PROBLEMATIKA ZERO DAY NAPADA I MOGUĆA ZAŠTITA

Toplak, Marina

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:873644

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

PROBLEMATIKA ZERO DAY NAPADA I MOGUĆA ZAŠTITA

Diplomski rad

Marina Toplak

Zagreb, rujan 2021.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski sveučilišni studij

Poslovna ekonomija – smjer Menadžerska informatika

PROBLEMATIKA ZERO DAY NAPADA I MOGUĆA ZAŠTITA

ISSUES OF ZERO DAY ATTACKS AND THE POSSIBILITY OF PROTECTION

Diplomski rad

Student: Marina Toplak

JMBAG studenta: 0067554567

Mentor: Prof. dr. sc. Mario Spremić

Zagreb, rujan 2021.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Marina Toplak

(student: Marina Toplak)

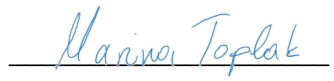
U Zagrebu, 23. kolovoza 2021.

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.

I declare that no part of the thesis has been written in an unauthorized manner, i.e., itis not transcribed from the non-cited work, and that no part of the thesis infringes any of the copyrights.

I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.



(student: Marina Toplak)

In Zagreb, 23. August 2021

Sažetak

Tehnologija postaje sve naprednija te se razvijaju nove tehnologije koje unapređuju i poboljšavaju poslovanje i svakodnevicu. Nažalost, nove tehnologije sa sobom nose i rizik kibernetičkih napada. Jedan od kompleksnijih i još nedovoljno shvaćenih napada je Zero day. Ovaj rad je osmišljen kako bi pružio uvid u kompleksnost samog napada. Što napad čini Zero day napadom, kako nastaje, tko ga provodi, zašto i koje su njegove moguće posljedice. Pošto je to vrlo složen napad koji se mijenja iz dana u dan i postaje sve sofisticiraniji i napredniji, opisani su i primjeri koji to pokazuju. Od nešto starijih napada kao što je Stuxnet i Duqu do novijih napada kao što je Sunburst i napad na Microsoft Exchange server. Zaštita od kibernetičkih napada je izazovna i ovisi o njihovoj složenosti i sofisticiranosti. Što se tiče Zero day napada, najučinkovitiji način za obranu je otkrivanje ranjivosti prije drugih i njihovo rješavanje. No, ljudi i istražuju načine koji će pomoći u zaštiti od Zero day napada. Upravo ta kompleksnost i problematika je prikazana u ovom radu.

Ključne riječi: Kibernetički napadi, kibernetička sigurnost, Zero day napad, Zero day ranjivosti, Zero day istraživanja

Summary

Technology is becoming more advanced and new technologies are being developed to improve and enhance business and everyday life. Unfortunately, new technologies carry the risk of cyber attacks. One of the most complex and still misunderstood attacks is Zero day. This paper is meant to provide insight into the complexity of the attack itself. What makes an attack a Zero day attack, how it starts, who is responsible for it, what are the consequences of this attack. Since this is a very complex attack that changes and becomes more sophisticated and advanced from day to day, there are given examples for better understanding. From slightly older attacks like Stuxnet and Duqu to newer attacks like Sunburst and an attack on a Microsoft Exchange server. Protection against cyber attacks is challenging and it depends on their complexity and sophistication. As for Zero day attacks, the most effective way of defending is to detect vulnerabilities before anybody and patching them. But people are still exploring the ways of detection and protection against Zero day attacks. This complexity and problematic are presented in this paper.

Keywords: Cyberattacks, cybersecurity, Zero day attack, Zero day vulnerabilities, Zero day research

SADRŽAJ

1. UVOD 1
1.1. Predmet i cilj rada 1
1.2. Izvor podataka i metoda prikupljanja 2
1.3. Sadržaj i struktura rada 2
2. KIBERNETIČKI NAPADI I SIGURNOST 3
2.1. O kibernetičkim napadima 3
2.1.1. Kibernetički napadi 4
2.1.2. Vrste napada 7
2.2. O kibernetičkoj sigurnosti 9
2.2.1. Položaj kibernetičke sigurnosti 9
2.2.2. Svijest o kibernetičkoj sigurnosti 11
3. ZERO DAY NAPADI 13
3.1. Što su Zero day napadi? 13
3.2. Tko su žrtve Zero day napada? 15
3.3. Otkrivanje ranjivosti 17
3.3.1. Zero day ranjivosti 17
3.3.2. Otkrivanje ranjivosti 20
3.3.3. Tržište ranjivostima 23
4. OBRADA ZERO DAY PRIMJERA 26
4.1. Napad lancem nabave na Solar Winds 26
4.2. Microsoft Exchange kibernetički napad 29
4.3. Ostali primjeri 32
4.3.1. Stuxnet 32
4.3.2. Duqu 33
4.3.3. Flame 33

5. ZAŠTITA OD ZERO DAY NAPADA 34
5.1. Problematika zaštite od Zero day napada 34
5.1.1. Otkrivanje Zero day napada 34
5.1.2. Problematika zaštite od Zero day napada 38
5.1.3. Moguće prednosti u zaštiti od Zero day napada 41
5.2. Osvrt na istraživanja o Zero day napadima 42
5.2.1. „Kontekstualni pristup detekcije anomalija za otkrivanje Zero day napada“ 42
5.2.2. „Skupovi podataka temeljeni na sustavu Windows za procjenu robusnosti sustava domaćina za otkrivanje upada (IDS) Zero day napada i prikrivenih napada“ 44
5.2.3. „Učinkovito otkrivanje Zero day crva na temelju sadržaja“ 46
5.2.4. Kratki osvrt 47
6. ZAKLJUČAK 48
7. POPIS LITERATURE 49
8. POPIS SLIKA 53
9. PRILOZI / ŽIVOTOPIS 54

1. UVOD

1.1. Predmet i cilj rada

U ovom radu će biti prikazan i objašnjen pojam Zero day napada te zašto ga je teško otkriti. Kako bi se pripremili i uveli u temu, prvo ćemo se upoznati s trendovima napada povezanih s digitalnom transformacijom. Definiran je pojam kibernetičkog napada, ali i predstavljen pogled na atribute koji ga definiraju, kao i dimenzije preko kojih ga se promatra. Nakon nekih osnova, definirani su napadi poput phishing-a, ransomware-a, DDoS napada te ponuđen uvodni opis u Zero day napad. Opisuje se pojam kibernetičke sigurnosti u odnosu na druga područja sigurnosti. I za kraj slijedi objašnjenje zašto je edukacija i razina svijesti o kibernetičkoj sigurnosti bitna.

U drugom poglavlju postavlja se pitanje što je to Zero day napad. Ime napada označava broj dana koji je ostao da se ranjivost ispravi, a to je nula. Ističe se kompleksnost samog napada i da još uvijek nema dovoljno istraživanja koja pomažu u njegovom suzbijanju. A tko su žrtve Zero day napada? Objašnjeno je postoji li točno određen tip meta ili ne, također je objašnjeno kakve posljedice trpe žrtve Zero day napada. Nakon toga slijedi pregled Zero day ranjivosti, to jest koje podjele postoje. Otkriva se na koje načine se ranjivosti otkrivaju te kako u konačnici napadači dolaze do Zero day ranjivosti.

Nakon toga su dani primjeri Zero day napada radi boljeg razumijevanja njihovih razmjera i učinaka. Na početku su prvo prikazana dva velika napada današnjice, napad na Solar Winds i napad na Windows Exchange, te je opisano kako uvelike utječu na svijest o kibernetičkoj sigurnosti. Oba napad su pogodila veliki broj žrtva preko jednih od najzaštićenijih i najkorištenijih softvera. U prikazima će biti vidljivi njihovi razmjeri i sofisticiranost. Za usporedbu tome ukratko su prikazana i 3 starija napada, koja su u svoje vrijeme bili jedni od kompleksnijih i sofisticiranijih napada.

Na kraju se razmatra način zaštite od Zero day napada. Postavlja se pitanje je li se uopće moguće u potpunosti zaštiti te kako. Prema svemu se zaključuje da je najučinkovitiji način za obranu pravovremeno otkrivanje ranjivosti i njihovo rješavanje. Kratko se prikazuje i problematika koja leži iza zaštite od Zero day napada. Svi problemi definiranja i promjene koje utječu na Zero day napade, otežavaju ne samo provedbu napada, nego i njihovo otkrivanje i zaštitu. Te kako bi se donio zaključak o mogućim načinima otkrivanja i zaštite pruža se osvrt na određena istraživanja. Na taj način se želi zaokružiti pregled Zero day napada, od njihove pozadine, provedbe pa do njihova otkrivanja.

U konačnici, cilj ovog rada bi bio detaljnije obraditi Zero day napad i prikazati njegove posljedice te na kraju donijeti zaključak o načinima zaštite od napada, to jest načinima otkrivanja Zero day napada.

1.2. Izvor podataka i metoda prikupljanja

Podaci korišteni za izradu ovog rada su prikupljeni iz sekundarnih izvora putem proučavanja i prikupljanja knjiga, znanstvenih članaka, istraživanja te internetskih izvora povezanih s temom koja se obrađuje.

1.3. Sadržaj i struktura rada

Na samom početku rada se nalazi uvod i opis teme koja se obrađuje, način prikupljanja podatka i opis strukture rada. U drugom poglavlju rada je obrađena tema kibernetičkih napada i kibernetičke sigurnosti kao uvod za ostatak sadržaja. Nakon toga, u idućem poglavlju, će se detaljnije opisati što su to Zero day napadi, zašto se oni koriste te njihovi oblici. Potom će se unutar tog poglavlja obrađivati tko su žrtve Zero day napada i kako napadači zapravo otkriju za određenu ranjivost. U četvrtom poglavlju će biti obrađeni primjeri Zero day napada, s tim da će fokus biti na Solar Winds i Microsoft Exchange napadima. Prikazat će se podaci o tome čime se organizacija bavi, tko bi mogli biti napadači, kolika je procijenjena šteta, te osvrt na cijeli događaj. Na kraju slijedi poglavlje u kojem će se obraditi problematika zaštite i otkrivanja ove vrste napada, te će biti napravljena obrada i usporedba različitih istraživanja o učinkovitosti otkrivanja Zero Day napada. Rad završava sa zaključkom o obrađenoj temi i literaturi.

2. KIBERNETIČKI NAPADI I SIGURNOST

Današnja poslovanja, ali i svakodnevni život gotovo su nezamislivi bez novih tehnologija, informacijskih sustava i sveukupnog kibernetičkog okruženja. Primjena digitalnih i informacijskih tehnologija je naglo porasla pod pritiskom COVID-19 pandemije. Mnoga poslovanja su trebala osigurati radnicima povezivanje na internu mrežu iz sigurnosti njihovih domova. Odvijanje školskog programa nije samo prešlo na slušanje nastave preko laptopa, nego su zaživjele i osvanule mnoge platforme za učenje, vježbanje i savladavanje gradiva. Ljudi su počeli shvaćati potencijal platformi poput e-građanina u svojoj novoj svakodnevnici. Digitalna transformacija je postajala sve brža. Bilo je ključno prilagoditi poslovanje novoj stvarnosti. Neki su već bili spremni na novi način poslovanja, neki se nisu dovoljno brzo prilagodili ili su jednostavno podcijenili situaciju, ali ima i onih koji djelovali brzo kako bi spasili poslovanje. Već mnogobrojan i osjetljiv informacijski sustav, moglo bi se reći da je postao još veći. Nažalost, informacijske tehnologije sa sobom nose i rizik kibernetičkih napada. Od najmanje igrice na mobitelu, pa do velikih sustava koji pohranjuju i obrađuju osjetljive podatke, sve je izloženo napadima i može prouzročiti ozbiljnu štetu. Kibernetička sigurnost je od iznimne važnosti za svakog pojedinca i za svako poslovanje.

2.1. O kibernetičkim napadima

Prema određenim statističkim podacima s Interneta, samo 5% podataka poduzeća je ispravno zaštićeno. Do hakerskog napada dolazi svakih 39 sekundi, to jest 2 244 puta na dan. Čak 95% kibernetičkih napada je uzrokovano ljudskom pogreškom. Zanimljivo je i to, da su se tijekom početka COVID-19 pandemije, napadi na Cloud povećali za nekih 630%. Kibernetički napadi u 2020. godini su opasnosti izložili čak 36 milijardi podataka. 86% njih je bilo motivirano novcem, a 10% njih je provedeno u svrhu špijuniranja. Prosječan trošak napada u 2020. je iznosio 3,86 milijuna USD, a prosječno vrijeme otkrivanja napada je bilo 207 dana. Procjenjuje se da se u svijetu koristi 300 milijardi lozinki. Svakodnevni napadi su nezaobilazni, što pokazuje i podatak da je prosječni godišnji trošak osiguranja od napada 2 691 USD po zaposlenoj osobi. Napadači svakodnevno traže nove mete i načine kojima bi mogli ukrasti ili oštetiti podatke, omesti, pratiti ili zaustaviti rad nekog sustava ili poslovanja, kako bi mogli prodati podatke, identitete, ukrasti novac, provesti ucjenu ili pak nešto treće. U isto vrijeme traže se rješenja kako otkriti i spriječiti kibernetičke napade kako bi se zaštitilo poslovanje, zaposlenici, korisnici i podaci. Moglo bi se reći da je to "igra" koja nema kraja, jer i kada se nađe način obrane od jedne vrste napada, pojavit će se drugi, i tako u krug.

Opasnost od napada na informacijsku i digitalnu tehnologiju je sveprisutna i naziva se kibernetičkim (eng. Cyber) rizikom. „Cyber rizici su one vrste informatičkih rizika koje se odnose na intenzivnu primjenu digitalnih tehnologija u poslovanju.“[1] Može se reći da kibernetički rizik predstavlja moguću opasnost od zlouporabe digitalnih tehnologija, napada ili iskorištavanja ranjivosti poslovanja ili softver bez obzira na lokaciju napadača koja u konačnici za rezultat ima određenu štetu za poslovanje, koja ne mora nužno biti novčani gubitak. Ranjivost predstavlja određenu slabost, manu ili rupu u softveru ili poslovanju koja predstavlja rizik, to jest predstavlja priliku za napadača.[2] Ranjivosti mogu bit različite, ali i omogućavati različit pristup napadačima, pa tako ponekad, jedna ranjivost ih vodi do iduće, i tako dok ne dođu do one koja im može pružiti pristup i ovlasti koje njima trebaju. Također, moguće je da napadači dođu do onoga što žele iskorištavajući određenu nespremnost i ne znanje zaposlenika ili pak vanjskih partnera koji nisu dovoljno zaštitili svoje poslovanje i tako izložili druge. Moglo bi se reći da je to zapravo većinom slučaj, da napadači ne žele izravno naštetiti poslovanju ili softveru kojeg napadaju, već da će preko njega napasti njihove korisnike, ukrasti podatke ili dobiti pristup još nečem trećem. Ipak se danas informacije i podaci mogu smatrati vrjednijima od novca. Nadalje, u općoj javnosti se osobu koja izvodi kibernetički napad naziva hakerom. „Haker je osoba koja nastoji prekršiti obranu i iskoristiti slabosti u sustavu ili mreži.“[3] Ipak, napadač može biti pojedinac, grupa pojedinaca, organizacija pa čak i određena državna služba.

2.1.1. Kibernetički napadi

Kada je ustanovljeno koji su trendovi u kibernetičkoj sigurnosti i napadima, prelazimo na kibernetičke napade. Postoje različite definicije koje objašnjavaju pojam kibernetičkog napada nastale posljednjih desetak godina. Pa se tako može zaključiti da se kibernetičkim napadom smatra svaka radnja u kibernetičkom prostoru kojom se nastoji izmijeniti, poremetiti ili uništiti računalni sustav ili mrežu, ili informacije i/ili program na njima u političke svrhe, svrhe nacionalne sigurnosti ili želje za moći. No jednu definiciju vrijedi istaknuti. „Operacije, bilo u napadu ili u obrani, namijenjene da izmjene, izbrišu, pokvare ili uskrate pristup računalnim podacima ili softveru u svrhu: (a) propagande ili obmane; i/ili (b) da djelomično ili potpuno

[1] Spremić, M.: Sigurnost i revizija IS-a u okruženju digitalne ekonomije, Ekonomski fakultet – Zagreb, Zagreb, 2016.
[2] Akram, J., Ping, L.: “How to build a vulnerability benchmark to overcome cyber security attacks”, The Institution of Engineering and Technology, Key Laboratory of Information System Security, School of Software, Tsinghua University China, Beijing, People's Republic of China, 2019.
[3] Akram, J., Ping, L.: “How to build a vulnerability benchmark to overcome cyber security attacks”, The Institution of Engineering and Technology, Key Laboratory of Information System Security, School of Software, Tsinghua University China, Beijing, People's Republic of China, 2019.

poremete rad ciljanog računala, računalnog sustava ili mreže i tim povezanu infrastrukturu; i/ili (c) da prouzrokuju vanjska fizička oštećenja računala, računalnog sustava ili mreže.“[4] Tijekom godina će se razvijati novi napadi i pojam kibernetičkih napad, radi prilagodbe novim tehnologijama i trendovima. Sukladno tome, razvijat će se i nove definicije kibernetičkih napada.

No kako bi napad bio uspješan, pretpostavlja se da je potreban scenarij za izvođenje napada. „Scenarij kibernetičkog napada je opis slijeda događaja koji proizlaze iz interakcije među pojedincima i organizacijama uključenima u kršenje internetske sigurnosti, kao i njihovi dionici.“[5] S druge strane postoji životni ciklus nastanka kibernetičkog napada koji opisuje slijed događaja od nastanka ideje, razrade napade i potrebnih prilagodbi do konačne provedbe napada.

Kod kibernetičkih napada ćemo spomenuti 7 bitnih faza životnog ciklusa:[6]

- 1.faza: istraživanje i analiza ranjivosti
- 2.faza: procjena identificiranih ranjivosti te izrada testnog napada
- 3.faza: provedba prvog testnog napada
- 4.faza: analiza rezultata i istraživanje sigurnosnih kontrola protiv napada
- 5.faza: ispravke i nadogradnje u svrhu poboljšanja napada
- 6.faza: provedba drugog testnog napada
- 7.faza: konačni razrađeni napad s ciljem

Iako nisu svi napadi dobro organizirani i detaljno razrađeni, svaki od njih je isplaniran, manje ili više, i ima točno određen cilj kojeg se želi ostvariti. Kako bi se kibernetički napadi bolje razumjeli, a time i lakše prepoznali i lakše provela obrana sustava i poslovanja, važno je upoznati se s potencijalnim atributima napada i njegovim dimenzijama. Pa tako će u nastavku biti predstavljene analize koje su pokušale upravo to.

Stoga, prema analizama kibernetičkih napada postoje 2 podjele bitnih čimbenika koji obilježavaju kibernetičke napade. Tako prema definicijama kibernetičkih napada, postoji 5 ključnih atributa, a to su napadači ili činitelji, ciljana imovina, motivacija, nastale posljedice

[4] Roscini, M.: Cyber Operations and the Use of Force in International Law, Oxford, Oxford University Press, 2014.
[5] Kadivar, M.: “Cyber-Attack Attributes”, Technology Innovation Management Review, 2014., 22.-27. str.
[6] Spremić, M., Šimunic, A.: “Cyber security challenges in digital economy”, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018, IAENG, Hong Kong, 2018., 341.-347. str.

na ciljanoj imovini te dužina samog napada, a nakon analize 10 različitih napada uvedeno je još 6 atributa, a to su vektor ili put napada, ranjivost, zlonamjerni softver, botnet, porijeklo i ciljana destinacija.[7] Može se reći da je tih 11 atributa ključno pri analizi određenog napada kako bi se prikupile sve potrebne informacije o veličini napada, šteti te potencijalnom pronalasku krivaca.

