Prosvetni pregled

Država: Srbija

Doseg:

Strana: 17

Površina: 569 cm^2

26.10.2017
četvrtak

1 / 2

РЕГИСТАР НАЦИОНАЛНОГ ИНТЕРНЕТ ДОМЕНА СРБИЈЕ

Проблеми и решења интернет безбедности

На подизању свести интернет корисника још много мора да се ради, неопходно је понављати и лекције које су већ испричане, како би доспеле до младих, нових корисника интернета, којих је свакога дана све више

Будући да се савремено друштво све више умрежава и своје функционисање заснива на интернет технологији, заштита на интернету била је тема овогодишњег скупа Регистра националног интернет домена Србије (РНИДС), а поводом Европског месеца сајбер безбедности. Истим поводом РНИДС организује дискусије већ пет година заредом, а овог пута назив је био „Проблеми и решења интернет безбедности".

У препуној сали Центра за промоцију науке, прошле седмице о реченој теми говорили су домаћи и страни стручњаци из области интернет безбедности: Бранко Стаменковић, посебни тужилац за високотехнолошки криминал из Тужилаштва за високотехнолошки криминал (ВТК) у Београду, Александар Павловић, систем инжењер компаније COMING из Београда, Жарко Кецић, в. д. директора РНИДС-а и руководилац сектора ИКТ сервиса, те Александар Венедјухин, истраживач руског Техничког центра за интернет.

О проблемима фишинга (phishing) и онлајн превара у Србији говорио је Бранко Стаменковић, који је истакао важност сарадње РНИДС-а и других сличних организација са тужилаштвима и другим државним органима, а на спречавању кривичних дела на интернету:

– Страна искуства показују да управо таквом сарадњом између државног и приватног сектора долази до најбољих резултата.

Проблем „фишинга" један је од највећих изазова, тај вид технолошког криминала није новост, али нападачи константно смишљају нове начине за реализацију тог типа превара.

И поред великих напора који се улажу у подизање свести корисника интернета, и даље се дешава да преваре успеју, напомиње Стаменковић:

– Очекивао сам да ће то да нестане, или бар да се спусти на ниво који је неприметан, маргиналан, но таква врста извршења кривичних дела поново постаје популарна" – упозорио је Стаменковић и подсетио на „нигеријску превару", тип социјалне манипулације у којој се путем мејла жртви обећава одређена награда, ако уплатом неке суме новца помогне нападачу да дође до решења свог „случаја", који је обично у вези са неким измишљеним наследством.

Описао је и два случаја фишинга на Фејсбуку, који су реализовани ради прикупљања личних података корисника ове друштвене мреже. У првом су подаци тражени да би се учествовало у лажној наградној игри, а у другом је тражено освежавања података на лажној Фејсбук страници. Нагласио је да су Тужилаштву руке у таквим случајевима обично везане, будући да су извршиоци углавном из земаља које још нису ратификовале Конвенцију о сајбер криминалу Савета Европе, која је тренутно једини међународно признати инструмент, а признаје га тек 57 земаља света.

На подизању свести интернет корисника још много мора да се ради, апелује тужилац, и истиче да је неопходно понављати и лекције које су већ испричане, како би доспеле и до младих, нових корисника интернета, којих је свакога дана све више.

Александар Павловић одржао је презентацију „Како сам преживео напад криптолокера", те поделио, како сам каже, неславно искуство једног корисника из Србије. Што се тиче напада, радило се о релативно непознатом малициозном софтверу, који шифрује податке својих жртава, рансомверу NM4 криптолокер. У овом случају нападнути су сервиси за бекап и мејл (бекап сервер и мејл сервер), који су после напада постали неупотребљиви. Нападачи су тражили накнаду у износу од три биткоина, што је у том тренутку износило 8000 долара (данас је то готово 17.000). До напада је дошло услед недовољне свести запослених о информатичкој сигурности, потенцијални кривац је мејл са малициозним софтвером, а томе је вероватно допринео недостатак система за филтрирање на мрежном слоју информатичке инфраструктуре, недостатак делегације права приступа и још неки пропусти.

