Policejní akademie České republiky v Praze

Fakulta bezpečnostního managementu

Katedra managementu a informatiky

Telekomunikace a kritická infrastruktura

Bakalářská práce

Telecommunication and critical infrastructure

Bachelor thesis

VEDOUCÍ PRÁCE
Ing. Bc. Hana Švecová

AUTOR PRÁCE
Miroslav Nešvera

Praha 2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, který jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Jablonném v Podještědí, dne 25. 08. 2022

Miroslav NEŠVERA

Poděkování

Rád bych tímto poděkoval paní Ing. Bc. Haně ŠVECOVÉ za odborné rady a cenné připomínky, kterými přispěla k vypracování této bakalářské práce.

Anotace

Předmětem této bakalářské práce jsou dopady kybernetických útoků na počítačovou infrastrukturu zdravotnických zařízení v České republice. V této práci se zaměřuji na kritickou infrastrukturu České republiky, orgány krizového řízení a příslušné zákonné předpisy. Zaměřuji se na historický vývoj telekomunikace od prvních počátků až po současné moderní technologie. Popisuji aktuální hrozby, se kterými se uživatel výpočetní techniky může setkat. Konkrétně se zaměřuji na šíření škodlivého vyděračského viru ransomware, který se šíří prostřednictvím maker v souborech kancelářského balíku Microsoft Office. Zabývám se postupy a opatřeními při kybernetickém útoku a požadavky pro vybudování bezpečné počítačové sítě.

Klíčová slova

Telekomunikace * Kritická infrastruktura * Kybernetický útok * Malware * Microsoft Office * Makro * Zdravotnické zařízení

Annotation

The subject of this bachelor's thesis is the impact of cyber attacks on the computer infrastructure of medical facilities in the Czech Republic. In this thesis, I focus on the critical infrastructure of the Czech Republic, crisis management authorities and relevant legal regulations. Furthermore, I focus on the historical development of telecommunications from the first beginnings to current modern technologies. I describe the current threats that a computer user may encounter. Specifically, I'm focusing on the spread of a malicious ransomware virus that spreads through macros in Microsoft Office files. I deal with the procedures and measures for a cyber attack and the requirements for building a secure computer network.

Keywords

Telecommunication * Critical infrastructure * Cyber attack * Malware * Microsoft Office * Macro * Medical facility

Obsah

Úvod **7**

1. Kritická infrastruktura **9**

1.1. Krizové řízení 9

1.2. Prvky kritické infrastruktury 13

2. Telekomunikace **17**

2.1. Tradiční telekomunikace 19

2.1.1. Světelné signály 19

2.1.2. Akustické signály 19

2.1.3. Kurýrní služba 20

2.1.4. Komunikace prostřednictvím zvířat 20

2.2. Moderní telekomunikace 21

2.2.1. Telegrafie 21

2.2.2. Telefonie 22

2.2.3. Radiofonie 23

2.2.4. Hromadné sdělovací prostředky 25

2.2.5. Počítačové sítě 25

3. Kybernetická bezpečnost **28**

3.1. Kybernetické hrozby 28

3.1.1. Phishing 30

3.1.2. Vishing 30

3.1.3. Počítačové viry 31

3.1.4. Počítačové červy 32

3.1.5. Scareware 32

3.1.6. Spyware 33

3.1.7. Adware 33

3.1.8. Trojský kůň 34
3.1.9. Ransomware 34
3.1.10. Denial of service 35
3.2. Kybernetické útoky na zdravotnická zařízení 35
3.3. Opatření při kybernetickém útoku 40
3.4. Bezpečnostní pravidla 43
4. Makra v elektronických dokumentech 49
4.1. Povolování VBA maker 49
4.2. Povolování XLM maker 52
4.2.1. Vytvoření XLM makra 53
Závěr 57
Seznam použité literatury 59
Seznam obrázků 65
Seznam tabulek 66

Úvod

Pojmy telekomunikace a kritická infrastruktura jsou velmi často spojovány se současnou moderní civilizací. Dalo by se však říct, že oba pojmy provázejí civilizaci od samého počátku. Již v době kamenné si člověk budoval svoji první primitivní infrastrukturu, kdy žil v kmenech, které měly svého vůdce, který jej vedl. Vůdce si musel umět poradit s nástrahami, které v té době člověka sužovaly. Jako další článek infrastruktury sem patří dělba tehdejší práce. Byli tu lovci, sběrači, hlídači ohně, zpracovatelé kožešin a další, kteří plnili své úlohy ve prospěch kmene. Oheň byl v této době velmi vzácnou komoditou, dal by se označit jako prvek kritické infrastruktury. Bez ohně přišel člověk o světlo a teplo, kdy tato ztráta měla velký negativní dopad na celý kmen.

Později člověk přišel na to, jak oheň rozdělat. Jedná se o jednu ze základních vlastností typické pro člověka. Při svém vývoji se vždycky snaží jít dopředu a zkoumat a vynalézat nové technologie, které mu usnadní práci a zvýší životní úroveň. Postupným vývojem začaly z kmenů vznikat osady, které se postupně vyvinuly v města, od kterých postupně vznikly první říše. Infrastruktura se tak stávala komplexnější a pro její udržitelnost byla potřeba vzájemná komunikace. Začaly se budovat cesty mezi městy a osadami pro snadnější pohyb osob a zboží. Vznikaly vodojemy pro distribuci vody z vodních toků. S rozvojem civilizace vznikaly také nové choroby, což dalo vzniknout prvním nemocnicím. S nárustem komplexnosti takové infrastruktury musel panovník své pravomoci delegovat na některé své poddané, aby mu pomohli se správou říše. Takto šel vývoj dále, kdy člověk při svém vývoji vynalézal nové technologie, které se postupně dostávaly do infrastruktury až dospěl ve vznik moderních státních zřízení.

