РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ
И ПОШТАНСКЕ УСЛУГЕ

Смернице за заштиту корисника од безбедносних ризика у ИКТ системима

САДРЖАЈ

Појмовник

Backup – процес креирања резервне копије;

Usb - Универзални преносни медијум, уређај на који се могу сместити подаци;

Claud - нови концепт у *информационим технологијама,* дељење ресурса преко мреже, најчешће Интернета. Крајњи корисници приступају апликацијама у облаку преко веб претраживача или десктоп апликације на мобилном телефону, док се софтвер и кориснички подаци налазе на серверима на удаљеној локацији;

Wi-Fi - бежични приступ Интернету;

Интернет - глобални електронски комуникациони систем сачињен од великог броја међусобно повезаних рачунарских мрежа и уређаја, који размењују податке користећи заједнички скуп комуникационих протокола;

Pin - лични индентификациони број (енг. Private Identification Number);

Phishing - Фишинг је сајбер напад који се примарно извршава уз помоћ електронске поште, тако што се пошиљалац лажно представља као ентитет од поверења (банка, Интернет провајдер и сл.) и тражи од жртве да поступи по наведеним инструкцијама ради одавања личних података.

Social engenering - Навођење корисника да преда информације не техничким методама;

Ransomware - Рансомвер је злонамерни софтвер који шифрира информације на уређајима или мрежама, а за приступ и откључавање датотека захтева плаћање откупа. Чест је случај да инфициране датотеке чак и након плаћања откупа остају закључане;

e-mail - Електронска порука је сваки текстуални, гласовни, звучни или сликовни запис, послат преко јавне комуникационе мреже, који се може похранити у мрежи или у терминалној опреми примаоца све док је прималац не преузме или јој приступи;

SSL - *Secure Sockets Layer*, безбедносни протокол који се користи за слање поверљивих података преко Интернета;

HTTP - *Hypertext Transfer Protocol*, представља главни и најчешћи метод преноса информација на Интернету;

HTTPS - HTTP *Secure*, је комбинација HTTP-а са SSL протоколом да би се обезбедила енкрипција и сигурна идентификација сервера;

Cookies - су мале датотеке „колачићи" који приликом посете сајтовима прикупљају податке о чланцима који се читају и тиме нарушавају приватност посетиоца;

VPN - Virtual Private Network , Приватна виртуелна мрежа;

3G и 4G usb modem - уређај за повезивање на *Интернет* путем *мобилне* мреже;

1. Креирање и заштита корисничког налога и лозинке

Креирање корисничког налога и лозинке је кључно за заштиту од неовлашћеног приступа рачунарима, мобилним уређајима и информационим системима. Када је реч о фабричком подешавању уређаја, најчешће се употребљавају корисничко име и лозинка ***Admin/Admin,*** скраћено од речи администратор.

У циљу заштите рачунара, мобилних уређаја и информационих система, препорука је да се по активирању уређаја, кориснички налог измени и прилагоди приватној или службеној употреби.

Уобичајена пракса у оквиру правних лица, је да се за потребе корисничког налога користи комбинација имена и презимена (име (.) презиме).

Приликом креирања лозинке, препорука је да она садржи најмање девет алфанумеричких и знаковних карактера (велика и мала слова, бројеви, знаци интерпункције и сл.) како би једноставан приступ уређају од стране трећих лица био онемогућен. Лозинка може бити креирана у виду реченице која у себи садржи најмање три речи са или без размака (енг. ***blank space***).

На уређајима који се користе у приватне сврхе, корисници најчешће креирају лозинке од 4 до 6 карактера што не представља задовољавајући ниво заштите.

Лозинке треба чувати од других, било да је реч о пријатељима, колегама, клијентима и сл. Уколико лозинку учини доступном, власник лозинке се излаже великом ризику да она буде злоупотребљена и тиме себе можете довести у ситуацију да сноси чак и кривичну одговорност.

Пример лоше праксе је креирање и коришћење једне лозинке за више различитих налога. Добра пракса показује да корисник треба да има засебну лозинку за сваки налог. Препорука је да се лозинка мења на полугодишњем нивоу, а по потреби и чешће. Такође, приватне налоге не треба користити у службене сврхе и обрнуто, како службени кориснички налози и домени правног лица не би били изложени злонамерним активностима. Употреба рачунара за личну намену може представљати додатан сигурносни ризик комплетног информационог система правног лица.