No, s drugog gledišta, možemo promatrati dimenzije kibernetičkih napada i to istraživanje će opisati u ostatku ovog odlomka.[8] Na prvi pogled se vidi sličnost s atributima, ali s nešto drugačijom podjelom. U dimenzije napada spadaju agenti napada ili napadači, koordinacija napada, porijeklo napada i njegova obilježja, motiv, vrijeme ili trenutak napada te sredstva za napad.[9] Napadačima se smatraju osobe koje su provele napad i stavlja se naglasak na njihovu ulogu, u kojoj su oni točka prelaska napada u kibernetički prostor. S obzirom na koordinaciju napada, dijele se na organizirane ili koordinirane i neorganizirane ili nekoordinirane napade. S tim da u neorganizirane napade, spadaju napadi koji nisu obavljeni putem jedne osobe, grupe ili organizacije, već oni koji su spojili ljude na različitim lokacijama koji inače nisu povezani. Porijeklo napada se odnosi na lokaciju napada i odakle je napad krenuo. U slučaju i da se dođe do mjesta s kojeg je krenuo napad, ne dolazi se nužno i do napadača. Ono što je zanimljivo, je da se i ovoj podjeli ističe uloga botnet-a i pružatelja usluge. Za razliku od prethodne podijele, u ovoj se ističe da određivanja atributa napada predstavlja poseban izazov, te da ih nije moguće jednoznačno odrediti. Nadalje, motivi za napad su različiti, od političkih, nacionalnih, financijskih, ekonomskih, etičnih pa sve do osobnih. Zanimljivo je i da do određenih napada dolazi netom poslije ključnih događaja ili na određene datume ili obljetnice, koji su služili kao okidač na napad. Uz to se ističe da ipak većina napada uključuje neki oblik osvete ili ljutnje kao oblika motivacije. To se može prepoznati i putem vremena izvođenja napada.

Zaključuje se da sredstva ovise o ostalim dimenzijama napada, to jest, tko je napadač, je li to organizirani napad, koji mu je motiv, odakle i kada će biti obavljen. Na posljetku je dodatno istaknuto da se napadi poput DDoS i Zero Day napada smatraju posebno složenima i smatra se da zahtijevaju ulaganje veće količine sredstava, vremena i znanja, te se tim obrazlaže težina obrane i prepoznavanja tih napada.

[7] Kadivar, M.: "Cyber-Attack Attributes", Technology Innovation Management Review, 2014., 22.-27. str.
[8] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: "Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural", IEEE Technology and Society Magazine, 2011., 28.-38. str.
[9] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: "Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural", IEEE Technology and Society Magazine, 2011., 28.-38. str.

2.1.2. Vrste napada

Upoznali smo se s pojmom kibernetičkoga napada, kako ga je moguće analizirati, tko su napadači i na koje podjele ih možemo podijeliti. U nastavku ovog odlomka će se pričati o nekim od najpoznatijim i najčešćim vrstama napada.

„Phishing je vrsta računalne prijevare s ciljem krađe identiteta.“[10] No, phishing nije uvijek imao isto značenje. S obzirom da se pojam koristi još od 1980. godine, vrlo je jasno da se oblik i način napada mijenjao tijekom godina, a s tim i njegova definicija. Uz to nastajali i različiti oblici phishing-a kao na primjer e-mail phishing i sms phishing. Phishing napad se najčešće odvija slanjem digitalnih poruka osobama za koje se očekuje da će otvoriti mail i link ili prilog unutar maila koji u sebi nosi virus ili neki kôd, ili pak putem kojeg će doći do potrebnih informacija od korisnika. No, iako su korisnici sve obrazovaniji i svjesniji mogućih phishing napada, u isto vrijeme i napadi postaju sve složeniji kako bi lakše zavarali žrtve. Uz pomoć strojnog učenja i analiziranja komunikacije meta, šalju mailove koji su namijenjeni baš toj osobi, na potrebnom jeziku pa čak i žargonu, tako da osobi poruke izgledaju vjerodostojno i zavaraju je.

Ransomware je vrsta zlonamjernog računalnog programa čija je svrha pristupiti podacima na temelju kojih će moći ucijeniti žrtvu. Osim prijetnje da će se objaviti određeni osjetljivi podaci, ukraćivanjem pristupa podacima u zamjenu za otkupninu i ransomware postaje sofisticiraniji. Noviji i napredeni oblici omogućuju šifriranje podataka te zahtijevaju otkupninu u kripto valutama kako bi im dali šifru zauzvrat, a kripto valute onemogućuju praćenje novca do počinitelja. Ovaj oblik virusa se također najčešće preuzima otvaranjem zaražene elektroničke pošte. Jedan od najpoznatijih primjera ovog napada je Wanna Cry napad.

„Botnets se odnose na mrežu tisuća ili milijuna računala (uređaja) pod kontrolom napadača koja se, mimo znanja korisnika, koriste kao sredstvo zlouporabe i metoda napada na ciljane i pomno odabrane računalne resurse (slanje neželjenih poruka elektroničke pošte - spam poruka, online oglašivačke zloporabe, pokretanje i izvođenje DDoS napada, podržavanje phishing napada, anonimnost mrežnoga prometa napadača itd.).“[11] Postoje dva oblika botnet mreže. Stariji oblik je model klijent-poslužitelj, gdje se preko jednog zajedničkog poslužitelja poveže s njegovim klijentima i bez njihovog znanja napravi 'botovima'. Drugi model je P2P model,

[10] Spremić, M.: Sigurnost i revizija IS-a u okruženju digitalne ekonomije, Ekonomski fakultet – Zagreb, Zagreb, 2016.
[11] Spremić, M.: Sigurnost i revizija IS-a u okruženju digitalne ekonomije, Ekonomski fakultet – Zagreb, Zagreb, 2016.

gdje kao 'botove' koriste računala unutar iste mreže koji nemaju nužno jednog istog poslužitelja. U oba slučaja, 'botovi' napadaju, zagušuju i ruše određenu žrtvu.

DDoS napadi ili raspodijeljeni napad uskraćivanjem usluge „kojima se koordinirano, upotrebom više računala, ponekada i botnet-a, napadaju određeni resursi sustava s ciljem onemogućavanja njihova rada.“[12] Botnet, koji je prethodno opisan i upravo on je jedan od češćih načina za provođenje DDoS napada, jer može u kratkom roku zaraziti dovoljnu količinu računala koja će potom preopteretiti mrežu žrtve i načiniti štetu. Smatra se da se koriste za osvetničke napade, ali i kao distrakcija dok se provodi još neki napad.

„Društveni inženjering (eng. social engineering) se odnosi na navođenje ili manipuliranje osobama kako bi otkrili što je moguće više podataka o sebi.“[13] Putem različitih medija i društvenih mreža napadači iskorištavaju slabost ljudske psihologije kako bi pristupili njihovim privatnim i osjetljivim podacima. Na taj način kradu on-line identitete u svrhu zloupotrebe i/ili daljnje prodaje.

Idući napadi spadaju pod takozvane vektor napade (eng. attack vectors). To su napadi koji stječu pristup računalu, računalnom sustavu i/ili bazi podataka kako bi ih zarazili zlonamjernim programom ili ukrali podatke.

Drive-by napad je ili lažna stranica ili stvarna stranica koja je zaražena zlonamjernim programom kojeg korisnik pokupi na računalo samim otvaranjem te stranice.

„Man-in-the-middle napad nastaje kada se napadač koji se nalazi na kanalu između tražitelja resursa i resursa iskorištava ranjivosti mreže i zaobilazi komunikacijske protokole, čime mu je omogućeno nadgledati sadržaj, pohranjivati datoteke i mijenjati sadržaj komunikacije.“[14] Pri tom ni jedna strana nije svjesna da netko prati, mijenja i kontrolira komunikaciju kako bi dobio podatke koji su mu potrebni.

SQL injection je napad kojim se u softver koji koristi SQL jezik, ubacuje zlonamjerni kôd. No, da bi taj napad bio moguć, prvo treba postajati ranjivosti ili rupa u kôdu u koju se može dodati takav zlonamjerni kôd. S tim kôdom mogu promijeniti ili dodijeliti ovlasti ili promijeniti određene funkcije programa.

[12] Spremić, M.: Sigurnost i revizija IS-a u okruženju digitalne ekonomije, Ekonomski fakultet – Zagreb, Zagreb, 2016.
[13] Spremić, M.: Sigurnost i revizija IS-a u okruženju digitalne ekonomije, Ekonomski fakultet – Zagreb, Zagreb, 2016.
[14] Spremić, M.: Sigurnost i revizija IS-a u okruženju digitalne ekonomije, Ekonomski fakultet – Zagreb, Zagreb, 2016.

Zero day napadom se smatra napad koji iskorištava Zero day ranjivost koja je dostupna prije nego što je popravljena. Odnosi se na softvere kod kojih je otkrivena ta ranjivost te napadači iskoriste svoju priliku prije nego što se razvije „zakrpa“ (eng. patch) za tu ranjivost.

To su samo neki od napada koji su svakodnevnica kibernetičkog prostora. Kako bi se otkrili na vrijeme i razvile potrebne mjere sigurnosti, potrebno je pratiti što se događa, koje promijene se događaju, kako napreduju te koji novi oblici se javljaju i zašto. Zato postoji kibernetička sigurnost, koja se bori protiv kibernetičkih napada kako bi osigurala što sigurniji prostor za daljnji razvoj i poslovanje. „Što su te kontrole učinkovitije i bolje oblikovane, manje je vjerojatno da će informacijski sustav biti izložen nekoj prijetnji i da će se neželjeni događaj ‘razviti’ u rizik za poslovanje.“[15]

2.2. O kibernetičkoj sigurnosti

Kada se priča o kibernetičkom prostoru i kibernetičkim napadima postavlja se pitanje zaštite podataka, programa, sustava i poslovanja. „Glavni fokus kibernetičke sigurnosti odnosi se na osmišljavanje i provedbu učinkovitih kontrola koje će pomoći u zaštiti poduzeća i pojedinaca od namjernih napada, kršenja, incidenata i posljedica.“[16] Ukratko, kibernetička sigurnost štiti kibernetički prostor i njegove sudionike od kibernetičkih napada.

2.2.1. Položaj kibernetičke sigurnosti

Kao i kod kibernetičkih napada, postoje različite definicije koje su nastale zadnjih desetak godina. Pa tako kibernetičku sigurnost možemo promatrat kao aktivnost, proces ili skupinu alata, tehnologija, procesa i ideja dizajniranih kako bi štitili i branili računala, računalne sustave i mreže kao i informacijski i komunikacijski sustav od napada s ciljem osiguranja njihove povjerljivost, integritet i dostupnost.[17] Iznimno je kompleksno ponuditi jednu definiciju i zato je više njih valjano i prihvaćeno. „Neke od tih definicija uključuju pozivanje na ne tehničke aktivnosti i ljudske interakcije, one pokazuju prevlast tehničke perspektive u literaturi.“[18] No, ne treba zaboraviti da je uloga ljudskog faktora također nezaobilazna.

[15] Spremić, M.: Sigurnost i revizija IS-a u okruženju digitalne ekonomije, Ekonomski fakultet – Zagreb, Zagreb, 2016.
[16] Spremić, M., Šimunic, A.: “Cyber security challenges in digital economy”, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018, IAENG, Hong Kong, 2018., 341.-347. str.
[17] Craigen, D., Diakun-Thibault, N., Purse, R.: “Defining Cybersecurity”, Technology Innovation Management Review, 2014., 13.-21. str.
[18] Craigen, D., Diakun-Thibault, N., Purse, R.: “Defining Cybersecurity”, Technology Innovation Management Review, 2014., 13.-21. str.

Potrebno i je razumjeti i poziciju kibernetičke sigurnosti naspram drugih domena te njenu ulogu. Kibernetička sigurnost nije u potpunosti isto što i informacijska sigurnost, već je dio informacijske sigurnosti. „U praksi se kibernetička sigurnost prvenstveno bavi onim vrstama napada, proboja ili incidenta koji su ciljani, sofisticirani i teško ih je otkriti ili kontrolirati.“[19] Što znači, kao što se i prethodno definiralo, kibernetička sigurnost se odnosi samo na određene napade, i to na one koji su povezani s tehnologijom.

Na slici 1. je prikazan položaj različitih područja sigurnosti, a ona su:[20]

- Informacijska sigurnost (eng. information security) – zaštita svih dostupnih informacija
- Sigurnost informacijskih i komunikacijskih sustava (eng. ICT security) – osiguranje informacijskih i komunikacijskih sustava povezanih na određenu mrežu
- Mrežna sigurnost (eng. network security) – zaštita dizajna, provedbe i rada mreža
- Sigurnost na Internetu (eng. Internet security) – zaštita i osiguranje dostupnosti usluga Interneta i povezanih ICT sustava
- Zaštita kritične informacijske infrastrukture (eng. critical information infrastructure protection) – osigurava da su ti sustavi i mreže zaštićeni i otporni protiv svih rizika unutar informacijske sigurnosti

Slika 1 Veza kibernetičke sigurnosti i ostalih područja sigurnosti

Izvor: Martínez Torres, J., Iglesias Comesaña, C., García-Nieto, P.J.: “Review: machine learning techniques applied to cybersecurity”, International Journal of Machine Learning and Cybernetics, 2019.

[19] Spremić, M., Šimunic, A.: “Cyber security challenges in digital economy”, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018, IAENG, Hong Kong, 2018., 341.-347. str.
[20] Martínez Torres, J., Iglesias Comesaña, C., García-Nieto, P.J.: “Review: machine learning techniques applied to cybersecurity”, International Journal of Machine Learning and Cybernetics, 2019.

„Kibernetička se sigurnost također ponekad neprikladno povezuje u javnoj raspravi s drugim pojmovima kao što su privatnost, razmjena informacija, prikupljanje obavještajnih podataka i nadzor. Privatnost je povezana sa sposobnošću pojedinačne osobe da kontrolira pristup drugih osoba informacijama o toj osobi.“[21] Prema tome, privatnost bi označavala količinu informacija koju određena osoba dijeli o sebi, a u kibernetičku sigurnost bi ušla zaštita osobnih podataka od zloupotrebe drugih. Razmjena informacija je namjerna i pri pristanku sudionika u komunikaciji, ali dolazak do informacija i podataka koje netko nije svojevoljno podijelio korištenjem tehnologije spada u kibernetičku sigurnost. Prikupljanje obavještajnih podataka prema zakonima i pravilima, kao i dozvoljeni nadzor osoba, poslovanja ili nečeg trećeg, ne smatra se problemom. Određenu granicu, što spada u kibernetičku sigurnost, a što ne, bitno je znati prepoznati.

2.2.2. Svijest o kibernetičkoj sigurnosti

U trošak osiguranja od napada, koji iznosi 2 691 USD po zaposlenoj osobi u 2020.godini, ulazi i edukacija zaposlenika o važnosti kibernetičke sigurnosti. I dalje je 95% kibernetičkih napada prouzrokovano ljudskom pogreškom. To je glavni pokazatelj da svijest o kibernetičkoj sigurnosti nije na razini na kojoj bi se očekivalo da bude u današnje doba. S obzirom na pristup beskrajnom broju informacija i edukaciji koja se potiče o kibernetičkim napadima, pojedinci ili i dalje nisu svjesni rizika ili pak nisu svjesni da je taj rizik sve veći iz dana u dan. „Svijest o kibernetičkoj sigurnosti je stupanj razumijevanja korisnika o važnosti informacijske sigurnosti i svoje odgovornosti i djela za izvršavanje dovoljnih razina kontrola informacijske sigurnosti radi zaštite podataka organizacije i mreža.“[22] Upravo ta svijest je jedna od ključnih čimbenika u zaštiti i osiguranju računala, sustava, mreže i poslovanja od mogućih kibernetičkih napada.

„Glavni čimbenik rizika informacijske sigurnosti je razina individualne svijesti o kibernetičkoj sigurnosti, koja se može opisati kao niska, srednja ili visoka.“[23] Niska svijest bi se mogla opisati i kao da svijest u opće ne postoji. Takve osobe se ne drže danih uputa kako sudjelovati u kibernetičkoj sigurnosti i smatraju ih irelevantnima. To može uključivati postupke od otvaranja elektroničke pošte bez ikakvog opreza, do ne ispunjavanja svojih obveza kao što je na primjer mijenjanje lozinke. Zbog svoje nesmotrenosti su jedna od glavnih prilika za napadače, to jest jedna od najslabijih točaka poduzeća. Srednja svijest bi se mogla gledati kao ne razumijevanje

[21] Fischer, E.A.: “Cybersecurity Issues and Challenges: In Brief”, Congressional Research Service, 2016.
[22] Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.J.: “The impact of information richness on information security awareness training effectiveness”, Computers & Education, 2009.
[23] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Fatih Cetin, F., Basim, H.N.: “Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study”, Journal of Computer Information Systems, 2020.

nekih složenijih opcija kibernetičke sigurnosti, pa bi se greške mogle gledati kao nenamjerne. Sukladno prethodnim objašnjenjima, jasno je da se visoka svijest onda smatra i najboljom i najučinkovitijom. Edukacijom o kibernetičkoj sigurnosti, cilj je postići upravo visoku svijest o kibernetičkoj sigurnosti.

Jasno je da osobe koje su završile obrazovanje u tehnološkom području i rade izravno u toj struci imaju veće predznanje, a time i svijest o mogućim opasnostima. No, u većini organizacija možda ne postoji ni odjela s takvim zaposlenicima, što znači da svi ili većina njih nisu upoznati s opasnošću. Tu nastupa edukacija. Edukacija je prvi korak k podizanju svijest. Potrebno kontinuirano podučavati zaposlenike i upoznavati ih s novim prijetnjama, ili bar podsjećati na one s kojima su se već upoznali. Podučiti ih kako prepoznati potencijalnu prijetnju te što učiniti u slučaju kad misle da postoji opasnost. Isto tako im treba dati upute što ako dođe do napada kojeg su oni svjesni, je li oni mogu nešto učiniti ili koga trebaju obavijestiti.

3. ZERO DAY NAPADI

Među mnogim kibernetičkim napadima posebnu ulogu stječu Zero day napadi. To nije obični napad čiji je postupak lako opisati ni definirati. Zero day napadi se provode u kombinaciji s drugim napadima. Zero day napadi iskorištavaju slobodan "ulaz" kako bi se neprimjetno ubacili u softver, sustav ili mrežu. Detaljnije o Zero day napadu, tko su potencijalne žrtve ovakvog napada i je li ih se može kategorizirati, te kako se otkrivaju ranjivosti saznat ćete u ostatku ovog poglavlja.

3.1. Što su Zero day napadi?

Jedno vrijeme se vjerovalo da Zero day napadi i nisu baš učestali. Zbog toga, a možda i zbog činjenice da ih je teško otkriti prije nego što se dogode, i dalje nema dovoljno istraživanja o njima. Također se smatralo da Zero day napad čini novo otkrivena ranjivost koja je otkrivena na dan izbacivanja novog softvera, te da je tada napad i proveden. Prevedeno na hrvatski zero day znači nulti dan. To jest, na nulti dan pokretanja softvera dolazi do iskorištavanja njegove ranjivosti, po čemu je i dobio naziv. Ali, na što se danas odnosi Zero day? Zero day danas predstavlja broj dana, koji je programerima ostao da isprave grešku u kôdu, to jest nađu zakrpu (eng. patch).

