akata banke vezanih uz informacijsku sigurnost kao i narušavanje temeljnih načela informacijskog sustava, prihvaćenih praksi vezanih uz informacijsku sigurnost te funkcionalnosti informacijskog sustava [2].

Upravljanje incidentima izuzetno je važno za otkrivanje, upravljanje i minimiziranje posljedica sigurnosnih incidenta. Cilj upravljanja incidentima je minimizirati utjecaj incidenta na poslovanje, smanjiti rizik od budućih incidenata i poboljšati sposobnost organizacije da se suoči s incidentima [3]. Upravljanje incidentima obuhvaća uspostavljanje procesa za otkrivanje, prijavljivanje, analizu, rješavanje i dokumentiranje incidenta [3]. Financijske institucije trebale bi uspostaviti i provoditi postupak upravljanja incidentima i problemima radi praćenja i bilježenja operativnih i sigurnosnih IKT incidenata te kako bi se financijskim institucijama omogućilo da u slučaju prekida pravovremeno nastave ili ponovno krenu obavljati kritične poslovne funkcije i procese [4]. Također, financijske institucije dužne su obavještavati nadležna tijela o značajnim incidentima koji su se dogodili, a ukoliko incident ima značajan učinak na kontinuitet usluga, nadležno tijelo može obavijestiti javnost o incidentu ili zatražiti kreditnu instituciju da obavijesti javnost, što može uzrokovati i reputacijsku štetu.

Za pravilno upravljanje incidentima izuzetno je bitno definirati politike, standarde i planove te osvijestiti sve sudionike o propisima te njihovim ulogama i odgovornostima u procesu odgovora na incidente. Da bi se ovo postiglo potrebno je redovno testirati planove i educirati sve relevantne sudionike i potencijalne sudionike u procesu odgovora na incidente. Ovaj rad opisuje postupak pripreme, provođenja i procjene vježbi odgovora na kibernetičke incidente kojima se testiraju uspostavljeni planovi i provodi edukacija zaposlenika. Nakon vježbi identificiraju se potencijalni nedostaci i definiraju se područja u kojima je potrebno unaprjeđenje. Upravljanje i odgovor na operativne incidente nisu uključeni u ovaj rad.

Rad je strukturiran na sljedeći način: drugo poglavlje rada opisuje vježbe odgovora na kibernetičke incidente, što uključuje tipove vježbi, faze provođenja vježbi te osobe ključne za planiranje i provođenje vježbi. Treće poglavlje opisuje postupak planiranja vježbe odgovora na kibernetičke incidente s prijedlogom procesa za definiranje i odabir relevantnog scenarija za vježbu. Četvrto poglavlje opisuje proces definiranja i pripreme scenarija za vježbu na konkretnom primjeru. Peto poglavlje opisuje postupak provođenja vježbe te daje smjernice za provođenje vježbe i smjernice za voditelja vježbe, kao i opis procesa za procjenu uspješnosti vježbe. Šesto poglavlje sadrži zaključak rada dok je u sedmom poglavlju dan pregled korištene literature.

2. VJEŽBE ODGOVORA NA KIBERNETIČKI INCIDENT

Provođenje vježbi za odgovor na kibernetičke incidente ključno je za organizaciju koja želi biti spremna pravilno odgovoriti na razne sigurnosne prijetnje. Takve vježbe pružaju mogućnost testiranja sposobnosti odgovora na incidente i pronalaženje slabih točaka u postojećim procesima odgovora na incidente. Vježbe trebaju biti organizirane periodički, s unaprijed definiranim intervalima prilagođenim potrebama financijske institucije, kako bi se osigurala kontinuirana spremnost tima za odgovore na incidente (engl. *Incident Response Team*, IRT) te kako bi se osiguralo da su procedure kontinuirano ažurne i primjenjive.

Svrha provođenja vježbi za odgovor na kibernetičke incidente je testiranje, provjera i poboljšanje sposobnosti u odgovoru na kibernetičke incidente. Konkretno, provođenjem vježbe provodi se provjera planova i postupaka. Provodeći simulaciju kibernetičkog incidenta, moguće je identificirati slabosti u planovima, otkriti propuste i poboljšati postupke kako bi bili učinkovitiji u stvarnim situacijama. Pored toga, provođenjem vježbe moguća je identifikacija nedostataka u pripremljenosti za kibernetičke incidente. Sudjelovanje u vježbama sudionicima omogućuje otkrivanje nedostataka u infrastrukturi, procesima, komunikaciji i suradnji među timovima. Na temelju tih saznanja, moguće je poduzeti korektivne mjere kako bi se ojačala sigurnost i odgovor na incidente. Također, provođenjem vježbe provodi se i osposobljavanje zaposlenika u postupcima i vještinama odgovora na incidente. Sudionici mogu poboljšati razumijevanje svojih uloga, poboljšati tehničke vještine, razviti sposobnost donošenja odluka pod pritiskom i uvježbati komunikacijske vještine potrebne tijekom kriznih situacija. Na kraju, vježbom se promiče poboljšanje suradnje te koordinacija. Sudionici timova za odgovor na incidente mogu naučiti kako bolje komunicirati, koordinirati aktivnosti, dijeliti informacije i donositi odluke kao tim. Poboljšanje suradnje pridonosi bržem, učinkovitijem i usklađenijem odgovoru na stvarne sigurnosne incidente.

Scenariji za organizirane vježbe mogu varirati od simuliranih značajnih incidenata temeljenih na stvarnim napadima, greškama ili nedostacima sustava sve do *tabletop* vježbi. Vježbe ne moraju uključivati samo tim za odgovor na incidente, nego mogu uključivati i druge interne organizacijske jedinice ili vanjske organizacije koje su uključene u upravljanje sigurnosnim incidentima.

2.1. Tipovi vježbi za odgovor na incidente

Tip vježbe koja će se provoditi ovisi o ciljevima koji se trebaju postići, kao i o dostupnom vremenu i resursima. Uobičajeni tipovi vježbi su [5]:

- vježbe temeljene na raspravi
- *tabletop*
- vježbe u realnom vremenu (engl. *live*)
- kombinacija gore navedenih vježbi

Kod vježbi temeljenih na raspravi i *tabletop* vježbi sudionici sudjeluju u diskusiji kako bi simulirali reakciju na sigurnosni incident. Cilj ovih vježbi obično je evaluirati postojeće planove i postupke odgovora na incidente, identificirati nedostatke, poboljšati suradnju među timovima i povećati svijest o ulogama i odgovornostima. Ovaj tip vježbi također može pružiti priliku za podizanje razine svijesti o sigurnosnim rizicima, politikama i procedurama. Kod ovih vježbi fokus je na analizi scenarija incidenta i razgovoru o postupcima koje treba poduzeti. Sudionici raspravljaju o incidentu, dijele ideje, iznose prijedloge i razmatraju moguće pristupe za rješavanje problema. Ove vježbe nisu usmjerene na praktičnu primjenu ili izvođenje tehničkih aktivnosti, već na raspravu i razumijevanje postupaka. Vježbe temeljene na raspravi i *tabletop* vježbe mogu uključivati članove tima za odgovor na incidente, upravljačke timove, komunikacijske stručnjake i druge relevantne dionike. Tijekom vježbe raspravu vodi moderator. On postavlja pitanja i potiče sudionike da dijele svoje mišljenje i iskustva. Tijekom vježbe važno je osigurati aktivno sudjelovanje sudionika u raspravi, iznošenje ideja, izazova i prepreka s kojima se suočavaju tijekom odgovora na sigurnosne incidente. Sudjelovanje u ovakvim vježbama može pomoći pri identifikaciji slabosti te poboljšanju postupaka odgovora na incidente.

Vježbe u realnom vremenu (engl. *live*) su simulacije koje uključuju aktivno i praktično rješavanje sigurnosnog incidenta. Kod vježbi u realnom vremenu fokus je na izvođenju vježbe u stvarnom okruženju kako bi se simulirao sigurnosni incident i provjerile stvarne sposobnosti tima za odgovor na incidente. Ova vrsta vježbe uključuje upotrebu stvarnih sustava, alata i postupaka koji se koriste tijekom odgovora na incidente. Tim za odgovor na incidente i drugi relevantni dionici aktivno sudjeluju u rješavanju simuliranog sigurnosnog incidenta tijekom vježbi u realnom vremenu. Ove vježbe mogu uključivati analizu i detekciju prijetnji, provođenje istrage, suzbijanje napada, obnovu sustava i druge aktivnosti povezane s odgovorom na incidente. Glavni cilj ovog tipa vježbi je testirati stvarne tehničke i operativne

sposobnosti tima za odgovor na incidente, procijeniti učinkovitost postupaka, identificirati područja za poboljšanje te razviti vještine i iskustvo u rješavanju sigurnosnih incidenata u stvarnom okruženju. Zbog prirode ovog tipa vježbi, važno je osigurati da se provode u kontroliranom okruženju kako bi se minimalizirali potencijalni rizici i utjecaj na stvarne poslovne funkcije. Ključ za uspjeh ovakvih vježbi je pravilno planiranje, koordinacija i suradnja s relevantnim dionicima.

Kombinacija vježbi odgovora na sigurnosne incidente koje uključuju vježbe u stvarnom vremenu i vježbe temeljene na raspravi organizacijama omogućuje da istovremeno iskoriste prednosti obiju vrsta vježbi. Kod ovog tipa vježbi sudionici prvo prolaze kroz simulaciju sigurnosnog incidenta u kojoj se aktivno suočavaju s scenarijem u stvarnom vremenu. Nakon toga slijedi rasprava o provedenoj simulaciji, analizi postupaka i donesenim odlukama. Tijekom *live* dijela vježbe, sudionici se suočavaju sa simuliranim sigurnosnim incidentom u stvarnom vremenu, što može uključivati analizu i detekciju prijetnji, donošenje odluka, poduzimanje radnji i komunikaciju unutar tima za odgovor na incidente. Ova faza pruža praktično iskustvo te sudionicima omogućuje primjenu svojih tehničkih vještina i postupaka odgovora na stvarnom scenariju. Nakon *live* dijela vježbe, slijedi rasprava u kojoj sudionici analiziraju i raspravljaju o provedenoj simulaciji. Ova rasprava uključuje pregled postupaka, odluka i radnji koje su poduzete tijekom prvog dijela vježbe. Sudionici dijele svoja iskustva, identificiraju vlastite jake strane te raspravljaju o poboljšanjima planova, postupaka i suradnji unutar tima.

2.2. Faze provođenja vježbi

Vježbe odgovora na kibernetičke incidente sastoje se od nekoliko faza koje pomažu u pripremi, provedbi i evaluaciji vježbe. Faze provođenja svake vježbe su [5]:

- planiranje i priprema
- provedba
- procjena uspješnosti vježbe

U fazi planiranja i pripreme vježbe određuju se ciljevi vježbe, definiraju se scenariji i utvrđuje se obuhvat vježbe. Također, identificiraju se sudionici, definiraju se njihove uloge i odgovornosti te se planira raspored vježbe. Nakon toga slijedi priprema vježbe pri čemu se pripremaju svi potrebni resursi za provedbu, što može uključivati pripremu simulacijskog okruženja, osiguravanje alata i tehnologija te pripremu materijala za sudionike. Pri tome se također najčešće provodi i obuka sudionika o vježbi, informiranje o njezinim ciljevima i iznose se očekivanja od vježbe.

Prilikom provedbe vježbe sudionici aktivno sudjeluju u simulaciji (simulaciji na stvarnim sustavima ako se radi o vježbama u stvarnom vremenu ili raspravi simuliranog scenarija ako se radi o *tabletop* vježbama) sigurnosnog incidenta i provode postupke odgovora na incident na temelju definiranog scenarija vježbe. Sudionici primjenjuju svoje vještine, donose odluke, koordiniraju aktivnosti i komuniciraju unutar tima za odgovor na incidente.

Faza procjene uspješnosti vježbe slijedi nakon same provedbe vježbe. U ovoj se fazi analiziraju rezultati vježbe, provjerava se postizanje ciljeva i procjenjuje se učinkovitost odgovora na sigurnosni incident. Sudionici raspravljaju o provedenoj vježbi, identificiraju snage, slabosti i područja za poboljšanje. Također, prikupljaju se povratne informacije sudionika o njihovom iskustvu i prijedlozima za unapređenje.

Planiranje i priprema vježbe temelje se na trenutnim planovima za odgovor na incidente i predviđenim budućim prijetnjama i trendovima, dok se rezultati procjene uspješnosti koriste kao ulazni podatak za unaprjeđenje planova odgovora na incidente. Unaprjeđenje planova nije faza vježbe, ali je neizostavni korak potreban za unaprjeđenje sposobnosti za odgovor na incidente. Na temelju rezultata procjene, identificiraju i implementiraju se poboljšanja u planovima, postupcima, komunikacijskim kanalima i suradnji unutar tima za odgovor na incidente. Također, osigurava se da naučene lekcije budu primjene u budućim vježbama i stvarnim incidentima.

