Сајбер криминал и мере заштите

Семинарски рад у оквиру курса Техничко и научно писање
Математички факултет

Богдан Мицић
bogdanmicic03vr@gmail.com
Никола Милорадовић
unesi mejl
Филип Антанасковић
unesi mejl
Исидора Перровић
unesi mejl

10. новембар 2022.

Сажетак

Огроман развој технологије је узроковао и развој сајбер криминала. Како је технологија све више присутнија у нашим животима, ми као појединци и компаније бивају угроженије од сајбер напада. Овај текст треба проширити свест о сајбер криминалу и његовој претњи као и начине како се боримо против њега и како се може заштити од њега.

Садржај

1 Мере заштите

Уколико знамо да се свакодневница све брже и брже одвија и да се технологија дословно развија из дана у дан, неодговорно је сматрати да је безбедност искључена из опсега развоја који за циљ поред свих других има и онај део наше стварности који се односи на дестибилизацију система и опасности од сајбер напада. Сајбер напади су све учесталији и у тренутку док пишем се десило више од 21 милиона напада у току овог дана. Али свест о опасности сајбер криминала није довољно проширена и то представља један од главних проблема. Велике компаније јесу углавном мете сајбер напада, али то не значи да мале и средње компаније и ми као појединци нисмо угрожени. Напротив, управо због слабијих мера заштита ми као појединци и мале и средње компаније постају чешће мете напада.
Наравно, ниједан систем није 100 % сигуран јер сваки има своје слабости у виду рањивости у безбедоносним подешавањима на систему и злоупотреби функција програма. Анализа рањивости система која се обавља у комбинацији са дигиталном форензиком је јако значајна са становишта заштите да би организације могле да знају који су пропусти присутни на системима, колико је тешко нападачу да их искористи и какве би последице могли да изазову. Безбедност на системима је добро описана кроз мото Ерис Соле-а: "Превенција је идеална, али је детекција обавезна". Већина организација заштиту на својим системима фокусирају на превенцији, али не и на детектовању злонамерних активности. На пример, већина компанија на својим системима има инсталиране firewall-ове који делују превентивно. При томе се јављају два проблема. Први је тај да организација не може да спречи комплетан саобраћај, што на неки начин отвара могућност за потенцијални напад. Ту се јавља и један важан изазов свакој организацији да нађе баланс између безбедности и функционалности и проточности. И други проблем лежи у чињеници да нису сви превентивни механизми прилагођени или исправно конфигурисани па самим тим пружају минималну заштиту. На пример антивируси не пружају потпуну заштиту из разлога што раде на основу базе у којој имају информације о малициозним програмима, али чим уђе у систем неки сасвим нов малициозни програм, антивирус га неће детектовати. Заштита се постиже непрекидним циклусом откривања слабости и њеним исправљањем. Само уколико постоји јасан став о разумевању безбедности рачунарских система у оквиру организације и план да се безбедносни ризици смање, могу се превазићи безбедносни проблеми. Превентивне методе које се могу применити јесу:

1. редовно ажурирање оперативног система и антивирусног софтвера
2. опрезност и одговорност запослених или нас појединаца(на пример не отварати садржину мејла ако долази од непознатог пошиљаоца)
3. спровођење редовних обука из домена сајбер безбедности
4. креирање профила за приступ, како би запослени приступали само оним деловима система који су неопходни за посао који обављају
5. креирање процедура за поступање у случајевима напада на информационе систем компаније и обезбеђивање континуитета пословања

6. коришћење комплексних лозинки које садрже велики број измешаних слова, бројева и знакова, додатно могу се користити лозинке које истичу
7. проактивно детектовање упада на систем коришћењем мамаца ханипотова(*Honeypot*) који симулирају рањиве сервисе система са циљем хватања нападача
8. употреба анализе рањивости

Ово су само неке од превентивних мера које се могу преузети. Важно је истаћи да не постоји начин да се рачунарски системи правилно заштите, уколико се не зна против чега је усмерена заштита.

2 Закључак

Шта даље очекивати од развоја како безбедоносних мера, тако и технологија помоћу којих се могу извршавати сајбер напади? Једно је сигурно, број сајбер напада ће се увећати у будућности и много више утицати на нас како се технологија буде све више интегрисала у нашим свакодневним животима. *Ransomware* је један од најзаступљенијих вируса у овој години и прави велику штету компанијама. То је само једна од многих претњи којима се нападачи користе. Технологија на претњу сајбер криминалу одговара развојем сигурносних система које би правила вештачка интелигенција тако што би учила на претходним примерима малициозних напада, научила да их детектује и у крајњем случају и уклони. Али са друге стране ту лежи и опасност примене вештачке интелигенције у развоју малициозних програма. Оно што ми можемо да предузмемо у нашој будућности је да поштујемо мере заштите и да будемо опрезни.