Každá infrastruktura čelí mnoha nástrahám, které ji mohou narušit, ať už se jedná o působení přírodních živlů či působení člověka. Proto je potřeba ji chránit. V první části své práce jsem se zaměřil na současnou kritickou infrastrukturu České republiky. Jaké konkrétní subjekty do ní spadají a jaké pravomoci a povinnosti tyto subjekty mají dány zákonem. Pokud je něco pro současnou infrastrukturu typické, tak je to elektrická energie a počítačové sítě. Současná společnost se stala na těchto komoditách natolik závislá, že při jakékoliv ztrátě

těchto komodit vzniká kritická situace, kdy člověk není schopen vykonávat svoji činnost a přichází o jednu z možností komunikace.

Vzhledem k velké závislosti na komunikaci skrze počítače jsem se v druhé části této práce zaměřil na komunikaci samotnou. Zaměřil jsem se na její historický a technologický vývoj. Je zřejmé, že některé dřívější způsoby komunikace nejsou schopny uspokojit potřeby moderního člověka, ale při výpadku počítačové komunikace mohou některé způsoby nabídnout dočasné alternativní řešení.

V další části práce jsem se zaměřil na jeden z prvků kritické infrastruktury a moderní způsob počítačové komunikace, kdy jsem si vybral kybernetické útoky na některá nemocniční zařízení v České republice. Tyto útoky na počítačovou infrastrukturu nejen nemocnic probíhají po celém světě a bývají velmi úspěšné. Útočníci se snaží zneužít oficiálních funkcí v aplikacích k distribuci škodlivého kódu, kterým se snaží proniknout do počítačové sítě a získat nad ní kontrolu. Tímto způsobem se snaží dostat k citlivým datům za účelem získání finančních prostředků prostřednictvím vydírání. Zaměřil jsem se na distribuci škodlivého kódu prostřednictvím maker v dokumentech kancelářského balíku Microsoft Office. Dále jsem se zaměřil na postup pro obnovení počítačové sítě při proniknutí útočníka a jak vybudovat bezpečnější počítačovou síť.

V poslední části práce jsem se zaměřil na makra samotná. Jaké druhy maker existují a jaké jsou možnosti pro spouštění maker v souborech kancelářského balíku Microsoft Office.

