Vysoké učení technické v Brně
Fakulta informačních technologií

Typografie a publikování – 4. projekt

Kybernetická bezpečnosť

24. júna 2023 Stanislav Letaši

1 Úvod

Bezpečnosť na internete je téma, ktorá v dnešnom digitálnom svete nadobúda každým dňom stále väčšiu podstatu. V dnešnej dobe je internet integrovaný do každodenného života čoraz viac, čo znamená, že ľudia sa musia učiť chrániť si svoje osobné údaje pred neoprávneným prístupom.

2 Ako sa ochrániť

Výskumníci z oblasti kybernetickej bezpečnosti zdôrazňujú, že je dôležité používať aktualizovaný antivírusový software a firewall pre ochranu počítača pred útokmi z internetu [5]. Taktiež spomínajú, že chrániť si svoje citlivé informácie pomocou silných hesiel a správneho šifrovania je v dnešnej dobe nevyhnutné. Slabé heslá môžu byť totiž častokrát zneužité hackermi, ktorí dokážu pomocou slovníkového útoku získať prístup na osobný účet napadnutej osoby, alebo do systému cieľovej organizácie [4]. *Journal of Cybersecurity* zverejnil článok, v ktorom sa autori zaoberajú problematikou vytvárania bezpečných hesiel na internete [10]. Štúdia Oxfordskej univerzity, ktorú článok spomína zistila, že väčšina ľudia je v dnešnej dobe oveľa viac obozretná, a dbajú na vytváranie si silnejších hesiel a nepoužívanie rovnakého hesla na viacerých stránkach.

3 Wiper malware

V roku 2022 boli pre digitálny svet najväčšou hrozbou takzvané „wiper attacks“. Ako je spomenuté v článku z *Infosecurity Magazine* [6], „wipers“ sú formou malware, ktorý nenávratne prepisuje dáta. Tieto útoky boli využité niektorými hackerskými skupinami pre finančný zisk tým, že sa vyhrážali postupným vymazaním systému, pokiaľ im napadnutá strana nevyplatí žiadané výkupné.

4 Nové technológie

Ziska Fields v svojej knihe [3] spomína, že v dnešnej dobe rýchleho vývoja technológií, ktoré sú súčasťou „štvrtej priemyselnej revolúcie“ je kybernetická bezpečnosť stále dôležitejšia. Taktiež zdôrazňuje potrebu rozvoja nových zabezpečovacích opatrení a technológií, ktoré budú schopné ochrániť všetky aspekty kybernetickej bezpečnosti.

Za posledné roky sa kybernetické útoky stávajú viac sofistikované a útočníci začínajú využívať stále novšie technológie a metódy. Preto je dôležité, aby organizácie neustále aktualizovali svoje bezpečnostné opatrenia a sledovali aktuálne trendy v oblasti kybernetickej bezpečnosti. Podľa *Forbes* článku *Top Cybersecurity Predictions 2023* [8] bude rozvoj Secure access service edge a Zero Trust Adoption najväčšími pokrokmi tohto roku v oblasti kybernetickej bezpečnosti.

5 SASE a Zero Trust

Secure access service edge - SASE, je nové riešenie pre prepojenie sietí a ochranu pred bezpečnostnými hrozbami [1]. SASE poskytuje užívateľom bezpečný priamy prístup ku cloudu, bez nutnosti pripájania sa prostredníctvom MPLS alebo VPN, a ponúka užívateľom bezpečnú bránu pre webové služby, izoláciu vzdialeného prehliadača a taktiež prevenciu prienikov.

Zero trust je prístup ku kybernetickej bezpečnosti, ktorý vychádza z myšlienky, že žiadne pripojenie k firemným sieťam a systémom by nemalo byť považované za dôveryhodné [7]. Model zero trust vyžaduje overenie užívateľov, zariadení a systémov pred pripojením a opakované overovanie pri prístupu k sieťam, systémom a dátam. Podľa nedávnych správ sa stále viac organizácií rozhoduje pre prístup zero trust, a percento organizácií prechádzajúcich k tomuto prístupu bude naďalej len rásť.