Kao i u svakom području, postoji određena terminologija za bolje razumijevanje teme. „Zero day ranjivosti su softverske ranjivosti za koje nisu objavljene zakrpe ili popravci.“[24] Da, zero day se bazira na softverskim ranjivostima, koje su nastale određenim propustom i nesvjesno. Zanimljivo je da jedan programer u prosjeku napravi oko 70 'bugova' u 1000 linija kôda, te otprilike njih 15 dođe do korisnika. Može se pretpostaviti da je razlog tome problem dugotrajnosti. Da obrazložimo, dok programer ispravi jedan 'bug', smatra se da može napisati oko 30 linija kôda. To je jedan od razloga zašto je teško napraviti besprijekoran kôd bez i jedne greške. „Zero day eksploatacija je softver, dio podataka ili slijed naredbi koji služe za iskorištavanje Zero day ranjivosti.“[25] Pojednostavljeno, eksploataciju čine načini iskorištavanja prikupljenih ranjivosti. „Zero day napad je onaj napad koji iskorištava Zero day ranjivost.“[26]

Među literaturama postoje određene razlike o karakteristikama Zero day napada. Pa tako jedne kažu da je pružatelj usluge svjestan Zero day ranjivosti koje nisu zakrpane, dok u drugim

[24] Ablon, L., Bogart, A.: Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, RAND Corporation, Santa Monica, CA, 2017.
[25] Kaur, R., Singh, M.: “A Survey on Zero-Day Polymorphic Worm Detection Techniques”, IEEE Communications Surveys & Tutorials, 2014.
[26] Kaur, R., Singh, M.: “A Survey on Zero-Day Polymorphic Worm Detection Techniques”, IEEE Communications Surveys & Tutorials, 2014.

literaturama ističu da nije upoznat s tim. Potom u nekima kažu da su Zero day ranjivosti javno objavljene, a u drugima da nisu, već je napadač do njih došao nekim drugim putem. Je li napadač došao do ranjivosti jer je javno objavljena ili ne, te je li pružatelj usluge nje bio svjestan ili ne, vjerojatno ovisi od situacije do situacije. Također, spominje se da napadači koriste Zero day napad kako bi došli do organizacija koje inače oprezno i redovito saniraju sve 'bugove', zato što se smatra da su im Zero day ranjivosti jedina prilika kako bi napali te organizacije.[27] Ono što je sigurno, napadač je došao do dostupne ranjivosti koja je već trebala biti sanirana.

Kako bi se dodatno ukazalo na učestalost Zero day opasnosti, slijede određena zapažanja:[28]

- Zabilježeni Zero day napadi su trajali 19 dana do 30 mjeseci
- Tipični Zero day napad traje 312 dana ili u prosjeku 10 mjeseci
- Od 18 prepoznatih ranjivosti, njih 11 su neprepoznate Zero day ranjivosti
- Nakon što su Zero day ranjivosti otkrivene, broj napada se poveća za 2-100 000 puta

Vrijeme trajanja Zero day napada je vrlo varijabilno. Činjenica da napadi mogu trajati i po 2 i pol godine, najbolji je prikaz koliko je kompleksno i teško otkriti Zero day napad. Kod napada otkrivenih nakon samo 19 dana moglo bi se čak komentirati koju ulogu je imala sreća, a koju tehnike otkrivanja napada. Postavlja se pitanje koliko su tehnike otkrivanja učinkovite i je li se dovoljno radi na unaprjeđivanju istih.

Zero day napad ne bi postojao bez Zero day ranjivosti. Pa ako bi promatrali životni ciklus Zero day napada mogli bi ga podijeliti na:

- 0.faza: Implementacija softvera s greškom u kôdu
- 1.faza: Otkrivanje Zero day ranjivosti
- 2.faza: Iskorištavanje ili eksploatacija Zero day ranjivosti
- 3.faza: Zero day napad
- 4.faza: Otkrivanje Zero day napada

Ovo bi bio jednostavni pogled na životni vijek uspješnog Zero day napada, od njegovog "začeća" pa do "smrti". Radi se na tehnikama otkrivanja Zero day napada prije nego što se oni dogode te onih koji su se već dogodili.

[27] Ablon, L., Bogart, A.: Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, RAND Corporation, Santa Monica, CA, 2017.
[28] Bilge, L., Dumitras, T.: "Before We Knew It: An Empirical Study of Zero-Day Attacks in The Real World", Association for Computing Machinery, New York, NY, United States, 2012., 833.-844. str.

3.2. Tko su žrtve Zero day napada?

U prethodnom poglavlju pričalo se o kibernetičkim napadima, koji su njihovi atributi, ciljevi i motivacija. Sada je došlo vrijeme da se upoznate s posljedicama tih napada i tko sve trpi posljedice tog čina. Napadi su provedeni zbog financijskih, političkih, statusnih, osobnih ili osvetničkih motiva. Određenim napadima je cilj nanijeti štetu meti, ali nekad je to samo put, koji vodi do nekog drugog cilja. Ako trebaju oštetiti podatke, prevariti zaposlenike određene organizacije, ukrasti novac, zahtijevati novac ili samo u tajnosti prikupljati podatke o organizaciji, napadačima većinom nije bitno tko bi sve mogao kasnije ispaštati zbog njihovih djela. To im je samo usputna šteta kako bi postigli ono što žele.

Zero day napad je napad koji iskorištava ranjivost kako bi napala metu. Metama ili potencijalnim žrtvama se najviše smatraju one organizacije, koje svoje softvere redovito i detaljno prate te saniraju nastale greške. Napadači čekaju jedan kobni propust koji će predstavljat njihovu prednost. Iz toga se može zaključiti da ciljane žrtve jesu određene organizacije. Uz to se može pretpostaviti da ciljaju kompanije koje razvijaju svoje softvere. Ne misli se da su to isključivo softverske organizacije, zato jer je danas dosta usluga i tehnologija popraćeno određenim program ili aplikacijom. Nadalje, uslugu organizacije, softver, aplikaciju ili sustav koriste dalje njihovi klijenti. Klijenti mogu biti druge organizacije, koje koriste određeni program u svom poslovanju ili pak proizvod s određenim softverom, te krajnji korisnici. U svakom slučaju, pri Zero day napadu se dolazi do tih klijenata te se napad širi s prve mete na sve s njom povezane činitelje. Iako nije pravilo, uočljivo da su napadi orijentirani na veće organizacije koje imaju širi spektar korisnika i koji imaju korisnike s visokim razinama povjerljivosti, što će se vidjeti i u primjerima. Zero day napad najviše ovisi o motivaciji i cilju koji želi ostvariti, te postoji li prilika za to. Osim poslovnih organizacija, Zero day napad, kao i bilo koji drugi kibernetički napad, može biti usmjeren i na državu, državne organizacije, kritične infrastrukture i pojedince.

Štete koje donose kibernetički napadi su: fizičke, financijske, informacijske, tehnološke i psihičke.[29] Prve vidljive štete su, tako reći, površinske. Fizičko oštećenje je lako primjetno i teško ga je sakriti. Ovisno o veličini štete i financijske posljedice su lako uočljive. Kada određena organizacija ostane bez dijela budžeta zbog kibernetičkog napada, i pri tom treba uložiti dodatni novac u zaštitu poslovanja, novac se oduzima iz odjela i od zaposlenika. Mogli bismo te dvije posljedice nazvati i vidljivim posljedicama napada. Ali, to nisu jedine posljedice

[29] Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: "Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural", IEEE Technology and Society Magazine, 2011., 28.-38. str.

koje poslovanje, zaposlenici i korisnici doživljavaju. Uz njih dolaze informacijski gubitci, tehnološke posljedice, ali i psihološke posljedice. Informacijske štete se odnose na štete od izmijenjenih, dodanih, izbrisanih ili ukradenih podataka. Ukradeni podaci ne moraju biti samo o poslovanju, već mogu biti i krađe osobnih podataka zaposlenika i korisnika. To dovodi i do tehnoloških posljedica. Nastaje sumnja i nestaje povjerenje u dotad osmišljenu zaštitu. Nastaje sumnja općenito u tehnologiju, zbog rizika koji predstavlja. I sve to ostavlja psihološke posljedice na pojedince. Ovom posljedicom ne moraju svi biti obuhvaćeni, ali oni koji jesu, mogu postat strahovati od najobičnijeg promidžbenog e-maila. Neki će čak zahtijevati odštetu i/ili osiguranje da se to više neće ponoviti. U svakom slučaju, nakon kibernetičkog napada organizacija, poslovanje, zaposlenici i korisnici snose svih 5 posljedica. Jedna utječe na drugu i nemoguće je da poduzeće osjeti samo jednu od njih.

Nakon što je određena organizacija postala žrtva kibernetičkog napada, osim prethodno navedenih 5 posljedica, postoji još jedna moguća posljedica, a to je gubitak korisnika. Nakon napada, korisnici počinju sumnjati u tehnologiju, počinju gubiti povjerenje i nastaje panika što će se dogoditi s ukradenim podacima, te se boje ponovnog napada. Razumljivo je da će napad povezivat s uslugom, proizvodom, softverom ili aplikacijom preko koje su postali žrtva napada. S tim gube povjerenje u organizaciju koja im je pružila tu uslugu, proizvod, softver ili aplikaciju, nakon čega korisnici napuštaju tu organizaciju u nadi da više neće biti izloženi opasnosti. Ako organizacija gubi korisnike, to znači da gubi profit, što je u konačnici može gurnuti preko ruba. Organizacija koja i sama žrtva zlonamjernog napada, postaje neprijatelj u očima svojih korisnika. Pri tome organizacija može pretrpjeti ne popravljivu štetu o svojoj reputaciji, koja će ostavi dugotrajne posljedice. Neke se možda neće ni oporaviti nakon toga.

Nepošteno je kategorizirati i reći da su Zero day napadi usmjereni k jednom tipu žrtve. Žrtvom postaju oni koji se nađu na meti napadača. Ono što napadačima daje priliku za napad je greška koja predstavlja Zero day ranjivost za poslovanje. Ali, nije pitanje hoće li napadači dobiti ranjivost koju mogu iskoristiti, nego kada će je dobiti. Trenutno nitko nije u potpunosti zaštićen i siguran od kibernetičkih napada, ali moguće je smanjiti rizik. Potrebno je prihvatiti da postoji opasnost i potruditi se razumjeti važnost kibernetičke sigurnosti. Prihvatiti da odgovornost nije samo na organizacijama, već pada i na pojedince. Osim njih, država i državne organizacije bi također trebale intenzivno raditi na suzbijanju kibernetičkog kriminala. Onima koji su postali žrtvama, potrebno je pružiti dodatnu edukaciju, ali i pomoć u prevladavanju posljedica napada. A te iste žrtve bi trebale pružiti informacije o napadu, jer kada bi svi bili transparentni, možda bi se već našao ključ u suzbijanju bar nekih napada.

3.3. Otkrivanje ranjivosti

Bez Zero day ranjivosti ne postoji Zero day napad. Do sad je ranjivost prikazana vrlo jednostavno, radi lakšeg razumijevanja ostalih poglavlja. No, u Zero day napadu one predstavljaju osnovu za napad. Kao što se prethodno spominjalo, teško je odrediti tko je i kada saznao za Zero day ranjivost ili je li javno objavljena ili ne. U nastavku slijedi objašnjenje Zero day ranjivosti, kako se one otkrivaju i kako točno do njih napadači mogu doći.

3.3.1. Zero day ranjivosti

Ranjivost predstavlja određenu slabost ili pogrešku. Svaka pogreška ne predstavlja ujedeno i ranjivost. Već se spominjalo da su okolnosti povezane s otkrivanjem Zero day ranjivosti ne jasne. No, to će se sada promijeniti. Kako bismo razumjeli različite situacije iskorištavanja Zero day ranjivosti, proći će se kroz njihovu jednostavnu podjelu. Za početak je bitno istaknuti ono što je sigurno. To je činjenica da Zero day ranjivosti su one ranjivosti koje nisu još ispravljene, te da se ranjivosti koje su popravljene više ne smatraju ranjivostima. I prema tome jesu li Zero day ranjivosti poznate javnosti? Može ih se podijeliti na privatne i javne ranjivosti.

Slika 2 Kategorizacija ranjivosti[30]

[30] Ablon, L., Bogart, A.: Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, RAND Corporation, Santa Monica, CA, 2017.

Kao što je prikazano na slici 2, javne ranjivosti se mogu podijeliti na ispravljene, djelomično ispravljene i neispravljene, a privatne ranjivosti se dijele na one koje su poznate jednoj osobi ili organizaciji, koje su poznat dvije ili više osoba ili organizacija bez da je javnost upoznata, na one koje žele podijeliti s javnost te na one koje su ispravljene bez da su o njima obavijestili javnost. Pri tome, javnost bi bili svi ljudi koje zanima, ali i koje ne zanima što se događa s nekom organizacijom. Može se zaključiti da su javne ranjivosti zapravo prikaz onoga što se smatra dovoljnim za predstaviti javnosti. Kao da javnost ne zanima tko je kada znao za određenu ranjivost, već samo je li ta ranjivost ispravljena ili nije. To jest je li određena greška više ne predstavlja ranjivost ili još uvijek je. Dok su u privatnoj kategorizaciji ranjivosti predstavljene kao moguće situacije o tome tko je i kada znao za određenu ranjivost. Moglo bi se reći da je privatna kategorizacija ranjivosti relevantnija za kategorizaciju Zero day ranjivosti.

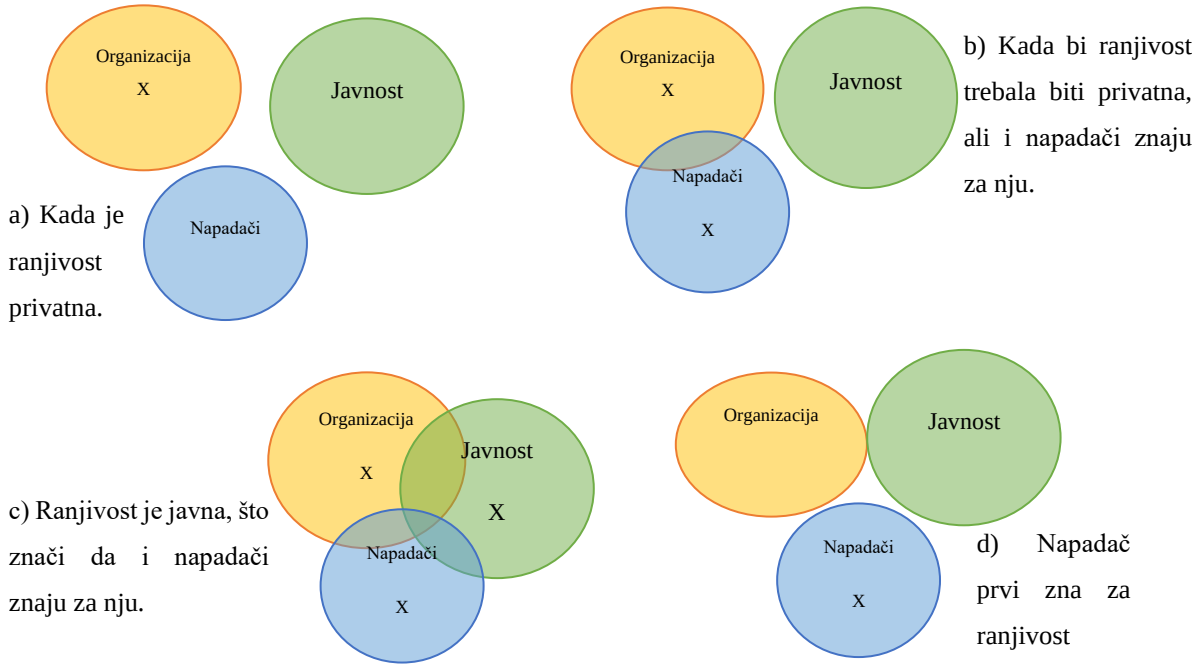
Nadalje, prethodno se spomenulo da nisu sve pogreške ujedno i ranjivosti. Određena pogreška, koja trenutno ne predstavlja ranjivost za poslovanje, ne znači da nikad neće. Je li neka pogreška ranjivost ili nije ovisi o okolnostima. Je li organizacija nekome na meti? Je li ih ta greška može dovesti do cilja? Je li se u tom trenutku ta greška uopće može iskoristiti? O tim, i mnogim drugim čimbenicima ovisi hoće li se određena pogreška ujedeno biti i ranjivosti. „Neprestano se razvijaju nove metode i tehnike pristupa koje dopuštaju korištenje prethodno neiskorištenih ranjivosti, a na sličan način uvode se ublažavanja koja sprječavaju daljnju uporabu trenutno iskoristivih ranjivosti.“[31] Ukratko, kao što određena pogreška može u nekom budućem trenutku postati ranjivost, isto tako ranjivost može isteći. Pod tim se misli da određena pogreška koja je predstavljala Zero day ranjivost za organizaciju, pri promjeni okolnosti, više nije iskoristiva za napad i ponovno postaje samo greška koju je potrebno ispraviti. Ono što je također zanimljivo je da napadači znaju čekati i iščekivati da određena greška postane ranjivost, ali to ne dočekaju. Zato jer organizacija ispravi pogrešku prije nego do toga dođe.

Kategorije Zero day ranjivosti također nisu statične, već s vremenom prelaze u neku drugih kategorija. Na početku možda za nju zna samo jedna osoba, pa dvije, pa više njih, pa organizacija saznaje za situaciju, pa druga organizacija i tako dalje. Ali te kategorizacije nije uvijek jednostavno odrediti. Ponekad nije jasno koliko osoba ili organizacija je upoznato s problemom, pa niti kada je točno javnost doznala za ranjivost.

[31] Ablon, L., Bogart, A.: Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, RAND Corporation, Santa Monica, CA, 2017.

Ali to nije sve, u slučaju kada se sazna za ranjivost, bitno je postaviti pitanje je li netko drugi također mogao doći do nje, je li moguće da ih netko napadne putem te ranjivosti? U stvarnom svijetu, netko je mogao namjerno ili nenamjerno procuriti informaciju o ranjivosti. To i dalje ne znači da je javno objavljena i da je cijela javnost upoznata s njom, već da je proširena osobama ili skupini koji će od nje imati koristi. Stoga, ako napravimo jednostavnu podjelu na organizaciju, javnost i napadače, možemo dobiti jasniju sliku o procesu ranjivosti. Bilo koja kategorija u kojoj ranjivost nije ispravljena, može se smatrati Zero day ranjivosti, te se upravo na njih odnosi iduća slika 3.

Slika 3 Tko je upoznat s ranjivosti?



a) Kada je ranjivost privatna.

b) Kada bi ranjivost trebala biti privatna, ali i napadači znaju za nju.

c) Ranjivost je javna, što znači da i napadači znaju za nju.

d) Napadač prvi zna za ranjivost

Na slici 3 su prikazane tri moguće situacije:

- Situacija A: Najpovoljnija za pojedinca ili organizaciju koji su odgovorni za određenu ranjivost. Nitko osim njih još ne zna za ranjivost.
- Situacija B: Osim pojedinca ili organizacije i napadači znaju za ranjivost. Organizacija treba brzo reagirati kako bi ispravila pogrešku.
- Situacija C: Svi su upoznati s postojećom ranjivosti. Osim što organizacija treba brzo reagirati kako bi se zaštitila od napada, ali i kako bi smirila korisnike.
- Situacija D: Najnepovoljnija situacija za organizaciju. Napadač je upoznat s ranjivosti i prije nego što organizacija zna za nju.

