UNIVERZITA PARDUBICE

Fakulta ekonomicko-správní

BAKALÁŘSKÁ PRÁCE

2023 Jan Konrád

Univerzita Pardubice
Fakulta ekonomicko-správní

Moderní prostředky pro zabezpečení počítačových sítí proti vnějším útokům

Bakalářská práce

2023 Jan Konrád

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jan Konrád**
Osobní číslo:	**E19127**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Moderní prostředky pro zabezpečení počítačových sítí proti vnějším útokům**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je vytvořit přehled v současnosti používaných prostředků pro zabezpečení počítačových sítí proti vnějším útokům ve formě podpůrného studijního materiálu.

Osnova:
– Vyhledání podkladů pro vytvoření přehledu běžných typů vnějších útoků na síť
– Vyhledání prostředků sloužících k zabezpečení.
– Vytvoření studijního materiálu.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

ELISAN, Christopher C., Michael A. DAVIS, Sean M. BODMER a Aaron LEMASTERS. Hacking exposed Malware and Rootkits. Second edition. New York: Mc Graw Hill Education, ?2017. ISBN 978-0-07-182307-4.
KERNIGHAN, Brian W. Jak porozumět digitálnímu světu: vše, co potřebujete vědět o internetu, bezpečnosti a soukromí. Přeložil Petr HOLČÁK. Praha: Argo, 2019. Zip., svazek 65. ISBN 978-80-7363-903-7.
SPURNÁ, Ivona. Počítačové sítě: praktická příručka správce sítě. Kralice na Hané: Computer Media, 2010. ISBN 978-80-7402-036-0.
ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2022**
Termín odevzdání bakalářské práce: **30. dubna 2023**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2022

Prohlašuji:

Práci s názvem moderní prostředky pro zabezpečení počítačových sítí proti vnějším útokům jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 15. 09. 2023

Jan Konrád v. r.

Poděkování:

Tímto bych rád poděkoval svému vedoucímu práce RNDr. Ing. Oldřichu Horákovi Ph.D. za jeho odbornou pomoc a cenná doporučení, která mi pomohla při zpracování bakalářské práce. Dále bych rád poděkoval rodině a přítelkyni za podporu a trpělivost.

ANOTACE

Tato bakalářská práce se zabývá problematikou moderních prostředků pro zabezpečení počítačových sítí proti vnějším útokům. Práce řeší bezpečnost v oblasti informatiky, možné kybernetické útoky a protiopatření. V závěru práce je popsána tvorba studijních materiálů.

KLÍČOVÁ SLOVA

Zabezpečení, sociální inženýrství, firewall, VPN, antivirus, studijní materiály

TITLE

Modern means for securing computer networks against external attacks

ANNOTATION

This bachelor thesis deals with the issue of modern means for securing computer networks against external attacks. The thesis deals with security in the field of computer science, possible cyber attacks and countermeasures. The thesis concludes with a description of the development of study materials.

KEYWORDS

Security, social engineering, firewall, VPN, antivirus, study materials

OBSAH

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

ISO 27000	Information Security Management System
RAM	Random Access Memory
VPN	Virtual Private Network
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NIDS	Network-based intrusion detection system
HIDS	Host-based intrusion detection system
MS OFFICE	Microsoft Office
2FA	Two-factor authentication
OSI	Open Systems Interconnection
DPI	Deep packet inspection
VLAN	Virtual LAN
DDoS	Denial of Service
BGP	Border Gateway Protocol
API	Application programming interface
PDF	Portable document format

ÚVOD

V současné době je nezbytné, aby firmy ve všech odvětvích nasazovaly informační systémy a informační technologie, aby dosáhly úspěchu a v konečném důsledku přežily. Informační technologie zažily v posledních desetiletích ohromný rozvoj a staly se klíčovým faktorem pro růst a konkurenceschopnost podniků. Práce s informacemi by bez těchto technologií byla nejen neefektivní, ale také časově náročná. Informační technologie znamenají významnou úsporu času a energie.

S rychlým rozvojem moderních informačních systémů však stoupá také riziko jejich zneužití. Počítačová kriminalita, zneužívání dat, elektronické krádeže a podvody jsou dnes běžnou součástí našeho života a rovněž zažívají obrovský nárůst, stejně jako samotné IT technologie.

S nárůstem počtu počítačových sítí se zvyšuje potřeba zabezpečení těchto sítí. Ochrana dat je jedním z nejdiskutovanějších aspektů IT. Citlivá data, obchodní tajemství a další informace přenášené počítačovými sítěmi jsou ohroženy různými formami útoků, které jsou stále sofistikovanější a obtížněji odhalitelné. Útočníci neustále hledají nové způsoby, jak prolomit zabezpečení sítí. Pro majitele a správce počítačových sítí je ochrana proti těmto útokům stejně důležitá jako stabilita samotné sítě. Zabezpečení sítě proti útokům je tedy klíčovou oblastí, která vyžaduje zvláštní pozornost a investice.

Cílem této bakalářské práce je vytvořit přehled v současnosti používaných prostředků pro zabezpečení počítačových sítí proti vnějším útokům ve formě podpůrného studijního materiálu.

První část se zaměřuje na potenciální bezpečnostní incidenty v kyberprostoru, což je oblast spojená s počítačovými sítěmi. V práci jsou objasněny pojmy jako je kyberprostor, síťová bezpečnost a dále jsou přiblíženy bezpečnostní mechanismy řízení přístupu a nejčastější hrozby ohrožující systém.

Druhá kapitola popisuje rozdíly mezi jednotlivými útočníky a nástroji, které běžně používají. Dále je vysvětlen pojem sociální inženýrství a také způsoby obrany proti tomuto typu útoku.

V další kapitole je popsána role obránců počítačových sítí a jsou představeny pojmy jako např. firewall, VPN, antivirus, DDos mitigation, dvoufaktorové zabezpečení a používaní silných hesel.

Poslední kapitola se zabývá vytvářením studijních materiálů, pravidly a doporučení při vytváření studijních materiálů. Následuje vlastní zpracování práce do formy studijních materiálů, které jsou v příloze.

Tato práce by měla přinést nové poznatky mírně pokročilým uživatelům, pro které by měla plnit účel podpůrného studijního materiálu.

1 Kyberprostor a internetová kriminalita

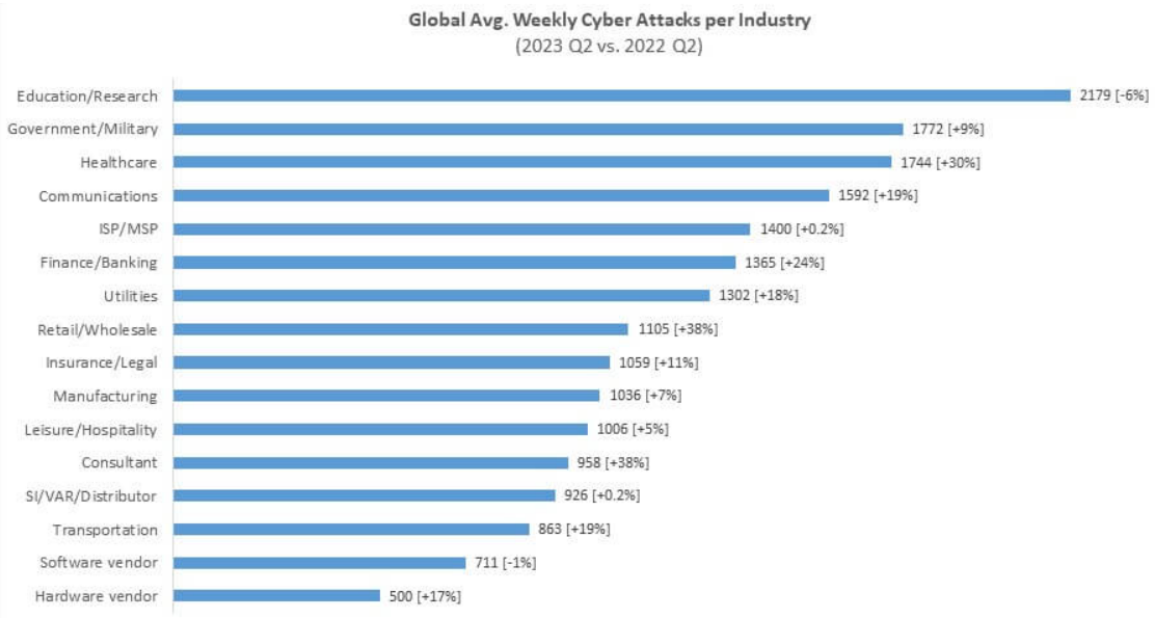
Vzhledem k využívání informačních a komunikačních technologií je termín kyberprostor používán i širokou veřejností. Pod pojmem kyberprostor si můžeme představit virtuální, nehmotný svět složený z moderních technologií jako je internet. Společnost tyto technologie využívá jako přirozenou součást svého každodenního života, což přináší mnoho výhod, ale také některá bezpečnostní rizika a problémy, které jsou spojeny se zvýšenou zranitelností sítí. Zabezpečení sítí je tedy nedílnou součástí nejen pro vojenské účely a podnikání, ale i pro jednotlivé koncové uživatele. S rostoucím využíváním moderních technologií rostou i nemorální, neetické nebo dokonce nezákonné aktivity, známé také jako kybernetická kriminalita.[18][20]

Identifikace a následné stíhání pachatelů kybernetické kriminality je obecně velmi obtížné. Obtíže souvisejí nejen s technickými požadavky, odbornými znalostmi, ale také s legislativním rámcem. Mezinárodně jsou stále vyvíjejí normy pro bezpečnost informací ISO 27000. Zde je třeba chápat, že pachatele informační hrozby či útoku (bezpečnostního incidentu) je velmi obtížné dohledat a následně prokazatelně usvědčit, takže je vždy o krok napřed.[5]

Hrozbu lze v kontextu bezpečnosti informací chápat jako jakoukoli situaci nebo faktor, který může potenciálně způsobit nežádoucí změny v informacích, chování systému nebo ovlivnit jeho parametry. Tato hrozba může využít slabinu nebo zranitelné body informačního systému k provedení útoku. Zranitelnost může být definována jako jakékoliv místo v informačním systému, které má slabinu, a které může být využito k poškození nebo ztrátě dat. Samotný útok představuje skutečné provedení této hrozby v praxi.[18]