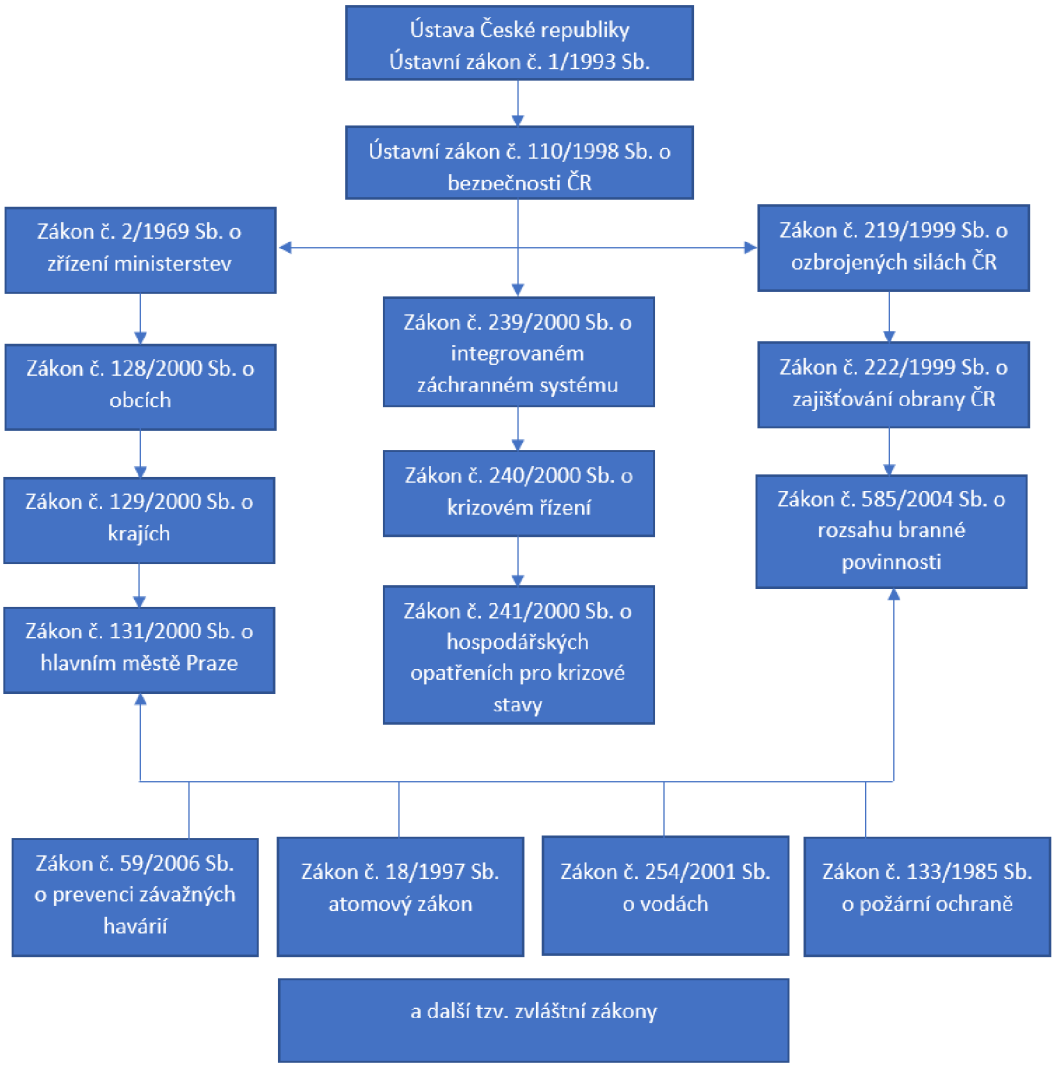
1. Kritická infrastruktura

Česká republika je demokratický právní stát, který je vázán zákony a mezinárodními smlouvami. Vystupuje prostřednictvím svých orgánů veřejné moci, kdy tyto orgány se podílejí na krizovém řízení. Samotný právní řád České republiky přímo stanovuje, že orgány veřejné moci mohou činit pouze to, co jim ukládá zákon. Povinnosti mohou být ukládány na základě a v mezích zákona. Do kritické infrastruktury tak patří v první řadě právní normy, které slouží jako nástroj orgánům veřejné moci při řešení krizové situace.

Součástí kritické infrastruktury je také krizové řízení. Krizové řízení je většinou chápáno jako řízení prostředků a sil při již vzniklé kritické události. Ovšem do tohoto řízení spadá i prevence proti takovéto události. Jedná se o takové řízení, při kterém je co nejefektivněji dosaženo nebo zabráněno vzniku kritické události, a to k tomu určenými prostředky. Stejně tak sem spadá i kontrola a vyhodnocování. Důležité je zmínit i zákonnost užitých prostředků, neboť při vzniku kritické události může docházet k vynucování právní povinnosti a dočasného omezení některých práv.

1.1. Krizové řízení

Mezi základní nástroje krizového řízení patří především platné právní normy, které dávají kompetence státním orgánům a dalším subjektům kritické infrastruktury ke krizovému řízení a vytváření dalších podmínek pro řešení krizových situací a jejich předcházení. Do těchto právních norem patří Ústava České republiky a ústavní zákony, zákony a podzákonné předpisy. Na základě těchto norem jsou orgány veřejné moci zmocněny k využití mimořádných opatření pro zvládnutí krizových situací.



Obrázek č. 1 - schéma legislativy krizového řízení[1]

Na obrázku č. 1 je uvedeno schéma zobrazující legislativu České republiky, která spadá do krizového řízení. Toto schéma je zjednodušeno, kdy jsou zde zobrazeny ty nejstěžejnější právní předpisy. Nejsou zde vyobrazeny další zákony, podzákonné předpisy a metodiky, které se taktéž zabývají ochranou kritické infrastruktury. Ze zobrazeného schématu lze učinit závěr, že kritická infrastruktura je komplexní systém, který do sebe zahrnuje několik různých oblastí. Mezi základním kameny kritické infrastruktury a krizového řízení na území České

[1] *Ministerstvo vnitra České republiky, generální ředitelství Hasičského záchranného sboru České republiky: Krizové řízení při nevojenských krizových situacích.* [online]. [cit. 10.02.2022]. Dostupné z: https://docplayer.cz/21764430-Ministerstvo-vnitra-generalni-reditelstvi-hasicskeho-zachranneho-sboru-ceske-republiky.html

republiky patří Ústava České republiky doprovázená Listinou základních práv a svobod a další ústavní zákony, především ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky, kdy na základě těchto ústavních zákonů byly položeny další zákony a jiné právní předpisy, sloužící jako nástroje při zvládání krizových situací a vymezením práv a povinností dotčených orgánů a osob, které jsou v těchto zákonech uvedeny. Ústavní zákon o bezpečnosti České republiky definuje nouzový stav, důvody k jeho vyhlášení a subjekty, které jsou oprávněny k jeho vyhlášení. V prvním odstavci článku 3 tohoto ústavního zákona je stanoveno: *„bezpečnost České republiky zajišťují ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby*“[2] a ve druhém odstavci je dále stanoveno: *„státní orgány, orgány územních samosprávných celků a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti České republiky, kdy rozsah povinností a další podrobnosti stanoví zákon.*“[3]

Pokud ústavní zákony nazveme základním kamenem kritické infrastruktury, tak následující zákony uvedené ve schématu můžeme nazvat jako hlavní stavební pilíře kritické infrastruktury, které na těchto kamenech stojí a dále jej rozvíjejí. V ústavním pořádku České republiky je stanovena dělba státní moci, kdy tato moc se rozděluje mezi další státní subjekty, prostřednictvím kterých je dále vykonávána státní správa. V levé části schématu jsou zobrazeny právní předpisy stanovující subjekty státní správy a územní samosprávy. V těchto právních předpisech je určena jejich struktura, činnosti, kompetence a působnost. V pravé části schématu jsou uvedeny právní předpisy, které se týkají problematiky vnějšího ohrožení bezpečnosti státu, především vojenského konfliktu.