3.3.2. Otkrivanje ranjivosti

„Softverske ranjivosti osnovni su uzrok mnogih sigurnosnih proboja, pa je razumijevanje softverskih sustava bitno za razvoj modela koji analizira kako i kada uložiti napor u osiguravanje softvera.“[32] Postoje različiti načini pronalaska određene pogreške i potencijalne ranjivosti. Određene greške se mogu uočiti pri izradi kôda, određene testiranjem aplikacije i daljnjim korištenjem, ali sve one koje se ne pronađu tako, pokušavaju se naći različitim algoritmima i softverima za otkrivanje ranjivosti. Ti algoritmi i softveri su namijenjeni za otkrivanje točno definiranih ranjivosti i potrebno ih je koristiti više od jednom kako bi se dobili što bolji rezultati.

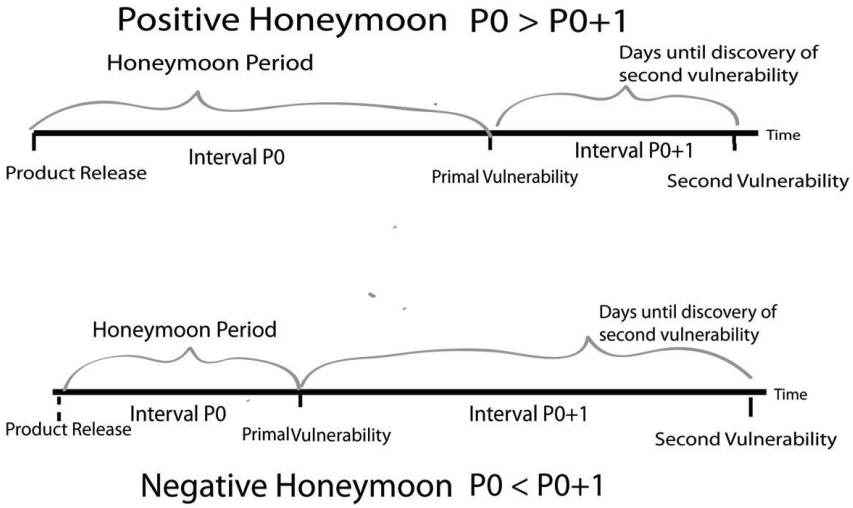
A kako funkcionira otkrivanje ranjivosti? Podrazumijeva se da organizacija čiji je softver, detaljno pregleda i provjeri program da li ima grešaka. To je normalna procedura, da se prije izbacivanja softvera obavi provjera i isprave pronađene pogreške, kako bi do korisnika došao što sigurniji program. Al kao što se već prethodno spominjalo, otprilike 15 'bugova' i dalje dođe do korisnika. Toga su svjesne i organizacije i programeri te očekuju da će u početcima korištenja softvera korisnici javljati da imaju određene probleme, a oni će biti spremni da brzo reagiraju i isprave ih. Možemo reći da je to planirano i kontrolirano izlaganje ranjivosti javnosti. No osim njih, napadači također traže greške kako bi pronašli određenu ranjivost prije nego ona bude ispravljena.

I organizaciji i napadačima je u cilju da oni prvi saznaju za pogrešku koja je potencijalna ranjivost za softver. Osim toga, sjećamo se da određena Zero day ranjivost ne mora zauvijek biti ranjivost. Ona s vremenom može postati ne iskoristiva i biti obična greška u sustavu. To možemo nazvati vremenskim vijekom ranjivosti, a predstavlja broj dana od kada se saznalo za ranjivost, pa dok se nije zakrpala ili jednostavno izgubila svoju vrijednost.[33] To znači da brzina igra bitnu ulogu pri otkrivanju ranjivosti. Ali, i u slučaju kada napadač prvi dođe do ranjivosti, rizik od napada je izuzetno visok, i dalje postoji mogućnost da organizacija ispravi pogrešku prije nego napadač uspije iskoristiti nađenu ranjivost. Također, kako vrijeme prolazi i ranjivosti se otkrivaju i ispravljaju, tako se rizik od napada sve više smanjuje, a određeni program postaje sve sigurniji za korištenje.

[32] Clark, S., Frei, S., Blaze, M., Smith, J.: “The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities”, Familiarity breeds contempt, Austin, Texas, 2010.
[33] Akram, J., Ping, L.: “How to build a vulnerability benchmark to overcome cyber security attacks”, The Institution of Engineering and Technology, Key Laboratory of Information System Security, School of Software, Tsinghua University China, Beijing, People's Republic of China, 2019.

Prema dosad navedenom, može se zaključiti da bi Zero day ranjivosti trebale biti otkrivene isti dan kada je određen softver stavljen u funkciju. Određena istraživanja pokazuju drugačije. Naime, vrijeme za otkrivanje prve ranjivosti, ali i vrijeme dok se otkriju druge ranjivosti je uglavnom duže od jednog dana i može varirati. Vrijeme koje je potrebno za otkrivanje ranjivosti može se promatrati i kao efekt medenog mjeseca (eng. honeymoon effect). Kao što se već navelo, i za organizaciju i za napadače je bitno da oni budu prvi koji će otkriti određenu ranjivost. Ako uzmemo u obzir da se neke jednostavne ranjivosti brzo nalaze, ali i da ih je više te da se radi većom brzinom, može se zaključiti da će se prva ranjivost naći najbrže, a svaka iduća sve sporije i sporije. Ali postoji mogućnost da se dogodi i suprotno. Prema tome se razlikuje negativni efekt medenog mjeseca i pozitivni efekt medenog mjeseca.[34] Ako se vrijeme otkrivanja ranjivosti s vremenom povećava, onda je to negativni efekt medenog mjeseca. Ako se vrijeme otkrivanja ranjivosti smanjuje s vremenom, onda je to pozitivni efekt medenog mjeseca. Efekt medenog mjeseca zapravo predstavlja razdoblje kada je softver pušten na korištenje, pri čemu se vjeruje da je rizik za napad nizak, pa do trenutka kad se otkrije prva Zero day ranjivost.[35] Ono predstavlja razdoblje stabilnosti dok još nije otkrivena nova ranjivost.

Slika 4 Vremenske linije pozitivnog i negativnog efekta medenog mjeseca

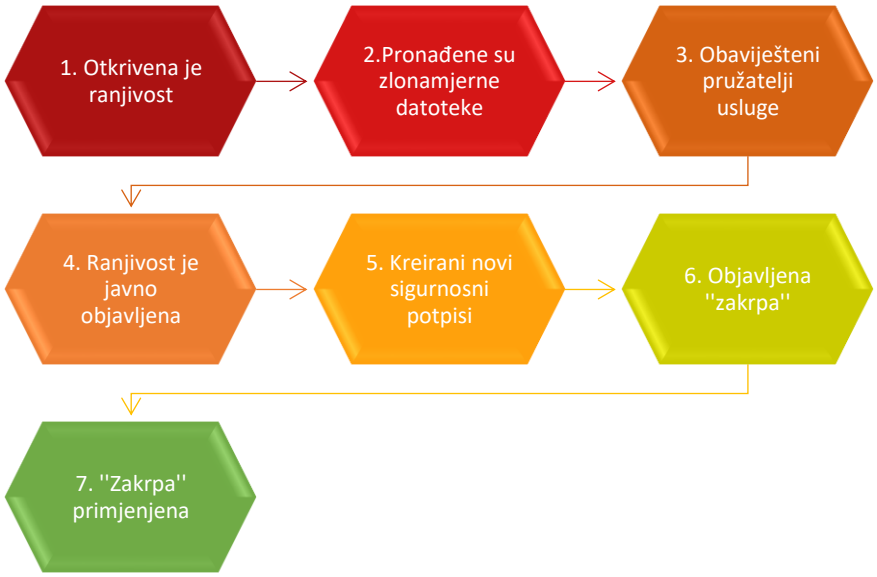


Izvor: Clark, S., Frei, S., Blaze, M., Smith, J.: "The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities", Familiarity breeds contempt, Austin, Texas, 2010.

[34] Clark, S., Frei, S., Blaze, M., Smith, J.: "The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities", Familiarity breeds contempt, Austin, Texas, 2010.
[35] Clark, S., Frei, S., Blaze, M., Smith, J.: "The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities", Familiarity breeds contempt, Austin, Texas, 2010.

Nakon što se otkrije određena ranjivost, postoji određeni proces saniranja te ranjivosti, prije nego što je netko iskoristi. Prvo je potrebno da organizacija i napadač otkriju određenu ranjivost. Potom se pretpostavlja da su napadači već pokušali iskoristi tu ranjivost za napad, te neka od takozvanih sigurnosnih skupina pronalazi zlonamjerne datoteke. One ne moraju nužno biti aktivne, postoji mogućnost da su samo implementirane i da pravi napad još nije krenuo. U trećoj fazi se obavještava pružatelja usluge o trenutačnoj situaciji. Na temelju toga pružatelj usluge odlučuje obavijestiti javnost da postoji ranjivost i određeni rizik od napada. Nakon toga je potrebno kreirati nove sigurnosne potpise. U predzadnjem koraku se izdaje "zakrpa" koja će u potpunosti ispraviti nastalu pogrešku i time zaštiti softver i korisnike. Sve što je preostalo da svi korisnici implementiraju zakrpu kako bi bili sigurno zaštićeni. Na slici 5 slijedi jednostavni prikaz životnog ciklusa Zero day ranjivosti.

Slika 5 Životni ciklus saniranja Zero day ranjivosti[36]



„Nakon što sigurnosna skupina pronađe i istraži ranjivost, detalji o ranjivosti distribuiraju se u javnoj obavijesti, a dobavljač softvera ili hardvera koji je pogođen može izdati zakrpu kako bi zajedno riješili problem.“[37]

[36] Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H.: “A hybrid layered architecture for detection and analysis of network based Zero-day attack”, Computer Communications, 2017.
[37] Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H.: “A hybrid layered architecture for detection and analysis of network based Zero-day attack”, Computer Communications, 2017.

3.3.3. Tržište ranjivostima

Upotreba interneta i načina na koji se može iskoristi rastu iz dana u dan. Od pronalaženja običnih informacija, do kupovine proizvoda ili usluga u zemlji ili na nekom drugom kraju svijeta, do vođenja poslovanja i sastanka uz pomoć Internet platformi. Može se reći da danas sve može naći i obaviti iz udobnosti svoga doma, sa svog računala putem Interneta. Kako se može iskoristi u dobre svrhe, tako može i u loše.

Istim procesom kojim se kupuje neki predmet preko Interneta, se danas može kupiti i Zero day ranjivost. Ovisno o tržištu postoje različite razine sigurnost pri takvoj kupnji. Što se tiče samih tržišta, ista su kao i svaka druga. Sastoje se od ponude i potražnje, a cijena se prilagođava njihovom odnosu. Tržišta na kojim se trguje s ranjivostima su: bijelo tržište (eng. White market), sivo tržište (eng. Grey market) i crno tržište (eng. Black market).

Bijelo tržište je u potpunosti legalno tržište. Ono se ne sastoji od velike količine ponuđača i potraživača usluga na jednom mjestu, već se sastoji od manjih ciljanih dogovora i transakcija. Sastoji se od pružatelja usluga i trećih strana koje nude svoje usluge traženja ranjivosti. Postoje 3 opcije trgovanja na bijelom tržištu ranjivosti:[38]

- Istraživači besplatno ponude pronađene ranjivosti pružateljima usluga .
- Organizacije samostalno organiziraju program traženja ranjivosti putem kojeg nude nagrade, to jest isplaćuju nagrade za pronađene ranjivosti.
- Organizacije putem platformi kao što je Hacker One, plate takoreći dobronamjerne hakere koji su odlučili prodat pronađenu ranjivost samim organizacijama, a ne nekom tko bi je mogao iskoristiti za napad.

Na bijelom tržištu raste ponuda istražitelja, platformi i hakera koji su putem njega odlučili prodati pronađene ranjivosti. U isto vrijeme, zbog povećanja svijesti o kibernetičkoj sigurnosti, raste i potražnja za tim ranjivostima kako bi se zakrpale prije nego ih netko drugi odluči iskoristiti. To je dovelo i do toga da prosječna cijena ranjivosti od 500 USD u 2016., poraste na prosječnu cijenu ranjivosti od 600 USD u 2018. godini.[39] Jedna zanimljivost o motivaciji ponuđača pronađenih ranjivosti na bijelom tržištu je ta da je glavni razlog učenje novih tehnika i trikova te vježba, a ne novac. To u isto vrijeme ne znači da to neki ne rade i zbog novca ili samo zbog novca, ali ono ipak ne za uzima prvo mjesto u motivaciji.

[38] Meakins, J.: "A zero-sum game: the zero-day market in 2018", Journal of Cyber Policy, 2018.
[39] Meakins, J.: "A zero-sum game: the zero-day market in 2018", Journal of Cyber Policy, 2018.

Sivo tržište, kao što naziv odaje, etički gledano nalazi se između bijelog i crnog tržišta. Razvilo se iz crnog tržišta i namijenjeno je isključivo za kupoprodaju ranjivosti. Ono se također smatra legalnim tržištem, ali tu se ranjivosti ne prodaju samo organizacijama čije te ranjivosti jesu, već bilo kome tko je zainteresiran za kupnju ili tko je spreman ponuditi više. Pa zašto se nalaze između ta dva tržišta? Tehnički gledano kupoprodaja ranjivosti, ponekad i njihovih zakrpi, je legalna. Smatra se ispravnom i legalnom razmjenom informacija za novac. Problem leži u tome što na ovom tržištu nije bitno tko ni iz kojih razloga kupuje neku ranjivost. Pa tako i dalje postoji mogućnost iskorištavanja ranjivosti u zlonamjerne svrhe ili kao određenu stratešku prednost. Zanimljivo je da države, vlade ili državne agencije spadaju pod jedne od učestalijih kupaca na ovom tržištu. Smatra se da one kupuju ranjivosti kako ne bi došle u krive ruke, ali iza toga stoji i želja za strateškom prednosti naspram drugih. Tako se sivo tržište nalazi na granici legalnog i ilegalnog postupanja.

Crno tržište je ilegalno tržište. To je virtualno ili digitalno tržište, što znači da nema geografsku lokaciju i da su njegovi sudionici rasprostranjeni po cijelom svijetu. U svrhu kibernetičke sigurnosti se traže i zatvaraju osobe koje pružaju uslugu crnog tržišta kako bi ugasili crna tržišta. Kako se jedno crno tržište zatvori, vrlo brzo se otvori novo. Koliko vremena je u prosjeku potrebno da se ugasi određeno tržište nije poznato, ali može se pretpostaviti da su potrebni brojni ljudski i novčani resursi te dosta vremena. Postoje lakše dostupna i teže dostupna crna tržišta. Radi pojačane kibernetičke sigurnosti i sve većih napora da se zatvore takva tržišta, ona postaju sve restriktivnija i prihvaćaju ili pozivaju samo određene osobe. Na crnom tržištu se trguje s različitim ilegalnim stvarima, a ne samo ranjivostima. Sudionici crnog tržišta su pojedinci, manje ili veće grupe, organizacije, grupe organiziranog kriminala, kibernetički teroristi, pa i hakeri aktivisti. Zašto su crna tržišta popularna kod te vrste ljudi? Osim što vjerojatno mogu pronaći što god da traže, uz to imaju osiguranu tajnost i dobar profit. Ako je moguće pronaći bilo što, onda je moguće pronaći i Zero day ranjivosti. Na crnom tržištu se ne prodaju bilo koje i bilo čije Zero day ranjivosti. Na njemu se prodaju teško dostupne ranjivosti, jer se smatraju izuzetno rijetkima i vrijednima. „Ono što je još više zastupljeno na crnom tržištu su "half-days" (ili, kako ih jedan stručnjak naziva, "1-days" ili "2-days"), pri čemu bi kreator softvera mogao znati za ranjivost, a zakrpa bi mogla biti dostupna, ali je malo korisnika svjesno i primjenjuje te zakrpe.“[40] Half-days ili poludnevne ranjivosti se smatraju vrijednima u slučajevima kada je šansa za pronalazak Zero day ranjivosti izuzetno niska.

[40] Ablon, L., Libicki, M.C., Golay, A.A.: Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, RAND Corporation, Santa Monica, CA, 2014.

Popularnost sivih i crnih tržišta Zero day ranjivosti raste. U isto vrijeme je porasla svijest o Zero day napadima. „Ljudi postaju tehnički sofisticiraniji; mlađe generacije svakodnevno koriste tehnologiju u školi, uče o digitalnoj tehnologiji u vrlo ranoj dobi. Prema riječima jednog stručnjaka, "hakiranje je postalo mala liga: svi počinju rano i provode puno vremena radeći na tome." “[41] Tako da popularnost potražnje na tržištu ne znači ujedno dolazi do porasta ponude ranjivosti. Ali to zasigurno neće dugo potrajati, zato jer će hakeri tražiti nove načine kako da otkriju i dođu do novih vrijednih Zero day ranjivosti.

Jedno istraživanje je usporedilo odnos programa za nagrađivanje traženja ranjivosti i Zero day tržište. Moglo bi se reći ujedno i odnos bijelog i sivog tržišta. Navedeni su razlozi zašto su ti načini plaćanja ranjivosti pozitivni, a zašto negativni. Neki od pozitivnih razloga su zato što pomažu organizacijama pronaći greške na softverima, pomažu utjecati na cijene ranjivosti i više ljudi istovremeno iz dobre namjere traži ranjivosti. Neke od negativnih bi bile što su te opcije možda moguće samo za velike organizacije kao Google ili Apple, postoji mogućnost zlonamjernog korištenja ranjivosti, ne smatra se ekonomičnim i stvara kobra efekt (eng. Cobra effect).[42] Kobra efekt znači da plaćanje nekoga da pronađe ranjivost bi moglo dovesti do tajnog podmetanja ranjivosti kako bi kasnije bili nagrađeni za njen pronalazak. Takvo je istraživanje pokazalo da zapravo ni jedan način trgovanja ranjivostima nije savršen te da oba nose određene posljedice. Usprkos tome, programi za nagrađivanje traženja ranjivosti (greške) dobivaju popularnost u komercijalnom svijetu, zajedno s interesom za srodna tržišta Zero day ranjivosti.[43]

[41] Ablon, L., Libicki, M.C., Golay, A.A.: Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, RAND Corporation, Santa Monica, CA, 2014.
[42] Egelman, S., Herley, C., van Oorschot, P.C.: "Markets for Zero-Day Exploits: Ethics and Implications", NSPW '13: Proceedings of the 2013 New Security Paradigms Workshop, 2013., 41–46.str.
[43] Egelman, S., Herley, C., van Oorschot, P.C.: "Markets for Zero-Day Exploits: Ethics and Implications", NSPW '13: Proceedings of the 2013 New Security Paradigms Workshop, 2013., 41–46.str.

4. OBRADA ZERO DAY PRIMJERA

U prethodnom poglavlju je objašnjen pojam Zero day napada. Prikazana je njegova kompleksnost te značaj tehničkih i financijskih resursa koji se nalaza iza njegove provedbe, ali i njegovog otkrivanja. Nekada je za bolje razumijevanje nekog pojma najbolje promotriti primjere istog. Stoga se su u ovom poglavlju prikazani neki od Zero day napada.

