Мултинационална командно-штабна вежба „Сајбер Тесла”

БИТКЕ НА ЕКРАНУ КОМПЈУТЕРА

Четврту годину заредом у оквиру Програма државног партнерства Србије и Охаја у области заштите сајбер простора одржана је вежба Војске Србије и Националне гарде Охаја „Сајбер Тесла”, чија је тема била одбрана телекомуникационо-информационог система од претњи из сајбер простора. Ове године посматрачи су били из оружаних снага Мађарске. Вежба је била посебна по томе што су се у улози бранитеља, овог пута SCADA система, нашла три плава тима, а формиран је и посебан тим Националног центра за превенцију ризика у ИКТ системима Србије – НЦЕРТ.

Пише Мира ШВЕДИЋ

Хакерске групе и појединци напали су електропривредни систем фиктивне „Беле земље". Циљ им је био да промене ниво воде у резервоару који је потребан за квалитетну производњу електричне енергије, а којим се даљински управља. Пробали су да подигну тај ниво, направе неповратну штету и изазову поплаву, а да притом уређаји приказују регуларно стање. Напади су били усмерени на SCADA системе, виртуелну инфраструктуру и Wireless мрежу.

Корисници рачунарске мреже која је нападнута, у овом случају електропривреде Беле земље, приметили су опасност и затражили помоћ државних институција. Руководиоци „Беле земље" одлучили су да ангажују Војску и формирају стручне тимове за одговор на безбедносне инциденте у сајбер простору. Ти тимови су наменске јединице састављене од припадника Војске Србије и представника приватног и јавног сектора у Републици Србији. Осим тога, на основу међудржавног уговора и билатералне војне сарадње ангажовани су и експерти из оружаних снага „Плаве земље", са којима је успостављена интензивна сарадња. Њихов задатак био је да уоче, одбране и опораве рачунарску мрежу од сајбер дејстава, употребом јавно доступних софтверских алата – програма и обученог људства.

Шта се потом дешавало, показали су учесници мултинационалне командно-штабне вежбе „Сајбер Тесла", која је одржана у касарни „Војвода Радомир Путник" у Горњем Милановцу од 11. до 15. новембра. Са српске стране руководећи тим предводио је начелник Управе за телекомуникације и информатику бригадни генерал Љубиша Ђоловић, а са америчке пуковник Гари Мекју, начелник здруженог штаба Националне гарде Охаја. У вежбу су били укључени и припадници Оружаних снага Мађарске, као посматрачи.

КОРАК НАПРЕД У КВАЛИТЕТУ И БРОЈНОСТИ

„Сајбер Тесла" је вежба која се већ четврту годину заредом изводи у оквиру Програма државног партнерства Србије и Охаја у области заштите сајбер простора. У њој поред информатичара из оружаних снага две земље учествују и представници државног, приватног, јавног и академског сектора наше земље, који обављају послове у области информационе безбедности. Наравно, највише је припадника Центра за командно-информационе системе и пројектовање – ЦКИСИП-а, зато што они имају најбројнији информатички кадар, ›

али су своје представнике дале и све јединице војске. Од домаћих фирми, били су присутни представници Електропривреде Србије, МУП-а, IBIS-а, IBM-а и банкарског сектора у Републици Србији.

– Ова вежба била је масовнија од претходних и по броју учесника, којих је било 90, и по до сад највећем броју институција из јавног и приватног сектора. Припремали смо је, планирали, организовали и рад координисали са припадницима Националне гарде Охаја током десет месеци. Ове године посебан изазов нам је био SCADA систем. То су ваљски системи, апарати којима се управља путем рачунарске мреже. За ту намену припадници Електропривреде Србије донели су макету бране на којој су постојали сензори за мерење нивоа воде. Црвени тим, нападаче, чинила су два хакерска тима, који су посебним алатима покушавали да нанесу штету електропривредном систему, а у одбрани SCADA система учествовала су три плава тима, а не један као претходних година. На овој вежби први пут су увежбаване и процедуре националног ЦЕРТ-а (НЦЕРТ). Ми из руководства вежбе смо, према одређеним критеријумима и мерилима, анализирали њихове реакције – истиче потпуковник Милун Недељковић, руководилац тима за сценарио, листу главних догађаја и супозиције из руководства вежбе.

