Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Zabezpečení počítačové sítě

Computer network security

Bakalářská práce

Autor: Jan Štěpán
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Tomáš Svoboda, Ph.D.

Hradec Králové duben 2021

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 28.4.2021 Jan Štěpán

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Tomáši Svobodovi, Ph.D. za metodické vedení práce a veškerou další pomoc, kterou mi při vypracovávání práce poskytl.

Anotace

Práce představuje problematiku zabezpečení počítačových sítí a kybernetické kriminality. Kybernetické útoky jsou v poslední době narůstající problém a mohou způsobit škody nejen u jednotlivých uživatelů internetu, ale i ve službách a v kritické infrastruktuře. Je zde provedena analýza principu fungování počítačových sítí a jejich topologií. Společně s tím práce obsahuje kategorizaci kybernetických útoků a útočníků se zhodnocením rizik, představení možností kybernetické obrany a popsání legislativních nařízení. Výsledkem práce je vytvořená konfigurace síťových prvků modelové zabezpečené počítačové sítě, která reflektuje potřeby, jenž vyvstávají z teoretické části práce. Zároveň je výsledkem práce soubor bezpečnostních doporučení pro malou nebo střední počítačovou síť v organizaci. Aplikace zmíněných doporučení a konfigurací pomůže k zajištění bezpečnosti sítě a uchování integrity, dostupnosti a důvěrnosti dat.

Annotation

Title: Computer network security

The thesis presents the topic of computer network security and cybercrime. Cyber attacks have recently been a growing problem and can harm many internet users as well as cause damage to a lot of public online services including the critical infrastructure. There is an analysis of the principle of computer networks and their topologies. Besides that, the bachelor's thesis contains a categorization of cyber attacks and attackers with a risk assessment, an introduction to many possibilities in a field of cyber security and a description of legislative regulations. The product of the thesis is configuration of network devices represented in a model network. These network devices are protected from cyber attacks from theoretical part of the thesis. There is also a set of security recommendations for computer network. Application of those measures will help to ensure network and data security.

Obsah

Seznam obrázků

1 Úvod

Komunikace tvoří základní stavební kámen nejen našeho druhu, ale i celé moderní civilizace. Dnešní informační doba je postavena na internetu, který je využíván nejen miliardami uživatelů, ale i většinou veřejných služeb a kritických infrastruktur. Souběžně s tím kritická infrastruktura, mezi kterou se řadí například zdravotnictví nebo energetika, využívá i své vlastní počítačové sítě a systémy. Právě zmíněné služby, kritické infrastruktury a kritické informační infrastruktury se často stávají cílem kybernetických útoků. S rostoucí integrací služeb do internetu se v poslední době zvyšuje i kybernetická kriminalita, což má za následek zvýšenou potřebu se aktivně a efektivně bránit.

Je třeba se zaobírat otázkami zabezpečení a principu fungování samotného internetu i počítačových sítí v rámci modelu ISO/OSI. Nedílnou součástí je i popsání nejpoužívanějších protokolů, které z obyčejné počítačové sítě umožnily udělat moderní celosvětovou platformu. Zároveň s tím vyvstává potřeba popsat jednotlivé typy útoků a druhy samotných aktérů. Aby bylo možné se efektivně bránit, je nutné znát jednotlivé metody ochrany a zabezpečení počítačových sítí. V případě kritické informační infrastruktury platí určitá legislativní nařízení, která však pouze vyjmenují potřebná opatření a už dále nedefinují způsob, jakým se tato opatření mají realizovat.

Modelovou situaci, na které budou východiska z teoretické části prezentována, tvoří návrh sítě pro firmu dodávající software kritické informační infrastruktuře. Na firmu tak platí legislativní pravidla pro dodavatele. V praktické části práce je stěžejní řešení konkrétní implementace zabezpečení počítačové sítě.

2 Cíl práce

Cílem a účelem práce je nejen poskytnou přehled o dotyčném tématu, ale hlavně ukázat základní zabezpečení jednotlivých síťových prvků s ohledem na druhy útoků z teoretické části a vytvořit tak zabezpečený model počítačové sítě, která by eventuelně mohla být převedena do reálného světa. V rámci modelu je možné ztvárnit pouze bezpečnost sítě samotné, jelikož není možné do modelu zahrnout chování různých uživatelů.

Aby bylo možné naplnit hlavní cíl práce, je třeba nejprve splnit několik dílčích cílů, kterými jsou:

- Popis principu fungování počítačových sítí ISO/OSI modelu.
- Analýza, kategorizace a zhodnocení rizik kybernetických útoků.
- Definice jednotlivých skupin útočníků a jejich motivace.
- Představení bezpečnostních prvků a možností ochrany.
- Zahrnutí legislativních opatření pro kritickou informační infrastrukturu.

3 Metodika zpracování

Metodika zpracování různých cílů a podcílů práce zakládá v první řadě na analýze počítačových sítí a kybernetické bezpečnosti. Zdrojem pro tato teoretická východiska je primárně psaná literatura, odborné články a příspěvky či statistiky od ověřených zdrojů, které se zaobírají danou problematikou.

Zpracování modelu je podpořeno poznatky získanými během analýzy a průzkumu teoretických témat. Využito je interní nápovědy programu Packet Tracer, respektive nápovědy u konfigurace jednotlivých prvků v příkazovém řádku. V práci není využito žádného dotazníkového či jiného šetření.

Na počátku zpracovávání práce byla stanovena hypotéza, která bude dále zkoumána: „Zabezpečení počítačové sítě sníží riziko výskytu kybernetických útoků.“

4 Počítačové sítě

4.1 Úvod

Komunikace je nejdůležitější vlastností našeho druhu. Je součástí celého našeho vývoje od pravěku až v moderní civilizaci. Stejně jako jsme se měnili my, se během naší historie měnil i způsob komunikace. První zvuky a slova se postupně změnily v souvislou řeč s pravidly a gramatikou. Později vzniklo i písmo a tato slova se začala sepisovat. S psaním se začaly posílat dopisy a zprávy, které se z počátku předávaly osobně. Až o mnoho let později se začaly zprávy posílat digitálně za pomocí telegrafu a telefonu.

A dnes je zde internet – celosvětová síť, kde poslat zprávu či fotografii napříč celým světem trvá jen pár okamžiků. Během několika málo let se z internetu stalo nejen komunikační médium pro předávání informací, ale i centrum práce a zábavy mnoha z nás. Tato platforma se natolik rozšířila, že dnes každý den zasahuje do životů většiny lidí na planetě. Trávíme na internetu svůj volný čas, používáme ho k nakupování či například k vyřízení bankovnictví. Právě tato univerzálnost a rozšířenost z něj dělá ideální cíl pro napadení. Než přijde řeč na útoky a obranu proti nim, je třeba se seznámit s tím, jak počítačová síť funguje a odpovědět si na otázky: „Co je vlastně internet a jak vznikl?“ [3][20]

4.2 Historie

Bylo by vhodné začít krátkým historickým přehledem faktů a příčin, vedoucí ke vzniku největší komunikační platformy v dějinách lidstva. V první polovině 20. století lidstvo zažilo dva doposud největší konflikty, které v celé historii nemají obdoby. Jedná se o první a druhou světovou válku. Právě tyto dva zmíněné konflikty, navzdory jejich kruté povaze, znamenaly velkou revoluci, převážně v oblasti vývoje nových technologií a v rychlém předávání informací. Po druhé světové válce nastalo období studené války. Právě studená válka je obdobím vzniku předka dnešního internetu. Ve Spojených státech amerických vyvstala potřeba nahradit tehdejší centralizovanou hierarchickou telefonní síť s přepínáním okruhů novou a lepší decentralizovanou sítí s přepínáním paketů. Největší výhodou decentralizované topologie je absence hlavního prvku, který sice přispívá k lepší správě celé sítě,

nicméně představuje velké riziko ochromení systému v případě jeho výpadku. Prvním pokusem o decentralizaci byla síť s názvem ARPANET. Tato síť, jež byla spuštěna v roce 1969, spojovala v USA původně pouze vybrané univerzity. S postupem času se ale rozrostla napříč Severní Amerikou a získala na popularitě. V reakci na to začaly po světě vznikat nové sítě. Od původního ARPANETU se v roce 1983 oddělila vojenská síť (MILNET). Postupně se některé sítě spojovaly a zaváděly se společné protokoly. Důležitým milníkem je rok 1983, kdy byla nasazena sada protokolů TCP/IP, která se v novějších verzích využívá do dnes. Zároveň se začala označovat tato „síť sítí" slovem internet. S blížícím se koncem tisíciletí se masově rozšířila elektronická pošta, vznikaly první webové stránky, internetové online obchody a později i například internetové bankovnictví. Po komerční sféře se přidal i zábavní průmysl a byly vytvořeny první online hry, streamovací služby, blogy, fóra a sociální sítě. Univerzálnost celého internetu z něj udělala největší platformu světa, která se v blízké budoucnosti plánuje ještě více rozšířit, a to zejména kvůli konceptům, jakými jsou například chytré domácnosti a Internet of Things. [3][20]

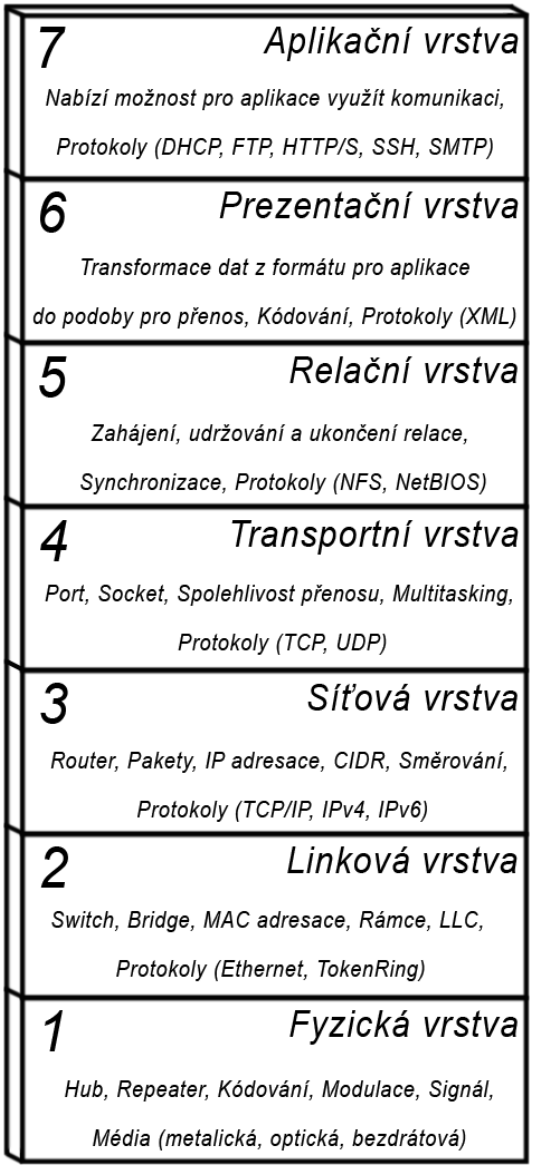
4.3 Internet

Je zřejmé, že internet změnil celý svět i nás samotné. Bylo by vhodné nyní odpovědět na druhou otázku z úvodu: Co je to internet? Jak je to s jeho fyzickým fungováním? Jak pracuje počítačová síť a z čeho se skládá?

Internet je celosvětová decentralizovaná počítačová síť s přepínáním paketů spojující mnoho menších sítí v jednu. Každá dílčí síť může nabízet určité služby, které poté mohou uživatelé využít za předpokladu, že jsou na tuto síť připojeni. Co je ale přesně počítačová síť? Jedná se o soustavu uzlů a spojů mezi nimi, která umožňuje vzájemnou komunikaci koncových klientů. Spoje jsou přímé propojení dvou prvků a slouží jako médium. Naproti tomu jsou uzly schopny předávat a směrovat datové jednotky podle potřeby z jednoho spoje na jiný. Kombinací těchto dvou prvků se může vytvořit síť, po které lze posílat data. Princip fungování počítačové sítě popisují dva základní modely – sedmivrstvý ISO/OSI model a čtyřvrstvý TCP/IP model. Je třeba si uvědomit, že oba modely popisují stejnou věc a pouze se liší v pohledu, z jakého počítačovou síť posuzují. [3][20]

4.4 Model ISO/OSI

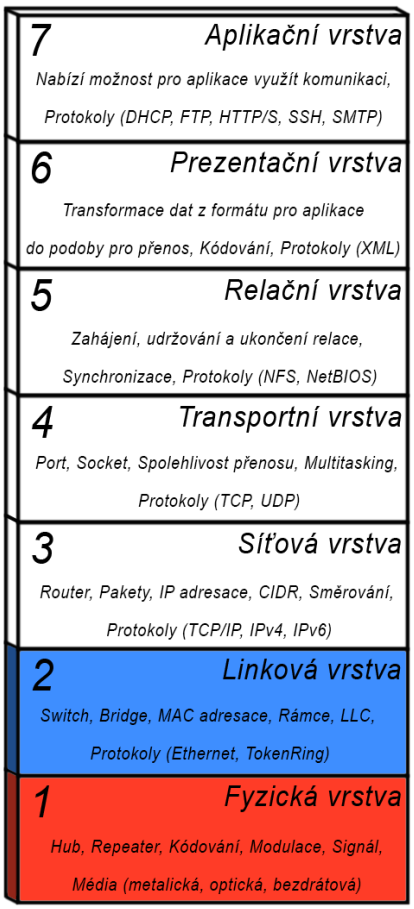
Bylo by vhodné začít detailnějším referenčním modelem ISO/OSI. Důvodem vzniku bylo vytvoření takového modelu, který rozdělí reálné fungování sítě do hierarchických, vzájemně nezávislých a oddělených vrstev. Jak již bylo zmíněno, ISO/OSI model tvoří sedm vrstev, kdy u každé z nich je definována její vlastnost, funkce a poskytované služby. Každá vrstva nabízí určitou službu a zároveň využívá ve výsledné komunikaci všechny služby vrstev, které má pod sebou. [2][3][20]