Плаћање откупа, као чин подстицања криминалних радњи, није долазило у обзир (одговорни у том случају могли су да сносе законске последице), а са друге стране, да је до плаћања и дошло, нико није могао да гарантује да ће подаци бити враћени. Тим који је радио на том проблему после два дана успео је да опорави мејл сервер, решавајући успут и додатне проблеме. Будући да се радило о врсти малициозног софтвера, који је заразио сервер, а са енкрипцијом почео тек после месец дана од инфилтрације у систем, проблем је био и са бекапом сервера, јер су се на њему још налазили заражени фајлови.

Као превентивна мера од оваквих напада, истиче Павловић, јесте неопходност дефинисања политике сигурности на нивоу организације, потом едукација запослених на тему информатичке сигурности и унапређење сигурности саобраћаја електронске поште, филтрирањем саобраћаја напредним решењима.

Регистар националног интернет домена Србије једини је национални интернет регистар у свету који има три нивоа заштите домена, нагласио је Жарко Кецић, који је говорио о томе на које начине РНИДС брине о безбедности националних домена .RS и .СРБ:

– Старамо се о .RS и . СРБ доменским просторима и обезбеђујемо њихов рад – ви бирате који ћете домен регистровати, а ми дајемо гаранцију да ће он да ради – рекао је и истакао важност DNS система (Domain Name System) за рад доменских простора, односно читавог интернета.

Као највећи проблем он истиче да се DNS-у не посвећује пажња коју заслужује, што доводи до многих ризичних ситуација, као што је опасност од преузимања контроле над појединим деловима DNS система, који могу да воде до преузимања контроле над било којом активношћу на интернету (приступ веб локацијама, веб сервисима, мејловима...).

Као мере заштите навео је редовно проверавање DNS записа у „родитељској" зони, потом забрану саобраћаја адресама које нису део корисниковог система (SAV – Source Adress Validation), редовно ажурирање софтвера, активацију опције Response Rate Limiting (RRL), тј. ограничавање броја упита на ауторитативним серверима, који повезују доменски систем са IP адресама, DNSSEC валидацију...

Гост из Русије Александар Венедјухин говорио је о DNSSEC-у (DNS Security Extensions) – систему сигурносних стандарда, који омогућава проверу интегритета података у DNS-у, те искуствима његове имплементације. Објаснио је да је

DNSSEC сигурносна екстензија DNS система, која штити кориснике од погрешних DNS података, које би могли да им пошаљу они који желе да их преусмере на погрешне веб адресе и домогну се њихових личних података. Одговори који прођу DNSSEC проверу дигитално су потписани, па корисник може да буде сигуран да подаци нису фалсификовани на путу од DNS сервера ка њима.

Примена DNSSEC-а у Русији почела је 2011. године, са .SU (Soviet Union) доменском зоном, која је у том тренутку била најмања, те је било разумно проверити нову технологију на мањем узорку пре него што се примени на већем. Примена нове технологије на главне руске домене, .RU и .РФ, почела је 2012. године и функционисала без икаквих проблема. Као главни разлог томе што DNSSEC није шире заступљен у руским доменским зонама, Венедјухин је навео то што администратори у то не желе да инвенстирају време, па је као решење предложио аутоматизацију која би тај процес поједноставила.

УВОЂЕЊЕ НАПРЕДНЕ СИГУРНОСТИ

РНИДС планира да уведе DNSSEC за обе доменске зоне највишег нивоа и све зоне другог нивоа које су у његовој надлежности. Организација константно прати функционисање система, користи адаптивни Response Rate Limiting на DNS серверима, а за доменске зоне највишег нивоа користи anycast сервис глобалних DNS оператера (више од 300 глобално распоређених сервера) и друга савремена решења за заштиту система и регистрацију домена.