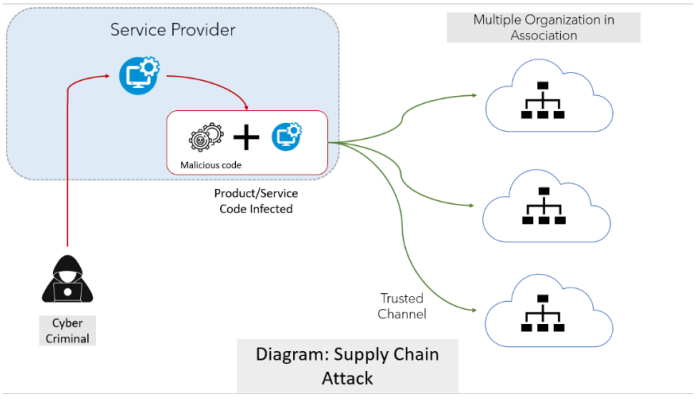
4.1. Napad lancem nabave na Solar Winds

Solar Winds je američka organizacija koja se bavi razvojem softvera. Prvenstveno se bavi alatima za upravljanje sustavima, mrežama i IT infrastrukturom. Te softvere uglavnom koriste IT stručnjaci, a jedan od njihovih najpopularnijih proizvoda je Orion. Orion je softver koji koristi preko 30 000 korisnika, u to spadaju privatne organizacije, ali i državne agencije.

Pa što je to Orion? To je sustav za upravljanje mrežom (NMS). S obzirom da je to sustav kojim se upravlja mrežom ima komunikaciju sa svim uređajima kojima upravlja. NMS samostalno može unositi određene promjene, kao što je promjena nekih funkcija ili pristupa. Čak kada to nije moguće, te sustav vrši samo nadzor mreže, napadači i dalje mogu pristupiti i vidjeti podatke i informacije iako ne mogu napraviti izmjene. Takvi sustavi su zbog svojih karakteristika i mogućnosti jedna od češćih meta napadača.

Napad je izveden u tajnosti, a način na koji je proveden se zove napad lanca nabave (eng. supply chain attack). Proveden je tako da je zlonamjerni softver, to jest zlonamjerni dio kôda, ubačen kao dio ažuriranja sustava Orion. Čak je bio potpisan važećim digitalnim certifikatom na ime Solar Winds-a. Sumnjalo se da je možda i digitalni certifikat bio ugrožen, ali ispostavilo se da je u potpunosti ispravan i da su ga napadači samo iskoristili u provedbi svog napada.

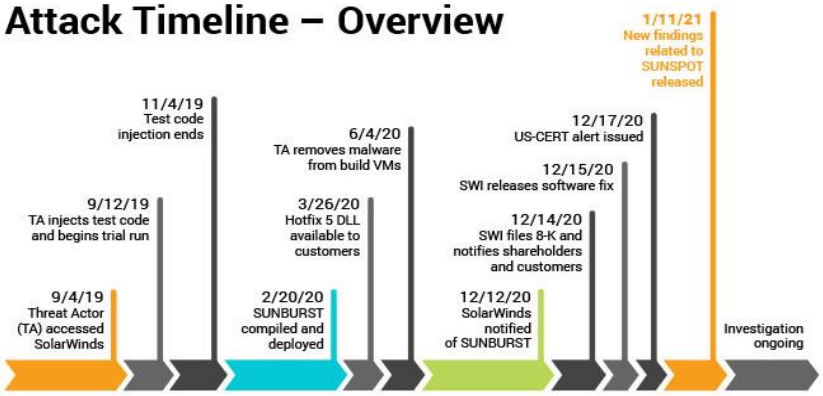
Slika 6 Prikaz napada lanca nabave (eng. supply chain attack)



Izvor: Dubey, S.: „SUNBURST: A Vital Case Study of Supply Chain Attack“, PureID, 2020., https://www.pureid.io/sunburst-a-vital-case-study-of-supply-chain-attack/

Iako je FireEye otkrio napad u prosincu 2020.godine, prema dosadašnjim otkrićima, smatra se da je napad počeo još u rujnu 2019. godine. Tada su napadači neovlašteno pristupili Solar Winds mreži i tako si stvorili put za napad. U listopadu 2019. su u Orion sustav ubacili testni kôd kako bi vidjeli kolike su im šanse za uspjeh. Kada im je to uspjelo, pripremili su pravi napad i 20. veljače 2020. godine implementirali zlonamjerni kôd u ažuriranje sustava Orion. S obzirom da je sve provedeno neprimijećeno, 26. ožujka 2020. godine Solar Winds je izdao zaraženo ažuriranje svojim korisnicima. Što znači da je cjelokupni napad trajao duže od godinu dana, a izloženost korisnika oko 9 mjeseci. Prema podacima koji su trenutno dostupni smatra se da je otprilike 18 000 korisnika preuzelo zaraženo ažuriranje i time izložilo svoje poslovanje napadačima.

Slika 7 Vremenski prikaz Sunburst napada



Izvor: Ramakrishna, S.: „New Findings From Our Investigation of SUNBURST“, Orange Matter, 2021., https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/

U ovom napadu su Solar Winds i njihov softver Orion bili iskorišteni kako bi se pristupilo osjetljivim podacima njihovih korisnika, ali i trećih osoba, to jest klijenata organizacija koje koriste Orion u svojem poslovanju. S obzirom na spektar funkcija Oriona i podataka kojima raspolaže, napadači su mogli pristupiti svim evidencijama, čak i određenim nedostacima korisnika Oriona, što se smatra da im je bilo putokaz u tome koje organizacije će biti lakše, a koje teže za zaraziti. Žrtve napada su bile privatne organizacije kao što su Microsoft, Cisco, Intel i Deloitte, ali i državne agencije kao što su Pentagon, odjel domovinske sigurnosti (eng. the Department of Homeland Security), odjel za energiju (eng. the Department of Energy) te druge organizacije kao što su bolnice i fakulteti. Broj od 18 000 napadnutih korisnika je samo procjena jer se za dio organizacija još i ne zna jesu li bile izložene napadu, a neki to neće ni priznati.

Kao što se već spomenulo, organizacija FireEye koja je koristila Orion u svom poslovanju u prosincu 2020. godine je prva otkrila napad. Prema izdanim informacijama postoje različita nagađanja tko je krivac. Na početku se sumnjalo da se Rusija nalazi iza ovog napada, točnije skupina SVR, zbog određenih sličnosti s njihovim dotadašnjim napadima. To je zaključila i državna sigurnost, ali i FireEye organizacija. Nakon toga je Microsoft ponudio drugu mogućnost, koja se za sada smatra ispravnom. Prema njihovim istraživanjima zaključili su da iza napada zapravo leži američka grupa pod nazivom Nobelium. Osim toga, postojale su i špekulacije da je možda Kina nekako povezana s ovim napadom, ali prema sadašnjim informacijama, sve su to još samo pretpostavke i ne zna se tko točno stoji iza napada. Iako postoje nagađanja tko je proveo napad, još se uvijek ne zna koji je cilj ili motiv napada bio.

Napad lancem nabave na Solar Winds ili napad Sunburst smatra se jednim od najvećih napada koji se za sad dogodio u ovom stoljeću. Ne samo da je napad na jedno od velikih organizacija ili jedan bitnih softvera koji sadrži osjetljive informacije korisnika, nego i zbog svoje ne opaženosti i prouzrokovanih posljedica i troška. Zaključeno je da je napad bio podijeljen na dva dijela, na početnu fazu koju su odvojili od faze napada u tijeku, kako bi smanjili mogućnost detekcije napada, što pokazuje sofisticiranost napadača. Zahvatio je brojne osjetljive organizacije koje raspolažu s vrlo osjetljivim podacima. Vjeruje se da će oporavak mreža zahvaćenih napadom trajati godinama, ali i nositi visoke financijske troškove. Za sad su poznati samo određeni troškovi Solar Winds-a. Iz Solar Winds-a su iznijeli da su na istraživanje i rješavanje napada već potrošili oko 19 milijuna USD. Uz to su im pale vrijednosti dionica što se pretpostavlja da će rezultirati gubitcima od nekih 17 milijuna dolara. Samo financijski troškovi ukazuju na razmjer posljedica ovog napada, a pri tome se ne smiju zaboraviti informacijske, tehnološke, ali i psihičke posljedice svih žrtava. Je li se nekim podacima manipuliralo ili koji su ukradeni nije poznato, ali može se pretpostaviti da je to bio jedan od ciljeva napada. To je sve dovelo do sumnje i nepovjerenja u Solar Winds i proizvode koje oni nude. Što znači da su sve žrtve pretrpjele više različitih posljedica ovog napada

Sunburst nije još službeno potvrđen kao Zero day napad. Kada je napad bio otkriven, vjerovalo se da je napad na Solar Winds bio Zero day napad, ali poslije toga su se počela postavljati pitanje je li to uistinu bio Zero day napad ili ne, a na njih još nitko nije izdao konkretan odgovor. Ali s obzirom da je napad obavljen ne primijećeno, kad Solar Winds nije bio svjestan prijetnje, može se pretpostaviti da je to uistinu bio Zero day napad.

4.2. Microsoft Exchange kibernetički napad

Microsoft je jedna od najvećih američkih multinacionalnih tehnoloških kompanija koja je osnovana još 1970-ih godina. Trenutno, u 2021. godini, prema prihodima je najveći proizvođač softvera. Imaju mnoge proizvode koji se svakodnevno koriste širom svijeta, kao što je Microsoft Windows, Microsoft Office, Visual Studio, LinkedIn, Outlook i mnogi drugi. Razvijaju različite proizvode, na primjer softvere, programe, igrice, operativne sustave i slično.

Jedan od njihovih popularnih proizvoda je Microsoft Exchange Server. To je server/poslužitelj pošte i kalendara. Točnije, to je platforma preko koje korisnik može pristupiti elektroničkoj pošti, kalendaru, kontaktima te praviti i organizirati raspored obaveza. Prva verzija je napravljena kao nasljednica na Microsoft Mail 3.5. te se iz tog razloga zvala Exchange Server 4.0. Od 1990-ih do danas je napravljeno je i izdano nekoliko unaprijeđenih verzija, a zadnja je bila Exchange Server 2019., koja se trenutno i koristi. Poslužitelj pošte kao što je Exchange server je neodoljiva meta napadača, zato što im omogućuje pristup povjerljivim tajnama poduzeća i korporativnim podacima.

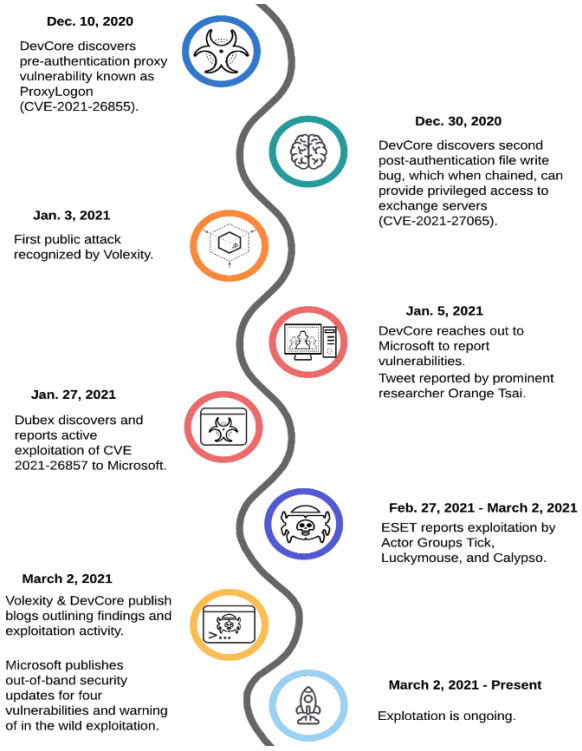
Smatra se da su ranjivosti zapravo nastale još 2013. godine, pri doradi verzije Exchange Server 2013. Tada su pri pokušaju unaprjeđenja servera i dizajna, CAS ili Client Access Service podijelili na sučelje i pozadinu. Pri tome je očigledno došlo do određenih grešaka pri izradi, jer se s tim stvorilo i 8 novih ranjivosti, bar ih je toliko trenutno poznato. Što znači da već skoro 10 godina postoje opasne Zero day ranjivosti koje su se prenosila s jedne verzije Exchange Servera na drugu. U ovom napadu je iskorištena kombinacija tih ranjivosti koje su bile kao lanac napada (eng. attack chain).

Hakeri su ranjivosti iskoristili kako bi na Microsoft Exchange serveru ugrozili pristup Outlook-u, u svrhu pristupanja serverima i mrežama korisnika Exchange servera. Potom slijedi zahtjev za adresu servera kako bi se ostvario pristup jednom ili više njih. Putem jedne od ranjivosti se povezuje s tim serverima i lažno potvrđuje autentičnost pristupa. Preko druge mijenja svoje ovlasti u tom serveru kako bi bili u mogućnosti pristupiti svim željenim informacijama, ali i manipulirati njima ako je potrebno. Druge dvije ranjivosti su korištene kako bi si osigurali pristup na poslužitelja s bilo kojeg mjesta u bilo koje vrijeme. Tako su stvorili 'web shell'. Takozvani stražnji ulaz koji im omogućuje kontinuiran i skriveni pristup serverima.

Početkom 2021. godine došlo je do napada na Exchange Server. Krajem prosinca 2020. i početkom 2021. godine, mala organizacija DevCore, koja je specijalizirana za otkrivanje nedostataka, to jest ranjivosti, otkrila je i prijavila Microsoft-u pronađene ranjivosti vezane uz

Exchange Server. Microsoft je i sam pronašao više Zero day ranjivosti i počeo raditi na potrebnoj zakrpi, koju je izdao početkom ožujka iste godine. Iz agencije za kibernetičku i infrastrukturnu sigurnost ili CIAS (eng. Cybersecurity and Infrastructure Security Agency) naglasili su da zakrpa vjerojatno nije dovoljna ako je određeni server već napadnut. Izjavili su da korisnici osim instaliranja zakrpe, trebaju provesti i druge mjere kako bi se uvjerili da nisu već napadnuti ili se pak obranili od napada u tijeku, oko čega se složio i Microsoft i objavio slične preporuke svojim korisnicima. No, tu nije kraj, nažalost tada još nisu bili upoznati sa svim ranjivostima, pa su tako ostale i dalje bile zloupotrebljavane. Nastavno na to, početkom travnja 202. godine se izdaju još 4 zakrpe za 4 novootkrivene ranjivosti. Koliko je poznato, još uvijek nisu svi korisnici softvera instalirali zakrpe kako bi se zaštitili od mogućih napada, što ostavlja prostora za daljnje iskorištavanje ranjivosti. Osim toga, još se istražuju moguće štete, žrtve te daljnje mogućnosti napada.

Slika 8 Vremenski tijek Microsoft Exchange napada



Izvor: https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/

Pod ovim napadom, kao dio ili možda kao posljedica ovog napada dogodilo se još par napada. Pa tako, nakon početnog napada koji je krenuo početkom siječnja 2021. godine, u ožujku iste godine je zabilježen ransomware napad pod nazivom DearCry pri kojem su se koristile iste Zero day ranjivosti kao i pri inicijalnom Exchange napadu. Ovaj napad je kreirao kriptirane kopije napadnutih podataka i pri tome brisao originalne podatke. Potom su se REvil-ov

ransomware napad na Acer mrežu, kao i Black Kingdom ransomware povezali s Microsoft Exchange napadom. Ali osim različitih ransomware napada, zahvaljujući istim ranjivostima zabilježen je i botnet napad pod nazivom Prometei.

U prvom tromjesečju 2021. godine je zabilježen nagli rast napada putem tih ranjivosti. Broj pokušaja napada putem Microsoft Exchange ranjivosti povećao se deset puta od 11. ožujka 15. ožujka, to jest sa 700 pokušaja napada na 7 200 u samo par dana. Broj žrtava i potencijalnih žrtava se još uvijek ne zna. Microsoftove ranjivosti su iskoristili mnogi, moguće da još i iskorištavaju.

S obzirom na određene ranjivosti iznošene su različite pretpostavke, a ona službena bi bila da je bilo 250 000 potencijalnih žrtava. Od toga da je već napadnuto njih 60 000 u svijetu, do toga da ih je toliko napadnuto samo u SAD-u. Što znači da će se na procijenjeni broj žrtva još trebati sačekati. Ali, objavljeno je da je većina do sad potvrđenih žrtava iz SAD-a i Njemačke, što ukazuje da je napad vjerojatno imao određene mete. Osim njih određen postotak meta je bio iz Ujedinjenog Kraljevstva, Nizozemske te Rusije. Američka vlada je provjerila svoje Microsoft Exchange servere i izrazila zabrinutost o nastaloj situaciji, no koliko je trenutno poznato, ona nije bila zahvaćena napadom. S druge strane, Europsko nadzorno tijelo za bankarstvo ili EBA (eng. the European Banking Authority) objavilo da je bilo zahvaćeno napadom radi čega provodi istragu kako bi utvrdili razmjere napada, ali i da će otkrivene informacije ostati tajne i povjerljive zbog osjetljivosti područja kojim se EBA bavi.

Kao što je već napisano, ovaj napad i njegove posljedice se još istražuju. Tako se još uvijek istražuje i tko je odgovoran za ovaj napad, ali već se donose određene procjene i pretpostavke. Za sad se sumnja da je jedna kineska organizacija Hafnium odgovorna za pokretanje ovog napada. Kao i u velikoj većini napada, i ovdje je to samo pretpostavka i vrlo je vjerojatno da se nikad neće znati tko je kriv sa stopostotnom sigurnošću. No, s obzirom da se radi o većem broju ranjivosti, nakon što je napad proveden, objavljene su ranjivosti i njihove zakrpe, pretpostavlja se da su i drugi napadači iskoristili priliku za napad.

Za ovaj napad još nisu poznate sve činjenice, čak još nije sigurno ni je li napad gotov ni jesu li svi korisnici zaštićeni. Zabrinjavajuće je da još jedna velika kompanija, koja široko korištene proizvode, kao što je i Solar Winds, pretrpjela veliki kibernetički napad u zadnje dvije godine. Može se reći da je i zabrinjavajuće da su ta dva napada dogodila u tako kratkom razdoblju. Za Microsoft Exchange napad se sumnja da će nositi čak i veće financijske, tehnološke i ostale posljedice, od napada na Solar Winds.

4.3. Ostali primjeri

Nakon što je neki napad otkriven, provode se razne analize kako bi se došlo do podatka koliko je napad trajao, koga je zahvatilo i tko je napadač. No, nažalost dosta toga zapravo ostane na pretpostavkama i procjenama. Prethodno su prikazana dva nova napada koji su ostavili značajne posljedice na današnje sustave, mreže i društvo. Sada će se ukratko pomoću jednog od istraživanja prikazati stariji napadi: Stuxnet, Duqu i Flame.[44] Oni su ostavili svoj otisak u razumijevanju napada i podizanju svijesti o kibernetičkoj sigurnosti.

4.3.1. Stuxnet

Stuxnet je jedan od prvih otkrivenih napada s visokom razinom kompleksnosti i sofisticiranosti. Napad je otkriven u lipnju 2010. godine. Primarna svrha mu je bila sabotiranje iranskog nuklearnog programa.

Napad je otkriven nakon što su osobe zadužene za sigurnost u nuklearnim postrojenjima uočile određene neobične događaje koje su odlučili dodatno istražiti. Pri istraživanju su saznali da se iste anomalije pojavljuju na više različitih uređaja. Nakon toga, u lipnju 2010. potvrđeno je da su Siemens softveri za nadzor industrijskih postrojenja bili napadnuti, korumpirani i manipulirani. Ispostavilo se da je to bio izrazito kompleksan i sofisticiran napad za kojeg je trebalo vremena, strpljenja i resursa. Uz to se saznalo da su imali probni napad koji je prozvan Stuxnet 0.5 koji je počeo još 2005.godine. Smatra se da je za provedbu takvog napada trebalo osigurati Zero day ranjivosti, testno okruženje, stručnjake, programe i stručnu opremu. Radi toga se pretpostavilo da iza napada stoji određena država koja je u mogućnosti financirati i osigurati sve potrebne resurse.