Obrázek 4-1 ISO/OSI model.
Zdroj: vlastní

4.4.1 Fyzická vrstva

První vrstvou modelu je fyzická vrstva. Úkolem fyzické vrstvy je zajistit přenos signálu (bitů) mezi dvěma body. Jedná se tedy o vrstvu, která definuje různá přenosová média, způsob komunikace na těchto médiích a fyzické prvky pro přenos signálu. Média se dají rozdělit na fyzická a bezdrátová. Fyzická média se dále dělí na metalická a optická. Mezi metalické kabely patří tlustý a tenký koaxiál a všechny varianty kroucené dvoulinky. Právě kroucené dvoulinky jsou dnes nejpoužívanějším typem metalického média. Dělí se do podkategorií podle jejich provedení, a to zejména podle izolace a opletení (UTP, STP, FTP). Optické kabely se rozřazují na jednovidové (singlevid) a vícevidové (multivid). Fyzická vrstva zároveň definuje i konektory těchto médií, jejich vysílací frekvence, modulace, kódování, popřípadě u optických vláken i vlnovou délku. Do této vrstvy se započítávají i některé prvky, které přímo souvisí s přenosem signálu. Prvkem fyzické vrstvy je hub (rozbočovač) a repeater (opakovač). [2][3][20]

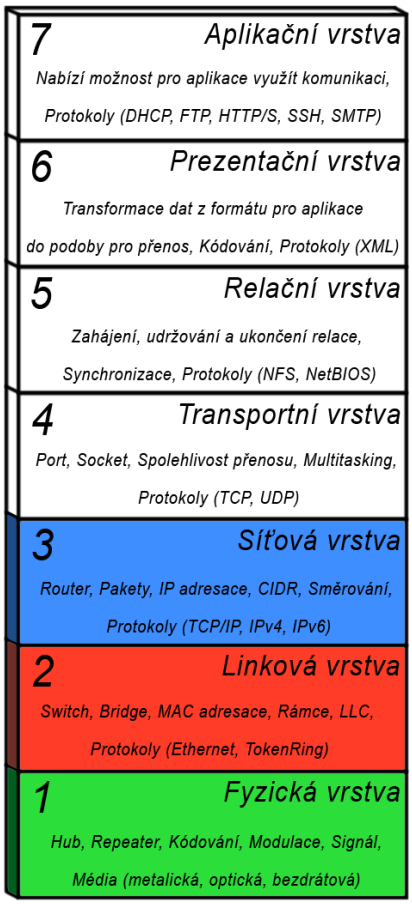


Obrázek 4-2 fyzická vrstva. Zdroj: vlastní

4.4.2 Linková vrstva

Další, v pořadí druhou, vrstvou je linková vrstva. Ta používá rámce jako datovou jednotku a adresování pomocí MAC adres. Dělí se na 2 podvrstvy, kterými jsou LLC a MAC. Zatímco LLC, která je „vyšší“ ze dvou podvrstev, operuje více s protokoly (nejčastěji Ethernet), MAC se stará o obsluhu „fyzické vrstvy“. Mezi funkce MAC podvrstvy patří například fyzická adresace, přepínání paketů pomocí definovaných metod (Store and Forward, Cut-Through), uplatňování metod přístupu k médiu a VLAN. Mezi zařízení pracující na této vrstvě patří switch (přepínač) a bridge (most). Na linkové vrstvě je možné provádět adresovatelnou

komunikaci pomocí MAC adres, kdy dosah vysílání je dán rozsahem broadcastové domény, která může být rozšířena přepínačem, popřípadě spojena s jiným segmentem sítě pomocí mostu. Funkcí celé vrstvy je poskytnou vyšším vrstvám modelu určitou „nezávislost na médiu“. Z tohoto důvodu definuje linková vrstva rámec, jakožto datovou jednotku, do které vloží pakety ze síťové vrstvy. Zároveň se vrstva stará o základní kontrolu chyb pomocí kontrolního součtu v zápatí rámce. Pokud se zjistí, že je přijatý rámec vadný, je ihned automaticky zahozen. Rámec je složen z preambule, která slouží pro synchronizaci, hlavičky, kde jsou umístěny MAC adresy zúčastněných zařízení a další doplňující informace, přeposílaných dat, označených jako náklad a patičky, ve které se nachází cyklický kontrolní součet CRC. [2][3][4][20][22]



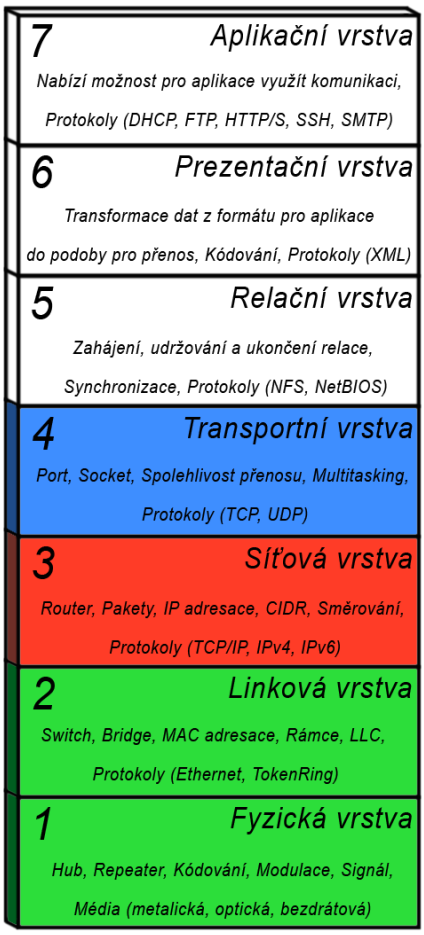
Obrázek 4-3 linková vrstva. Zdroj: vlastní

4.4.3 Síťová vrstva

Třetí vrstva modelu ISO/OSI je síťová vrstva. Datovou jednotku této vrstvy nazýváme paket. Už z názvu vyplývá, že hlavní funkcí bude rozdělení na sítě, jejich adresování a přeposílání zpráv mezi nimi. Dnes nejčastěji používaným protokolem síťové vrstvy je Internet Protocol. Dnes je stále nejrozšířenější IP ve verzi 4, nicméně postupně je nahrazován novějším IPv6. Jelikož se jedná o základ celého současného internetu, bylo by vhodné si protokol více představit a ukázat některé rozdíly mezi verzemi. Jak přesně protokol implementuje funkce síťové vrstvy?

Pro zajištění adresace sítí a koncových zařízeních používá protokol IP adresy. V paketu se tyto adresy ukládají do hlavičky. Společně s adresami je v hlavičce i mnoho podpůrných informací, mezi které patří například životnost paketu TTL.

Jedná se o informaci, která udává, kolik ještě skoků může paket udělat, než bude zahozen. Je to jednoduchý prostředek, který zaručí, že vadné pakety nebudou cestovat sítí nekonečně dlouho. Kromě životnosti jsou zde i informace o velikosti, verzi protokolu, příznacích a v neposlední řadě je zde i kontrolní součet. Za něj jsou umístěna data, která budou odeslána na adresu příjemce. Ve verzi IPv4 je adresa tvořena 32 bity, které jsou psané po 8 bitech v dekadické hodnotě oddělené tečkou. Každý byte může nabývat hodnot od 0 do 255. Příklady IPv4 adres oddělených středníkem jsou: „8.8.8.8; 198.54.65.121; 250.46.125.154“. Jelikož může IP adresa popisovat nejen uživatele, ale i celou síť, je třeba znát masku cílové sítě. Ta udává velikost každé sítě a vymezuje tak rozsah adres. Dříve zastupovaly masku třídy IP adres (A, B, C, D, E), nicméně jejich velice hrubé dělení bylo později nahrazeno CIDR bloky, které používají dělení po bitu, namísto dělení po 8 bitech. Výhodou CIDR bloků bylo výrazné snížení plýtvání s IP adresami a umožnění podsíťování, neboli hierarchického přidělování adres. To, i další opatření jako například NAT, prodloužilo použitelnost protokolu IPv4 o několik let. I přes všechny snahy nakonec došlo k vyčerpání adresního prostoru a bylo tedy třeba uvažovat o jiném řešení.



Obrázek 4-4 síťová vrstva. Zdroj: vlastní

V tu dobu přichází nová verze protokolu IP verze 6. Ta se dočkala mnohých vylepšení, a to nejen v oblasti adresního prostoru, ale i například v bezstavové autokonfiguraci (SLAAC) či v rozšiřujících hlavičkách. IP adresa ve verzi 6 byla rozšířena z původních 32 bitů na 128 bitů, což oproti původním přibližně 4,3 miliardám adres rozšířilo celý prostor na 2^{128} ($3{,}4*10^{38}$) adres. Zároveň se změnila hlavička paketu, která je nyní přehlednější, zbavena kontrolního součtu a udělána tak, že veškeré dodatkové služby se budou přidávat podle potřeby jako

další rozšiřující hlavičky. K polovině roku 2020 je celosvětová průměrná integrace IPv6 u uživatelů asi 40 %. [1]

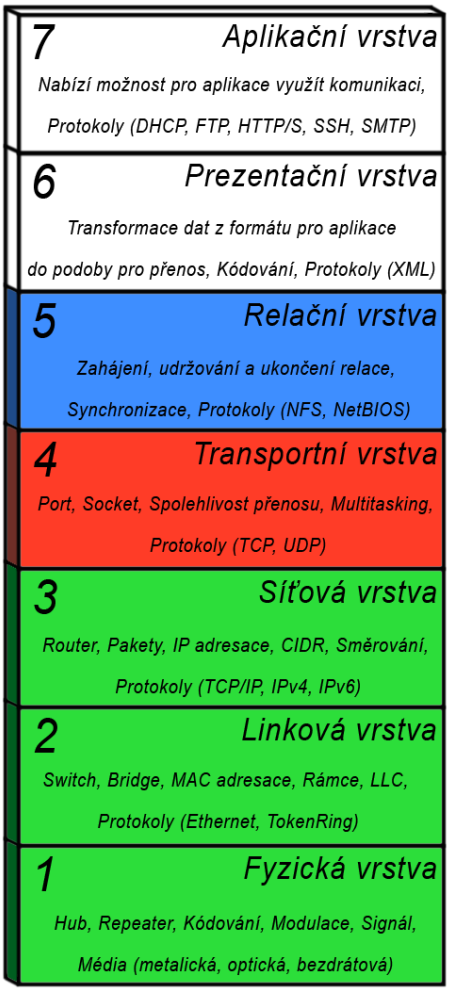
Toto byl základní přehled Internet Protokolu, pracujícího na síťové vrstvě ISO/OSI modelu. Jak bylo řečeno, na této vrstvě probíhá kromě adresace sítí i směrování. Prvek pracující na třetí vrstvě se nazývá router (směrovač). Směrování je proces, při kterém se router rozhoduje, na které rozhraní poslat přijatý paket, aby dorazil do svého cíle. Směrování je možné rozdělit na statické a dynamické, nicméně proces jako takový je stejný, liší se pouze v tom, jak se router daný směr dozvěděl. Zda byl zadán ručně, v případě statického směrování, nebo zda byl zaslán jiným routerem pomocí některého dynamického směrovacího protokolu (RIP, OSPF, EIGRP, BGP). Router po přijetí paketu zkontroluje v hlavičce adresu příjemce a porovná ji s adresami, které má ve své směrovací tabulce. Hledá co nejpřesnější shodu se svým záznamem adres. Pokud nenajde kýžený záznam, nastává jedna ze dvou situací. V prvním případě, pokud má router nastavenou výchozí bránu, která je definována IP adresou 0.0.0.0 s maskou sítě 0.0.0.0, odešle router paket na definovanou výstupní adresu nebo rozhraní vedoucí k této bráně. V opačném případě, pokud není nakonfigurovaná výchozí brána a není nalezena cílová síť, router zahodí dotyčný paket. Síťová vrstva nám tedy poskytuje základní strukturu a komunikaci v sítích. [2][3][4][20][22]

4.4.4 Transportní vrstva

V pořadí čtvrtá vrstva modelu ISO/OSI se nazývá transportní vrstva. Jak již bylo dříve zmíněno, linková vrstva nám poskytuje základní kontrolu chyb v každém rámci a síťová vrstva je schopna zahodit pakety, které nemůže poslat do jejich destinace, či cestují sítí již příliš dlouho. Avšak nic z výše uvedených nedokáže zajistit, že příjemce data, která potřebuje bezpečně a spolehlivě získat, opravdu dostane. Kontroly chyb na nižších vrstvách se pouze zbavují vadných jednotek, ale už nepočítají s jejich znovu odesláním. A právě toto je jeden z problémů, které řeší transportní vrstva pomocí implementace protokolů TCP a UDP.

Protokol TCP zajišťuje spolehlivost přenosu a garantuje doručení dat. Je třeba poukázat na fakt, že tato spolehlivost je implementována tak, že pokud dorazí

vadný paket a je zahozen, tak je znovu vyžádán od odesílatele. Nejedná se o zbavení chyb v komunikaci, jako spíš o opravení či jisté nahrazení chybějících nebo poškozených dat. Bezchybnost přenosu rámců a paketů jako takových TCP neumí zaručit. U protokolu TCP se vyskytuje relativně velká režie, a proto ho není vhodné používat u veškeré komunikace. Na místech, kde je potřeba potvrdit přijatá data, což je například u přenášení souborů, či posílání DNS záznamů mezi DNS servery, je tento způsob vyžadován. Celý proces komunikace TCP zahajuje třícestný handshake. Jedná se o metodu, kdy se obě strany domluví na parametrech komunikace. Až poté začne vlastní přenos, který je pravidelně kontrolován, podle domluvené velikosti okna. Po odeslání dat je vyžadováno spojení také uzavřít. Tento celý proces by trval příliš dlouho a zbytečně by zatěžoval síť, jen aby odeslal data, u kterých není vyžádáno potvrzení.



Obrázek 4-5 transportní vrstva. Zdroj: vlastní

Z tohoto důvodu vznikl i druhý protokol, který je de facto opakem k TCP a tím je protokol UDP. Tento protokol posílá datagramy, které jsou jednoduché a nemají žádnou kontrolu doručení. Toto řešení je výhodné pro typ komunikace, kde výpadek jednoho či několika málo paketů je irrelevantní. UDP se používá pro internetová vysílání, ať už hudby, videí, videokonferencí, pro přenášení hlasu a v neposlední řadě pro komunikaci klienta s DNS serverem, kde při výpadku dotyčného paketu pošle klient nový dotaz po určitém časovém limitu a není třeba kvůli každému dotazu navazovat TCP připojení.

