

TRENDS AND PRACTICES IN COLLEGE CYBERSECURITY

TRENDY A POSTUPY V KYBERNETICKEJ BEZPEČNOSTI VYSOKÝCH ŠKÔL

Andrej Štefánik a Martin Kučerka

Abstract

The introduction of modern technology into the academic environment brings with it not only new opportunities but also an increased risk of cyber-attacks. Universities now find themselves on the front line of defense against increasingly sophisticated threats to the integrity of their information systems and the confidentiality of academic data. This paper focuses on current trends and challenges in cybersecurity in higher education. We analyze the various strategies that universities are adopting to protect their IT infrastructures, including carefully tuning existing technologies, implementing new security solutions, and changing the security awareness of all stakeholders – students, employees, and management.

Key words: *Cyber security, security technology, virus, firewall*

Abstrakt

Zavádzanie moderných technológií do akademického prostredia prináša so sebou nielen nové možnosti, ale aj zvýšené riziko kybernetických útokov. Univerzity sa v súčasnosti ocitajú v prvej línii obrany proti čoraz sofistikovanejším hrozbám, ktoré ohrozujú integritu ich informačných systémov a dôvernosť akademických dát. Tento príspevok sa zameriava na aktuálne trendy a výzvy v oblasti kybernetickej bezpečnosti na vysokých školách. Analyzujeme rôzne stratégie, ktoré univerzity prijímajú na ochranu svojich IT infraštruktúr, vrátane dôkladného nastavenia existujúcich technológií, implementácie nových bezpečnostných riešení a zmeny bezpečnostného povedomia všetkých zainteresovaných strán - študentov, zamestnancov a vedenia.

Kľúčové slová: *Kybernetická bezpečnosť, bezpečnostné technológie, vírus, firewall*

ÚVOD – VYMEDZENIE ZÁKLADNÝCH POJMOV KYBERNETICKEJ BEZPEČNOSTI

GDPR Slovensko (2024) vymedzuje kybernetickú bezpečnosť ako ochranu systémov, sietí a dát, pred rôznymi digitálnymi útokmi. Tieto útoky môžu byť zamerané na získanie prístupu k citlivým informáciám, ich zmenu alebo zničenie, vydieranie používateľov alebo prerušenie bežných operácií. V dnešnej dobe, kedy sú organizácie a univerzity čoraz viac závislé na digitálnych technológiách, je kybernetická bezpečnosť kľúčová na ochranu informácií a zaručenie dôveryhodnosti a integrity systémov. Kybernetickú bezpečnosť si môžeme vysvetliť a vnímať ako aj digitálne zabezpečenie, je postupom ochrany digitálnych informácií, zariadení a aktív. Patria sem vaše osobné informácie, kontá, súbory, fotografie a dokonca aj peniaze. Definovanie kybernetickej bezpečnosti môžeme z viacerých zdrojov či autorov, ale myslíme si, že všetky vedú k jednotnosti slova ochrana, prevencia, zabezpečenie, zábezpeka k všetkým štruktúram organizácie a ľudí pracujúcich v nej. Podľa uznávanej spoločnosti Microsoft by sme chceli uviesť do problematiky ďalší pojem CIA (Microsoft, 2024), „ktorý sa používa na znázornenie troch pilierov kybernetickej bezpečnosti, t. j.

Confidentiality (Dôvernosť) - uchovávanie tajomstiev a zabezpečenie, že k vašim súborom a kontám budú mať prístup iba oprávnení ľudia. Integrity (Integrita) – uistenie sa, že vaše informácie sú také, aké majú byť, a že nikto bez vášho povolenia nič vložil, upravil ani neodstránil. Môžeme napríklad zlomyseľne zmeniť číslo v tabuľkovom hárku. Access (Prístup) – zabezpečenie prístupu k informáciám a systémom v prípade potreby. Príkladom problému s prístupom by bol útok odmietnutia služby (DNS), pri ktorom útočníci zaplavia váš systém sieťovými prenosmi, aby k nim bol takmer nemožný prístup, alebo útok prostredníctvom ransomvéru, ktorý zašifruje systém a zabráni v jeho používaní.“

