Сајбер безбедност

СКОКОВИТ ПОРАСТ ПРЕТЊИ

Пише **Милена МИЛЕТИЋ**

Технолошка будућност о којој смо само читали до пре коју годину, захваљујући сајбер свету, већ је ту – далеко је од жељене, утопистички обећавајуће слике, а претње се само умножавају и траже све брже одговоре. У историји ратовања један од најбитнијих циљева је постићи максималан ефекат уз најмање губитке. Сајбер свет баш то омогућује, чувајући живу силу и материјалне ресурсе.

Да ли сте, можда, недавно на свој мејл добили поруку у којој пише да Пошта Србије врши одређене провере, те да уколико не одете на један од два понуђена линка, нећете моћи да преузмете пошиљку која вам је стигла? Ако јесте, знајте да је овакав мејл једна у низу *фишинг* превара које последњих година надиру као поплава. У сајбер свету ове преваре одавно су познате. Има и опаснијих, сајбер ратовање, на пример. „Нажалост, створили смо тај огромни простор, интернет, и уместо да из њега црпемо само добробити, допустили смо да постане опасно место за све – и одрасле и децу", каже у разговору за „Одбрану" Катарина Јонев Ћираковић, стручњак за безбедност деце на интернету.

УЗНЕМИРУЈУЋА СЛИКА УМЕСТО УТОПИЈСКИ ОБЕЋАВАЈУЋЕ БУДУЋНОСТИ

Будућност о којој смо читали у научнофантастичним причама већ је у великој мери ту – настава на даљину и преко екрана, свет усамљености, нове технологије... Од првих компјутера „великих као соба", до паметних телефона данас, технологија комуникација расла је скоковито, преко свемирских програма, одбрамбених система попут америчког „Ратова звезда" и совјетског „Ока", а сајбер свет, као неминовна последица свега тога, данас се простире чак и на мале кућне апарате. Самим тим безбедност унутар тог простора, што аутоматски значи и претње, јесте немерљиво широко поље које обухвата личну безбедност појединаца, безбедност привреде, великих система, стратешких објеката, система одбране, влада итд.

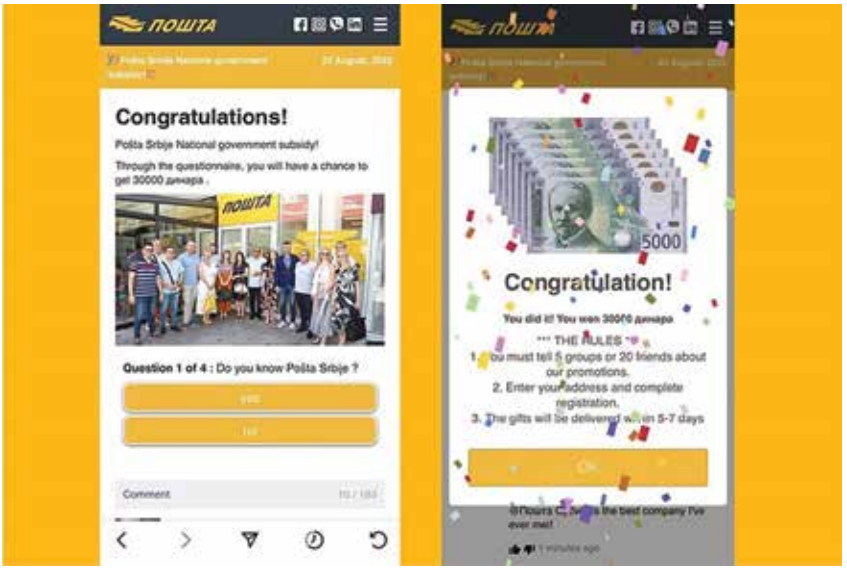
На сајту Регистра националног интернет домена Србије (РНИДС) стоји да је због „нагле интеграције интернета у скоро све облике људске делатности повећана рањивост савременог друштва од сајбер напада. Интернет је део критичне глобалне инфраструктуре и многи други битни сервиси савременог друштва (е-трговина, е-банкарство…) све више зависе од интернета и чести су мета сајбер напада...". Зато се сајбер безбедност више не може посматрати одвојено од реалног света и наших стварних живота. У смислу претњи то практично значи све, од вршњачког насиља на интернету и напада на појединца, преко крађе личних података и њихове злоупотребе, финансијског криминала, других облика криминала (апликације за комуникацију међу припадницима организованог криминала, шверц наркотика итд.), тероризма, удара на велике системе, попут недавног на Републички геодетски завод, до правог сајбер ратовања.