2.3. Ključne osobe za planiranje vježbe

Jedan od najznačajnijih faktora za uspješno provođenje vježbe je dobro planiranje i definiranje vježbe koje provodi tim za planiranje vježbe. Tim za planiranje vježbe nadzire i snosi odgovornost za utemeljenje, dizajniranje i razvoj vježbe te često i provodi procjenu. Tim određuje ciljeve vježbe, određuje scenarije koji odgovaraju potrebama banke te sastavlja dokumentaciju koja se koristi za procjenu, kontrolu i simulaciju [6]. Članovi tima za planiranje također pomažu u stvaranju i dijeljenju materijala potrebnih prije provođenja vježbe te informiranju i educiranju. Kako su članovi tima za planiranje dosta uključeni i u vježbu idealan su izbor za voditelje vježbe, nadzornike i procjenitelje.

Druge važne uloge za vježbu su sljedeće [6]:

- Sudionici koji reagiraju sukladno predstavljenoj situaciji na osnovu stručnosti za pojedina područja i poznavanja trenutnih planova, procedura i spoznaja dobivena edukacijom i iskustvom.

- Promatrači zaduženi samo za opservaciju vježbe. Promatrači ne sudjeluju u raspravama.
- Voditelji koji su, u idealnim uvjetima, stručne osobe koje olakšavaju raspravu tijekom vježbe. Voditelji su odgovorni za osiguravanje rasprave usredotočene na ciljeve vježbe te istraživanje ključnih problema.
- Sakupljači podataka koji su odgovorni za prikupljanje bitnih podataka koji proizlaze iz rasprava tijekom vježbe. Sakupljači podataka prikupljene podatke kasnije koriste za izvješće nakon vježbe i plan unaprjeđenja.

3. POSTUPAK PLANIRANJA VJEŽBE

U ovom poglavlju razmotriti će se ključni koraci u planiranju vježbi odgovora na sigurnosne incidente. Ključni koraci za planiranje su identificiranje ciljeva vježbe, definiranje i odabir scenarija, definiranje uloga i odgovornosti, planiranje vremenskog okvira, definiranje komunikacijskog plana te planiranje opreme i resursa. Za korak definiranja i odabira scenarija u ovom radu predloženo je korištenje TIBER-EU okvira koji je razvijen kako bi financijske institucije poboljšale kibernetičku otpornost pružajući standardizirani pristup provođenju vježbi etičkih hakiranja.

3.1. Identificiranje ciljeva vježbe

Prvi korak u planiranju vježbe je identifikacija i definiranje ciljeva vježbe. Ova faza je ključna jer će ostatak vježbe biti usmjeren prema postizanju definiranih ciljeva. Svrha identificiranja i definiranja ciljeva vježbe je da kreditna institucija jasno definira što želi postići vježbom i koja područja želi testirati. Ciljevi bi trebali biti jasni, mjerljivi i relevantni. Ciljevi bi također trebali biti u skladu s općim ciljevima banke za upravljanje sigurnošću.

Kako je i detaljnije opisano u prethodnom poglavlju, ciljevi vježbe mogu biti sljedeći [5]:

- Procjena planova i odgovora na incidente.
- Edukacija kako bi svi sudionici bili svjesni plana i svojih odgovornosti te kako bi lakše i učinkovitije provodili odgovor na incidente.
- Testiranje trenutno uspostavljenih procedura i procesa.

Pored navedenih ciljeva, provođenje vježbi utječe na poboljšanje suradnje i komunikacije između sudionika vježbe, najčešće različitih organizacijskih jedinica financijske institucije ili financijske institucije i vanjskih organizacija koje sudjeluju u odgovorima na incidente. Vježbe često imaju više od jednog cilja koji su većim dijelom utvrđeni na osnovu cjelokupne zrelosti informacijskog sustava. Cilj vježbi utječe na odabir tipa vježbe, a tablica 1 može poslužiti za odabir tipa vježbe na osnovu definiranih ciljeva.

Tablica 1. Povezanost ciljeva vježbi i tipova vježbi

Cilj	**Tip vježbe**
Procjena novih planova	Vježbe temeljene na raspravi *Tabletop*
Edukacija	Vježbe temeljene na raspravi *Tabletop* Vježbe u realnom vremenu
Provjera valjanosti postojećih planova	*Tabletop* Vježbe u realnom vremenu

Identificiranje ciljeva vježbe ključno je za uspješno planiranje i provedbu vježbe odgovora na sigurnosni incident. Ciljevi vježbe trebaju biti jasno definirani kako bi se osiguralo da svi sudionici razumiju što se očekuje od njih tijekom vježbe i kako bi se pravilno testirala sposobnost otkrivanja, prijave i odgovora na sigurnosni incident.

3.2. Definiranje i odabir scenarija

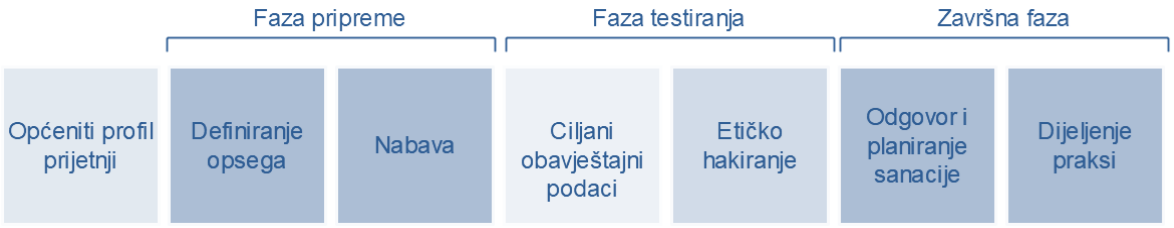
Nakon što su ciljevi vježbe definirani, potrebno je definirati i odabrati scenarij za vježbu. Scenarij treba biti relevantan za financijsku instituciju i obuhvaćati sigurnosni incident koji bi mogao imati utjecaj na poslovanje. Financijska institucija također bi trebala razmotriti mogućnost korištenja scenarija koji uključuje više različitih vrsta sigurnosnih prijetnji kako bi se testirale različite sposobnosti odgovora na incident. Pri odabiru scenarija važno je osigurati da je scenarij usklađen s ciljevima vježbe i sposobnostima financijske institucije za rješavanje incidenata. Scenarij također treba biti dovoljno realističan kako bi vježba zaista bila korisna i relevantna za sudionike. Scenariji za vježbe odgovora na kibernetičke incidente ponekad se nazivaju i vinjete (engl. *vignette*).

Za definiranje što realističnijih scenarija koji odgovaraju stvarnim prijetnjama i ranjivostima sustava moguće je koristiti rezultate modeliranja prijetnji (engl. t*hreat modelling*). Također, modeliranje prijetnji može pomoći u određivanju uloga i odgovornosti tijekom vježbe, što je

sljedeći korak pri planiranju vježbe. Osim toga, profil prijetnji može pomoći u definiranju prioritetnih akcija koje treba poduzeti u slučaju sigurnosnog incidenta.

Kako planiranje vježbe na ovaj način može značiti značajno povećanje resursa potrebnih za planiranje, može se koristiti proces predložen TIBER-EU okvirom, koji prvo nalaže korištenje općenitijeg profila prijetnji za bankarski sektor za zemlju u kojoj se testiranje provodi, a zatim, na osnovu tih informacija, definiranje opsega, pa nakon toga izradu ciljanih obavještajnih izvješća o kibernetičkim prijetnjama (engl. *Threat Intelligence,* TI) koja će sadržavati relevantne scenarije. TIBER-EU okvir temelji se na skupu standarda i smjernica koje je razvila Europska središnja banka (engl. *European Central Banke*, ECB) u suradnji s nacionalnim središnjim bankama i drugim financijskim institucijama kako bi pomogla financijskim institucijama poboljšati svoju kibernetičku otpornost pružajući standardizirani pristup provođenju vježbi etičkih hakiranja. Kako TIBER-EU okvir definira standardizirani način za provođenje vježbi etičkih hakiranja, definira i način identifikacije realnog i vjerojatnog scenarija incidenta, pa se na isti način mogu definirati scenariji za vježbu odgovora na kibernetičke incidente.

Slika 1 prikazuje TIBER-EU proces, kod kojega se u prvom koraku koristi općeniti profil prijetnji, nakon čega se definira opseg, a zatim provodi ciljani obavještajni rad o kibernetičkim prijetnjama.



Slika 1. TIBER-EU proces [7]

Općeniti profil prijetnji uključuje općenitu procjenu prijetnji za financijski sektor i specifičnu banku koja će provoditi vježbu te identificirane relevantne visokorizične aktere.

Pružatelji platnih usluga trebali bi klasificirati utvrđene poslovne funkcije, procese za podršku i informacijska sredstva prema njihovoj kritičnosti [8]. U scenariju je poželjno simulirati incidente koji zahvaćaju kritične funkcije za poslovanje banke, ali i drugi nekritični sustavi mogu biti uključeni. Kritične funkcije su definirane kao ljudi, procesi i tehnologije potrebne kako bi banka nastavila isporučivati ključne usluge koje bi u slučaju prekida mogle

imati štetni učinak na financijsku stabilnost, sigurnost entiteta i klijenata te njihovih postupaka na tržištu [9].

Na primjer, neke od kritičnih funkcija između ostalih mogu biti:

- Polaganje depozita i štednje
- Usluge posuđivanja i kreditiranja
- Investicije i tržište kapitala
- Tržišta veleprodajnog financiranja
- Plaćanja, kliring, usluge skrbništva i namire

Svaka od kritičnih funkcija može imati potkategorije, kako i prikazuje tablica 2.

Tablica 2. Primjer kritične funkcije i pripadajućih potkategorija

Kritična funkcija	**Potkategorija**	**Obrazloženje za uključivanje u vježbu**
Polaganje depozita i štednje	Tekući računi	Prihvat depozita i usluge štednje osnovna su funkcija stvarne ekonomije, a bilo kakvo narušavanje sigurnosti tih usluga imalo bi štetan utjecaj na bazu korisnika. U slučaju incidenta korisnici prihvatitelja depozita mogu izgubiti neposredan pristup svojim depozitima i stoga neće biti u mogućnosti izvršiti plaćanja. U slučaju incidenta kod značajnog prihvatitelja depozita, rezultirajući manjak likvidnosti mogao bi imati ozbiljne negativne učinke na aktivnost u široj ekonomiji.
	Štedni računi	
	Internetsko bankarstvo	
	Debitne kartice	
	Gotovinske kartice	
	Kreditne kartice	

Nakon odabira kritične funkcije potrebno je identificirati sustave koji će biti uključeni u vježbu, a primjer odabira prikazuje tablica 3. Identifikaciju je moguće napraviti iz popisa

imovine koji prema EBA smjernicama treba sadržavati međuovisnost imovine kako bi se pomoglo u odgovoru na sigurnosne i operativne incidente, uključujući kibernapade [4].

Tablica 3. Primjer kritične funkcije i povezanih sustava

Kritična funkcija ili potkategorija	**Ime sustava**	**Obrazloženje za uključivanje u vježbu**
Štednja i polaganje depozita – Internet bankarstvo	Baza podataka	Unutar polaganja depozita i usluga štednje koje banka pruža, internetsko bankarstvo za maloprodajne korisnike je osnovna funkcija koja služi stvarnoj ekonomiji, a bilo kakvo narušavanje ove usluge bi imalo štetan utjecaj na bazu korisnika.
	Analitika	
	Front-end - Investicije	
	Front-end - Plaćanja	
	Prijava	
	Middleware	

