ОЧЕКИВАЊА АГЕНЦИЈЕ ЗА БАНКАРСТВО РЕПУБЛИКЕ СРПСКЕ ВЕЗАНО ЗА ИМПЛЕМЕНТАЦИЈУ ОБАВЕЗНИХ И ПРЕПОРУЧЕНИХ БЕЗБЈЕДНОСНИХ КОНТРОЛА СЕРВИСА ЗА МЕЂУБАНКАРСКУ КОМУНИКАЦИЈУ (SWIFT)

У последње вријеме учестала је појава сајбер напада на мрежу Сервиса за међубанкарску комуникацију (SWIFT). Ови напади користе рањивости у процесима и процедурама финансијских институција које користе услуге SWIFT-а, посебно финансисјких институција из земаља у којима су регулаторне и безбједносне контроле мање захтијеване.

Највећи сајбер напади у 2016. години су довели до губитка од преко 100 милиона долара (Централна банка Бангладеш, Banco del Austro из Еквадора, ...). Према званично доступним информацијама напади се нису десили на инфраструктури која је у надлежности SWIFT-а, него у дијеловима инфраструктуре која је у надлежности банке и реализовани су:

- коришћењем рањивости у инфраструктури банке,
- крађом валидних кредендијала запослених за приступ SWIFT систему и
- техникама социјалног инжењеринга.

Иако су сви корисници одговорни за безбједност властитог окружења, имајући у виду да је цијели систем јак колико и његов најслабији корисник, SWIFT је увео Програм безбједности корисника (CSP) како би подржао кориснике у борби против сајбер напада.Овим програмом се уводе обавезне безбједносне контроле, нове услуге у циљу спречавања и откривања неуобичајених и сумњивих активности и размјена информација на нивоу заједнице.

Као прво корисници треба да заштите своје локално окружење, те је SWIFT дефинисао контролни оквир корисничких безбједносних контрола (SWIFT Customer Security Controls Framework) који описује 16 обавезних и 11 препоручених безбједносних контрола. Сви корисници су у обавези да почев од другог квартала 2017. године обаве самопроцјену усаглашености са обавезним контролама (након тога на годишњој основи), а до краја 2017. године имплементирају обавезне контроле унутар локалне SWIFT инфраструктуре. Препоручене контроле су засноване на добрим праксама и њихова имплементација и употреба се препоручује од стране SWIFT-а. Статус усклађености сваког корисника биће доступан заинтересованим странама, те ће оне бити у могућности да на основу процјене ризика доносе одлуке са ким ће пословати.

SWIFT је увео нове алате за извјештавање како би корисницима, посебно малим, пружио дневне извјештаје о активностима који пружају независну евиденцију о њиховим трансакцијама преко SWIFT-а. Омогућена је додатна провјера трансакција како би се спријечиле и открили преваре, као и преглед великих и неуобичајених токова.

У следећој табели дајемо преглед обавезних и препоручених (П) контрола и очекивања Агенције за банкарство Републике Српске везано за имплементацију истих, а које су и у

складу са подзаконским актима Агенције која регулишу управљање информационим системом у банкама.

Обавезне и препоручене контроле		Очекивања Агенције
1. Ограничити приступ интернету и издвојити критичне системе од осталог ИТ окружења		
1.1 Заштита SWIFT окружења	Обезбиједити заштиту локалне SWIFT инфраструктуре корисника од потенцијално компромитованог осталог ИТ окружења, као и ванског окружења.	Локалну SWIFT инфраструктуру треба издвојити у посебну безбједносну зону, како би била заштићена од злоупотребе и напада из интерне мреже Банке и ванског окружења. Ограничити приступ интернету на корисничким радним станицама.
1.2 Контрола привилегованог приступа оперативном систему	Ограничити и контролисати употребу и додјелу налога са администраторским привилегијама.	Ограничити приступ налозима са администраторским привилегијама (предефинисани налози, root,...) на најмању могућу мјеру. Употребу ових налога строго контролисати, надзирати и дозволити само за одређене активности као што су инсталација и конфигурација софтвера, одржавање и хитне активности. У свим другим случајевима, користити налоге са мањим привилегијама. Редовно анализирати записе о употреби ових налога.
2. Смањити изложеност нападима и рањивостима		
2.1 Заштита интерног преноса података	Обезбиједити повјерљивост, интегритет и аутентичниост података у преносу између SWIFT апликација и од апликација до корисничких радних станица	Обезбиједити заштиту података у интерном преносу од неовлаштеног објављивања, измјене и приступа било да се ради о преносу између SWIFT апликација или између корисничке радне станице и SWIFT апликација.
2.2 Безбједносна ажурирања	Смањити појаву рањивости унутар локалне SWIFT инфраструктуре обезбјеђењем подршке произвођача, примјеном обавезних ажурирања софтвера и правовременом	Обезбиједити да сав хардвер и софтвер унутар локалног SWIFT окружења, као и на корисничким радним станицама има адекватну подршку произвођача, примјењена обавезна ажурирања софтвера и благовремено примјењене