Stotožňujeme sa s názorom, že kybernetickú bezpečnosť tvoria tri hlavné časti dôvernosť, integrita a prístup. Aké je prepojenie kybernetickej bezpečnosti a kybernetického útoku? Cieľom kybernetických útokov je poškodiť alebo získať kontrolu či prístup k dôležitým dokumentom a systémom v rámci podnikovej alebo osobnej počítačovej siete. Kybernetické útoky šíria jednotlivci alebo organizácie s politickým, kriminálnym alebo osobným zámerom zničiť utajované informácie alebo k nim získať prístup. Používanie spoľahlivého softvéru a stratégie kybernetického zabezpečenia môže znížiť pravdepodobnosť, že dôjde k zasiahnutiu podnikovej alebo osobnej databázy kybernetickým útokom. Kybernetický útok je úmyselný pokus jednej osoby alebo organizácie o narušenie informačného systému inej osoby alebo organizácie. Útočník zvyčajne dúfa, že narušením siete obete niečo získa (isvs.cz, 2023). Kybernetický útok môžeme ešte definovať ako „akékoľvek protiprávne jednanie útočníka v kyber-priestore, ktoré smeruje proti záujmu inej osoby“ (Kolouch, 2016, s. 55).

Už teraz vieme povedať, že kybernetická bezpečnosť je ochranný mechanizmus kybernetického útoku a vedie k ochrane majetku, dát, osôb a spoločnosti. Pre lepšie objasnenie akými rôznymi druhmi môže byť kybernetický útok vedení, zobrazíme si na Obr. 1.



Obr. 1 – Kybernetické útoky (Zdroj: vlastné spracovanie)

Každý jeden druh hackerského útoku má svoje špecifiká, na ktoré sa treba pripraviť a mať svoju stratégiu na jeho odolávanie. Aké sú možnosti ochrany a prípadne nastavovania IKT pre útokmi sa dozvieme v ďalšej podkapitole.

1 OCHRANA A NASTAVENIA IKT PRED ÚTOKMI

Predmetná kapitola sa bude venovať možnými spôsobmi obranného mechanizmu pred hackerskými útokmi na univerzite. Bližšie si definujeme ako zabezpečiť siete či nasadiť antivírusové programy.

1.1 ZABEZPEČENIE SIETE AKO SPÔSOB OCHRANY

V tejto časti sa zaoberáme problematikou zabezpečenia siete aby sa čo najlepšie ochránili pred hackerskými útokmi. Segmentácia siete podľa (definícia z technológie - zabezpečenia, 2024) je „*myšlienka vytvorenia podsiete v rámci podnikovej siete alebo nejakého iného typu celkovej počítačovej siete. Segmentácia siete umožňuje zamedziť výskytu škodlivého softvéru a iných hrozieb a môže zvýšiť efektívnosť z hľadiska výkonu siete.*“

Natovanie siete podľa (Cisco, 2023) je služba, ktorá funguje na smerovači na pripojenie súkromných sietí k verejným sieťam (internet). Organizácia s NAT potrebuje jednu IP adresu alebo jednu obmedzenú verejnú IP adresu, aby reprezentovala celú skupinu zariadení, ktoré sa pripájajú mimo svojej siete. Ďalší krok po nastavení segmentovania a natovania siete je kúpa a fyzické osadenie, nastavenie perimetrových firewallov a sieťových sond.

Perimetrový firewall môže fungovať aj ako proxy služba, sprostredkovateľ medzi používateľmi a internetom, ktorý umožňuje administrátorovi väčšiu kontrolu prístupu. Keď cez perimetrový firewall prechádza obsah dátového paketu, dokáže ho prečítať a na základe informácií v hlavičke paketu a obsahu samotného paketu zistiť, či obsahuje hrozbu. Perimetrový firewall dokáže filtrovať ako aj internú tak aj externú prevádzku. Perimetrový firewall funguje ako bariéra aj ako vstupný bod do internetu alebo internej siete. Perimeter siete môžeme zabezpečiť perimetrovým zariadením, ako je firewall ale aj virtuálnou súkromnou sieťou (VPN) (Fortinet, 2024).