2. Редовно ажурирање постојећих хардверских и софтверских решења

Како би деловали превентивно и умањили изложеност могућим рањивостима, неопходно је редовно ажурирање хардверских и софтверских решења, у складу са препорукама произвођача рачунара, мобилних уређаја или информационих система.

Свако неблаговремено ажурирање омогућава злоупотребу од стране злонамерних хакера, односно нападача, који могу искористити постојеће рањивости, чиме се угрожава целолкупан садржај на одређеном рачунару, мобилном уређају односно информационом систему. Свако хардверско и софтверско решење треба ажурирати искључиво верзијама које су препоручене и одобрене од стране произвођача, лиценцираних произвођача, или овлашћених заступника продаје.

Физичка лица сносе одговорност за ажурирање оперативних система на својим уређајима. Веома често се ово занемарује, због чега ови уређаји најчешће буду мета хакера.

3. Редовно креирање резервне копије – *Backup*

Један од изузетно важних корака у циљу постизања високог нивоа заштите од напада на рачунаре, мобилне уређаје или информационе системе је креирање резервних копија свих важних докумената и фајлова. Губитак рачунара, крађа рачунара, оштећење или изложеност малициозном садржају су само неки од начина који могу да доведу до губитка важних докумената и фајлова.

Једини начин да спречите губитак докумената и фајлова је редовно креирање резервних копија, односно ***Backup*** података. Резервне копије је потребно чувати на различитим местима, односно уређајима, јер чување више копија једног документа на једном рачунару или уређају није одговарајуће решење. Копије се морају чувати одвојено и на такав начин да носач података (диск, USB и сл.) не буду прикључени на рачунар који је на мрежи, односно рачунар на којем се налазе оригинални документи и фајлови.

Поред мануелних копија, постоје и аутоматизоване копије које се најчешће користе у већим системима, али се могу применити по потреби корисника, без обзира на структуру правног лица.

Постоје и резервне копије које се постављају на тзв. „Облак" (енг. ***Cloud)*** окружење, за које је неопходно креирати налог и одговарајућу лозинку.

Резервне копије треба ограничити само на документа и фајлове који не могу бити поново креирани. Губитак ових података представља велики ризик у оквиру правних лица, јер може угрозити, или знатно успорити наставак њиховог пословања. Није неопходно креирати резервне копије видео игара или другог садржаја који је доступан на Интернету и који се једноставно може преузети поново.

4. Заштита тачака за бежично повезивање на Интернет – *Wi-Fi* приступ

Коришћење тачака за бежични приступ Интернету (***Wi-Fi***) је веома уобичајен начин за повезивање на Интернет, без обзира да ли је реч о физичким лицима, малим и средњим предузећима или великим компанијама. Како би приступ тим уређајима био онемогућен неовлашћеним корисницима, неопходно је сваки уређај заштитити одговарајућом лозинком. Уколико се укаже потреба да поделите лозинку за приступ ***Wi-Fi*** уређају, по завршетку је неопходно изменити лозинку, јер постоји могућност злоупотребе откривене лозинке.

Приватни корисници најчешће добијају уређаје са предефинисаним називом мреже и лозинком. У договору са интернет провајдером, ови параметри се могу изменити.

Правна лица такође користе бежичне тачке за приступ Интернету и због тога је неопходно да своје ***Wi-Fi*** уређаје заштите одговарајућом лозинком, коју треба редовно мењати, нарочито у оним случајевима када је деле са трећим лицима. Инсталирање и употреба ових уређаја у оквиру правних лица треба бити дефинисана и посебним процедурама.

5. Заштита мобилних уређаја

Заштита мобилних уређаја, пре свега подразумева заштиту паметних телефона и таблета. Заштита ових уређаја је веома важна, јер неовлашћени приступ овим уређајима може нанети велику штету пре свега власницима ових уређаја, али и другим лицима, односно правним лицима, уколико је реч о службеном мобилном уређају.