1.1 Síťová bezpečnost

Oblast síťové bezpečnosti je obrovská a stále se rychle vyvíjí. Počet zaznamenaných bezpečnostních incidentů rok od roku roste. I přes výrazné zlepšení v oblasti bezpečnosti sítí a počítačů jsou tyto systémy nyní více zranitelné než kdy jindy. Jak technologie komunikace a zpracování dat postupují kupředu, přinášejí s sebou nové bezpečnostní hrozby a rizika, která vyžadují nová řešení. Bohužel technický pokrok probíhá rychleji, než můžeme vytvořit odpovídající bezpečnostní opatření. S nárůstem sofistikovanosti útoků je nutné implementovat stále více bezpečnostních opatření k ochraně počítačových a komunikačních sítí.[32]



Obrázek 1: Statistika zaznamenaných kybernetických útoků

Zdroj: [26]

V grafu můžeme vidět, že se každým rokem navyšuje celkový počet spáchaných kybernetických útoků. V druhém čtvrtletí roku 2023 zaznamenal nejvyšší počet útoků sektor vzdělávání/výzkum, kde na jednu organizaci připadalo v průměru 2179 útoků týdně, což představuje 6% pokles ve srovnání s druhým čtvrtletím roku 2022. Druhým nejčastěji napadaným sektorem byl vládní/vojenský sektor s průměrným počtem 1772 útoků týdně, což představuje 9% nárůst oproti paralelnímu období loňského roku. V těsném závěsu následoval sektor zdravotnictví s průměrem 1744 útoků týdně, což odráží výrazný meziroční nárůst o 30 %.[26]

Zabezpečení sítě souvisí s různými činnostmi, které zvyšují úroveň ochrany sítě. Toto zabezpečení se týká aspektů jako dostupnost, důvěrnost, integrita a bezpečnost sítí a dat. Zabezpečení sítě je klíčovým požadavkem pro všechny komunikační systémy, a to jak v podnikovém prostředí, tak pro běžné uživatele. Je nezbytné zajistit adekvátní ochranu pro všechny sdílené informace a data, která mohou být velmi citlivá, jako jsou čísla kreditních karet nebo firemní informace.[32]

Nicméně zabezpečení sítě nezahrnuje pouze ochranu koncových počítačů. Je také nezbytné chránit samotný komunikační kanál, aby nebyl snadno napadnutelný. Nedostatečně zabezpečený komunikační kanál by mohl umožnit útočníkovi snadný přístup k přenášeným datům, jejich dešifrování a následnou změnu nebo podvržení. Ochrana přenosových sítí je stejně důležitá jako zabezpečení koncových zařízení a šifrování přenášených zpráv. Efektivní

zabezpečení sítě musí brát v úvahu různé druhy útoků a rizik a snažit se zabránit jejich proniknutí do sítě a jejich šíření. Bezpečnost sítě je klíčovým faktorem pro zajištění plynulého fungování internetových operací.[32]

Každý počítač nebo počítačová síť je tak bezpečná, jak je bezpečná její nejslabší část. Největším rizikem je připojení počítače k počítačové síti. Rizikem rozvinuté informační společnosti je vytvoření závislosti na informačních a komunikačních systémech. Moderní technologie nám na jedné straně usnadňují život, ale na druhé straně zvyšují riziko zneužití.[14]

1.2 Bezpečnostní mechanismy – řízení přístupu

Řízení přístupu je klíčovým konceptem v oblasti bezpečnosti informací, který se zaměřuje na vzájemný vztah mezi subjektem (například uživatelem, procesem nebo aplikací) a objektem (například databází, souborem nebo paměťovým médiem). Tento koncept je klíčový pro zajištění tří základních aspektů informační bezpečnosti, známých jako triáda CIA:

- Důvěrnost (Confidentiality) znamená, že informace nesmí být zpřístupněny neoprávněným subjektům.
- Integrita (Integrity) zabezpečuje, že informace zůstávají důvěryhodné a mohou být upravovány pouze oprávněnými subjekty.
- Dostupnost (Availability) zajistí, že autorizovaným subjektům je umožněn rychlý přístup k informacím, aby mohli provádět potřebné operace.[33]

Kromě triády CIA existuje několik dalších důležitých bezpečnostních funkcí, včetně:

- Identifikace - tvrzení subjektu o své identitě nebo příslušnosti k určitému kontextu.
- Autorizace - proces získání povolení k provedení konkrétní činnosti nebo operace.
- Autentizace - proces ověření totožnosti subjektu nebo entity.
- Účtovatelnost – ručení odpovědnosti subjektů za svoji činnost a rozhodování.
- Audit - záznam o událostech, které mohou mít vliv na bezpečnost informací a slouží k monitorování a vyhodnocování bezpečnostních opatření.[33]

1.3 Nejčastější hrozby, které mohou ohrozit bezpečnostní systém

Kybernetické hrozby jsou schopny způsobit nežádoucí události, které mohou zahrnovat škody na systémech a aktivitách organizace. Tyto hrozby mohou být jak náhodné, například v důsledku technických chyb, tak i záměrné, jako jsou útoky hackery, malware nebo špionáž.[6]

Je důležité, aby organizace identifikovaly a vyhodnotily kybernetické hrozby, abychom byli schopni se bránit proti potenciálním rizikům. Toto vyžaduje proaktivní přístup k řízení rizik, identifikaci nebezpečí a rychlou reakci na jejich dopady. Každá hrozba má specifické charakteristiky, které organizaci pomáhají identifikovat zdroje, motivace a sílu této hrozby.[6]

- Výpadek dodávky elektrické energie: Nedostatek elektrické energie může způsobit problémy s integritou a má potenciál způsobit další poruchy, jako je selhání hardware. Toto selhání nemusí omezit pouze hardware, ale může ovlivnit i další prvky infrastruktury, jako jsou klimatizace, zálohování a další.

- Selhání hardwaru: Technické poruchy, jako je selhání síťových komponent nebo serverů, mohou mít za následek ztrátu dostupnosti dat uložených v těchto systémech. Tyto problémy mohou vzniknout z různých důvodů, včetně nedostatečné údržby nebo nevhodných provozních podmínek.

- Škodlivý software (malware): Malware, jako jsou viry, trojské koně a ransomware, může poškodit, změnit nebo dokonce zničit data. Malware může způsobit vážné problémy pro informační systémy a organizace, pokud není rychle detekován a odstraněn.

- Selhání komunikačních služeb: Chyby a poruchy v komunikačních zařízeních a službách mohou ovlivnit dostupnost informací, které jsou přenášeny prostřednictvím těchto služeb.[6]

2 Klasifikace útočníků

Bezpečnostní hrozby jsou často prováděny útočníky, kteří se obvykle mohou rozdělit podle stupně svých schopností a náročnosti činnosti. Tato část představuje stručné shrnutí charakteristik spojených s danou dovedností a úrovni činnosti daného typu útočníka.[32]

Úspěšnost útočníka v oblasti síťové bezpečnosti závisí na několika klíčových faktorech:

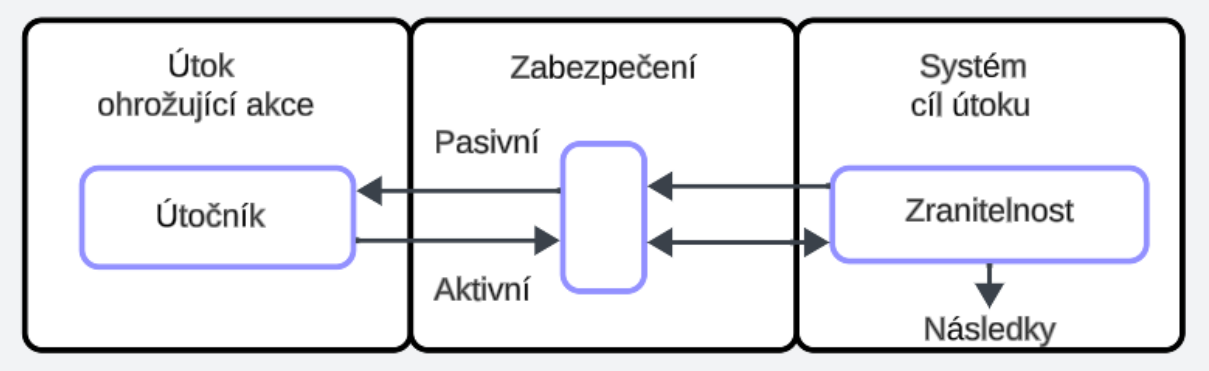
- Náklady: Útočníkova schopnost provést úspěšný útok souvisí s finančními náklady, které musí vynaložit na potřebné zařízení. Tyto náklady mohou být relativně nízké, například pokud potřebuje pouze základní nástroje, nebo mohou být velmi vysoké, pokud vyžaduje drahá testovací zařízení nebo speciální technologie.

- Zkušenosti: Úspěch útočníka je také závislý na jeho dovednostech a znalostech. Určité útoky mohou být proveditelné i pro méně zkušené útočníky, pokud mají přesné pokyny, zatímco jiné vyžadují pokročilé znalosti a dovednosti.
- Vystopovatelnost: Tento faktor odkazuje na stopy a indicie, které útočník může zanechat. Pokud útok nezanechá žádné stopy a síťové uzly zůstanou v původním stavu, může být obtížné útok odhalit, pokud nedojde k fyzickému poškození zařízení.[32]

Aktivity útočníka lze obecně rozdělit na:

- Aktivní – cílem těchto útoků je změnit systémové prostředky (včetně dat) nebo ovlivnit funkčnost. Při tomto typu útoku se útočník pokouší smazat, přidat nebo jinak změnit data přenášená přes odpovídající kanál s jakýmkoliv zařízením účastnícím se komunikace.