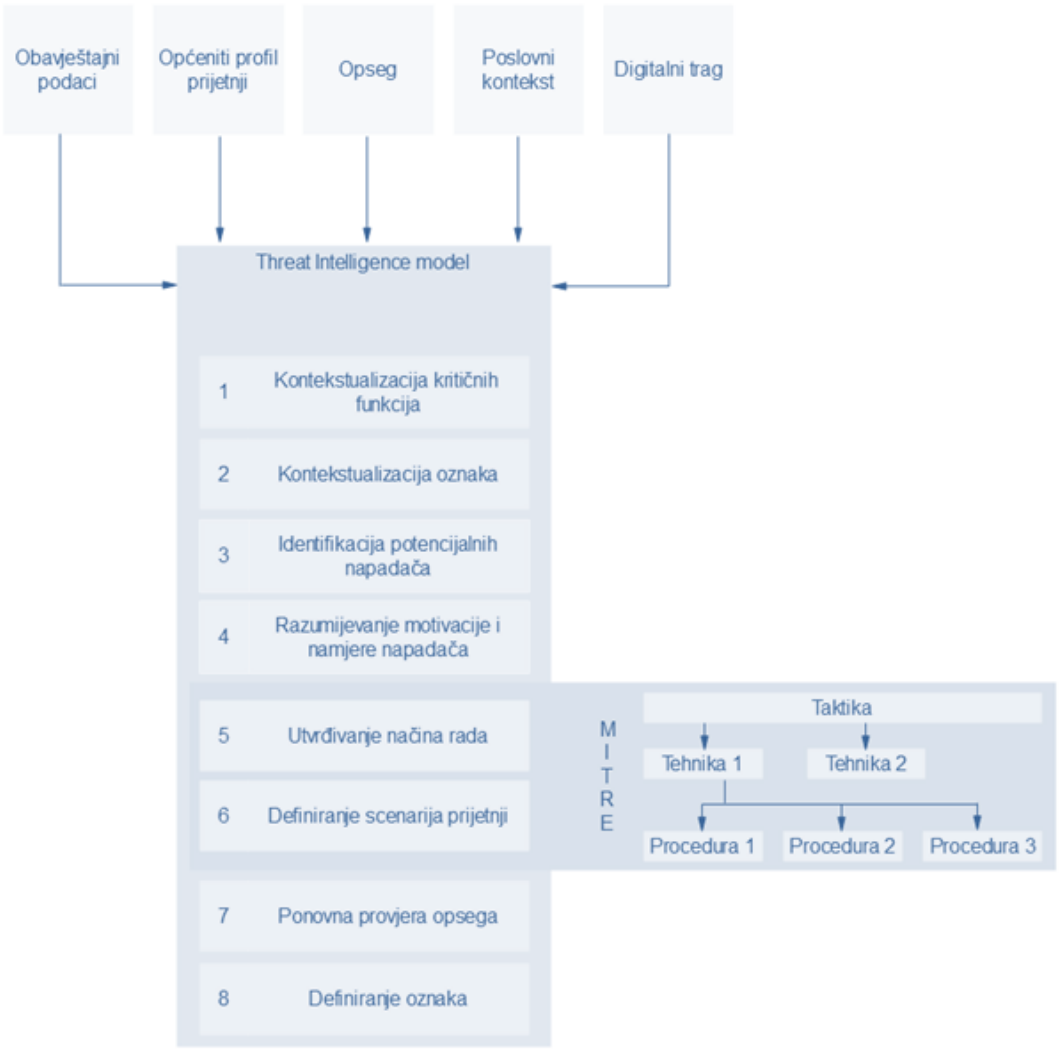
Nakon odabira kritične funkcije i identificiranih sustava potrebno je analizirati sustave i servise te definirati potencijalne ciljeve koje bi potencijalni napadač mogao pokušati ostvariti.

Definiranje potencijalno ostvarivih ciljeva sa sobom povlači razmatranje primarnih rizika za poslovanje koji bi mogli proizaći iz kompromitacije sustava ili servisa. Tablica 4 prikazuje primjer definiranih ciljeva.

Tablica 4. Definirani ciljevi

Kritična funkcija	Polaganje depozita i štednje
Odredišni sustav/Ime servisa	Internet bankarstvo koje se sastoji od baze podataka, *middlewarea*, aplikacijskih servera itd.
Kategorija prijetnje (povjerljivost, integritet ili dostupnost)	Integritet
Opis sustava/servisa	Središnji bankarski sustav
Potencijalni cilj	Mogućnost iniciranja neautoriziranog prijenosa sredstava

Nakon prikupljenih informacija iz prethodnih koraka te dodatno podataka o poslovanju institucije i digitalnog traga (engl. *footprint*) moguće je prikupiti ulazne podatke o prijetnjama te nakon toga modelirati prijetnje i identificirati scenarij. Prema TIBER *Threat Inelligence* modelu modeliranje i identifikacija provodi se u osam koraka, kako prikazuje slika 2.



Slika 2. TIBER *Threat Inelligence* model [10]

Kontekstualizacija kritičnih funkcija

U ovom koraku identificiraju se kritične funkcije, a njihova kritičnost procjenjuje se u smislu utjecaja na cjelokupno poslovanje financijske institucije. Ova faza uključuje pregled poslovnih procesa, identifikaciju kritičnih točaka, procjenu rizika i prijetnji, kao i razmatranje regulatornih zahtjeva. Uspješna kontekstualizacija kritičnih funkcija osigurava da se vježba usredotoči na najkritičnije aspekte poslovanja i omogućuje pravilno testiranje sposobnosti institucije da odgovori na napade usmjerene na ključne funkcije.

Kontekstualizacija oznaka

Ovaj korak odnosi se na dodavanje specifičnih informacija o načinu koji bi napadač planirao upotrijebiti kako bi kompromitirao kritične funkcije te povezane sustave i servise te time postigao ciljeve. Na primjer, dodatne informacije mogu biti dobivene iz profila zaposlenika na

društvenim medijima ili obavještajni podaci o kibernetičkim prijetnjama mogu otkriti ranjivosti povezanih sustava i servisa. Ove informacije mogu se iskoristiti kako bi se proveo uspješan napad.

Oznake se koriste kao upozorenja na moguće incidente i važno je da se uzmu u obzir prilikom planiranja vježbe odgovora na incidente kako bi se osiguralo da se kritični resursi u instituciji zaštite na pravilan način.

Identificiranje prijetnji i razumijevanje motivacije i namjere napadača

Cilj ovog koraka je identificirati potencijalne napadače i razumjeti njihove motive i namjere. U tu svrhu, moraju se detaljno analizirati mogući napadači i njihove karakteristike, kao što su vrsta organizacije, financijski kapaciteti, stručnost, dostupnost alata, ideologija, politički motivi, kriminalna povijest, itd. Osim toga, treba razumjeti kako bi napadači mogli iskoristiti određene ranjivosti, koja bi bila ciljana područja napada te kako bi se taj napad mogao izvesti. Na kraju, sve informacije treba integrirati u cjelokupnu procjenu prijetnji kako bi se razumjelo koje su prijetnje najvažnije i kako bi se mogli izraditi učinkoviti planovi za njihovo sprečavanje ili ublažavanje njihovih posljedica.

Analiza mora biti temeljena na dokazima i mora sadržavati dobru analizu motivacije i namjere. Tijekom ovog koraka mogu se mapirati potencijalni napadači i kritične funkcije zajedno s motivima i namjerama, kako prikazuje tablica 5.

Tablica 5. Primjer potencijalnih napadača i potencijalne ciljane kritične funkcije sa pripadajućim motivima i namjerama

Potencijalna napadačka skupina	**Upravljanje imovinom**	**Procesiranje plaćanja**	**Procesiranje osobnih podataka**
TA-505 (Organizirana kriminalna skupina)	Financijski dobitak – Krađa financijskih sredstava	Financijski dobitak – Transfer imovine prevarantu	Financijski dobitak – Krađa i prodaja osobnih podataka
Cobalt group/Money taker/ FIN7 (Organizirana kriminalna skupina)	Financijski dobitak – Krađa financijskih sredstava, Krađa i prodaja ili iskorištavanje osjetljivih podataka o tržištu	Financijski dobitak – Krađa financijskih sredstava	Financijski dobitak – Krađa i prodaja osobnih podataka
APTxx (organizacija sufinancirana od strane države)	Špijunaža – Krađa povjerljivih informacija		Špijunaža – Nadzor protivnika

Utvrđivanje načina rada

Ova aktivnost uključuje analizu metoda i postupaka koje bi napadač mogao koristiti kako bi iskoristio ranjivosti u instituciji te izazvao štetu. U ovom koraku, stručnjaci za sigurnost provode analizu općih tehnika i alata koji su često korišteni u sličnim napadima, kao i tehnike koje su specifične za ciljanu napadačku skupinu. Ovo uključuje identifikaciju vrsta napada koje bi mogle biti korištene, kao što su *phishing*, raspodijeljeni napad uskraćivanja usluge (engl. *Distributed Denial of Service*, DDoS), krađa identiteta i sl. Također, procjenjuju se scenariji napada, uključujući načine na koje bi napadač mogao kompromitirati sustave, mreže i podatke. Važno je da se u ovom koraku napravi detaljna analiza taktika, tehnika i procedura (engl. *Tactics, Techniques, and Procedures*, TTP) koje bi napadač koristio, a pri tome je za modeliranje preporučljivo koristiti MITRE ATT&CK radni okvir. U ovom koraku trebaju se mapirati kritične funkcije, ciljevi/oznake i napadačke skupine sa taktikama, tehnikama i procedurama koje bi najvjerojatnije bile iskorištene u stvarnom napadu. Tablica 6 prikazuje primjer ovakvog mapiranja.

Tablica 6. Primjer mapiranja kritičnih funkcija, ciljeva/oznaka i napadačkih skupina sa taktikama, tehnikama i procedurama

Napadačka skupina	**Cilj/oznaka**	**Taktika**	**Tehnika**	**Procedura**
APTxx (organizacija sufunancirana od strane države)	Eksfiltracija osjetljivih podataka	Eksfiltracija	Automatizirana eksfiltracija	Machete USBStealer

Konačni cilj ovog koraka je razumijevanje načina na koji bi se napadač mogao pokušati infiltrirati u instituciju te načina na koji bi izveo napad. Timu za sigurnost je na ovaj način omogućeno da unaprijed analizira i pripremi obranu protiv tih tehnika i alata, a financijskoj je instituciji omogućeno da se pripremi na odgovor za potencijalni incident izvršen identificiranim tehnikama i alatima.

Definiranje scenarija prijetnji

Na osnovu informacija prikupljenih tijekom analize potrebno je dokumentirati scenarije prijetnji. Scenariji trebaju biti definirani na osnovu obavještajnih podataka i temeljeni na dokazima, a trebaju elaborirati i motive napadačke skupine. Scenariji prijetnji ne bi se trebali temeljiti samo na povijesnim podacima. Pri izradi scenarija potrebno je razmišljati o tome gdje će se prijetnja pojaviti i koje će nove pristupe napadač istražiti i pokušati iskoristiti. Također, potrebno je uzeti u obzir sljedeće:

- sofisticiranost tehnika koje će napadač koristiti
- agilnost napadača (tj. kojom brzinom će se napadač prilagoditi promjenjivim okolnostima i kako će to učiniti)
- koliko su napadači usmjereni prema svom krajnjem cilju (tj. idu li izravno prema kritičnoj funkciji ili prvo ostvaruju široko prisustvo u mreži i/ili lutaju u potrazi za prilikama)
- njihovo znanje o financijskom sektoru, funkcijama i korištenim sustavima (tj. jesu li prije ciljali financijski sektor ili slične sustave)

Pri izradi scenarija preporuča se korištenje MITRE ATT&CK okvira.

Na temelju prikupljenih obavještajnih informacija potrebno je napraviti popis nacrta scenarija prijetnji koji su ocijenjeni na temelju sposobnosti napadača i namjere. O tim scenarijima bi nakon toga trebao raspraviti tim za organizaciju vježbe, koji nakon rasprave treba i odabrati scenarije za vježbu odgovora na incidente.

Na temelju prethodno izrađenih izvješća i scenarija prijetnji, potrebno je ponovno provjeriti specifikaciju opsega i po potrebi je revidirati (uključujući oznake).

3.3. Definiranje uloga i odgovornosti

Sljedeći korak u planiranju vježbe, nakon odabira scenarija za vježbu odgovora na sigurnosni incident, jest definiranje uloga i odgovornosti sudionika. Ovaj korak uključuje identificiranje svih osoba koje će sudjelovati u vježbi te dodjelu specifičnih uloga i odgovornosti svakoj osobi.

Uloge i odgovornosti koje su potrebne u vježbi ovise o vrsti organizacije i scenariju koji se koristi. U nekim slučajevima, mogu biti potrebne različite vrste timova za upravljanje incidentom, kao što su timovi za tehničku podršku, komunikaciju s javnošću i koordinaciju. Tablica 2.7. prikazuje uobičajene sudionike vježbe, a temeljena je na osnovi prethodno provedenih vježbi provedenih u drugim sektorima.

Tablica 7. Uobičajeni sudionici vježbi [5]

Interni sudionici	**Vanjski sudionici**
- Poslovni vlasnik - Član uprave - Zaposlenici odjela fizičke sigurnosti - Zaposlenici odjela IT podrške - Tim za odgovor na kibernetičke incidente - Zaposlenici odjela odnosa s javnošću - Zaposlenici odjela komunikacija - Zaposlenici pravnog odjela	- Dobavljači - Konzultanti za informacijsku sigurnost

Svaka osoba mora imati jasno definiranu ulogu i odgovornost kako bi se osigurala učinkovita suradnja i koordinacija u rješavanju incidenta. Također, važno je osigurati da su uloge i odgovornosti razumljive za sve sudionike vježbe.

3.4. Planiranje vremenskog okvira

Planiranje vremenskog okvira četvrti je korak u planiranju vježbe odgovora na sigurnosni incident. Ovaj korak uključuje određivanje vremena potrebnog za pripremu, provedbu i evaluaciju vježbe te planiranje vremena za obuku sudionika.

Vremenski okvir za vježbu mora biti realističan i treba uzeti u obzir sve važne faktore kao što su raspoloživost sudionika, vrijeme za pripremu, vrijeme za provedbu vježbe te vrijeme za evaluaciju i izvještavanje. Također, ako se radi o vježbi u kojoj se procjenjuju novi planovi odgovora na incidente važno je uzeti u obzir koliko je vremena potrebno za obuku sudionika.