Uprostřed schématu jsou uvedeny právní předpisy týkající se krizového řízení, tzv. „krizové zákony“. Tyto krizové zákony definují kritickou infrastrukturu a subjekty, které se na ní podílejí. Krizový zákon kritickou infrastrukturu v České republice definuje jako *„prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, jehož narušení funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo*

---

[2] *Česko: Ústavní zákon č. 110 ze dne 22. dubna 1998 o bezpečnosti České republiky.* In Sbírka zákonů České republiky. 1998, částka 39, s. 5386 [online]. [cit. 11.02.2022]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3146

[3] Tamtéž

ekonomiku státu"[4]. Krizové zákony dále vymezují orgány krizového řízení (viz obrázek č. 2). Dále ukládají povinnosti a stanovují úkoly orgánům krizového řízení. Při přípravě na kritickou situaci ukládá povinnosti i dalším subjektům, které se podílejí na kritické infrastruktuře. Stejně tak stanovuje sankce za porušení povinností uložených tímto zákonem. Dále řeší zřizování bezpečnostních rad a bezpečnostních štábů. Zřizují integrovaný záchranný systém, kdy se jedná o koordinovaný postup záchranných složek při likvidaci následků krizové situace a obnovení této situace zpět do neohrožujícího funkčního stavu.[5]

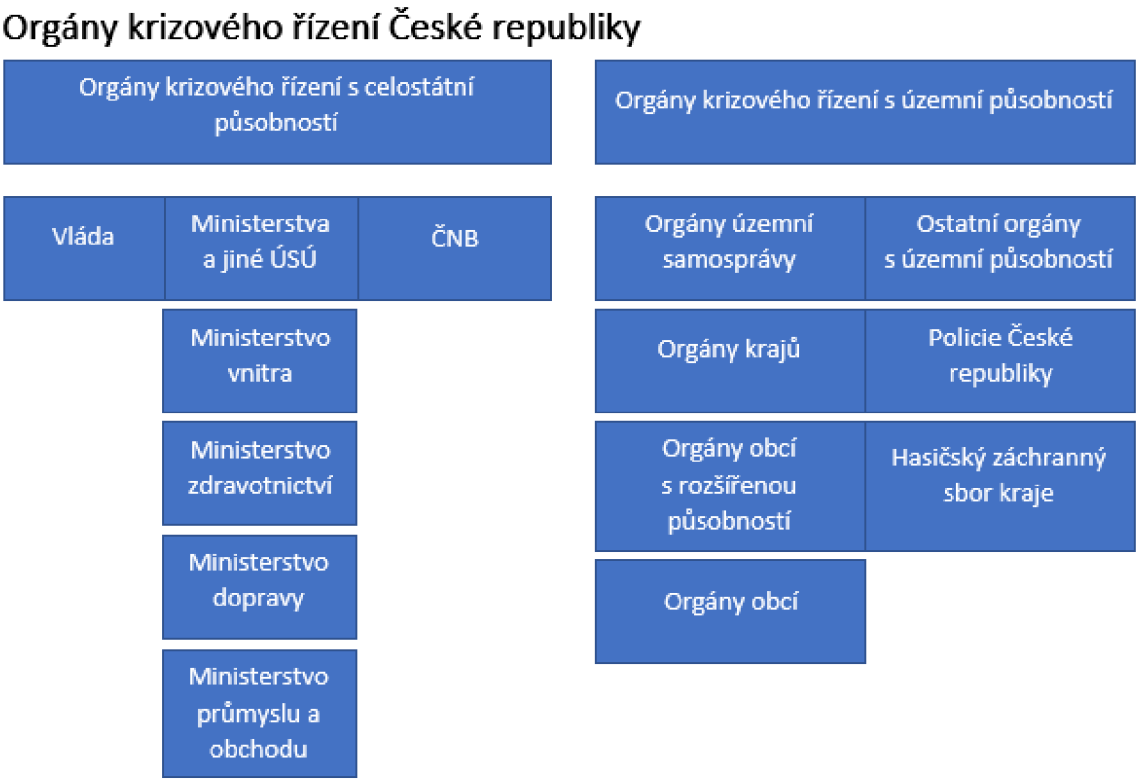
Ve spodní části schématu jsou uvedené právní předpisy, které upravují specifickou problematiku ohrožení infrastruktury. Zákon o vodách se zabývá problematikou povodní, atomový zákon se zase zabývá problematikou ochrany před nebezpečím ionizujícího záření v souvislosti s využíváním jaderné energie, zákon o požární ochraně řeší problematiku ochrany před požáry a poskytování pomoci při živelních pohromách atd.

Na následujícím obrázku č. 2 je zobrazeno schéma orgánů státní správy krizového řízení vymezených zákonnými předpisy. Tyto orgány z hlediska působnosti rozdělujeme na orgány s celostátní působností a orgány s územní působností. Tyto orgány v rámci krizového řízení vytvářejí krizové plány, kdy se jedná o dokumenty obsahující opatření a postupy při vzniku krizových situací. Tato krizová opatření se pak dotýkají kritických infrastruktur, které mají jednotlivé orgány ve své územní nebo věcné působnosti. U orgánů s celostátní působností se jimi vytvořené krizové plány dotýkají celého území České republiky, kdy jednotlivá ministerstva a ústřední správní úřady pak vydávají plány a opatření k infrastrukturám, které spadají do jejich kompetencí. Zároveň jak tyto krizové plány, tak i další metodiky v daných oblastech slouží dalším orgánům, především orgánům s územní působností při vytváření krizových opatření v rámci jejich samosprávy.