Ďalším krom ku bezpečnosti ktorý musíme nasadiť a nastaviť je pripájanie sa do univerzity a systémov univerzít pomocou technológie VPN. VPN z anglického slova virtual private network je technológia, ktorá umožňuje vytvoriť bezpečné a šifrované spojenie medzi zariadením a internetom. Všetky údaje, ktoré odosielate a prijímate v tejto sieti, sú chránené pred neoprávneným prístupom a sledovaním. VPN funguje spôsobom, že vaše internetové údaje presmeruje cez server VPN, ktorý vám poskytne novú IP adresu, vďaka čomu zostane vaša skutočná poloha a identita ukrytá (ESET, 2024). Ak sa správcovi podarí úspešne nasadiť a ochrániť zabezpečenie perimetra a tam kde je to možné a nevyhnutné použiť technológiu pripojenia klientov cez VPN bude správca potrebovať a aplikovať sieťové sondy a funkcie protokolovania a monitorovania. Sieťové sondy, sieťová sonda je kriticke potrebným nástrojom pre správcov siete na monitorovanie výkonu siete v reálnom čase. Funguje ako doručovateľ, doručuje otázky sieťovým zariadeniam a získava údaje na analýzu pomocou softvéru na monitorovanie siete. Sondy pomáhajú predchádzať úzkym miestam, spomaleniam a prestojom poskytovaním informácií o sieti takmer v reálnom čase, čo umožňuje správcovi rýchlo konať. Keď sonda otestuje zariadenie, dostane akékoľvek údaje, ktoré výrobca a správca siete tohto zariadenia sprístupnil a nastavil. Sonda vracia tieto údaje späť do vašej aplikácie na monitorovanie siete v reálnom čase. Ak dôjde k prekročeniu niektorej z prednastavených prahových hodnôt výkonu, sonda vykoná vami zadané akcie, napríklad spustí alarm alebo automatickú aktivitu. (Jackson, 2024)

Protokolovanie je veľmi dôležitý proces zaznamenávania udalostí a aktivít, ktoré sa vyskytujú v zariadení alebo aplikácii. Akákoľvek udalosť ako sú prihlásenia používateľov, systémové chyby, zlyhania aplikácie, zmeny povolení a ďalšie sa zaznamená do systému alebo aplikácie vo forme denníkov. Protokolovanie tieto protokoly a údaje systematicky zaznamenáva a spravuje, aby sa dali použiť na riešenie problémov, ako aj na prevádzkové a bezpečnostné účely. Protokolovanie nám zhrnie všetky výstupy z našich bezpečnostných zariadení a nasadených systémov. Tým pádom správca dostane ihneď prehľad o svojej organizácii a jej bezpečnosti a vie vo veľmi krátkom čase reagovať, spraviť nápravu alebo vykonať akciu proti prebiehajúcejmu útoku.

Monitorovanie poskytne správcovi podrobný prehľad o jeho sieťových prvkoch, aplikáciách a serveroch. Správca monitorovanie potrebuje nasadiť aj z dôvodu že sieťové prvky aplikácie a servery majú veľa funkčných častí, príliš veľa na to, aby ich správca mohol sledovať 24 hodín denne a 7 dní v týždni. Hlavným cieľom použitia monitorovacieho nástroja je rozpoznať problém a poslať informáciu danému správcovi systému, že ho má opraviť skôr, ako dôjde ku otvoreniu cesty pre hackerský útok alebo znefunkčneniu služby a systému.

1.2 ANTIVÍRUSOVÝM RIEŠENÍM PRED KYBERNETICKÝM ÚTOKOM

Ako sme si už vyššie spomínali, pred kybernetickým útokom je možné sa chrániť správnym zabezpečením siete ale i antivírusovým programom/softvérom.

