BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
AGENCIJA ZA BANKARSTVO FEDERACIJE BOSNE I HERCEGOVINE

Broj: 03-4- 1225/17
Sarajevo, 27.03.2017. godine

**Predmet: Očekivanja Agencije u vezi implementacije sigurnosnih kontrola u procesu SWIFT usluga**

U posljednje vrijeme učestala je pojava cyber napada na mrežu usluga servisa za međubankarsku komunikaciju (SWIFT), uključujući i ponovljene incidente sa Centralnom bankom Bangladeša i bankama u Filipinima i Vijetnamu. Na osnovu do sada poznatih informacija, napadi se nisu desili na dijelu mreže koji je pod ingerencijom servisa SWIFT, nego u dijelovima infrastrukture koja je pod odgovornošću banke. Napadi su se desili na jedan od sljedećih načina:

- krađom legalnih kredencijala bančinih uposlenika za pristup sistemu SWIFT-a,
- korištenjem slabosti u bančinoj infrastrukturi (nedostatak ili neadekvatna konfiguracija firewall-a, neadekvatni routeri, upotreba default-nih ili dobro poznatih lozinki i slično) i
- sistemom socijalnog inžinjeringa koristeći tzv „phishing" napade, koji su odigrali ključnu ulogu.

Prema do sada poznatim informacijama, napadači su primjenili tradicionalni pristup „preuzimanja računa", pri čemu zlonamjerni unutrašnji ili vanjski napadač šalje SWIFT poruke finansijske institucije sa radne stanice povezane sa lokalnim interfejsom prema SWIFT mreži. Na osnovu javno objavljenih informacija, procjenjena šteta do sada iznosi više od 100 miliona dolara.

Navedeni korišteni pristup „preuzimanja računa" se zasniva na iskorištavanju ranjivosti koje su vezane uz neadekvatnu primjenu sigurnosnih praksi i slabosti uposlenika.
U mnogim slučajevima dešava se sljedeće:

- žrtve ne prate osnovne sigurnosne standarde, koji uključuju, između ostaloga, redovnu primjenu patch-eva, mrežne segmentacije i pristupa „najmanje moguće" privilegije, te
- prilikom planiranja cyber napada, uvijek se traže najslabije karike u sistemu, te se najčešće koriste ljudske greške i socijalni inžinjering kako bi se ostvarili ciljevi.

Nedavni cyber napadi su pokazali mogućnost sljedećeg:

- upada u i kompromitovanja infrastrukture banke, pri čemu se zaobilaze sigurnosne kontrole,
- nabave i korištenja validnih kredencijala sa pravima kreiranja, odobrenja i slanja SWIFT poruka,
- primjene sofisticiranih znanja i razumjevanja načina transfera operacija slanja novca,
- korištenje visoko prilagođenih malicioznih kodova kako bi se onemogućilo logiranje (sistem zapisa) i izvještavanje, kao i druge operativne kontrole za prevenciju i detekciju lažnih transakcija i
- prebacivanje ukradenih sredstava preko više različitih nadležnosti u kratkom vremenskom periodu kako bi se onemogućio povrat sredstava.

71000 Sarajevo, Zmaja od Bosne 47b, Bosna i Hercegovina
Tel: ++387 33 72 14 00, Fax: ++387 33 66 88 11
E-mail: agencija@fba.ba Web site: www.fba.ba

Servis SWIFT je poduzeo niz aktivnosti na budućoj prevenciji i detekciji cyber upada u mrežu međubankovne komunikacije. Neke od njih su sljedeće:

- definisana je lista od 16 obaveznih i 11 preporučenih sigurnosnih kontrola koje bi banke trebale implementirati u svrhu zaštite od neželjenih upada u sistem (lista objavljena na Web stranici SWIFT-a je u razmatranju, te se zvanična potvrda liste i kontrola očekuje u martu 2017. godine).
- SWIFT će počev od Q2 2017. godine zahtijevati od svojih klijenata da obave detaljnu samoprocjenu usaglašenosti sa obaveznim kontrolama. Primjena 16 obaveznih kontrola će biti obavezna, počev od januara 2018. godine. Također, SWIFT će provesti pregled odabranih klijenata, pregledom revizorskih izvještaja sačinjenih od strane internih i eksternih revizora kako bi se uvjerio u kvalitet primjene gore definisanih kontrola. Detaljni status implementacije kontrola kod svih klijenata će biti omogućen zainteresovanim stranama putem SWIFT-a.
- također, SWIFT je uveo Program za podršku sigurnosti klijenata, koji sadrži niz alata, između ostalih i tzv. „Daily Validation report", servis kojim se omogućava potvrda svih dnevnih transakcija odvojenim kanalom od samog kanala putem kojeg su obavljene transakcije, kao i slanje liste dnevnih transakcija različitom timu osoblja na potvrdu.

