Народна Банка на Република Македонија

Ризиците присутни во дигиталниот простор

Дирекција за теренска супервизија

17 февруари 2016 година

Агенда

1. **Нови трендови, закани и ризици**
2. Активности на НБРМ
3. Алатка за самооценка на ризиците од дигиталниот простор
4. Активности на Банките

Нови трендови-закани и ризици

- рапидно зголемување на бројот на трансакциите кои се изведуваат дигитално во светски рамки и се повеќе компании ги извршуваат своите деловни активности преку интернет (евтина процесорска моќ и расположива меморија во cloud)
- дигиталната економија генерира промет помеѓу 2 и 3 трилиони $ во светски рамки и истата расте (McAfee: Estimating the Global Cost of Cybercrime- Economic Impact of cybercrime- Center for strategic and international studies June 2014)
- 5 милјарди уреди поврзани на интернет во 2015-та, предвидувањата се 25 милјарди до 2020-та (Gartner)

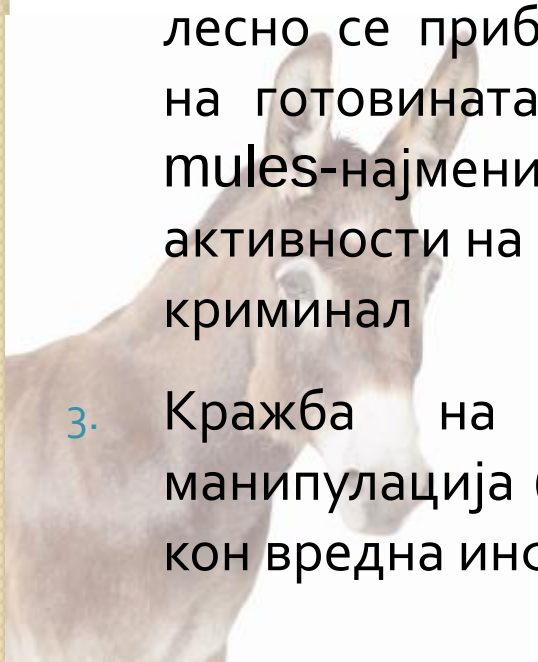
Нови трендови-закани и ризици

- **Компјутерски криминал или криминал во дигиталниот простор (cybercrime)** е криминал кое се врши преку компјутер и телекомуникациски мрежи како што е интернет (**Wikipedia**)
- Cybercrime е криминал кој носи голем приход по релативно ниска цена за криминалците. Криминалците се свесни дека ризиците и трошоците за нив се ниски, а добивката е висока.
- Cybercrime ги подјадува перформансите на компаниите, ги уништува интелектуалните сопственички права и ја ослабува националната економија.

Нови трендови-закани и ризици

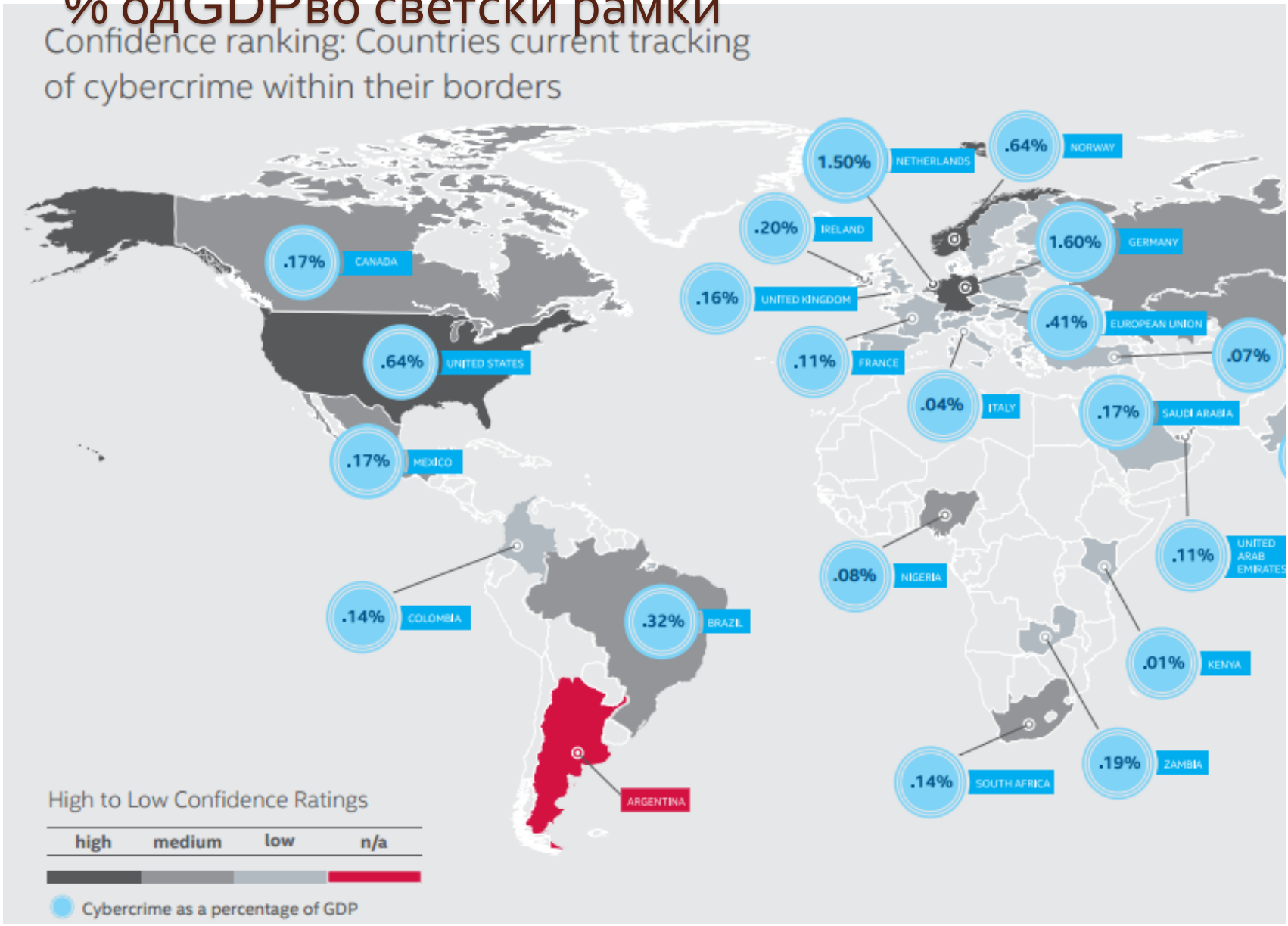
Главни цели на cybercrime:

