Politika [Serbia]

Page: 19
Reach: 223959
Country: SERBIA
Size: 403 cm2

23.10.2013

Сајбер опасност велика, свест о њој мала

Наши мејлови, банковни рачуни, сајтови, рачунари и бежични интернет на мети појединачних хакера, али и одлично организованих сајбер криминалаца

Домаћи корисници рачунара и интернета нису у довољној мери безбедни на светској мрежи нити сасвим упознати са дигиталним опасностима које се крећу од хаковања сајтова појединаца жељних пажње до напада озбиљних сајбер криминалаца. Осим овога, стручњаци за безбедност на мрежи су на јучерашњем панелу „Сајбер безбедност сајбер Србије" истакли и то да су на мети рачунарских зналаца са лошим намерама сајтови, мејлови, налози на друштвеним мрежама, банковни рачуни, пословне тајне и лични подаци из различитих база података.

На београдском скупу у организацији Регистра националног интернет домена Србије (РНИДС), експерти су се сложили да од оваквих ризика морају да се обезбеде компаније, али и индивидуални корисници.

Прва грешка коју појединац прави – не штити бежични интернет. Хакери који се прикључују на његову мрежу могу да направе низ преступа или кривичних дела, а онда он мора да доказује да не стоји иза ових дигиталних напада. Компаније су у обавези да штите податке клијената, али за разлику од америчких, фирме које послују у Србији нису дужне да јавно кажу да су биле мете сајбер напада. Ипак, Милан Николић, директор корпоративне безбедности у компанији „Теленор Србија" каже да је његова фирма у првих девет месеци ове године приметила 196 озбиљних и 66 напада средње јачине.

– Корисник очекује да ће бити безбедан, али апсолутне безбедности од супернападача нема. Заштита информационих система је у великој мери идентификација нападача и процена њихових могућности – сматра Николић.

Како објашњава Лука Герзић, специјалиста за ИТ безбедност, домаће компаније углавном чекају да им неко упадне у систем, украде податке, избрише, на пример, буџет, па тек онда реагују.

– Напади су све софистицираниј, па је безбедност све компликованија. Системи заштите каскају за хакерима, али ипак напредују – примећује Герзић.

Владимир Маринков, адвокат специјализован за сајбер криминал, објашњава да се 95 одсто случајева који се воде пред српским судовима односи на појединачне хакере, а врло мали број случајеве на организовани сајбер криминал.

– Прво што треба да урадите јесте да обавезно сачувате налог, да обавестите банку или „Фејсбук" или „Хотмејл", а затим и Тужилаштво за високотехнолошки криминал –поручује Маринков. Он додаје да се поступци за сајбер криминал воде пред редовним српским судовима, што није добро, јер судије често не познају ову област.

Због неупућености, и сваком приватном кориснику може да се деси да са интернета скине софтвер који ће се не његовом рачунару инсталирати као – вирус. Милош Ранчић, систем администратор из друштвено-технолошког центра „Хаклаб", каже да су неки од тих вируса веома добро маскирани и да заиста могу да их уоче само стручњаци. Он, међутим, додаје да нису сви хакерски напади малициозни.

– Неке врсте хаковања значајне су јавно добро, као што је то случај Едварда Сноудена. Он је неовлашћеним приступом показао да је било неовлашћених приступа – оцењује Ранчић.

Коначно, после процене да домаће компаније недовољно улажу у обезбеђивање својих дигиталних информација, па тиме често и личних података својих клијената, панелисти поручују да је рачуница око сајбер сигурности врло јасна. По њима, однос уложеног и добити је један према десет, то јест сваки уложени динар компанији се, на крају, десетоструко врати.

Ј. Стевановић

Пет генерација виртуелних преступника

Како објашњава Николић, појединци углавном страхују од индивидуалних хакера, али ова област се у великој мери развијала од појединачних напада ка организованом криминалу:

ПРВИ СТАДИЈУМ: хакери ентузијасти који се доказују
ДРУГИ: монетизовање ових знања
ТРЕЋИ: организовани напади на финансијске институције
ЧЕТВРТИ: сајбер криминал
ПЕТИ: хакери као предузетници које државе унајмљују зарад политичких интереса (раде и за терористе)

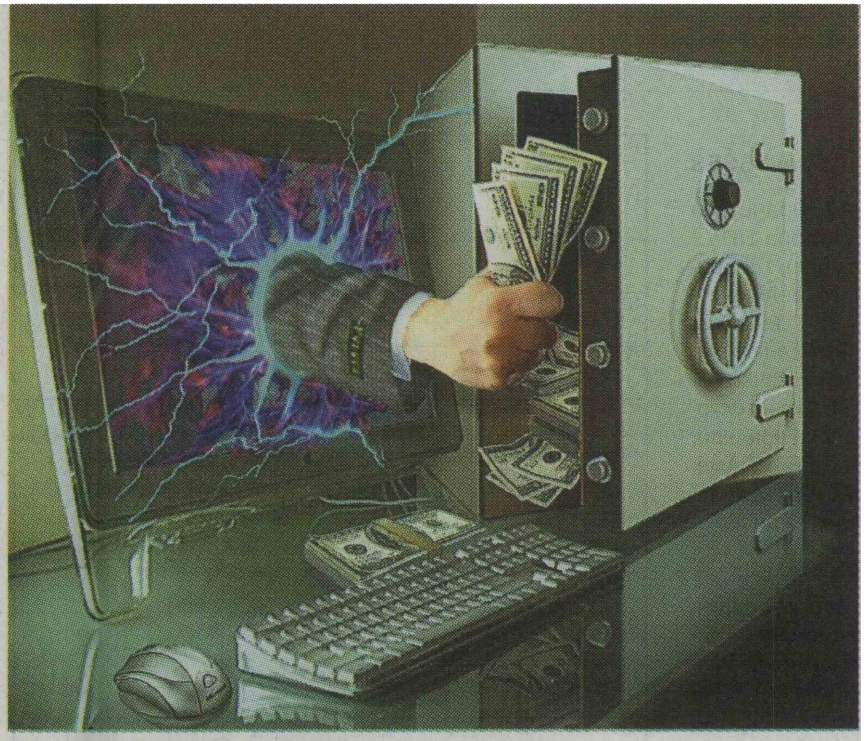

Фото freakingnews.com

Много новца се губи услед дигиталних упада