Određivanje vremenskog okvira za provedbu vježbe može pomoći u osiguravanju učinkovite provedbe. Tablica 8 prikazuje primjer vremenskog plana provedbe vježbe u kojoj se provodi vježba za više scenarija, odnosno provodi se za više vinjeta. Vremena u scenariju potrebno je prilagoditi sadržaju, a prilikom izvođenja vježbe bitno je osigurati da se rasprava tijekom vježbe prekida samo kada je nužno, kako bi sudionici imali dovoljno vremena za dubinsku analizu i donošenje odluka na osnovu analize.

Tablica 8. Primjer vremenskog plana provedbe vježbe

Aktivnost	**Vrijeme**
Prijava	8:00 – 8:30
Otvaranje vježbe (dobrodošlica, uvod i smjernice)	8:30 – 9:00
Vinjeta I	9:00 – 9:30
Vinjeta II	9:30 – 10:05
Pauza	10:05 – 10:20
Vinjeta III	10:20 – 10:55
Vinjeta IV	10:55 – 11:30
Zatvaranje vježbe (dojmovi i kratka analiza)	11:30 – 12:00

3.5. Komunikacijski plan

Peti korak u planiranju vježbe odgovora na sigurnosni incident izrada je komunikacijskog plana. Komunikacijski plan opisuje način na koji će sudionici vježbe međusobno komunicirati tijekom vježbe, kao i način na koji će se simulirati obavijesti prema vanjskim stranama (npr. mediji, partneri i klijenti), ako je to potrebno.

Komunikacijski plan obično uključuje sljedeće elemente:

- popis sudionika: treba navesti sve sudionike vježbe i njihove kontakte. To uključuje osobe koje su dio tima za upravljanje incidentom, kao i druge sudionike poput poslovnih partnera ili regulatora.
- vrste komunikacije: plan bi trebao definirati vrste komunikacije koje će se koristiti tijekom vježbe. To može uključivati direktnu komunikaciju, telefonske pozive, e-poštu, interne sustave za razmjenu poruka, video konferencije i druge oblike komunikacije.

Izrada komunikacijskog plana pomaže u osiguravanju učinkovite i koordinirane komunikacije tijekom vježbe. Ovime se osigurava da svi sudionici imaju pravovremen pristup relevantnim informacijama.

3.6. Planiranje opreme i resursa

Šesti je korak u planiranju vježbe odgovora na sigurnosni incident je planiranje opreme i resursa. Ovaj korak uključuje provjeru postoje li resursi potrebni za provedbu vježbe, kao i provjeru opreme, sustava i infrastrukture koja će se koristiti tijekom vježbe.

Prilikom provjere potrebno je razmotriti sljedeće elemente:

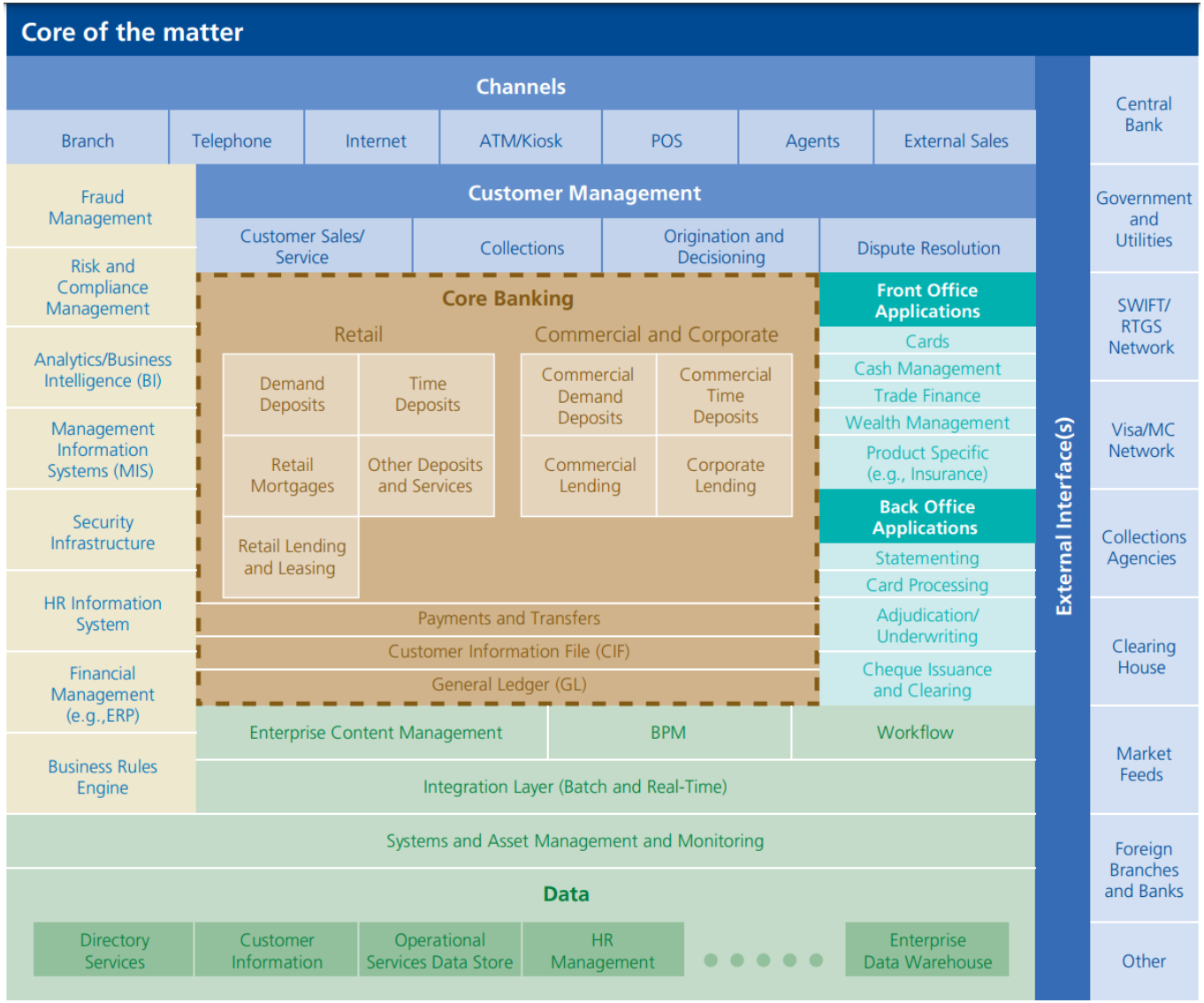
- Oprema: potrebno je provjeriti jesu li svi potrebni uređaji dostupni i ispravni za upotrebu tijekom vježbe.
- Komunikacijska infrastruktura: potrebno je provjeriti jesu li svi komunikacijski sustavi, uključujući telefonske linije, internetsku vezu, internu mrežu i druge relevantne sustave, funkcionalni i dostupni tijekom vježbe.
- Članovi tima: potrebno je provjeriti jesu li svi potrebni članovi prisutni i spremni za sudjelovanje u vježbi. Također potrebno je provjeriti jesu li svi članovi upoznati s njihovim zadacima i odgovornostima.
- Prostori: potrebno je provjeriti jesu li svi potrebni prostori dostupni i spremni za upotrebu tijekom vježbe. Ovo uključuje provjeru radnih mjesta, soba za sastanke, dvorane za obuku ili drugih potrebnih prostora. *Tabletop* vježbe većinom se provode u dva tipa formata: grupirani i plenarni [11]. Prilikom izvođenja u grupiranom formatu potrebno je formirati nekoliko grupa koje sjede za različitim stolovima pri čemu svaka grupa nakon što je scenarij prezentiran razmatra svoje aktivnosti na osnovu pravila, politika i procedura. Ukoliko vježba uključuje nekoliko vinjeta, grupe se po potrebi ponovo raspoređuju tijekom plenarne sjednice koja slijedi nakon zaključka svake vježbe. Prilikom izvođenja u plenarnom formatu svi sudionici vježbe nalaze se u istom prostoru, bez predviđenog vremena za rasprave u manjim grupama, a komentari i preporuke dijele se sa svim sudionicima vježbe.
- Tehnologija: potrebno je provjeriti jesu li svi relevantni tehnološki sustavi, poput softverskih aplikacija, baza podataka, sigurnosnih sustava i drugih tehnologija, dostupni i ispravni za upotrebu tijekom vježbe.

4. PRIMJER PRIPREME SCENARIJA ZA VJEŽBU

U ovom poglavlju prema prethodno opisanom postupku biti će definiran scenarij za vježbu koji će nakon toga biti razrađen i pripremljen za provođenje vježbe. Kako je prethodno opisano, prvi korak za definiranje realnog scenarija jest odabir prijetnji iz generičkog profila prijetnji. Generički profil prijetnji preuzet je za bankarski sektor, a prikazuje ga slika 3.

Slika 3. Najznačajnije prijetnje u bankarskom sektoru [12]

Za potrebe ovog rada korištena je referentna arhitektura za financijske institucije u svrhu općenitog pregleda servisa u bankarskom sektoru. Prilikom izrade scenarija svaka financijska institucija sustave treba identificirati iz popisa imovine i njihove međuovisnosti.



Slika 4. Primjer arhitekture bankarskog sustava [13]

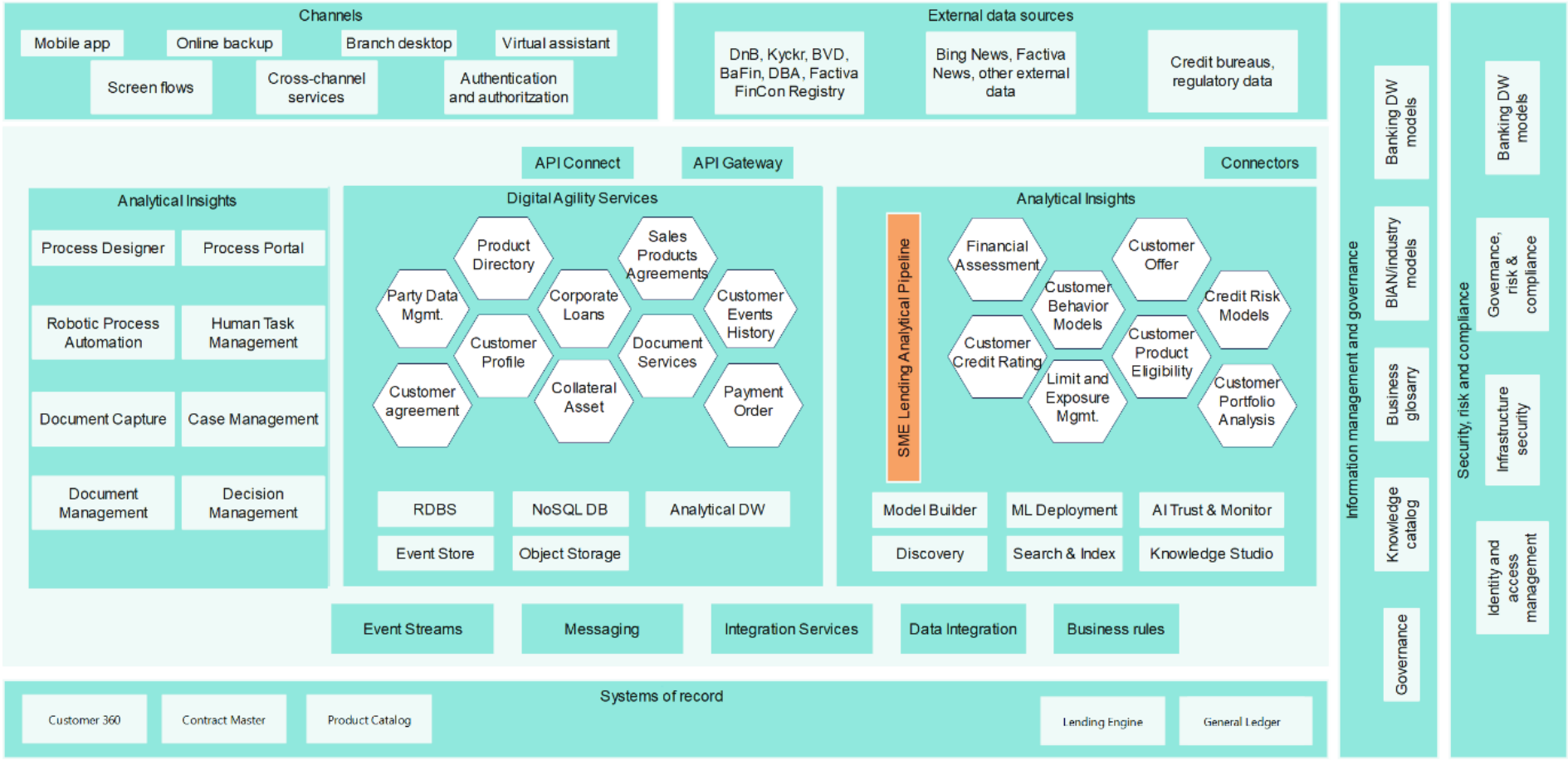
4.1. Definiranje scenarija

Za potrebe ovog rada bit će korištene odabrane kritične funkcije s EBA predloška za definiranje kritičnih funkcija [14]. Scenarij će biti definiran za kritičnu funkciju „Usluge posuđivanja i kreditiranja“, zajedno s pripadajućim potkategorijama kako prikazuje tablica 9.