U nastavku je dat pregled obaveznih i preporučenih SWIFT kontrola, te očekivanja Agencije u vezi konkretnog načina implementacije kontrole u okviru informacionog sistema banke, kao i korespondirajući član regulative Agencije (Odluka o minimalnim standardima upravljanja informacionim sistemima u bankama i Odluka o minimalnim standardima upravljanja eksternalizacijom), koji zahtijeva implementaciju navedene kontrole.

# SWIFT obavezne i preporučene sigurnosne kontrole

SWIFT je izdao set ključnih sigurnosnih standarda koji će postati obavezni za sve SWIFT klijente. Primjena ovih standarda će podići nivo sigurnosti za klijente SWIFT mreže, te podržati klijente u njihovim nastojanjima da preveniraju i detektiraju zloupotrebu njihove infrastrukture. Implementacija ovih standarda će također podići svijest o sigurnosti i edukaciji o potrebi kontinuirane borbe protiv prevara povezanih sa cyber kriminalom.

Ovaj ključni set zahtjeva će se primjeniti za sve SWIFT klijente i isti se zasniva na tri cilja i osam principa koji su opisani u tabeli dole ispod. Navedenih 16 obaveznih i 11 preporučenih kontrola podupiru sljedećih osam principa.

## Obavezne sigurnosne kontrole

| Naziv sigurnosne SWIFT kontrole | Zahtjevi vezani uz sigurnosnu kontrolu | Aktivnosti koje Agencija očekuje od banke | Referenca na podzakonske akte koji regulišu upravljanje IS u bankama |
|---|---|---|---|
| **1. Ograničiti pristup internetu i segregirati (odvojiti) kritične SWIFT sisteme od općeg dijela IT okruženja** | | | |
| 1.1 Segregacija (odvajanje) SWIFT okruženja | Lokalna SWIFT infrastruktura treba biti segregirana u sigurnosnu zonu, kako bi bila osigurana od zloupotrebe i napada koji dolaze iznutra iz banke i eksternog okruženja. | Banka treba uspostaviti odvojeni mrežni segment za dijelove infrastrukture koji se upotrebljavaju za obavljanje SWIFT usluge (u nastavku SWIFT infrastruktura, koja obuhvata dio mrežne infrastrukture, printere, servere i druge resurse koji čine poslovni proces pružanja SWIFT usluge; gdje god je moguće uključiti i radne stanice), kao i zabraniti pristup internetu u okviru ove zone. Sve što je vezano za SWIFT infrastrukturu je potrebno odvojiti od opšteg IT okruženja. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| 1.2 Kontrola (nadzor) privilegovanog pristupa operativnom sistemu | Pristup lokalnom operativnom sistemu cjelokupne SWIFT infrastrukture sa administratorskim pravima treba biti ograničen do maksimalne moguće mjere. Korištenje administratorskih ovlasti treba biti kontrolisano, nadzirano i dozvoljeno samo za relevantne aktivnosti kao što je instalacija i konfiguracija software-a, održavanje i hitne aktivnosti. U bilo koje drugo vrijeme, pristup navedenim resursima je ograničen. | Banka treba ograničiti administratorski pristup SWIFT infrastrukturi na najmanju moguću mjeru, uključiti kreiranje logova za cjelokupnu SWIFT infrastrukturu. Na kontinuiranoj osnovi potrebno je pratiti operativne i sistemske zapise cjelokupne SWIFT infrastrukture, naročito računa sa većim privilegijama. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| **2. Umanjiti (reducirati) površinu i ranjivosti prostora za napad** | | | |
| 2.1 Sigurnost internog protoka podataka | Povjerljivost, integritet i autentikacijski mehanizmi trebaju biti implementirani kako bi protok podataka u SWIFT | Banka treba osigurati povjerljivost, integritet i autentikacijske mehanizme unutar SWIFT sigurnosne zone. | Član 15. Odluke o minimalnim standardima upravljanja |

