UDK 336.71:004.056

Smernice upravljanja kibernetske varnosti v finančnem sektorju

*Grega Prešeren**

GUIDELINES FOR CYBERSECURITY MANAGEMENT IN THE FINANCIAL SECTOR

The article will address the current cybersecurity issues in the banking and financial sectors. We will focus on the most common attack vectors, vulnerabilities, and techniques for improving an organization's cybersecurity posture. Security testing and user awareness will be discussed in detail. Cybersecurity management has become integral to various regulatory frameworks, leveraging its importance, and moving it closer to management. Cybersecurity management will be discussed in terms of NIS2 directive, DORA regulation, NIST cybersecurity framework, and ISO 27001 standard.

JEL G21 K24 O38

Uvod

Kibernetska varnost je v zadnjih letih zagotovo postala ena ključnih prioritet bančnega in širšega finančnega sektorja. Velike baze uporabnikov, ogromne količine občutljivih podatkov in finančna sredstva, ki so povezana s temi podatki, postavljajo finančne institucije v posebej ranljiv položaj. Od napadov na bančne sisteme in uporabnike imajo organizirane hekerske skupine direktno finančno korist, kar je največkrat tudi njihov končni cilj. Kot odgovor na vedno naprednejše oblike napadov vpeljujejo odgovorni za kibernetsko varnost strateške načine upravljanja kibernetske varnosti. V pričujočem članku bomo naslovili najpogostejše ranljivosti in vektorje napadov ter predstavili dobre prakse upravljanja kibernetske varnosti, ki med drugim vključujejo redno testiranje sistemov in ozaveščanje uporabnikov.

1. Najpogostejši vektorji napadov

Finančne institucije se soočajo s plejado potencialnih kibernetskih groženj, od napadov z ribarjenjem (*ang. phishing*), izsiljevalske kode (*ang. ransomware*) in kampanj s škodljivo kodo (*ang. malware*). V nadaljevanju opisujemo uspešne vektorje napadov, ki jih najpogosteje zasledimo pri testiranju finančnih institucij.

Napadi s socialnim inženiringom

Napadalci uporabljajo metode socialnega inženiringa, da posameznike pregovorijo v razkrivanje zaupnih informacij ali posredovanje poverilnic za dostop do zaščitenega omrežja. Socialni inženiring se izvaja v različnih oblikah. Najpogosteje se srečujemo z napadi z ribarjenjem po elektronski pošti, ne smemo pa zanemariti niti poskusov napadov prek SMS-sporočil ali celo osebnega pristopa na lokacijah. Tovrstni napadi so zelo učinkoviti, ker smo ljudje pogosto preveč radovedni ali ustrežljivi. Že klik na škodljivo povezavo ali odprtje škodljive priponke lahko hekerjem odpre vrata v vaš informacijski sistem.

Napadi s škodljivo in izsiljevalsko kodo

Napadalci uporabljajo škodljivo programsko opremo, ki lahko resno poškoduje IT-sistem ali podatke organizacije. Zlasti nevarni so napadi z izsiljevalsko kodo, ki zakleni (zašifrira) podatke, napadalci pa za povrnitev podatkov ali preprečitev njihove javne objave zahtevajo visoke odškodnine. Res je sicer, da s pogajanji višino odškodnine lahko deloma znižate, v vsakem primeru pa je ob takšnem dogodku na udaru ugled podjetja, ogroženi so podatki komitentov, poleg tega pa pride tudi do slabše uporabniške izkušnje, saj so storitve običajno vsaj nekaj časa onemogočene. Današnje zaščite pred škodljivo programsko kodo so deloma učinkovite, tipično pa ne preprečijo najbolj naprednih napadov. Zato so potrebni dodatni tehnični ukrepi.

* Grega Prešeren, univ. dipl. ing. el., CTO, gpreseren@carbonsec.com, Carbonsec d.o.o.

