НАРОДНА БАНКА НА РЕПУБЛИКА МАКЕДОНИЈА
„ИНТЕРНО"

Сектор за супервизија, банкарска регулатива и финансиска стабилност

Бр. _____ **Скопје, 10.2.2016 година**

До сите банки
- **за управниот одбор**

Народната банка изработи алатка за оценување на ризиците поврзани со компјутерски напади во дигиталниот простор за да им помогне на органите на Банката да извршат мерење на нивната изложеност и способност да се соочат со потенцијалните закани присутни во дигиталниот простор (англ. cyberspace). Алатката е достапна на интернет-страницата на Народната банка, во папката „Банкарска супервизија и регулатива/Извештаи, показатели, презентации и обрасци / Алатки / Алатка за самооценување на ризиците поврзани со компјутерски напади во дигиталниот простор". Овие активности се дел од годишниот план за теренски контроли, одобрен од страна на Гуверенерот на Народна Банка на Република Македонија. Ваквиот начин на контрола се изведува за да се увидат одредени практики на хоризонтална основа низ целокупниот финансиски систем на Република Македонија. Доколку одредени процеси отскокнуваат кај некоја Банка и/или за истите има потреба да се доразработат со одредени методологии, Народната Банка ќе преземе соодветни активности.

По добивањето на овој допис, треба да назначите одговорно лице - координатор и да преземете навремени мерки за спроведување плански активности за извршување на овој процес на самооценување во вашата банка. Банката треба да подготви краток план за спроведување на активностите и истиот да го достави до Народната банка најдоцна до 26-ти февруари 2016 година. Краен рок за спроведување на самооценувањето и доставување на материјалите од извршената оценка до Народната банка е 31 март 2016 година. Со цел да се олесни спроведувањето на самооценката од страна на банките, Народната банка ќе организира презентација за овој процес на 17.02.2016 година, со почеток во 10 часот, во просториите на Народната банка на 8-ми кат. На презентацијата ги повикуваме да присуствуваат: еден член од управниот одбор (задолжен за информативната технологија или ризици), лицето одговорно за сигурноста на информативниот систем и раководителот на организациската единица за ИТ.

Одговорни лица за спроведување на активностите поврзани со оваа тематска контрола се: Горан Јанкоски, самостоен советник и Василка Апостолска, самостоен советник супервизор во Дирекцијата за теренска супервизија. Со оглед на тоа дека оваа практика на самооценување на ризиците за првпат ќе се изведува во нашиот финансиски систем,

Народната банка препорачува органите на банките да ги спроведат активностите, за да се комплетираат информациите во зацртаните временски рамки.

Раководството треба да ја користи алатката за самооценување на редовна основа, а не само при барање од Народната банка. Доколку имате одредени забелешки и прашања за делови од прашањата содржани во алатката, ве молиме да ги испратите на: jankoskig@nbrm.mk

Со надеж дека на овој начин ќе ја зајакнеме нашата заедничка цел за унапредување на подготвеноста на деловните банки во однос на новите закани и ризици присутни во модерното време, Ви благодариме на соработката.

Генерален директор
Милица Арнаудова Стојановска

Прилог:

Алатка за самооценување на ризиците поврзани со компјутерски напади во дигиталниот простор

Народната банка внимателно ги следи активностите коишто се однесуваат на директни и индиректни штети поврзани со организирани компјутерски напади во дигиталниот простор (англ. cybercrime). Се забележува нагло зголемување на бројот на нападите коишто се случуваат кај банките во нашето соседство, во делот на платниот промет, платежните картички и брзиот трансфер на пари. Како мета на напад, сè почесто, се клиентите на банките - правни и физички лица кои се корисници на услугите на интернет и на мобилно банкарство. Напаѓачите користат напредни компјутерски техники за кои производителите сè уште немаат издадено сигурносни поправки или, пак, ги користат познатите слабости на банките од ненавремено ажурирање на своите ИТ-системи. Мотивите на овие напаѓачи не се ограничени исклучиво на остварување финансиска добивка. Тие се насочени кон нарушување на репутацијата на Банката, предизвикување нефункционалност на одредена банкарска услуга, како и кон нарушување на паричните текови во целиот финансиски систем. Притоа, напаѓачите имаат помош од лица резиденти во Република Македонија, кои за остварувањето на таа цел стануваат клиенти во банките. Нивната задача е да воспостават логистика (отворање денарски и девизни сметки, отворање електронско и мобилно банкарство) и да обезбедат информации за воведените банкарски производи и технологии, видовите на апликациите коишто банките ги користат и нивото на заштита присутна кај одредена финансиска институција.