Обавезне и препоручене контроле		Очекивања Агенције
	примјеном безбједносних ажурирања у складу са процјеном ризика.	безбједносне исправке.
2.3 Ојачавање система	Смањити изложеност нападима компоненти локалне SWIFT инфраструктуре примјеном безбједносних препорука.	Унутар локалне SWIFT инфраструктуре провести безбједносне препоруке (препоруке произвођача, добре праксе,..). Као минимум измијенити предефинисане лозинке, онемогућити и преименовати непотребне корисничке налоге, онемогућити и ограничити непотребне сервисе, портове и протоколе,…
2.4П Заштита преноса података у back office-у	*Обезбиједити повјерљивост, интегритет и обострану аутентичност у преносу података између back office-а (или middleware) апликација и компоненти SWIFT инфраструктуре.*	*Обезбиједити заштиту података од неовлаштеног објављивања, измјене и приступа у преносу између back office-а и SWIFT апликација.*
2.5П Заштита екстерног преноса података	*Заштити повјерљивост података који се односе на SWIFT при преносу и похрањивању изван безбједносне зоне.*	*Осјетљиви подаци у складу са интерном класификацијом банке и важећом регулативом при преносу и приликом чувања (резерне копије података) изван локалног SWIFT окружења морају бити криптовани. Потребно је примијенити безбједне алгоритме криптовања.*
2.6П Повјерљивост и интегритет корисничке сесије	*Заштити повјерљивост и интегритет интерактивних корисничких сесија на локалну SWIFT инфраструктуру*	*Интерактивне корисничке сесије реализовати коришћењем безбједних протокола (ssh, https,….)*
2.7П Провјера рањивости	*Идентификовати потенцијалне рањивости унутар локалног SWIFT окружења редовним провођењем провјере рањивости.*	*Редовно проводити провјеру рањивости локалног SWIFT окружења, а обавезно након значајних промјена. Користити ажурне специјализоване алате познатих произвођача. Резултате документовати, а уочене*

Обавезне и препоручене контроле		Очекивања Агенције
		рањивости анализирати, отклонити или ублажити.
2.8 П Екстернализација критичних активности	*Заштити локалну SWIFT инфраструктуру од изложености ризику екстернализације критичних активности*	*Обезбиједити да су за екстернализоване критичне активности најмање примијењени стандарди заштите који би били примјењени у случају да се ове активности проводе унутар банке.*
2.9П Пословне контроле трансакција	*Ограничити активности трансакција само према провјереним и одобреним клијентима и у оквире очекиваних граница "нормалног" пословања*	*Имплементирати пословне контроле које ће омогућити детекцију, превенцију и валидацију тако да ограниче трансакционе активности у оквире нормалног пословања (радно вријеме, износи трансакција, валута,...) и смање могућност за слање и пријем неуобичајених и сумњивих трансакција.*
3. Физичка безбједност окружења		
3.1 Физичка безбједност	Спријечити неовлаштен физички приступ осјетљивој опреми, радном окружењу, просторијама у којима се налази локална SWIFT инфраструктура и подаци.	Имплементирати мјере заштите и контроле приступа просторијама у којима је се налази осјетљива опрема, локална SWIFT инфраструктура и подаци.
4. Спријечити компромитовање креденцијала		
4.1 Политика лозинки	Обезбиједити да су лозинке отпорне на нападе погађања имплементацијом и наметањем јаке политике лозинки.	Сви налози за приступ апликацијама и оперативним системима треба да користе јаке лозинке при чему параметри као што су дужина, комплексност, трајање и број неуспјешних покушаја логовања требају бити у складу са безбједносним препорукама.
4.2 Мултифакторска аутентификација	Спријечити могућност да компромитивање једног фактора аутентификације омогући приступ SWIFT	Обезбиједити мултифакторску аутентификацију за приступ SWIFT апликацијама и корисничким радним станицама.