На сајту Регистра националног интернет домена Србије (РНИДС) стоји да је због „нагле интеграције Интернета у скоро све облике људске делатности повећана рањивост савременог друштва од сајбер напада. Интернет је део критичне глобалне инфраструктуре и многи други битни сервиси савременог друштва (е-трговина, е-банкарство...) све више зависе од интернета и чести су мета сајбер напада...". Зато се сајбер безбедност више не може посматрати одвојено од реалног света и наших стварних живота.

Наиме, у историји ратовања један од најбитнијих циљева је – постићи максималан ефекат уз најмање губитке. Сајбер свет баш то омогућује, чувајући живу силу и друге ресурсе.

У ПОЧЕТКУ..., ОДМАХ БЕШЕ ЦРВ

У освит наглог ширења сајбер света десио се инцидент који одлично показује суштинску разлику између одлучивања човека и машине, тј. алгоритма. Пол Шар, један од водећих стручњака за ратовање нове генерације, на почетку своје књиге „Војска без војника" каже да је у ноћи 26. септембра 1983. само један човек делио планету од нуклеарног армагедона – потпуковник Станислав Петров, који је дежурао у бункеру са контролом за одбрамбени систем „Око" (совјетски одговор на „Ратове звезда"). Оног тренутка кад су на екранима засветлеле лампице показујући да је противничка супер-сила испалила пет нуклеарних пројектила на СССР, Петров је требало да одмах телефоном алармира систем, и покрене узвратне ударе. Потпуковник је, ипак, застао, размислио више пута, питајући се није ли реч



Катарина Јонев Ћираковић: Није све до система, већ и до грађана. Сајбер свет је такав да родитељи морају деци постављати границе у васпитању, а сви грађани бити свесни да је безбедност нешто што морају и сами да подижу

Средином јуна Републички геодетски завод био је мета хакерског напада. Према расположивим подацима, серија напада извршена је вирусом *ransover fobos*, из четири земље (Холандија, Бугарска, Сејшели и Литванија), а било је заражено шест од укупно 3.500 рачунара и 20 од 460 сервера. Подаци завода били су закључани, а све трансакције у вези с власничким односима у Србији обустављене су на месец дана.

о грешци потпуно новог система. Пол Шар каже да би машина поступила супротно, без размишљања и разумевања последица своје активности. Значајна разлика кад је реч о ратовима нове генерације.

Шар подсећа да су се вируси одмах са ширењем рачунара појавили као проблем, те да је први прави сајбер удар почео 1988. године, кад је интернет био мали, са само око 60.000 компјутера. Тада се појавио тзв. интернет црв – *малвер,* који је заразио око десет одсто интернета. Није ништа посебно радио, мапирао је интернет, самоумножавао се, али је ипак, због недостатка безбедносних процедура, успео да зарази рачунаре, успори их и учини готово неупотребљивим.

Данашњи *малвери* су много озбиљнији, а обим свакодневне сајбер активности је огроман – неке од влада су пре седам година објављивале цифре од више десетина хиљада сајбер напада. Неки од тих напада превазилазили су класичну шпијунажу, закључавали су целе државе системе. Један од таквих напада је чувени *Стакснет вирус*.

ВИРУС ИЗ ПАКЛА, АУТОНОМИЈА ПАРАЛЕЛНОГ СВЕТА И ХАОС

Пласиран 2010. године, овај вирус нападао је сам корен рачунара и деловао скоро потпуно аутономно. Пројектован да тражи конкретан тип софтвера – *Сименс Степ 7* – вирус се показао као право паклено оружје са самонавођењем које је нападало затворене системе у објектима посебне намене, попут електрана (центрифуге), фабрика, система одбране и деловао би само на оне рачунаре чији су софтвери били уписани као мета у његов програм. Тада би се активирао, како каже Пол Шар, „одашиљући две енкриптоване ‘бојеве главе’”. Једна од њих би преотела програм компјутера, променила поставке, а друга би снимала редовне операције и пуштала их људима као лажни видео на камерама током неке пљачке. И док се открије да нешто није у реду, прође доста тзв. нултог времена (време када мета још не зна да је нападнута; данас представља чак огромну финансијску вредност).