Стандардите за сигурност на информативниот систем коишто ги користат банките во поширокиот регион се на исто или слично ниво со нашата регулатива и тие не ги опфаќаат во целост сегментите поврзани со заканите од дигиталниот простор. Оттука, имајќи го предвид зголемениот број на нападите во непосредното соседство, како и недостигот од превентивни средства од страна на Банките, се наметна потребата **Народната банка да подготви алатка со која секоја банка ќе може да изврши оценувањето на инхерентниот ризик и да воведе соодветно ниво на подготвеност**. Во алатката се вградени стандардите коишто Народната банка ги има воспоставено во делот на соодветното управување со ризиците во делот на сигурноста на информативниот систем, а користени се и најдобрите практики и индустриски стандарди во делот на сигурноста во дигиталниот простор (Cybersecurity[1]).

Со оваа алатка Банката ќе може да ја измери својата подготвеност од ваков тип закани и ќе ги унапреди и ќе ги прошири своите сознанија во делот на соодветното управување со сигурноста во дигиталниот простор преку:

- утврдување на факторите коишто придонесуваат кон зголемено ниво на ризик од заканите од ваков тип;
- утврдување на нивото на подготвеност од вакви напади и проверка дали тој е усогласен со профилот на ризик;
- утврдување пакет корективни активности коишто се потребни за подобрување на постојното ниво и за постигнување на посакуваното ниво;
- подобрување на информираноста за овие ризици во Банката и воспоставување размена на корисни информации за навремено спречување на ваквите напади во иднина.

[1] Процес на заштита на информацијата којшто се одвива преку навремено преземање контроли за спречување напади, рано откривање на нападите и нивно запирање (def. NIST-Cybersecurity)

Алатката не е наменета само за еднократно мерење и оценување и треба да се користи постојано за потребите на институцијата. Заради соодветно управување со процесите на самооценување, потребно е Управниот одбор да ги изврши следниве задачи:

- да назначи координатор на оваа активност и да изготви план со активности за да се спроведе самооценувањето;
- да ги одобри резултатите од извршеното самооценување;
- да предложи стратегија за воспоставување соодветно ниво на подготвеност и акциски планови;
- да воспостави акциски план за одржување на нивото на подготвеност и надминување на утврдените слабости;
- активно да ги следи информациите поврзани со нови закани и ризици во делот на сигурноста во дигиталниот простор;
- да ги анализира резултатите од спроведеното самооценување и да ги информира членовите на Надзорниот одбор за резултатите од самооценувањето и спроведените активности.

Улогата на Надзорниот одбор во процесот на самооценување се однесува на следново:

- следење на плановите и резултатите од извршеното самооценување, вклучувајќи ги и резултатите и мислењата спроведени од други независни и стручни тимови на овој процес на самооценување;
- ревидирање на одлуките на раководството за постојното ниво на подготвеност и одобрување на предложената стратегија за воспоставеното ниво на подготвеност.

Алатка за самооценување

Со алатката е предвидено процесот на самооценување да се одвива во два чекора. Како прв чекор, потребно е да се одреди инхерентото ниво на ризик, за потоа да се изврши оценување на нивото на подготвеност (cybersecurity maturity). По комплетирањето на двата дела од овој процес, раководството треба да пристапи кон анализа на податоците и носење деловни одлуки поврзани со овој процес.

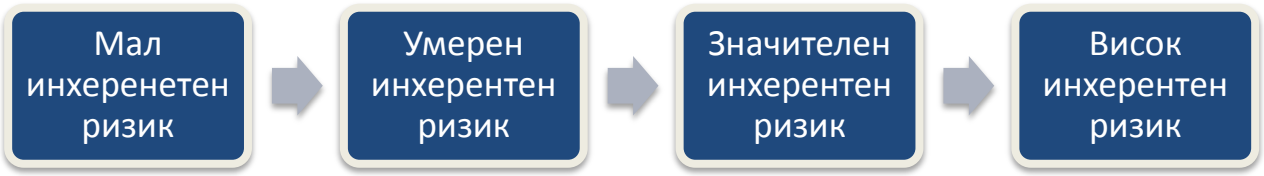
Чекор 1: Утврдување на инхерентниот ризик

Инхерентниот ризик во делот на сигурноста во дигиталниот простор се утврдува преку анализата на пет области:

1. Технологии и типови на поврзување (применетата информативна технологија и типот на поврзување со надворешните системи);
2. Алтернативни канали (отворените канали преку кои може да се разменуваат информации со надворешни лица и клиенти);
3. Производи коишто се достапни преку алтернативните канали (електронско, мобилно банкарство, платежни картички);
4. Организациски карактеристики и
5. Надворешни закани.