---

[4] *Česko: Zákon č. 240 ze dne 28. června 2000 o krizovém řízení a o změně některých zákonů*. In Sbírka zákonů České republiky. 2000, částka 73, s. 3745 [online]. [cit. 11.02.2022]. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240

[5] *Generální ředitelství Hasičského záchranného sboru ČR: Integrovaný záchranný systém* [online]. [cit. 11.02.2022]. Dostupné z: https://www.hzscr.cz/clanek/integrovany-zachranny-system.aspx



Obrázek č. 2 - schéma orgánů krizového řízení ČR[6]

1.2. Prvky kritické infrastruktury

V rámci krizového řízení je nutno stanovit jednotlivé konkrétní oblasti a služby moderní společnosti, kdy jakýkoliv výpadek nebo omezení těchto oblastí, by mohl mít značně negativní dopady na fungování společnosti, státu a životy lidí. Tyto oblasti jsou nazývány prvky kritické infrastruktury, kdy kritéria jednotlivých prvků kritické infrastruktury jsou stanovena vládou České republiky, a to konkrétně nařízením č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury. Tato kritéria jsou označována jako průřezová a odvětvová kritéria.

Průřezová kritéria jsou definována v ustanovení § 1 uvedeného nařízení, kdy „*průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko:*

- *obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,*

[6] *Ministerstvo vnitra České republiky, generální ředitelství Hasičského záchranného sboru České republiky: Krizové řízení při nevojenských krizových situacích*. [online]. [cit. 11.02.2022]. Dostupné z: https://docplayer.cz/21764430-Ministerstvo-vnitra-generalni-reditelstvi-hasicskeho-zachranneho-sboru-ceske-republiky.html

- *ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo*
- *dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob.*“[7]

Průřezovými kritérii jsou určeny hodnoty, od kterých se daný prvek stává součástí kritické infrastruktury, kdy určujícím hlediskem je tedy rozsah negativního dopadu na řádný chod společnosti v případě ohrožení tohoto prvku.

Odvětvová kritéria jsou uvedena v příloze nařízení vlády o kritériích pro určení prvku kritické infrastruktury, kdy tato kritéria jsou rozdělena v následující tabulce.

Energetika	• elektřina • zemní plyn • ropa a ropné produkty • centrální zásobování teplem
Vodní hospodářství	• zásobování vodou • úprava vodního díla
Potravinářství a zemědělství	• rostlinná výroba • živočišná výroba • potravinářská výroba
Zdravotnictví	• poskytování zdravotních služeb • výroba léčivých přípravků
Doprava	• silniční doprava • železniční doprava • letecká doprava • vnitrozemská vodní doprava
Komunikační a informační systémy	• technologické prvky pevné sítě elektronických komunikací • technologické prvky mobilní sítě elektronických komunikací • technologické prvky sítí pro rozhlasové a televizní vysílání • technologické prvky pro satelitní komunikaci • technologické prvky pro poštovní služby • technologické prvky informačních systémů • oblast kybernetické bezpečnosti

[7] *Česko: Nařízení vlády č. 432 ze dne 22. prosince 2010 Sb. o kritériích pro určení prvku kritické infrastruktury.* In Sbírka zákonů České republiky. 2010, částka 149, s. 5623 [online]. [cit. 12.02.2022]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=21413

Finanční trh a měna	• výkon činnosti České národní banky • poskytování služeb v bankovnictví a pojišťovnictví
Nouzové služby	• integrovaný záchranný systém • radiační monitorování • předpovědní, varovná a hlásná služba
Veřejná správa	• veřejné finance • sociální ochrana a zaměstnanost • státní sociální podpora • sociální pomoc • ostatní státní správa • zpravodajské služby

Tabulka č. 1 - odvětvová kritéria[8]

Na uvedené tabulce jsou v levém sloupci vypsány jednotlivé prvky odvětvových kritérií. V pravém sloupci se nacházejí jednotlivé podkategorie, které spadají pod daný prvek. Uvedená kritéria a jejich podkategorie reflektují potřeby moderní společnosti, kdy právě tyto prvky jsou nejen v České republice, ale i ve většině států světa v dnešní době nezbytné pro zajištění řádného fungování státu a lidské společnosti jako takové. Mezi velmi kritické prvky patří ty komodity, které není Česká republika si schopna samostatně vyrobit. Jako příklad může posloužit v oblasti energetiky podkategorie ropa a zemní plyn. Právě tyto produkty není Česká republika schopna samostatně vyrábět v takovém množství, aby mohla uspokojit své obyvatelstvo, kdy v této oblasti je zcela závislá na dovozu těchto produktů z jiných zemí. V této oblasti hrají velkou roli mezinárodní vztahy se státy, od kterých jsou uvedené komodity odebírány. V souvislosti s touto problematikou je třeba zmínit Státní správu hmotných rezerv, kdy právě tento orgán státní správy hraje významnou roli v opatřeních pro krizové stavy, kdy tato role spočívá ve vytváření a ochraňování hmotných rezerv surovin určených pro zajištění státu a jeho obyvatel v případě vzniku krizových situací.[9]

V rámci kritické infrastruktury nelze opomenout ani právnické osoby, neboť některé prvky kritické infrastruktury jsou ve vlastnictví těchto podnikatelských