- Pasivní – s jejich pomocí je možné získat informace ze sítě pouhým sledováním aktuálního připojení. Tyto útoky zahrnují činnosti, jako je analýza provozu, sledování nechráněné komunikace, dešifrování slabě zašifrovaného provozu a získávání ověřovacích informací, jako jsou uživatelská jména a hesla. Tyto útoky tedy přímo neovlivňují systémové prostředky. Někdy může být pasivní útok použit jako přípravná fáze pro aktivní útok.[32]



Obrázek 2: Schéma útoku

Zdroj: vlastní podle [27]

Dále lze útoky dělit na neinvazivní, poloinvazivní a invazivní:

- Neinvazivní útoky - tyto útoky nepoškozují napadané zařízení ani jeho funkčnost.
- Poloinvazivní útoky – manipulují a mění informační obsah napadeného zařízení, ale nemají přímý přístup k jeho integrovaným obvodům.

- Invazní útoky – jsou takřka bez omezení z hlediska získávání informací z napadaného zařízení (např. průzkumné sondovací stanice).[32]

Toto jsou klíčové faktory, které ovlivňují, jak útočníci přistupují k útokům na síťovou bezpečnost a jakým způsobem se snaží proniknout do systémů.

2.1. Nástroje útočníků

Útočník pří svých akcích mimo jiné využívá technické znalosti, dovednosti a nástroje, které lze obecně rozdělit:

- Hardwarové nástroje – hledání a následné využití slabých míst v hardwaru.
- Softwarové nástroje – jde o nejčetněji skupinu technik, které bývají využívány. Jsou založené na existenci softwaru, který je navržen a přizpůsoben pro konkrétní účel. Zahrnuje metody pro hledání bezpečnostních děr v běžných programech a softwarových systémech.
- Sociální inženýrství – popsáno v podkapitole 2.3.[18]

2.2 Programové nástroje útočníků

Exploit je software, který využívá systémovou chybu nebo zranitelnost k tomu, aby umožnil útočníkovi proniknout do systému nebo aplikace. Tato bezpečnostní chyba umožňuje útočníkovi provádět neautorizované operace nebo získávat neoprávněný přístup k systému. Po odhalení této slabiny, vytvoří vývojáři operačního systému nebo bezpečnostního softwaru vytvoří "záplatu", která tuto zranitelnost odstraní. Po instalaci této opravy exploit ztrácí svou účinnost. Tento proces bezpečnostních aktualizací a objevování nových zranitelností je neustálým cyklem v bezpečnosti počítačových systémů.[18]

Malware je obecný termín pro škodlivý software určený k infiltraci, převzetí nebo poškození systému, ve kterém se nachází. Společný znak malwarů je, že se snaží na napadeném počítači ukrýt a snaží se přežít restart počítače. K proniknutí do počítače je nutná větší či menší spolupráce ze strany oběti.[4]

Může se jednat například o tzv.:

- Phishing, jedná se o kybernetický útok využívající techniky sociálního inženýrství, při kterém se útočník snaží získat důvěrné informace oběti nebo spustit škodlivý kód na zařízení oběti. Ve většině případů je phishingový útok proveden pomocí podvodného e-mailu, který požaduje informace o naší platební

kartě nebo přihlašovací údaje do našeho internetového bankovnictví. Můžeme se s ním setkat i na chatovacích programech a sociálních sítích.[22]

- Drive-by download malware, kdy k jeho stažení stačí pouze navštívit infikovanou webovou stránku. Tento škodlivý kód nejprve detekuje operační systém oběti, její prohlížeč, verzi Javy nebo flashe. Poté stáhne Java applet nebo flashovou animaci z jiného serveru, který obsahuje aplikaci, která využívá zranitelnosti zařízení. Stáhne spustitelný soubor do zařízení a infikuje zařízení. Uživatel nemusí nic dělat, stačí navštívit napadený server.[36]
- Trojanizovaná aplikace, která se může nacházet jak na neoficiálním, tak ale i oficiálním marketu, na úložišti nebo přenositelném médiu.[36]

Podle způsobu šíření můžeme malware rozdělit na několik typů:

- Virus, je kód, který přidá svou kopii do spustitelného souboru nebo do spouštěcího sektoru. Když je infikovaný soubor spuštěn, je zapsán do dalšího spustitelného souboru. Dnešní antivirus však takovou operaci snadno odhalí, takže viry dnes nepředstavují velkou hrozbu. Virus by neměl být zaměňován se souvisejícími termíny, jako jsou červi, trojské koně, zadní vrátka a další malware, ačkoli vlastnosti všech těchto termínů mají tendenci se překrývat.[36]
- Worm neboli červ, je program, který se posílá e-mailem na jiné e-mailové adresy nebo se šíří po síti a vyhledává další zařízení, využívá jejich slabin, slabých hesel nebo zastaralého softwaru a kopíruje se po síti. To je obzvláště nebezpečné, protože oběť obdrží e-mail od někoho, koho zná, a tak nepojme podezření a přílohu otevře.[4]
- Makrovirus, kód napsaný v makrojazyku (např. ve Visual Basicu), který se při spuštění makra zkopíruje do jiných souborů MS Office. Dá se snadno odhalit, takže se moc nepoužívá. Macrovirus se používá jako tzv. dropper, který se používá ke stažení dalšího malwaru.[36]
- Spyware je výzvědný software. Nainstaluje se do počítače bez vědomí uživatele a funguje zde jako „špion“. Odesílá informace o uživateli přes internet. Ve většině případů se do zařízení dostane spolu s další aplikací, kterou bývá nejčastěji trojský kůň. Poměrně často se vyskytují případy, kdy je sběr a odesílání uživatelských dat zmíněno v licenčních podmínkách. Mezi spyware také spadá keylogger, který zaznamenává úhozy, a proto se používá ke krádeži hesel.[34]

- Trojský kůň se vydává za užitečnou aplikaci nebo aktualizaci, která dorazí do počítače poté, co si ji uživatel stáhne a nainstaluje. Na pozadí však provádí další škodlivé činnosti. Mohou to být například keyloggery, které zaznamenávají hesla. Snímače obrazovky, které zaznamenávají obrazovku, nebo minery, které těží kryptoměny.[4]
- Adware neboli reklamní software. Zobrazuje nežádoucí reklamu na napadeném zařízení. Často je to pro autora jediná možnost, jak získat zpět část peněz investovaných do vývoje.
- Ransomware je software, který zašifruje data na disku a za jejich obnovu požaduje určitou peněžní částku.
- Scareware je falešný antivirus. Obvykle se zobrazí jako doporučení ke stažení, když uživatel prochází web a dostane se na infikovanou stránku.
- Logical bomb je aplikace, která čeká na splnění určitých podmínek. Nejčastěji se do počítače dostává prostřednictvím nespokojených zaměstnanců.
- Rootkit se skrývá uvnitř kompromitovaného zařízení a umožňuje útočníkovi vzdáleně ovládat zařízení.[36]
- Banking malware je speciální typ malwaru, který krade bankovní přihlašovací údaje. Pokud dvoufaktorová autentizace a autorizace transakce nejsou implementovány správně, může je obejít.
- Backdoor je skrytý program, který obchází běžné metody k ověřování nebo připojení a uděluje neoprávněný přístup k počítači.[11]

2.3 Sociální inženýrství

Nejslabší prvek jakéhokoliv systému je vždy sám člověk. Sociální inženýrství je způsob manipulace lidí k provedení určité akce nebo k získání určitých informací. Tímto způsobem se autoři podvodných e-mailů snaží upoutat vaši pozornost a donutit vás k akci za účelem získání určitých informací nebo získání přístupu k počítačovému systému. Termín obecně označuje jako podvod nebo podvodnou činnost. Ve většině případů není útočník v osobním kontaktu s obětí. Je to typ triku důvěry k získání informací, podvodu nebo získání přístupu k systému, který se liší od tradičního „podvodu“, protože je často jedním z mnoha kroků ve složitějším podvodném schématu. Je také definován jako jakýkoli čin, který přiměje osobu jednat, tak jak může nebo nemusí být v jejím nejlepším zájmu.[29]

Jedním z největších skutečných příkladů sociálního inženýrství je únik dat na americkém ministerstvu spravedlnosti v roce 2016. Až 200 GB dat uniklo ze záznamů poté, co se hacker úspěšně vydával za jednoho zaměstnance. Kombinace kompromitované interní e-mailové adresy a některých základních triků umožnila útočníkovi přesvědčit ostatní zaměstnance, aby mu poskytli plný přístup k interním souborům. Toto je vynikající příklad toho, jak dalekosáhlé účinky mohou mít i ty nejzákladnější techniky sociálního inženýrství.[30]

Techniky, které se využívají:

- Baiting (návnada) - pokud chceme získat to, co hledáme, např. oblíbený film, musíme si nejprve stáhnout infikovaný soubor v podobě falešného videopřehrávače.
- Phishing - snaží se o nalákání na podvodné e-maily obsahující osobní údaje, předstírání jiné identity (útočník se vydává za někoho jiného, s cílem získat přístup k důvěrným informacím).
- Malware - zobrazuje falešná varování o riziku malwarového útoku, doporučení k instalaci antiviru, který infikuje váš počítač.[31]

Jak se bránit před sociálním inženýrstvím?

Vzhledem k tomu, že sociální inženýrství je více než soubor technik, na rozdíl od virových útoků není skutečně možné jej z počítače odstranit. Nejlepší způsob, jak se vyhnout pastím sociálního inženýrství, je nenaletět podvodu. Pokud s manipulačními technikami neumíme bojovat sami, je nejlepší použít kvalitní antivirový program, který odstraní všechny škodlivé soubory a pomůže vytvořit silná a bezpečná hesla.[31]

Můžeme se alespoň řídit těmito poučkami:

- Nepřijímat žádné nevyžádané nabídky.
- Neklikat na odkazy od neznámých zdrojů.
- Nikdy nikomu neposílat heslo nebo bankovní údaje.
- Bezmezně nevěřit ničemu, o čem si nejsme stoprocentně jistí.[31]

3 Nástroje obránců

Moderní prostředky pro zabezpečení počítačových sítí se neustále vyvíjejí, aby udržely krok s neustále se měnícími hrozbami. Zde je několik klíčových prvků a technologií, které se v současnosti často používají. Je důležité si uvědomit, že žádná jednotlivá technologie není stoprocentně účinná, a proto se doporučuje použít kombinaci různých opatření a neustále zvyšovat úroveň zabezpečení, aby se minimalizovala šance na úspěch útoků.

