DIGITALNO INOVACIJSKO STIČIŠČE SLOVENIJE
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA GOSPODARSKI RAZVOJ IN TEHNOLOGIJO
EVROPSKA UNIJA
EVROPSKI SKLAD ZA REGIONALNI RAZVOJ
NALOŽBA V VAŠO PRIHODNOST
Naložbo sofinancirata Republika Slovenija in Evropska unija iz Evropskega sklada za regionalni razvoj.

Zavedanje pomena kibernetske varnosti v letu 2022

Gregor Burger, Digitalno inovacijsko stičišče Slovenija

Povzetek — Povečana potreba po digitalni transformaciji, pandemija virusa Covid-19 ter geopolitične razmere zahtevajo dodatno zavedanje in ukrepanje na področju kibernetske varnosti. V objavi prestavljamo aktivnosti in pobude na ravni Evropske unije kot tudi domače iniciative. Sledi razdelitev in pregled delovanja različnih hekerjev, katerih način delovanja opredeljujemo z barvo klobukov. Nato predstavljamo najbolj pogosto tipe kibernetskih napadov ter objavo zaključujemo s predstavitvijo tvegan spletnih aplikacij po oceni organizacije OWASP.

Ključne besede — digitalna preobrazba, kibernetska varnost, kibernetski napad, heker

Abstract — The increased need for digital transformation, Covid-19 pandemic and geopolitical situation call for increased awareness and action in the field of cyber security. In this publication, we outline the activities and initiatives at European Union level as well as domestic initiatives, followed by a breakdown and overview of the activities of the different types of hackers. We define hackers by the colour of their hats. We then present the most common types of cyber-attacks and conclude the list with a presentation of the most important risks of web applications as assessed by OWASP.

Keywords — Digital transformation, Cyber security, Cyber attack, Hacker

1. UVOD

Digitalna transformacija s prehodom na elektronsko poslovanje družbe povečuje potrebo po zagotavljanju ustrezne ravni kibernetske varnosti. Število kibernetskih napadov in spletnih zlorab se konstantno povečuje na letni ravni, o čemer pričajo podatki primerjave letnih statistik varnostnih organizacij področja kibernetske varnosti. Že samo v letu 2020 so se napadi z izsiljevalsko programsko opremo (angl. Ransomware attack) na letni ravni povečali za 150%, število napadov pa se je v zadnjih dveh letih še dodatno povečalo. V letu 2022 je na dnevni ravni pričakovano 30.000 kibernetskih napadov spletnih strani, 64% podjetij v svetovnem merilu pa je v zadnjem letu doživelo vsaj eno obliko kibernetskega napada. Realno se kibernetski napad na svetovni ravni zgodi vsakih nekaj sekund [1], [2]. Pandemija virusa Covid-19, ki je še pospešila tempo digitalne transformacije, in vojaški konflikt v Ukrajinile le še dodatno povečujeta tveganje kibernetske grožnje.

Grožnja nevarnosti kibernetske varnosti zahteva takojšnje ukrepanje vseh deležnikov, naj si bo to na ravni držav, gospodarstva, organizacij ali pa slehernega uporabnika elektronskih orodij. V Evropski strategiji za kibernetsko varnost [3] Evropska unija izpostavlja odpornost, tehnološko suverenost in EU kot vodilno silo v kibernetski varnosti med poglavitne akcijske točke strategije.

Po podatkih Agencije EU za kibernetsko varnost (ENISA) [4] so najbolj ranljivi, a ob tem kritični elementi:

- javna uprava,
- ponudniki digitalnih storitev,
- splošna javnost,
- zdravstvo,
- finančne in bančne storitve.

V Republiki Sloveniji sledimo aktivnostim EU iniciativ in drugih deležnikov. Na različnih ravneh se pripravljajo programi in iniciative za povečanje kibernetske varnosti. Eden izmed deležnikov področja je Slovenska digitalna koalicija [5], ki snuje nabor programov institucij delujočih na področju kibernetske varnosti, z željo združiti iniciative in informacije za skupnem mestu. Med drugim so to:

- SI-CERT - https://www.cert.si
- Varni na internetu - https://www.varninainternetu.si
- URSIV - https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/
- Strateške skupine za:
  - digitalne kompetence in izobraževanje,
  - digitalno regulativo in okolje,
  - digitalizacijo gospodarstva,
- ter številne delovne skupine.