6 Stále nebezpečenstvo Phishing útokov

Aj napriek nespočetným technológiám na ochranu bezpečnosti užívateľov a spoločností je jeden z najčastejších spôsobov ako útočníci získajú prístup do systému phishing. Phishing útok je forma sociálneho inžinierstva, v ktorej sa útočník vydáva za dôveryhodnú osobu a snaží sa od obete získať citlivé informácie alebo prístup do zabezpečeného systému [2]. V snahe zabrániť týmto útokom bolo vyvinutých veľa ochranných systémov, najnovšie systémy používajúce umelú inteligenciu na rozpoznanie varovných signálov nachádzajúcich sa vo phishingových správach [9].

7 Záver

S vývojom nových technológií na ochranu pred kybernetickými útokmi bohužiaľ prichádzajú aj nové spôsoby ako tieto ochrany obísť. Neopatrnosť len jedného človeka môže viesť napríklad k napadnutiu vnútorného systému spoločnosti, v ktorej pracuje. Preto je stále relevantné zostať obozretný a riadiť sa základnými pravidlami internetovej bezpečnosti, ako používanie silných hesiel, vyhýbanie sa podozrivým stránkam a sťahovanie súborov z neoverených zdrojov.

Literatúra

[1] Chen, R.; Yue, S.; Zhao, W.; aj.: Overview of the Development of Secure Access Service Edge. In *Signal and Information Processing, Networking and Computers: Proceedings of the 10th International Conference on Signal and Information Processing, Networking and Computers (ICSINC)*, 52 Huayuan Bei Lu, Beijing, China: Springer, 2023, ISBN 978-981-19-9967-3, s. 138–145, dostupné z: `https://link.springer.com/chapter/10.1007/978-981-19-9968-0_17`.

[2] Dohnal, V.: *Microservices for Automated Threat Response to Phishing*. Bakalářská práce, Fakulta Informatiky MUNI v Brně, Brno, Česká Republika, 2022, dostupné z: `https://is.muni.cz/th/e58fc/`.

[3] Fields, Z.: *Handbook of research on information and cyber security in the fourth industrial revolution*. University of KwaZulu-Natal, South Africa: IGI Global, první vydání, 2018, ISBN 9781522547631, dostupné z: `https://www.academia.edu/38987286/Handbook_of_Research_on_Information_and_Cyber_Security_in_the_Fourth_Industrial_Revolution`.

[4] Hodes, V.: *Moderní kybernetické útoky*. Bakalářská práce, Fakulta informačních technologií VUT v Brně, Brno, Česká Republika, 2015, dostupné z: `https://www.vut.cz/studenti/zav-prace/detail/85240`.

[5] Johnson, T. A.: *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. St.Louis,Missouri, USA: CRC Press, první vydání, 2015, ISBN 9781482239232, dostupné z: `bit.ly/41d3l22`.

[6] Poireault, K.: A new tool in the cyber-criminals' playbook. *Infosecurity Magazine*, ročník 20, č. 1, 2023: s. 9–11, ISSN 1754-4548, dostupné z: `https://bit.ly/3mwQHMv`.

[7] Pratt, M. K.: The history and evolution of zero-trust security [online]. *techtarget*, 10 2022, dostupné z: `https://bit.ly/3mC7eyB`.

[8] Sayegh, E.: Top Cybersecurity Predictions 2023 [online]. *Forbes*, 12 2022, dostupné z: `https://www.forbes.com/sites/emilsayegh/2022/12/15/top-cybersecurity-predictions-2023/?sh=6c5e73ef1d09`.

[9] Sennovate: The Role of Artificial Intelligence in Detecting Phishing Attacks [online]. *Sennovate*, 1 2023, dostupné z: https://bit.ly/3MHrR7a.

[10] Wash, R.; Rader, E.: Prioritizing security over usability: Strategies for how people choose passwords. *Journal of Cybersecurity*, ročník 7, č. 1, 06 2021, ISSN 2057-2085, dostupné z: https://academic.oup.com/cybersecurity/article-pdf/7/1/tyab012/38462200/tyab012.pdf.