1. Кражба на интелектуална сопственост – главна цел се компании кои се занимаваат со развој, индустрија, фармација (тешко да се одреди вистинската загуба во пари, огромни загуби по компаниите)
2. Кражба на финансиски средства преку неовластен пристап до финансики институции и трговски ланци каде се извршуваат голем број на on-line трансакции (релативно лесно се прибираат финансиските средства, трансферот на готовината се врши од страна на лица т.н.мулиња-mules-најмени луѓе кои мислат дека извршуваат активности на некоја легитимна компанија) = Организиран криминал
3. Кражба на доверлива информација и пазарна манипулација (хакирањето на НБМ или МФ може да води кон вредна информација за движењето на пазарот сл.)



Нови трендови-закани и ризици

% одGDPво светски рамки



Нови трендови-закани и ризици

- Земјите од Г-20 имаат највисоки загуби од cybercrime, поготово трите најразвиени економии (Америка 0,64%, Кина 0,63% и Германија 1,6 % од GDP)
- Побогатите земји (0,9% од GDP) се поатрактивни мети за криминалците но истите имаат и подобри одбранбени механизми. Посиромашните земји се повеќе ранливи.
- Послабо развиените земји (0.2% од GDP загуби) не прибираат информации за загубите кои настанале од овој тип, но и тие ќе се се почеста мета на криминалците бидејќи населението рапидно користи мобилна инфраструктура при извршувањето на операциите и поврзувањето со интернет.
- Годишните загуби над 200 милјарди $ (10-20% од целокупниот промет на дигиталната економија). **Предвидувањата се 3 трилиони $ загуби во 2020 година.**

Нови трендови-закани и ризици во светски рамки

Cybercrime претставува **данок на иновациите** и го успорува темпото на развој на компаниите преку намалување на процентите на повраќ на средствата кои биле вложени.

Cybercrime е индустрија во пораст. Годишните загуби на глобалната економија се проценуваат над **200 милјарди $ годишно** и се изразуваат во процент од GDP.

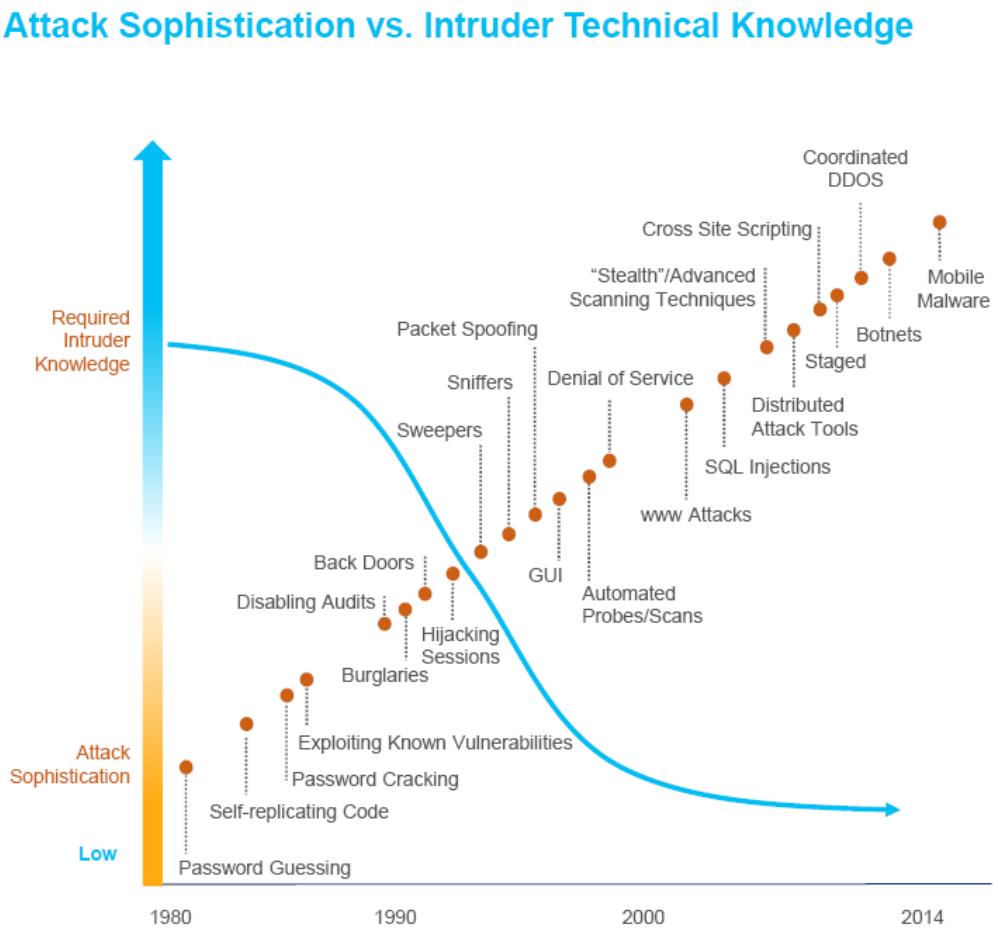
Голем дел од компаниите или **не се свесни** или не пријавуваат загуби поврзани со cybercrime.