| | | | |
|---|---|---|---|
| | infrastrukturi bio zaštićen, uključujući i link do računara korisnika. | | informacionim sistemima u bankama (kontrole pristupa) |
| 2.2 Sigurnosna ažuriranja | Sav hardware i software unutar SWIFT sigurnosne zone - infrastrukture, uključujući korisničke računare, treba imati podršku od strane dobavljača, biti ažuriran sa obaveznim software-skim verzijama, te sa pravovremenom primjenjenom (instalacijom) sigurnosnih ažuriranja - patcheva (uključujući antivirusnu zaštitu). | Sav software i hardware koji se nalazi u okviru SWIFT infrastrukture treba biti redovno održavan od strane dobavljača hardware/software-a, treba biti pravovremeno i adekvatno ažuriran sa software-skim verzijama (operativni sistem i drugi software u sigurnosnoj zoni), te osigurati pravovremeno instalirane sigurnosne patcheve, kao i ažurnu antivirusnu zaštitu. | Članovi 17., 19. i 20. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (upravljanje promjenama) |
| 2.3 Osnaživanje sistema | Osnaživanje (eng. „hardening“) sistema treba da se provodi na svim sistemima i cjelokupnom SWIFT infrastrukturom, uključujući i korisničke računare. | Sav hardware i software unutar SWIFT infrastrukture 'osnažiti', u smislu tzv. „custom“ instalacije operativnog sistema i ostalih software-a, koji osiguravaju pokretanje samo neophodnih servisa, otvaranje samo neophodnih portova i slično. Na SWIFT infrastrukturi se nalazi instaliran samo software koji je neophodan za obavljanje SWIFT usluga. Na routerima treba biti dozvoljen samo saobraćaj koji se isključivo odnosi na SWIFT. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| **3. Fizička sigurnost okruženja** | | | |
| 3.1 Fizička sigurnost | Fizičke sigurnosne kontrole trebaju biti uspostavljene kako bi se zaštitio pristup osjetljivoj opremi, „hosting“ stanicama i skladištu podataka. | Banka je dužna fizički osigurati prostorije u kojima se nalazi IT infrastruktura koja se odnosi na pružanje SWIFT usluge. | Član 27. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (fizičke kontrole) |
| **4. Preveniranje zloupotrebe kredencijala** | | | |
| 4.1 Politika lozinki | Politike lozinki na svim računima (na svim aplikacijama i operativnim sistemima) su dovoljno jake, sa odgovarajućim parametrima kao što su dužina, kompleksnost, validnost lozinke, kao i broj neuspješnih pokušaja prijave. | Banka je dužna uspostaviti adekvatnu snažnu politiku lozinki za pristup operativnom sistemu, serveru, router-u, aplikacijama koje se nalaze u SWIFT infrastrukturi. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| 4.2. Multi-faktorska autentikacija | Multi-faktorska autentikacija treba da se koristi za interaktivan pristup korisnika prema aplikacijama koje su povezane sa SWIFT-om, kao i računima operativnog sistema. | Banka je dužna osigurati najmanje dvo-faktorsku autentikaciju za pristup aplikacijama koje se odnose na SWIFT, kao i računima operativnog sistema. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| **5. Upravljanje identitetom i segregacija privilegija** | | | |
| 5.1. Upravljanje korisničkim računima | Pristup SWIFT infrastrukturi treba biti definisan u skladu sa sigurnosnim principima na bazi onoga što je potrebno znati (eng. | Potrebno je osigurati adekvatno upravljanje računima za aplikacije koje se odnose na SWIFT, te cjelokupnu SWIFT infrastrukturu, odnosno | Član 15. Odluke o minimalnim standardima upravljanja |