Došli su do zaključka da su iza napada stajali SAD i Izrael, najvjerojatnije iz političkih razloga. S obzirom na okolnosti, zaključilo se da je napad ubačen u sustav tako što su zlonamjerni kod preko USB-a ubacili u sustav, a onda se on dalje širio mrežom Windows sustava. Stuxnet je bio namijenjen da reprogramira PLC (eng. Programmable Logic Controllers) kako bi centrifuge postrojenja radile na brzinama izvan prihvatljivih granica, uzrokujući njihov kvar i na kraju uništenje. Prema određenim podacima zaključuje se da se zarazilo oko 200 000 uređaja i 14 postrojenja, pri čemu se uništilo čak 10% centrifuga. To znači da je došlo do fizičkih oštećenja infrastrukture što je usporilo razvoj napadnutog programa za 4 godine.

[44] Virvilis, N., Gritzalis, D., Apostolopoulos, T.: "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", 2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE 10th International Conference on Autonomic & Trusted Computing, 2013.

4.3.2. Duqu

Duqu napad se vodi kao napad sličan Stuxnet-u, samo s drugačijom svrhom. Zato ga se povezuje s istim grupama napadača, kao i Stuxnet. Otkriven je u rujnu 2011. godine, svrha ovog napada je i dan danas ostala nepoznata.

Moglo bi se reći da je ovaj napad u neku ruku još uvijek misterija. Napad je iskoristio Zero day ranjivost Microsoft Word-a. Započeo je u veljači 2010. godine i trajao samo 36 dana. S obzirom da napad nije otkriven, napadači su mogli napad nastaviti i duže, ali su postavili samouništenje nakon 36 dana. Još uvijek se ne zna zašto je napad trajao tako kratko niti što su htjeli ili možda čak jesu li postigli željeni cilj. Misli se da mu je svrha prikupljanje informacija, pa možda čak i da je bio samo probni napad kako bi prikupili informacije za neki drugi.

Čak je u 2015. godini zabilježen napad Duqu 2.0 na hotele u Austriji i Švicarskoj, ali nikakve detaljne informacije o razmjeru napada ili posljedicama nisu objavljene, te se o njemu zapravo ne zna mnogo. Poznato je samo da je napad sofisticiraniji i napredniji od onog 2011. godine, što dovodi do pitanja može li se kibernetička sigurnost toliko brzo prilagođavati, koliko brzo napadi mogu napredovati.

4.3.3. Flame

Flame napad je slučajno otkriven dok su se tražili drugi napadi u svibnju 2012. godine. Naziva se još i Flamer, sKyWIper i Skywiper. Ovaj napad koji je koristio 2 Zero day ranjivosti te je zarazio na tisuće Windows sustava, od kojih je većina iz zemalja Bliskog (Srednjeg) istoka.

Ovaj napad karakteriziraju određene netipičnosti. Kao prvo, smatra se da je napad bio aktivan i neotkriven od 5 do možda čak 8 godina, to jest da je aktiviran 2010. godine, ali postoje sumnje da je aktiviran 2007., kao i Stuxnet i Duqu. Drugo bi bio podatak da je bio veličine od 20 megabajta, što je poprilično velik kôd i nije tipično za ove kibernetičke napade. Pomalo je zastrašujuće da je tako velik kôd, koji bi trebao biti lako uočljiv, godinama ostao neotkriven.

Flame je imao više različitih svrha i modula napada. Jedan od njih je mogućnost pokretanja mikrofona na uređajima kako bi se snimali razgovori i prikupljale informacije. Modul koji pomoću Bluetooth-a pretražuje druge uređaje s aktivnim Bluetooth-om kako bi došli od privatnih i osjetljivih podataka, ali i kontakata. Nadalje, jedan od modula je spremao i slao napadačima snimke zaslona sa uređaja. Svrha cijelog napada bila je prikupiti što više bitnih, osjetljivih i povjerljivih informacija. Vjerojatno u svrhu mogućnosti manipuliranja i upravljanja procesima.

5. ZAŠTITA OD ZERO DAY NAPADA

Od nekih kibernetičkih napada se jednostavnije zaštiti, a od drugih teže. Neki su detaljnije istraženi i analizirani, dok drugi još uvijek nisu dovoljno istraženi. Veliki broj kibernetičkih napada je omogućila ljudska greška, pa se dovodi u pitanje je ili slučajna ili namjerna pogreška. „S druge strane, kibernetički incidenti ne događaju se zbog bilo kakve „nesreće“ ili „peha“, već zbog lošeg upravljanja informacijskim sustavima i nedovoljnih kompetencija u kibernetičkoj sigurnosti.“[45] Čovjek je stvorio informatički i kibernetički prostor i brani sudionike tog prostora od drugog čovjeka, koji ga putem tog kibernetičkog prostora napada. Što se tiče Zero day napada, najučinkovitiji način za obranu je pravovremeno otkrivanje ranjivosti i njihovo rješavanje. Je li moguće otkriti Zero day napad u tijeku te je li postoji neka sigurna zaštita od njega, diskutirat će se u nastavku ovog poglavlja.

5.1. Problematika zaštite od Zero day napada

S obzirom na već istaknutu kompleksnost ovog napada, ali i činjenicu da o njemu treba obaviti još više istraživanja, ni otkrivanje ni zaštita od tih napada nije u potpunosti moguća. Slijedi prikaz potencijalnih načina otkrivanja napada i obrazloženje problematike zaštite od tih napada.

5.1.1. Otkrivanje Zero day napada

Dok se god koristi informatička i digitalna tehnologija postojat će i opasnost od kibernetičkih napada. Pošto ne postoji način da ih se u potpunosti zaustavi radi se na razvijanju metoda za otkrivanje napada. Kod Zero day napada su bitne i metode za otkrivanje ranjivosti, a ne samo napada, jer se tako mogu ispraviti greške i spriječiti Zero day napadi.

Različita istraživanja pružaju različite metoda identificiranja Zero day napada. Jedna od njih analizira prisutnost ranjivosti na Internetu i na taj način identificira Zero day napade. Sastoji od 4 ključna koraka:[46]

- Prikupljanje informacija o ranjivostima
- Povezivanje ranjivosti s njihovim iskorištavanjem, to jest napadima
- Analiza prisutnosti iskorištenih ranjivosti na internetu
- Identifikacija Zero day napada

[45] Spremić, M., Šimunic, A.: “Cyber security challenges in digital economy”, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018, IAENG, Hong Kong, 2018., 341.-347. str.

[46] Bilge, L., Dumitras, T.: “Before We Knew It: An Empirical Study of Zero-Day Attacks in The Real World”, Association for Computing Machinery, New York, NY, United States, 2012., 833.-844. str.

U tom istraživanju su prikupljeni podaci analizirani prema prethodnim koracima, a prikazani su u ostatku odlomka.[47] Treba naglasiti da je to istraživanje u kontroliranim uvjetima s poznatim podacima. To se treba uzeti u obzir, jer postoji mogućnost da je vrijeme napada manje zbog unaprijed poznatih činjenica. Što su točno radili u istraživanju? Za početak su prikupili sve potrebne podatke o ranjivostima koje su se smatrale Zero day ranjivostima u zadnjih par godina. Kao što je datum otkrivanja, oznaka, datum izdane zakrpe i slično. Kao drugo, pregledava se u kojim napadima su se koristile te ranjivosti. Nadalje, poslije utvrđivanja koliko je ranjivosti poznato javnosti slijedi opcionalni korak, koji ne spada u 4 ključna koraka. Preispituju se datoteke koje su manipulirane tijekom napada, da utvrde koja je sudjelovala u Zero day napadu. To jest, pomoću njega se potvrđuje je li neka od Zero day ranjivosti iskorištena u Zero day napadu. Potom su pretražili postoji li na Internetu zabilješka o tim ranjivostima, to jest da vide jesu li javno objavljene. Tu su utvrdili da veći dio ranjivosti zapravo nije javno objavljen i da nema nikakva zabilješka o postojanju te ranjivosti ni njenoj ispravci. To se može gledat kao negativna stvar, zato jer uz pomoć podataka o postojećim ranjivostima se mogu poboljšavati i nadograđivati metode otkrivanja Zero day ranjivosti, a s tim i Zero day napada. Za kraj se na temelju tih podataka identificiraju Zero day napadi. Između ostalog prikazan je kritični period u kojem se ranjivosti iskorištavaju. „Eksploatacija 42% ranjivosti, prema terenskim podacima, se pojavljuje unutar 30 dana nakon datuma otkrivanja. To ilustrira činjenicu da kibernetički kriminalci pomno prate otkrivanje novih ranjivosti kako bi ih počeli iskorištavati, što uzrokuje značajan rizik za krajnje korisnike.“[48] Što nas vraća na činjenicu da se Zero day ranjivosti ne pronalaze nužno odmah nakon puštanja softvera na korištenje, već u nekom bližem vremenskom razdoblju. Ali i ova metoda, kao i sve ostale, ne pokriva sve Zero day napade i zato nije u potpunosti korisna. Također treba uzeti u obzir da postoje određeni Zero day napadi koji će iskakati od drugih te time utječu na podatke istraživanja.

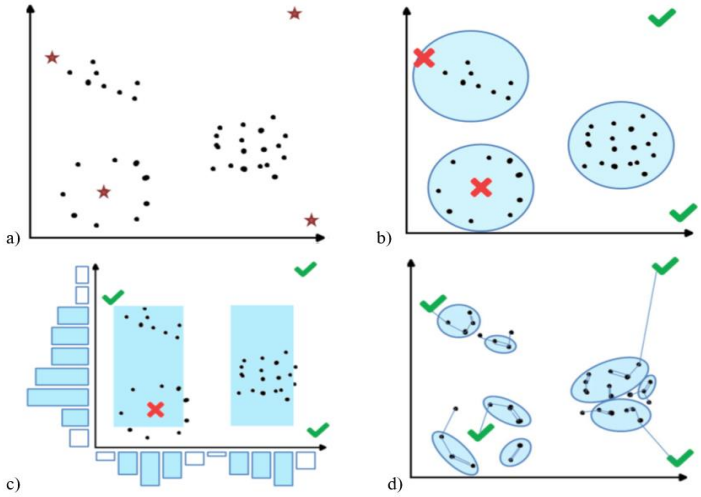
Ovakve metode identificiranja Zero day napada preko njihovih ranjivosti, iako ne pokrivaju baš sve, odličan su korak u daljnjem razumijevanju Zero day napada. Ističe se važnost dijeljenja informacija o Zero day ranjivosti i napadima. Isto tako se pokazalo, da je broj napada koji iskorištava neku ranjivost 5 puta veći kada se ona objavi i najavi zakrpa. U nekim slučajevima i nakon što se objavi zakrpa, dok je svi ne primjene u svojim sustavima.

[47] Bilge, L., Dumitras, T.: “Before We Knew It: An Empirical Study of Zero-Day Attacks in The Real World”, Association for Computing Machinery, New York, NY, United States, 2012., 833.-844. str.
[48] Bilge, L., Dumitras, T.: “Before We Knew It: An Empirical Study of Zero-Day Attacks in The Real World”, Association for Computing Machinery, New York, NY, United States, 2012., 833.-844. str.

Nadalje će se promatrati usporedba nadziranih (eng. supervised) i nenadziranih (eng. unsupervised) algoritama. Nadzirani algoritmi su najučinkovitiji kada se koriste za otkrivanje već poznatih napada. S druge strane, nenadzirani algoritmi imaju problema s razlikovanjem Zero day napada od drugih napada. S obzirom da je svaki Zero day napad drugačiji, teško je napravit jednu kategorizaciju. Strojno učenje bi moglo biti ključ za pronalazak i otkrivanje Zero day napada, ali i Zero day ranjivosti kako bi se napadi unaprijed mogli spriječiti.

Nenadzirano strojno učenje koristi ne kategorizirane, ne označene podatke i na temelju njih donosi zaključke. Kod tih algoritama se isti podaci smještaju u iste grupe, a različiti u različite grupe. U nenadzirano učenje na primjer spadaju algoritmi za klastere (eng. clustering algorithms), algoritmi za klasifikacije (eng. classification algorithms), statistički algoritmi (eng. statistical algorithms) i algoritmi bazirani na sličnostima (eng. neighbour-based algorithms).[49] Zanimljivo je to da su algoritmi iz iste kategorije nenadziranog strojnog učenja, rezultati su u potpunosti drugačiji, kao što je prikazano na slici 9. „Međutim, svi nenadzirani algoritmi imaju konstantno vrijeme ispitivanja, pa su stoga sposobni trenutno obraditi i klasificirati nove točke podataka, što je važno, na primjer, za analizu tokova podataka.“[50]

Slika 9 Prikaz detekcije anomalija preko 3 različita algoritma:
a)prikaz anomalija zvjezdicama, b)klasteri, c)statistički, d)bazirani na sličnostima



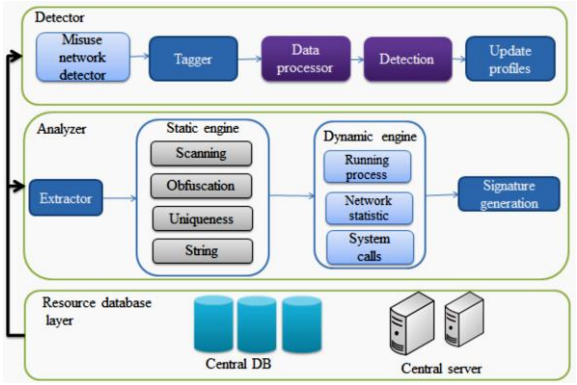
Izvor: Zoppi, T., Ceccarelli, A., Bondavalli, A.: “Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application”, IEEE, 2021.

[49] Zoppi, T., Ceccarelli, A., Bondavalli, A.: “Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application”, IEEE, 2021.
[50] Zoppi, T., Ceccarelli, A., Bondavalli, A.: “Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application”, IEEE, 2021.

Nadzirano strojno učenje je novija strategija korištenja nekoliko strategija rudarenja informacija u svrhu razlikovanja i rangiranja Zero day zlonamjernih softvera.[51] Provodi se na već poznatim podacima koji su prethodno označeni. Tim strojnim učenjem sustav uči iz prethodnih podataka i pravi njihovu klasifikaciju. Susjedne ili slične podatke smješta u iste klase. To potom dovodi do sažetih i jednostavnijih podataka o napadima. Smatra se da se na taj način ne mogu učinkovito pronalaziti Zero day napadi, zato što vrlo vjerojatno nove napade neće znati prepoznati. Nadzirani algoritmi se temelje na pravilima, potpisima i nadzoru zbog čega ne mogu pouzdano identificirati nove Zero day napade.

Prethodno prikazani podaci za otkrivanje Zero day napada nisu jedini. Kao što se već spominjalo i kod ranjivosti, iako još nije dovoljno istraženo, to ne znači da već ne postoje različiti pokušaji istraživanja i algoritmi koji rade na otkrivanju Zero day napada. Osim proučavanja pojedinačnih metoda, počelo se raditi na mogućim kombinacijama algoritama i općenito načina otkrivanja, kao potencijalno boljim opcijama. Znaju se nazvati hibridnim pristupima za otkrivanje Zero day napada. U jednom takvom istraživanju dan je prikaz slojeva arhitekture procesa za otkrivanje Zero day napada.[52] Prvi sloj se zove detektor i on pronalazi potencijalno zaražene mreže i otkriva nepoznate napade. Drugi sloj je analizator i u tom sloju se analiziraju rad mreže putem statičnih i dinamičnih analiza. Treći sloj je sloj baze podataka resursa koji uključuje poslužitelje za obradu, koji omogućuje provedbu procesa u prva dva sloja.

Slika 10 Slojevi otkrivanja Zero day napada



Izvor: Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H.: "A hybrid layered architecture for detection and analysis of network based Zero-day attack", Computer Communications, 2017.

[51] Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H.: "A hybrid layered architecture for detection and analysis of network based Zero-day attack", Computer Communications, 2017.
[52] Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H.: "A hybrid layered architecture for detection and analysis of network based Zero-day attack", Computer Communications, 2017.

5.1.2. Problematika zaštite od Zero day napada

Nakon objašnjenja općenito kibernetičkih napada, napadača i kibernetičke sigurnosti, te detaljnijeg pregleda motiva i uzroka Zero day napada, neke stvari jednostavno nije moguće jasno definirati i predstavljaju prepreku pri zaštiti od napada. U ovom radu se više puta isticala složenost Zero day ranjivosti, Zero day napada te načina njihovih otkrivanja. Pa tako problematika Zero day napada leži upravo u njegovoj složenosti i promjenjivosti.

Promatrano od Zero day ranjivosti pa do Zero day napada, sve je promjenjivo. Ovisno o okolnostima određena greška može postati ili prestati biti Zero day ranjivost. Potrebno je vremena da se otkrije, te odredi njena vrijednost i njena iskoristivost. „Vjerojatnost pronalaska ranjivosti vrijedne iskorištavanja mijenja se ovisno o tome koliko je osoba već pregledalo kôd, o dubini analize kôda, složenosti kôda, stopi promjena proizvoda, zrelosti proizvod i funkciju proizvoda.“[53] Treba odrediti i u koju kategoriju Zero day ranjivosti spada, privatne ili javne. Problematika se javlja i kod otkrivanja Zero day ranjivosti, točnije motiva koji leže iza njihovih otkrivanja i načina na kojih se distribuiraju. Kao što se već spominjalo, osim programera koji su radili na određenom softveru, u otkrivanju ranjivosti pomažu korisnici koji prijave određene greške, ali i plaćene agencije za traženje ranjivosti te hakeri kojima je cilj prodati Zero day ranjivost na sivom ili crnom tržištu.

Potom se treba sjetiti i promjenjivosti samog napada. Zero day napad je tako prozvan, jer se smatralo da na nulti dan pokretanja softvera dolazi do iskorištavanja njegove ranjivosti, a danas predstavlja broj dana, koji je programerima ostao da isprave grešku u kôdu. Kod određenih stručnih literatura javljaju se različita mišljenja i oko toga je li napadač došao do ranjivosti jer je javno objavljena ili ne, te je li pružatelj usluge nje bio svjestan ili ne. Također, određivanje koja je motivacija pokrenula napad i koji cilj se želi postići možda nekada je teško točno odrediti. Pri otkrivanju napada i obrani jedan od problema može predstavljati i količina ranjivosti koja je bila potrebna za njegovu izvedbu. S obzirom da je teško naći jednu vrijednu Zero day ranjivost, ponekad se eksploatacija sastoji od više ranjivosti, jer inače izvedba napada ne bi bila moguća. Dosta toga nije točno određeno i vrlo jasno predstavlja zašto je teško prepoznati, odrediti i otkriti Zero day napade. Zero day napadi i sve u vezi njih ovisi o okolnostima i o promjenama tih okolnosti.

[53] Ablon, L., Bogart, A.: Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, RAND Corporation, Santa Monica, CA, 2017.