Нови трендови-закани и ризици во светски рамки

- Користење на постојните слабости на системите
  - Не се врши редовна надградба на слабостите на ИТ системите
- Новите платформи креираат нови можности за напади
  - Нови начини за злоупотреба на ИТ системите на банките и клиентите
- Се потешко се разграничуваат актерите (хактивист, држави, организирани криминални банди, вработени) во нападите
  - Комерцијализација на алатки, ресурси и инфраструктура
- Унапредување на тактиките врз основа на online однесувањето
  - социјалните мрежи овозможуваат поефикасни и таргетирани напади (spear phishing)
- Унапредување на малициозните програми
  - Деструктивни програми и/или уценувачки-крипто програми

Нови трендови-закани и ризици во светски рамки

- Техничкото познавање за да се направи софистициран напад со текот на времето се намалува и заканите стануваат се поинтензивни
- Неодамнешните напади откриваат дека напаѓачите имаат добро познавање за технологијата, инфраструктурата и системите на нападнатите цели
- Хакерите ги напаѓаат и клиентите, добавувачите и надворешните лица на банката



Нови трендови-закани и ризици случај Р. Хрватска

Генерални информации

- Март – Мај 2014:
  - Околу 100 корисници на интернет банкарство беа жртви на организиран компјутерски криминален напад чија мета беа правни и физички лица
  - 190 неавторизирани трансакции беа генерирани од нивните сметки
  - 15 трансакции беа успешно комплетирани (парите се исплатени и подигнати)
  - Материјална штета е 1,75 мил HRK (220.000 ЕУР)
  - **Нападите беа насочени кон компјутерите на клиентите на банката**
- Дополнително инфо:
  - Регулативата и стандардите во Р. Хрватска во поглед на инфорамтивната сигурност и електронското банкарство се многу слични со нашата регулатива
  - Сите банки во Р. Хрватска користат двојна потврда на идентитетот
  - Нападнатите банки користат за физичките лица хардверски или софтверски токен, а правните лица сертификати сместени на smartcard или USB токен

Нови трендови-закани и ризици случај Р. Хрватска

OPASNOST NA INTERNETU

Upozorenje bankara: Budite oprezni, hakeri napadaju računala!

Autor: Novi list
Objavljeno: 28. ožujka 2014. u 22:51

Ovim napadom nisu ugroženi sigurnosni sustav
niti sustavi intern
molimo da svaki s
zahtijevaju tajni p
transakcija dojave

Hrvatska udruga bar
napadi na računala g

"Prema informacijam
računala nekih klijen
(virusi, trojanci i slič
vlasnika i korisnika (
računa i sl.) što omo
pristup aplikacijama
sustav). Računala se
otvaranjem zaraženi

HNB TRAŽI HITNU ISTRAGU

Oprez, hakeri izvlače novac s bankovnih računa!

Kriminalci pomoću virusa i dalje kradu novac: S računa hrvatskih tvrtki nestalo dva milijuna kuna!