Společně se zajišťováním spojení řeší transportní vrstva i další problém. Internet se rozšiřoval a aplikací, které ho využívali, rapidně přibývalo. Pro odlišení aplikací, které si příchozí data vyžádaly, zavedla transportní vrstva port. Jedná se

o číslo, které identifikuje aplikaci či službu, pro kterou jsou data určena. Rozsah identifikátoru portu je určen 16 bity, které se předvádí do dekadické soustavy. Čísla portů jsou tedy v rozsahu od 0 do 65535. Port společně s IP adresou tvoří soket. [2][3][20][22]

4.4.5 Relační vrstva

Další, v pořadí již pátou, vrstvou je relační vrstva. Jak název napovídá, vrstva zajišťuje správu relací zúčastněných stran. Vytváří, synchronizuje, ukončuje a obnovuje spojení mezi klienty. Vrstva zajišťuje funkce autentizace, autorizace a synchronizace. [2][3][4]

4.4.6 Prezentační vrstva

Předposlední vrstvou ISO/OSI modelu je prezentační vrstva. Tato vrstva přetváří data z vyšší aplikační vrstvy na data, která jsou připravena na předání nižším vrstvám k jejich následnému odeslání. Prezentační vrstva nezná význam transformovaných dat. Na straně příjemce funguje prezentační vrstva opačně, neboť překládá přijatá data do podoby dat, které potřebují aplikace ve vyšší vrstvě. [2][3][20]

4.4.7 Aplikační vrstva

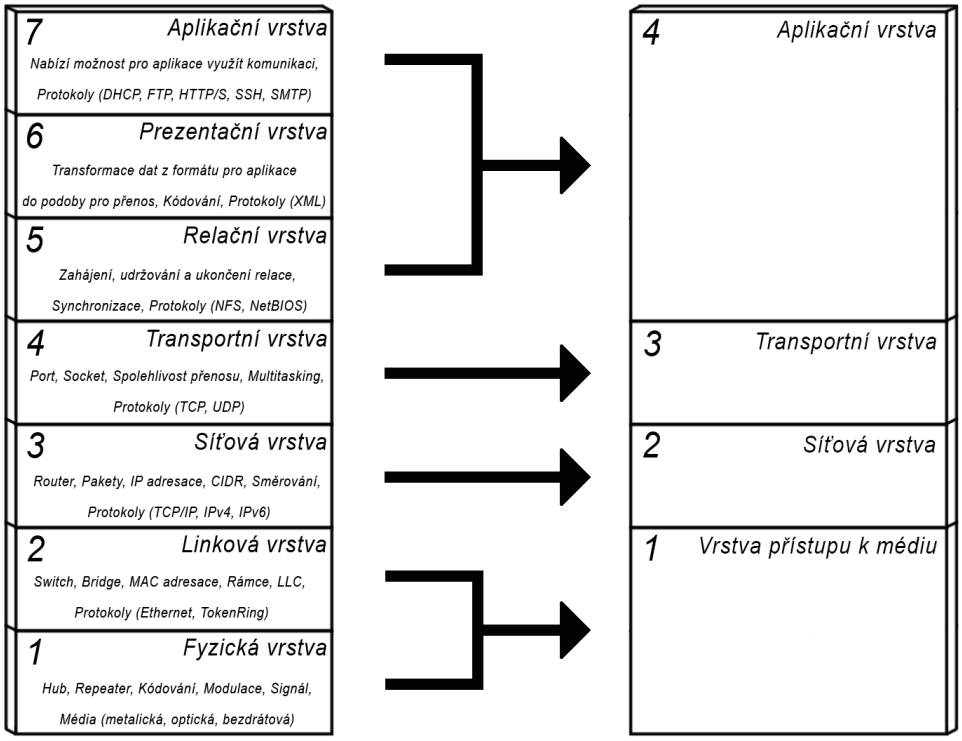
Poslední, sedmá, vrstva se nazývá aplikační. Tato vrstva je nejblíž k uživateli a jedná se o veškeré služby, které umožňují běžným aplikacím využít komunikaci přes počítačovou síť. Operují zde protokoly a služby jako DHCP, HTTP, FTP, SSH, POP3, SMTP, DNS a mnoho dalších. [2][3][4][20]

4.4.8 Komunikace ISO/OSI

Celý proces komunikace funguje tak, že se u odesílatele vygenerují data v sedmé vrstvě. Ty postupně propadávají vrstvami směrem dolů k první vrstvě. Každá vrstva přidá k datům svou funkční část. Když data dorazí na první vrstvu, začíná proces posílání dat od odesílatele. Cestou k cíli jsou data, podle síťových prvků, na které narazí, z části rozbalena a poté opět zabalena. Jakmile data dorazí k příjemci, začínají je vrstvy postupně rozbalovat a dekódovat.

4.5 Model TCP/IP

Na začátku bylo zmíněno, že kromě ISO/OSI modelu existuje i čtyřvrstvý model TCP/IP. Oba protokoly, které má druhý model v názvu, již byly krátce představeny. Právě z jejich pohledu je konstruován TCP/IP model, což má za následek zachování síťové a transportní vrstvy, na kterých dané protokoly operují. Nicméně došlo ke spojení ostatních vrstev. Všechny vrstvy nad transportní vrstvou jsou sjednoceny v aplikační vrstvu a linková vrstva s fyzickou vrstvou je sloučena ve vrstvu přístupu k médiu. [3][20][22]



Obrázek 4-6 porovnání ISO/OSI a TCP/IP modelu. Zdroj: vlastní

4.6 Topologie

Základní princip fungování počítačových sítí byl představen. V úvodu bylo zmíněno, že internet vznikl jako náhrada za původní hierarchickou telefonní síť. Internet jako takový je decentralizovaný, což znamená, že nikde není jeho hlavní ústředna a celá zátěž se rozkládá po celé síti. Nicméně zde existuje několik topologií, které se v internetu vyskytují.

První a nejjednodušší topologií je sběrnice. Jedná se o jednu společnou linku sdílenou několika klienty, na kterou se každý připojí. Mezi její výhody patří nízká

cena a jednoduchost. Za nevýhodu by se dalo považovat zarušení a omezená kapacita z důvodu přítomnosti několika klientů na společném médiu. [3][22]

Z důvodu možného rušení je třeba použít přístupovou metodu k médiu. U protokolu Ethernet se jedná o metodu CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Tato přístupová metoda naslouchá na médiu a vysílá pouze tehdy, když nedetekuje na lince probíhající provoz. Problém nastává, když ve stejnou chvíli začnou vysílat dvě stanice. Rušení je díky interferenci vlnění rozpoznáno jako součet amplitud signálů a každé zařízení si nastaví svou časovou jednotku na náhodný čas, po kterém může začít opět normálně vysílat. Kolize je detekována a vyřešena způsobem, kdy obě stanice, které původně vysílaly, mají nastavený náhodný čas, než mohou opět začít vysílat. Šance, že obě stanice dostanou stejný čas je velmi malá. Existuje i druhá metoda CSMA/CA, která se nejčastěji používá na IEEE 802.11 (Wi-Fi) sítích. Písmena v názvu přístupové metody znamenají doslova předcházení kolizím (Carrier Sense Multiple Access with Collision Avoidance). Tato metoda funguje v principu na přihlášení se o komunikaci. V podstatě se jedná o stejný systém, který většina lidí zná ze školy jako: „Kdo chce mluvit, tak se musí nejdříve přihlásit o slovo." [3][22]

Další z topologií je kruhová topologie. Klienti se propojí navzájem tak, že vznikne kruh a komunikace probíhá přes jednotlivé stanice. Aby se zamezilo rušení je zde často posílán token. Klient, který drží token, může vysílat, zatímco ostatní pouze naslouchají. Po určitém časovém limitu se token pošle dalšímu uživateli a takto cestuje v síti mezi všemi klienty. Výhodou této topologie je cena, jednoduchost a absence rušení. Nevýhodou je modifikace topologie, při které musí být pro přidání nového klienta síť na chvíli přerušena a odstavena. Zároveň se zde objevuje riziko, kdy jedna ze stanic vypadne a přeruší tím komunikaci. Celý tok dat je směrován skrz další stanice, což může znamenat potenciální bezpečnostní riziko. V některých případech se využívá dvojitý kruh pro větší robustnost sítě. [3][22]

Příkladem centralizované topologie je hvězdicová topologie. Hvězda se skládá ze stanic, které jsou připojeny do společného prvku. Výhodou i nevýhodou je právě společný prvek, který poskytuje řízení celé sítě, nicméně při jeho výpadku dojde k ochromení celé struktury. Při výpadku stanice, či jejího spoje, dojde

k přerušení spojení pouze pro danou stanici, a ne pro další klienty. Za nevýhodu se dá považovat i vyšší pořizovací cena z důvodu nutnosti nákupu centrálního prvku.

Bude-li se vycházet z hvězdicové topologie a uspořádá se do více hierarchické struktury, vznikne stromová topologie. Jedná se o zřetězené zapojení hvězdicových topologií. Výhoda spočívá ve skutečnosti, že pokud vypadne centrální prvek, pak zbytek větve funguje dále bez problémů. Nevýhodou může být právě výpadek centrálního prvku, který znepřístupní komunikaci mezi větvemi. [3][22]

Další a nejdražší topologií je úplná topologie. Ta spojuje všechny prvky se všemi a vytváří tak přímá spojení mezi všemi uživateli. Je extrémně drahá a složitá, nicméně poskytuje spojení všem se všemi, což v praxi znamená, že pokud vypadne jeden spoj, neohrozí, ani jinak neomezí zbytek sítě. [3][22]

Poslední je smíšená topologie. Mezi uzly existují kromě nezbytných spojů i redundantní spoje. Výhodou této topologie je odolnost proti výpadku spoje či celého uzlu, jelikož se zde nachází určitá míra redundance. Nevýhodou je absence řídícího prvku či sdíleného média. To v praxi znamená, že je třeba na prvcích nastavit statické, nebo dynamické směrování toku dat. [3][22]

Všechny vyjmenované topologie se dnes více, či méně používají a mají své klady, zápory a uplatnění. V koncových sítích je možné nalézt zejména hvězdicovou topologii s výjimkou velkých korporátů a firem, kde se spíš lze setkat se stromovou topologií. Na druhou stranu ve spojovacích sítích lze nalézt často smíšenou topologii, kdy některé její menší segmenty mohou tvořit topologii úplnou. [3][22]

5 Kybernetická bezpečnost

5.1 Úvod

Nástup internetu znamenal revoluci ve způsobu, jakým lidstvo doposud komunikovalo a ovlivnil i směr, kterým se komerční, zábavní a mediální průmysl odvíjí. S přibývajícím počtem uživatelů a služeb se začal zvyšovat i počet kybernetických útoků. Kybernetická kriminalita, stejně jako běžná kriminalita, má mnoho podob, různé důsledky a důvody. Se zmíněným nárůstem se ale začal vyvíjet i způsob obrany proti těmto útokům. V rámci zachování konkurence na trhu a také z důvodu velkému množství specializovaných programů, však nemůže být nařízeno používání jednoho „bezpečného“ softwaru, který by eliminoval většinu potenciálních útoků. Právě proto je dnešní obrana proti kybernetické kriminalitě soubor pravidel a doporučení, které zamezí samotným útokům, popřípadě zmírní škody, které by mohly nastat. Zároveň s legislativními opatřeními je i součástí počítačové bezpečnosti proškolení a znalosti samotných uživatelů. Příkladem může být kategorie útoků zvaná sociální inženýrství. Ta nevyužívá bezpečnostních slabin uvnitř systému jako takového, ale nepozornosti uživatelů. Může se jednat o telefonáty, které postupně zjišťují informace o firmě a její struktuře, o podvodné emaily s přílohou obsahující malware nebo například o email s falešným odkazem vedoucím na jinou stránku, než na kterou si uživatel myslí, že jde. Z tohoto důvodu platí legislativní pravidla, podle kterých se musí zabezpečit jednotlivá zařízení, na kterých jsou citlivé údaje a musí se proškolit či poučit uživatel používající toto zařízení.

5.2 Kritická infrastruktura

Obecně platí, že kybernetická bezpečnost je obor, který má za úkol chránit systémy před napadením či minimalizovat dopady kybernetických útoků. Přísná bezpečnostní pravidla a restrikce však není potřeba aplikovat na veškeré systémy na světě. Pojem kritická infrastruktura vymezuje takové oblasti lidské činnosti, které je však nutné zabezpečit. Jedná se o takové služby a odvětví, které jsou nezbytné pro chod organizační jednotky, nad kterou jsou pravidla vytvářena.

V tomto případě, kdy organizační jednotkou je stát, je třeba ochránit všechny prvky, které jsou nezbytné pro chod samotného státu a veškeré služby nezbytné k uspokojení základních potřeb obyvatel dané země. Musí být tedy zaručena maximální ochrana infrastruktury v segmentech energetiky, dopravy, bankovnictví, infrastruktury finančních trhů, zdravotnictví, vodního hospodářství, digitální infrastruktury a chemického průmyslu.[6] Právě výše vyjmenovaná odvětví jsou nezbytné pro zachování bezpečnosti a integrity státu.

5.3 Kritická informační infrastruktura

S kritickou infrastrukturou rovněž souvisí pojem kritická informační infrastruktura, která je definována v zákonu o kybernetické bezpečnosti 181/2014 Sb. následovně: *„V tomto zákoně se rozumí kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti“*.[6] Určování systémů, které patří do kritické informační infrastruktury, je realizováno za pomocí kritérií a následné charakteristiky daného systému. Pokud dotyčný systém splňuje podmínky pro zařazení do kritické informační infrastruktury, pak jsou na něj kladeny požadavky na určitý druh zabezpečení. Diagram, který detailně popisuje kritéria pro zařazení do kritické infomační infrastruktury, je v příloze práce. (Příloha č.1)

V podstatě se jedná o důležité informační systémy kritické infrastruktury a o veřejné komunikační systémy, které využívá větší počet lidí. Zároveň se do této skupiny řadí i veřejné databáze, které obsahují statisíce osobních informací či lékařských záznamů. Tyto systémy podléhají nutnosti být řádně zabezpečeny. Je zde především kladen důraz na bezpečnost informací a zaručení důvěrnosti, dostupnosti a integrity dat.[6][8]

Důvěrnost je ve slovníku pojmů z kybernetické bezpečnosti definována jako: „*Vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.*“[8] Tento pojem vyjadřuje nárok na diskrétnost pro data a informace kritické informační infrastruktury. Provozovatel systému musí zajistit, aby se k datům nedostala žádná neoprávněná osoba. Zabezpečit je třeba jak fyzický, tak vzdálený přístup k datům. Důvěrnost lze kupříkladu zajistit po fyzické stránce uzamčením serverové místnosti či povolením

přístupu pouze vybraným zaměstnancům. Z pohledu vzdáleného přístupu se může jednat o použití VPN a uzamčení nevyužitých portů.