2. ETIČNI HEKERJI

V medijih pogosto zasledimo novice povezane s hekerji (angl. Hacker), ki so primarno negativne narave. Novice poročajo o vdorih v poslovne

sisteme, podjetja, krajah podatkov, kraji denarja, kraji kripto valut, izsiljevalskih napadih, napadih na infrastrukturo itd. Niso pa vsi hekerji enaki, primarno jih delimo v tri skupine. [6], [7]. Pogosto za njihovo ločitev uporabljamo prispodobo s klobuki (angl. Hat), belimi, sivimi in črnimi klobuki. Vsaka barva tako imenovanega klobuka predstavlja določen tip delovanja hekerjev.

2.1. Hekerji s črnimi klobuki

Hekerji s črnimi klobuki (angl. Black hat hacker) so, kot vsi hekerji, strokovnjaki za vdiranja v računalniške mreže in izogibanje varnostnim protokolom. Snujejo škodljivo programsko opremo, ki jim omogoča dostop do računalniških mrež, računalnikov in mobilnih naprav preko katerih zbirajo informacije o svojih žrtvah. Njihova motivacija je pogosto želja po pridobitvi osebne finančne koristi, pridobivanje tajnih podatkov ali izvajanju protestov. Številni hekerji nezakonito pridobljene podatke prodajo na črnem trgu ali pa delujejo z namenom povzročitve direktne škode.

Informacije o hekerji s črnimi klobuki najpogosteje zasledimo v medijih pri prebiranju novic o vdorih v podatkovne shrambe, kraji osebnih in finančnih podatkov, podatkov zdravstvenega zavarovanja, različna gesla in podatke za dostop. Tarče smo lahko vsi, posamezniki, podjetja, organizacije, vlade itd. Kot že omenjeno je motivacija za vdore finančna korist, izsiljevalskih namenov, osramotitev izbrane organizacije itd.

2.2. Hekerji s sivimi klobuki

Hekerje s sivimi klobuki (angl. Grey hat hacker) uvrščamo med hekerje z belimi in črnimi klobuki. Čeprav njihov primarni namen ni povzročanje škode oz. kraja podatkov, pri svojem delu pogosto delujejo brez dovoljenja lastnikov omrežja ali sistema. V primeru najdenih napak ali ranljivosti omrežja oz. sistema bodo od lastnika zahtevali finančno plačilo za odpravo napak in pomanjkljivosti. Včasih nove odkrite ranljivosti objavijo na spletnih omrežjih in lahko povzročijo večje varnostne težave do oprave njihovih pomanjkljivosti. Predvsem pa želijo za svoje delo prejeti finančno kompenzacijo.

2.3. Hekerji z belimi klobuki

Hekerji z belimi klobuki(angl. White hat hacker) so prav tako vešči vdiranja v računalniške sisteme in izrabljanje varnostnih lukenj. Pogosto jih imenujemo tudi etični hekerji, saj svoje delo izrabljajo za odpravljanje ranljivosti v sistemih. Kot strokovnjaki za kibernetsko varnost delujejo za podjetja in organizacije, ki skrbijo za varnost računalniških sistemov in storitev. Predvsem pa so specializirani za odkrivanje potencialnih varnostnih pomanjkljivosti.

Čeprav uporabljajo enake metode in znanje kot hekerji s črnimi klobuki, se od njih razlikujejo v enem pomembnem dejstvu. Svoje delo opravljajo z dovoljenjem lastnikov sistema, izvajajo penetracijske teste in varnostne preglede sistemov ter s tem omogočajo njihovo varno uporabo. Pogosto pa so zaposleni tudi v nacionalnih varnostnih agencija.

3. VRSTE KIBERNETSKIH NAPADOV

Področje kibernetske varnosti je široko in obravnava celotnega področja presega okvire te objave. Naštejmo le nekaj najbolj pogostih tipov kibernetskih napadov [8].

Botneti so omrežja računalnikov okuženih z zlonamerno kodo, ki delujejo pod kontrolo hekerjev. Okužbe je pogosto zelo težko zaznati, saj računalniki na videz delujejo brez posebnosti, a prikrito pošiljajo ne željeno pošto, razširjajo zlonamerno kodo ali pa so del napadov zavrnitve storitev (angl. Destributed denial of service – DDoS attack).

Distribuirani napadi zavrnitve storitev (Destributed denial of service – DdoS attack) so napadi botnetov na spletni strežnik, pri čemer s svojimi zahtevami za storitve povzročijo preobremenitev strežnika, ki posledično preneha izvajati storitve ali zaradi prekomerne obremenitve postane nedosegljiv. Obstajajo posebni protokoli in načini za zaznavanje ter zmanjšanje nevarnosti DDoS napadov.