При оценувањето на инхерентниот ризик се земаат предвид големината, комплексноста, видот и обемот на активностите коишто се изведуваат во Банката, како и специфичните закани на кои е изложена во своето работење. **При оценувањето на инхерентниот ризик не се земаат предвид спроведените контроли за намалување на постојните ризици.** За утврдување на нивото на инхерентен ризик водете се од насоките во алатката коишто се дадени за полесно одредување на соодветното ниво. Со точното одредување на нивото на

инхерентен ризик може да се утврдат присутните ризици во деловните процеси и агрегатното ниво на инхерентен ризик на кое е изложена Банката. Агрегатното ниво на инхерентен ризик се пресметува автоматски, врз основа на сите одговори за инхерентниот ризик во петте области. *Согласно со методологијата за оценувањето на инхерентните ризици во деловните процеси, предвидени се четири нивоа за категоризација на инхерентниот ризик, и тоа: мал, умерен, значителен и високо ниво на ризик*.



Во продолжение се наведени критериумите за категоризација на агрегатното ниво на инхерентен ризик:

- **Мал инхерентен ризик** - Банката користи едноставна технологија при извршувањето на своите активности со мал број на компјутери и апликации. Банката нема големо портфолио на банкарски производи, ниту во број, ниту во обем. Активностите главно се извршуваат во централата на Банката. Постои ограничен број на експозитури и филијали коишто се поврзани со централата. Јадрото на банкарските операции може да биде сместено во друштво за помошни услуги. Банката користи докажани, сигурни технологии при извршувањето на своите активности. Таа одржува само мал број на поврзувања со надворешни лица и клиенти со ограничена сложеност.

- **Умерен инхерентен ризик** - Банката користи посложена технологија во извршувањето на своите активности. Операциите коишто ги извршува се со зголемен обем. За одредени помошни финансиски активности, Банката може да користи друштво за помошни услуги од областа на ИТ, меѓутоа јадрото на банкарските услуги е сместено интерно. Постојат различен број на производи и услуги коишто се нудат преку различни алтернативни канали до крајните клиенти.

- **Значаен инхерентен ризик** - Банката користи главно комплексна технологија и нуди комплексни банкарски производи, од кои одреден број се засновани врз најнови информатички технологии. Интерно, во Банката се сместени и се одржуваат значителен број на системи и апликации. Се користат значителен број на различни персонални уреди во секојдневното работење. Банката има телекомуникациска инфраструктура за поврзување со експозитурите, клиентите и надворешните институции. Банката има значително учество (по број и вредност) во вкупниот обем на платни трансакции (во земјата и во странство).

- **Висок инхеренетен ризик** - Банката користи најкомплексни технологии за да ги поддржи своите сложени банкарски производи и услуги. Голем број од тие производи и услуги се со највисоко ниво на ризик. Новите напредни технологии коишто се појавуваат редовно се вградуваат во ИТ-системите. Банката користи друштво за помошни услуги од областа на ИТ за обработка на своето јадро на банкарски услуги, но одредени системи може да бидат сместени и во Банката. Банката одржува голем број различни точки на интерконекција со надворешни ИТ-системи за размена на податоци со надворешни фирми и/или клиенти.

Чекор 2: Утврдување на нивото на подготвеност (Cybersecurity maturity)