Tablica 9. Kritična funkcija i potkategorija za definiranje scenarija

Kritična funkcija	**Potkategorija**	**Obrazloženje za uključivanje u vježbu**
Usluge posuđivanja i kreditiranja	Hipotekarni stambeni krediti	Prihvat depozita i usluge štednje su osnovna funkcija stvarne ekonomije, a bilo kakvo narušavanje sigurnosti tih usluga imalo bi štetan utjecaj na bazu korisnika. U slučaju incidenta korisnici prihvatitelja depozita mogu izgubiti neposredan pristup svojim depozitima i stoga neće biti u mogućnosti izvršiti plaćanja. U slučaju incidenta kod značajnog prihvatitelja depozita, rezultirajući manjak likvidnosti mogao bi imati ozbiljne negativne učinke na aktivnost u široj ekonomiji.
	Drugi zajmovi	
	Kreditiranje malih ili srednjih poduzeća (SME)	
	Kreditiranje velikih poduzeća	

Za kritičnu funkciju odabrana je potkategorija „Kreditiranje malih i srednjih poduzeća“ te će daljnja analiza biti usmjerena na ovu potkategoriju. Arhitekturu servisa koji podržava odabranu kritičnu funkciju prikazuje slika 5., dok tablica 10 sadrži popis najvažnijih sustava ovog servisa.



Slika 5. Arhitektura servisa za posuđivanje i kreditiranje malih i srednjih poduzeća [15]

Kako je vidljivo u prikazu arhitekture servisa za posuđivanje i kreditiranje malih i srednjih poduzeća, servis se sastoji od brojnih komponenti, a najvažnije komponente te komponente s najvećom izloženošću i rizikom biti će odabrane tijekom analize.

Tablica 10. Sustavi povezani s odabranom kritičnom funkcijom

Kritična funkcija ili potkategorija	**Ime sustava**	**Obrazloženje za uključivanje u vježbu**
Usluge posuđivanja i kreditiranja	Sustav za autentifikaciju i autorizaciju klijenata	Unutar polaganja depozita i usluga štednje koje banka pruža, internetsko bankarstvo za maloprodajne korisnike osnovna je funkcija koja služi stvarnoj ekonomiji, a bilo kakvo narušavanje ove usluge imalo bi štetan utjecaj na bazu korisnika.
	Front-end applikacija za djelatnike poslovnica – Izdavanje kredita	
	Internet bankarstvo	
	Sustavi za automatizaciju	
	Middleware	
	Centralni bankarski sustav	
	Baza klijenata, proizvoda i ugovora	
	Centralni bankarski sustav (modul za kreditiranje)	
	Sustav za analitiku	
	Integracija s drugim Front-office aplikacijama (npr. upravljanje kampanjama, prodaja itd.)	

Kako bi se odredili potencijalni ciljevi potrebno je razmotriti rizike za informacijsko-komunikacijske tehnologije i sigurnosne rizike. Financijske institucije trebale bi utvrditi rizike IKT-a i sigurnosne rizike koji utječu na utvrđene i klasificirane poslovne funkcije, podržavajuće procese i informacijsku imovinu, u skladu s njihovom kritičnošću. Ta bi se procjena rizika trebala provoditi i dokumentirati na godišnjoj osnovi ili u kraćim razmacima, ako je to potrebno [4]. Rezultati procjene rizika mogu se koristiti za određivanje potencijalnih ciljeva prilikom kibernetičkog napada.

Kako se u ovom radu analiza provodi na osnovi općenitog primjera, a za procjenu rizika potrebno je analizirati stvarne procese, poslovne funkcije i imovinu, rizik je definiran na osnovu činjenice da velik broj tradicionalnih financijskih institucija još uvijek koristi zastarjele centralne sustave [16]. Na osnovu ove činjenice temelji se pretpostavka da ovi sustavi imaju više kritičnih ranjivosti ili da su instalirani na zastarjelim operativnim sustavima s otkrivenim ranjivostima za koje ne postoje zakrpe kako prikazuje tablica 11.

Tablica 11. Definirani ciljevi

Kritična funkcija	Usluge posuđivanja i kreditiranja
Odredišni sustav/Ime servisa	Modul za kreditiranje unutar centralnog bankarskog sustava
Kategorija prijetnje (povjerljivost, integritet ili dostupnost)	Dostupnost
Opis sustava/servisa	Središnji bankarski sustav
Potencijalni cilj	Kriptiranje svih podataka

Kreditiranje može biti kritična funkcija ako se likvidnost i poteškoće u financiranju za mala ili srednja poduzeća dogode prije nego što pronađu alternativne izvore kredita. Stvarna ekonomija ovisi o redovnom protoku kredita te incident u kreditnoj instituciji može izložiti zajmoprimce kratkoročnim i dugoročnim ograničenjima likvidnosti. Sposobnost zajmoprimaca za prilagodbu neuspjeha banke u izdavanju zajmova i kreditiranju ovisit će o uvjetima pod kojima posuđuju i mogućnosti pronalaženja alternativnih izvora. Ova situacija za kreditnu instituciju može uzrokovati smanjenje prihoda, reputacijsku štetu te gubitak klijenata.

LockBit ransomware grupa odgovorna je za više od trećine ransomware napada tijekom druge polovice 2022. godine [17]. Atento, tvrtka za upravljanje odnosima s klijentima, u svom izvještaju o financijskom poslovanju objavljenom 2021. godine prikazala je utjecaj napada od strane LockBit grupe u iznosu od 42,1 milijuna dolara. Kako je vrlo vjerojatno broj organizacija napadnutih od strane LockBit grupe puno veći, ukupni financijski gubitak uzrokovan zlonamjernim djelovanjem LockBita može premašiti milijarde dolara. Dok je zadnja verzija LockBit 3.0 ciljala Windows, Linux i VMware ESXi servere, navodno su identificirane nove

verzije LockBit-a koje mogu utjecati i na macOS, ARM, FreeBSD, MIPS i SPARC procesore. S obzirom na značajnu količinu napada ove grupe, broj ciljanih uređaja vjerojatno će se nastaviti povećavati, što bi moglo rezultirati značajnim porastom napada LockBit-a. Grupa cilja brojne zemlje, među kojima je i Hrvatska, a uloženi napori u razvoj zloćudnog koda u svrhu proširenja broja odredišnih sustava ukazuje na povećanu opasnost za sve institucije, a među njima i financijski sektor koji je jedan od ciljanih sektora za ovu grupu.

Tablica 12. Motivi i namjere potencijalnog napadača

Potencijalni napadač	**Povjerljivi podaci**
Bitwise Spider ili LockBitSUpp,StealBit,LockBit (Organizirana kriminalna skupina)	Financijski dobitak – Krađa i prodaja osobnih podataka
Labyrinth Chollima (Organizirana kriminalna skupina)	Financijski dobitak – Krađa i prodaja osobnih podataka

LockBit ransomware grupa prilikom napada koristi taktike i tehnike navedene u tablici, a tehnike označene narančastom bojom u tablici najvjerojatnije su za izvršavanje napada za definirano okruženje.

Tablica 13. Taktike i tehnike potencijalnog napadača [17][18]

Taktika	**Tehnika**	**MITRE ID**
Initial Access	Valid Accounts	T1078
	Exploit External Remote Services	T1133
	Drive-by Compromise	T1189
	Exploit Public-Facing Application	T1190
	Phishing	T1566
Execution	Software Deployment Tools	T1072
	Valid Accounts	T1078
Persistence	Boot or Logo Autostart Execution	T1547
	Obfuscated Files or Information	T1027
Privilege Escalation	Indicator Removal: File Deletion	T1070.004
	Execution Guardrails: Environmental Keying	T1480.001
Defense Evasion	OS Credential Dumping: LSASS Memory	T1003.001
	Network Service Discovery	T1046
	System Information Discovery	T1082
Credential Access	System Location Discovery: System Language Discovery	T1614.001
Discovery	Remote Services: Remote Desktop Protocol	T1021.001
	Application Layer Protocol: File Transfer Protocols	T1071.002
	Protocol Tunnel	T1572
Lateral Movement	Exfiltration	TA0010
Command and Control	Exfiltration Over Web Service	T1567
	Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002
Exfiltration	Data Destruction	T1485
	Data Encrypted for Impact	T1486
	Service Stop	T1489
Impact	Inhibit System Recovery	T1490
	Defacement: Internal Defacement	T1491.001

Na osnovu prethodne analize scenarij može biti sljedeći:

- U svrhu financijske dobiti napadačka skupina LockBit pokušava doći do povjerljivih informacija financijske institucije kako bi ih prodala na crnom tržištu te dodatno i potencijalno zaradila od otkupnine ukoliko ju financijska institucija pristane platiti.
- Napadačka skupina prije početka napada radi izvide skeniranjem mreže i prikupljanjem informacija o financijskoj instituciji te ne otkriva potencijalno iskoristive ranjivosti na servisima izloženim na internetu. Skeniranje se provodi sporo tijekom prva tri tjedna napada i sustavi banke nisu u mogućnosti detektirati povećanu aktivnost skeniranja s interneta.
- Napadačka skupina odlučuje se provesti napad preko dobavljača te zaposlenicima dobavljača šalje *phishing* poštu i nakon kompromitiranja sustava dobavljača banci šalje *phishing* poštu sa malicioznim privitkom. Nakon što je jedan od zaposlenika otvorio zlonamjerni prilog e-pošte zlonamjerni softver je pokrenut, a napadači su dobili pristup sustavu.
- Zlonamjerni kod koristi Mimikatz za prikupljanje dodatnih korisničkih računa i propagaciju. Također, koristi se Advanced Port Scanner za skeniranje mreže radi pronalaska odredišnog sustava. Nakon pronalaska odredišnog sustava napadači koriste Cobalt Strike za lateralno kretanje. Nakon spajanja na odredišni sustav napadači koriste StealBit zloćudni program za eksfiltraciju podataka i na kraju kriptiraju sav sadržaj servisa za kreditiranje malih i srednjih poduzeća.

4.2. Priprema scenarija za vježbu

Nakon što je definiran realan scenarij, potrebno ga je detaljnije raspisati i pripremiti za provođenje vježbe. Prethodno navedeni scenarij biti će podijeljen u dva modula vježbe kako bi se ciljano evaluirali određeni aspekti odgovora na incident i identificirale potrebe za dodatnom edukacijom ili doradom procesa. Također, podjela će omogućiti lakšu organizaciju u izvođenje vježbe.

Kako bi se osiguralo lakše razumijevanje događaji tijekom incidenta prikazani su u Gant dijagramu u Tablica 14, dok su detalji događaja i predložena pitanja za voditelja vježbe opisani u sljedećim potpoglavljima.

Tablica 14. Prikaz događaja tijekom incidenta

		Tjedan								
Br.	**Opis**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	Detektiran novi zlćudni ucjenjivački kod. Primljena obavijest nacionalnog CERT-a.									
2	Detektirana nova phishing kampanja. Primljena obavijest središnje banke.									
3	Zaposlenici dobavljača dobivaju *phishing* email. Neki zaposlenici otvaraju maliciozni privitak iz emaila.									
4	Zaposlenici banke dobivaju email od dobavljača s malicioznim privitkom. Jedan zaposlenik otvara email.									
5	Zlonamjerni kod koristi Mimikatz za prikupljanje dodatnih korisničkih računa i propagaciju.									
6	Napadači koriste Advanced Port Scanner za skeniranje mreže radi pronalaska odredišnog sustava.									
7	Napadači koriste Cobalt Strike za lateralno kretanje.									

		Tjedan								
Br.	**Opis**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
8	Zaposlenici se žale na sporost aplikacije. Napadači eksfiltriraju podatke na nekoliko zaraženih računala i Stealbit zlućudnim programom ih eksifiltriraju izvan banke.									
9	Nekoliko zaposlenika se žali na sporost računala.									
10	Poruke zlućudnog koda pojavljuju se na zaraženim računalima te aplikacija više nije funkcionalna.									
11	Pojavljuju se članci u medijima u kojima se navodi da je banka izložena kibernetičkom napadu.									
12	Pojavljuju se članci u medijima u kojima se navodi da je i dobavljač izložen kibernetičkom napadu.									

4.2.1. Modul 1

- **1. dan incidenta**

Nacionalni CERT objavljuje upozorenje o novoj varijanti zloćudnog ucjenjivačkog koda koji se koristi u kampanjama koje ciljaju državne institucije i bankarski sektor.