Napadi z onemogočanjem storitev
Napadi z onemogočanjem storitev (DDoS) tipično temelijijo na pošiljanju velike količine prometa proti strežnikom organizacije, kar v prvi fazi upočasni delovanje omrežja in spletnih strani, v drugi fazi pa pride do odpovedi delovanja sistema.

Napadi po dobavni verigi
Napadi po dobavni verigi so eden novejših vektorjev napadov in vključujejo več deležnikov. Uporabljajo se zlasti takrat, ko želijo napadalci dostopati do omrežja velikega podjetja, ki ima dobro kibernetsko zaščito, prek interneta pa se povezuje z manjšimi podjetji oz. od njih dobavlja strojno ali programsko opremo. Napadalci izberejo enega teh manjših podjetij, ki običajno slabše skrbijo za kibernetsko varnost, in se po dobavni verigi pomikajo do končne tarče. Tako s hekerskimi tehnikami, ki morda niso učinkovite v ciljnem podjetju, po drugi poti, t. i. poti z najmanjšim odporom, vdrejo v ciljno podjetje.
Finančne institucije morajo strategije upravljanja kibernetske varnosti oblikovati z mislijo na najpogostejše vektorje napada in krepitev odpornosti še intenzivneje graditi na teh področjih. Pri tem se moramo zavedati, da ni pomembna le namestitev varnostnih naprav, temveč njihova pravilna umestitev v posamezno okolje, prilagoditev nastavitev posameznemu okolju ter spremljanje delovanja v življenjskem ciklu IT-okolja. Različne nadgradnje in druge spremembe lahko pomembno vplivajo na pravilno prepoznavanje škodljivih vsebin in poskusov napadov.

2. Najpogostejše ranljivosti

Eden od razlogov, zakaj so finančne institucije tako ranljive in posledično privlačne za kibernetske kriminalce, je njihova usmerjenost k uporabnikom ter obsežnost in kompleksnost informacijskega sistema. V nadaljevanju bomo opisali pri testiranjih najpogosteje zaznane ranljivosti v finančnem in bančnem sektorju.

Nezavarovana omrežja in zastarela programska oprema
Dobro zaščiteno omrežje in posodobljena programska oprema sta dve osnovni predpostavki za zagotavljanje varnosti v informacijskem sistemu. Z varnostnimi napravami na perimetru omrežja in v zadnjem času tudi v samem omrežju nadzorujemo promet in zaznavamo morebitne deviacije. Odsotnost varnostnih naprav, njihova neustrezna umestitev in pomanjkljivo spremljanje dogajanja na omrežju so pogost vzrok uspešnih napadov.

Pomanjkljivo izobraženi zaposleni
Zaposleni, ki ne znajo prepoznati potencialne kibernetske grožnje in se nanjo odzvati, lahko za organizacijo predstavljajo veliko ranljivost. Po drugi strani je to ranljivost, ki jo lahko z izobraževalnimi programi za uporabnike precej enostavno rešujemo, dovzetnost za napade s socialnim inženiringom pa se že v nekaj mesecih bistveno zmanjša. Ozaveščanje uporabnikov bomo podrobneje naslovili v nadaljevanju.

Šibki varnostni mehanizmi za prijavo v sisteme
Napadalci lahko pridobijo dostop v poslovno omrežje z ukradenimi ali šibkimi gesli, zato je vpeljava politike močnih gesel nujna za zagotavljanje varnosti. Za dostop do javnih in ključnih sistemov in aplikacij je zelo priporočljiva uporaba večfaktorske avtentikacije (*ang. multi-factor authentication*) s sistemom enkratnih gesel, avtentikatorjev na mobilnem telefonu, ali tehnologije FIDO.
Odpravljanja ranljivosti se je smiselno lotevati celostno in strateško. Ad-hoc načini reševanja kibernetskih tveganj niso zaželeni, saj lahko sicer kratkoročno rešijo težavo, pogosto pa ne prispevajo k splošnemu izboljšanju kibernetskovarnostne drže.