Piše: R.I.
ponedjeljak, 28.4.2014. 11:31

Recommend 97

Tekst

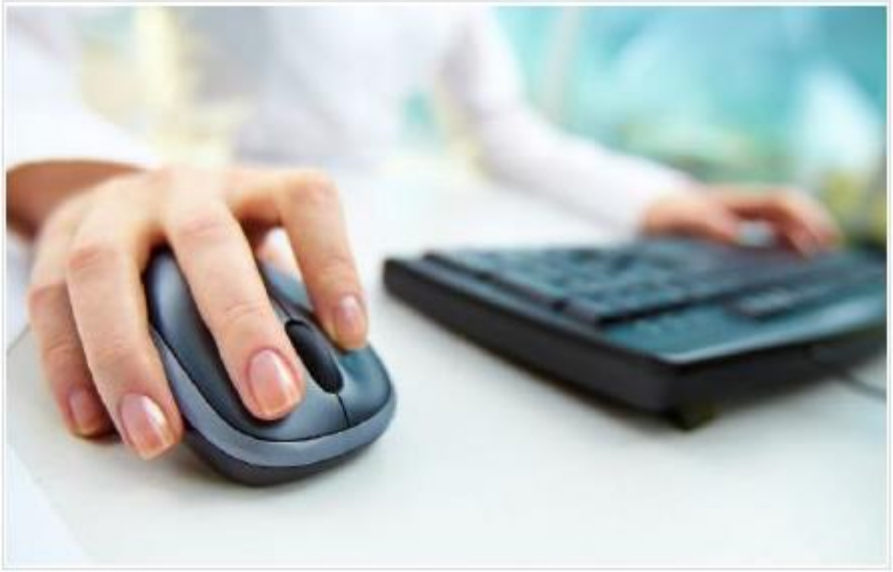


Foto: Ilustracija

Objava: 26.4.2014 | 15:05

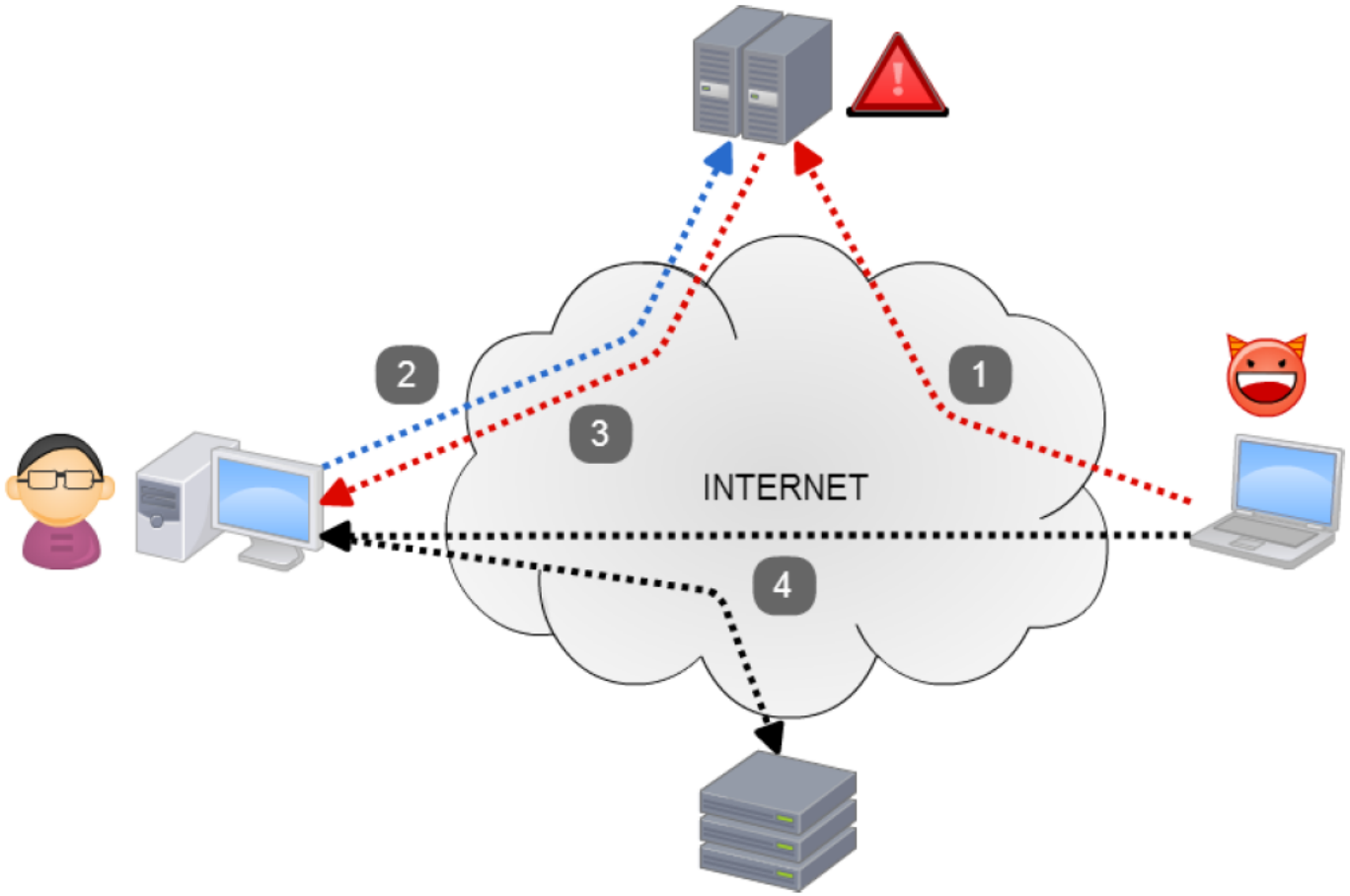
internetskih računa

27110 PREGLEDA 4.4 BODOVA

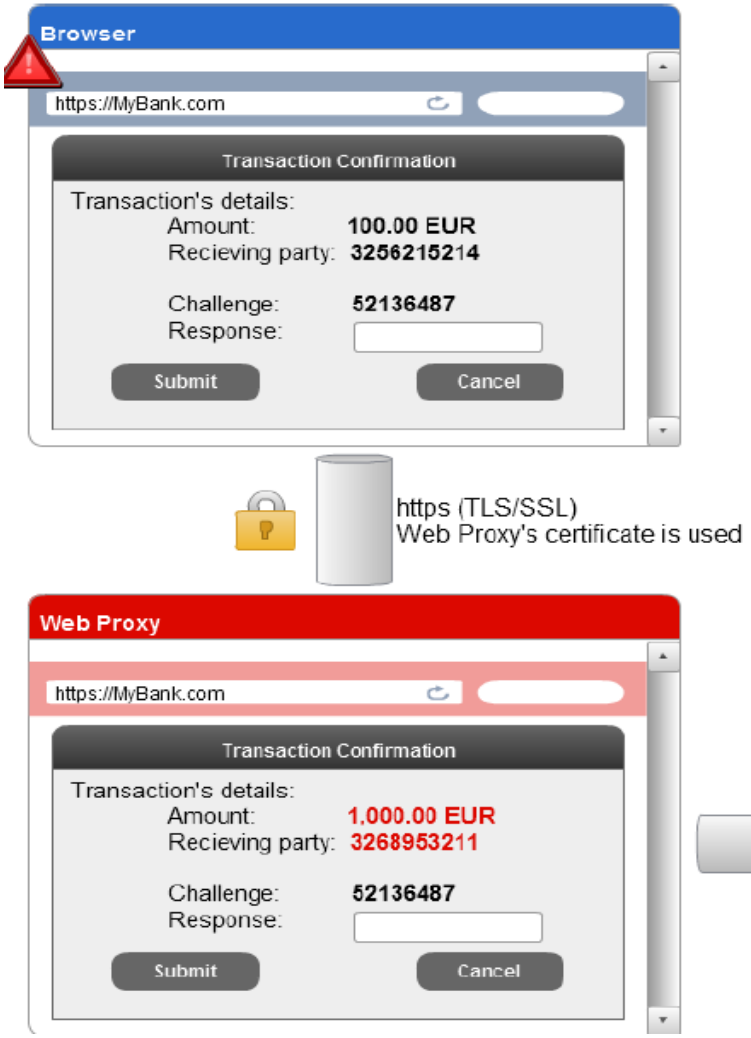
Нови трендови-закани и ризици случај Р. Хрватска