Iduće što čini Zero day napad problematičnim za otkrivanje su motivi za njegovu provedbu i razumijevanje odabira načina napada. Osim što se pri izvođenju Zero day napada najčešće koristi više različitih ranjivosti, za izvođenje nekoga napada, pa tako i Zero day napada najčešće ima i više opcija za izvedbu napada. Postoje različiti načini izvedbe zero day napad i iskorištavanja Zero day ranjivosti. Možda bi se moglo pretpostaviti da napadači nasumično odabiru određeni način napada između dostupnih metoda, ali zapravo ljudski um većinom razmišlja logički i strateški. Napadači uglavnom odabiru određeni način ili metodu provedbe napada na temelju toga žele li najlakši, najbrži ili možda najsigurniji način provedbe napada.[54] Najlakši bi značilo da traže napad koji je najjednostavnije provesti u djelo, najbrži onaj koji će zahtijevati najmanje vremena za provedbu i prvi pružiti određene rezultate, a najsigurniji bi bio onaj kojeg će se najteže otkriti i zaustaviti. Razumijevanje zašto je odabran baš određeni način za napad i povezivanje toga s motivima i ciljevima bi moglo pomoći u boljem razumijevanju Zero day napada. Ali kada to nije moguće onda predstavlja jedan od problema i prepreka bi razumijevanju i otkrivanju Zero day napada.

Promjena okolnosti, pa i najmanjih detalja može utjecati na Zero day napad. Svaki dio računala, sustava, softvera i mreže može utjecati na provedbu i konačni rezultat napada i obrane. To jest, može prouzrokovati promjenu u napadu ili obrani. Može doći do problema određivanja tijeka napada i obrane, to jest što se kada dogodilo. To predstavlja problem jer se onemogućuje ili otežava određivanje uzročno-posljedične veze između određenih događaja putem analiza i istraživanja. Prethodno navedena problematika također utječe na analize i istraživanja tako što otežava njihovu provedbu. Za istraživanja su potrebni točno definirani podaci, pa kada se nešto ne može točno kategorizirati, vremenski odrediti ili definirati, ti podaci mogu biti ne iskoristivi ili dodatno zakomplicirati provedbu istraživanja. „U laboratoriju, okolnosti pri ispitivanju ostaju iste: Opterećenje mreže i latencija je kontrolirana i dosljedna, a sustav se iskorištava isključivo u svrhu testiranja.“[55] Zato stvarni napadi nisu uvijek jednaki kao što je prikazano u istraživanjima. Nažalost u stvarnom svijetu nema savršenih uvjeta, štoviše oni se konstantno mijenjaju i s njima se mijenjaju uvjeti napada i obrane.

Svi problemi definiranja i promjene koje utječu na Zero day napade, otežavaju ne samo provedbu napada, nego i njihovo otkrivanje i zaštitu. Iza toga leži i problem ne objavljivanja

[54] Cohen, F.: “Simulating Cyber Attacks, Defences, and Consequences”, Computer & security, Sandia National Laboratories, Livermore, CA 94550, USA, 1999.
[55] Ablon, L., Bogart, A.: Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits, RAND Corporation, Santa Monica, CA, 2017.

svih detalja o već provedenim napadima, a neki napade nisu uopće prijavili. Time su uskraćene dragocjene informacije koje bi bile korisne u analizama Zero day napada.

Još jedan problema u zaštiti od Zero day napada danas je način pisanja kôda. No to se u jednu ruku može smatrati problemom, a u drugu prednosti. Danas je pisanje programa dosta lakše i postoje dijelovi kôda koji se pronalaze na internetu i primjenjuju u praksi. Određenu liniju ili skup linija kôda često koristi više osoba, bilo u različitim organizacijama ili samo unutar jedne. Problem leži u tome što određena greška se može nalaziti baš u tom dijelu kôda, a on će se kopirat iznova i iznova po potrebi. „Ponekad, ako se jedna ranjivost iskoristi u jednom sustavu kao Zero day ranjivost, ista ranjivost može postojati u nekim drugim sustavima, ali nije pronađena ili iskorištena.“[56] Drugi problem može biti u tome ako se pisanje kôda bazira na tim prije pripremljenim dijelovima, što može doći do propusta pri spajanju tih linija i to može biti greška koja će predstavljati određenu ranjivost. To ne znači da problema ne bi bilo da se ništa ne kopira. Štoviše i u slučaju da se sve piše posebno, dolazi do mogućnosti da postoji neka ranjivost. Kao što se već spomenulo, u 1000 linija kôda se napravi 70 grešaka ili 'bugova'. Greške u kôdu se ne mogu izbjeći, a bez njih ne bi bilo ni ranjivosti ni zero day napada. Stoga se može reći da su one glavni problem u zaštiti od Zero day napada.

To su neke od stvari koje predstavljaju problem pri zaštiti od Zero day napada. Za izvedbu takovog napada potrebno je ispuniti više različitih uvjeta. Od pronalaska Zero day ranjivosti, potrebe za većim brojem ranjivosti pri izvođenju jednog napada, pa do pronalaska pravog trenutka, načina napada i konačne provedbe. S druge strane imamo problem predviđanja i otkrivanja Zero day napada. Vrlo vjerojatno je nemoguće predvidjeti točan napad zato što ovisi o previše različitih varijabli. Ono što bi bilo moguće je pronaći Zero day ranjivosti, kako bi se moglo predvidjeti koja od njih bi se mogla iskoristiti. Samo otkrivanje već provedenog Zero day napada je povezano s prethodno opisanim problemima. Radi se na načinima otkrivanja napada, ali sama kompleksnost cijele teorije povezane s njim usporava i otežava napredak. Iako postoji mnogo istraživanja na tu temu i dalje se smatra da to nije dovoljno. Zero day napadi su sve sofisticiraniji iz dana u dan, a s tim raste i njihova kompleksnost. Nisu se u potpunosti istražili ni stari napadi, a već je potrebno provoditi nova istraživanja.

[56] Akram, J., Ping, L.: “How to build a vulnerability benchmark to overcome cyber security attacks”, The Institution of Engineering and Technology, Key Laboratory of Information System Security, School of Software, Tsinghua University China, Beijing, People's Republic of China, 2019.

5.1.3. Moguće prednosti u zaštiti od Zero day napada

Nakon što se pričalo o problematici Zero day napada potrebno je spomenuti i neke stvari koje potencijalno olakšavaju zaštitu od tih napada. Određene stvari koje se primjenjuju u praksi mogu biti jedna od prepreka za izvršenje napada.

Ovdje ćemo pričati o raznolikosti mreže kao prednosti kod zaštite od Zero day napada. „Različitost se već dugo smatra sigurnosnim mehanizmom za poboljšanje otpornosti softvera i mreža na različite napade.“[57] U pravo tako, raznolikost mreža predstavlja jednu od dodatnih potpora zaštiti sustava od poznatih i nepoznatih ranjivosti. To je važno zato što nekih Zero day ranjivosti organizacije nisu svjesne u isto vrijeme kada i napadači.

Koja je točno uloga raznolikosti mreže pri zaštiti. Raznolikost mreže se može promatrati kao omjer minimalnog broja resursa i minimalnog broja koraka koji su potrebni za izvođenje Zero day napada na nekoj mreži. Ta raznolikost se očituje u samoj strukturi mreže, broj članova, softverima koji se koriste, također i u antivirusnim softverima te nekim drugim dodacima. Može se reći da je postizanje raznolikosti mreža u svrhu bolje zaštite sustava, organizacije i mreže vrlo jednostavna i svi je mogu iskoristiti. No, za takav pothvat je potrebno vrijeme i resursi, pogotovo za manje organizacije koje nisu izravno u takvom poslovanju. Također, s obzirom na količinu organizacija u današnjem okruženju, vrlo je teško postići da se razlikuju u baš svemu. „Glavno ograničenje raznolikosti dizajna leži u velikoj složenosti stvaranja različitih verzija, što možda ne opravdava korist.“[58] Pogotovo organizacije koje rade u istom području i koriste iste softvere. O širini područja i učinaka koju pruža raznolikost mreža, govori i to da se promatraju učinci raznolikosti dizajna, učinci generiranih raznolikosti te oportunističke raznolikosti među različitim softverima.

Određena istraživanja su na putu k formalnim modelima za definiranje raznolikosti mreža. U njima se procjenjuje i povezanost raznolikosti mreže i zaštite od Zero day napada. Još uvijek postoje određena ograničenja u ovim istraživanjima, ali se vjeruje da iza njih postoji potencijal kako bi dodatno ojačale kibernetičku sigurnost.

[57] Zhang, M., Wang, L., Jajodia, S., Singhal, A., Albanese, M.: “Network Diversity: A Security Metric for Evaluating the Resilience of Networks against Zero-Day Attacks”, IEEE Transactions on Information Forensics and Security, 2016.

[58] Zhang, M., Wang, L., Jajodia, S., Singhal, A., Albanese, M.: “Network Diversity: A Security Metric for Evaluating the Resilience of Networks against Zero-Day Attacks”, IEEE Transactions on Information Forensics and Security, 2016.

5.2. Osvrt na istraživanja o Zero day napadima

U zadnjem dijelu ovog rada će se prikazati određena istraživanja o Zero day napadima te pružiti osvrt na njih. Već su se spominjali mogući načini otkrivanja Zero day napada, ali sada će se pružiti detaljniji prikaz konkretnih analiza. Istraživanja su bazirana na različitim načinima provedbe Zero day napada, ovisno je li im cilj općenito prikazati opcije za otkrivanje napada, otkriti zlonamjerni kôd ili nešto drugo.

5.2.1. „Kontekstualni pristup detekcije anomalija za otkrivanje Zero day napada“

Slijedi prikaz istraživanja „Kontekstualni pristup detekcije anomalija za otkrivanje Zero day napada“ (eng. „A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks“).[59] U ovom radu se opisuje kontekstualni pristup mogućoj zlouporabi u kombinaciji s tehnikama za otkrivanje anomalija povezanih s Zero day napadima.

U ovom istraživanju se ističe da IDS ili sustav za detekciju napada (eng. Intrusion Detection Systems) ima ulogu nadgledanja i kontrole veza unutar mreže. Točnije, da pri detektiranju neodobrenih načina upotrebe sustava i traženju anomalija, uz pomoć tih procesa, određuje granice normalne funkcije sustava. Predstavljen je problem lažnih rezultata i nemogućnosti otkrivanja još nezabilježenih napada. Navedeno je i kako je većina ostalih istraživanja fokusirana na nenadzirane algoritme, koji su se spominjali u prethodnim poglavljima. Kod njih također leži problem lažnih rezultata, jer oni prepoznaju napade na temelju poznatih napada.

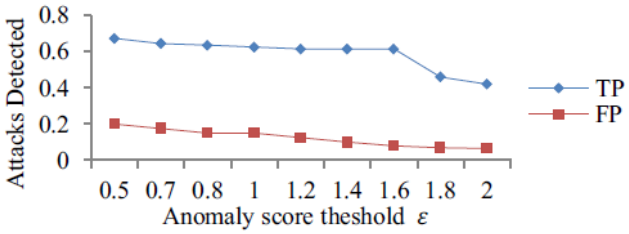
Zbog toga su u ovom istraživanju predstavili kontekstualni pristup pri detektiranju anomalija i otkrivanju Zero day napada. Taj model je implementiran u sustav koji je nalik na stvarnu mrežu, kako bi se dobili što vjerodostojniji rezultati. Zamišljeno je da se ispituju veze unutar sustava ili mreže putem kontekstualnog pristupa. Prvo su odredili koje su karakteristike napada i njihove međusobne sličnosti te moguće anomalije kako bi odredili uzorke. Potom se provodi procjena učinkovitosti i točnosti na sustavu. Ako se otkrije uzorak koji se u potpunosti slaže s jednim ili više kontekstualnih profila, onda se šalje obavijest administratoru o otkrivenom napadu. No, ako se djelomično slaže s nekim od profila, da se šalje obavijest o promjeni u sustavi koja nije identificirana kao napad, ali mu je slična, te treba dodatno ispitivanje. A tri važna dijela pri ovoj analizi su modul za detekciju neispravne upotrebe sustava, modul za detekciju anomalija i spremište za pohranu procjena.

[59] AlEroud, A., Karabatis, G.: „A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks“, International Conference on Cyber Security, Department of Information Systems, University of Maryland, Baltimore, USA, 2012

Analize su proveli pomoću postojeće KDD baze podataka iz 1998.godine koja sadrži 500 000 podataka, to jest zapisa veza. Na temelju tih podataka su se kreirali kontekstualni profili. Nadalje, podaci iz baze su podijeljeni na 2 dijela, na dio za vježbu i dio za testiranje. Mjere koje su korištene pri provođenju eksperimenta su istinito pozitivna stopa (TP), lažno pozitivna stopa (FP), i točnost procjene (AC).

Analiza u kojoj se mjeri stopa otkrivanja novih Zero day napada korištenjem ocjene sličnosti profila je imala najlošije rezultate. Pri najnižoj ocjeni sličnosti vrijednosti TP i FP su visoke. A kako se ocjena sličnosti povećava, smanjuju se i TP i FP. Može se zaključiti da se na temelju sličnosti ne mogu dobiti dovoljno vjerodostojni podaci. U drugoj analizi, na temelju anomalija otkrivaju novi Zero day napadi, rezultati su bolji nego kod sličnosti, ali i dalje ne dovoljno dobri. Pri ovoj analizi, pri niskim razinama anomalija ili promjena, TP i FP su dosta visoke, kao i kod prethodne analize. Kako razina promjena raste, FP dolaze na vrlo niske razine, dok se TP malo smanjuj, ali zadržavaju visoku razinu točnosti. U trećoj analizi se uz pomoć vrijednosti anomalija preciziralo predviđanje sličnosti poznatih Zero day napada s novim Zero day napadima. „Svrha ovog eksperimenta je dvostruka: prvo, kako bi se smanjilo potrebno vrijeme izračuna ako su svi zapisi veza proslijeđeni modulu za otkrivanje anomalija; drugo, smanjenje stope lažno pozitivnih rezultata ocjene sličnosti profila.“[60] U ovoj trećoj analizi, s rastom razine anomalija i TP i FP lagano pada, ali pri svim razinama anomalija TP zadržava visoke vrijednosti, a FP niske vrijednosti. U ovoj analizi se postiže najveća točnost prepoznavanja novih Zero day napada, što je dokaz da je istraživanje postiglo željeni učinak.

Slika 11 Grafički prikaz rezultata treće analize otkrivanja novih Zero day napada uz pomoć vrijednosti anomalija pri preciziranju ocjena sličnosti



Izvor: AlEroud, A., Karabatis, G.: „A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks“, International Conference on Cyber Security, Department of Information Systems, University of Maryland, Baltimore, USA, 2012

[60] AlEroud, A., Karabatis, G.: „A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks“, International Conference on Cyber Security, Department of Information Systems, University of Maryland, Baltimore, USA, 2012

5.2.2. „Skupovi podataka temeljeni na sustavu Windows za procjenu robusnosti sustava domaćina za otkrivanje upada (IDS) Zero day napada i prikrivenih napada“

Slijedi prikaz jednog Australskog istraživanja „Skupovi podataka temeljeni na sustavu Windows za procjenu robusnosti sustava domaćina za otkrivanje upada (IDS) Zero day napada i prikrivenih napada“ (eng. „Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks“).[61] Ovo je jedno od istraživanja koje ne radi izravno na otkrivanju Zero day napada, već mu je svrha osigurati vjerodostojne podatke, to jest baze podataka, za buduća istraživanja povezana s Windows-om i Zero day napadima. U ovom istraživanju se procjenjuje složenost IDS-a, točnije HBADS-a (eng. Host Based Anomaly Detection System) u obrani od Zero day napada i prikrivenih napada (eng. Stealth attack) pomoću novih baza podataka. U ovom osvrtu će fokus biti na rezultatima analiza u vezi s Zero day napadima.

Iako je Windows jedan od najpopularnijih sustava za računala, baze podataka koje se koriste u istraživanjima o Zero day napadima kao što je KDD 98 ili ADAF-LD, zapravo nisu primjenjive s Windows-ovim IDS-om. U isto vrijeme se smatra da iako Windows ima više načina zaštite i detekcije napada, ni jedan nije uspješan u detektiranju Zero day napada. Stoga su uz pomoć DLL-a ili biblioteke dinamičkih poveznica (eng. Dynamic Link Library) odlučili stvoriti sveobuhvatnu bazu podatak koja je primjenjiva u Windows sustavu kako bi se našao način otkrivanja Zero day napada.

Tako su stvorili skup podataka ADFA-WD koji se koristi istraživanja o Zero day napadima, te proširenu verziju pod nazivom ADFA-WD:SAA koja je usmjerena na prekrivene napade. ADFA-WD skup podatak sadrži identificirane Zero day napade po njihovim ranjivostima. U isto vrijeme je primjenjiv na Windows-u. Reprezentativnost stvorenog skupa podataka se naglašava uključivanjem različitih veza unutar sustava. Nadalje, u ADFA-WD-u se za konstrukciju napada uzimaju u obzir odnosi između prethodno identificiranih 12 ranjivosti i trenutnih vektora napada, to jest TCP portovi, napade preglednika, vektore temeljene na webu i privitke zlonamjernog softvera. Upravo ti vektori napada su izabrani kako bi se podaci modernizirali i tako bili u skladu s Windows-ovom literaturom. Još što je bitno za ovaj skup podataka je to da se sastoje od normalnih podataka i napadnutih podataka.

[61] Haider, W., Creech, G., Xie, Y., Hu, J.: “Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks”, Future Internet, 2016.

Kako bi se napravila procjena stvorenih baza podataka, napravljene su 2 analize. Pomoću njih su htjeli odgovoriti na 2 pitanja: kako bi se mogla mjeriti sličnost ili diskriminacija između napadnutih i normalnih podataka, te koja je njihova razina složenosti, to jest je li predstavljaju sofisticirane napade?[62]

Prva je bila analiza složenosti skupa podataka metodom raspodijele frekvencija. Pri ovoj analizi se ispituje devet DLL poziva koji predstavljaju revizijske podatke. Revizijski podaci mogu predstavljati ponašanje sustava. Provedena je analiza DLL poziva na napadnutim i normalnim podacima. Uočeno je da su frekvencije DLL -a u napadnutim i normalnim podacima vrlo blizu jedna drugoj. Ta niska razina sličnosti znači da postoji srednja razina hakiranja, to jest ne smatraju se visoko klasificiranima već srednje zahtjevnima.

Drugo je provedena analiza složenosti skupa podataka pomoću okvira otkrivanja anomalija. Provedena je kako bi se procijenila kompleksnost skupa podataka na IDS-u. Ukratko, ova druga analiza nažalost nije pružila željeni rezultat. Koristili su i linearne i nelinearne klasifikatore, ali ni s jednim nisu postigli optimalne rezultate. Također, nisu uspjeli otkriti koje su prirodne razlike između normalnih i napadnutih veza. Iznose da postoji par razloga zašto je to tako. Jedan od njih je to što novi skupovi podataka nisu imali dovoljno raznolike napade, od manje sofisticiranih od više sofisticiranih. Putem ove analize pokazalo se da je ADFA-WD nešto vjerodostojni skup podataka od ADFA-WD:SSSA, ali ga treba nadograditi i nadopuniti.