Další složkou bezpečnosti informací je dostupnost. Ta značí vlastnost přístupnosti a použitelnosti dat, které si oprávněná entita může kdykoliv vyžádat.[8] Systém musí být navržen a zabezpečen tak, že data musí být neustále k dispozici. Této vlastnosti lze dosáhnout například kvalitním zabezpečením, decentralizací nebo redundantním systémem. Z fyzického hlediska se může jednat i o záložní napájení ve formě generátoru, baterie UPS nebo připojení na více nezávislých elektrických okruhů.

Třetím pojmem, tedy integritou dat, se rozumí: „*Vlastnost přesnosti a úplnosti. Jistota, že data nebyla změněna.*“[8] U důležitých dat a informací je třeba zajistit, že data, která se ukládají nebo posílají, jsou pravdivá, nezměněná, validní a konzistentní. Integrity dat se dá dosáhnout pomocí hashovacích funkcí, kontrolních součtů, duplicity nebo samo-opravných kódů.[8] Integrita však nemusí být narušena pouze chybou při přenosu, ale také například při cíleném útoku. V takovém případě na málo zabezpečené síti může být útočník schopen zastat roli jednoho z přenosných bodů a informace číst a měnit během přenosu. Obranou proti takové ztrátě integrity je například využití šifrovaných protokolů či využití SSL certifikátů. Integrita přenosu dat je nutná, neboť je nezbytné, aby příchozí informace přesně a věrně reprezentovala informaci odesílanou.

5.4 Bezpečnostní opatření

Bude-li se vycházet z legislativy pro Českou republiku, která je dána zákonem o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) a vyhláškou o kybernetické bezpečnosti (vyhláška č. 82/2018 Sb.), rozdělují se bezpečnostní opatření do dvou hlavních kategorií. Následující organizační a fyzická opatření a jejich definice budou brána z vyhlášky o kybernetické bezpečnosti. [6][7]

5.4.1 Organizační opatření

Systém řízení bezpečnosti informací – jedná se o základní stavební kámen řízení kybernetické bezpečnosti v organizaci. Do této části spadá vymezení cílů a rozsahu pro řízení bezpečnosti informací, zavedení a schválení bezpečnostní politiky, zajištění provedení bezpečnostního auditu, zavedení bezpečnostních opatření a jejich následná průběžná evaluace společně se zhodnocením celkového stavu systému.

Řízení aktiv – je veškerá správa aktiv. Povinná osoba v rámci řízení aktiv stanoví pravidla pro jejich identifikaci, dále eviduje samotná aktiva a určí garanty jednotlivých aktiv. Hodnocení aktiv probíhá z hlediska důvěrnosti, integrity a dostupnosti. Následně jsou tato primární aktiva zařazena do několika úrovní. Zde se rozlišuje rozsah a důležitost údajů, rozsah narušení vnitřních činností, poškození zájmů organizace s výsledkem peněžní ztráty či například vliv na průběh činnostní a veřejných služeb organizace. Zároveň se určí vazby mezi primárními a podpůrnými aktivy, které jsou následně zhodnoceny. Pro každou úroveň aktiv je vytvořena skupina pravidel na zacházení s daným aktivem, jeho přenos, duplikaci, sdílení a likvidaci.

Řízení rizik – pojednává o nastavení bezpečnostních limitů. Hlavní funkcí této fáze je kategorizace rizik, stanovení akceptovatelnosti rizik, zhodnocení možných dopadů hrozeb, vypracování ohodnocení rizik a vymezení hrozeb a zranitelností v návaznosti na jednotlivá aktiva. S tím související zpracování výsledků hodnocení rizik, které obsahuje aplikované i neaplikované bezpečnostní opatření a odůvodnění nepoužití, či naopak způsob plnění daného opatření. Dalším důležitým krokem je i zavedení plánu zvládání rizik včetně identifikace důležitých osob, prostředků a způsobů řešení incidentů.

Organizační bezpečnost – stanovuje bezpečnostní politiku včetně rozdělení osob a zdrojů potřebných pro řízení bezpečnosti. Součástí je i informování zaměstnanců, stanovení firemních pravidel, neustálé prosazování zlepšování systému a zachování diskrétnosti u lidí, kteří mají větší vhled do systému. Vyhláška definuje několik rolí, které by měly být zastoupeny a vykonávány. Jsou jimi manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, garant aktiva

a auditor kybernetické bezpečnosti. Právě tyto role společně s administrátory musí zachovat diskrétnost a nesmí odhalit zabezpečení systému neautorizované osobě.

Bezpečnostní role – jsou přiřazeny důvěrným osobám, které mají na starosti bezpečnost. Pro jejich vykonávání je zapotřebí patřičného vyškolení a odborná praxe. První rolí je manažer kybernetické bezpečnosti. Tato role je odpovědná za celý systém řízení bezpečnosti informací. Manažer pravidelně informuje vedení o činnostech a stavu systému. Druhou rolí je architekt kybernetické bezpečnosti, který vhodně navrhuje bezpečnostní opatření. Třetí zmiňovanou rolí je garant aktiva. Úkol této role spočívá v zajištění rozvoje, použití a v samotné bezpečnosti aktiva. V poslední řadě se zde nachází auditor kybernetické bezpečnosti. Osoba s touto rolí odpovídá za provádění auditu kybernetické bezpečnosti, který musí být nezaujatý. Z povahy pracovní náplně jednotlivých rolí nesmí auditoři s manažery zastávat jinou bezpečnostní roli v organizaci.

Řízení dodavatelů – řeší evidenci dodavatelů a definuje pro ně pravidla, se kterými je také seznamuje. Současně řídí rizika spojená s dodavateli, kontroluje nově uzavírané smlouvy, zda splňují bezpečnostní opatření a při změnách v bezpečnosti prochází již uzavřené smlouvy, jestli splňují definované závazky na řízení bezpečnosti informací.

Bezpečnost lidských zdrojů – sestavuje plán rozvoje, podle kterého následně probíhá vzdělávání, proškolování a informování zaměstnanců, administrátorů a osob s bezpečnostní rolí. Ti jsou poučení o pravidlech bezpečnosti, jejich funkci v systému a v neposlední řadě jim je zajištěno potřebné školení.

Řízení provozu a komunikace – pojednává o celkovém přístupu k provozu a komunikaci v organizaci s ohledem na bezpečnost informací. Zavádí standardy a postupy pro spuštění, ukončení a obnovu systému po mimořádné události, povinnosti a práva zaměstnanců, administrátorů a osob s bezpečnostní rolí, řízení technických zranitelností a definuje postupy sledování kybernetických událostí. Součástí tohoto opatření je i určení intervalu pro zálohování dat.

Řízení změn – analyzuje nadcházející změny v systému a vyhodnocuje jejich dopad a rizika na systém. Všechny významné změny musí být zaznamenány a je-li to nutné, pak po některých je potřeba změnit či upravit bezpečnostní politiku. Každá změna v systému by měla být předem zhodnocena, otestována pomocí penetračního

testu a udělána tak, že existuje možnost vrátit systém do původního konzistentního stavu, jestliže by tato změna narušila současný fungující stav systému.

Řízení přístupu – rozděluje přístup k informačním a komunikačním systémům pomocí mechanismu přístupových práv. Cílem je eliminace přístupu k částem systému nepovolanou osobou. Každý zaměstnanec a administrátor dostane patřičná práva k přístupu do systému. Do řízení přístupu patří i odebírání práv zaměstnancům, kteří odchází z organizace či při změně bezpečnostní politiky. Hlídají se i používaná zařízení zaměstnanců společně s nainstalovaným softwarem. Snaha je tak o eliminaci přístupu do systému z neověřeného, potenciálně nebezpečného, zařízení, které může obsahovat malware, či jiný škodlivý kód.

Akvizice, vývoj a údržba – definuje postup, který je nutné zajistit při získání nového aktiva. Přidání aktiva do systému zahrnuje znovu provést řízení rizik, určit významné změny a s tím spojená rizika, stanovení bezpečnostních požadavků a jejich následná aplikace do systému. Tím, že se jedná o změnu je třeba důkladně otestovat funkčnost, bezpečnost a ochranu dat.

Zvládání bezpečnostních událostí a incidentů – určuje pravidla pro situace, kdy nastane bezpečnostní incident. I v dobře zabezpečeném systému se může objevit slabina či na něj může být zaútočeno z vnější strany. V takovém případě je nutné incident co nejrychleji detekovat, identifikovat, neutralizovat, obnovit stabilní stav systému, jestliže byl narušen a incident zaznamenat a nahlásit. Bezpečnostní incident, či jinou slabinu v systému může zaznamenat sám administrátor nebo se o nahlášení mohou postarat zaměstnanci, kteří musí být předem poučeni o nutnosti a způsobu takového nahlašování. V závislosti na rozsahu se určí, zda se jednalo o kybernetickou událost, nebo incident. Dalším nezbytným krokem je i analýza útoku a vhodné upravení bezpečnostní politiky, aby v budoucnosti nedošlo k využití stejné slabiny, či se co nejvíce oslabil další podobný útok.

Řízení kontinuity činností – hodnotí rizika a analyzuje dopady kybernetických incidentů. Na základě těchto dat poté stanoví minimální doby odstavení a úrovně služeb, aby nebyla narušena kontinuita činnosti. Jedná se tedy o vymezení funkcí, které jsou nezbytné pro zajištění služeb či o dobu, po kterou může být systém maximálně vyřazen, aby nedošlo k ohrožení služby poskytované organizací. Tyto krizové plány jsou následně testovány a upravovány podle potřeby.

Audit kybernetické bezpečnosti – dokumentuje a zaznamenává dodržování bezpečnostní politiky. Částečný audit je prováděn při důležitých změnách právě v dané oblasti, kde se změna uskutečnila. Celkový audit je prováděn pravidelně každé 2 až 3 roky. Audit musí být nezávislý a realizovaný osobou, která se nijak neangažuje v další bezpečnostní roli v organizaci. Výsledky auditu jsou předváděny správci daného informačního systému.[7]

5.4.2 Technická opatření

Souběžně s první kategorií zde stojí i druhá kategorie, která řeší naopak technická opatření. Na rozdíl od organizačních požadavků na bezpečnost, které řešili bezpečnostní politiku organizace, bezpečnostní role a obecný přístup k informacím a nakládání s těmito informacemi, se jedná o fyzické prvky zabezpečení, používané šifrování a možnosti aktivní obrany proti škodlivému kódu. Technická opatření tedy neřeší bezpečnost z pohledu organizace a její struktury. Mezi technické opatření se řadí následující pojmy.

Fyzická bezpečnost – vyjadřuje požadavky na fyzickou bezpečnost aktiv. Ta je třeba chránit před poškozením, zneužitím nebo proti krádeži. Prostředkem, kterým lze dosáhnout fyzické bezpečnosti je vymezení chráněné oblasti. Oblast by měla být chráněna a zabezpečena proti všemu, co by mohlo narušit chod služeb či důvěrnost, dostupnost a integritu dat. Je žádoucí, aby taková oblast byla zabezpečená nejen proti lidskému narušení, ale také proti vlivům prostředí a přírody. Myslet je třeba například na záložní zdroje energie nebo pokud je to možné, tak na vyvarování se rizikovým geografickým oblastem, které by mohly způsobit odstavení systému. Hlavním cílem fyzické bezpečnosti je zajištění kontinuity poskytovaných služeb a znemožnění přístupu neautorizovaných osob.

Bezpečnost komunikačních sítí – definuje pravidla pro bezpečný přenos po síti a její správné rozdělení. Jedním z prvků bezpečnosti sítě je její vhodná segmentace. Rozdělení na část, která tvoří logický celek a je oddělena od zbytku sítě. Jelikož se jedná o komunikaci na síti, je třeba zajistit šifrování dat, které pomůže zajistit důvěrnost dat. Dalším stavebním kamenem bezpečné sítě je ochrana proti nežádoucí komunikaci, realizovaná nejen segmentací samotné sítě, ale i například

přes filtry ACL. Síť jako taková by měla držet co největší integritu. Toho je možné docílit kupříkladu zálohováním konfigurací prvků a zvolením vhodné topologie.

Správa a ověřování identit – je další část technických opatření řešící autorizaci a autentizaci uživatelů, kteří chtějí přistupovat do zabezpečené části systému. Mezi nástroje pro ověření identity osob přistupujících k systému patří přihlášení, nastavení počtu neúspěšných pokusů o přihlášení, ochrana uložených zašifrovaných autentizačních údajů v systému před krádeží, ověření identity po určité době neaktivity a centralizovaná správa identit. V důležitých systémech se využívá více faktorového mechanismu přístupu, který kombinuje faktor znalostní s faktorem vlastnickým. Přihlášení není prováděno pouze za pomocí loginu a hesla, nýbrž i například se zadáním zaslaného kódu z mobilního telefonu uživatele či za použití hardwarového klíče. V některých případech není možné okamžité zavedení více faktorového ověřování. V těchto případech je mezitím zapotřebí systém zabezpečit jinými způsoby, především podmínkami na složitost hesel. Minimální délka hesla musí být alespoň 12 znaků u uživatelů a 17 znaků u administrátorů. Velikost pole pro heslo musí být dlouhé alespoň 64 znaků a nesmí být omezené používání písmen, speciálních znaků nebo číslic. Systém nesmí umožnit uživatelům nastavit si jako heslo nejčastěji používaná hesla, alespoň 12 předchozích hesel a hesla, kde se mnohokrát za sebou opakují stejné znaky nebo obsahují jméno či email uživatele. Dále je stanoven interval změny hesla, který nemůže být delší než 18 měsíců. Při vytvoření nového účtu nebo při změnách v pravidlech hesel je zapotřebí co nejdříve vynutit změnu u uživatelů systému.

Řízení přístupových oprávnění – vyjadřuje potřebu řízení přístupových oprávnění jednotlivých uživatelů systému. Uživatelům je dán přístup k určitému aktivu, nebo se jedná o práva pro čtení a zápis jednotlivých dat. Osoba pověřená řízením přístupových práv může kdykoli změnit oprávnění jednotlivým uživatelům.