Hacking je postopek s katerim nekdo ali nekaj pridobi nepooblaščen dostop do računalnika ali druge naprave. Napadalec skuša izrabiti varnostne pomanjkljivosti sistema in pridobiti dostop do zasebnih informacij, vriniti škodljivo kodo ali podatke.

Malware je škodljiva programska koda, ki okuži napadeni računalnik. Vključuje lahko računalniške viruse, trojanske konje in oglaševalsko programsko kodo. Koda omogoča hekerju pridobitev nadzora nad okuženo napravo ali pa dostop do zasebnih podatkov.

Pharming je pogost način spletne prevare. Uporabnika spletne strani se preusmeri k uporabi zlonamerne spletne strani pri čemer se spletna stran predstavlja kot zakonita spletna stran.

Phising je metoda s katero spletni prevaranti želijo pridobiti uporabnikove podatke, pri tem se

pretvarjajo, da so uradne storitve ali podjetja. Od uporabnika želijo pridobiti osebne podatke, gesla za dostop do storitev ali pa bančne podatke.

Ramsomware je tip škodljive kode, ki omeji dostop do uporabnikove naprave. Uporabnik ne more dostopati do naprave, podatki na napravi postanejo kriptirani in posledično niso več dostopni uporabniku. Za ponoven dostop do podatkov in naprave je pogosto potrebno plačati neko odškodnino.

Spam oz nezaželena elektronsko pošta je ena najbolj znanih metod za razširjanje ali zbiranje informacij o ljudeh. Masovno se pošiljajo elektronska sporočila polna oglasov ali spletnih poveza, ki omogočajo druge tipe kibernetskih napadov.

Spyware so programi, ki zbirajo osebne podatke uporabnikov brez uporabnikove vednosti. Programi so pogosto del drugih programov, ki jih uporabniki prenesejo iz svetovnega spleta. Zbrani podatki se posredujejo napadalcu ali pa se uporabniku prikazujejo neželeni oglasi.

Virusi so škodljivi računalniški programi, pogosto se razširjajo kot priponke elektronskih sporočil. Njihove delovaje je različno, ali omogočajo nepooblaščen dostop do računalnikov, pošiljajo neželeno elektronsko pošto, zbirajo osebne podatke, onemogočajo varnostne nastavitve in podobno.

Spleti črvi (angl. Worms) delujejo avtonomno v spominu naprave in se skušajo razširiti na druge naprave v omrežju katerega del je okužena naprava.

Industrijski IoT napadi so napadi na industrijska omrežja in njihove IoT (Internet of Things) naprave z namenom povzročanja izpadov delovanja, prevzema nadzora omrežja, zbiranja podatkov ali industrijskega vohunjenja. Tipični primeri takšnih napadov so napadi na energetska omrežja.

4. TVEGANJA SPLETNIH APLIKACIJ

Digitalna transformacija in povečano elektronsko poslovanje zahteva dodatno skrb za varnost spletnih aplikacij. Pomena kibernetske varnosti se zavedamo tudi na DIH-u Slovenije, kjer je podjetjem na voljo vavčer digitalne varnosti. Vavčer omogoča penetracijske teste aplikacij in varnostne preglede sistemov [9]. Specializirane organizacije skrbijo za preučevanje, ozaveščanje, preprečevanje in opravljanje kibernetske nevarnosti. Ena izmed takšnih organizacij je tudi OWASP [10]. Predstavljamo povzetek spiska najbolj pogostih varnostnih tveganj spletnih aplikacij organizacije OWASP [11].

Vrivanje (angl. Injection) je napaka, pri kateri spletna aplikacija ne preveri vhodnih podatkov t.i. vhodnega parametra ali spletnega obrazca, preden se podatki posreduje v izvedbo na strežniku podatkovnih baz. Vrivanje omogoča napadalcu nepooblaščen dostop do občutljivih in zaupnih podatkov ali pa morebitno pridobitev administratorskih pravic nad podatkovno bazo.

Napaka pri avtentikaciji in upravljanju sej (angl. Autrehntication) je napačna implementacija funkcionalnosti preverjanja pristnosti in upravljanja sej. Aplikacija ne uspe zaščititi poverilnic ali žetonov seje pri njenem delovanju. Uspešna izvedba napada omogoča krajo uporabniških podatkov za prijavo ali ponarejanje podatkovne seje, s čemer je mogoče pridobiti nepooblaščen dostop do spletnega mesta.