Вирус је био пројектован да делује аутономно, независно од оног ко га је послао на задатак. Најизразитији пример штете коју је направио био је напад на иранска нукле-

арна постројења у Натанцу – центрифуге су нагло пале и тој земљи је требало две године да поврати свој нуклеарни програм. Био је, према Полу Шару, прво стварно сајбер оружје, неумољиво, ефикасно. Код овог вируса најважнија је чињеница да је деловао скоро потпуно аутономно.

Бројни ИТ стручњаци данас ће рећи да је у сајбер ратовању аутономија од суштинске важности како за само сајбер оружје, нападача, тако и за одбрану. Јер, нападе је готово немогуће похватати у потпуности кад већ почну, па је зато важно да браниоци и пре напада имају могућност активне одбране тј. чувања изнутра и сталног проналажења *малвера* и поправљања рањивости. Шар подсећа на сведочење америчког генерала Кита Александера пред сенатским комитетом 2015, кад је овај покушавао да објасни колико је тешко мануелно бранити и поправљати рањивости на 15.000 компјутера Министарства одбране, што је трајало месецима. „То би требало аутоматизовати, изместити људе из петље", рекао је Александер. На томе се већ ради – кроз бројне игре тзв. великих изазова ДАРПА, агенција америчког министарства одбране, у вишегодишњим напорима дошла је до система који сами проверавају сваки софтвер и у њему траже слабости подобне за сајбер нападе. Данас је један од таквих система познат као ХАОС.

НОВИ ТРЕНДОВИ У САЈБЕР РАТОВАЊУ

Сада су већ познати бројни примери и другачије, офанзивније врсте сајбер ратовања – обарања државних или непријатељских система уочи војних интервенција користе се већ неколико година уназад, у већини ратних сукоба који су избили у време појаве *Стакснета* и потом. Беспилотне летелице су такође производ за нову генерацију ратовања, тако и функционишу. А тако функционише и њихово обарање, тј. приземљење (случај у Ирану). Све државе света развијају стратегије употребе сајбер простора у војне сврхе. За САД на пример се зна да су овај простор дефинисале као „пету област ратовања", којом се бави око 300.000 људи у министарствима.

Слично раде и Кина и Русија, као и многе друге земље. Поједине државе имају веома отворене програме, нарочито оне који се баве прикупљањем података и праћењем

Др Марко Крстић, Руководилац службе за информациону безбедност и послове Националног ЦЕРТ-а, РАТЕЛ

ПРАВОВРЕМЕНА РЕАКЦИЈА ЈЕ НАЈБИТНИЈА

Пратећи све оно што се дешава на пољу сајбер безбедности у свету, као и претње које су одавно почеле да се појављују унутар тог виртуелног света у нашој земљи, Србија је још пре више година почела са радом на правним актима који би дефинисали сајбер претње и одговоре на њих, као и телима чији ће задатак бити да чувају безбедност државе и грађана, и да, кад се већ проблем појави, реагују. Приликом усвајања прве верзије *Закона о информационој безбедности 2016. године*, у тексту тог документа предвиђено је оснивање Националног ЦЕРТ-а, који би пратио, прикупљао и размењивао информације о ризицима, обавештавао јавност и реаговао. Већ 2017. године у оквиру РАТЕЛ-а формирана је служба која обавља послове Националног ЦЕРТ-а. Др Марко Крстић, руководилац службе за информациону безбедност и послове Националног ЦЕРТ-а, истиче у разговору за „Одбрану" кључну улогу ЦЕРТ-а – да редовним праћењем и дељењем информација омогући правовремене реакције на ове претње:

– Национални ЦЕРТ прати стање о инцидентима на националном нивоу, пружа рана упозорења, најаве и информише релевантне институције о ризицима и инцидентима, реагује по пријављеним инцидентима физичких и правних лица и пружа савете и препоруке на основу расположивих информација, подиже свест грађана, привредних субјеката и органа власти о значају информационе безбедности. За послове Националног ЦЕРТ-а надлежна је Регулаторна агенција за електронске комуникације и поштанске услуге.