Ochrana před škodlivým kódem – stanovuje požadavky na zabezpečení zařízení důležitých aktiv. Vyžaduje nasazení aktivní ochrany na těchto zařízeních. Nepřetržitá automatický ochrana se vztahuje na koncové stanice, mobilní zařízení, servery, datové úložiště a nosiče, komunikační sítě a jejich prvky a další obdobná zařízení. Paralelně se samotným monitorováním se řeší i oprávnění ke spuštění cizího kódu. Pravidlem kvalitního fungování ochrany je aktualizace operačního

systému a antivirového programu. Dalším významným krokem k lepší ochraně proti škodlivému kódu je poučení uživatelů systému a jejich školení v základním rozpoznání potenciálních hrozeb.

Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů – je jedním z principů fyzické bezpečnosti a spočívá ve vytváření logů aktivity systému a jeho uživatelů. Rozsah zaznamenávání aktivit závisí na důležitosti sledovaného aktiva. Rozpoznáváme 2 druhy událostí, a to bezpečnostní a provozní události. U obou kategorií se zaznamenávají důležité informace, kterými jsou datum a čas, typ činnosti, identifikátor účtu a zařízení ze kterého byla činnost provedena, identifikátor aktiva, které činnost zachytilo a zda operace byla úspěšná či nikoliv. Souběžně se zaznamenává i stav systému, převážně tedy přihlašování a odhlašování všech uživatelských účtů, neúspěšné pokusy o přihlášení, akce provedené administrátory, veškeré manipulace s účty a právy, neúspěšné činnosti, které selhaly z důvodu nedostatečných práv, činnosti uživatele ohrožující systém a činnosti technických aktiv včetně kritických i chybových hlášení. Všechny vytvořené záznamy je nutné zabezpečit před veškerými změnami. Veškeré pokusy o změnu logů jsou taktéž zaznamenávány a ukládány. Jelikož je součástí všech záznamů časový údaj, musí se alespoň jednou za den ve všech technických aktivech synchronizovat čas. Vytvořené logy je nutné nadále ukládat minimálně po dobu 12 až 18 měsíců v závislosti na důležitosti aktiv.

Detekce kybernetických bezpečnostních událostí – ukládá povinnost ověřovat a kontrolovat provoz na síti a detekovat kybernetické bezpečnostní události. Míra detekce je závislá na důležitosti aktiva. Detekce je prováděna na koncových stanicích, mobilních zařízeních, serverech, datových úložištích a nosičích a aktivních prvcích sítě.

Sběr a vyhodnocení kybernetických bezpečnostních událostí – souvisí s předchozími pojmy, tedy s detekcí a zaznamenáváním událostí. Úlohou pověřené osoby je seskupovat související incidenty a monitorovat, zda neprobíhá nějaký pokus o narušení bezpečnosti sítě či některého zařízení nacházejícího se v síti. Jestliže je nalezena souvislost mezi více incidenty, předává se tato informace určené bezpečnostní roli k prošetření. Kvalitní vyhodnocování událostí může kompletně předcházet incidentům nebo alespoň sloužit jako včasné varování. Analýza dat

a následné vyhodnocení probíhá podle určitých pravidel, které je třeba s časem aktualizovat a upravovat tak, aby se zmenšil počet nesprávně vyhodnocených incidentů.

Aplikační bezpečnost – testuje bezpečnost aplikace pomocí pokusu o vnější narušení. Jedná se o metodu používání penetračních testů, které jsou provedeny před nasazením aplikace do systému nebo při jeho významné změně. Aplikace, informace a transakce musí být trvale chráněné proti provádění neoprávněných akcí a popření provedených činností.

Kryptografické prostředky – slouží k šifrování dat v systému a k šifrování komunikace na síti a tím zaručení důvěrnosti informací. Osoba, odpovídající za kryptografické prostředky v organizaci, zajistí používání odolných a aktuálních kryptografických algoritmů a klíčů. Dále bude realizována správa klíčů a certifikátů, která bude zajišťovat generování, distribuci, ukládání, změny, zneplatnění certifikátů a likvidaci klíčů.

Zajišťování úrovně dostupnosti informací – je důležitou kategorií z technických opatření. Osoba pověřená tímto úkolem se snaží o maximalizaci dostupnosti systému. Předpokladem je odolnost systému proti kybernetickým hrozbám. Odolnost systému je dosažena pomocí detekce, vyhodnocení a samotnému zabezpečení. Dále se může jednat o decentralizaci či redundanci aktiv, aby se zamezilo vyřazení jednoho důležitého prvku, jehož absence by ohrozila dostupnost.

Průmyslové, řídící a odborné specifické systémy – popisují specifické oblasti a pravidla pro tyto oblasti z pohledu používaného typu softwaru a dalších nároků na zabezpečení. Mezi nástroje této kategorie patří využití specifických technických a programových prostředků, omezení fyzického přístupu k zařízení specifických systémů, vytvoření oddělené části sítě pro komunikaci systémů a omezení či úplné zakázání vzdáleného přístupu. Zároveň je třeba zamezit zneužití známých slabin těchto systémů a být připraven vždy obnovit systém co nejrychleji zpět do konzistentního stavu po bezpečnostním incidentu.

Digitální služby – kladou požadavky na poskytovatele digitálních služeb na vymezení významných prvků, které je nutné zabezpečit a nad kterými je nutné zavést řízení bezpečnosti. Povinností poskytovatelů je také posuzování a nahlašování kybernetických incidentů.

5.5 Kybernetický útok

Už bylo zmíněno, že se kybernetická bezpečnost zabývá ochranou systémů před kybernetickými útoky. Zároveň zde byly vyjmenovány a popsány bezpečnostní opatření, které pomáhají úplně zamezit kybernetickým útokům, či se snaží alespoň co nejvíce omezit jejich dopad. Co to ale vlastně je kybernetický útok? Kybernetický útok je definován jako: „*Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace.*“[8] Jedná se tedy o snahu útočníka napadnout cizí systém a získat tak data nebo například znemožnit používání tohoto systému. Útočníci mohou napadat systémy z finančních, vojenských, špionážních, politických či osobních důvodů, ke kterým může patřit například získání věhlasu či provedení pomsty.

5.5.1 Typy útočníků

Existuje několik typů útočníků, kdy každý provádí útoky z různých důvodů a sleduje tak své vlastní cíle. Útočníky lze rozdělit často podle úrovně znalostí, motivu a organizovanosti. V následujícím seznamu bude popsáno 7 typů aktérů, kteří jsou odpovědní za kybernetické útoky.[9]

Kyber-teroristé – jsou první a zároveň nejnebezpečnější skupinou na seznamu útočníků. Jejich cílem je především způsobovat rozsáhlé škody v různých kritických infrastrukturách. Důvodem k útokům je nejčastěji upozornění na jejich skupinu a věc, za kterou bojují či jako odplata za určité akce dané organizace.[9]

Státem podporovaní aktéři – představují skupinu útočníků, která je financována z peněžních prostředků určité země. Jedná se o tým či jednotlivce, kteří mají díky finančnímu prostředí přístup k nejlepšímu vybavení a disponují ohromnými znalostmi. Jejich cílem je často špionáž a krádež dat z důležité infrastruktury jiného státu či ze státních firem. Jsou schopni vyvíjet vlastní škodlivé programy a velice schopně využívat metod sociálního inženýrství.[9]

Kybernetiční zločinci – patří do kybernetického organizovaného zločinu. Pro tuto skupinu je typické získávání důvěrných a citlivých informací, které později prodávají v aukcích a na černém trhu. Jedná se o zločince, kteří jdou pouze za finančním ziskem. Z tohoto důvodu se občas mohou pokusit o krádež peněžních prostředků za pomocí odcizených platebních údajů uživatele. Velice oblíbeným

nástrojem této skupiny je typ malwaru zvaný ransomware, který zašifruje data napadeného uživatele a požaduje za jejich obnovení výkupné. Četně využívanou metodou u jedinců jsou podvodné e-maily a sociální inženýrství.[9]

Hacktivisté – jsou aktéry kybernetických útoků, kteří jednají především na základě jejich idejí a přesvědčení. Místo organizování útoků za účelem získání peněz či poškození majetku se soustředí na odhalování pravdy a skrytých údajů od pro ně zlých korporací. Jejich finanční a znalostní možnosti jsou omezeny podle členů týmu.[9]

Vnitřní aktéři – pracují zevnitř cílové organizace. Může se jednat o infiltrátory či o zaměstnance dané společnosti. Motivací k útokům těchto aktérů může být finanční odměna, osobní pomsta či průmyslová špionáž. Jedná se o velice závažného aktéra, jelikož má přístup k systému z vnitřku organizace, kde nefungují bezpečností opatření navržené na odražení útoku zvenčí. Znalosti o systému a míra přístupu jsou dány pracovní pozicí.[9]

Skript děťátka – je název pro skupinu amatérských hackerů, kteří nemají rozsáhlé znalosti z oblasti kybernetických útoků. Do této kategorie patří lidé, kteří používají malware vytvořený jiným hackerem a napadají již dobře známé a stále neopravené slabiny různých systémů. Nedokážou vytvořit vlastní způsoby nabourání do systémů a disponují malou výpočetní kapacitou. Často se projevují jako internetoví vandalové, kteří pouze bezhlavě způsobují škody. Jejich motivací je nejčastěji zábava či jiný osobní důvod.[9]

Chyba uživatele – je poslední skupinou aktérů kybernetických útoků a jedná se o velice zvláštní kategorii. Na rozdíl od ostatních typů se tato skupina odlišuje faktem, že útok či jiné narušení systému je způsobeno chybou uživatele a není úmyslné. Stejně tak jako u vnitřních aktérů je i zde narušení provedeno zevnitř systému, což může mít za následek rozsáhlé finanční škody, pozastavení funkce celé firmy, poškození fyzických prvků systému či například ztrátu dat.[9]

5.5.2 Pasivní kybernetické útoky

Kybernetické útoky je možné rozdělovat nejen podle kategorie útočníka, dopadu, cíle, ale také podle samotného druhu útoku. Rozlišují se proto útoky pasivní

a aktivní. V závislosti na podstatě a účelu útoku může být použit jeden z typů útoků či jejich kombinace. Pasivní útoky slouží především pro odposlouchávání a analýzu koncové sítě či cílového klienta. Jedná se o útoky, které jsou většinou nedetekované, nikoli však nedetekovatelné. Probíhají bez vědomí oběti a důležitým faktem je, že nemodifikují odposlouchávané zprávy. Velké účinnosti nabývají zejména na nešifrovaných sítích, kde mohou snadno odposlechnout hesla a další důležité informace. Pasivní útoky v podobě odposlechu představují riziko pro důvěrnost dat. Kromě odposlouchávání do této kategorie patří i analýza sítě a koncového zařízení. Využívá se zde například portscan, který zmapuje otevřené porty koncového klienta a zjistí tak, které služby jsou zablokované a které jsou naopak otevřené. Tyto informace mohou být dále využity aktivním útokem. Do pasivních útoků spadá i pasivní kategorie malwaru. Pasivní malware se vyznačuje tím, že o něm uživatel neví a slouží k získávání informací. Patří sem zadní vrátka do systému, sledování klávesnice (keylogger) a sledování dat z ostatních aplikací.[13]

5.5.3 Aktivní kybernetické útoky

V kontrastu s pasivními útoky zde stojí útoky aktivní. Aktivní útoky mohou narušit komunikaci, služby či cílové stanice pomocí změny nebo vytvoření nových zpráv. Aktivní útoky mají mnoho podob a od pasivních se liší tak, že je uživatel může lehce rozpoznat. Rozlišují se aktivní útoky prováděné od jednoho zdrojového zařízení a distribuované útoky, které používají více útočících zařízení najednou. Takto spolupracující stanice tvoří botnet, který je řízen útočníkem. Bylo by vhodné si aktivní útoky rozepsat a detailněji popsat.[13]

DoS/DDoS – je aktivní kybernetický útok, při kterém se cíl zahltí ICMP pakety nebo jinými nerelevantními dotazy. V důsledku toho je poté server či klient neschopen provádět jiné funkce a může tak dojít k výraznému zpomalení, nebo úplnému vyřazení dané služby. Je téměř nemožné kompletně zastavit větší veřejnou službu za pomocí jednoho útočícího počítače. Z tohoto důvodu existuje i distribuovaná varianta tohoto útoku označená jako DDos, ve které je zapojen botnet. K narušení dostupnosti služby či k jejímu úplnému zhroucení může dojít několika způsoby. Mezi hlavní metody patří zahlcení cíle pakety, posíláním poškozených paketů nebo spuštěním takzvané fork bomby. [11]

DNS spoofing – se řadí mezi velice nebezpečné útoky. Jedná se o podstrčení falešného DNS záznamu či dokonce celého falešného DNS serveru klientovi, který následně navštěvuje jiné stránky, než původně zamýšlel. Na těchto webech se v lepším případě nachází reklama. V horším případě nastane situace, kdy falešné stránky jsou nerozeznatelné s originální stránkou a uživatel tak může omylem zadat své osobní údaje, které mohou být následně snadno ukradeny. Důležitým faktorem při ochraně proti tomuto typu útoku je samotná pozornost uživatele, který si může snadno ve svém prohlížeči zobrazit certifikát a zda se nachází na zabezpečené stránce. Technickým řešením jsou pak samotné certifikáty a end-to-end šifrování.[10]

ARP spoofing – využívá podvrženého záznamu v klientské ARP tabulce. Jedná se o podobný princip jako u předchozí metody, nicméně uživatel nedostane špatný DNS záznam, který ho přesměruje na jinou webovou stránku, ale získá falešnou ARP odpověď. ARP tabulka obsahuje jednotlivé páry IP a MAC adres. Útočník tak zamění svou MAC adresu za jinou a díky tomu přesměruje komunikaci pro dotyčnou IP na svoje zařízení. Uživatel nemá žádnou šanci detekovat útok. Z toho důvodu se tomuto úroku dá bránit statickými ARP záznamy či speciálním softwarem.[12]

