Национални ЦЕРТ
Републике Србије

СРБ-ЦЕРТ

РЕПУБЛИКА СРБИЈА
РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ
И ПОШТАНСКЕ УСЛУГЕ

01 Увод

Појам информациона безбедност је све присутнији у целокупном друштву, како у свету, тако и код нас. Сведоци смо чињенице да је доскорашњи начин коришћења Интернета, претежно у циљу забаве, престао да постоји. Данас је Интернет саставни део свакодневног живота, било да га користимо у приватне или пословне сврхе. Самим тим, већ више од две деценије, Интернет са собом носи и одређене опасности, не само на нивоу појединца, већ и на нивоу друштва. Све су учесталији примери напада на информациону инфраструктуру државних институција, финансијских групација, компанија различитих профила, академских удружења, али и рачунара које користимо у својим домовима.

У тексту који следи, Национални ЦЕРТ Републике Србије ће покушати да приближи корисницима рачунара и мобилних уређаја своја искуства и знања у вези са сигурнијим и безбеднијим коришћењем Интернета

Веома је важно на који начин се користе рачунари и мобилни уређаји, јер је све присутнија опасност од губитка података, онемогућавања приступа подацима, крађе креденцијала или идентитета, али све чешће долази и до злоупотребе рачунара за приступ другим рачунарима. Овакве злоупотребе најчешће имају за циљ стицање противправне финансијске користи.

Циљ Националног ЦЕРТ-а Републике Србије је да сваком кориснику представи основне принципе безбедног и сигурног коришћења Интернета, односно свих погодности које Интернет пружа.

Опште је познато да милиони људи широм света у сваком тренутку користе Интернет мрежу. Већина њих спада у категорију савесних и одговорних корисника. Ипак, постоје и они који Интернет мрежу не користе на такав начин, већ, сакривени иза виртуелне завесе, покушавају на различите начине да наруше функционисање вашег, или система других корисника који су на мрежи.

Начини злонамерних приступања рачунарским системима могу бити различити. Главна подела је на активне и пасивне приступе. Активни приступ претпоставља измену неких података, што се накнадно може утврдити форензичким анализама, док се пасивни приступ теже открива, јер он не врши никакву измену података у информационом систему, већ најпре има улогу такозваног 'ослушкивања' мреже и најчешће се примењује у случајевима шпијунаже.

Неки од начина које злонамерни корисници Интернета примењују за приступ рачунарима или мобилним уређајима су 'Phishing', затим упад у неадекватно заштићени приватни или јавни бежични приступ Интернет мрежи (Wi-Fi) или бежични пренос података (Bluetooth), као и злоупотреба сигурносних пропуста инсталираног софтверског решења на рачунару, односно информационом систему.

За највећи број напада се користе једноставне методе, као што су *'Phishing'*, *'Spam'* и слично.

02 Phishing

'Phishing' је једна од метода којом злонамерни корисници Интернета прослеђују имејл поруке на што већи број адреса, у очекивању да ће неко од корисника који добију овакву поруку поступити по наведеним инструкцијама. Најчешће то буде порука на лажном линку, која често садржи и лажни формулар, а коју вам, наводно, прослеђује ваша банка или Интернет провајдер, и у којој се од вас захтева да унесете своје личне податке. На овакав начин, злонамерни корисници Интернета покушавају да добију ваше личне податке, односно ваше креденцијале - корисничко име и лозинку, помоћу којих даље приступају вашим налозима, као што су 'Facebook', 'e-mail' и слично.

На овакав начин, злонамерни корисници Интернета добијају могућност да измене садржај на вашим налозима, шаљу поруке или фотографије, односно видео записе вашим пријатељима, или другим корисницима. Злоупотребе оваквог карактера могу нанети штету не само вама, већ и члановима ваше породице, пријатељима, па чак и оним људима до којих стигне таква једна порука, а које ви заправо и не познајете.

03 Безбедно бежични

Опште је познато да се данашњи рачунари и други мобилни уређаји у стандардном пакету опреме нуде са опцијом Wi-Fi (бежичног повезивања на приватне или јавне мреже), и Bluetooth (бежични пренос података). Овакав приступ Интернету нам омогућава једноставнију и лакшу употребу и доступност свих жељених садржаја, како код куће, тако и на јавним местима као што су хотели, ресторани, образовне или културне установе и слично.

Оно што је важно напоменути, та доступност није омогућена само вама, већ и свим другим корисницима Интернета који се налазе у вашој близини и користе ту тачку приступа. Уколико неки од њих припадају групи злонамерних корисника, пружена им је могућност да искористе све недостатке оваквог начина преноса података и да приступе вашим налозима које ће злоупотребити на начин који им се, у датом тренутку, учини најпогоднијим. То може бити дељење ваших фотографија, или видео записа са вашег налога, али исто тако могу слати и фотографије, односно видео записе, или неки други садржај који није ваш, а чијом дистрибуцијом вам може бити нанета велика штета. Оно што Национални ЦЕРТ Републике Србије посебно препоручује, јесте избегавање коришћења јавних бежичних тачака за приступ Интернету приликом извршавања финансијских трансакција, или провере стања банковних рачуна, уколико наведена тачка приступа није адекватно заштићена. Сугестија је да бежичне тачке за приступ Интернету на рачунарима обавезно буду осигуране лозинком која не садржи информације везане за ваш датум рођења, имена кућних љубимаца и слично, јер се такве лозинке лако могу открити.