| | | | |
|---|---|---|---|
| | need-to-know access), najmanjih mogućih privilegija (eng. least privilege) i segregaciji dužnosti. | potrebno je osigurati da samo lica koja obavljaju poslove vezane uz SWIFT imaju pristup, koji je usklađen sa poslovnim potrebama radnog mjesta na principu najmanje moguće privilegije i segregacije dužnosti. | informacionim sistemima u bankama (kontrole pristupa) |
| 5.2 Upravljanje tokenom | Tokenima za autentikaciju treba da se upravlja na odgovarajući način tokom izdavanja, povlačenja, korištenja i skladištenja. | Banka je dužna definisati upravljanje tokenima koji uključuju procese izdavanja, povlačenja, korištenja i skladištenja tokena, te voditi evidenciju za svaku pojedinačnu aktivnost od strane osoblja koji su nadležni za provođenje istih, vodeći računa o segregaciji dužnosti i realizaciji aktivnosti putem dva kanala, gdje god je to moguće. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| **6. Otkriti anomalije nad sistemima i/ili evidencijama o transakcijama (zapisima)** | | | |
| 6.1. Zaštita od malicioznog koda | Zaštita od malicioznog koda od dobavljača sa reputacijom treba da je uspostavljena i da se održava ažurnom na svim sistemima. | Banka je dužna implementirati mjere zaštite od malicioznog koda, odnosno imati instaliranu antivirusnu zaštitu na cjelokupnoj SWIFT infrastrukturi. Antivirusna zaštita treba biti ažurna, te se vršiti redovno skeniranje resursa. Također, anitivirusni software koji se koristi treba biti kupljen od strane proizvođača sa reputacijom. | Član 17. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (maliciozni kod) |
| 6.2. Integritet software-a | Provjera integriteta software-a treba da se provodi na redovnoj osnovi nad sučeljem (eng. interface) razmjene poruka, sučeljem komunikacija i drugim aplikacijama povezanim sa SWIFT-om. | Banka je dužna osigurati kontrole provjere integriteta aplikacija i ostalog software-a koji se nalazi u SWIFT infrastrukturi (upravljanje promjenama). | Član 20. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (upravljanje promjenama) |
| 6.3. Integritet baze podataka | Provjera integriteta baze podataka treba da se provodi na redovnoj osnovi nad bazama podataka u okviru kojih se zapisuju (evidentiraju) SWIFT transakcije. | Banka/pružalac usluga treba implementirati kontrole redovne provjere integriteta baza podataka. | Član 20. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (upravljanje promjenama) |
| 6.4. Zapisi i nadzor | Mogućnosti za otkrivanje nepravilnih/nestandardnih aktivnosti treba da su implementirane, te da je uspostavljen proces ili alat kako bi se redovno arhivirali i pregledali zapisi. | Banka je dužna osigurati adekvatan proaktivan nadzor nad operativnim i sistemskim zapisima cjelokupne SWIFT infrastrukture, te procesu/sistemu za uočavanje nestandardnih aktivnosti. Nadzor nad operativnim i sistemskim zapisima treba biti osiguran i kod pružaoca usluga. | Član 16. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (operativni i sistemski zapisi) |
| **7. Plan za odgovor na incidente i dijeljenje informacija** | | | |
| 7.1. Planiranje odgovora na cyber incident | Plan za odgovor na cyber incidente treba biti uspostavljen. | Banka treba imati definisan plan koraka za odgovor i oporavak od cyber incidenta. | Član 22. Odluke o minimalnim standardima upravljanja |

| | | | |
|---|---|---|---|
| | | | informacionim sistemima u bankama (incidenti) |
| 7.2. Edukacija o sigurnosti i podizanje svijesti | Godišnji plan za podizanje svijesti o sigurnosti treba da se provodi za svo osoblje, uključujući specifične edukacije prilagođene ulogama uposlenika u SWIFT procesu koji imaju privilegovani pristup. | Banka je dužna provoditi specifične treninge i edukaciju vezanu uz SWIFT kontrole koja je namijenjena naročito uposlenicima koji rade na SWIFT okruženju. Naročitu je pažnju potrebno posvetiti upoznavanju korisnika sa tzv. „phishnig" metodama, uključujući objavljivanje podataka na društvenim mrežama, nenamjerno otkrivanje kredencijala ili ostalih detalja vezanih uz radno mjesto. Potrebno je obratiti pažnju na dosljednu primjenu sigurnosnih standarda upotrebe računara u banci. | Član 24. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (edukacija) |

## Preporučene sigurnosne kontrole

| Naziv sigurnosne SWIFT kontrole | Zahtjevi vezani uz sigurnosnu kontrolu | Aktivnosti koje Agencija očekuje od Banke | Referenca na podzakonske akte koji regulišu upravljanje IS u bankama |
|---|---|---|---|
| **2. Reducirati (umanjiti) površinu i ranjivosti prostora za napad** | | | |
| 2.4A Sigurnost protoka podataka u Back Office-u | Povjerljivost, integritet i autentikacijski mehanizmi treba da su implementirani kako bi se zaštitio protok podataka između sistema Back Office ili „middleware" i sigurnosne SWIFT zone. | Banka je dužna osigurati kontrole povjerljivosti, integriteta i autentikacijskog mehanizma prilikom razmjene podataka između ključne bankarske aplikacije i ostalih sistema i SWIFT infrastrukture. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| 2.5A Eksterna zaštita podataka u transmisiji (tranzitu) | Osjetljivi podaci koji napuštaju sigurnosnu zonu trebaju biti kriptovani. | Banka je dužna osigurati (izvršiti enkripciju) enkripciju podataka prilikom tranzita SWIFT podataka između sigurnosne SWIFT zone i ostatka sistema. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| 2.6A Integritet korisničke sesije | Integritet i povjerljivost interaktivne korisničke sesije koja se konektuje na sigurnosnu SWIFT zonu trebaju biti osigurani (zaštićeni). | Kontrole koje osiguravaju integritet i povjerljivost korisničke sesije na sigurnosnu SWIFT zonu trebaju biti implementirane. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| 2.7A Skeniranje ranjivosti | Skeniranje ranjivosti treba da se provodi u okviru sigurnosne SWIFT zone, uključujući i korisničke računare korištenjem ažurnih | Banka treba da provodi testiranje (skeniranje) ranjivosti na periodičnoj osnovi korištenjem adekvatnih alata. | Član 5. tačka 8. Odluke o minimalnim standardima |