3. Testiranje kibernetske varnosti

Testiranje kibernetske varnosti je ena najpomembnejših komponent učinkovite varnostne strategije. Organizacijam pomaga prepoznavati šibke točke na sistemih, da lahko ukrepajo, preden ranljivosti izrabijo napadalci. Bančni sektor je na področju izvajanja varnostnih testov po naših izkušnjah v slovenskem prostoru eden najbolj naprednih, saj večina bank že leta vestno skrbi za kibernetsko varnost s testiranjem, ozaveščanjem uporabnikov in implementiranjem različnih varnostnih rešitev. Kljub temu se pri varnostnem testiranju pogosto izkaže, da so občutljivi podatki odloženi na lahko dostopnih mestih, na primer v datotekah v skupni rabi, v katerih so zapisana administratorska gesla različnih sistemov. Avtomatski testi takšno ranljivost tipično označijo kot nizko ali info, dejanski vpliv izrabe ranljivosti na poslovanje in ugled banke pa je lahko ogromen. Takšni anomaliji se lahko izognemo z ročnim penetracijskim oz. vdornim testom ali z uporabo avtomatiziranih rešitev, ki poskušajo odkrite ranljivosti v danem sistemu tudi izrabiti. Ob ustreznih vhodnih podatkih (npr. specificiranju, kateri podatki so za nas kritični) bo izbrana rešitev takšno ranljivost rangirala z višjo stopnjo kritičnosti.
Testiranja kibernetske varnosti potekajo na različnih ravneh in na različni infrastrukturi. Kljub vsemu pa lahko klasični varnostni test razdelimo na tri osnovne faze: popis ranljivo-

sti, penetracijsko testiranje in ocena tveganja. Nekoliko drugačen potek pa je pri kibernetski vaji Red Teaming, ki jo bomo v nadaljevanju tudi natančneje opisali.

Popis ranljivosti

S popisom ranljivosti identificiramo potencialne ranljivosti v poslovnem sistemu in jih razvrstimo po pomembnosti. To je prvi korak pri testiranju varnosti sistema, ki se mora nujno nadaljevati z natančnim pregledom in preizkusom izrabe odkritih ranljivosti (penetracijski test). Pri tem se ne smemo osredotočiti le na ranljivosti, ki so v popisu označene za kritične ali visoke, temveč moramo pregledati tudi tiste z oznako info ali nizko, saj se med njimi pogosto skrivajo ranljivosti, ki na prvi pogled neposredno ne predstavljajo večje grožnje, lahko pa vsebujejo podatke, ki napadalcem omogočijo izvajanje nadaljnjih napadov prek drugih virov.

Penetracijsko testiranje

Cilj penetracijskega testa je na podlagi simulacije hekerskega napada preveriti, kako varen je informacijski sistem organizacije. Penetracijski test lahko izvajamo na zunanjem ali notranjem omrežju, na celotnem omrežju ali le na vnaprej določenem segmentu, več segmentih, na aplikacijah ali programskih vmesnikih, t. i. API-jih. Priporočljivo je, da se varnostno testiranje izvaja ciklično, saj se zaradi velike dinamike informacijskih okolij neprestano pojavljajo nove ranljivosti in grožnje. Smiselno je, da organizacije razmislijo o uporabi avtomatiziranih orodij, ki omogočajo redno in učinkovito izvajanje standardiziranih testov, na daljše časovno obdobje (npr. enkrat letno) pa se izvede obsežnejši penetracijski test. Pri izbiri avtomatiziranega orodja je dobro, da to ne le popiše ranljivosti in jih razvrsti po objavljeni stopnji kritičnosti (CVE), temveč jih tudi oceni glede na to, ali je ranljivost v vašem sistemu dejansko mogoče izrabiti in predlaga postopek odprave.

Ocena tveganja

Na podlagi izsledkov popisa ranljivosti in penetracijskega testa se izdela ocena tveganja, ki poleg tehničnega dela vključuje tudi poslovni vpliv. V oceni tveganja povežemo ranljivosti s potencialnimi posledicami njihove izrabe in se na podlagi rezultatov odločimo, katere je smiselno najprej reševati ter predlagamo ustrezne ukrepe za zmanjšanje ali odpravo tveganj.