04

Malware

Малициозни софтвер

Већина корисника рачунара је имала прилике да се упозна са појмовима као што су: тројанац, црв или вирус. Неки корисници су чак били принуђени да отклањају последице које овакви малициозни софтвери изазивају на рачунарима, односно информационим системима. За разлику од других видова злоупотребе рачунара, малициозни софтвери могу причинити највећу штету крајњим корисницима, али и информационим системима уопште.

Овде посебну пажњу треба скренути на оне типове малициозних софтвера који се инсталирају на рачунар путем пропуста откривених на оперативним системима. Тиме је омогућено да особа која је поставила такав малициозни софтвер може у потпуности преузети контролу над тим рачунаром, без знања власника, и тиме омогући остваривање свих жељених циљева. Поред пропуста који се односе на оперативне системе (нпр. Microsoft Windows, MAC OS) који су инсталирани на рачунарима, постоје и пропусти који се тичу инсталираних Интернет претраживача (нпр. Internet Explorer, Opera, Google Chrome), или алата који омогућавају читање мултимедијалних датотека (нпр. Windows Media Player), или докумената (нпр. Adobe Acrobat Reader).

Национални ЦЕРТ Републике Србије би скренуо посебну пажњу на тип малициозног софтвера који је познат под називом 'Ransomware'. Овај тип малициозног софтвера несавесни корисници Интернета постављају у рачунаре, односно информационе системе како би криптовали податке и тиме онемогућили њихову употребу, а причињена штета може бити немерљива. Знајући да последице овако причињене штете могу бити изузетно велике, злонамерни корисници захтевају исплату одређене суме новца, како би заузврат доставили кључеве за енкрипцију, односно омогућили да поново приступите и користите инфициране датотеке. Највећи проблем у оваквој ситуацији је тај што корисник није сигуран да ће заиста добити кључеве за енкрипцију оштећених података, или ако их и добије, њиховом применом можда неће бити могуће приступити свим подацима који су били инфицирани оваквим малициозним софтвером. Додатни проблем је то што плаћањем откупнине, корисници финансирају криминалне организације и зато је препорука Националног ЦЕРТ-а Републике Србије, али и других организација које се баве информационом безбедношћу, да се откупнина не плаћа.

05

Препоруке

Постоји више препорука како заштитити рачунар од напада злонамерних корисника. Основна препорука је обавезно инсталирање неког од антивирусних софтвера на рачунаре или мобилне уређаје. Тиме ћете онемогућити једноставан приступ било ком злонамерном кориснику. Додатни видови заштите су: постављање одређеног 'Firewalla' на рачунар, затим благовремено ажурирање оперативног система и апликација које се налазе на рачунару, односно мобилном уређају, примена аутоматског ажурирања оперативног система и апликација уколико постоји таква опција, затим постављање одговарајуће лозинке чијим уносом се омогућава пријава корисника на рачунар. Лозинка би требало да садржи сваки од препоручених словних или знаковних карактера, како би сложеност лозинке била што већа и тиме отежала неовлашћени приступ рачунару. Савет је да лозинка не буде креирана од информација који су личног карактера. Ту пре свега мислимо на датуме рођења, имена родитеља, деце или кућних љубимаца и слично, јер су то информације које злонамерни корисници најпре уносе као опцију приликом покушаја упада у рачунар.

Додатни видови заштите рачунара се своде на савесно руковање и коришћење рачунара, односно свих погодности које нуди Интернет. Овде најпре мислимо на редовно креирање резервних копија (енг.'Backup') свих важних докумената, затим безбедно отварање електронске поште, односно имејла, који у себи могу садржати одређене прилоге (енг. 'attachment') путем којих се дистрибуирају рачунарски вируси. Поруке које стигну од непознатих корисника не треба отварати без претходне провере. Сугестија је да се посећују искључиво заштићене Интернет странице, које у својој адресној линији обавезно садрже ознаку 'http://', или 'https://', odnosno 'HTTPS protokol' (енг. 'Hypertext Transfer Protocol Secure').

Национални ЦЕРТ Републике Србије скреће пажњу свим родитељима чија деца активно користе различите типове социјалних мрежа на Интернету, да на адекватан начин објасне својој деци који подаци, односно садржаји могу, или треба да буду доступни на Интернет налогу, а које не би требало објављивати. Последице које могу да се јаве због неадекватно објављеног садржаја на Инетрнету не морају увек бити материјалне природе, већ се могу одразити и на психу детета, јер смо сведоци све присутнијег вршњачког насиља, а један вид таквог насиља управо може бити објављивање неког неадекватног садржаја на Интернету.

06 Закључак

Интернет је саставни део свакодневног живота и, као такав, стално се унапређује у квалитативном и квантитативном смислу, а крајњи циљ је да свим корисницима олакша обавезе, али и живот учини забавнијим. Све ове олакшице остављају простор за злоупотребу и самим тим кориснике чине изложенијим и рањивијим и у том смислу Национални ЦЕРТ Републике Србије, у сарадњи са другим ЦЕРТ тимовима, чини све како би пружио максималну заштиту корисницима Интернета.

Будите одговорни према себи и другима док радите и уживате на Интернету!

РЕПУБЛИКА СРБИЈА

РАТЕЛ

РЕГУЛАТОРНА АГЕНЦИЈА ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ И ПОШТАНСКЕ УСЛУГЕ

АДРЕСА
Палмотићева 2
11103 Београд
Република Србија

www.cert.rs