| | | | |
|---|---|---|---|
| | standardnih (eng. up-to-date industry-standard) alata za skeniranje. | | upravljanja informacionim sistemima u bankama (upravljanje rizicima) |
| 2.8A Eksternalizacija kritičnih aktivnosti | Eksternalizovane kritične aktivnosti treba da su zaštićene, kao minimum, istim standardom kvalitete (brige) kao da se aktivnost provodi u okviru izvorne organizacije (banke). | Banka treba osigurati standarde kvaliteta pružanja usluga koji bi bili primjenjeni u slučaju obavljanja istih aktivnosti unutar banke. Banka se treba uvjeriti koji su sigurnosni standardi implementirani kod pružaoca usluga. | Član 16. Odluke o minimalnim standardima upravljanja eksternalizacijom (kvalitet usluge) |
| 2.9A Poslovne kontrole nad transakcijama | Ograničiti podnošenje transakcije i potvrde o transakciji na očekivani okvir (granicu) normalnog poslovanja. | Ograničiti podnošenje transakcije i potvrde o transakciji na očekivani okvir (granicu) normalnog poslovanja. | Članovi 5. i 18. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (upravljanje rizicima i aplikativne kontrole) |
| **5. Upravljanje identitetima i segregacija privilegija** | | | |
| 5.3A Proces provjere osoblja | Osoblje koje radi na lokalnoj SWIFT infrastrukturi treba da se provjerava prije inicijalnog upošljavanja i periodično nakon upošljavanja. | Banka treba provjeravati dosijee lica koji rade na SWIFT uslugama prije upošljavanja istih, kao i periodično tokom njihovog rada u banci. | Član 5. tačka 8. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (upravljanje rizicima) |
| 5.4A Fizičko i logičko odlaganje lozinki | Sve evidentirane lozinke za privilegovane račune treba da se odlažu na lokacije koje su zaštićene fizički ili logički, sa ograničenim pristupom na bazi onoga što je potrebno znati (eng. need-to-know access). | Banka treba odlagati lozinke za privilegovane račune SWIFT infrastrukture na sigurnu lokaciju, te utvrditi ko ima pristup navedenim lozinkama. Lozinke se odnose na operativne sisteme, aplikacije i mrežne komponente. | Član 15. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa) |
| **6. Detektovati nepravilne aktivnosti nad sistemima i/ili evidencijama transakcija (zapisima)** | | | |
| 6.5A Otkrivanje upada | Otkrivanje upada treba biti obezbijeđeno kako bi se detektovao neautorizovani pristup mreži. | Banka treba osigurati zaštitu od upada u sistem na način da se vrši proaktivan nadzor saobraćaja na router-u, odnosno treba nadzirati mrežni saobraćaj. | Članovi 15. i 16. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (kontrole pristupa i upravljanje zapisima) |
| **7. Plan za odgovore na incidente i dijeljenje informacija** | | | |

| | | | |
|---|---|---|---|
| 7.3A Penetraciono testiranje | Penetraciono testiranje nad aplikacijama, serverima i mreži SWIFT infrastrukture treba da se provodi najmanje godišnje, uključujući i korisničke računare. | Banka treba osigurati provođenje penetracionog testiranja nad resursima koji se koriste u svrhu SWIFT servisa. | Član 5. tačka 8. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (upravljanje rizicima) |
| 7.4A Procjena rizika na bazi scenarija | Procjena rizika na bazi scenarija treba da se provodi redovno kako bi se unaprijedila pripremljenost za odgovore na incidente i kako bi se povećala zrelost sigurnosnog programa organizacije. | Banka treba provoditi procjenu rizika koji su povezani sa SWIFT uslugama, a kako bi pripremila odgovore na incidente, kao i sigurnost SWIFT infrastrukture. | Član 5. tačka 8. Odluke o minimalnim standardima upravljanja informacionim sistemima u bankama (upravljanje rizicima) |

FEDERACIJA BOSNE I HERCEGOVINE — AGENCIJA ZA BANKARSTVO FEDERACIJE BOSNE I HERCEGOVINE — SARAJEVO

DIREKTOR

Jasmin Mahmuzić