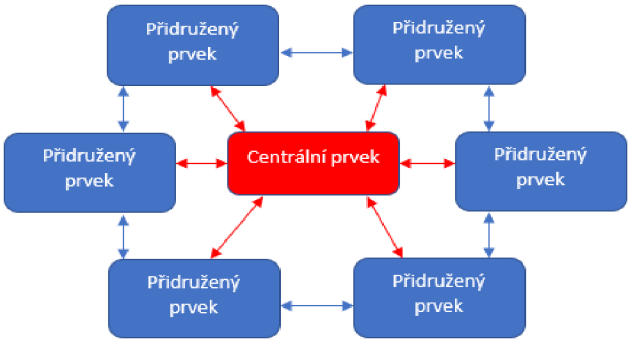
[8] *Česko: Nařízení vlády č. 432 ze dne 22. prosince 2010 Sb. o kritériích pro určení prvku kritické infrastruktury*. In Sbírka zákonů České republiky. 2010, částka 149, s. 5623 [online]. [cit. 12.02.2022]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=21413

[9] *Česko: Zákon č. 97 ze dne 25. února 1993 o působnosti Správy státních hmotných rezerv*. In Sbírka zákonů České republiky. 1993, částka 27 [online]. [cit. 12.02.2022]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=2671

subjektů, kdy tyto prvky jim slouží k podnikatelské činnosti. Spolupráce státních orgánů a soukromých subjektů při budování a ochraně kritické infrastruktury je tedy nezbytná.

2. Telekomunikace

Komunikace je sdělování informací mezi dvěma nebo více subjekty. V telekomunikaci je při sdělování informací využito technické zařízení nebo nějaké přenosové médium. Díky přenosu informací tak dochází ke vzájemnému propojení subjektů, kdy toto propojení nám může sloužit ke sbírání údajů a dat k jejich analýze, ke kontrole funkčnosti a k zpětné vazbě. Pod pojmem telekomunikace si nelze představit jen současné moderní technologie, ale do této kategorie spadají také technologie, která byla na našem území využívána v historických dobách při vzniku krizové situace, ať už se jedná o světelné signály ve formě signalizačních ohňů či akustické signály ve formě bubnování, hraním na varovné trubky, posíláním vzkazů prostřednictvím cvičeného ptactva anebo kurýrní služba prostřednictvím poslů. Pokud se podíváme do historie naší země, můžeme spatřit některé dobové prvky kritické infrastruktury. Jako první se nabízí budování sídel na vyvýšených kopcích, kdy právě takovéto umístění vedlo k lepšímu přehledu nad krajinou a včasnějšímu spatření případných hrozeb. Dále zde bylo sníženo riziko možného zaplavení sídla zvýšenou hladinou vodních toků. Tato sídla byla ovšem záměrně budována na kopcích z důvodu dohledu na sousední sídlo, kdy v případě mimořádné situace sídlo, které bylo v ohrožení vyslalo signál sousednímu sídlu. Díky tomuto způsobu komunikace tak byla vyslána informace o vzniklé situaci, která se postupně dostala k dalším sídlům až k samotnému panovníkovi. Vzhledem k tehdejším poměrům a tehdejšímu technologickému vývoji, by se jednotlivá panská sídla dala zařadit mezi prvky kritické infrastruktury.[10]



Obrázek č. 3 - komunikační schéma

[10] *Wikipedie: Otevřená encyklopedie: Komunikace* [online]. [cit. 25.02.2022]. Dostupné z https://cs.wikipedia.org/w/index.php?title=Komunikace&oldid=21357436

Na obrázku č. 3 je zobrazeno modelové znázornění uspořádání panských sídel, kdy centrálním prvek představuje sídlo panovníka a přidružené prvky představují sídla jednolitých šlechtických rodů, které panovníku sloužily. Je zde znázorněno komunikační schéma s centrálním prvkem, tak i komunikační schéma mezi sousedícími prvky. Přidružené prvky sloužily jako prodloužené paže a oči panovníka při správě země a zároveň sloužily také jako obrana centrálního prvku před cizím narušitelem. V případě narušení nebo zničení centrálního prvku došlo k destabilizaci nebo pádu celé země. Pohledem na moderní uspořádání České republiky lze vidět podobnost k historickému modelu. Z pohledu řízení kritické infrastruktury si lze za centrální prvek dosadit úřad vlády a jednotlivá ministerstva a za přidružené prvky si lze dosadit jednotlivé územní samosprávné celky. V rámci kritické infrastruktury centrální prvek nemusí být schopen řídit celou infrastrukturu sám, například vzhledem rozsahu území, na kterém je infrastruktura vybudována. Musí tedy řízení dále delegovat na přidružené prvky, které se na tomto řízení dále podílí, kdy k řízení je zapotřebí komunikace jak s centrálním prvkem, tak i mezi sebou.

Pro telekomunikaci je zásadní přítomnost prvku, jehož prostřednictvím je informace dále přenášena. Jedná se o druh komunikace, při které člověk nepředává informaci vlastními tělesnými funkcemi, které mu jsou fyziologicky dány. Při telekomunikaci je tedy informace přenášena prostřednictvím zařízení, které člověk vytvořil anebo prostřednictvím živého média (tvora), které vycvičil. Zásadním obdobím v oblasti telekomunikací je období konce devatenáctého a začátek dvacátého století, kdy v této době dochází k vynálezům umožňujících komunikaci na velkou vzdálenost. Dále dochází k budování a rozšiřování infrastruktury elektrické sítě. Právě vynález elektrické energie přinesl zásadní zlom jak v telekomunikaci, tak i v lidské společnosti. Příchodem elektrické energie a technologií s ní souvisejících můžeme označit vznik moderní společnosti, jak ji známe dnes. Podle elektrické energie lze telekomunikaci rozdělit do kategorií na tradiční způsoby a moderní způsoby přenosu informací.[11]

[11] *Wikipedie: Otevřená encyklopedie: Telekomunikace* [online]. [cit. 05.03.2022]. Dostupné z https://cs.wikipedia.org/w/index.php?title=Telekomunikace&oldid=19883798

2.1. Tradiční telekomunikace

Pro tradiční telekomunikaci je specifická absence závislosti na přísunu elektrické energie. Pro tento typ telekomunikace je specifické přímé využití přírodních zdrojů anebo přímé působení člověka. Tuto kategorii můžeme dále rozvětvit.