Antivírusový softvér (antivírusový program) je bezpečnostný program určený na prevenciu, detekciu, vyhľadávanie a odstraňovanie vírusov a iných typov škodlivého softvéru z počítačov, sietí a iných zariadení. Antivírusový program, ktorý sa najčastejšie inštaluje do počítača ako proaktívny prístup ku kybernetickej bezpečnosti, môže pomôcť zmierniť rôzne kybernetické hrozby napríklad: únoscov prehliadača, trójskych koní, červov, rootkitov, spywaru, adwaru, botnetov, pokusov o phishing a útokov ransomware.

Antivírusový softvér (Jovanović, 2019) zvyčajne beží na počítači ako proces na pozadí, skenuje počítač, servery alebo mobilné zariadenia, aby zistil a obmedzil šírenie malvéru. Mnohé antivírusové softvérové programy zahŕňajú detekciu a ochranu hrozieb v reálnom čase na ochranu pred potenciálnymi zraniteľnosťami a vykonávajú kontroly systému, ktoré monitorujú zariadenia a systémové súbory a hľadajú možné riziká.

Antivírusový softvér zvyčajne vykonáva tieto základné funkcie:

- Skenuje adresáre alebo špecifické súbory proti knižnici známych škodlivých podpisov, aby zistil abnormálne vzory naznačujúce prítomnosť škodlivého softvéru.
- Umožňuje používateľom naplánovať kontroly, aby sa spúšťali automaticky.
- Umožňuje používateľom kedykoľvek spustiť nové kontroly. Odstráni všetok škodlivý softvér, ktorý zistí buď automaticky na pozadí, alebo upozorní používateľov na infekcie a vyzve ich, aby vyčistili súbory. Na komplexné skenovanie systémov musí mať antivírusový softvér vo všeobecnosti privilegovaný prístup k celému systému.

Okrem základného balíka a služieb antivírusového programu ktoré sme si popísali vyššie je v dnešnej dobe nevyhnutné aby si univerzita zakúpila a nasadila služby ako sú: XDR, EDR, MDR, SIEM, SOAR. Sú to nové nástroje a služby kybernetickej bezpečnosti ktoré by si mal každý správca a univerzita nasadiť z dôvodu častých

a sofistikovaných hackerských útokov ktoré na univerzity prebiehajú. (*EDR vs. XDR vs. SIEM vs. MDR vs. SOAR*. Sysdig , 2024)

- EDR (Endpoint Detection and Response) je nástroj, ktorý zisťuje, skúma a reaguje na pokročilé hrozby pre koncové body. Má dopĺňať nedostatky tradičných riešení ochrany koncových bodov z hľadiska predchádzania všetkým útokom. Funkcia EDR má úplný prehľad o všetkých aktivitách koncových bodov súvisiacich so zabezpečením. Okrem iného zaznamenáva sieťové pripojenia, spúšťanie procesov, načítanie ovládačov, zmeny registrov, prístup na disk, prístup do pamäte a zmeny v registroch.
- XDR (Extended Detection and Response) je bezpečnostné riešenie, ktorého účelom je identifikovať, skúmať a reagovať na pokročilé hrozby, ktoré pochádzajú z rôznych zdrojov vrátane cloudu, sietí a e-mailu. Integruje údaje z viacerých bezpečnostných systémov s cieľom zlepšiť viditeľnosť hrozieb a skrátiť čas potrebný na zistenie a reakciu na útok.
- SIEM (Security Information and Event Management) nástroj pre správu bezpečnostných informácií a udalostí , ktorý pomáha podnikom identifikovať, hodnotiť a reagovať na bezpečnostné hrozby. Poskytuje centralizovaný prehľad pre všetky dáta súvisiace s bezpečnosťou, vyžaduje sa aby organizácia monitorovala systémy a hlásila podozrivé aktivity. SIEM obsahuje aj forenzné vyšetovanie a možnosti nahlasovania súladu, ktoré sú nevyhnutné pre reakciu na incidenty a dodržiavanie predpisov.
- MDR (Managed Detection and Response) je služba kybernetickej bezpečnosti a zvyčajne sa skladá z kombinácie technológií, procesov a ľudí, ktorí spolupracujú pri zisťovaní a reagovaní na kybernetické hrozby. Je navrhnutý tak, aby poskytoval nepretržitú ochranu pred kybernetickými hrozbami, ich detekciu a reakciu. Riešenia MDR využívajú strojové učenie na skúmanie, varovanie a potláčanie kybernetických hrozieb vo veľkom rozsahu.
- SOAR (Security Orchestration, Automation, and Response) je softvérový balík, ktorý umožňuje spoločnosti zhromažďovať informácie o bezpečnostných hrozbách a reagovať na bezpečnostné udalosti bez potreby ľudského zásahu.