Man-in-the-Middle – je takový útok, kde útočník přesměruje komunikaci na sebe a je schopen odposlouchávat celou konverzaci, či dokonce měnit odesílané nebo přijímané zprávy. Tím, že je komunikace přesměrována na útočníka, nepotřebuje se dostávat přes zabezpečení koncového klienta. Tento útok může mít dvě varianty. Fyzická podoba útoku představuje situaci, kdy se útočník fyzicky napojí na síťové prvky. Virtuální podoba útoku využívá spoofing útoku, kdy útočník předstírá, že je jeden z přenosných bodů. Dnes už jeho zastoupení klesá, a to zejména kvůli jednoduché ochraně, kterou je end-to-end šifrování.[11]

Brute force – neboli útok hrubou silou, se řadí mezi aktivní kybernetické útoky. Cílem je prolomit heslo pomocí zkoušení mnoha kombinací. Útok hrubou silou se provádí systematicky a postupně. Existuje ještě jedna varianta, takzvaný slovníkový útok, který využívá externí seznam nejčastějších hesel. Takový slovník se poté prochází a zkouší se jeho jednotlivé záznamy. Vzhledem ke skutečnosti, že vyzkoušení všech kombinací roste exponenciálně, je hlavní a efektivní obranou silné heslo, které je dlouhé a obsahuje nejrůznější kombinace písmen, znaků a čísel.[11][14]

Sociální inženýrství – definuje kategorii kybernetických útoků, během kterých je pozornost útoku zaměřena na oklamání uživatele. Velice známou metodou sociálního inženýrství je takzvaný phishing a jeho modifikace spear phishing. Jedná se o útoky, během kterých není primárním cílem zařízení uživatele, nicméně snaha ovlivnit uživatele natolik, aby zaslal svoje údaje, použil podvržený odkaz či poslal peníze útočníkovi. Útok může mít podobu podvodného telefonátu, e-mailu či například reklamy. Phishing je velice oblíbený a populární útok, který je především distribuován mezi velkou masu lidí. U takto masových útoků podvodník doufá, že se chytí alespoň malé procento lidí. Převážná většina uživatelů však útoku odolá. Z toho důvodu existuje i druhý, více specializovaný, spear phishing. Tento typ si zakládá na útoku na jednu konkrétní osobu, o které si zjistí největší možné množství informací. Jestliže má útočník mnoho informací, pak je obrana proti takovému útoku velice obtížná. [11]

Pro phishing je kromě podvodných odkazů také typický malware, který se snaží útočník dostat na klientské zařízení. Může se jednat o klasické viry, červy a trojské koně, avšak častým příkladem je ransomware. Právě ransomware má zejména v posledních letech velké zastoupení. Jedná se o malware, který zašifruje data na napadeném zařízení a následně vyžaduje výkupné za jejich obnovení.[14]

Zero-day exploit – vyjadřuje situaci, kdy určitá aplikace obsahuje chybu, o které ještě vývojář daného softwaru neví nebo ji zatím neopravil. Tato chyba může být zneužita pro proniknutí do aplikace a získání dat. Samotnou slabinu pak často po objevení opraví vývojář pomocí aktualizace. Proti tomuto typu útoku se téměř nedá bránit. Uživatel se v tomto případě může spoléhat pouze na časté aktualizace a vlastní opatrnost při otevírání neznámých souborů. [14]

SQL injection a XSS – je označení dvou útoků, které využívají podstrčení škodlivého skriptu či příkazu do aplikace pomocí nezabezpečeného vstupního formuláře. Prvním útokem je SQL injection, jehož podobou je škodlivý příkaz v databázovém jazyce SQL. Podstata útoku spočívá v tom, že útočník ukončí původní dotaz, který měl zapsat, či vypsat data z databáze a hned na to vloží do stejného pole příkaz nový. Nezabezpečená aplikace tak provede oba příkazy a útočník pomocí toho je schopen získat, modifikovat či smazat data z databáze.

Podobně funguje i cross-site scripting, zkráceně též XSS. Tato metoda se nevyskytuje u databáze, nicméně v samotné webové aplikaci. Útočník vloží vlastní skript do neošetřeného vstupního pole, podobně jako tomu je u SQL injection. Aplikace poté vykoná i obsah uživatelského skriptu. Takový skript je schopen přidávat nový obsah v aplikaci, měnit či mazat stávající obsah, přesměrovat další uživatele na určitou webovou stránku, nebo se v neposlední řadě pokusit o stažení souboru.

Ochrana proti zmíněným útokům musí být naprogramována v samotné aplikaci zpracovávající uživatelské vstupy. U SQL injection útoků se jedná kupříkladu o předpřipravené dotazy a u XSS o filtrování vstupních polí a zneplatnění speciálních znaků.[14][11]

5.5.4 Nejznámější kybernetické útoky

Není tajemstvím, že kybernetické útoky nejsou žádnou výjimečnou záležitostí. Dějí se jich každý den tisíce po celém světě. Zřídka se však stane, že se určitému útoku povede rozšířit po celém světě a nakazit miliony zařízení. Některé útoky jsou cílené na veřejnost, zatímco jiné na firmy či kritickou infrastrukturu. Ze začátku by bylo vhodné se zmínit o několika útocích, které byly těmi nejznámějšími a největšími na světě. Pomocí analýzy známých útoků se lze poučit a navrhnout zabezpečení tak, aby stejným typům útoků bylo v budoucnu zabráněno.

V první řadě se jedná o útoky na kritickou informační infrastrukturu. Za posledních 10 let bylo zaznamenáno hned několik nebezpečných útoků. Jedním z nich byl útok na energetickou infrastrukturu na Ukrajině v roce 2015. Důsledkem výpadku energetické sítě zůstalo bez proudu 230 tisíc obyvatel po dobu několika hodin. Útok začal spear phishingem a následovalo použití malwaru. Poté byly nabourány jednotlivé elektrické distribuční stanice, které byly vypínány a systém byl zároveň zahlcen DDoS útokem. Z tohoto důvodu došlo k znepřístupnění vzdáleného připojení a vyřazení zákaznické podpory. [15]

Druhým významným incidentem byl útok na přehradu Rye Brook v New Yorku. Útočníci zde převzali kontrolu nad řídící jednotkou přehrady. Útok byl proveden v roce 2013, nicméně k jeho odhalení došlo až o tři roky později. Bylo

využito zranitelnosti v jednom ze starších datových modemů, ze kterého se poté útočníci dostali do dalších částí systému přehrady. [15]

Třetím známým napadením kritické informační infrastruktury je útok z roku 2020 na jaderné elektrárny v USA. Vzhledem k důležitosti cíle byly útoky vyšetřovány FBI a vnitřním bezpečnostním úřadem a nebylo tak odhaleno mnoho podrobností o útoku samotném. Kritické systémy takové důležitosti jsou však velmi dobře zabezpečeny, a proto je nejpravděpodobnějším typem útoku spear phishing s následným přiloženým malwarem. Útočníci neměli přímý přístup k ovládání elektrárny, přesto však útok vznesl vlnu obav o veřejnou bezpečnost. [15]

Jak již bylo zmíněno, kybernetické útoky se netýkají pouze kritické infrastruktury, ale i širší veřejnosti. Zářným příkladem je ransomware WannaCry, který nakazil více než 200.000 počítačů ve 150 zemích světa. Obětí útoku se stalo i několik zdravotnických zařízení a továren, kde došlo k přeložení mnoha operací a odstavení výrobního provozu. Metodou distribuce útoku byl phishingový mail s obsaženým malwarem využívajícím zranitelnosti EternalBlue a zadních vrátek DoublePulsar, které byly vytvořeny skupinou hackerů z NSA. Zranitelnost byla nalezena v operačním systému Windows, přesněji v protokolu SMB. K útoku došlo v roce 2017 a jedná se o útok s jedním z největších dosahů za posledních několik let. Jeho škoda se odhaduje na 4 až 8 miliard dolarů. [16]

Dalším rozsáhlým útokem byl NotPetya. Jeho škoda se odhaduje na více než 10 miliard dolarů. Jednalo se o ransomware využívající zranitelností EternalBlue a EternalRomance u protokolu SMB. NotPetya napadl ve výsledku méně počítačů než například výše zmíněný WannaCry, nicméně způsobil mnohem větší škody, a to zejména kvůli skutečnosti, že se šířil více ve finanční sféře. Útočníci se nabourali do aktualizačního serveru finančního softwaru MeDoc, malware zamaskovali jako aktualizaci pro běžné uživatele, kterou následně vydali. [16]

Ne všechny útoky jsou původně cíleny na napadení co největšího množství počítačů. Známým velice specializovaným útokem byl Stuxnet, původně vytvořený pro poškození uranové centrifugy v Íránu. Stuxnet se dokázal úspěšně šířit i přes přenosná média, díky kterým se dostal k počítačům, které nebyly připojeny do internetu, či do jiné sítě. Svůj úkol splnil, nicméně se poté rozšířil i do světa, kde

napadl velké množství dalších počítačů. Tím, že byl Stuxnet vytvořen velice specializovaně, nebyla většina zasažených počítačů nijak ovlivněna. [16]

Posledním představovaným útokem bude DDoS botnetu Mirai. Tento útok se stal v roce 2016 a byl speciální hned v několika aspektech. V první řadě byl tento útok proveden v období rozkvětu chytrých domácností a internetu věcí. Mirai využil všechna tato chytrá zařízení, pomocí malwaru je napojil do botnetu a poté provedl rozsáhlý DDoS útok na různé cíle. Jedním z cílů byl americký poskytovatel internetu, kterého útok naprosto vyřadil. To mělo za následek i vyřazení služeb Netflix, Twitter, Sony Playstation online, Paypal a Spotify. K nabourávání do málo zabezpečených chytrých zařízení byl použit útok hrubou silou. Jednalo se o útok, který upozornil na nezabezpečenost prvků chytrých domácností a poukázal na sílu těchto zařízení a na následky, které mohou nastat při jejich zneužití.[16]

Je patrné, že se útoky často kombinují a není to vždy využití jednoho specifického typu. Společně s tím lze vypozorovat, že se pro méně zabezpečené, nebo starší zařízení využívají více útoky hrubou silou a známé exploity. Což naopak u zabezpečených systémů není tak četné a používá se zde velmi často cílený spear phishing. V útocích na širší veřejnost lze hojně spatřit plošný phishing ve formě spamů, podvodných emailů, podvržených odkazů. Oblíbeným malwarem distribuovaným do veřejnosti je ransomware či malware, který je schopen ukrást platební informace oběti. Zmíněné poznatky budou využity v praktické části práce pro návrh zabezpečené sítě a doporučení pro zaměstnance případné firmy.

5.5.5 Zabezpečení vrstev ISO/OSI

O samotných útocích, útočnících, metodách a nejznámějších představitelích již zmínka byla. Nicméně k velice důležité součásti patří metody a způsoby samotné obrany společně s celkovou minimalizací rizika vzniku útoku a jeho úspěšnosti. V této kapitole budou popsány různé možnosti ochrany po jednotlivých vrstvách síťového referenčního modelu ISO/OSI.

První vrstvou ISO/OSI je fyzická vrstva. Ta přenáší data v podobě bitů přes fyzické médium za pomocí optických či elektrických signálů. Jaké zabezpečení se týká právě této vrstvy? Jedná se o veškerá fyzická opatření, která zabraňují

neoprávněnému přístupu do sítě nebo k jejím prvkům. Společně s tím se jedná o kvalitní topologii, použití vhodného přenosového média a vhodných síťových komponentů, základní zabezpečení pro bezdrátový přístupový bod i další síťové prvky a v neposlední řadě vymezení perimetru. Součástí této obrany je i detekce přerušení spojení, při kterém by mohlo dojít ke změně topologie v případě napojení útočníka. Jedná se tedy o veškerá opatření spojená s fyzickou bezpečností. Za jmenovité příklady lze například použít kamerový systém, využití systému autentizace pro pověřené osoby pomocí bezpečnostních karet či jiného tokenu a v neposlední řadě i bezpečnostní alarm v uzamčené serverové místnosti. [17][21]

Linková vrstva reprezentuje druhou vrstvu relačního modelu. Jde o logickou vrstvu, jejíž datovou jednotkou jsou rámce. V problematice řešení bezpečnosti na linkové vrstvě bude kladen důraz především na MAC adresy, ARP protokol, zabezpečení všech rozhraní a vytvoření VLAN. O pasivním odposlouchávání v síti či aktivním útokem man-in-the-middle je známo, že využívá podvržení ARP záznamu. Z toho důvodu je třeba nastavit prvky sítě tak, aby si pamatovaly MAC adresu zařízení na daném portu. Pokud by došlo k připojení jiného zařízení, pak má být daný port ihned automaticky vypnut. V rámci bezpečnosti se doporučuje vypnout veškerá nepoužitá rozhraní a služby. Dále je vhodné používat pro vzdálenou správu zařízení zabezpečený protokol. Jedná se sice o protokoly vyšších vrstev, nicméně pro konfiguraci switchů je v takovém případě vhodnější použít protokol SSH namísto nezabezpečeného protokolu Telnet. Součástí bezpečnosti na linkové vrstvě je i nastavení virtuálních LAN. Tyto virtuální sítě umožňují fyzickou topologii logicky rozdělit na různé segmenty. [17][19][21]