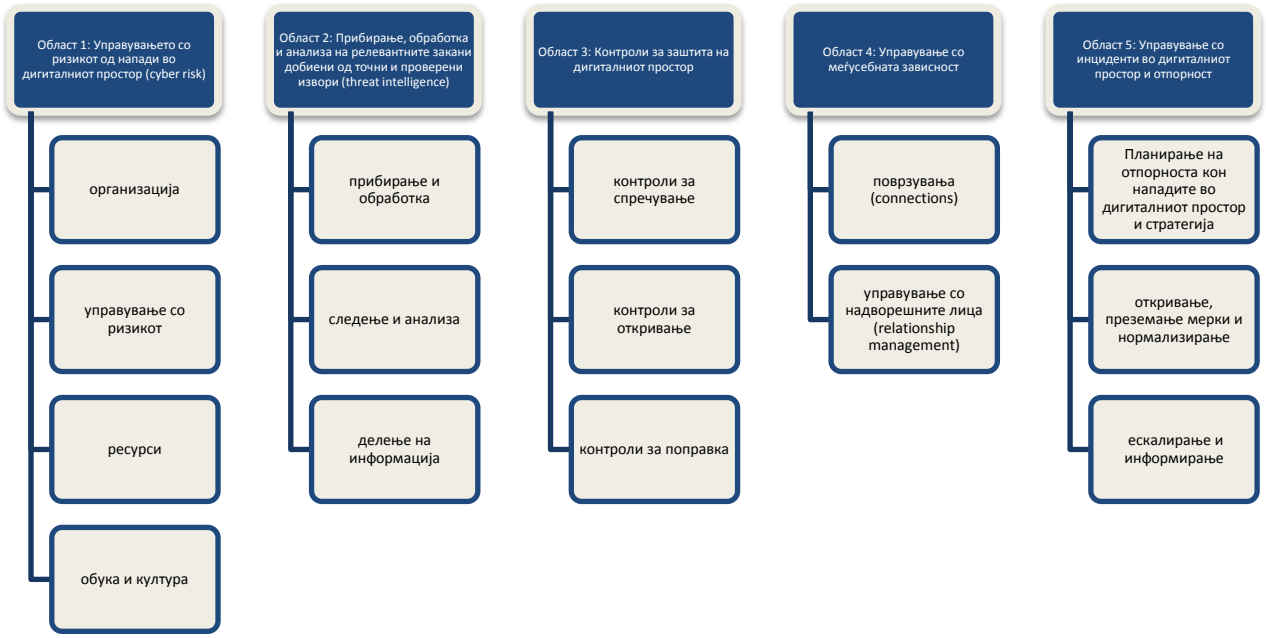
Вториот чекор во самооценувањето е одредувањето на нивото на подготвеност на Банката за справување со ризиците. Ова ниво ќе се одреди преку извршената оценувањето на инхеренетниот ризик направена со претходниот чекор и оценувањето на ефикасноста на имплементираните контроли. *Нивото на подготвеност е категоризирано во три нивоа, и тоа: основно, средно и напредно.*

Одредувањето на соодветното ниво е чекор којшто е од суштинско значење за целиот процес.

Оценувањето на нивото на подготвеност се прави посебно во **пет одделни области**, и тоа:

1. Управување со ризикот од напади во дигиталниот простор (cyber risk),
2. Прибирање, обработка и анализа на релевантните закани добиени од точни и проверени извори (threat intelligence),
3. Контроли за заштита на дигиталниот простор,
4. Управување со меѓусебната зависност и
5. Управување со инциденти во дигиталниот простор и отпорност.

Овие пет области се поделени на повеќе фактори за оценување, а составен елемент на факторите за оценување се компоненти. За оценување на секоја компонента, во алатката се дадени соодветни насоки. За секоја компонента се разработени фрази (декларативни реченици) коишто даваат опис за секое ниво. За секоја компонента, за секое ниво (основно, средно и напредно), се подготвени различни фрази. **Раководството треба да процени и да одлучи која фраза најдобро ја прикажува постојната ситуација и практика во Банката.** Доколку се избере повисоко ниво на подготвеност (cybersecurity maturity), треба да се задоволени новите фрази од повисокото ниво, како и сите фрази од пониските нивоа. Изборот на соодветна фраза ќе ја утврди оценката за одредена компонента. Идејата е да се добие соодветна оценка за нивото на подготвеност (cybersecurity maturity level) за секоја од областите, а не општа (агрегирана) оценка. На графиката подолу се прикажани петте области со поодделните фактори за оценување.



На табелата подолу се прикажани зависностите помеѓу инхерентното ниво на ризик и нивото на подготвеност. Раководството треба да донесе одлука за нивото на подготвеност во секоја област од нападите во дигиталниот простор, во зависност од оценките на инхерентното ниво на ризик. Доколку има суштински измени во инхерентното ниво на ризик, со појавата на нови закани и слабости и значајни измени во организациската структура се очекува ревидирање на одлуките коишто ги донесло раководството во претходните фази. **Општата препорака на Народната банка е да се спроведе основно или средно ниво на подготвеност. Народната банка може да препорача постигнување повисоко ниво на подготвеност во одреден временски период, доколку оцени дека тоа е потребно.** Очекувањата се дека банките со текот на времето ќе се подобруваат и ќе се унапредуваат во повисоки нивоа на подготвеност.