Ak sa univerzite podarí nakúpiť a nasadiť vyššie popísané doplnky k antivírusovému programu, správca zaznamená výrazné zníženie úspešných prienikov a útokov. Navyše získa detailnejší prehľad o typoch útokov, ich priebehu a bude môcť automatizovať viac ochranných opatrení proti nim.

ZÁVER

Záverom možno konštatovať, že kybernetické hrozby predstavujú stále rastúcu výzvu. V tomto článku sme sa zamerali na základné princípy zabezpečenia podnikových sietí a jednotlivých zariadení. Predstavili sme rôzne typy útokov a ochranné mechanizmy. Je dôležité si uvedomiť, že kybernetická bezpečnosť je neustály proces, ktorý vyžaduje pravidelné aktualizácie a školenie používateľov. Aj napriek všetkým opatreniam však neexistuje stopercentná ochrana.

Podakovanie

Tento príspevok bol podporený projektom KEGA 004UMB-4/2024 a VEGA 1/0323/23.

Literatúra

1. Kolouch, J. (2016). *CyberCrime*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-15-7.
2. Jackson, K. (2024). *Technical Solutions Consultant View Profile. Everything you need to know about network probes*. Fortra. <https://www.fortra.com/blog/everything-you-need-know-about-network-probes>
3. Jovanović, B. (2019). Virus alert: Antivirus statistics and trends in 2020. *Data prot* [online]. [cit. 2020-02-26]. Dostupné z: <https://dataprot.net/statistics/antivirus-statistics/>
4. *Čo je to kyberbezpečnosť?*. GDPR Slovensko. 2024. <https://gdpr-slovensko.sk/co-je-to-kyberbezpecnost/>
5. *Microsoft*. Podpora spoločnosti Microsoft. <https://support.microsoft.com/sk-sk/topic/%C4%8Do-je-kybernetick%C3%A1-1-bezpe%C4%8Dnos%C5%A5-8b6efd59-41ff-4743-87c8-0850a352a390>
6. ISVS.CZ, R. (2023). *Kybez: Nejčastější Typy Kybernetických útoku*. ISVS.CZ. Aktuálně to nejdůležitější o ISVS a eGovernmentu zde na jednom místě. <https://www.isvs.cz/kybez-nejcastejsi-typy-kybernetickych-utoku/>
7. *Čo je útok ddos? Zabezpečenie od spoločnosti Microsoft*. <https://www.microsoft.com/sk-sk/security/business/security-101/what-is-a-ddos-attack>
8. CISCO. (2023). *What is Network Address Translation (nat)?* Cisco.
9. *What is an intrusion prevention system?* Palo Alto Networks. <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips>
10. *Čo Je vpn a Prečo Ju Používať?* ESET. <https://www.eset.com/sk/internetova-ochrana-domacnosti/co-je-vpn/>
11. *EDR vs. XDR vs. Siem vs. MDR vs. soar. Sysdig. (2024)*. <https://sysdig.com/learn-cloud-native/edr-vs-xdr-siem-vs-mdr-vs-soar/>

Kontakty

Andrej Štefánik, Ing. Martin Kučerka, PhD.
Univerzita Mateja Bela v Banskej Bystrici, Fakulta prírodných vied
Tajovského 40, 974 01 Banská Bystrica
Tel: +421/48 446 7219
E-mail: andrej.stefanik@student.umb.sk, martin.kucerka@umb.sk