Třetí vrstvu ISO/OSI modelu tvoří síťová vrstva. Datovou jednotkou jsou pakety, které je třeba určitým způsobem filtrovat. V rámci síťové vrstvy je možno aplikoval paketové filtry Access Control List. Tento prvek, označovaný často jako ACL, je základním obranným prvkem síťové vrstvy. ACL je možné podle potřeby nastavit buď v příchozím nebo v odchozím režimu. Příchozí režim zajišťuje, že veškeré nevyhovující příchozí pakety budou zahozeny. Neprojdou tedy ani směrovacím procesem uvnitř zařízení, při kterém router vybírá další cíl pro daný paket. Tento typ filtru se používá zejména pro rozhraní přistupující do internetu na routeru, kde všechna další rozhraní vedou do privátní sítě. Nepoužívá se v situaci,

kdy router má více rozhraní vedoucích do internetu, protože by došlo k zahození daného paketu. Opakem tohoto typu je odchozí režim. Ten zajišťuje, že router nepošle na dotyčné rozhraní nevhodný paket. Tento filtr je aplikován až po směrovacím procesu, kdy router už rozhodl, které rozhraní bude použito pro odeslání paketu. Aplikuje se především na rozhraní vedoucí do privátní sítě, jelikož definuje povolené pakety pro daný segment. Dalším zabezpečovacím prvkem síťové vrstvy je firewall. Prvek firewall kontroluje příchozí pakety a následně rozhoduje, zda budou propuštěny dále do sítě. Existují i jeho dvě nástavby, které aktivněji zasahují do komunikace. Prvním typem modulu pro firewall je IDS, z anglického intrusion detection system, a druhým IPS, z anglického intrusion prevention system. Zatímco IDS detekuje potenciální hrozby a informuje o této skutečnosti, IPS aktivně potlačuje veškeré podezřelé aktivity. Firewall funguje ve svém principu jako paketový filtr vylepšený o sledování portů a dnes už i o sledování relací. Do síťového zabezpečení je možné zařadit i NAT. Přestože se nejedná o metodu, která by jakýmkoliv způsobem detekovala či neutralizovala hrozby, je možné ji využít pro skrytí topologie vnitřní sítě. Technologie NAT provádí překlad vnitřních adres na veřejné adresy, které poté vystupují v internetu. Existuje statický, dynamický a přetížený překlad adres. Dalšími bezpečnostními doporučeními jsou nastavení limitu odpovídání na protokol ICMP, případně i jeho úplné zablokování, jestliže není nijak dále explicitně vyžadován, a vypnutí všech nevyužitých rozhraní routeru. Poslední zmíněnou metodou ochrany třetí vrstvy ISO/OSI modelu je IPsec. Jedná se o autentizační verzi protokolu IP obohaceného o šifrování jednotlivých paketů, která dopomáhá udržovat integritu a důvěrnost dat. [17][18][21][22]

Další, v pořadí již čtvrtou, vrstvou je transportní vrstva. Tato vrstva umožňuje rozlišovat patřičné služby příchozích paketů pomocí čísla portu. V rámci bezpečnosti se doporučuje uzavřít veškeré nepoužívané porty, aby nedošlo k jejich napadení. Zároveň na této vrstvě lze provádět sledování portů, které může odhalit blížící se útok. Tyto pakety je možné odstranit za pomocí paketového filtru ACL nebo pomocí prvku firewall. [17][18][21]

Pátou vrstvou ISO/OSI modelu je relační vrstva, která se stará o vytvoření, udržení a ukončení relací. Mezi funkce relační vrstvy patří autorizace, autentizace a správa jednotlivých sezení. Zabezpečením na této vrstvě se tedy rozumí provedení

validní autentizace, autorizace a zabránění neoprávněných narušení sezení. [17][21][22]

Předposlední vrstva referenčního modelu se jmenuje prezentační vrstva. Její funkcí je transformace ze surových dat aplikační vrstvy do podoby vhodné pro přenos. Zde je třeba zajistit validní konverzi dat. [17][21][22]

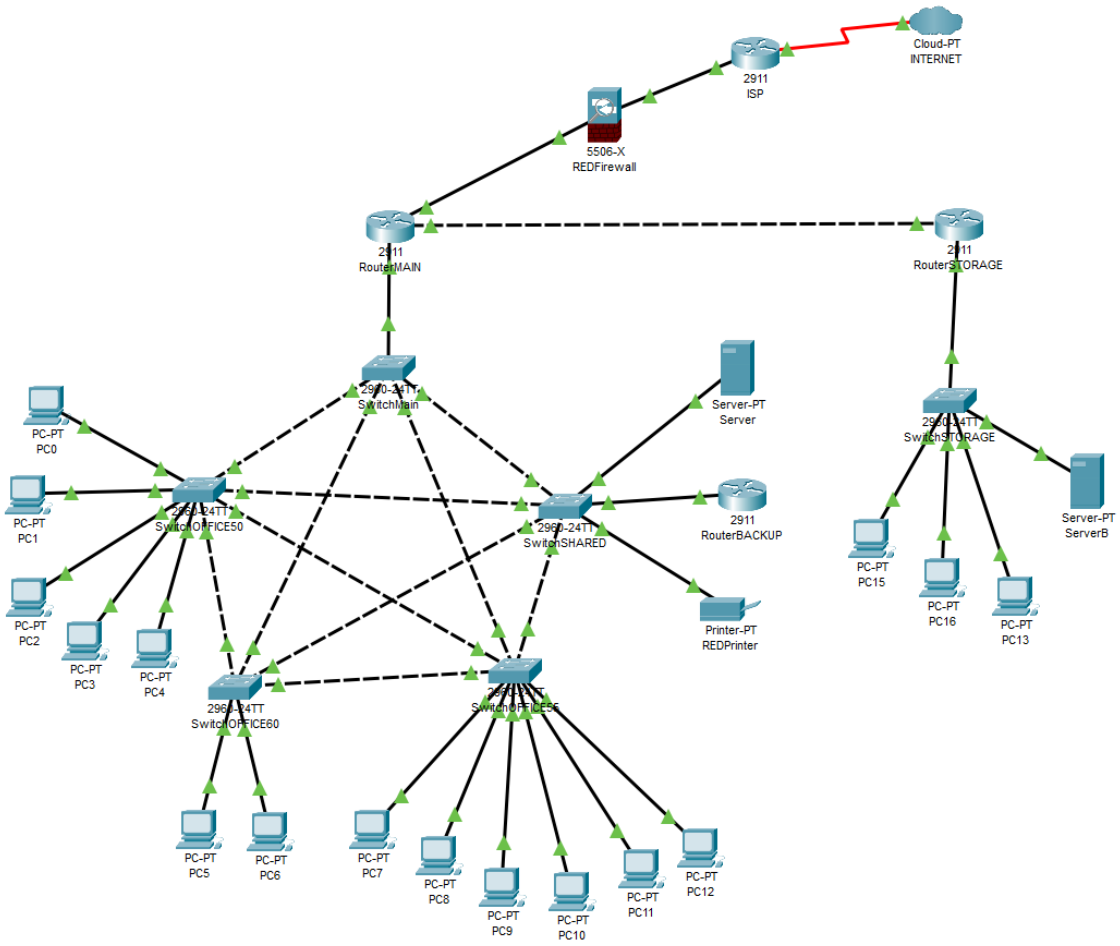
Aplikační vrstva je sedmou a také nejvrchnější vrstvou celého referenčního modelu ISO/OSI. Vrstvu reprezentují aplikace a protokoly, které umožňují komunikaci přes síť. V bezpečné síti musí být využito zabezpečených verzí jednotlivých protokolů. Příkladem může být HTTPS, SSH a SSL, popřípadě jeho novější verze TLS. [17][21][22]

6 Návrh sítě

Teoreticky byly již popsány základní principy fungování počítačových sítí, různé druhy hrozeb a zabezpečení. V praktické části proto bude využito těchto poznatků k vytvoření návrhu zabezpečené sítě podle jednotlivých vrstev. V textu jsou popsány použité metody zabezpečení, včetně vyobrazení jednotlivých částí konfigurace pomocí vloženého obrázku. Kompletní konfigurační soubory všech prvků jsou uvedeny v příloze.

Pro modelovou situaci byla vytvořena fiktivní firma pojmenovaná REDSoftware. Tato firma zaměstnává ve zmíněné lokaci 20 lidí a skládá se ze dvou blízkých poboček. Primárním zaměřením firmy je vývoj softwaru pro kritickou informační infrastrukturu. Z tohoto důvodu je třeba síť zabezpečit podle pravidel pro dodavatele, které určí odběratel daného softwaru patřící do kritické informační infrastruktury. Podle vedení firmy je kritická především práce na vývoji softwaru. Všechny kroky tohoto vývoje probíhají uvnitř samotné organizace a vše je uloženo na firemním serveru. Dále vedení požaduje, aby síť nebyla úplně izolovaná, ale zaměstnanci měli přístup k internetu. Důležitým místem pro firmu je hlavní budova s kancelářemi, kde je vymezené patro pro zaměstnance a speciální oddělené prostory pro uložení serveru. Druhá pobočka, sídlící hned ve vedlejší budově, má sloužit především jako datový sklad, kde se budou ukládat a analyzovat vybraná firemní data. Tato větev má být přístupná pouze z vnitřku organizace a nesmí být připojena k internetu. V celé organizaci bude využita služba active directory pro správu oprávnění a zaměstnanci si budou muset pravidelně nastavovat silná hesla. Všechny nepotřebné služby budou zakázány.

V modelu byly využity a konfigurovány síťové prvky společnosti Cisco v programu Cisco Packet Tracer. Tento software umožňuje přímé modelování opatření druhé, třetí, čtvrté a z části první vrstvy. Všechny následující obrázky a konfigurace jsou prací autora.



Obrázek 6-1 REDSoftware model

V rámci první vrstvy je třeba zabezpečit fyzickou bezpečnost. Toho je v modelu, a tedy i v potenciální reálné firmě, dosaženo redundancí, zvolením vhodné topologie a aplikováním adekvátních přístupových bezpečnostních opatření. Jelikož má být síť co nejvíce robustní, je patrné, že nebude použita čistě centralizovaná topologie. Podle přání vedení firmy je primárním účelem fungování samotného vnitřku společnosti. Z tohoto důvodu je uvnitř hlavní budovy několik duplicitních prvků switch, které jsou propojeny topologií plné mřížky. V rámci bezpečnosti a administrativy byla síť rozsegmentována do několika VLAN. Směrování mezi nimi je zajištěno topologií router-on-a-stick. V případě výpadku hlavního routeru je zde přítomen i záložní router, který přebere jeho funkci. Toho je zajištěno pomocí proprietárního protokolu HSRP od společnosti Cisco, jehož volně dostupnou alternativou je protokol VRRP. Dalším krokem v zabezpečení je samotný přístup

do místnosti se serverem a s dalšími síťovými prvky. Tyto prostory budou oddělené od normálních prostor zaměstnanců, budou řádně uzamčené a opatřené alarmem. Kvůli riziku výpadku elektrické energie je třeba zajistit náhradní napájení UPS na dobu nezbytně nutnou pro bezpečné uložení a vypnutí. Okolí budovy i celý objekt včetně vnitřních prostor bude hlídán kamerovým systémem.

Po zajištění fyzické bezpečnosti by bylo vhodné vyřešit i bezpečnost sítě jako takové. Na druhé vrstvě byly vybrány jako zabezpečovací prvky VLAN v kombinaci s port security nastavené na všech prvcích switch. Byla vytvořena samostatná konfigurační VLAN, do které mají přístup pouze počítače vedoucího pracovníka a administrátora sítě. Vzdálený přístup ke konfiguraci prvků je realizován pouze s využitím zabezpečeného protokolu SSH.

```
ip access-list extended REDManagement
permit ip 198.167.12.32 0.0.0.7 5.5.5.0 0.0.0.255
deny ip any any
exit

int g0/1.99
ip access-group REDManagement out
exit

line vty 0 15
ip access-class REDManagement in
exit
```

Obrázek 6-2 zabezpečení administrátorské VLAN

```
hostname SwitchOFFICE50
banner motd "Neopravnena modifikace zarizeni zakazana"
enable secret REDConfigX404
service password-encryption
ip domain-name REDNetwork
crypto key generate rsa
2048
ip ssh version 2
ip ssh authentication-retries 3
ip ssh time-out 120
username REDAdmin privilege 15 password REDConfigB101

line console 0
password REDConfigA202
login
exit

line vty 0 15
transport input ssh
login local
exit
```

Obrázek 6-3 základní konfigurace včetně SSH

Nastavení port security zahrnuje vypnutí veškerých nepoužívaných rozhraní a nastavení pravidel pro zapojená koncová zařízení. Zde je limit jedné MAC adresy na rozhraní, kterou si prvek zapamatuje při první komunikaci. Jakmile se koncový uživatel změní je rozhraní automaticky vypnuto a je třeba jej manuálně znovu zapnout. Toto slouží jako ochrana proti připojení útočníkova zařízení místo některého zaměstnance.

```
int range fa0/6-20
shutdown
exit

int range fa0/1-5
switchport mode access
switchport access vlan 50

switchport port-security
switchport port-security mac-address sticky
switchport port-security violation shutdown
no sh
exit

int range g0/1-2
shutdown
exit
```

Obrázek 6-4 konfigurace port-security

Jelikož jsou pobočky oddělené sítě, vzniká zde problém se směrováním. Za normálních podmínek by byl ve větších sítích využit dynamický směrovací protokol. V této situaci, kde je vyžádána lepší bezpečnost a síť je malá, je vhodné využít bezpečnější statické směrování. Na třetí vrstvě se také nachází paketové filtry ACL, které jsou nastavené tak, aby nepovolili přístup do administrativní VLAN vstup z neoprávněných sítí a zabraňovali přístup z internetu do druhé pobočky. Vnitřní struktura sítě je v internetu skryta s využitím přetíženého překladu adres NAT (přesněji PAT či také overload NAT).

```
int g0/1
ip nat inside
exit

int g0/0
ip add 198.160.0.5 255.255.255.252
ip nat outside
no sh
exit

access-list 150 permit ip 198.167.12.0 0.0.0.255 any
ip nat inside source list 150 interface g0/0 overload
```

Obrázek 6-5 konfigurace překladu adres

Postupně se přechází ze třetí do čtvrté vrstvy, kde operuje firewall. V modelové situaci je realizován na prvku ASA 5506-X, který kontroluje příchozí komunikaci protokolů ICMP, HTTP a DNS. Zbytek komunikace je automaticky blokován. Na prvku budou nasazeny moduly IPS a IDS, které ovšem není možné v programu Packet Tracer modelovat.

Na páté až sedmé vrstvě je zabezpečení sítě dáno používáním zabezpečených verzí protokolů a odblokováním pouze nutně potřebných služeb využívaných programů. Každý software má ve své specifikaci vyjmenované služby, které musí být na zařízení zapnuty pro jeho správný provoz.

7 Shrnutí výsledků

V závěru práce je třeba zhodnotit získané poznatky. Z teoretické části, respektive z oblasti kybernetických útoků, je možné s velkou mírou pravděpodobnosti určit souvislost mezi úspěšností útoku a nízkou úrovní zabezpečení počítačové sítě. Zároveň lze vypozorovat, že na méně zabezpečenou síť se s větší pravděpodobností využije útok hrubou silou či jiná verze útoku na systém samotný. U více zabezpečených systémů převládá naopak útok na samotné uživatele pomocí sociálního inženýrství či útok na nejméně zabezpečené zařízení v řetězci, které poslouží jako přístup do sítě. Při útoku na širší veřejnost je oblíbenou praktikou phishing a z malwaru ransomware.