2.1.1. Světelné signály

Od dob ovládnutí přírodní síly ohně se jedná o jeden z nejstarších prostředků telekomunikace. Pro světelné signály je specifické jejich světelné záření, které je schopno upoutat pozornost lidského oka na velkou vzdálenost. V minulosti byly signalizační ohně jedním z hlavních prostředků pro komunikaci na větší vzdálenost. Pro vytvoření takového signálu postačují jednoduše dostupné přírodní zdroje. V moderní době bývají pro světelnou komunikaci využívány signalizační světlice nebo světelná zařízení poháněná elektrickou energií Nevýhoda tohoto druhu komunikace spočívá v nutnosti umístění zdroje na vyvýšené místo, pokud chceme tímto signálem upoutat co největší pozornost. Dále zde hraje značnou roli počasí, kdy za velmi špatné viditelnosti může dojít k přehlédnutí světelného signálu. Další nevýhodou je, že tímto způsobem lze přenést pouze jedinou informaci (pozor, nebezpečí, pomoc).[12]

2.1.2. Akustické signály

Pro tento druh telekomunikace je zcela jednoznačně specifický vytváření a přenos zvukového projevu. Pro vytvoření akustického signálu je zapotřebí člověkem vyrobeného nástroje, pomocí kterého je zvuk vytvořen a přenesen do okolí. K vytváření těchto akustických projevů jsou většinou využívány bubny, trubky, zvonů anebo sirény. U tohoto druhu telekomunikace je výhodou, že zde není nutná přímá viditelnost na zdroj signálu. Dále je zde možnost přenést více informací oproti světelnému signálu, například změnou rytmu nebo změnou melodie. Nevýhodou je neustále působení člověka na nástroj při vytváření akustického projevu. Dále má na přenos zvuku vliv prostředí, ve kterém je přenášen a vliv počasí, kdy může dojít k útlumu zvukového přenosu nebo i k jeho

[12] *Wikipedie: Otevřená encyklopedie: Telekomunikace* [online]. [cit. 05.03.2022]. Dostupné z https://cs.wikipedia.org/w/index.php?title=Telekomunikace&oldid=19883798

přehlučení. V moderní době jsou v rámci kritické infrastruktury k akustickým signálům využívány převážně hasičské sirény, které bývají ovládány za pomoci elektrické energie.[13]

2.1.3. Kurýrní služba

Pod pojmem kurýrní služba chápeme přenos informace, která je buď v psané nebo tištěné formě, posílána mezi odesílatelem a příjemcem prostřednictvím člověka. Jako přenášená informace je tedy zpráva, která je zaznamenána na určitém médiu. Může se jednat o text na papíře, ale spadá sem i obrazový nebo zvukový záznam uložený na datovém nosiči. Výhodou kurýrní služby je, že daná zpráva může obsahovat velké množství informací. Nevýhodou je pomalejší předání informace v závislosti na vzdálenosti subjektů a způsobu dopravy. Další nevýhodou může být ohrožení kurýra nebo zásilky během přepravy, kdy může dojít k poškození, zničení nebo zmocnění se zásilky. Kurýrní služba je hojně využívána i v dnešní době. Zejména u státních orgánů a bezpečnostních složek při přepravě důležitých a utajovaných dokumentů, kdy tuto činnost provádějí prověření pracovníci. Dále do této kategorie spadají i poštovní služby. V současné době ovšem některé aspekty kurýrní služby bývají nahrazovány elektronickou komunikací.[14]

2.1.4. Komunikace prostřednictvím zvířat

V tomto případě se jedná o přenos informace prostřednictvím cvičené zvěře. Zpráva je připevněna k tělu zvířete, které je následně dopraví adresátovi. Pro tento účel byli v minulosti využíváni především poštovní holubi. Jejich výhoda spočívá v tom, že nejsou omezováni obstrukcemi v terénu, kdy můžou vzduchem přímo letět se zprávou k adresátu. Nevýhoda spočívá v menší velikosti holuba, kdy jeho menší vzrůst je limitem pro velikost zprávy. Další nevýhodou je možný útok predátora. Jako další zvíře se k doručování zpráv využíval pes. Například v dobách první světové války se pes využíval k předávání zpráv mezi frontovými liniemi. Jeho výhoda spočívá v rychlosti, agilnosti a menšímu vzrůstu oproti

---

[13] *Wikipedie: Otevřená encyklopedie: Akustika* [online]. [cit. 05.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Akustika&oldid=20173963

[14] *Wikipedie: Otevřená encyklopedie: Kurýrní služba* [online]. [cit. 05.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Kur%C3%BDrn%C3%AD_slu%C5%BEba&oldid=20207260

člověku, čímž byl těžším cílem pro nepřátelskou palbu. Oproti holubu měl výhodu ve větším vzrůstu, tudíž mohl unést více zpráv. Na druhou stranu byl při přepravě omezován obstrukcemi terénu. Nevýhodou v této kategorii telekomunikace je také časová náročnost při výcviku zvířat.[15]

2.2. Moderní telekomunikace

Moderní telekomunikace zahrnuje předávání informací prostřednictvím prostředků, které ke své funkčnosti vyžadují přísun elektrické energie. Tyto prostředky jsou schopny ve velmi krátkém čase předat velké množství informací na velkou vzdálenost mnoha příjemcům. Jejich nevýhoda spočívá v závislosti na připojení k elektrické síti nebo k jinému zdroji elektrické energie, kdy v případě odpojení od takového zdroje, dochází k jejich výpadku.