*Зашто је поједине алгоритме тешко победити? Имамо бројне примере, рецимо игрица или видео-снимака на друштвеним мрежама које је готово немогуће уклонити или блокирати...

– Приликом коришћења друштвених мрежа и играња игрица корисници би требало да обрате пажњу на услове коришћења и сигурносна подешавања. У сигурносним подешавањима треба проверити да ли постоји начин да се нежељени садржаји блокирају и користити оне апликације/услуге чији су нам услови коришћења прихватљиви. Треба водити рачуна о понашању на друштвеним мрежама.

С друге стране, у случајевима када постоје сазнања да се на некој интернет страници у Србији налази малициозни садржај или да се та страница користи за спровођење сајбер напада, Национални ЦЕРТ обраћа се телекомуникационим операторима/регистрима домена како би се предузеле неопходне мере и спречили даљи напади. Слична је ситуација и када је неопходно спречити даље ширење напада из друге земље, само што тада Национални ЦЕРТ Републике Србије обавештава национални ЦЕРТ земље у којој се налази сервер на коме је постављена поменута интернет страница.

*Каква нас будућност чека када је реч о претњама у сајбер простору?

– Информациона безбедност је веома динамична област у којој нападачи константно развијају нове технике напада, али и у којој се одбрана од новодетектованих напада непрестано унапређује. Једино што је константно у овој области јесте људски фактор, стога без обзира које нас нове претње чекају, веома је важно радити на едукацији људи и унапређењу свести из области сајбер безбедности – на чему Национални ЦЕРТ континуирано ради.

телекомуникационог саобраћаја чији је циљ стварање огромних база података о становништву зарад предиктивне аналитике. У Француској то ради агенција „Френшел”, у Шведској агенција „Оникс”.

Текући рат између Русије и Украјине такође је полигон за сајбер ратовање – две државе међусобно се оптужују за бројне нападе, које су искусиле и оне земље које немају везе са тим сукобом. Србија, на пример, од почетка интервенције у Украјини – мало је недеља било а да на Аеродром „Никола Тесла” не стигну дојаве о бомбама, нарочито на летовима за Москву. Претње су се проширили на школе, болнице и друге установе и месецима су антидиверзантски одреди били заузети проверама често и више стотина објеката на дан.

Искусили смо и другу врсту сајбер ратовања – када албански хакери нападну странице разних установа код нас, нарочито оних које се баве Косовом и Метохијом, и поставе своју заставу или неке претеће поруке.

МИ И САЈБЕР ПРЕТЊЕ

Средином јуна Републички геодетски завод био је мета хакерског напада. Према расположивим подацима, серија напада извршена је вирусом *ransover fobos*, из четири земље (Холандија, Бугарска, Сејшели и Литванија), а било је заражено шест од укупно 3.500 рачунара и 20 од 460 сервера. Подаци завода били су закључани, а све трансакције у вези с власничким односима у Србији обустављене су на месец дана. У отклањању последица напада учествовало је више агенција и партнерских фирми: тим из Русије, америчка фирма „Карбон Блек”, ЕУ фирма „Есет”, као и кластер домаћих фирми „Октакрон”, „Сага”, „МДС”, Канцеларија за ИТ Владе Србије, БИА, појединачни стручњаци итд. Колико знамо данас, ниједан податак није украден, па осим застоја у раду, што се одразило на мноштво установа и послова, није било веће штете. Шта ће донети наставак истраге, видећемо. Међутим, опасност од овог напада мери се чињеницом да су укупни подаци геодетског завода једне земље основ њеног интегритета и државности, што је дефинисано документима Уједињених нација. Ово је од посебне важности за нашу одбрану, рецимо, права на Космет.