Припадници Националне гарде Охаја налазили су се у руководству вежбе и били су подељени у три плава тима. Није их било у црвеном.

Према речима учесника, та вежба можда не би била занимљива војничкој популацији, јер нема ратне технике, покрета јединица, препознатљиве динамике, конкретних дешавања, али је стручњацима из ИТ сектора била и те како интересантна и они су уживали у информатичком рату који се водио између црвеног и плавих тимови. Била је то борба са пуно динамике и победа извојеваних на екрану компјутера. Битке које су вођене тих дана биле су покушаји да се уђе у мрежу, да се поремете одређени параметри. Највише времена чланови плавих тимова изгубили су да утврде да ли се заиста десио напад или је била реч о аномалији система.

ТИМОВИ У БОЈАМА

Поред белог тима (руководство вежбе) и зеленог (електропривреда „Беле земље"), постојали су црвени тим (нападачи) и три плава тима (бранитељи). На вежби је био и златни тим, у улози консултанта. Прошле године ту улогу имао је „Мајкрософт", а ове IBM.

ЦРВЕНИ ТИМ НАПАДА

Црвени тим припадао је руководству вежбе и представљао је имитациони апарат. Његови припадници имали су задатак да симулирају и имитирају нападе, односно сајбер инциденте у простору, на рачунарској инфраструктури и на сервисима који се бране, а који су били у власништву три плава тима на вежби. Потпуковник Владан Никачевић, вођа тима за одговор (црвеног), каже да су током прва два дана вежбе извели девет напада. Сваки плави тим био је три пута нападнут, а трећег дана изведен је најкомплекснији напад, хоризонтални, који је био уперен на сва три плава тима истовремено.

– Током прва два дана циљ нам је био да чланови плавог тима прођу кроз стандардне оперативне процедуре – да утврде да се десио напад, шта је нападнуто, да одбране своју инфраструктуру и да врате у функционално стање сервис који је наш црвени тим оштетио. На почетку трећег дана сви плави тимови били су успешни. Детектовали су да се нешто догађа. Приметили су наше активности. Успели су и да утврде трагове којима смо се кретали и шта смо радили. И на крају, известили су НЦЕРТ о томе шта се десило. НЦЕРТ је у Рателу и по Закону о информационој безбедности морају им се слати извештаји, које они обрађују и обавештавају друге плаве тимове, а у реалности друге институције и компаније, о сајбер нападу који се десио, како би се заштитиле од таквог напада. То је суштина. Тако да смо и ту компоненту проигравали – истиче вођа црвеног тима.

Објашњавајући улогу НЦЕРТ-а Никачевић каже је то четврти полигон одбране, али и да га иностране армије не укључују у своје сајбер вежбе. Ми смо први који су то урадили и, како кажу, изненадили смо Американце.

ТРИ ТИМА ОДБРАНЕ

Насупрот тајновитости црвеног тима и затамњене собе у којима су били нападачи скривени од јавности, вође три плава тима (мајор Бобан Стојановић, вођа плавог тима број 1, мајор Бојан Милошевић, вођа другог тима и Иван Кузмановић из МУП-а, вођа трећег тима) морале су да смирују узавреле страсти браниоца. У тим собама било је напето јер је почео свеобухватан, комплексан и истовремени напад на све плаве тимове. Био је то почетак неке врсте ратних игара, које су члановима тима биле изузетно занимљиве, попут добро осмишљених видео-игрица.