Штета може бити материјална, а може бити и психолошког карактера, јер корисници на својим мобилним уређајима чувају своје податке, фотографије или видео записе, а у највећем броју случајева имају и неометан приступ ка својим имејл налозима, односно налозима на друштвеним мрежама као што су Фејсбук, Твитер, Инстаграм и сл. Неовлашћени приступ налозима омогућава злонамерним корисницима да са тих налога дистрибуирају различите типове садржаја, који могу бити у вези са власником налога, али то може бити и садржај који није у вези са власником мобилног уређаја. Такав вид злоупотребе доводи у опасност власника мобилног уређаја, односно налога.

Како би умањили могућност било какве злоупотребе, неопходно је заштитити мобилне уређаје одговарајућим лозинкама или ПИН-ом. Корисници треба да креирају шифру која се не може лако открити, што подразумева да шифра не треба да буде састављена од бројева који су у вези са корисниковим датумом рођења, или завршне године студија и сл.

Као додатни вид заштите, савремени уређаји имају и опцију скенирања отиска прста или препознавања лица.

6. Безбедно коришћење имејл налога

За сваки налог електронске поште је неопходно креирати одговарајуће корисничко име и лозинку, како би се знало ком кориснику припада одређени налог. Када је реч о службеном корисничком налогу електронске поште, налог се најчешће креира на основу имена и презимена (име(.)презиме) корисника за чије потребе се налог креира, а у складу са прописима правног лица. Физичка лица произвољно креирају своје налоге уз одређена ограничења власника домена.

Хакерски напади на рачунаре, мобилне уређаје и информационе системе веома често користе имејл налог као тачку за упад у одређени рачунар, односно информациони систем и самим тим је од веома великог значаја за безбедност рачунара и система начин на који рукујемо овим налозима.

Најчешћи типови напада путем електронске поште су фишинг кампање. Уз злонамерни имејл се најешће као прилог доставља ***Ransomware,*** чијим покретањем се шифрују сви подаци на уређају.

Поред оваквог типа напада на имејл системе корисника, постоје и тзв. упади у имејл преписке, а то се најчешће дешава у преписка између руководилаца правних лица и службеника који су запослени у сектору финансија. Приликом такве врсте напада, нападачи пресретну одређену преписку и покушавају да симулирају слање одређеног имејла ка руководиоцима правног лица са молбом за хитну уплату одређене суме новца на неки рачун. Због легитимности изгледа налога, овакав вид напада на правна лица, често буде веома успешан за нападаче. Препорука је да се сваки захтев за хитан трансфер средстава на рачун ван правног лица, обавезно провери усменим путем уз тражење сагласности овлашћеног лица.

У службене сврхе не треба користити јавне бежичне тачке за приступ интернету, због опасности од могућег пресретања и праћења саобраћаја. Неауторизована и незаштићена употреба Интернета може омогућити неовлашћеним лицима приступ поверљивим пословним информацијама. Додатна препорука је да се не врше финансијске трансакције путем ових приступних тачака.

7. Безбедно плаћање путем Интернета – *Online* плаћање

Корисници банкарских услуга за електронско плаћање, као и плаћање роба и услуга путем Интернета су изложени могућим злоупотребама од стране хакера, односно нападача.

Да би се корисници ових услуга заштитили, неопходно је да пре уноса података за приступ својим рачунима или налозима провере да ли је Интернет страница банке, односно продавца легитимна. Та провера се може извршити увидом у адресну линију, која се налази на врху странице Интернет претраживача и која најчешће почиње ознаком HTTP://, односно HTTPS:// .

Додатни вид заштите је креирање квалитетних лозинки које у себи треба да садрже најмање девет алфанумеричких и знаковних карактера (велика и мала слова, бројеви, знаци интерпункције и сл.) како би се онемогућио једноставан приступ налогу од стране трећих лица.

Уколико се од корисника захтева унос и измена постојећих креденцијала (корисничког имена и лозинке) не треба поступити по захтеву, јер креденцијале корисници мењају по личном нахођењу, а не на захтев банке или неке друге институције, односно ***Online*** продавнице. Клијенти у оваквим ситуацијама треба да контактирају банку или ***Online*** продавницу директно и на тај начин спрече могућу злоупотребу свог налога.

8. Заштита дигиталног идентитета, личних и пословних података

Упркос законима и напретку технологије који се баве заштитом дигиталних идентитета, личних и пословних података, могућност да они буду украдени и даље представља велику претњу са Интернета. Једину пуну заштиту података можемо остварити ми сами.