У ретким извештајима о нападима те врсте на Србију може се доћи до тога да је само

„САЈБЕР ТЕСЛА”

Као и већина савремених војски, и Војска Србије се припрема за свет сајбер напада и ратовања. У оквиру својих програма међународне војне сарадње, Војска Србије учествује и у вежбама које се баве сајбер претњама. Једна таква је „Сајбер Тесла” која се од 2016. године изводи у сарадњи са Националном гардом Охаја, САД, али и са другим армијама, као и представницима привреде, цивилног сектора. Сложеност сајбер напада одавно захтева ангажовање више сегмената сваког друштва. Зато је у новембру прошле године, у Касарни „Војвода Радомир Путник” у Горњем Милановцу, изведена вежба која се бавила електропривредом. Наиме, у замишљеном нападу, електропривреду Беле Земље напали су хакери Црвеног тима с циљем да дејством на уставе и турбине електрана произведу поплаву, нанесу велику штету, а да при томе браниоци имају утисак да је све у реду. Напади су усмерени на SCADA системе, бежичну интернет мрежу и виртуелну инфраструктуру. Оног тренутка када је примећен удар, држава је позвала у помоћ Војску и стручне тимове из јавног и приватног сектора у земљи и формирала три Плава тима за одбрану.

Вежба је показала да је најтежи део посла и најдуготрајнији, било утврђивање да ли је реч о нападу или грешки система. Овај проблем одузео је браниоцима два дана, али кад су већ утврдили да је реч о нападу, трећег дана вежбе су детектовали како се крећу нападачи, известили о томе Национални ЦЕРТ (први пут је ова установа учествовала на оваквим вежбама), који је у нашем систему четврти полигон одбране. Обавештене су и друге установе битне за реакцију и одбрану од напада. Сценарио вежбе није предвиђао уништење нападача, већ увежбавање процедура и самог одговора, па су тимови одбране били доведени у максимално реалну ситуацију.

У вежби су први пут учествовали и представници војске Републике Мађарске, а били су присутни и представници ИБМ-а, МУП-а, ИБИС-а, ЕПС-а.

У освит наглог ширења сајбер света десио се инцидент који одлично показује суштинску разлику између одлучивања човека и машине, тј. алгоритма. Пол Шар, један од водећих стручњака за ратовање нове генерације, на почетку своје књиге „Војска без војника” каже да је у ноћи 26. септембра 1983. само један човек делио планету од нуклеарног армагедона.

2020. године било више од 17 милиона покушаја упада у информационо-комуникационе системе (без навођења о којим системима је реч), више од осам милиона неовлашћеног прикупљања података и више од 60.000 покушаја постављања злонамерних софтвера на туђе мреже и опрему. У једном интервјуу за домаће медије Бранко Стаменковић, тужилац за високотехнолошки криминал, рекао је да је прошле године забележено 11% више напада и претњи него претходних година: „У 2021. години имали смо 5.274 кривична дела која су пријављена Посебном тужилаштву, а која се тичу нечега што би могло бити сајбер криминал”.

Нека истраживања показала су да се у Србији на сваких 39 секунди деси сајбер напад, било на појединца или на организацију. На страницама стручних медија и група који се баве овим проблемом може се наћи податак из истраживања наручених од интернет провајдера Верајзон 2021. да је чак

43% напада усмерено на мала и средња предузећа. Највише има привредног криминала. Такође, највећи број напада почиње управо *фишинг* кампањама попут оне с почетка овог текста. ПТТ систем Србије, на пример, и раније је био изложен сличним претњама. У фебруару ове године ЦЕРТ је упозорио на још једну сајбер превару, овога пута на Фејсбуку.

И МЕДИЈИ НА УДАРУ

Ни српски медији нису избегли нападе. Недавно је Удружење новинара Србије објавило податке агенције „Шер" која се бави сајбер безбедношћу – у последњих осам година извршено је чак седамдесет удара на инфраструктуру домаћих медија, а циљеви нападача били су пресретање комуникације, цурење поверљивих информација, објављивање садржаја које редакције нису одобриле итд. А ту је и такозвани фишинг. Најбројнији су били тзв. ДДОС напади, чији је циљ обарање сајтова.

ЛИЧНИ АСПЕКТ ПРЕТЊИ

Највећи број напада, претњи још увек је у домену личног (мада је код претњи у сајбер простору лично и опште тешко одвојиво). „Злоупотребе су бројне – фотографије, извргавање руглу физичког изгледа због гојазности и других мана, вршњачко насиље, религијско насиље, злоупотребе других врста... Предатори су крими-групе, секте, терористи, нарко-дилери, педофили... Чак и у Србији нарко-дилери користе сада и Телеграм да продају наркотике малолетницима", каже за „Одбрану" Катарина Јонев Ћираковић.