Red Teaming

Posebna vrsta varnostnega testiranja je t. i. kibernetska vaja oz. Red Teaming, ki je simulacija dejanskega hekerskega napada na organizacijo. Če pri penetracijskem testiranju velja, da naročnik definira obseg testa (npr. segmente omrežja, aplikacijo ipd.) in se izvajalci držijo dogovorjenega obsega, se pri vaji Red Teaming test izvaja na organizaciji kot celoti, uporablja pa se najbolj aktualne hekerske taktike in tehnike. Cilj takšne vaje je preveriti, kako dobra sta zaznava in odziv organizacije na kibernetski napad. Na strani naročnika je tipično ena kontaktna oseba, ki z izvajalcem koordinira potek testa, drugi uporabniki o vaji niso obveščeni. Prav zato je pri takšnem testu pomembno, da se interno vnaprej dobro pojasni, zakaj ima organizacija v določenem letu ali polletju namen izvesti kibernetsko vajo in kaj je cilj takšnega testa.
Red Teaming je edini varnostni test, s katerim ne preverite le varnosti omrežja, temveč dejansko odpornost organizacije na kibernetski napad. Čeprav se morda sliši vabljivo, kibernetska vaja ni primerna za vsako organizacijo. Smiselno je, da podjetje prej že doseže določeno zrelostno raven kibernetske varnosti, kar pomeni, da ima izkušnje z izvajanjem penetracijskih testov, morda tudi z ozaveščanjem uporabnikov in skrbjo za skladnost. Eden od ciljev kibernetske vaje je lahko tudi trening ekipe za odziv. Na podlagi izsledkov vaje ekipa izvajalca (Red Team) poda priporočila ekipi za odziv (Blue Team), ki lahko z njimi izboljša prepoznavanje potencialnih napadov in s tem varnostno držo organizacije. Naprednejša oblika urjenja ekipe za odziv pa je t. i. Purple Teaming, kjer s premišljenimi tehnikami napadov organizacija testira zaznavo napada in glede na reakcijo ekipe za odziv uvede nadaljnje izpopolnjevanje veščin.

4. Ozaveščanje uporabnikov

Poleg testiranja kibernetske varnosti je izredno pomembno tudi neprestano izobraževanje in ozaveščanje uporabnikov. Po statistikah in izkušnjah iz prakse so uporabniki še vedno zelo ranljiv del informacijskega sistema. Z dobro pripravljenim lažnim sporočilom velik delež uporabnikov napadalcem neposredno ali posredno posreduje svoje poverilnice. Sodobni napadi so temeljito premišljeni, pogosto usmerjeni v pridobivanje podatkov o točno določeni osebi ali profilu v organizaciji. Napadalci informacije poiščejo na družabnih omrežjih in spletu ter tudi s pomočjo umetne inteligence pripravijo usmerjena lažna sporočila (*ang. spear phishing*), ki nimajo slovničnih napak, na podlagi katerih jih je bilo mogoče enostavno prepoznati v preteklosti.
Organizacije naj svoje zaposlene izobražujejo o najboljših praksah na področju kibernetske varnosti, kot so močna gesla, varno shranjevanje zasebnih podatkov in zaščita pred napadi z ribarjenjem. V tem kontekstu je priporočljivo, da organizacije spodbujajo zaposlene, naj poročajo o