Man-in-the-Browser (MitB) Zeus Malware

- #1 threat of online banking (source: http://youtube.com/watch?v=4bPlAFZajuo https://www.youtube.com/watch?v=DUnZMwXCkyw)



Нови трендови-закани и ризици - Р. Хрватска

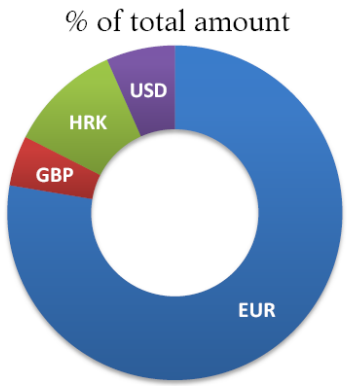


- Клиентот испраќа налог, напаѓачот динамички го менува во позадина и таков се испраќа до Банката
- Податоците се шифрирани за време на трансферот
- Можен индикатор за детекција:
  - дополнителни барања од електронската банка за потврда на идентитетот на места на кои претходно не биле побарани

- **Налозите генерирани на овој начин Банката ги добила како валидни налози кои се испратени преку системот за интернет банкарство, спремни за процесирање преку платните системи на товар на клиентот**

Нови трендови-закани и ризици случај Р. Хрватска

Анализа на нападите во однос на типот на потврда видот на налозите и регионите каде завршиле



A&A mechanism	1 - PREVENTED	2 - RETURNED	3 - BLOCKED	4 - OPEN	5 - STOLEN	9 - OTHER	Total
Challenge / Reponse	21	2	1	3	3		30
Smart card	33	59	28	26	12		158
TAN						1	1
Smart card & m-token	1						1
Total	**55**	**61**	**29**	**29**	**15**	**1**	**190**

Region	1 - PREVENTED	2 - RETURNED	3 - BLOCKED	4 - OPEN	5 - STOLEN	9 - OTHER	Total
Croatia	15	9	15	12	12	1	64
Central Europe	9	13		6	1		29
Eastern Europe	15	36	12	6			69
Northern Europe	2						2
Southern Europe	2	1			2		5
Western Europe	11	2	2	5			20
Other	1						1
Total	**55**	**61**	**29**	**29**	**15**	**1**	**190**

Нови трендови-закани и ризици случај Р. Хрватска

Подобрувањата кои банките во Р. Хрватска ги имплементирале во делот на интернет банкарство биле:

- воспоставување на вонредни механизми за мониторинг на трансакциите (дополнителна или одложена верификација на налозите кои пристигнуваат преку интернет преку друг канал, следење на однесувањето на клиентите);
- обука на клиентите на интернет банкарство за измена на навиките (број 1 препорака е смарт картичката/усб токенот по завршувањето на сесијата да не се остава приклучен на компјутерот и сл.);
- подобрувања на начинот на кој се врши потврда на идентитетот на клиентот и неотповикливоста на трансакцијата (во одредени интернет банки кај правните лица, воведени се смарт картички и ОТП токени дополнително, зајакнување на апликативните контроли и сл.)
- измена на постојните договори за интернет банкарство со оглед на ре-дефинирање на одговорноста за настанати штети;
- подигање на свеста на банките за новите улоги и одговорности кои се очекуваат од нивна страна и активности кои треба да се преземат;
- воспоставување на заеднички протокол за размена на настанати штетни настани и инциденти во делот на интернет банкарство.

Нови трендови-закани и ризици случај Р. Хрватска – PSD security on extra mile

- FAQ on PSD, question 395:
  - http://ec.europa.eu/internal_market/payments/docs/framework/transposition/faq_en.pdf
  - *Article 60 states that the payment service provider of the payer has to refund the payer immediately in the case of an unauthorised transaction.*
  - *(3) As for the cases in the **grey area** (e.g., the **payer claims that he has not failed to keep the personalised security features of the payment instrument safe**), Article 60(1) would grant an **immediate refund right to the payer once the notification has been made** in accordance with Article 58. Once the payer has been reimbursed, the payment service provider will then have the time necessary to look for evidence, in accordance with Article 59*

Агенда

1. Нови трендови, закани и ризици
2. **Активности на НБРМ**
3. Алатка за самооценка на ризиците од дигиталниот простор
4. Активности на Банките

Активности на НБРМ

Активности на Народната банка во изминатиот период беа главно насочени кон:

- Анализа на новите закани и напади во делот на сигурноста на дигиталниот простор во глобални и регионални рамки
- Информирање на банките за ризиците од користењето на застарени информативни системи Windows XP кај работни станици и кај ATM-банкомати
- Спроведувањето на редовни теренски ИТ контроли со посебен акцент во делот на зајакнување на :
  - Сигурноста на системот за електронско банкарство преку негово вклучување во системот за ревизорска трага и обезбедување на буџет за негово најразлично тестирање од страна на независни и соодветно обучени тимови
  - Системот за ревизорска трага како **предуслов за имплементација на систем од кој ќе се прибираат релевантни внатрешни закани по сигурноста на системот**
  - Унапредување на начинот на кој банката ги води штетите од настанатите инциденти (база на штетни настани) и зајакнување на процесот на управување со инциденти.