3.1 Firewall

Firewall je brána mezi počítačovou sítí a vnějším světem. Jeho úkolem je monitorovat a kontrolovat veškerý provoz, který prochází mezi těmito dvěma oblastmi. Existují dva hlavní typy firewallů: síťové a osobní. Síťové firewally jsou umístěny na hranici sítě a chrání celou síť před neautorizovaným přístupem a škodlivým provozem. Osobní firewally (nebo softwarové firewally) jsou nainstalovány na konkrétních zařízeních a kontrolují jejich provoz.[36]

Obrázek 3: Schéma firewallu

Zdroj:[37]

Síťový firewall, se nejčastěji používá jako hardwarové řešení a je prvním filtračním prvkem síťové komunikace.[12]

Osobní firewall je aplikace určená ke sledování síťového provozu do a z počítače. Buď povoluje nebo blokuje komunikaci ve výchozím nastavení nebo na základě bezpečnostní politiky klienta. Osobní firewall chrání pouze koncového uživatele pracujícího na hostiteli, na kterém je software nainstalován. Většina osobních firewallů je nakonfigurována tak, aby

fungovala v automatickém režimů, což znamená, že software sám podle nastavení bezpečnostní politiky volí, zda komunikaci povolí nebo odmítne. Nebo může pracovat v manuálním módu což znamená, že koncový uživatel volí, kterou akci provede. V souhrnu lze osobní firewally považovat za varování před autentizací, chováním a hrozbami. To nás přivádí k funkci detekce narušení, kterou najdeme v mnoha aplikacích osobních firewallů, které používají sady statických podpisů. Detekční engine založený na signaturách je jen tak dobrý, jak dobré jsou jeho signatury. Většina osobních firewallů poskytuje koncovému uživateli nebo správci systému značné množství funkcí, včetně:

- Monitorování a upozorňování na příchozí a odchozí pokusy o spojení.
- Informace o cílové adrese přenosů od hostitele nebo aplikaci, která se pokouší připojit k hostiteli.
- Řízení programu pro různé aplikace, které se pokoušejí o přístup k síti.
- Ochrana proti vzdálenému skenování portů pomocí skrytí systému před nevyžádaným provozem.
- Monitorování všech aplikací, které naslouchají příchozím síťovým připojením.
- Ochrana před nežádoucím síťovým provozem z místních aplikací, které se snaží získat přístup k jiným systémům v síti.[11]

Máme několik možností různých firewallů. Některé jsou zdarma, zatímco další jsou součástí celého ochranného balíčku. Při výběru je ze všeho nejdůležitější vědět, jaké máme požadavky, aby výsledný firewall uspokojil naše potřeby.

3.2 Antivirový software

Známý také jako antivir, je určen k ochraně počítače nebo zařízení před škodlivým softwarem, jako jsou viry, červi, trojské koně, adware, spyware a další formy malwaru. Antivirový software pravidelně skenuje náš systém a hledá známé škodlivé kódy, aby je odstranil nebo umístil do karantény.[11]

Antivirové programy jsou vybaveny moderními technologiemi a disponují několika vrstvami ochrany, které slouží k obraně proti různým druhům hrozeb. Tyto vícevrstvé antivirové systémy poskytují uživatelům nejvyšší možnou úroveň ochrany. Jejich multifunkčnost spočívá v boji proti mnoha formám škodlivých aktivit, včetně krádeží hesel a účtů, neoprávněné těžby kryptoměn, šifrování souborů prostřednictvím ransomwaru, získávání citlivých osobních informací, potírání spamu, odhalování podvodů a dalších druhů kybernetických útoků. Pro splnění těchto cílů využívají antivirové programy dvě různé metody.

- Procházení souborů na místním disku a paměti RAM za účelem nalezení sekvence v databázi, která odpovídá definici počítačového viru.
- Identifikaci podezřelého chování počítačového programu, které může naznačovat infekci. Tato technologie zahrnuje analýzu nasbíraných dat, sledování jednotlivých aktivit portů nebo další techniky.[1]

3.3 VPN (Virtual Private Network)

VPN je technologie, která umožňuje využívat veřejnou datovou síť, například internet, k zabezpečené komunikaci. Toho se dosahuje vytvořením šifrovaného internetového připojení. VPN se často využívají pro bezpečné spojení vzdálených uživatelů s jejich privátní sítí, což umožňuje rozšiřovat rozsah privátní infrastruktury po celém světě. Jinými slovy, VPN umožňují výměnu dat mezi dvěma počítači prostřednictvím veřejných sítí, jako je internet, takže to vypadá, jako by šlo o přímé spojení, i když komunikace probíhá přes veřejné sítě. Znamená to, že uživatelé mohou komunikovat prostřednictvím zabezpečeného spojení, které je vnímáno jako soukromá síť, i když data putují přes veřejnou síť. Zde se odvozuje název "virtuální privátní síť" (VPN). Existuje mnoho důvodů, proč se používají sítě VPN, ale společným cílem je virtualizace určitého množství podnikové komunikace tak, aby byla pro vnější pozorovatele téměř neviditelná, zatímco se využívají výhody veřejné komunikační infrastruktury.[32]

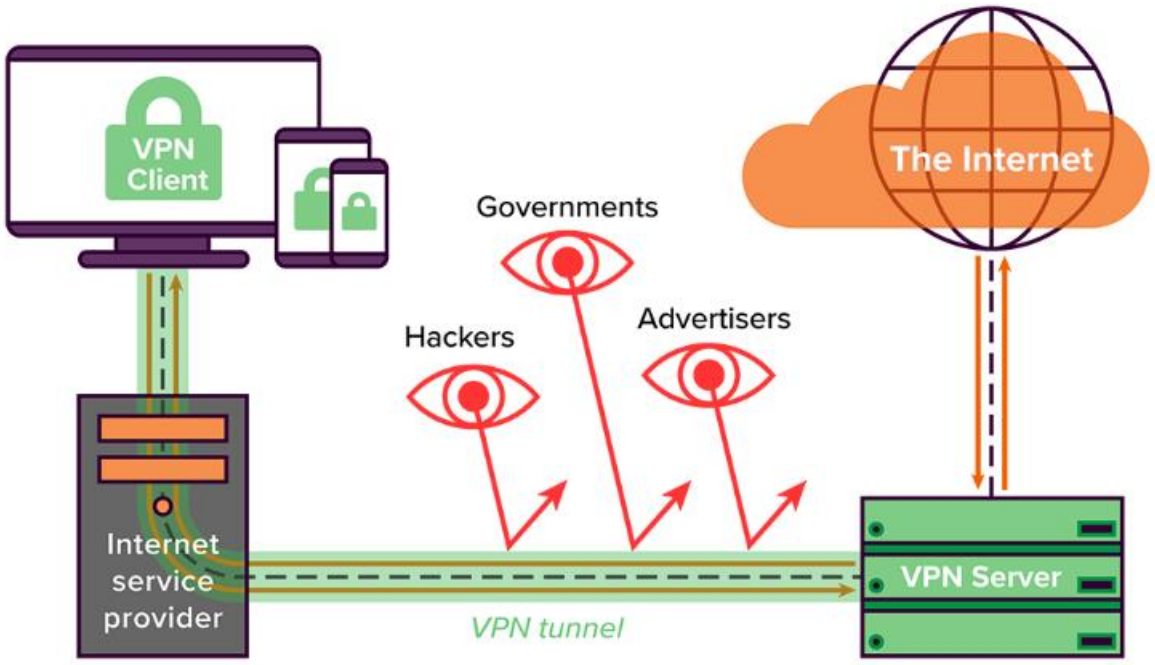
VPN vykonává především tyto funkce:

- Ověření uživatele – VPN umožňují pouze přístup oprávněným uživatelům, proto je důležité vždy ověřit jejich identitu. Kromě toho by VPN měly poskytovat a uchovávat informace o provedených kontrolách.[32]
- Šifrování dat je proces, při kterém se původní čitelná data přemění do nečitelné podoby (tzv. šifrovaného textu) za použití matematických algoritmů a klíčů. Tento proces zajišťuje ochranu dat tím, že potenciálním útočníkům brání v jejich čtení a porozumění bez odpovídajícího dešifrovacího klíče.[19]
- Správa klíčů – je nutná před samotným šifrováním dat, uživatelé nejprve definují a nastavují parametry šifrování (algoritmy, klíče, ...).[32]

Používání VPN má několik výhod. Poskytuje takovou úroveň anonymizace, že je prakticky nemožné určit původ vašeho připojení. Před připojením si můžete vybrat z různých IP adres, a pokud má váš VPN poskytovatel dostatečné zdroje, může vám nabídnout IP adresy z různých geografických oblastí po celém světě.[3]

Využívání VPN přináší několik výhod:

- Streamování odkudkoliv: Pokud jsme v zahraničí a chceme používat streamovací službu, kterou používáme doma, může se stát, že tato služba na aktuálním místě není dostupná. Avšak pomocí VPN a nastavení IP adresy z domovské země budete moci přistupovat k oblíbeným webovým stránkám, jako doma.
- Přístup k blokovaným webovým stránkám: Některé instituce, jako školy, knihovny nebo pracoviště, mohou omezovat přístup k určitým webovým stránkám, například sociálním sítím. VPN však umožní tato omezení obejít díky šifrovanému připojení.
- Obcházení cenzury: V některých zemích provádí státní orgány cenzuru internetu a omezují svobodný přístup k informacím. I když obcházení těchto omezení může být nezákonné, svoboda informací je zásadní. VPN umožnuje přistupovat k informacím bez omezení.
- Ochrana před cenovou diskriminací: Cenová diskriminace na základě polohy a sledování nákupních návyků může ovlivnit, kolik zaplatíme za různé služby a produkty online. VPN ochrání soukromí a znemožní poskytovatelům sledovat nákupy a zvyky.
- Ochrana před sledováním: Existuje mnoho entit, které mohou sledovat vaši online aktivitu, včetně hackerů, kybernetických zločinců, korporací, státních orgánů a poskytovatelů internetového připojení. VPN poskytuje ochranu před sledováním a zabezpečuje soukromí.[3]



Obrázek 4: Schéma VPN

Zdroj:[38]

Existují některé nevýhody spojené s používáním VPN, ale ve srovnání s jejich výhodami jsou tyto nevýhody zanedbatelné. Nicméně je dobré být obeznámen s těmito potenciálními omezeními.