- **4. dan incidenta**

Središnja banka objavljuje upozorenje o nedavno primijećenoj *phishing* kampanji. *Phishing* e-pošta sadrži zlonamjerni privitak koji, kada je otvoren, instalira zloćudni ucjenjivački kod na korisnikovo računalo bez njegovog znanja. U p*hishing* e-pošti traži se hitna i obavezna nadopuna informacija u dokumentima organizacijske jedinice ljudskih resursa ili se u phishing e-pošti nalazi račun koji financijska institucija treba platiti.

- **11. dan incidenta**

Zaposlenici dobavljača dobivaju e-mail od svog odjela ljudskih resursa u kojem ih mole da provjere jesu li njihove informacije ispravne. Uz e-mail je priložen dokument za pregled i ažuriranje po potrebi. Neki korisnici prijavljuju e-mail kao sumnjiv, dok ga drugi otvaraju i šalju obrazac.

- **16. dan incidenta**

Zaposlenici banke primaju e-mail od dobavljača u vezi s računom za ovomjesečne troškove. Zaposlenik otvara e-mail i vidi da je dokument prazan. Zaposlenik e-mailom kontaktira dobavljača kako bi razjasnio e-mail i privitak. Dobavljač navodi da nemaju evidenciju slanja e-maila te istražuju njegovo porijeklo.

- **Pitanja za raspravu**

1. Ovaj scenarij opisuje dva upozorenja u vezi sa kibernetičkim sigurnosnim prijetnjama. Biste li primili ta upozorenja?
    a. Koje izvore obavještajnih podataka o kibernetičkim prijetnjama prima vaša financijska institucija?
    b. Koje informacije o kibernetičkim prijetnjama su najkorisnije?
    c. Jesu li informacije koje dobivate pravovremene i primjenjive?
    d. Tko je odgovoran za prikupljanje informacija u vašoj financijskoj instituciji?
    e. Kakve biste akcije poduzeli na temelju informacija o kibernetičkim prijetnjama iznesenim u scenariju?
    f. S kime još dijelite informacije o kibernetičkim prijetnjama?

i. Osoblje?
ii. Rukovodstvo?
iii. Dobavljači?

2. Provodi li vaša financijska institucija osnovnu obuku iz informacijske i kibernetičke sigurnosti za sve korisnike (uključujući menadžere i više rukovodstvo)?
    a. Što obuhvaća obuka?
    b. Za koga je obuka obavezna?
3. Imate li sigurnosne zahtjeve u ugovorima u kojima tražite dobavljače da provode istu obuku?
4. Je li vaša financijska institucija provela primjerenu procjenu kibernetičkih rizika radi identifikacije specifičnih prijetnji i ranjivosti?
    a. Koje su najznačajnije prijetnje i ranjivosti?
5. Imate li uspostavljen plan/program upravljanja zakrpama (engl. *patch management*)?
    a. Jesu li provedene procjene rizika za sve poslužitelje u mreži?
    b. Jesu li uspostavljeni procesi za proaktivnu procjenu važnosti i primjenjivosti zakrpi na svakom poslužitelju?
    c. Uključuje li ovaj plan strategiju upravljanja rizicima koja obuhvaća sljedeća razmatranja:
        i. Rizike nedostatka zakrpa za prijavljene ranjivosti?
        ii. Produljeno vrijeme nedostupnosti?
        iii. Ograničenu funkcionalnost?
        iv. Gubitak podataka?
6. Kako zaposlenici prijavljuju sumnjive pokušaje *phishinga*?
    a. Jesu li uspostavljene formalne politike ili planovi koji se slijede?
    b. Koje akcije vaša financijska institucija poduzima kada se prijave sumnjiva e-pošta?
    c. Provodi li vaša financijska institucija evaluaciju podložnosti phishing napadima?
7. Biste li neke od događaja opisanih u ovom modulu identificirali kao kibernetičke incidente ili događaje? Ako da, kako bi se oni rješavali?

4.2.2. Modul 2

- **47. dan incidenta**

Nekoliko zaposlenika kontaktira IT podršku žaleći se na sporost aplikacije. IT pokušava riješiti probleme, ali ne uspijeva pronaći uzrok problema. Većina korisnika dobiva uputu da ponovno pokrene aplikaciju.

- **50. dan incidenta**

Nekoliko zaposlenika kontaktira IT i žali se da su im računala zamrznuta ili da se ne odazivaju, dok se drugi žale da ne mogu pristupiti mrežnim resursima i zajedničkim pogonima. IT počinje istraživati probleme, ali još uvijek ne zna uzrok problema.

- **51. dan incidenta**

Poruke zlćudnog ucjenjivačkog koda pojavljuju se na nekoliko zaraženih računala, a korisnici zaraženih računala prijavljuju da ne mogu pristupiti svojim datotekama. Također, svi korisnici aplikacije prijavljuju da ne mogu pristupiti aplikaciji. Usluga kreditiranja za SME segment ne radi te klijenti banke ne mogu završiti procese kreditiranja.

Na zaraženim računalima, koja su se između ostaloga i koristila za eksfiltraciju podataka prikazuje se poruka koja navodi da su sve datoteke šifrirane i zahtijeva se plaćanje od <X> Bitcoina po računalu, vrijednih otprilike $<X> kako bi ključ za dešifriranje bio poslan. Poruka također upozorava da će ključ isteći ako se plaćanje ne primi u roku od 48 sati.

- **54. dan incidenta**

Nekoliko medijskih izvora počinje izvještavati da vaša banka doživljava napad zlćudnim ucjenjivačkim kodom. Primili ste više medijskih upita u kojima se traži komentar o incidentu s zlćudnim ucjenjivačkim kodom. Medijske priče dobivaju široku pažnju na internetu i društvenim medijskim platformama.

- **55. dan incidenta**

Izvješća medija sada ukazuju da je i dobavljač također žrtva napada zlćudnog ucjenjivačkog koda.

- **Pitanja za raspravu**

1. Kako bi se ovi incidenti procijenili unutar vaše banke? Imate li definirane razine ozbiljnosti kibernetičkih incidenata i/ili kriterije za eskalaciju?

2. Imate li osoblje zaduženo za odgovor na incidente ili poseban tim za odgovor na kibernetičke incidente?
    a. Ako da, koji prag se mora doseći da bi se aktiviralo osoblje za odgovor na kibernetičke incidente? Doseže li ovaj scenarij taj prag?
    b. Tko je odgovoran za aktiviranje osoblja za odgovor na kibernetičke incidente i pod kojim okolnostima?
    c. Kakve su uloge i odgovornosti tima/osoblja za odgovor na kibernetičke incidente?
3. Kojim internim i eksternim obavijestima (npr. rukovodstvu organizacije, korisnicima, klijentima, policiji, regulatoru) biste se obratili?
4. Ima li vaša financijska institucija dobar plan za oporavak podataka?
    a. Gdje se pohranjuju sigurnosne kopije? Jesu li izvan mreže ili online, pohranjene na sigurnom mjestu ili upravljane od treće strane?
    b. Jesu li sigurnosne kopije testirane kako bi se osiguralo da rade i da nisu oštećene?
    c. Koliko se dugo kopije čuvaju?
    d. Kako se testiraju sigurnosne kopije i kako se osigurava da nisu zaražene istim zlonamjernim programima?
    e. Koliko često se provode testovi povrata podataka iz pričuvnih kopija?
5. Biste li platili otkupninu?
    a. Tko donosi odluku?
    b. Koji je postupak za donošenje odluke o tome hoće li se platiti otkupnina ili ne?
    c. Koje su prednosti/nedostaci plaćanja?
    d. Kakve političke posljedice ima odluka o plaćanju?
    e. S kojim vanjskim partnerima/entitetima trebate stupiti u kontakt ako odlučite platiti?
6. Koje vještine i resursi su potrebni za odgovor na ovaj incident?
    a. Koga biste kontaktirali ako vam treba dodatna pomoć?
7. Koje su vaše brige u vezi s javnim odnosima?
    a. Tko je odgovoran za koordinaciju objava prema javnosti?
    b. Je li ovaj postupak dio definiranog plana?
    c. Kako bi vaša banka odgovorila na medijske izvještaje?
    d. Koje informacije dijelite s javnošću i zaposlenicima?

e. Da li je osoblje za informiranje javnosti educirano za upravljanje porukama vezanim uz kibernetičke incidente?
f. Imate li unaprijed pripremljene izjave za odgovor medijima?

5. PROVOĐENJE VJEŽBE ODGOVORA NA KIBERNETIČKI INCIDENT

Prije izvedbe vježbe bitno je da sve uključene strane znaju da se ne radi o stvarnom napadu ili incidentu kako ne bi poduzeli aktivnosti koje mogu imati utjecaj na poslovanje. Ovo pravilo ne treba se primjenjivati u posebnim okolnostima u kojima se vježbe izvodi u strogo kontroliranom okruženju kojim je spriječeno da se efekt vježbe odrazi na operativno poslovanje.

5.1. Smjernice za provođenje vježbe

Prilikom provođenja vježbe važno je imati na umu da vježba nije test, nego prilika za unaprjeđenje timskog rada, ispitivanje planova, politika i procedura, unaprjeđenje koordinacije i samopouzdanja, unaprjeđenje vještina, pomnije definiranje uloga i odgovornosti te otkrivanje ranjivosti. Općenite smjernice za vježbu su sljedeće [6]:

- Ovo je otvorena rasprava koja ne bi trebala uzrokovati stres. Različita gledišta, čak i neslaganja, su očekivana. Potrebno je odgovarati na temelju znanja o trenutnim planovima, sposobnostima (npr. isključivo korištenje postojećih resursa) i uvidima dobivenim iz edukacija.
- Odluke nisu presedan i možda ne odražavaju konačan stav banke o određenom pitanju. Vježba je prilika za raspravu i prezentiranje višestrukih opcija i mogućih rješenja.
- Potrebno je uzeti u obzir suradnju i podršku drugih organizacija.
- Fokus rasprava treba biti usmjeren na rješavanje problema. Sugestije i preporučene akcije vrijednije su od identificiranja problema.
- Pripremljeni scenarij i materijali temelj su za raspravu tijekom vježbe.

Za svaku vježbu primjenjuju se sljedeće pretpostavke:

- Scenarij za vježbu je vjerojatan, a događaji su se dogodili kako je prezentirano prilikom početka vježbe.
- Iza vježbe ne postoji skrivena agenda i ne postavljaju se trik pitanja.
- Svi sudionici dobivaju informacije istovremeno.
- Scenarij može i ne mora biti deriviran iz profila prijetnji banke koja provodi vježbu.

Šest su glavnih aktivnosti ciklusa upravljanja odgovorima na incidente: priprema, identifikacija, detekcija i analiza, suzbijanje, eliminacija i oporavak te aktivnosti nakon incidenta [19]. Voditelj vježbe treba osigurati da se navedeni koraci rasprave tijekom svake vježbe. Ukoliko vježba ima više vinjeta, a koraci su raspravljeni tijekom jedne od prethodnih vinjeta, nije ih potrebno ponavljati. Aktivnosti tijekom rasprave mogu uključivati sljedeće faze [20]:

1. Priprema: Teme za raspravu tijekom pripremne faze vježbe uključuju politike i procedure, kritične dokumente, kontakte (npr. vanjske partnere), alate, resurse, te dostupnost dokumentacije i informacija.
2. Identifikacija: Točke koje je potrebno raspraviti tijekom identifikacijske faze su kriteriji za proglašavanje razine utjecaja incidenta, podataka koji trebaju biti prikupljeni, razmjera incidenta i podataka trećih strana, ako je to primjenjivo. Nakon što je sve to određeno treba se odviti rasprava o podacima i razini rizika za banku i bankarski sektor.
3. Detekcija i analiza: Rasprava tijekom ove faze treba uključivati strategiju i prioritete istrage, dodijeljene timove (npr. uloge i odgovornosti prema definiranom planu), opseg incidenta (npr. mreža, interni poslužitelji, klijenti, partneri), nalaze iz izvješća relevantnih alata, razmjenu informacija u timu i izvan tima, izvještavanje uprave i izvore informacija (npr. opise konkretnog zloćudnog koda i upute za oporavak, informacije proizvođača opreme ili softvera).
4. Ograničavanje: Rasprava tijekom ove faze treba biti usmjerena na metode suzbijanja incidenta, prikupljanja forenzičkih informacija i uklanjanje podataka ako su potencijalno objavljeni na internetu.
5. Eliminacija i oporavak: Tijekom ove faze potrebno je raspraviti ranjivosti okruženja (npr. moguće točke upada), brisanje i oporavak zahvaćenih uređaja ili sustava, pristupne točke i dostupnost, instaliranje zakrpa, ponovno konfiguriranje uređaja ili softvera i sve ostale otkrivene ranjivosti.
6. Aktivnosti nakon incidenta: Rasprava tijekom ove faze treba biti usmjerena na promjene u nadzornim sustavima, naučenim lekcijama i unaprjeđenju upravljanja, što se ne odnosi samo na banku koja simulira incident, već i na partnere i pružatelje usluga u oblaku. Potrebno je pripremiti upitnik i prikupiti odgovore od sudionika vježbe kako bi se prikupili komentari i preporuke vezane uz scenarij i potencijalne ranjivosti identificirane tijekom vježbe.