Активности на НБРМ

Следење на активности и препораките на Базел, Светска банка и останатите централни банки во поглед на подобрување на контролите во одредени сегменти :

- Cyber resilience in financial market infrastructures (Committee on Payments and Market Infrastructures November 2014)
- Cybersecurity Framework NIST (February 2014)
- World Economic Forum Partnering for Cyber Resilience (2014)
- World Bank Group (Financial Sector Advisory Center FinSAC) - Regional Cyber Security Issues and Options (May 2015)
- FFIEC Cyber Preparedness Framework (2015)

Активности на НБРМ

Клучни согледувања од овие документи :

- Народната банка треба да обезбеди услови за навремени адекватни и координирани реакции за спречување, откривање и брзо поправање на штетните последици од нападите во дигиталниот простор;
- Централните банки (регулаторите и супервизорите) треба да преземат чекори кон зајакнување на стандардите во поглед на натамошно унапредување на ИТ инфраструктурата, како и во поглед на свесноста за овие ризици и нивна интеграција во рамката за управување со ризиците, унапредувањето на начинот на размена на информации при нивно откривање и сл.
- Банките треба да имаат имплементирано системи кои ќе може промптно да реагираат во случај напади за да го одржат интегритетот на податоците и на инфраструктирата, да ги заштитат ценовно чуствителните и доверливи информации и интелектуалната сопственост.
- Сите финансиски и нефинансиски институции се од ризик во различна форма од новите напади, затоа треба да се подигне нивото на ПОДГОТВЕНОСТ кон ваквите напади. Пред се на Банките бидејќи тие се најчеста и најпосакувана мета на напади.

Активности на НБРМ

Согледувања на Народната банка :

- **Опкружувањето во кое се настаните штетните настани во Р. Хрватска, а поврзани со нападите од дигиталниот простор е многу слично** со состојбата во Р. Македонија (за физички лица се користи OTP, а за правни лица се користат дигитални сертификати на USB медиум и свесноста на клиентите била на слично ниво пред нападите)
- **Клиентите користат застарени информативни системи** и/или истите не се надградени со последните надградби препорачани од производителите и на тој начин се изложени кон повисок ризик.
- Клиентите и вработените во Банката се мета на напади од типот на социјален инженеринг и фишинг нападите.
- **Банките немаат системи за анализа на однесувањето на корисниците** на информативниот систем кој би помогнале за идентификација на измама и/или напад од дигиталниот простор.
- **Банките немаат протокол за размена на информации при настанати напади** со другите учесници во платниот промет во Р. Македонија.
- Потенцијалните штети: финансиска, оперативна, правна и репутациска. За да се избегнат или намалат овие штетни последици НБРМ подготви АЛАТКА.

Агенда

1. Нови трендови, закани и ризици
2. Активности на НБРМ
3. **Алатка за самооценка на ризиците од дигиталниот простор**
4. Активности на Банките

Алатка за самооценка

Главна цел :

- Да им помогне на Банките да ги идентификуваат нивните ризици и да одредат соодветно ниво на подготвеност во поглед на нападите од дигиталниот простор.
- Оваа алатка треба да се употребува континуирано за да му обезбеди на менаџментот мерливи резултати со кои ќе се утврди насоката на инхерентните ризици и оцени нејзината спремност кон напади од дигиталниот простор.

Вградени се :

- Важечките стандарди за сигурност на информативниот систем на територијата на Р. Македонија
- Индустриски стандарди и најдобри практики во делот на управување со ризиците поврзани со нападите од дигиталниот простор

Се состои од два дела :

1. Проценка на инхерентните ризици
2. Избор на ниво на подготвеност

Алатка за самооценка
Чекор 1

Инхеренетен ризик оценет преку анализа на пет категории :

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 кои се достапни преку алтернативните канали (електронско, мобилно банкарство, платежни картички)
4. Организациски карактеристики и
5. Надворешни закани.

Оценката на инхерентниот ризик ги зема во предвид големината, комплексноста, видот и обемот на активностите кои се изведуваат во Банката, како и специфичните закани на кои е изложена во своето работење.

При оценката на инхерентниот ризик не треба да се земаат во предвид имплементираните контроли за намалување на постојните ризици.

Алатка за самооценка

За оценка на инхерентните ризици во деловните процеси, предвидени се 4 нивоа за категоризација на инхерентниот ризик

Алатка за самооценка

Инхеренетен ризик оценет преку анализа на пет категории :

Инхерентен ризичен профил на Банката — Македонска банка за поддршка на развојот АД

КАТ. 1 : ТЕХНОЛОГИИ И ТИПОВИ НА ПОВРЗУВАЊЕ	Ниво на инхерентен ризик				Направи избор
	Мал	**Умерен**	**Значаен**	**Висок**	
Вкупен број на точки на поврзување со провајдер на интернет (вклучувајќи ги и поврзувањата со експозитури)	од 1 до 20 поврзувања	од 21 до 50 поврзувања	од 50 до 100 поврзувања	над 100 поврзувања	
Број на поврзувања преку „несигурни" протоколи (FTP, telnet, rlogin)	нема	помалку од 5	од 5 до 10	над 10 поврзувања	
Бежичен пристап до мрежа (wirele	не се користи	се користи како мрежа за гости; логички е одвоена од корпоративната мрежа; има помалку од 25 пристапни точки и помалку од 50 корисници	примарна мрежа каде имаат пристап сите вработени; има повеќе од 25 пристапни точки и од 50-100 корисници	примарна мрежа каде имаат пристап сите вработени; има повеќе од 50 пристапни точки и повеќе од 100 корисници	

Мал
Умерен
Значаен
Висок

НИВОА НА ИР

АКТИВНОСТ/СЕРВИС

Точното одредување на нивото на инхерентен ризик има за цел да ги идентификува присутните ризици во деловните процеси и агрегатното ниво на инхерентен ризик на кое е изложена Банката.