- Potenciálně pomalejší připojení: Data, která putují přes VPN, mohou být pomalejší, protože procházejí více serverů než obvykle. Nicméně většina VPN poskytovatelů se snaží optimalizovat své služby a umožňují uživatelům používat VPN bez výrazných omezení.
- Problémy s kvalitou služeb: VPN služby nemají standardizovanou kvalitu služeb, což znamená, že není možné je jednotně srovnávat. Uživatelé se musí spoléhat na profesionální recenze a zkušenosti ostatních uživatelů.
- Blokování VPN: Některé organizace mohou blokovat známé IP adresy používané VPN službami, pokud zjistí, že zaměstnanci používají VPN k obcházení pracovních omezení. Avšak provozovatelé VPN služeb průběžně přidávají nové IP adresy, které lze použít.
- Nedokonalé soukromí: Přestože VPN šifruje připojení a chrání soukromí, stále jsme identifikovatelní na základě souborů cookie v prohlížeči. Je důležité si vypnout používání souborů cookie sami, pokud chceme dosáhnout vyššího stupně anonymizace.[3]

3.4 Intrusion Detection/Prevention Systems (IDS/IPS)

Intrusion Detection System (IDS) je systém detekce narušení. Představuje další vrstvu bezpečnostního opatření, která má za cíl odhalit počítačové útoky tím, že sleduje síťový provoz. Tento systém využívá databázi vzorů (signatur) a heuristickou analýzu k identifikaci podezřelých vzorků, které mohou indikovat útoky na síť nebo systém, s cílem proniknout do systému nebo mu způsobit škodu.[32]

Systémy IDS existují jak ve softwarové, tak v hardwarové podobě a slouží k detekci různých typů útoků. Tyto zařízení monitorují síťové připojení a jsou schopny detekovat již započaté útoky. Některé IDS systémy pouze sledují síťový provoz a informují o potenciálních hrozbách, zatímco jiné se aktivně snaží blokovat útoky. Systém IDS lze přirovnat k bezpečnostní kameře a senzoru pohybu, které identifikují neoprávněné nebo podezřelé aktivity a okamžitě vyvolají varování, aby bylo možné přijmout opatření k zastavení této činnosti.[32]

Lze identifikovat několik způsobů kategorizace IDS:

- Detekce zneužití vs. detekce anomálie: V případě detekce zneužití analyzuje IDS shromážděné informace a porovnává je s rozsáhlými databázemi signatur útoků. Cílem je nalézt konkrétní známý útok. Podobně jako antivirový software závisí účinnost systému detekce zneužití na kvalitě a rozsahu databáze útočných podpisů. V případě detekce anomálií určuje správce systému normální stav sítě, její zátěž, rozložení protokolů a obvyklou velikost paketů. Detektor anomálií následně monitoruje segmenty sítě a hledá odchylky od této normální linie.
- Založené na síti vs. hostitelské systémy: Systémy založené na síti (NIDS) analyzují jednotlivé pakety, které procházejí sítí. Jsou schopny identifikovat škodlivé pakety, které se pokoušejí obejít jednoduchá pravidla brány firewall. Na druhé straně systémy hostitelské (HIDS) zkoumají aktivitu na jednotlivých počítačích nebo hostitelích.
- Pasivní systém vs. reaktivní systém: V pasivním systému IDS identifikuje potenciální bezpečnostní hrozby, zaznamenává informace o nich a generuje výstrahy. Naopak v reaktivním systému IDS reaguje na podezřelou aktivitu například odhlášením uživatele nebo úpravou pravidel brány firewall, aby zablokoval podezřelý síťový provoz.[2]

Tímto způsobem lze rozdělit a zařadit různé aspekty systémů detekce narušení (IDS) podle jejich charakteristik a chování v různých scénářích kybernetické bezpečnosti.

Systémy prevence narušení provádějí analýzu provozu v síti, filtrování požadavků a na základě toho buď povolují nebo blokují tyto požadavky. Oproti systémům detekce narušení jsou systémy prevence narušení (IPS) aktivnější, neboť mají schopnost reagovat na specifické chování. Tato aktivita však může být pro IT týmy náročná, protože i neškodná, ale odlišná aktivita může generovat výstrahy a zatížit technický personál. Prevence narušení má také tendenci k výskytu falešně pozitivních a negativních zpráv: falešný poplach může zablokovat legitimní paket, který vypadá podezřele, zatímco falešný negativ může propustit škodlivý provoz. Implementace strojového učení do systému prevence narušení může pomoci zlepšit jeho schopnost rozpoznávat síťové vzorce a přesněji identifikovat skutečné hrozby. Pokročilá automatizace může snížit počet falešných poplachů a negativních zpráv. Bezpečnostní týmy často musí upravit pravidla, aby se vyhnuly spouštění falešných nebo nepodstatných upozornění.[9]

Služby prevence narušení mohou být implementovány jako síťové nebo hostitelské. Síťový IPS je umístěn blízko brány firewall a sleduje celkový síťový provoz. Naopak hostitelský IPS je umístěn blíže k jednotlivým počítačům nebo jiným koncovým bodům.[9]

3.5 Aktualizace a záplaty

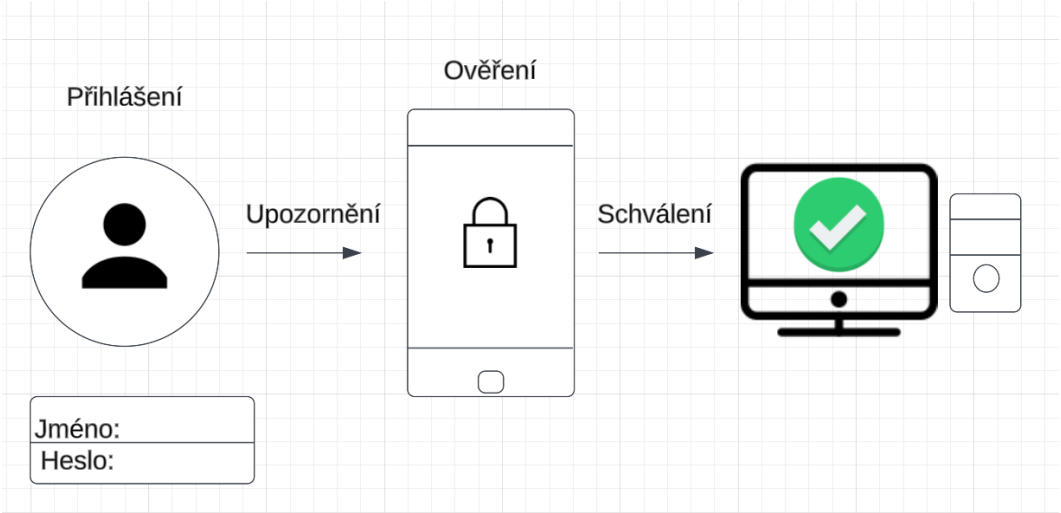
Na začátku je vhodné zdůraznit, že aktualizace přinášejí do operačního systému a aplikací nejen nové funkce a design, ale také opravy chyb, což je z hlediska bezpečnosti klíčové. Avšak často se stává, že lidé se brání provádění aktualizací. Hlavním důvodem je obava z výrazných změn ve vzhledu nebo funkcích, které mohou být pro uživatele nepříjemné. Někteří jsou například zmateni, když se tlačítko Start přesune z levého dolního rohu, jak se stalo ve Windows 8. Tyto změny vyvolávají u uživatelů nejistotu a nesnáze, a tak raději zůstávají u starší verze systému. To však může mít za následek využití chyb, které mohou být zneužity k útokům. U počítačů a notebooků je nejpodstatnější mít operační systém a aplikace vždy aktuální. Je důležité věnovat zvýšenou pozornost i internetovému prohlížeči. Ten se sice obvykle aktualizuje sám, ale je nutné jej občas restartovat. Proto je nevhodné nechávat počítač neustále zapnutý, protože prohlížeč s množstvím otevřených záložek zůstává aktivní a nemá možnost se aktualizovat.[23]

Aktualizovaný operační systém znamená mít nainstalovánu jakoukoli verzi, kterou výrobce nadále podporuje. Důležité je také mít nainstalovaný a pravidelně aktualizovaný antivirový program, nejlépe centrálně spravovaný. Tím získáte přehled o stavu programu, jeho aktualizacích a zachycených událostech. Centrální správa umožňuje mít kontrolu nad všemi

antivirovými programy a jejich funkcemi a aktualizacemi. Získání novější verze je otázkou několika kliknutí. Tato centralizace má řadu výhod, včetně možnosti ovládat některé funkce operačního systému, například vynucení vzdálené aktualizace.[23]

3.6 Dvoufaktorová autentizace (2FA) a silná hesla

Dvoufaktorová autentizace (2FA) představuje použití dvou odlišných informačních prvků pro úspěšné přihlášení. Tyto prvky jsou získávány z nezávislých zdrojů. Tímto požadavkem na dodatečný prvek pro přihlášení je zvýšena úroveň zabezpečení. Důvodem je výrazné snížení pravděpodobnosti, že by útočník dokázal současně prolomit více nezávislých zabezpečení. Konkrétně to znamená, že ochrana účtu je posílena vůči potenciálním útokům. I kdyby útočník dokázal proniknout skrze primární heslo, je velmi nepravděpodobné, že by disponoval i fyzickým přístupem k používanému chytrému telefonu, který je propojen s aplikací pro dvoufaktorovou autentizaci.[17]



Obrázek 5: Dvoufaktorová autentizace

Zdroj:[10]

Dále je také důležité používat silná hesla. Při vytváření a správě hesel se často objevují chyby, kdy lidé volí příliš jednoduchá a snadno odhadnutelná hesla, nebo dokonce používají jedno heslo pro všechny své účty. Pokud máte zájem o zabezpečené a pevné heslo, doporučuje se držet následujících pravidel:

- Nikdy a s nikým nesdílet hesla.
- Nepoužívat opakující se nebo sekvenční znaky (např. 1234, bbbb, …).
- Nepoužívat běžná slova a slovní spojení (např. osobní informace, jména oblíbených knih, ...).