kakršnem koli sumljivem dogajanju, ki ga opazijo na omrežju ali v elektronski pošti.
Drugi zelo pomemben del ozaveščanja pa je praktični trening prepoznavanja kibernetskih napadov s socialnim inženiringom. V ta namen obstajajo rešitve, ki ponujajo različen obseg vsebin, raznovrstne učne materiale, ki so lahko razvrščeni tudi po težavnosti in tako spodbujajo vedno višjo stopnjo ozaveščenosti in sposobnosti prepoznavanja napadov. Ključni del treninga ozaveščanja je povratna informacija o uspešno ali neuspešno opravljeni vaji. Uporabnike, ki vaje niso uspešno opravili, seznanimo z mesti, ki bi jih v vaji morali prepoznati kot škodljiva (*ang. red flags*), ponudimo jim dodatna izobraževalna gradiva in po določenem času ponovno pošljemo podobno vajo. Skrbnikom programa ozaveščanja je na voljo statistika klikov, s katero lahko merijo trend izboljšanja in uspešno prepoznavajo, kateri oddelki ali skupine uporabnikov bolje napredujejo in jim lahko ponudijo težja gradiva, in kateri potrebujejo dodatne vaje na nižji ravni.
Smiselno je, da organizacije vpeljejo politiko upravljanja z varnostnimi incidenti in določijo postopke, ki jih je treba upoštevati pri poročanju o incidentu. Tako se bodo zaposleni zavedali svoje odgovornosti pri poročanju o incidentih ter se bodo nanje odzvali hitreje in bolj učinkovito. V varnostnih politikah oz. internih pravilnikih naj organizacije določijo pravice in odgovornosti glede na različne uporabniške vloge, hkrati naj po vlogah tudi prilagodijo vrsto in zahtevnost izobraževanja.
Dokumentacija naj bo shranjena na mestu, kjer je dostopna vsem zaposlenim s ciljem, da jo uporabljajo kot smernice pri vsakdanjem delu.
Bančne institucije se pogosto srečujejo tudi s posledicami kibernetskih napadov na komitente. V tem pogledu opažamo vedno večjo angažiranost bank, da z različnimi sredstvi obveščanja komitente opozarjajo na poskuse napadov in jih ozaveščajo o ustreznem ravnanju in prepoznavanju pasti. S takšnimi akcijami banke bistveno pripomorejo k izboljšanju ozaveščenosti o kibernetskih napadih v širšem družbenem kontekstu.
Pri ozaveščanju o kibernetski varnosti je pomembno tudi, da organizacije redno pregledujejo svoje varnostne politike in ustrezno obravnavajo najnovejše kibernetske grožnje. K temu zavezujejo organizacije v finančnem in bančnem sektorju tudi različni standardi in direktive, ki spodbujajo učinkovito upravljanje kibernetske varnosti.

5. Direktiva NIS2 in uredba DORA

Konec leta 2022 je Evropska unija sprejela dva pomembna dokumenta, ki bistveno spreminjata položaj kibernetske varnosti v velikem delu gospodarstva in javne uprave. Direktiva NIS2 določa ukrepe za skupno visoko raven kibernetske varnosti v Evropski uniji, ki jih morajo države članice v lokalno zakonodajo implementirati do sredine oktobra 2024. Med drugim direktiva širi nabor zavezancev, ti pa bodo morali po novem spremljati tudi kibernetska tveganja svojih dobaviteljev. S tem direktiva naslavlja vedno bolj pereč problem napadov prek dobavne verige.
Uredba DORA pa je specializirana za digitalno operativno odpornost finančnega sektorja in je kot taka zavezujoč pravni akt v vseh državah članicah EU. V praksi bo začela veljati 17. januarja 2025 in do takrat se morajo vse institucije, ki jih uredba zavezuje, nanjo ustrezno pripraviti. Obe regulativi sta pomembni za zagotavljanje ustreznih ukrepov, s katerimi se bodo organizacije zaščitile pred potencialnimi kibernetskimi grožnjami in krepile kibernetsko odpornost. Ti ukrepi vključujejo vpeljavo varnostnih pregledov in testiranj, krepitev ozaveščenosti uporabnikov, zaznavanje škodljivih aktivnosti na omrežjih in ustrezen odziv. V primeru kibernetskih incidentov se morajo organizacije odzvati hitro, a koordinirano, odločitve morajo biti preudarne in vsi postopki dokumentirani.
NIS2 in DORA ponujata organizacijam ogrodje, s katerim si lahko pomagajo pri sistematični krepitvi varnostne drže.