Banke bi trebale razviti i materijale za provođenje vježbe kako bi se lakše provodilo izvršavanje vježbe. Materijali obično sadržavaju:

- Smjernice za voditelja vježbe – uključuju narativni scenarij, popis pitanja za vođenje vježbe te plan odgovora na incident koji se provodi.
- Smjernice za sudionike vježbe – uključuje iste materijale kao za voditelja, ali bez popisa pitanja
- Izvješće nakon aktivnosti – pruža kriterije za procjenu na osnovu ciljeva vježbe kako bi se odredilo u kojoj su mjeri ciljevi ispunjeni te gdje bi mogle biti potrebne dodatne mjere.

U dodatku ovog rada priloženi su predlošci za gore navedene materijale i dodatno predlošci za povratne informacije o vježbi te plan unaprjeđenja.

5.2. Smjernice za voditelja vježbe

Voditelj vježbe odgovoran je za koordinaciju grupnih aktivnosti tijekom vježbe, a odgovornosti voditelja su sljedeće [6]:

- Usmjeravanje tijeka vježbe.
- Održavanje rasprava na pravom putu i na primjerenoj razini.
- Slijediti utvrđene procese.
- Identifikacija i rješavanje odgovarajućih problema.
- Nadzor nad izradom sažetaka.

Karakteristike dobrog voditelja vježbe su sljedeće [6]:

- Održavanje rasprava na pravom putu i unutar utvrđenih vremenskih ograničenja. Kontroliranje dinamike grupe i jakih ličnosti te sposobnost kompetentnog i samopouzdanog govora o temi bez dominiranja ili usmjeravanja razgovora
- Ekspertiza ili iskustvo u funkcionalnom području
- Znanje trenutnih planova, politika, procedura i mogućnosti institucije
- Mogućnost izrade kratkih bilješki rasprave, kako bi se one uključile u Izvješće nakon aktivnosti i plan unaprjeđenja

Ako se vježba organizira u formatu gdje sudionici sjede za više stolova, nakon uvoda u scenarij ili dodataka dolazi do moderirane rasprave na svakom stolu. Nakon definiranog vremena, moderirana rasprava za svakim stolom završava, a moderirana rasprava o ključnim

nalazima svakog stola započinje. Sudionici bi trebali raspravljati o svojim odgovorima na temelju znanja o trenutnim planovima, politikama, postupcima i sposobnostima.

U moderiranim raspravama, predstavnik sa svakog stola svim sudionicima vježbe prezentira ključne nalaze i probleme, kao i neriješene probleme ili pitanja iz grupe. Unutar planiranja vremena za raspravu tijekom izrade plana vježbe uzima se u obzir i rasprava tijekom zaključka vježbe za koju je često potreban veći vremenski okvir. Svaka grupa trebala bi se usredotočiti samo na materijal prezentiran za danu vinjetu tijekom svake rasprave.

Ponekad je potrebno odrediti i pomoćnika koji će voditelju vježbe pomoći zapisivati glavne točke rasprave ili svakoj grupi pomoći pripremiti materijale koji će se koristiti tijekom plenarnih sjednica. Voditelj vježbe nije osoba koja prezentira informacije tijekom plenarnih sjednica, ako se radi o plenarnom formatu vježbe. Iako bi u raspravi tijekom plenarnih sjednica često htjelo sudjelovati nekoliko članova svake grupe, potrebno je što ranije odrediti jednog predstavnika koji će moderirati pripremu prezentacije i prezentirati informacije.

5.3. Procjena uspješnosti vježbe

Nakon završetka vježbe, organizacija bi trebala provesti procjenu uspješnosti vježbe. Ova procjena ima za cilj utvrditi jesu li ciljevi vježbe postignuti i jesu li sudionici učinkovito odgovorili na simulirani sigurnosni incident.

Za procjenu uspješnosti vježbe, potrebno je razmotriti sljedeće:

- Analizirati postignute rezultate vježbe, što uključuje evaluaciju uspješnosti provedenih zadataka, podataka o vremenu reakcije, aktivnostima koje su poduzete i uspješnosti tih aktivnosti te koordinacije sudionika.
- Identificirati nedostatke u vježbi, što uključuje evaluaciju procesa i procedura, opreme i infrastrukture koja se koristila tijekom vježbe, kao i identifikaciju nedostataka u obuci sudionika.
- Procijeniti uspješnost vježbe uspoređujući je s industrijskim standardima industrije i internim standardima organizacije.

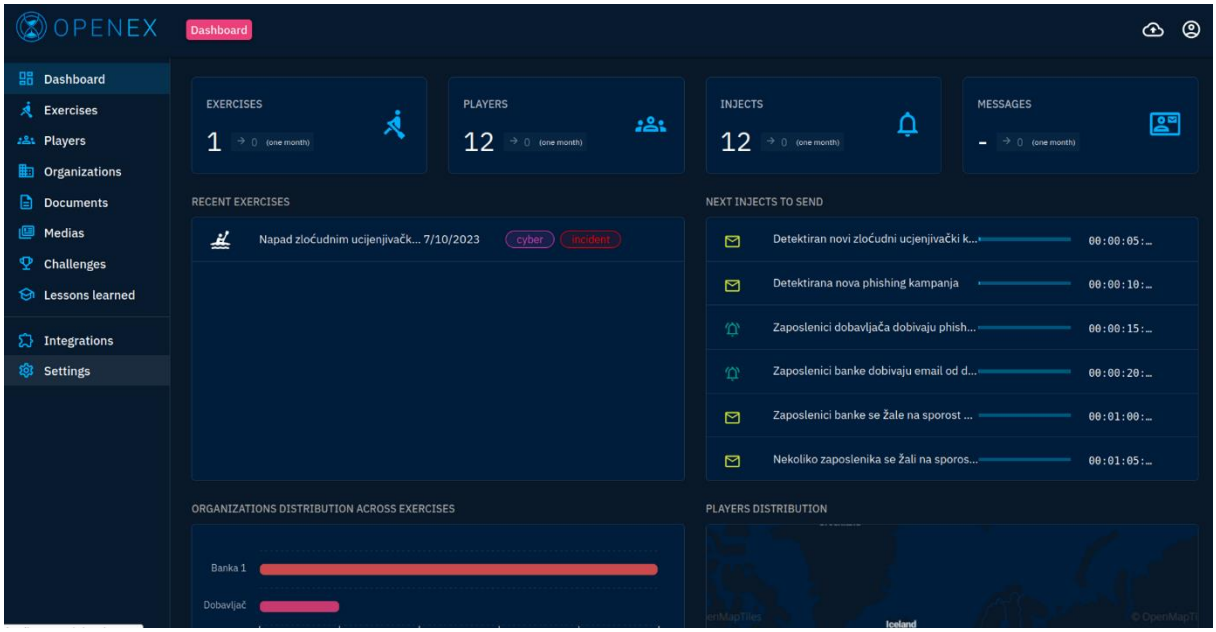
Procjena uspješnosti vježbe ključna je za osiguranje kontinuiranog poboljšanja procesa za odgovor na sigurnosne incidente. Analiza rezultata i povratne informacije sudionika omogućuju organizaciji identifikaciju nedostataka u postupcima, procedurama i obuci sudionika te razvoj strategije za rješavanje identificiranih nedostataka. Ovime će se postići bolja reakcija na buduće sigurnosne incidente i smanji rizik od ozbiljnih posljedica koje mogu proizaći iz njih.

5.4. Simulacija vježbe u OpenEX simulatoru

OpenEx platforma napredni je alat otvorenog koda (engl. *Opensource*) razvijen kako bi organizacijama i timovima omogućio učinkovito planiranje, simuliranje i provođenje vježbi za krizne situacije. Ova platforma korisnicima omogućuje simuliranje realističnih scenarija za krizne situacije, praćenje tijeka događaja i napretka u rješavanju situacije te učenje iz stečenog iskustava kako bi poboljšali svoje sposobnosti upravljanja krizama. Ključne značajke simulatora su:

1. **Stvaranje scenarija:** OpenEx korisnicima omogućuje stvaranje kompleksnih scenarija kriza koji odražavaju stvarne situacije. Mogu se definirati faktori poput vrste krize, stupnja ozbiljnosti, relevantnih dionika i vremenskog okvira.
2. **Prilagodljivost**: Platforma omogućuje prilagodbu scenarija prema potrebama korisnika. Mogu se dodati specifični elementi ili uvjeti kako bi se simulirale situacije koje su najrelevantnije za organizaciju ili tim.
3. **Realistične simulacije**: OpenEx koristi napredne tehnologije kako bi stvorio realistične simulacije kriznih situacija. To uključuje simulaciju komunikacije, brze promjene okolnosti i dinamičke reakcije dionika.
4. **Timski rad:** Platforma podržava višekorisničko sudjelovanje, omogućujući timovima da surađuju u rješavanju krize. Članovi tima mogu djelovati kao različiti dionici i razmjenjivati informacije i odluke.
5. **Praćenje i analiza:** OpenEx omogućuje korisnicima praćenje tijeka vježbe i analizu njihovih reakcija i odluka. Ovo pruža uvid u učinkovitost upravljanja krizom i identificira područja za poboljšanje.
6. **Poučavanje i učenje:** Nakon završetka vježbe, platforma omogućuje korisnicima da analiziraju rezultate i uče iz iskustva. To je korisno za prilagodbu protokola i strategija upravljanja krizama.

Pripremljeni scenarij vježbe opisan u prethodnim poglavljima definiran je i u OpenEX simulatoru, a konfiguracija vježbe nalazi se u prilogu rada.



Slika 6. OpenEX simulator

6. ZAKLJUČAK

Ovaj rad svojevrsni je pregled procesa i daje smjernice za pripremu, provođenje i procjenu vježbi za kao i odgovor na kibernetičke incidente s fokusom na bankarski sektor. Također, u radu su predloženi popratni materijali i scenariji koji se mogu koristiti prilikom provođenja vježbe. Za izradu scenarija predloženo je korištenje TIBER-EU okvira, a za prijedlog procesa korišteni su različiti izvori, uključujući NIST 800-61 reviziju 2, kako bi se osiguralo da su predlošci adekvatni i prilagođeni bankarskom sektoru.

Rezultati ovog rada ukazuju na to da su vježbe reakcije na sigurnosne incidente neophodan dio sigurnosnog programa svake banke. Predloženi scenariji i predlošci mogu pomoći financijskim institucijama da se bolje pripreme za potencijalne sigurnosne incidente te osiguraju učinkovitu reakciju u slučaju incidenta.

U budućnosti bi se moglo nastaviti s ovom temom provođenjem praktičnih vježbi u financijskim institucijama, što bi moglo pomoći u daljnjem poboljšanju procesa za provođenje vježbi odgovora na sigurnosne incidente, kao i unaprjeđenju predloženih scenarija i razvoju novih scenarija.

7. LITERATURA

[1] International Organization for Standardization, „ISO/IEC 27001 Information security management systems, Information technology — Security techniques — Information security management systems — Requirements“, Geneva, Switzerland, 2013.

[2] Hrvatska narodna banka, „Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika“ , dostupno na: https://www.hnb.hr/documents/20182/639854/h-smjernice-za-upravljanje-informacijskim-sustavom.pdf/e5579931-e846-47ab-af23-6809debef700 (02.05.2023.)

[3] ISO/IEC 27035-1:2016, „Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management“, Geneva, Switzerland, 2016.

[4] European Banking Authority, „Smjernice EBA-e o upravljanju rizicima IKT-a i sigurnosnim rizicima“, dostupno na: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880816/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_HR.pdf (02.05.2023.)

[5] ISO/IEC 27035-2, „Information technology— Security techniques— Information security incident management— Part 2: Guidelines to plan and prepare for incident response“, Geneva, Switzerland, 2015.

[6] U.S. Department of Homeland Security, „Cyber Tabletop Exercise for the Healthcare Industry, Facilitator and Planner Guide“

[7] European Central Bank, TIBER-EU FRAMEWORK, How to implement the European framework for Threat Intelligence-based Ethical Red Teaming, dostupno na: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (10.07.2023.)

[8] European Banking Authority, „Smjernice o sigurnosnim mjerama za operativne i sigurnosne rizike povezane s platnim uslugama na temelju Direktive (EU) 2015/2366 (Direktiva PSD2)“, dostupno na:

https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2081899/e66850a4-00ef-4cb4-bdc9-

f6b803cf16f4/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20%28EBA-GL-2017-17%29_HR.pdf?retry=1 (02.05.2023.)

[9] European Central Bank, „TIBER-EU - Scope Specification Template“ , dostupno na: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Scoping_specification_template_July_2020.pdf (02.05.2023.)