Алатка за самооценка

Инхерентен ризик оценет преку анализа на пет категории :

ЧЕКОР 1 : ОЦЕНКА НА НИВОТО НА ИНХЕРЕНТЕН РИЗИК

Вкупно	Мал	Умерен	Значаен	Висок
Број на селектирани избори по пооделни прашања во Категорија 1:	1	10	3	0
Број на селектирани избори по пооделни прашања во Категорија 2:	0	2	1	0
Број на селектирани избори по пооделни прашања во Категорија 3:	1	6	2	0
Број на селектирани избори по пооделни прашања во Категорија 4:	0	7	0	0
Број на селектирани избори по пооделни прашања во Категорија 5:	0	1	0	0

34 прашања систематизирани во 5 категории

ВКУПЕН БРОЈ ВО СИТЕ КАТЕГОРИИ:	2	26	6	0

Автоматска пресметка на нивото

Пресметано ниво на Инхерентен ризик:	УМЕРЕН	2,12

Агрегатното ниво на инхерентен ризик се пресметува автоматски врз основа на сите одговори за инхерентниот ризик во петте области.

Алатка за самооценка Чекор 2

Ниво на подготвеност во пет области :

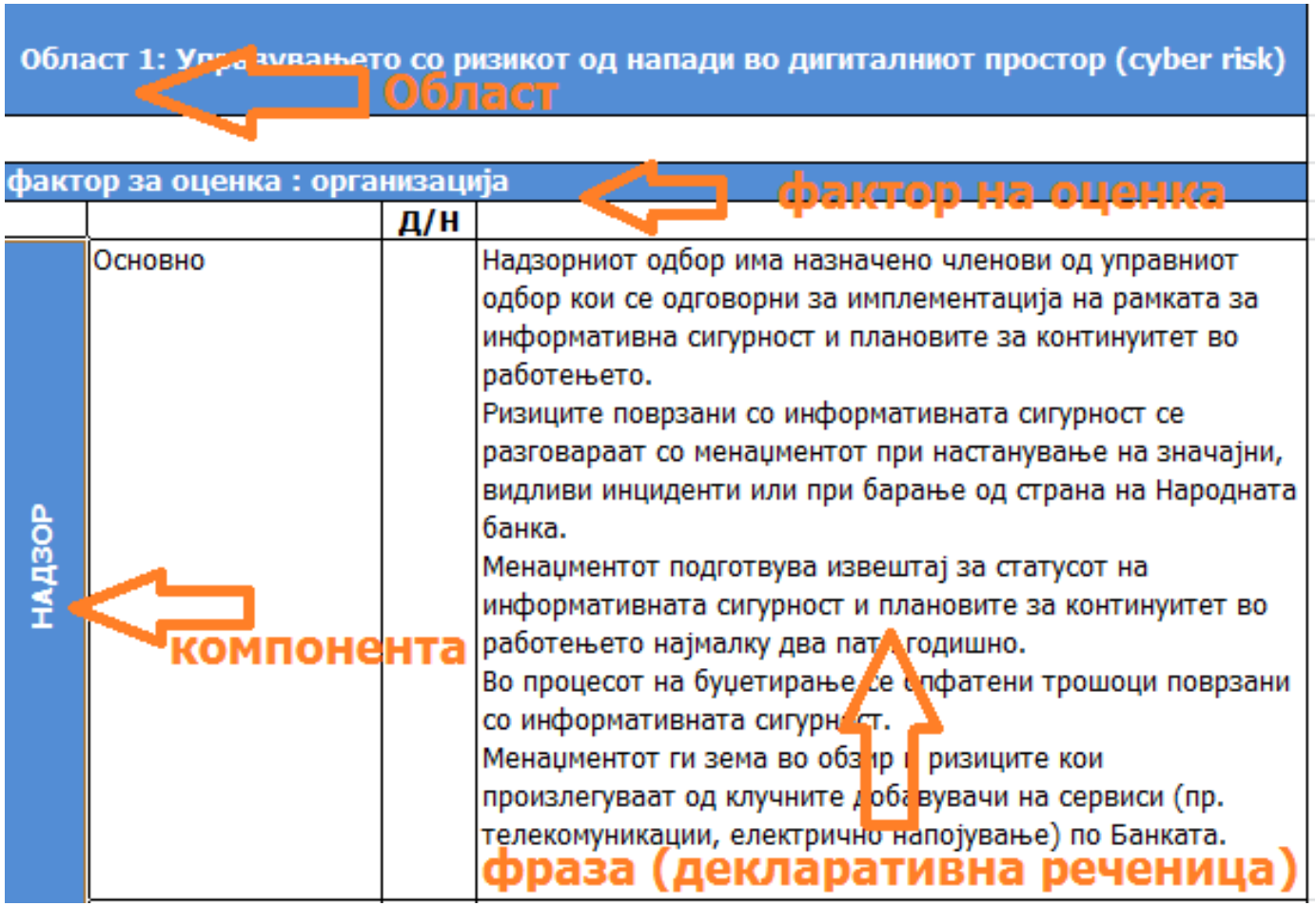
Алатка за самооценка

Ниво на подготвеност :

Овие пет **области** поделени се на повеќе **фактори за оценка,** а составен елемент на факторите за оценка се **компоненети**. За оценка на секоја компонента во алатката се дадени соодветни насоки. За секоја компоненета разработени се **фрази** (декларативни реченици) кои даваат опис за секое ниво.

Алатка за самооценка

Ниво на подготвеност :



Алатка за самооценка

Нивото на подготвеност е категоризирано во во три нивоа и тоа: основно, средно и напредно.

За секоја компонента за секое ниво (основно, средно и напредно) подготвени се различни фрази.