Вођа првог плавог тима мајор Бобан Стојановић истиче да је одбрана организована на више нивоа, јер тако онемогућава противнику да јој лако приђе. Што је више нивоа одбране, противнику је теже да је преброди.

А ко су борци? Плави тим у свом саставу има вођу битке, који је руководилац техничког дела приче. Има хантере, који специјализованим алатима могу одмах да региструју ако се нешто деси у систему. Затим систем администраторе који прате, прелиставају логове да виде шта се десило и каква је врста напада. Поред њих постоје и мрежни администратори који прате стање мреже – какав је саобраћај, да ли је неко приступио мрежи, где и слично.

– Ове године убачена је SCADA. То је део инфраструктуре којој ми раније уопште нисмо имали приступ. SCADA-е нема у војсци, једино је користе ЕПС и друге фирме. Она је као лавиринт. Добили смо је готову кад је почела вежба и нисмо имали детаљнија подешавања – објашњава мајор Стојановић.

КООРДИНАЦИЈА ИНФОРМАЦИЈА

Посебност овогодишње вежбе је постојање четворочланог тима националног ЦЕРТ-а. На ранијим вежбама припадници НЦЕРТ-а нису били издвојени и учествовали су у руководству вежбе. Некад су били чланови плавог или црвеног тима, али на овој вежби, према речима др Марка Крстића, први пут увежбавају процедуре НЦЕРТ-а и комуникацију између одбрамбених тимова.

– Наша улога на вежби састоји се у координисању између институција надлежних за контролу сајбер простора наше земље. Ми смо надлежни да, уколико се деси неки напад и добијемо информације које су од значаја за остале учеснике, дистрибуирамо те информације преосталим учесницима, водећи при томе рачуна да им не изнесемо неке тајне информације, односно да не нарушимо репутацију фирме или институције у којој се напад десио. Те податке дајемо другим институцијама у систему. На овој вежби проценили смо, у складу са тренутним стањем фирме која је била погођена, а то је електропривреда „Беле земље", на ком нивоу се налази инцидент и да је потребно да обавестимо јавност, тужилаштво, институције релевантне за такву врсту обавештавања и у реалном животу. Урадили смо оно што бисмо иначе радили – истиче др Крстић.

НАЗИВ ВЕЖБЕ

Пуковник Тери Вилијамс из Националне гарде Охаја у руководству вежбе је од 2016. године. Прича да у почетку, кад су планирали вежбу, нису знали како да је назову. Дан пре почетка вежбе посетила је Музеј Николе Тесле, научника који повезује Америку и Србију и тада јој је синула идеја да вежбу назове „Сајбер Тесла".

У реалном животу национални ЦЕРТ има телефон за хитне позиве који је доступан 24 часа седам дана у недељи, па су се и на овој вежби трудили да симулирају ту улогу. Увек је половина тима остајала да прати ситуацију, чак и током паузе. Искуство им је говорило да се напади најчешће догађају изненада.

Али руководство вежбе није сценаријем предвидело да онемогући црвени тим да изврши напад. Супротно. Требало је учеснике ставити у реалну ситуацију из које могу да науче шта све може да се догоди. Циљ вежбе био је да постепено усавршавају процедуре које су раније вежбане. Колико су у томе успели, показаће анализе, које се раде по завршетку сваке вежбе, а оне детаљне након пар месеци. Уколико су анализе показале да у нечему нису дорасли, да могу боље, то ће планирати за наредну вежбу. То је изазов који „Сајбер Теслу" вуче даље.

– Имамо још много тога да учимо јер се ИТ свет развија. Сајбер напад једноставно нема границу и једини је лек будност. Морамо бити свесни да су нападачи увек у предности од браниоца, јер се брани простор који има милион врата и веома га је тешко бранити. Нападач ће увек знати на која ће врата ући и он је увек корак испред. Ми се трудимо да их пронађемо – каже потпуковник Милун Недељковић.

Фото: Даримир Банда