- Používání dlouhých hesel, čím delší tím lépe - alespoň 12 znaků.
- Použití jedinečných hesel pro každý účet.
- Používání speciálních znaků a diakritiky.[28]

3.7 Segmentace sítě

Segmentace sítě je proces rozdělení velké sítě nebo infrastruktury na menší a snadněji spravovatelné části, známé jako segmenty nebo podsítě. Tato technika se často používá v oblasti informačních technologií, zejména v oblasti správy sítě a bezpečnosti. Existuje několik strategií pro vytváření komplexního bezpečnostního systému. Zaměřme se na ty klíčové:

- Segmentace sítě na fyzické vrstvě: Tento přístup zahrnuje rozdělení sítě na dvě fyzicky oddělené sítě. To zajišťuje vysokou úroveň zabezpečení, ale může být náročné na správu a růst s ohledem na potřeby podniku.
- Segmentace kanálů pro přenos dat (OSI vrstva 2/3): U průmyslových řídicích systémů, které vznikly před několika desítkami let, je často nutné využít stávající infrastruktury. Jedním z častých přístupů je použití virtuálních sítí (VLAN – virtuální lan)[33], které umožňují rozdělit datové toky. Některé přepínače také podporují seznamy řízení přístupu na úrovni portů nebo více bran firewall pro práci se třetí vrstvou sítě.
- Segmentace sítí na úrovni ověřování paketů (OSI vrstva 4-7): Tento způsob spočívá v hloubkové kontrole paketů (DPI). DPI poskytuje podrobný dohled nad provozem a umožňuje filtrování průmyslových protokolů dle specifických požadavků. Příkladem může být komunikace mezi zařízeními v síti.[16]

3.8 Bezpečnostní politiky a školení zaměstnanců

Vytváření a dodržování bezpečnostních politik a pravidel je klíčové pro udržení bezpečnosti sítě. Důležité je také pravidelně školit zaměstnance v oblasti kybernetické bezpečnosti, aby rozuměli aktuálním hrozbám a mohli se vyvarovat rizikům vyplývajícím z lidské chyby.

Největší riziko ve firemním prostředí představují počítače uživatelů. Odborníci se obvykle pečlivě starají o zabezpečení serverů. Avšak hackeři nejčastěji využívají lidské chyby či nedostatečnou informovanost jako nejjednodušší cestu k ohrožení dat.[15]

3.9 DDoS mitigation: DDoS (Distributed Denial of Service)

Výraz „zmírnění DDoS“ označuje proces úspěšné ochrany cíle před útokem distribuovaného odmítnutí služby (DDoS).[8]

Obvyklý postup zmírnění lze obecně rozčlenit do následujících čtyř fází:

- Detekce: Zahrnuje identifikaci odchylek v toku provozu, které by mohly naznačovat přípravu DDoS útoku. Úspěch se měří schopností rozpoznat útok co nejdříve, kde konečným cílem je okamžitá detekce.
- Odklonění: Provádí se přesměrování provozu mimo cíl, buď pomocí směrování DNS (Domain Name System) nebo BGP (Border Gateway Protocol). Následně se rozhodne, zda tento provoz filtrovat či zcela zahodit. DNS směrování je neustále aktivní a rychle reaguje na útoky, což je efektivní proti útokům na aplikační i síťové vrstvě. BGP směrování může být buď stále aktivní nebo aktivováno na vyžádání.
- Filtrování: DDoS provoz se odstraní, často identifikací vzorů, které rychle odlišují mezi legitimním provozem (jako jsou lidé, API volání a vyhledávací roboti) a škodlivými návštěvníky. Úspěch spočívá v tom, že útok je zablokován bez narušení uživatelského zážitku. Cílem je, aby bylo řešení pro návštěvníky webové stránky plně transparentní.
- Analýza: Protokoly a analýzy systému pomáhají shromažďovat informace o útoku, ať už k identifikaci pachatele či ke zlepšení budoucí odolnosti. Tradiční protokolování poskytuje vhled, avšak není v reálném čase a může vyžadovat detailní manuální analýzu. Pokročilé techniky bezpečnostní analýzy nabízejí podrobný pohled na útočný provoz a rychlé pochopení podrobností útoku.[8]

Tyto opatření společně tvoří komplexní ochranu počítačových sítí proti vnějším útokům a jsou důležité pro zajištění bezpečnosti dat a zařízení.

4 Studijní materiály

Hlavním cílem této práce je vytvořit studijní materiály, které se zaměřují na moderní prostředky zabezpečení počítačových sítí proti vnějším útokům. Následující část práce se věnuje tématu studijních materiálů. Tyto materiály mohou nabývat různých forem a typů, a proto jsou následující kapitoly věnovány představení rozmanitých podob a druhů materiálů. Čtvrtá sekce práce také definuje termín „studijní materiál“ a uvádí prvky, které mohou být obsaženy v studijních materiálech.

4.1 Co je to studijní materiál?

Studijní materiály zahrnují širokou škálu sdělení, která mají za cíl předat vzdělávací informace. Tato sdělení mohou být ve formě textových informací, grafů, obrázků, videí nebo zvukových nahrávek. Tyto materiály slouží k podpoře procesu vzdělávání tím, že umožňují studentům získat hlubší porozumění danému tématu. Studijní materiály mohou být ve formě učebních textů, prezentací, videí s výkladem, interaktivních simulací nebo online kurzů.[21]

Tyto materiály hrají klíčovou roli ve vzdělávání na různých úrovních, od středních škol až po vysoké školy. Jsou navrženy tak, aby pomohly studentům zvládnout obsah určitého oboru. Může se jednat o náročné technické koncepty, historické události, literární díla nebo jiná témata. Důležitou vlastností studijních materiálů je schopnost přizpůsobit se potřebám různých typů studentů. Mohou být strukturovány tak, aby nabízely různé úrovně obtížnosti nebo přístupy k informacím.[39]

Celkově lze říct, že studijní materiály jsou klíčovým nástrojem ve vzdělávacím procesu, který umožňuje studentům získávat nové znalosti a dovednosti prostřednictvím různých forem sdělení, které jsou přizpůsobeny danému tématu a vzdělávacímu prostředí.

4.2 Druhy studijních materiálů

Samotný popis termínu "studijní materiál", který byl výše prezentován, naznačuje, že existuje různorodá škála forem a druhů těchto materiálů. Moderní technologie rovněž značně usnadňují proces tvorby vlastních materiálů, které mohou učitelé přizpůsobit specifickým požadavkům výuky.[21]

Typy studijních materiálů:

- Prostředky pro digitální prezentace.
- Knihy určené k výuce.
- Dodatečné a cvičební materiály pro studenty.

- Odborné a metodické publikace pro pedagogy.
- Materiály pro vzdělávání na dálku.
- Prostředky pro digitální prezentace.
- Zdroje informací dostupné online.
- Fyzické výukové pomůcky.[21]

V minulé části bylo také řečeno, že studijní opory představují specifický typ studijního materiálu, který má využití při vysokoškolském distančním vzdělávání. Jak bude patrné v následujících odstavcích, studijní opory lze také rozdělit do různých kategorií. Studijní opory mohou sloužit buď jako hlavní materiál pro distanční vzdělávání, nebo jako doplňující zdroj k dalším studijním materiálům. Tyto opory lze dále kategorizovat do textových, audiovizuálních a e-learningových nástrojů.[24]

Nejčastěji používané druhy tištěných studijních opor.

- Materiály vytvořené speciálně pro distanční studium.
- Návody a doporučení pro efektivní studium.
- Psané přednášky, výukové materiály.
- Slovníky, tabulky, mapy a další relevantní podklady.[24]

Existuje velká různorodost výukových materiálů, což je zřejmé tím, že i samotní učitelé mohou vytvářet různé studijní materiály. To znamená, že nemůžou být vypsány všechny možné formy a typy studijních materiálů. Avšak některé kategorie materiálů jsou využívány častěji než ostatní, přičemž učebnice patří mezi ty nejběžnější.[21]

Vzdělávací učebnice mají zvláštní roli a jsou klíčovým prvkem ve vzdělávání. Učebnice můžeme považovat za základní materiál pro studium a často bývají doplněny dalšími výukovými texty, jako jsou cvičebnice, sborníky nebo slovníky. Tyto dodatečné materiály mohou rozšířit obsah učebnice.[21]

4.3 Obsah a uspořádání studijních materiálů

Většina dokumentů má svůj záměr a cíl. Při zahájení projektu je důležité stanovit konkrétní problém, který má být řešen, a určit, pro koho je dokument určen. Studijní materiály jsou specifické dokumenty, které mají svůj účel a obsahují vybrané informace. Mnoho autorů souhlasí s tím, že struktura obsahu je také klíčovým aspektem.[13]

Obsah studijních materiálů můžeme rozdělit na dvě hlavní části: textovou a mimo textovou. Tyto části obsahují další komponenty.[24] Textová část je zpravidla největší částí studijních materiálů. Důležité jsou také ilustrace a fotografie, které mohou lépe než slovní popis předávat informace.[21]

Obsah studijních materiálů je dále strukturován a organizován pomocí makrostruktury a mikrostruktury. Makrostruktura slouží k organizaci celého materiálu a zahrnuje členění obsahu do tematických celků, kapitol, lekcí a odstavců. To také zahrnuje výkladový text, řídící text a text, který pomáhá čtenáři orientovat se. Mikrostruktura se používá k organizaci menších částí, jako jsou odstavce, a zahrnuje grafické značky a polygrafické signály.[24]

Makrostruktura zahrnuje také grafické a typografické prvky, které jsou klíčové pro vhodnou strukturu jakéhokoli dokumentu.[13] Správně navržená struktura je důležitá i pro online kurzy, které zahrnují různé prvky, jako jsou studijní články, úkoly, cvičení, testy, autotesty, diskuse a ankety. Obsah těchto kurzů může být rozdělen do kapitol, přičemž každá kapitola by měla mít jasný začátek a konec.[25]

V rámci studijních materiálů je také vhodné zahrnout úvodní pasáž, která má motivovat studenty a navazovat na spojitosti mezi jednotlivými kapitolami. Úvodní slovo může také obsahovat doporučenou literaturu pro další studium.[25]

Z toho vyplývá, že struktura a obsah studijních materiálů by měly být pečlivě promyšleny tak, aby usnadňovaly orientaci a zdůrazňovaly důležité části. Makrostrukturace pomáhá rozdělit text na části a mikrostruktura využívá grafické prvky k lepšímu uspořádání. Studijní materiály mohou zahrnovat různé prvky a měly by být přizpůsobeny specifickému typu materiálu, jako jsou online kurzy, které vyžadují odlišný přístup k textu.[24]

5 Vytvoření studijních materiálů

Tato část práce se věnuje vytvoření podpůrných studijních materiálů na téma moderní prostředky zabezpečení počítačových sítí proti vnějším útokům. První kapitola se zabývá strukturou a obsahem materiálů, zatímco druhá kapitola zpracovává grafickou stránku.