[10] European Central Bank, „TIBER-EU - Guidance for Target Threat Intelligence Report“, dostupno na: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf (10.07.2023.)

[11] Internal Revenue Service, „IRS Safeguards Technical Assistance Memorandum, Incident Response Test and Exercise Guidance“ , dostupno na: https://www.irs.gov/pub/irs-utl/incidentresponsetest-and-exerciseguidance.doc (02.05.2023.)

[12] European Central Bank, „The Quick and the Dead: building up cyber resilience in the financial sector“, dostupno na: https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230308~92211cd1f5.en.html (10.07.2023.)

[13] Dawson, D.,Wang, J, Bakht, A., Bourdeau, A., Chatterjee, D., Colaco, J., Gray, C., Lee, J., Young, K., Delloite, „When legacy is not enough“, dostupno na: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-us-why-legacy-is-not-enough-2008.pdf (10.07.2023.)

[14] European Banking Authority, „Annex I - RESOLUTION TEMPLATES“ , dostupno na: https://www.eba.europa.eu/documents/10180/1986661/Annex+I+-+Resolution+Templates.xlsx (02.05.2023.)

[15] IBM, „Small and medium enterprise loan origination on IBM Cloud for Financial Services“, dostupno na: https://www.ibm.com/cloud/architecture/architectures/loan-origination/ (02.05.2023.)

[16] ComputerWeekly, „Is time running out for legacy payments technology used by banks?“ , dostupno na: https://www.computerweekly.com/news/252522603/Is-time-running-out-for-legacy-payments-technology-used-by-banks (02.05.2023.)

[17] SOCRadar, „Dark Web Profile: LockBit 3.0 Ransomware“ , dostupno na: https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/ (02.05.2023.)

[18] Trend Micro, „Ransomware Spotlight – Lockbit“, dostupno na:

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit (02.05.2023.)

[19] NIST Special Publication 800-61, Revision 2, „Computer Security Incident Handling Guide“, 2012.

[20] Larry G. Wlosinski, „Cybersecurity Incident Response Exercise Guidance, ISACA“ JOURNAL VOL 1., dostupno na:

https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2022/volume-1/cybersecurity-incident-response-exercise-guidance_joa_eng_0122.pdf, (02.05.2023.)

DODATAK A: POPIS KRATICA, SLIKA I TABLICA

A.1.: Popis oznaka i kratica

ISMS	Information Security Management System
IKT	Informacijsko-komunikacijske tehnologije
CSIRT	Computer Security Incident Response Team
IRT	Incident Response Team
TIBER-EU	*Threat Intelligence-Based Ethical Red-Teaming*
ECB	European Central Bank
TTP	Tactics, Techniques, and Procedures
EBA	European Banking Authority
SME	Small and medium-sized enterprises

A.2.: Popis tablica

A.3.:Popis slika

DODATAK B: MATERIJALI ZA PRIPREMU I PROVOĐENJE VJEŽBI

B.1.: Aktivnosti za planiranje vježbe

Zadaci za planiranje vježbe	Odgovornost
Odrediti proračun za vježbu	
Odrediti vremenski plan za planiranje vježbe	
Definirati tim za planiranje vježbe	
Organizirati prvi sastanak za pripremu vježbe	
I. Dizajn vježbe	
Sastanci za planiranje	
Pripremiti i poslati pozivnice i po potrebi dokumentaciju	
Definirati plan i kratak uvod za vježbu	
Odrediti ciljeve i scenarije za provođenje vježbe Ako se definiraju novi scenariji potrebno je slijediti korake opisane u 3.2 Definiranje i odabir scenarija	
Upoznati sudionike ako se prvi puta susreću	
Pronaći lokaciju za provođenje vježbe	
Odrediti datum za sljedeći sastanak za planiranje	
Dodijeliti rokove i odgovornosti za zadatke	
Pregledati sve materijale za vježbu, dokumentaciju i zadatke	
Napisati zapisnike o sastancima	
Dokumentacija	
Započeti pregled i unos podataka u dokumentaciju za vježbu	
Lokacija vježbe	
Definirati detalje o lokaciji sastanka (mjesta za sjedenje itd.)	
Javne informacije (ako je potrebno)	
Definirati pravila za simuliranje kontakta medija	
Definirati predloške za objavu podataka javnosti	
Logistika	
Rezervirati sobu za sastanke	
Odrediti i rezervirati ostalu opremu (npr. Mikrofone, projektore, zaslone, ploču za pisanje, markere)	
Ako je potrebno pripremiti pločice s imenima i forme za prijavu	
Naručiti hranu i piće	

Zadaci za planiranje vježbe	Odgovornost
Definiranje sudionika	
Odrediti uloge u vježbi (npr. Voditelj, prikupljač podataka itd.)	
Odabrati i educirati sudionike	
II. Provođenje vježbe	
Kratke upute	
Prezentirati multimedijski sadržaj za vježbu	
Dokumentacija	
Podijeliti situacijski priručnik sudionicima	
Podijeliti druge materijale ako su napravljeni	
Podijeliti upitnike za povratne informacije	
Vježba	
Pripremiti mjesto za provođenje vježbe	
Provesti vježbu	
Provesti raspravu nakon vježbe	
III. Evaluacija	
Izvješće nakon vježbe	
Napraviti zapisnik na osnovu rasprave nakon vježbe	
Napraviti skicu izvješća nakon vježbe	
Poslati skicirano izvješće na pregled timu za planiranje vježbe	
IV. Planiranje unaprjeđenja	
Sastanak nakon vježbe	
Odrediti termin sastanka	
Pripremiti i poslati pozivnice	
Održati sastanak nakon vježbe	
Završiti izvješće nakon vježbe	
Definirati plan unaprjeđenja	
Planiranje unaprjeđenja	
Poslati lekcije nakon vježbe, najbolje prakse, izvješće nakon vježbe te plan unaprjeđenja	
Inicirati implementaciju unaprjeđenja	
Pratiti implementaciju unaprjeđenja	

B.2.: Obrazac za opis vježbe

<table>
<tr><th>Ime vježbe</th><th colspan="2">[Unijeti ime vježbe]</th></tr>
<tr><td>Datum, vrijeme i lokacija vježbe</td><td colspan="2">[Datum]
[Vrijeme, npr. 09:00 – 14:00]
[Lokacija]</td></tr>
<tr><td rowspan="11">Raspored vježbe</td><td>Vrijeme</td><td>Aktivnost</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>[Vrijeme]</td><td>[Aktivnost]</td></tr>
<tr><td>Opseg</td><td colspan="2"></td></tr>
<tr><td>Svrha</td><td colspan="2"></td></tr>
<tr><td>Ciljevi</td><td colspan="2"></td></tr>
<tr><td>Prijetnja</td><td colspan="2">Kibernetički incident</td></tr>
<tr><td>Scenarij</td><td colspan="2"></td></tr>
<tr><td>Organizacije koje sudjeluju u vježbi</td><td colspan="2"></td></tr>
<tr><td rowspan="3">Kontakti</td><td>Organizacija</td><td>Kontakt</td></tr>
<tr><td>[Organizacija]</td><td>[Kontakt]</td></tr>
<tr><td>[Organizacija]</td><td>[Kontakt]</td></tr>
</table>

B.3.: Obrazac za evidenciju sudionika vježbe

Ime banke	
Datum	
Opis scenarija	

Popis sudionika		
Ime i prezime	***Potpis***	***Radno mjesto***

B.4.: Obrazac za povratne informacije

Potrebno je unijeti odgovore u odgovarajuća polja te označiti ulogu u vježbi odgovora na incidente.

Ime i prezime:				
Titula:				
Organizacija:				
Uloga:	Sudionik ☐	Voditelj ☐	Promatrač ☐	Prikupljač ☐

Dio 1: Preporuke i korektivne aktivnosti

1. Navedite prve tri pozitivne strane vježbe ili područja u kojima je potrebno unaprjeđenje temeljem današnjih rasprava te identificiranih zadataka.
    1. _____
    2. _____
    3. _____

2. Identificirajte korake ili aktivnosti koje bi se trebale poduzeti kako bi se riješili gore identificirani nedostaci. Za svaki korak navedite prioritet po svojoj procjeni.

Korektivna aktivnost	Prioritet

3. Opišite korektivne aktivnosti koje su potrebne u svojoj domeni. Kome se treba dodijeliti odgovornost za svaku od aktivnosti?

Korektivna aktivnost	Prijedlog zaposlenika za dodjelu odgovornosti

4. Napišite politike, planove i procedure koje treba pregledati I unaprijediti. Definirajte razinu prioriteta za svaku od aktivnosti.

Dokument koji je potrebno pregledati	Prioritet

Dio II: Procjena pripreme i izvedbe vježbe

Ocijeniti vježbu ocjenom na razini od 1 do 5, pri čemu je 1 najniža ocjena, a 5 najviša.

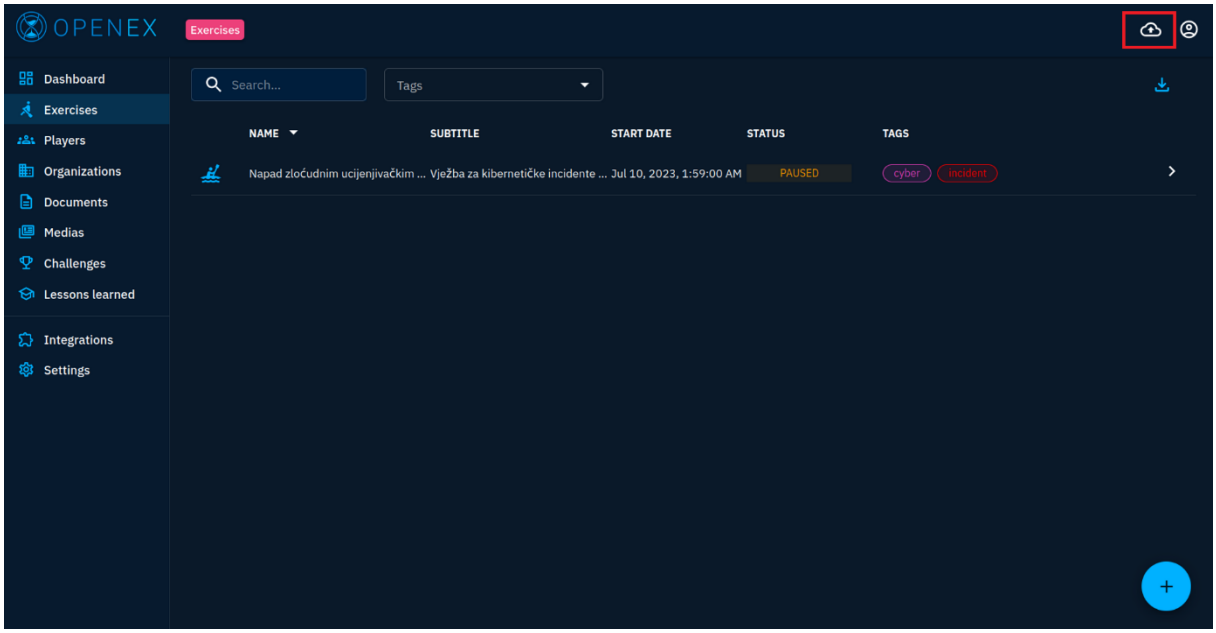
Čimbenik procjene					
Vježba je dobro strukturirana i organizirana.	1	2	3	4	5
Scenarij za vježbu je realan i vjerojatan.	1	2	3	4	5
Multimedijska prezentacija pomogla je u shvaćanju i uključivanju u scenarij.	1	2	3	4	5
Voditelj ima znanje o materijalima, držao je vježbu usmjerenom i dobro je procijenio dinamiku grupe.	1	2	3	4	5
Situacijski priručnik koje je korišten tijekom vježbe je dobar alat za provođenje vježbe.	1	2	3	4	5
Sudjelovanje u vježbi je prikladno za nekoga na mojoj poziciji.	1	2	3	4	5
Sudionici uključeni u vježbu dobro su odabrani s obzirom na ulogu u organizaciji.	1	2	3	4	5

Dio III: Ostale povratne informacije

Koje bi promijene unijeli u vježbu? Molimo dajte preporuku kako bi buduće vježbe mogle biti unaprijeđene. Također, dajte bilo koju drugu povratnu informaciju za koju mislite da bi bila korisna prilikom planiranja sljedećih vježbi.

DODATAK C: KONFIGURACIJA VJEŽBE U OPENEX ALATU

Konfiguracija vježbe u OpenEX alatu pohranjena je na medij koji je dodan uz rad. Konfiguracija se nalazi u zip datoteci u koju je pohranjena .json datoteka. Konfiguracija se može učitati klikom na „Import an exercise“ gumb na „Exercices“ kartici u OpenEX software-u, nakon čega se odabere .json datoteka, kako je prikazuje slika 7.



Slika 7. Uvoz konfiguracije u OpenEX simulator