Izpostavljenost občutljivih podatkov (angl. Sensitive data exposure) je napaka pri kateri aplikacija ne zaščiti občutljivih podatkov, naj si bo to zaradi različnih ranljivosti sistema, malomarnosti skrbnikov itd. Posledično pride do razkritja podatkov med katerimi so lahko tudi osebnih podatkov in drugi podatki, ki morajo biti zakonsko zaščiteni.

Zunanje entitete XML (XXE) (angl. XML external entities) je ranljivost, ki napadalcu z vrivanjem zunanjih XML entitet omogočajo poseganje v način obdelovanja XML datoteke v aplikaciji. Z vrivanjem XML datoteke napadalec lahko pridobi dostop do lokalno shranjenih podatkov ali izvede napad na druge notranje sisteme.

Napačen nadzor dostopa (angl. Broken access control) je napaka avtorizacije uporabnika, ki nakazuje nepravilno implementacijo dovoljen aktivnosti overjenega uporabnika. Posledica so zavračanje dostopa upravičenim uporabnikom ali pa omogočanje dostopa nepooblaščenim uporabnikom.

Napačna varnostna konfiguracija (angl. Security misconfiguration) se opredeljuje kot nepravilno izvajanje vseh varnostnih kontrol na strežniku ali v spletni aplikaciji. Druga možnost je izvajanje varnostne kontrole s pomanjkljivostmi. Pomanjkljivost potencialno vodi do kraje ali spremembe podatkov in splošne ogroženosti sistema.

Vrivanje skriptne kode (XSS) (angl. Cross-site scripting) je ranljivost, ki naslavlja interakcijo med uporabniki in ranljivo spletno aplikacijo. Napad se izvede na strani odjemalca, z vrivanjem zlonamerne kode v kodo spletnega mesta, z namenom vplivanja na spletno aplikacijo in njene končne uporabnike.

Posledica je potencialna kraja osebnih podatkov, kraja sejnih piškotov in poverilnic ter prevzem identitete.

(Ne)varna deserializacija (angl. Insecure deserialization) je ranljivost, ko se z nepreverjenimi podatki zlorabi logika aplikacije. Uspešno izveden napad omogoča napadalcu oddaljeno izvajanje kode, zaobiti mehanizme preverjanja dostopa do podatkov ter v določeni primerih celo napade onemogočanje storitev.

Uporaba komponent z znanimi ranljivostmi (angl. Using components with known vulnerabilities) so pomanjkljivosti uporabljenih komponent, ki so bile zaznane že v preteklosti. Potrebna je skrb za implementacijo obstoječih popravkov in dopolnitev ali pa zamenjavo ranljivih komponent.

Nezadostno beleženje in spremljanje (angl. Insufficient logging & monitoring) pomeni nepravilno beleženje varnostih kritičnih dogodkov. Pomanjkanje beleženja dogodkov oteži odkrivanje zlonamernih dejavnostih in vpliva na učinkovito obvladovanje incidentov. Pravočasno odkrivanje kibernetskih napadov znižuje povzročene stroške škode potencialnih kibernetskih napadov.

LITERATURA

[1] https://techjury.net/blog/how-many-cyber-attacks-per-day/ (prvi dostop: 1.3 . 2022)

[2] https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-/ (prvi dostop: 1.3 . 2022)

[3] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies#ecl-inpage-kmq7bt98 (prvi dostop: 16. 3. 2022)

[4] https://www.europarl.europa.eu/news/sl/headlines/society/20220120STO21428/kibernetska-varnost-najnevarnejse-in-rastoce-groznje-infografika (prvi dostop: 16. 3. 2022)

[5] https://digitalna.si/ (prvi dostop: 16. 3. 2022)

[6] https://us.norton.com/internetsecurity-emerging-threats-black-white-and-gray-hat-hackers.html (prvi dostop: 3. 3.2022)

[7] https://www.globaltechcouncil.org/cyber-security/white-hat-vs-black-hat-vs-grey-hat-hacker/ (prvi dostop: 3. 3.2022)

[8] https://techjury.net/blog/cyber-security-statistics/ (prvi dostop: 1.3 . 2022)

[9] https://dihslovenia.si/vavcerji/vavcer-za-kibernetsko-varnost (prvi dostop: 3. 3.2022)

[10] https://owasp.org/ (prvi dostop: 3. 3.2022)

[11] https://owasp.org/www-project-top-ten/ (prvi dostop: 3. 3.2022)