Дигитални идентитет нису само име и презиме и матични број, већ су то сви подаци који на било који начин одређују наше присуство на мрежи. Ту спадају адреса електронске поште, лични домен, назив Интернет странице, па и надимак који користимо на друштвеним мрежама.

Сваки лични податак на Интернету који се остави на друштвеним мрежама (име, презиме, место становања, школа, компанија, интересовања, фотографије, видео садржаји, коментари) остављају траг у дигиталном свету и постају део дигиталног отиска.

Приликом отварања профила на друштвеним мрежама, није нужно оставити све податке, а нарочито треба избегавати остављање података попут броја телефона и адресе становања, бројева кредитних картица и банковних рачуна. Уколико се то не може избећи, проверити да се ти подаци не приказују јавно.

Мале датотеке „колачићи" (***cookies***) приликом посете сајтовима прикупљају податке о чланцима који се читају и тиме се прате корисници и њихове навике. Како бисмо спречили да овакве податке прикупља трећа страна, у поставкама претраживања треба изабрати опцију „блокирај колачиће трећих страна".

Да би се пословни подаци адекватно заштитили, неопходно је идентификовати осетљиве податке и одредити права приступа. За пренос оваквих података препоручује се безбедан канал комуникације (***SSL***) и сертификат издат од стране регистрованог сертификационог тела. Пословне мобилне уређаје и лаптопове је неопходно заштитити лозинкама, а осетљиве податке је потребно и шифровати.

Коришћењем јавних бежичних тачака за приступ Интернету, ризикује се пресретање података, како личних тако и пословних, па их треба избегавати и користити само познате проверене приступне тачке.

9. Закључак

Непрекидно унапређење информационих технологија поставља заштиту података од злоупотребе и неовлашћеног приступа, као један од кључних приоритета.

Ова смерница пружа неколико корисних савета како се подаци могу сачувати док сте у покрету:

- Потребно је да сви уређаји које користите, било да се ради о лаптопу, мобилном уређају, таблету и сл., буду заштићени лозинком и то од најмање девет алфанумеричких и знаковних карактера (велика и мала слова, бројеви, знаци интерпункције и сл.);
- Проверити да ли су сви налози на Интернет претраживачу заштићени лозинком и да нису сачувани у претраживачу.

Уколико дође до крађе уређаја, претходна два савета спречавају да дође до крађе података директно са уређаја.

- Редовно ажурирање оперативног система и антивирусног софтвера пружа заштиту од најновијих верзија малициозног софтвера, чиме се спречава неовлашћено прикупљање података и могућност праћења;
- Визуелна сигурност података – водити рачуна где се користите уређаји и ко може да види шта на њима корисник ради, покушати да се спречи да други људи гледају у ваш екран, најчешће злоупотребе се дешавају у јавном превозу (аутобуси, возови, авиони итд.);
- Избегавати *WiFi* мреже без лозинке, нарочито за *Online* банкарство и друге финансијске трансакције.
- Приликом приступа пословној мрежи преко јавне *WiFi* мреже, препоручује се коришћење *VPN*-а;
- Приликом боравка у хотелу распитати се за тачан назив њихове *WiFi* мреже. Уколико се приликом конекције захтева ажурирање софтвера да би се повезало на мрежу, потребно је одмах прекинути конекцију и пријавит надлежној служби.;
- За повезивање на Интернет док сте у покрету, пожељно је користити 3G или 4G *USB* модем. Коришћење личног уређаја за приступ Интернету обезбеђује већу заштиту ваших података и уређаја;
- Шифровати податке, било на систему у целини или на одређеним датотекама. Већина правних лица има софтвер за шифровање дискова и свих датотека које су сачуване на њима. Да би се прочитала шифрована датотека или приступи шифрованом уређају, мора се имати одговарајући кључ или лозинка. Шифровање се може извршити и на мобилним уређајима, користећи *PIN* или лозинку.

Шифровањем се штитите подаци од злоупотребе, јер се спречава приступ без одговарајућег кључа или лозинке.

- Размотрити који подаци се носе на физичким уређајима. Размислити да ли неки од њих могу бити сачувани у „облаку" ради лакшег приступа са других локација. Ако се не жели остављање података у „облаку" , онда користити шифровани *USB* диск

www.ratel.rs