Součástí práce bylo navržení modelu počítačové sítě. Na něm byly aplikovány bezpečnostní opatření, které brání danou síť proti útokům na zařízení z teoretické části. Jak již bylo zmíněno, jedná se o modelovou situaci, a ne o reálný produkt, což má za následek nemožnost zahrnutí lidského aspektu a případné obrany proti útokům sociálního inženýrství. Model demonstruje ochranu proti zmíněným útokům na druhé, třetí a čtvrté vrstvě ISO/OSI modelu. Další bezpečnostní opatření, zejména na první, páté, šesté a sedmé vrstvě, nelze do modelu zahrnout, a proto jsou vypsána v praktické části bakalářské práce.

8 Závěry a doporučení

Kybernetická kriminalita je stále narůstající problém, který nelze ignorovat. Chránit je potřeba nejen jednotlivé uživatele, ale také kritickou informační infrastrukturu. Jak již bylo mnohokrát avizováno, hlavním problémem počítačových sítí s malou úrovní zabezpečení je jejich snadné přímé napadení, zatímco u zabezpečených systémů se jedná především o lidský faktor, který lze využít k získání přístupu. Jak se tedy efektivně bránit?

Jestliže se jedná o ochranu firemní sítě, pak je vhodné dodržovat opatření vypsaná v praktické části práce. Je třeba zajistit fyzické a konfigurační zabezpečení prvků sítě. Pro úplnou bezpečnost je však i potřeba poučit uživatele systému o existujících útocích, zejména pak o sociálním inženýrství. Obranu koncových zařízení v síti je dále potřeba zajistit nainstalováním anti-malwarového programu.

V případě běžného uživatele internetu se jedná především o obranu proti masovému phishingu v podobě podvodných emailů a zpráv. Zároveň s tím by měl uživatel být na pozoru před stahováním a spouštěním neznámých souborů na svém zařízení společně. V klientském zařízení by měl být nainstalovaný a aktualizovaný anti-malwarový software a uživatel by měl sám důkladně kontrolovat, že se nachází na správné doméně s platným certifikátem, jestliže zadává osobní či přihlašovací údaje.

Jelikož je kybernetická bezpečnost dnes dána pouze legislativními doporučeními, bylo hlavním cílem práce vytvoření konkrétního modelu zabezpečené sítě a vytvoření konfigurace pro dosažení úrovně zabezpečení proti běžným útokům. Pro úspěšné splnění hlavního cíle bylo potřeba dosáhnout několika dílčích cílů, mezi které patřila analýza útoků, vysvětlení a popsání fungování principů počítačových sítí a představení možností kybernetické obrany. Veškerých stanovených hlavních i vedlejších cílů bylo dosaženo. Problém však nastal s ověřením počáteční hypotézy. Jelikož se jedná pouze o model, který nikdy nebyl nasazen v praxi, je možné pouze spekulovat o výsledku. Hypotézu tedy nelze ověřit, a tedy ani potvrdit či vyvrátit. Nicméně na základě teoretické části věnující se útočníkům lze učinit odhad. Vzhledem k pouze omezené skupině aktérů, kteří mají

k dispozici znalosti, prostředky i motiv pro komplexnější útoky, je možné s velkou mírou pravděpodobnosti odhadnout, že by byla hypotéza potvrzena.

Na základě analýzy nejznámějších kybernetických útoků v poslední době bylo zjištěno, že při velké části útoků bylo cíleno na samotné uživatele systému, především tedy s využitím metody spear phishing. Zde se nabízí možnost dalšího výzkumu stejného tématu. Práce by mohla být teoreticky rozšířena i o obranu proti sociálnímu inženýrství a v modelové situaci by mohl být i prostor pro nasimulování lidského faktoru a vymodelování jeho ochrany. Stejné téma by bylo možné zkoumat i z druhé strany, tedy ze strany útočníka, kde by se mohl zaobírat napadením počítačové sítě.

9 Seznam použité literatury

[1] 6lab Cisco. 6lav IPv6 website [online]. Sunnyvale, CA, USA: Cisco, 2020 [cit. 2020-08-29]. Dostupné z: https://6lab.cisco.com/stats/

[2] X.200 : Information technology - Open Systems Interconnection - Basic Reference Model: The basic model [online]. Ženeva, Švýcarsko, 2008 [cit. 2020-08-29]. Dostupné z: https://www.itu.int/rec/T-REC-X.200-199407-I/en

[3] ŠEDA, Petr a Jan ŠTĚPÁN. Střední průmyslová škola elektrotechnická Pardubice, Univerzita Hradec Králové, předmět Počítačové sítě, Počítačové sítě 1, 2 a 3: Vlastní poznámky. Pardubice, Hradec Králové 2020

[4] ORACLE CORPORATION. Introducing the protocol suite. Introducing the protocol suite [online]. USA: ORACLE CORPORATION, 2010 [cit. 2021-01-04]. Dostupné z: https://docs.oracle.com/cd/E19455-01/806-0916/6ja85398m/index.html

[5] 2schemakii-cz.pdf [online]. Česká republika: NCKB, 2014 [cit. 2021-01-17]. Dostupné z: https://img.ihned.cz/attachment.php/300/61041300/CER0yIPTNf9SMhwjnH6qz8Wm1Jd5OQAL/2schemakii-cz.pdf

[6] Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: . Česká republika: Sagit, 2014, ročník 2014, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

[7] Vyhláška č. 82/2018 Sb.: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: . Česká republika: Sagit, 2018, ročník 2018, číslo 82. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

[8] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník Kybernetické bezpečnosti. Praha, 2015. Dostupné také z: https://cybersecurity.cz/data/slovnik_v310.pdf

[9] 7 TYPES OF CYBER THREAT ACTORS AND THEIR DAMAGE. *Redlegg* [online]. Chicago: Redlegg Blog, 2020 [cit. 2021-02-23]. Dostupné z: https://www.redlegg.com/blog/cyber-threat-actor-types

[10] What is DNS Spoofing and Cache poisoning? Kaspersky [online]. Moskva: KasperskyLab, 2021 [cit. 2021-03-10]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/dns

[11] The 15 most common types of cyber attacks. Lepide [online]. Austin, Texas, USA: lepide, 2020 [cit. 2021-03-12]. Dostupné z: https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/

[12] ARP Spoofing. Imperva [online]. Kalifornie, USA: Imperva, 2020 [cit. 2021-03-13]. Dostupné z: https://www.imperva.com/learn/application-security/arp-spoofing/

[13] Difference between active attack and passive attack. Geeksforgeeks [online]. Noida: Geeksforgeeks, 2020 [cit. 2021-03-13]. Dostupné z: https://www.geeksforgeeks.org/difference-between-active-attack-and-passive-attack/

[14] Cyber attack. Upguard [online]. Hobart (Austrálie): Upguard, 2021 [cit. 2021-03-14]. Dostupné z: https://www.upguard.com/blog/cyber-attack

[15] Top 5 infrastructure hacks. Techmonitor [online]. Nottingham: New Statesman Media Group, 2021 [cit. 2021-03-14]. Dostupné z: https://techmonitor.ai/techonology/cybersecurity/top-5-infrastructure-hacks

[16] Five most notorious cyberattacks. Kaspersky [online]. Moskva: Kaspersky, 2018 [cit. 2021-03-20]. Dostupné z: https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/

[17] GREGG, Michael, REIS, Chris, George MAYS, Stephen WATKINS, Ron BANDES a Brandon FRANKLIN, ed. Hack the Stack [online]. Rockland, MA, USA: Syngress, 2006 [cit. 2021-3-13]. ISBN 1-59749-109-8. Dostupné z: http://www.staroceans.org/kernel-and-driver/Hack%20the%20Stack%20-%20Using%20Snort%20and%20Ethereal%20to%20Master%20the%208%20Layers%20of%20an%20Insecure%20Network%20(Syngress%2C%202006)%20WW.pdf

[18] YADAV, Ajay. Network design: Firewall, IDS/IPS. Infosec [online]. USA: Infosec, 2020 [cit. 2021-3-14]. Dostupné z: https://resources.infosecinstitute.com/topic/network-design-firewall-idsips/

[19] Security features on switches. Ciscopress [online]. CA, USA: Ciscopress, 2008 [cit. 2021-2-10]. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=12

[20] Cisco Networking Academy, CCNAv6 1 & CCNAv6 2 & CCNAv7 3 study materials [online]. USA: Cisco, 2020 [cit. 2021-4-26]. Dostupné z: https://www.netacad.com/portal/learning

[21] CyberSecurity [online]. Praha, Česká republika: CZ.NIC, z. s. p. o., 2019 [cit. 2021-2-5]. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[22] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2. Česká republika: Kopp, 2009. ISBN 978-80-7232-388-3.

10 Přílohy

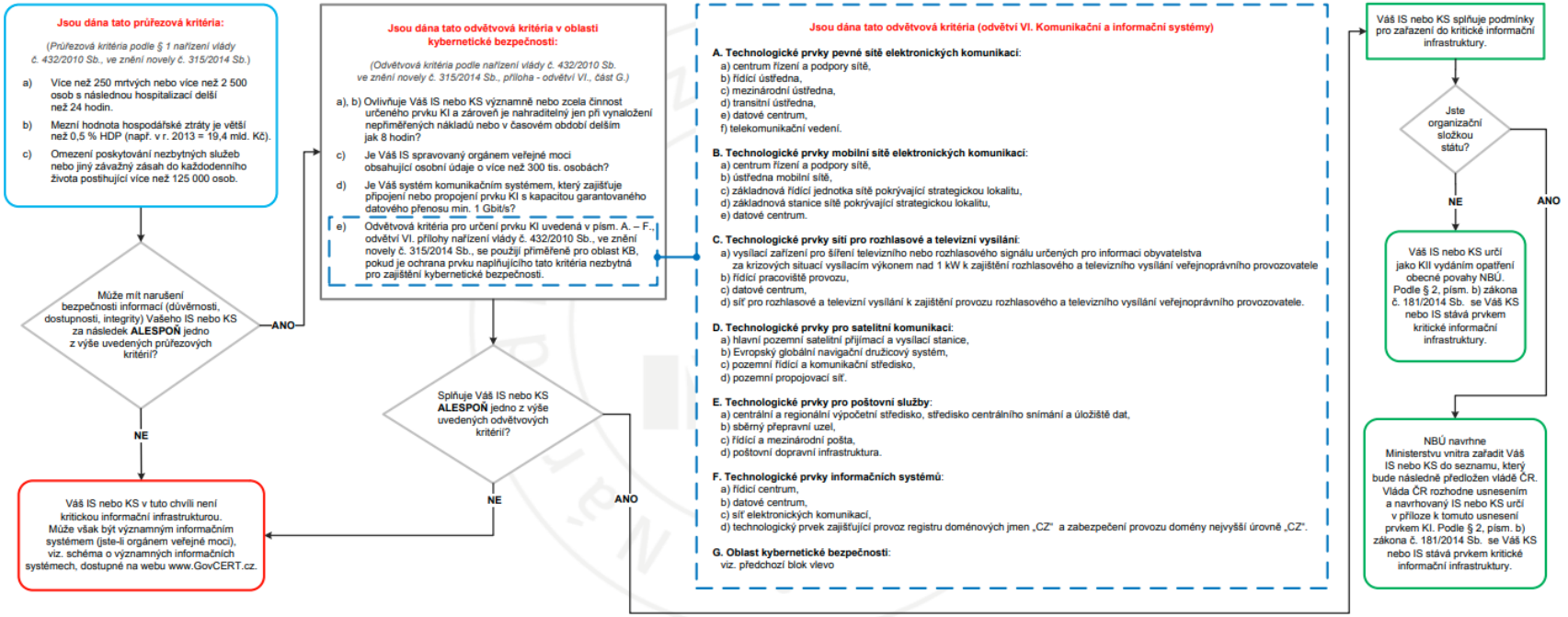
1) Určování kritické informační infrastruktury. Dostupné online: https://img.ihned.cz/attachment.php/300/61041300/CER0yIPTNf9SMhwjnH6qz8Wm1Jd5OQAL/2schemakii-cz.pdf
2) Archiv konfiguračních souborů síťových prvků a modelové sítě v programu Cisco Packet Tracer

Kritická informační infrastruktura

Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb.

Národní centrum kybernetické bezpečnosti



Použité zkratky: IS - informační systém, KB - kybernetická bezpečnost, KI - kritická infrastruktura, KII - kritická informační infrastruktura, KS - komunikační systém, NBÚ - Národní bezpečnostní úřad, OOP - opatření obecné povahy

Poznámka:

V rámci procesu určování kritické informační infrastruktury (KII) bude NBÚ s dotčenými subjekty jednat a to již před samotným určením. Samotné určení pak proběhne, po oboustranném jednání. U organizačních složek státu probíhá určení prvků KII vydáním usnesení vlády ČR. U orgánů nebo osob, které nejsou organizační složkou státu, probíhá určení vydáním opatření obecné povahy (OOP), které vydá NBÚ. NBÚ je k dispozici k případnému jednání a k poskytnutí metodické pomoci v rámci posouzení naplnění určujících kritérií.

Upozornění:

Dokument slouží pouze jako podpůrné vodítko, nenahrazuje žádný ze zákonů a souvisejících prováděcích předpisů. Právo změny tohoto dokumentu vyhrazeno.

Více informací naleznete na www.GovCERT.cz

Verze: 3.0

Příloha č. 1

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Jan Štěpán**
Studium:	I1800235
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Zabezpečení počítačové sítě**
Název bakalářské práce AJ:	Computer network security

Cíl, metody, literatura, předpoklady:

Cílem práce je představit architekturu a fungování počítačových sítí společně s tématem kybernetických hrozeb a útoků s důrazem na představení a praktické ověření možností mitigace jednotlivých hrozeb v rámci malé/střední počítačové sítě.

Osnova:

- Úvod
- Historie a vývoj internetu
- Vrstvy ISO/OSI modelu
- Kyberbezpečnost
- Kybernetické hrozby a útoky
- Bezpečnostní opatření a doporučení
- Závěr

CyberSecurity CZ.NIC edice https://knihy.nic.cz/files/edice/cybersecurity.pdf

ISO/OSI dokumentace https://www.itu.int/rec/T-REC-X.200/en/

Vlastní poznámky z předmětu Počítačové Sítě 1, 2

Cisco NetAcad CCNA Curriculum

Další statistické a informační zdroje

Garantující pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Tomáš Svoboda, Ph.D.
Datum zadání závěrečné práce:	21.10.2019