5.1 Struktura a obsah studijních materiálů

V úvodu této práce je stanovena definice obsahu studijních materiálů. Dále je zdůrazněn význam strukturování a vizuální prezentace těchto dokumentů. Další část práce se zaměří na podkapitoly, které detailněji popisují metody a přístupy použité při tvorbě materiálů, které se týkají moderních prostředků k zabezpečení počítačových sítí proti vnějším útokům.

V následujících částech jsou rozvinuty a podrobněji vysvětleny metody a postupy, které jsou použity při tvorbě studijních materiálů souvisejících s moderními technikami ochrany počítačových sítí před vnějšími hrozbami.

5.2 Obsah

Cílem studijních materiálů je prezentovat čtenářům technologie týkající se zabezpečení počítačových sítí. První část práce byla věnována základním termínům v oblasti kyberprostoru, síťové bezpečnosti, bezpečnostním mechanismům a hrozbám. Druhá část se zaměřuje na rozdělení útočníků a jejich používané nástroje.

Vzhledem k tomu, že většina studijních materiálů je složena z textového obsahu, lze je označit za sumarizační texty, které shrnují obecně uznávané poznatky z dané oblasti.[24] Pro vytvoření studijních materiálů byla využita kompilace různých zdrojů.

Důležitou součástí studijních materiálů jsou také ilustrace a fotografie. Ty jsou získány z různých zdrojů.

Vzhledem k rozsahu tématu byl obsah studijních materiálů strukturován do tří samostatných částí, které byly pojmenovány následovně:

- Kyberprostor, síťová bezpečnost a hrozby.
- Klasifikace útočníků, nástroje, sociální inženýrství.
- Nástroje obránců, firewall, VPN, segmentace sítě.

První část série studijního materiálu má za cíl seznámit potenciální čtenáře se základními pojmy spojenými s kyberprostorem, síťovou bezpečností, bezpečnostními mechanismy a hrozbami, které mohou ohrozit bezpečnostní systém.

V druhém díle jsou detailně rozebrány kategorie útočníků a jejich používané nástroje. Je zde představen i pojem sociální inženýrství a jeho techniky a také, jak se proti němu bránit.

Třetí a zároveň poslední díl se zaměřuje na nástroje a mechanismy, které správci sítí využívají k obraně před různými útoky.

5.3 Struktura

Struktura materiálů vychází z prvků makrostrukturace. Téma týkající se moderních prostředků pro zabezpečení počítačových sítí proti vnějším útokům bylo rozčleněno do tří dílů, z nichž každý obsahuje specifické tematické celky. Tyto díly jsou následně strukturovány do dalších komponentů, kde každý díl je dále rozčleněn na jednotlivé kapitoly a podkapitoly.

V předchozí sekci se také hovořilo o významu řídícího textu a textu usnadňujícího orientaci. Studijní opory vydávané Univerzitou Pardubice, mají společný prvek a to, že na konci každé kapitoly poskytují souhrn klíčových informací a definují důležité pojmy, které by si měli studenti nebo čtenáři zapamatovat.

V předchozí části byla také zdůrazněna významnost úvodního slova. Ve studijních materiálech, které se týkají moderních prostředků zabezpečení počítačových sítí proti vnějším útokům, byly implementovány tyto tři důležité prvky: úvodní slovo, shrnutí kapitol a klíčové pojmy.

Dále byly do těchto materiálů začleněny další prvky makrostrukturace, konkrétně piktogramy. Piktogramy byly použity pro vizuální rozlišení různých částí textu, klíčových pojmů, shrnutí a otázek. Pro klíčové pojmy byl vybrán piktogram ve tvaru vykřičníku. Pro identifikaci shrnujících textů bylo využito řeckého písma Sigma a pro otázky piktogram otazníku.

Obrázek 6: Struktura studijních materiálů

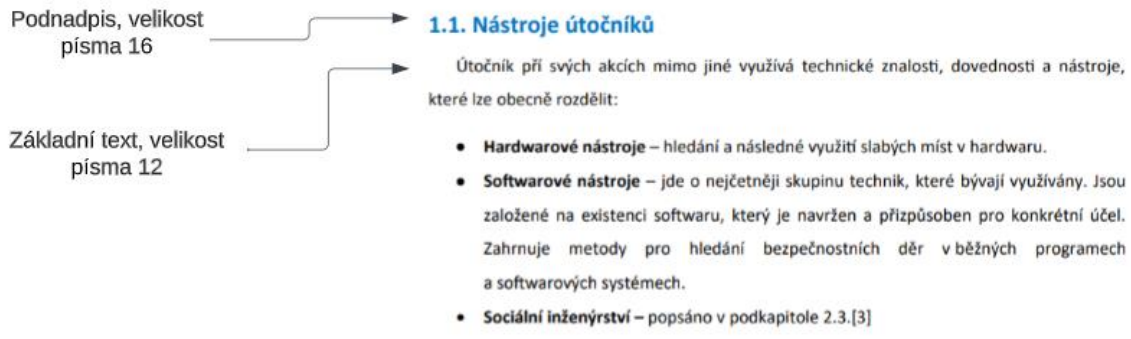
Zdroj: vlastní

Pro zvýraznění srozumitelnosti byly tyto studijní materiály obohaceny ilustracemi a fotografiemi. V každém díle série byly také začleněny autotesty, které obsahují otázky pro ověření nabytých znalostí. Všechny díly těchto materiálů mají jednotnou úvodní stránku a obsahují další prvky, jako je seznam použité literatury a výčet obrázků a tabulek.

5.4 Písmo

Většina studijních materiálů a dokumentů je zpravidla tvořena textovou částí, což platí i pro většinu jiných dokumentů. Písmo je základním prostředkem komunikace v těchto dokumentech a má významný vliv na celkovou atmosféru dokumentu. Proto by výběr vhodného typu písma neměl být podceňován. Volba správného písma je náročný a důležitý úkol, protože je potřeba brát v úvahu mnoho kritérií, jako je účel dokumentu, čitelnost a kvalita zpracování.[13]

Jak už bylo vícekrát řečeno, je také důležité, aby dokumenty měly jasnou hierarchii. Proto se v textu objevuje pouze jeden druh písma a pouze se mění velikost u nadpisů a podnadpisů.



Obrázek 7: Studijní materiály – písmo

Zdroj: vlastní

Pro studijní materiály bylo vybráno jedno z nejběžněji používaných písem Calibri z důvodu dobré čitelnosti dokumentu.

5.5 Barvy

Neméně důležitým aspektem je také barva, která tvoří nedílnou součást dokumentů a může hrát roli například vytvářením kontrastu mezi různými částmi dokumentu nebo přispívat k celkové atmosféře dokumentu. Při tvorbě dokumentu lze pracovat s jednou barvou nebo kombinovat různé barvy. Vzájemná interakce barev může ovlivňovat lidské vnímání a vyvolávat různé reakce, což závisí na tom, zda barvy spolu harmonizují nebo spolu naopak nesouzní což je do jisté míry subjektivní.[7]

Při návrhu grafického designu by mělo být pečlivě vybráno barevné schéma, které působí vyváženě a zároveň by mělo být zohledněno, jak jednotlivé barvy spolu interagují. V případě studijních materiálů, které jsou součástí této bakalářské práce, byla použita kombinace jedné barvy s různými odstíny. Tato barva byla využita k zvýraznění nadpisů a k oddělení bloků textu obsahujících shrnující informace a klíčová slova.

ZÁVĚR

Kybernetická kriminalita je neustále rostoucí problém, který nelze ignorovat. Je třeba chránit nejen jednotlivé uživatele, ale také klíčovou informační infrastrukturu. Hlavním problémem málo zabezpečených počítačových sítí je jejich snadná zranitelnost vůči přímým útokům. Naopak u dobře zabezpečených systémů je rizikem především lidský faktor, který může být využit k získání neoprávněného přístupu.

Pokud jde o ochranu sítě, je důležité dodržovat uvedená bezpečnostní opatření. Nicméně pro dosažení úplné bezpečnosti je také důležité informovat uživatele systému o různých druzích útoků, zejména o technikách sociálního inženýrství. Kromě toho je nezbytné zajistit ochranu koncových zařízení v síti instalací anti-malwarového softwaru.

Pokud jde o běžného internetového uživatele, je klíčové bránit se masovým podvodným praktikám, jako je phishing prostřednictvím falešných emailů a zpráv. Uživatelé by měli být také obezřetní při stahování a spouštění souborů z neznámých zdrojů na svých zařízeních. Je také důležité, aby měli aktualizovaný operační systém na svých zařízeních a pečlivě kontrolovali, že webové stránky, na kterých zadávají osobní nebo přihlašovací údaje, jsou legitimní.

Cílem této práce bylo vytvořit přehled v současnosti používaných prostředků pro zabezpečení počítačových sítí proti vnějším útokům ve formě podpůrného studijního materiálu.