Алатка за самооценка

Избор на нивото на подготвеност

- **Менаџментот треба да процени и одлучи која фраза најдобро ја прикажува постојната ситуација и практика во Банката.**
- Изборот на адекватна фраза ќе ја идентификува оценката по одредена компоненета
- Доколку се избере повисоко ниво на подготвеност треба да се задоволени новите фрази од повисокото ниво, како и сите фрази од пониските нивоа.
- Идејата е да се добие адекватна оценка за нивото на подготвеност поодделно по секоја од областите, а не општа агрегирана оценка.

Алатка за самооценка

Избор на ниво на подготвеност

- зависностите помеѓу инхерентното ниво на ризик и нивото на подготовеност

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

Алатка за самооценка

Избор на нивото на подготвеност

- Менаџментот треба да донесе одлука за нивото на нивото на подготвеност во секоја пооделна област од нападите во дигиталниот простор во зависност од оценките за инхерентното ниво на ризик.
- **Генералните препораки на Народната банка е да се имплементира основно или средно ниво на подготвеност.**
- **Народната банка може да препорача постигнување на повисоко ниво на подготвеност во одреден временски период, доколку оцени дека тоа е потребно.**
- Очекувањата се банките со текот на времето да се подобруваат и унапредуваат во повисоки нивоа на подготвеност.
- Доколку има суштински измени во инхерентното ниво на ризик, со појава на нови закани и слабости и значајни измени во организациската структура се очекува ревидирање на одлуките кои ги донел менаџментот.

Алатка за самооценка

Акциски планови

- Менаџментот треба да одлучи кои активности треба да се спроведат за да се намали инхерентното ниво на ризик или 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 насоките дадени во фразите за поодделните нивоа.
- Менаџментот во одредени случаи треба да преземе дополнителни заштитни контроли за задржување на постојното ниво или подигнување на истото. Менаџментот може во одреден временски период да изврши подигање на нивото на подготвеност, доколку оцени дека постои веројатност да се материјализира одредена закана.
- Алатката да се користи континуирано, а поготово при промени во инхерентниот профил на ризик кога нови закани се појавуваат во регионот и пошироко, при измени во деловната стратегија со воведување на нови модерни банкарски производи и сервиси, ширење на други пазари и воведување на други надворешни лица и добавувачи.

Алатка за самооценка

Улогата на надзорниот одбор :

- следење на плановите и резултатите од извршената самооценка, вклучувајќи ги и резултатите и мислењата спроведени од други независни и стручни тимови на овој процес на самооценка;

- ревидирање на одлуките на менаџментот за постојното ниво на подготвеност и одобрување на предложената стратегија за воспоставеното ниво на подготвеност.

Алатка за самооценка

Улогата на управниот одбор :

- да назначи координатор на оваа активност и да изготви план со активности за да се спроведе самооценка;
- да ги одобри резултатите од извршената самооценка;
- да предложи стратегија за воспоставување на соодветно ниво на подготвеност и акциски планови;
- да воспостави акциски план за одржување на нивото на подготвеност и надминување на идентификуваните слабости;
- активно да ги следи информациите поврзани со нови закани и ризици и настанати сигурносни инциденти во делот на сигурноста во дигиталниот простор (cybersecurity);
- да ги анализира резултатите од спроведената самооценка и да ги информира членовите на Надзорниот одбор за резултатите од самооценувањето и спроведените активности.

Алатка за самооценка

Предности за институциите :

- идентификување на факторите кои придонесуваат кон зголемено ниво на ризик од заканите од ваков тип;
- утврдување на нивото на подготвеност од вакви напади и проверка дали истиот е усогласен со ризичниот профил;
- утврдување на сет на корективни активности кои се потребни за подобрување/задржување на постојното ниво и постигнување на посакуваното ниво;
- подобрување на информираноста за овие ризици во Банката и воспоставување на размена на корисни информации за навремено спречување на вакви напади во иднина.

Агенда

1. Нови трендови, закани и ризици
2. Активности на НБРМ
3. Алатка за самооценка на ризиците од дигиталниот простор
4. **Активности на Банките**

Тематска контрола

Активности:

- Народна банка ќе ги координира активностите за навремено завршување на процесот кај сите Банки во предвидените временски рокови вклучувајќи и теренски посети;
- Банките да припремат кратки плановите за имплементација на активностите и истите да бидат доставени до Народната банка најдоцна до 26-ти февруари 2016 година.
- Во текот на март 2016-та година, Ви стоиме на располагање за одредени прашања, предлози и сугестии во делот на процесот на самооценка.
- Како краен рок за имплементација на комплетниот процес на самооценка и достава на материјалите до Народната банка е : 31 март 2016-та година.
- До НБРМ треба да се достави алатката за самооценување со соодветните одговори. Одговорите на прашањата треба да бидат поткрепени со соодветна документација. Дополнително треба да се достави стратегија за воспоставување на соодветно ниво на подготвеност и акцискиот план за задржување/посигнување на посакувано ниво на подготвеност.

Тематска контрола

Активности:

- Народната банка ќе ги прибере и анализира информациите од процесот на самооценка за да се оцени подготвеноста на нашиот финансиски систем кон ризиците присутни во дигиталниот простор;
- Доколку се оцени дека одредени активности треба да се доразработат во законската регулатива ќе се направат предлози за измена на регулативата;
- Прв чекор да се имплементира основно или средно ниво на подготвеност.
- повисоко ниво на подготвеност во одреден временски период, доколку оцени дека тоа е потребно кај одредени банки или целокупно за системот.

Тематска контрола

Коментари и сугестии:

- Доколку имате одредени забелешки и прашања за делови од прашањата содржани во алатката Ве молиме да ги испратите на : jankoskig@nbrm.mk

- Ви благодариме на соработката -