Ризик/Ниво на подготвеност		Инхерентен ризик			
		Мал	Умерен	Значаен	Висок
Ниво на подготвеност (cybersecurity maturity level) за секоја област	Напредно				
	Средно				
	Основно				

Раководството треба да одлучи кои активности треба да се спроведат за да се намали инхерентното ниво на ризик или за да се постигне посакуваното ниво на подготвеност. Оваа активност треба да се спроведе преку акциски план за надминување на слабостите и постигнување на утврденото ниво на подготвеност, согласно со насоките дадени во фразите за поодделните нивоа. Раководството во одредени случаи треба да преземе дополнителни заштитни контроли за задржување на постојното ниво или за негово подигнување.

Раководството треба да ја користи оваа алатка за самооценување на редовна основа, а особено при промени во инхерентниот профил на ризик, кога се појавуваат нови закани во

регионот и пошироко, при измени во деловната стратегија со воведување нови модерни банкарски производи и услуги, ширење на други пазари и воведување на други надворешни лица и добавувачи.

Раководството треба да обезбеди процесот на самооценување да се спроведе на ниво на целата банка, за да бидат опфатени сите деловни процеси и за да бидат соодветно коригирани сите утврдени слабости, во зависност од донесената одлука за нивото на подготвеност.

Во наредниот дел се дадени прашања коишто треба да му помогнат на раководството при извршувањето на самооценувањето и изборот на соодветното ниво на подготвеност.

Одредување на инхерентното ниво на ризик (Inherent Risk Profile)

- Дали е воспоставен процес на оценување на инхеренетниот ризик и на ниво на подготвеност во поглед на сигурноста во дигиталниот простор?
- На каков начин се постапува со информациите коишто се добиваат од самооценувањето? Дали овие резултати ја даваат целосната слика за ризиците во целата банка?
- Кои се областите со највисоко ниво на инхерентен ризик?
- Дали раководството има предвидено да врши ажурирање на инхерентното ниво на ризик при промена во деловна активност, нови услуги и производи?

Ниво на подготвеност од заканите во дигиталниот простор (Cybersecurity maturity)

- Дали воспоставениот процес на оценување и мерење на ризиците ги опфаќа и ризиците присутни во дигиталниот простор? Колку се ефикасни воспоставените контроли согласно со извршеното оценување?
- Дали постои подобар начин за општо подобрување на начинот на управување со ризиците и воспоставување контроли?
- Кои се клучните процеси каде што има зголемено инхерентно ниво и кои се клучните контроли за намалување на овие ризици?
- Дали се користат надворешни лица при извршување критични деловни активности?
- Кој метод го користи институцијата за надгледување на ризиците присутни кај друштвото и како влијае тоа врз инхерентниот ризик и прифатливото ниво на ризик?
- Каков процес е воспоставен за надгледување на типот и големината на нападите од дигиталниот простор?
- Дали институцијата има воспоставено процес на размена на информации за потенцијални закани со надлежните институции и/или со критични надворешни лица и/или банки и/или клиенти, преку одделни процедури за размена на информации за напади во дигиталниот простор?

Управување и надзор над сигурноста во дигиталниот простор (Cybersecurity management & oversight)

- Кои се потенцијалните закани во дигиталниот простор (cyber threats) за институцијата?
- Дали институцијата претрпела штета (директна и индиректна) од вакви напади?
- Дали подготвеноста за отпорност од напади од дигиталниот простор се разгледува на седници на членовите на Управниот одбор и/или нивен одбор?
- Дали интерните акти се ажурирани во зависност од изборот на соодветното ниво на подготвеност од страна на раководството?
- Дали постои редовен процес на прибирање, мерење, следење и информирање за настанатите слабости и потенцијални ризици?

- Кој е одговорен за мерење и управување со ризиците коишто произлегуваат од промена на деловната стратегија и/или промена на технологијата?
- Дали инхерентниот профил на ризик и нивото на подготвеност се на очекуваните нивоа поставени од страна на раководството, дали е разработен акциски план за надминување на утврдените слабости? Дали делови од овој процес се дел од рамката за управување со другите ризици (оперативен/ИТ)?