Обавезне и препоручене контроле		Очекивања Агенције
	системима имплементацијом мултифакторске аутентификације.	
5. Управљање идентитима и раздвајање привилегија		
5.1 Логичке контроле приступа	Додјељивање корисничких налога вршити у складу са принципима безбједности : треба да зна (need-to-know), принцип најмањих могућих привилегија и раздвајање дужности.	Обезбиједити да се ауторизација корисника заснива на принципу додјеле најмањих могућих права приступа потребних за обављање послова. Корисницима омогућити приступ само оном што треба да знају и онолико дуго колико постоји та потреба. Обезбиједити раздвајање осјетљивих дужности.
5.2 Управљање токенима	Обезбиједити адекватно управљање, праћење и употребу токена за аутентификацију (ако се користе токени).	Уколико се користе токени за аутентификацију успоставити адекватан процес управљања (издавање, употреба, чување).
5.3 П Процес процјене подобности особља	*Обезбиједити поузданост особља које има приступ локалном SWIFT окружењу провођењем процјене подобности особља.*	*Успоставити процес процјене подобности особља, које ће имати присуп локалној SWIFT инфраструктури, приликом запошљавања, као и периодично након тога.*
5.4 П Физичка и логичка заштита лозинки	*Обезбиједити адекватну заштиту лозинки било да се чувају физички или логички.*	*Физички заштити лозинке привилегованих налога уколико се чувају записане на папиру или неки други начин, а уколико се чувају у електронском облику криптовати локације на којима се чувају. Дозволити приступ запосленима на принципу need-to-know.*
6. Детектовати неуобичајене активности на системима и трансакцијама		
6.1 Заштита од малициозног кода	Обезбиједити да је локална SWIFT инфраструктура заштићена од малициозног кода.	Инсталирати софтвер за заштиту од малициозног кода од познатог произвођача и одржавати га ажурним. Најмање седмично вршити потпуно скенирање.

Обавезне и препоручене контроле		Очекивања Агенције
6.2 Интегритет софтвера	Обезбиједити интегритет софтвера SWIFT апликација.	Успоставити редовну провјеру интегритета софтвера на интерфејсу за размјену порука, комуникационом интерфејсу и другим SWIFT апликацијама. Провјеру вршити приликом покретања и најмање још једном у току дана.
6.3 Интегритет базе података	Обезбиједити интегритет базе података SWIFT интерфејса за размјену порука.	Обезбиједити редовну провјеру интегритета базе података у коју се записују SWIFT трансакције, како би се осигурао интергритет на нивоу слога.
6.4 Записи и праћење	Обезбиједити да се записују безбједносни догађаја и детектују неуобичајене радње и операције унутар локалног SWIFT окружења.	Имплементирати системе за откривање неуобичајених активности, како би се редовно биљежили, архивирали и прегледали записи.
6.5A Детекција напада	*Открити и спријечити неуобичајене мрежне активности према локалном SWIFT окружењу и унутар њега.*	*Имплементирати системе за детекцију напада како би се открио неовлашћен приступ мрежи.*
7. План за одговор на инциденте и дијељење информација		
7.1 План одговора на сајбер инцидент	Обезбиједити досљедан и ефикасан приступ за управљање сајбер инцидентима.	Банка треба израдити и тестрати план одговора на сајбер инциденте.
7.2 Едукација и подизање свијести	Обезбиједити да су запослени свјесни и да испуњавају своје одговорности везано за безбједност, провођењем редовних едукација и активности о подизању свијести о безбједности.	У оквиру годишњег програма за успостављање и подизање свијести о безбједности ИС проводити едукацију запослених који раде на пословима SWIFT-а. Од посебног је значаја да запослени који имају привилегован приступ имају адекватна знања и искуство.

Обавезне и препоручене контроле		Очекивања Агенције
7.3 A Пенетрационо тестирање	*Оперативно провјерити безбједност конфигурација и идентификовати безбједносне недостатке провођењем пенетрационих тестова.*	*Најмање једном годишње проводити пенетрациона тестирања апликација, сервера и мреже унутар локалног SWIFT окружења и корисничких радних станица.*
7.4 A Процјене ризика на бази сценарија	*Процијенти ризик и спремност организације на основу могућих сценарија сајбер напада.*	*Редовно проводити процјену ризика на бази различитих сценарија сајбер напада како би се утврдила вјероватноћа и утицај на банку. Резултати процјена треба да помогну у идентификовању ризичних подручја, захтијевају додатне активности, ублажавање ризика и ажурирање планова за одговор на сајбер инцидент.*

Број: 01-110-1011 /17
26.05.2017. год.
Бања Лука

ЗАМЈЕНИК ДИРЕКТОРА

Драган Сердар