Посебно рањива група су, наравно, деца. Напади имају разне облике, почев од вршњачког насиља преко педофилије до сусрета са непосредним криминалом попут наркотика. Катарина Јонев Ћираковић подсећа на плакате поред аутобуских станица у Новом Саду са QR кодом који је директно водио до Телеграм групе за продају наркотика. Кад је о деци реч, много је већи проблем лош утицај игрица, другог садржаја, као и особа од утицаја на њихову свест и норме: „Лош је и врло опасан утицај дигиталних узора који данас често преко најмасовнијих сајбер медија, пласирају заправо антивредности. Нове генерације деце су генерације јутјубера, присталица Инстаграма, тиктокера. Ту виде лажне слике живота које потом желе да достигну".

А нису то само лажни животи старлета и других особа од утицаја већ и игре изазова. У последње време веома популаран изазов „Blackout/Gubitak svesti" постао је популаран, али је однео и 110 дечијих живота.

Смрт Кристине Кике Ђукић, тзв. јутјуберке, како је наведено, због претњи које је добијала од насилника међу пратиоцима, изазвала је велико узнемирење јавности и покретање петиције за усвајање тзв. Кикиног закона, који би посебно кажњавао ову врсту злостављања. Шта то Србија има за одговор на нове просторе претњи?

ИЗМЕЂУ СТРАТЕШКИХ ДОКУМЕНАТА, ЗАКОНА И КОНКРЕТНОГ ДЕЛОВАЊА

Када ће бити усвојен неки нови закон који ће се немилосрдно обрачунавати са свим нападачима из сајбер простора, видећемо. Оно на чему се сигурно ради јесте закон о криптовалутама. Наиме, пред помамом за тзв. рударењем сајбер валута у том свету, као и случајем једанаест нишких хакера оптужених пред судом у САД да су варали клијенте који су захваљујући њима почели да рударе на сумњивим платформама и остали без новца, Србија је кренула у прављење закона о криптовалутама. Од прописа за сада имамо *Закон о информационој безбедности*, затим *Закон о изменама и допунама постојећег документа*, Уредбу Владе Србије, *Кривични законик*. Опасности из сајбер простора су препознате и у нашој Стратегији националне безбедности.

„Поред Одељења за борбу против високотехнолошког криминала при МУП-у Србије, имамо и Тужилаштво за ову врсту криминала", каже Катарина Јонев Ћираковић. „Ту су и РАТЕЛ, односно ЦЕРТ, затим Војска, Министарство за телекомуникације, Министарство за људска и мањинска права, Министарство правде – школе су често прва инстанца за борбу против вршњачког насиља. Такође, имамо број 19833, невладин сектор".

У Влади Србије постоји и координационо тело за борбу против сајбер изазова. Али и поред система који већ постоји, регулативе, борба погођених је веома тешка и често се своди на личну акцију, осим у случају насиља над децом (Тужилаштво и МУП већ годинама воде веома успешно акцију „Армагедон" против педофилије на интернету, а кад су деца у питању, ту систем одмах реагује). Катарина Јонев Ћираковић и бројни стручњаци за ИТ сектор кажу да је ствар у томе што није све до система, већ и до грађана. Сајбер свет је такав да родитељи морају деци постављати границе у васпитању, а сви грађани бити свесни да је безбедност нешто што морају и сами да подижу. Бројни напади у последње време показали су још нешто што би било пожељно – сарадња међу државама и међународним организацијама. Много је питања, а време пред нама није више бесконачни простор који омогућава да се све боље сагледа. Сајбер свет је свет који тражи огромну брзину и стално прилагођавање. Чини се, ипак, да је одговор у интензивној сарадњи, како међу системима унутар самих држава, тако и на међународном плану, колико год је то могуће.

Данашњи *малвери* су много озбиљнији, а обим свакодневне сајбер активности је огроман – неке од влада су пре седам година објављивале цифре од више десетина хиљада сајбер напада. Неки од тих напада превазилазили су класичну шпијунажу, закључавали су целе државе системе. Један од таквих напада је чувени *Стакснет вирус*.