U ovom istraživanju je bio cilj stvoriti skup podataka koji je primjenjiv na Windowsu i pomoću kojeg će se moći odrediti kompleksnost IDS-a. Iako su stvorili dva skupa podataka ADFA-WD i ADFA-WD:SAA, pri provođenju preliminarnih testiranja, ispostavilo se da ih se treba poboljšati kako bi se mogli koristiti u daljnjim istraživanjima. Usprkos neočekivanim rezultatima, ovo istraživanje je napravilo korak naprijed u razvoju skupova podataka za Windows koji će se moći koristiti u istraživanju Zero day napada. „Rezultati su pokazali da se, kako bi se dizajnirao učinkovit HADS za Windows OS, mora obratiti pozornost na odabir/konstrukciju značajki i prilagodbu stroja odlučivanja zbog uočene složenosti skupova podataka.“[63]

[62] Haider, W., Creech, G., Xie, Y., Hu, J.: “Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks”, Future Internet, 2016.
[63] Haider, W., Creech, G., Xie, Y., Hu, J.: “Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks”, Future Internet, 2016.

5.2.3. „Učinkovito otkrivanje Zero day crva na temelju sadržaja“

Za razumijevanje ovog istraživanja je potrebno prvo razumjeti što je to računalni crv. Računalni crv je mrežni virus koji se rasprostranjuje putem samo kopirajućeg kôda. Širi se bez obzira na interakciju s čovjekom, te mu ne treba ni program ni datoteka na računalu kojom će se širiti. Računalni crv se širi toliko brzo da može zaraziti i desetak tisuća računala u sat vremena. Naravno, nisu svi crvi jednako brzi. Što je crv manji, to se može brže širiti. Uglavnom su namijenjeni kako bi preopteretili sustav kopirajući i oštećujući podatke, ali ako mu se dodaju posebni dijelovi kôda koji se nazivaju teretom (eng. payloads), onda može vršiti i druge zlonamjerne radnje na računalu.

Istraživanje koje će se prikazati je „Učinkovito otkrivanje Zero day crva na temelju sadržaja“ (eng. „Efficient Content-Based Detection of Zero-Day Worms“).[64] Ponuđena je nova metoda za otkrivanje novih crva na osnovi identifikacije sličnosti s već poznatim crvima. Pri tome su se odlučili koristiti i Rabinovim otiskom prsta (eng. Rabin fingerprint).

Umjesto promatranja samih ponavljajućih paketa, promatrali su podnizove u kojima se nalaze paketi s crvima. Određeni napadači mogu sakriti svoj napad tako da jedan paket, to jest nove dijelove kôda, rasporede u manjim dijelovima na različita mjesta. Zbog toga su pri analizi koristili i algoritam za sastavljanje prethodno rastavljenih paketa. S obzirom da se crv širi s klijenta na klijenta fokus je stavljen na zahtjeve klijenta, a ne na servere, u nadi da se smanje lažno pozitivni rezultati. Uzevši to u obzir, kako bi osigurali što manje ponavljanja i nepotrebnih troškova u analizi su odbacivali odgovore poslužitelja te odabirali samo potrebne otiske (Rabinove otiske). Odabir otisaka su proveli zato što se mnogi od njih ponavljaju, pa tim postupkom nisu gubili na vjerodostojnosti podataka.

Pri analizi su se koristili stvarnim podacima koji su se prikupili o mreži. U prvoj analizi se koristio parametar duljine pod niza (eng. substring length), u drugoj je parametar bio prag različitih odredišta (eng. distinct destinations threshold), u trećoj je parametar veličina pred memorije pod niza (eng. substring cache size,), te u četvrtoj je parametar pomaka granica protoka (eng. flow offset limit). Uz te parametre, u svakoj analizi su korištene promatrane mjerne veličine su lažno pozitivni rezultati, tokovi koji su bili slični tokovima crva, ali je bila lažna uzbuna, te otkrivanje s zakašnjenjem, što znači da je otkriven tok s crvom, ali s zakašnjenjem.

[64] Akritidis, P.; Anagnostakis, K.; Markatos, E.P.: “Efficient Content-Based Detection of Zero-Day Worms”, IEEE International Conference on Communications, 2005., 837.-843. str.

Iz provedenih analiza su donijeli neke bitne zaključke. Jedan od njih je da se povećanjem duljine pod niza smanjuje broj lažno pozitivnih rezultata, a otkrivanje s zakašnjenjem ostaje konstantno. Nadalje, ispostavilo se da istraživana metoda nije učinkovita pri otkrivanju crva u razdoblju koje je kraće od razdoblja s kojim su povezani otisci prstiju. To jest crv može izbjeći otkrivanje pri manjim vrijednostima pred memorije. Prikazano je i da smanjenje granica protoka smanjuje kašnjenje otkrivanja crva, ali u isto vrijeme povećava broj lažno pozitivnih rezultata. Ustanovljeno je da postoje određene prepreke, ali i na koji način se mogu dobiti potrebni rezultati.

Prikazali su da se Zero day crv može otkriti pretraživanjem nizova s velikom stopom prijenosa na različite ciljeve. Također je prikazano da se lažno pozitivni rezultati mogu ukloniti razmatranjem nizova većih veličina u vezama koje generiraju razumno male količine prometa. Iznose i da je detekcija bez lažno pozitivnih rezultata moguća pri otkrivanjima crva s zakašnjenjem, što smatraju ohrabrujućim. S druge strane se pokazalo da nakon 11 lažnih napada dolazi do sumnje da je to pravi napad, što dovodi do lažno pozitivnih rezultata. Taj prag od 11 lažnih napada koji uzrokuje sumnju, smatra se relativno niskim, te predlažu uzorkovanje tokova kako bi se to izbjeglo. Ali to još treba biti istraženo i potvrđeno.

Ovo je još jedno istraživanje koje je pokušalo naći metodu koja je najbolja za otkrivanje crva. Iako se možda metoda nije pokazala najboljom dosad, prikazali su pozitivne strane ove metode i unaprijedili dosadašnje. Prikazali su probleme na koje su naišli i potencijalne načine kako da se isprave. To je još jednom jedan korak naprijed u zaštiti od Zero day crva i mogući početak za neka druga istraživanja.

5.2.4. Kratki osvrt

Ova 3 istraživanja su samo dio provedenih istraživanja o Zero day napadima. Odličan su prikaz da bilo koji pothvat je korak naprijed u boljoj zaštiti i otkrivanju Zero day napada. I ona istraživanja koja ne pronađu rješenje kojem su se nadali, pronađene pozitivne i negativne podatke su podijelili s drugima. Iz negativnih rezultata i problema na koje se naišlo moguće je naučiti još više nego iz pozitivnih. Ukazujući na probleme potiče se rješavanje istih. Te konstantnim istraživanjima i učenjem jedni od drugih i nadograđivanjem već postojećih metoda razvijaju se nove i bolje. A upravo to i je cilj svakog istraživanja, naći potrebno rješenje.

6. ZAKLJUČAK

Opasnost od kibernetičkog napada na informacijsku i digitalnu tehnologiju je sveprisutna i naziva se kibernetičkim rizikom. Kibernetičkim napadom smatra se svaka radnja u kibernetičkom prostoru kojom se nastoji izmijeniti, poremetiti ili uništiti računalni sustav ili mrežu, ili informacije i/ili program na njima u političke svrhe, svrhe nacionalne sigurnosti ili želje za moći. Među mnogim kibernetičkim napadima posebnu ulogu stječu Zero day napadi.

Jedno vrijeme se vjerovalo da Zero day napadi i nisu baš učestali. Zbog toga, a možda i zbog činjenice da ih je teško otkriti prije nego što se dogode, i dalje nema dovoljno istraživanja o njima. Važno je povećati svijest o opasnosti svih kibernetičkih napada, uključujući Zero day napade. Putem ovog rada se pokušalo prikazati i objasniti okolnosti koje mogu utjecati na ovaj napad i u kojima se ovaj napad može odvijati. Objasnila se kompleksnost definiranja napada te dao prikaz faza kroz koje Zero day napad prolazi. Za izvedbu takovog napada potrebno je ispuniti više različitih uvjeta. Od pronalaska Zero day ranjivosti, potrebe za većim brojem ranjivosti pri izvođenju jednog napada, pa do pronalaska pravog trenutka, načina napada i konačne provedbe. Također se utvrdilo i da napadači koji koriste Zero day napad kako bi ostvarili svoj cilj, nemaju određenu kategoriju ciljanih meta, ali je ipak uočljivo da su orijentirani na veće organizacije koje imaju širi spektar korisnika i koji imaju korisnike s visokim razinama povjerljivosti. Preko primjera se može uočiti upravo ta karakteristika žrtava, kao i posljedice koje žrtve proživljavaju. Žrtve napada preživljavaju fizičke, financijske, informacijske, tehnološke i psihičke štete, čak sve njih ili bar većinu poslije nekog napada. Preko primjera se također potvrdila činjenica da su Zero day napadi iz dana u dan sve sofisticiraniji i ostavljaju sve veće posljedice. No, još je dug put u području otkrivanja i zaštite od Zero day napada. Istraživanja koja trenutno postoje su napravila određen pomak i stvorila smjer u kojem bi se iduće istraživanja mogla razvijati. Nada u rješavanju problematike Zero day napada leži u daljnjim istraživanjima.

Zero day napadi su jedan od najvećih izazova kibernetičke sigurnosti. Štoviše, iz dana u dan sve više napreduju i postaju sve kompleksniji i sofisticiraniji. Nemoguće je u potpunosti se zaštiti od njega ili bilo kojeg drugog kibernetičkog napada. Ali nije nemoguće smanjiti rizik od napada uz pomoć potrebnih mjera, podizanja svijesti i novih istraživanja. Kibernetička sigurnost predstavlja svakodnevnu borbu i potrebu za napretkom kako bi bila u korak s novim tehnologijama i napadima.

7. POPIS LITERATURE

1. Ablon, L., Bogart, A.: **Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits**, RAND Corporation, Santa Monica, CA, 2017.
2. Ablon, L., Libicki, M.C., Golay, A.A.: **Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar**, RAND Corporation, Santa Monica, CA, 2014.
3. Akram, J., Ping, L.: "How to build a vulnerability benchmark to overcome cyber security attacks", **The Institution of Engineering and Technology**, Key Laboratory of Information System Security, School of Software, Tsinghua University China, Beijing, People's Republic of China, 2019.
4. Akritidis, P.; Anagnostakis, K.; Markatos, E.P.: "Efficient Content-Based Detection of Zero-Day Worms", **IEEE International Conference on Communications**, 2005., 837.-843. str.
5. AlEroud, A., Karabatis, G.: „A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks", **International Conference on Cyber Security**, Department of Information Systems, University of Maryland, Baltimore, USA, 2012
6. Bilge, L., Dumitras, T.: "Before We Knew It: An Empirical Study of Zero-Day Attacks in The Real World", **Association for Computing Machinery**, New York, NY, United States, 2012., 833.-844. str.
7. Clark, S., Frei, S., Blaze, M., Smith, J.: "The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities", **Familiarity breeds contempt**, Austin, Texas, 2010.
8. Cohen, F.: "Simulating Cyber Attacks, Defences, and Consequences", **Computer & security**, Sandia National Laboratories, Livermore, CA 94550, USA, 1999.
9. Craigen, D., Diakun-Thibault, N., Purse, R.: "Defining Cybersecurity", **Technology Innovation Management Review**, 2014., 13.-21. str.
10. Egelman, S., Herley, C., van Oorschot, P.C.: "Markets for Zero-Day Exploits: Ethics and Implications", **NSPW '13: Proceedings of the 2013 New Security Paradigms Workshop**, 2013., 41–46.str.
11. Fischer, E.A.: "Cybersecurity Issues and Challenges: In Brief", **Congressional Research Service**, 2016.
12. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: "Dimensions of Cyber-Attacks: Social, Political, Economic, and Cultural", **IEEE Technology and Society Magazine**, 2011., 28.-38. str.

13. Haider, W., Creech, G., Xie, Y., Hu, J.: "Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks", **Future Internet**, 2016.
14. Kadivar, M.: "Cyber-Attack Attributes", **Technology Innovation Management Review**, 2014., 22.-27. str.
15. Kaur, R., Singh, M.: "A Survey on Zero-Day Polymorphic Worm Detection Techniques", **IEEE Communications Surveys & Tutorials**, 2014.
16. Martínez Torres, J., Iglesias Comesaña, C., García-Nieto, P.J.: "Review: machine learning techniques applied to cybersecurity", **International Journal of Machine Learning and Cybernetics**, 2019.
17. Meakins, J.: "A zero-sum game: the zero-day market in 2018", **Journal of Cyber Policy**, 2018.
18. Roscini, M.: **Cyber Operations and the Use of Force in International Law**, Oxford, Oxford University Press, 2014.
19. Shaw, R.S., Chen, C.C., Harris, A.L., Huang, H.J.: "The impact of information richness on information security awareness training effectiveness", **Computers & Education**, 2009.
20. Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H.: "A hybrid layered architecture for detection and analysis of network based Zero-day attack", **Computer Communications**, 2017.
21. Spremić, M., Šimunic, A.: "Cyber security challenges in digital economy", **Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering WCE 2018**, IAENG, Hong Kong, 2018., 341.-347. str.
22. Spremić, M.: **Sigurnost i revizija IS-a u okruženju digitalne ekonomije**, Ekonomski fakultet – Zagreb, Zagreb, 2016.
23. Virvilis, N., Gritzalis, D., Apostolopoulos, T.: "Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?", **2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE 10th International Conference on Autonomic & Trusted Computing**, 2013.
24. Zhang, M., Wang, L., Jajodia, S., Singhal, A., Albanese, M.: "Network Diversity: A Security Metric for Evaluating the Resilience of Networks against Zero-Day Attacks", **IEEE Transactions on Information Forensics and Security**, 2016.

25. Zoppi, T., Ceccarelli, A., Bondavalli, A.: "Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application", **IEEE**, 2021.
26. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Fatih Cetin, F., Basim, H.N.: "Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study", **Journal of Computer Information Systems**, 2020.

OSTALI IZVORI:

1. https://www.thesslstore.com/blog/the-ultimate-guide-to-zero-day-attacks-exploits/
2. https://www.csoonline.com/article/3284084/zero-days-explained-how-unknown-vulnerabilities-become-gateways-for-attackers.html
3. Williams, J.: „What You Need to Know About the SolarWinds Supply-Chain Attack", SANS, 2020., https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/
4. Oladimeji, S., Kerner, S.M.: „SolarWinds hack explained: Everything you need to know", Whaits, TechTarget, 2021., https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know?fbclid=IwAR29SGxn0IQv1dXByH7wIaB0ozwB6Qg6WK3O7CzlVKny5z4NkGm8PFNZS4E
5. Dubey, S.: „SUNBURST: A Vital Case Study of Supply Chain Attack", PureID, 2020., https://www.pureid.io/sunburst-a-vital-case-study-of-supply-chain-attack/
6. Ramakrishna, S.: „New Findings From Our Investigation of SUNBURST", Orange Matter, 2021., https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
7. Jibilian, I., Canales, K.: „The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal", Business Insider, 2021., https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?fbclid=IwAR1P4Lrdppvw0-eoaTUFUWnGCwczCqLDMh_7dD8ST5BjgoPx750o03HAgus

8. Osborne, C.: „Everything you need to know about the Microsoft Exchange Server hack“, Zero Day, 2021., https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/
9. Panettieri, J.: „Microsoft Exchange Server Cyberattack Timeline“, MSSP Alert, 2021., https://www.msspalert.com/cybersecurity-news/microsoft-exchange-hafnium-attack-timeline/
10. Vass, L.: „Exchange Servers Under Active Attack via ProxyShell Bugs“, Threat Post, 2021., https://threatpost.com/exchange-servers-attack-proxyshell/168661/
11. https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/
12. Heller, M.: „Sunburst Hack Costs SolarWinds At Least $18M“, CFO, 2021., https://www.cfo.com/cyber-security-technology/2021/04/sunburst-hack-costs-solarwinds-at-least-18m/
13. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks
14. https://www.openrefactory.com/intelligent-code-repair-icr/

8. POPIS SLIKA

Slika 1 Veza kibernetičke sigurnosti i ostalih područja sigurnosti 10
Slika 2 Kategorizacija ranjivosti 17
Slika 3 Tko je upoznat s ranjivosti? 19
Slika 4 Vremenske linije pozitivnog i negativnog efekta medenog mjeseca 21
Slika 5 Životni ciklus saniranja Zero day ranjivosti 22
Slika 6 Prikaz napada lanca nabave (eng. supply chain attack) 26
Slika 7 Vremenski prikaz Sunburst napada 27
Slika 8 Vremenski tijek Microsoft Exchange napada 30
Slika 9 Prikaz detekcije anomalija preko 3 različita algoritma: a)prikaz anomalija zvjezdicama, b)klasteri, c)statistički, d)bazirani na sličnostima 36
Slika 10 Slojevi otkrivanja Zero day napada 37
Slika 11 Grafički prikaz rezultata treće analize otkrivanja novih Zero day napada uz pomoć vrijednosti anomalija pri preciziranju ocjena sličnosti 43

9. PRILOZI / ŽIVOTOPIS

MARINA TOPLAK

Tijekom zadnjih godina sam se posvetila svom obrazovanju. Iako sam puno naučila, svjesna sam da me pravo znanje tek čeka. Ipak, stručna znanja i vještine se stječu s radom. Posebno se radujem novim izazovima, pa i nepoznanicama za savladati i riješiti.

KONTAKT

Državljanstvo: hrvatsko
Spol: žensko
Adresa: Bjelovarska ulica 23A, 10360 Sesvete, Hrvatska
E-mail: marinatoplak4@gmail.com
Kontakt broj: (+385) 998435581

RADNO ISKUSTVO

2015 – 2020 **SEZONSKI POSAO - Prodavačica slastičarskih proizvoda**
ADRIANA obrt za ugostiteljstvo i proizvodnju - izdvojeni pogon "LEUT"
Živogošće Blato, Hrvatska

- Sezonski posao u ljetnim mjesecima tijekom zadnjih 6 godina Školovanja.
- Rad na blagajni i rad s ljudima.

2014 – 2014 **SEZONSKI POSAO - Konobarica**
Caffe bar Scooby Doo
Igrane, Hrvatska

- Rad na blagajni, posluživanje i rad s ljudima.

DIGITALNE VJEŠTINE

Jako dobro poznavanje
MS Office (MS Word, MS PowerPoint, Ms Excel) / G-Suite Google (Google Meet, Google Docs, Google Forms, Google Disk, itd.) / Komunikacijski programi (Skype, MS Teams, Zoom) / Društvene mreže (Facebook, Instagram, Youtube, LinkedIn)
Dobro poznavanje
Bizagi / MindMeister / MS Outlook
Osnove
R Studio / MS Navision / SAS / Canva / WinAutomation (RPA Software) / Visual Studio (#C) / Moqups

OBRAZOVANJE I OSPOSOBLJAVANJE

2016 – U TIJEKU **MAGISTRA EKONOMIJE**
Sveučilište u Zagrebu - Ekonomski fakultet
Integrirani studij Poslovne ekonomije
Zagreb, Hrvatska

- Smjer: Menadžerska informatika

2012 – 2016 **EKONOMISTICA**
SŠ fra Andrije Kačića Miošića
Ekonomska škola
Makarska, Hrvatska

JEZICI

HRVATSKI	-	materinski
ENGLESKI	-	B2
NJEMAČKI	-	A1

VOZAČKE DOZVOLE

- Dozvola za motorna vozila B kategorije
- Dozvola za voditelja brodice B kategorije

KOMUNIKACIJSKE I MEĐULJUDSKE VJEŠTINE

- Timski rad
- Slušanje
- Analitičko razmišljanje
- Organiziranost
- Emocionalna inteligencija
- Empatija
- Kreativnost
- Racionalnost
- Prilagodljivost
- Savjesnost u poslu

HOBIJI

- Crtanje
- Kuhanje