6. NIST Cybersecurity Framework

Pri učinkovitem upravljanju kibernetske varnosti se lahko organizacije oprejo tudi na NIST Cybersecurity Framework, ogrodje za upravljanje kibernetske varnosti, ki ga je razvil ameriški nacionalni inštitut za standardizacijo in tehnologijo (NIST). Ogrodje podaja smernice, kako prepoznavati potencialna tveganja in ranljivosti, razviti politike in postopke, da jih lahko obravnavamo,, in razviti načrt odzivanja na incidente. Poleg tega je ogrodje v pomoč tudi pri ocenjevanju zrelosti organizacije na področju kibernetske varnosti ter izpostavljenosti organizacije tveganjem.
Trenutna verzija ogrodja NIST vsebuje petstopenjski krog upravljanja kibernetske varnosti: identifikacija – zaščita – zaznava – odziv – obnova (*ang. identify – protect – detect – respond – recover*). Glavni cilj je cikličnost postopka, s čimer so poudarili, da je kibernetska varnost neprestano razvijajoče se področje, ki zahteva nenehno spremljanje in izboljšave.
V začetku leta 2024 pričakujemo novo verzijo ogrodja NIST, ki uvaja novo kategorijo »upravljanje« (*ang. governance*) in jo postavlja nad vseh pet stopenj kroga. S tem so avtorji ogrodja poudarili pomen obvladovanja kibernetskih tveganj in upravljanje kibernetske varnosti pomaknili bližje vodstvu in odločevalcem.

Če se v okviru tako prepoznanega ogrodja, kot je NIST Cybersecurity Framework, uveljavlja pojem upravljanja, naj si tudi odgovorni za kibernetsko varnost v organizacijah prizadevajo, da sprememb na tem področju vodstvu in upravam ne bodo predstavljali v obliki podatkov o številu novo odkritih ranljivosti ali novo nameščenih varnostnih napravah. Večji poudarek naj bo na vsebini, kot je spremenjeno področje napada, različne oblike groženj in tveganj, in šele nato, kako bodo te izzive naslovili znotraj ekipe in organizacije. Pomembno je prepoznavati kibernetsko varnost kot enega od temeljev za uspešno poslovanje podjetja in tudi varuha ugleda, saj zlasti v ustanovah, kjer se obdeluje veliko osebnih in občutljivih podatkov, vsak vdor in razkritje zelo verjetno pomenita tudi veliko negativno publiciteto. Organizacije, ki so vpeljale standard ISO 27001, so že dokazale, da vodstvo prepoznava informacijsko varnost kot vodilo pri poslovanju, nova verzija standarda iz leta 2022 pa dodatno vpeljuje nekatere kontrole, ki so bolj tehnološko naravnane.

7. Sklepne misli

Če se torej NIST Cybersecurity Framework z dodajanjem elementa upravljanja približuje poslovodstvu, se ISO 27001 v verziji 2022 s tehničnimi kontrolami približuje področju kibernetske varnosti. Ugotovitev je v obeh primerih podobna: kibernetska in informacijska varnost sta področji, ki ju obravnavamo tako s tehnološkega kot poslovodnega vidika in prispevata k uspešnemu delovanju organizacij. Doseganje višje ravni kibernetske varnosti v organizacijah je cikličen postopek, ki zahteva stalno spremljanje, odzivanje na aktualne razmere in izboljševanje. Temelj za izboljšave je jasna slika o stanju kibernetske varnosti, ki jo prikažejo rezultati varnostnih testov in priporočila, osnovana na podlagi teh rezultatov.

Viri

ISO/IEC, 2022: Standard ISO 27001:2022
NIST, 2018: Cybersecurity Framework V1.1
Uradni list Evropske unije, 2022: Direktiva EU 2022/2555
Uradni list Evropske unije, 2022: Uredba EU 2022/2554