Vzhledem k omezenému rozsahu práce byla úvodní část věnována obecné terminologii související s bezpečností počítačové sítě. Byl vysvětlen pojem bezpečnostního mechanismu řízeného přístupu a byly popsány největší hrozby, které mohou ohrozit bezpečnostní systém.

Dále je práce věnovaná útočníkům, kteří byli rozděleni podle různých faktorů. Tato část také zahrnovala seznámení se softwarovými nástroji útočníků a jejich technikami. Práce také pojednává o pojmu sociální inženýrství a jak je možné mu předcházet.

Následně byli představeni obránci počítačových sítí a jejich možnosti obrany počítačové sítě proti vnějším útokům. Dále byla prezentována určitá pravidla a zásady, díky kterým lze zvýšit bezpečnost počítačové sítě. Je nutné však říct, že žádný systém není stoprocentně bezpečný, a proto je potřeba být neustále na pozoru a nadále zvyšovat úroveň zabezpečení.

V předposlední části byl popsán studijní materiál a jeho ideální parametry. Je nutno však říci, že studijní materiál se může lišit v závislosti na tom, kdo ho vypracoval a co mu přijde jako ideální řešení.

V poslední části byl jeden studijní materiál představen a měl by sloužit mírně pokročilým uživatelům jako návod, jak lze zvýšit celkové zabezpečení počítačové sítě.

POUŽITÁ LITERATURA

[1] *Antivirus. Antivirus* [online]. Česká republika: Eset, c1992–2023 [cit. 2023-07-30]. Dostupné z: https://www.eset.com/cz/antivirus-software/

[2] *Co je to systém detekce narušení? Co je to systém detekce narušení?* [online]. c2023 [cit. 2023-08-30]. Dostupné z: https://soubory.info/info/co-je-to-system-detekce-naruseni/

[3] *Co je VPN a jak funguje? Váš základní průvodce. Co je VPN a jak funguje? Váš základní průvodce.* [online]. Česká republika: Avast, 2019 [cit. 2023-09-06]. Dostupné z: https://blog.avast.com/cs/co-je-vpn-a-jak-funguje

[4] *Cyber_vyzkum_studie_pojmy.pdf. In: Základní definice, vztahující se k tématu kybernetické bezpecnosti* [online]. 2009 [cit. 2023-09-06]. Dostupné z: http://www.mvcr.cz/clanek/o-NAS-bezpecnost-a-prevence-dokumenty-bezpecnost-aprevence-dokumenty-kybernetricke-hrozby.aspx.

[5] *Česká televize. Studio 6* [online]. 2012 [cit. 2023-06-27]. Dostupné z: https://www.ceskatelevize.cz/porady/1096902795-studio-6/212411010100229/

[6] ČSN ISO/IEC TR 13335-1:1999 Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 1: Pojetí a modely bezpečnosti IT

[7] DANNHOFEROVÁ, Jana. *Velká kniha barev: kompletní průvodce pro grafiky, fotografy a designéry*. Brno: Computer Press, 2012. ISBN 978-80-251-3785-7.

[8] *DDoS Mitigation: The Definitive Buyer's Guide. DDoS Mitigation: The Definitive Buyer's Guide* [online]. Imperva, c2023 [cit. 2023-08-31]. Dostupné z: https://www.imperva.com/learn/ddos/ddos-mitigation-services/

[9] *Detekce a prevence narušení (IDP) Detekce a prevence narušení (IDP)* [online]. c2023 [cit. 2023-08-30]. Dostupné z: https://soubory.info/info/detekce-a-prevence-naruseni-idp/

[10] *Dvoufaktorové ověřování přístupu do administrace WordPressu. Dvoufaktorové ověřování přístupu do administrace WordPressu* [online]. 2022 [cit. 2023-09-11]. Dostupné z: https://blog.jirivanek.eu/cs/2022/08/03/dvoufaktorove-overovani-pristupu-do-administrace-wordpressu/

[11] ELISAN, Christopher C., Michael A. DAVIS, Sean M. BODMER a Aaron LEMASTERS. *Hacking exposed Malware and Rootkits.* Second edition. New York: Mc Graw Hill Education, ©2017. ISBN 978-0-07-182307-4.

[12] *Firewall. Firewall* [online]. Česká republika: Eset, c1992–2023 [cit. 2023-07-30]. Dostupné z: https://www.eset.com/cz/firewall/

[13] HORNÝ, Stanislav a Petra BEDŘICHOVÁ. *Praktická učebnice tvorby multimediálního obsahu*. Professional Publishing, 2018. ISBN 978-80-88260-29-5.

[14] *HRŮZA, Petr. Kybernetická bezpečnost* [online]. Brno: DUKASE, 2012 [cit. 2023-07-25]. ISBN 978-80-7231-914-5. Dostupné z: https://www.researchgate.net/profile/Petr-Hruza/publication/275029169_Kyberneticka_bezpecnost/links/552f93a10cf2acd38cbc094e/Kyberneticka-bezpecnost.pdf

[15] *CHRAŇTE SVÁ DATA PROTI HACKERŮM!. CHRAŇTE SVÁ DATA PROTI HACKERŮM!* [online]. [cit. 2023-08-31]. Dostupné z: https://www.cybersec.cz

[16] *Jak chránit průmyslovou síťovou infrastrukturu OT a IT systémů. Jak chránit průmyslovou síťovou infrastrukturu OT a IT systémů* [online]. ipc2u, c2023 [cit. 2023-08-31]. Dostupné z: https://ipc2u.cz/blogs/news/jak-chranit-prumyslovou-sitovou-infrastrukturu-ot-a-it-systemu

[17] *Ještě více ochrany pro Vaše hesla!. Ještě více ochrany pro Vaše hesla!* [online]. sw, c2023 [cit. 2023-08-31]. Dostupné z: https://www.sw.cz/blog/silna-ochrana-hesel-na-internetu/

[18] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[19] KERNIGHAN, Brian W. *Jak porozumět digitálnímu světu: vše, co potřebujete vědět o internetu, bezpečnosti a soukromí*. Praha: Argo, 2019. Zip (Argo: Dokořán): Dokořán): Dokořán). ISBN 978-80-7363-903-7.

[20] *Kyberhrozby a kyberterorismus. In: Kyber - CESES* [online]. 2011 [cit. 2023-05-20]. Dostupné z: http://ceses.cuni.cz/CESES-70-version1-Kyber.pdf.

[21] LEPIL, Oldřich. *Teorie a praxe tvorby výukových materiálů: zvyšování kvality vzdělávání učitelů přírodovědných předmětů.* Olomouc: Univerzita Palackého v Olomouci, 2010. ISBN 978-80-244-2489-7.

[22] *Phishing. Phishing* [online]. Česká republika: Eset, c1992–2023 [cit. 2023-07-30]. Dostupné z: https://www.eset.com/cz/phishing/

[23] *Proč je důležité aktualizovat. Proč je důležité aktualizovat* [online]. Česká republika: Edu, c2022 [cit. 2023-08-31]. Dostupné z: https://www.edu.cz/proc-je-dulezite-aktualizovat/

[24] PRŮCHA, Jan. *Učebnice: teorie a analýzy edukačního média: příručka pro studenty, učitele, autory učebnic a výzkumné pracovníky.* Brno: Paido, 1998. Edice pedagogické literatury. ISBN 80-859-3149-4.

[25] ROHLÍKOVÁ, Lucie a Jana VEJVODOVÁ. *Vyučovací metody na vysoké škole: praktický průvodce výukou v prezenční i distanční formě studia*. Praha: Grada, 2012. ISBN 978-80-247-4152-9.

[26] *Security. Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research* [online]. 2023 [cit. 2023-09-11]. Dostupné z: https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

[27] *SHIREY, Robert W. Internet Security Glossary, Version 2. Rfc4949* [online]. RFC 4949, 2007 [cit. 2023-09-07]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc4949

[28] *Silné a bezpečné heslo. Anatomie hesel a pokročilé techniky při jejich vytváření a správě. Silné a bezpečné heslo. Anatomie hesel a pokročilé techniky při jejich vytváření a správě* [online]. Legislativa, 2023, 09.06.2023 [cit. 2023-08-31]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/silne-bezpecne-heslo

[29] *Social Engineering Defined. Social Engineering Defined* [online]. Security through education, c2023 [cit. 2023-08-30]. Dostupné z: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

[30] *Sociální inženýrství – to není jen phishing. Sociální inženýrství – to není jen phishing* [online]. Česká republika: Avast, 2019 [cit. 2023-08-30]. Dostupné z: https://blog.avast.com/cs/social-engineering-hacks

[31] *Sociální inženýrství. Sociální inženýrství* [online]. Česká republika: Avast, c1988–2023 [cit. 2023-08-30]. Dostupné z: https://www.avast.com/cs-cz/c-social-engineering

[32] *SORIANO, Miguel. Moderní systémy zabezpečení* [online]. Techpedia, 2017 [cit. 2023-06-15]. ISBN 978-80-01-06206-7. Dostupné z: http://techpedia.fel.cvut.cz/single/?objectId=76

[33] SPURNÁ, Ivona. *Počítačové sítě: praktická příručka správce sítě*. Kralice na Hané: Computer Media, 2010. ISBN 978-80-7402-036-0.

[34] *Spyware. Spyware* [online]. Česká republika: Eset, c1992–2023 [cit. 2023-07-30]. Dostupné z: https://www.eset.com/cz/spyware/

[35] STEWART, James Michael, TITTEL, Ed, a CHAPPLE, Mike. CISSP: *Certified Information Systems Security Professional study guide*. 3rd ed. San Francisco: SYBEX, c2005, 759 p. ISBN 07-821-4443-8.

[36] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[37] *What Is a Firewall and Why Do You Need One? What is a firewall?* [online]. 2022 [cit. 2023-09-11]. Dostupné z: https://www.avast.com/c-what-is-a-firewall

[38] *Zabezpečení. Co je to VPN a jak ji můžeme využít?* [online]. 2020 [cit. 2023-09-11]. Dostupné z: https://www.forscope.cz/blog/co-je-vpn/

[39] KOLÁŘ, *Zdeněk. Výkladový slovník z pedagogiky: 583 vybraných hesel.* Praha: Grada, 2012. ISBN 978-80-247-3710-2.

SEZNAM PŘÍLOH