2.2.1. Telegrafie

Pojem telegrafie by se mohl zařadit i mezi tradiční komunikaci, kdy do telegrafie se dají zařadit například kouřové signály, kdy posloupností kouřových mraků lze na větší vzdálenost poslat vzkaz. Ke konci 18. století byl vynalezen a následně do širšího využití nasazen optický telegraf. Jednalo se o systém věží, které byly navzájem na dohled dalekohledem. Na těchto věžích byly na stožárech umístěny vahadla, na jejichž koncích byla kratší ramena. Tento mechanismus byl ovládán za pomocí lan a kladek. Jednotlivým polohám ramen byly přiřazeny znaky abecedy, kdy pohybem tohoto mechanismu byla odeslána zpráva. Tento systém byl později nahrazen vynálezem elektrického telegrafu. Elektrický telegraf můžeme označit jako první zařízení, které pro přenos zpráv využívalo elektrickou energii. Jednotlivé telegrafní stanice byly propojeny elektrickým vedením. Zde byla nevýhoda, která spočívala v nutnosti zavedení elektrických kabelů do míst, kam měla být telegrafní stanice umístěna. S rozvojem radiového vysílání byl později vynalezen bezdrátový telegraf, u kterého zavedení elektrických kabelů odpadlo. Stačilo, aby zařízení bylo v dosahu vysílače. V případě bezdrátového telegrafu musela ale být obsluha neustále přítomna u zařízení pro příjem zpráv, kdežto u

[15] *Wikipedie: Otevřená encyklopedie: Zvířata během první světové války* [online]. [cit. 05.03.2022]. Dostupné z: https://cs.frwiki.wiki/wiki/Animaux_durant_la_Premi%C3%A8re_Guerre_mondiale

kabelového telegrafu se zpráva zapisovala na papírový pásek, který bylo možné si přečíst později. Další nevýhoda spočívala v nutnosti odborné znalosti tzv. telegrafní abecedy. Zpráva přenášena pomocí telegrafních přístrojů byla kódována posloupností teček a čárek, kdy jednotlivým posloupnostem těchto znaků bylo přiřazeno písmeno abecedy.[16]

2.2.2. Telefonie

S nástupem telefonie došlo k nahrazení telegrafů telefonními přístroji. Výhoda telefonie je jednoznačně v možnosti přenášení lidského hlasu v reálném čase na velkou vzdálenost. Díky tomu odpadává jakákoliv nutnost kódovat zprávy a znalost dešifrovacích postupů. Komunikace prostřednictvím telefonů je tedy mnohem rychlejší a efektivnější. Telefonii lze opět rozdělit na drátovou a bezdrátovou.[17] U drátových telefonů jsou telefonní přístroje prostřednictvím kabelového vedení připojeny k telefonní ústřednám, kdy tyto ústředny slouží k propojování telefonních hovorů. Prostřednictvím kabelového připojení jsou koncová telefonní zařízení napájena elektrickým proudem, tudíž v případě výpadku elektrického proudu, jsou telefonní přístroje dále napájeny z telefonních ústředen, které v případě výpadku elektrického proudu jsou napájeny náhradními zdroji elektřiny. Zde se opět nabízí nevýhoda v podobě budování kabelové sítě a zavedení kabelového připojení k telefonnímu přístroji. Dále pokud dojde k výpadku telefonní ústředny, dojde i k výpadku telefonních přístrojů. Stejně tak v případě poškozením kabelového vedení dojde k výpadku zařízení. Na druhé straně kabelové vedení není náchylné vůči podnebním podmínkám, čímž dokáže poskytnout vyšší kvalitu přenosu informací.[18] V souvislosti s kabelovým připojením je třeba v telefonii zmínit také telefax, tedy zařízení, které umožňuje přenos statického obrazu prostřednictvím telefonní linky.[19] V dnešní době je telefax nahrazen elektronickou počítačovou komunikací. U bezdrátové telefonie komunikují telefonní přístroje mezi sebou a základnovou stanicí prostřednictvím

---

[16] *Wikipedie: Otevřená encyklopedie: Telegrafie* [online]. [cit. 10.03. 2022]. Dostupné z https://cs.wikipedia.org/w/index.php?title=Telegrafie&oldid=21426540
[17] *Wikipedie: Otevřená encyklopedie: Telefonie* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Telefonie&oldid=21610990
[18] *Wikipedie: Otevřená encyklopedie: Telefon* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Telefon&oldid=21409833
[19] *Wikipedie: Otevřená encyklopedie: Fax* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Fax&oldid=21254984

rádiových vln. Základnová stanice je zařízení, které vysílá a přijímá radiové signály z mobilních telefonů. Výhodou je mobilita přístroje, odtud vznikl název mobilní telefon. Pro přenos komunikace stačí, aby mobilní telefon byl v dosahu základové stanice. Vzdálenost od základové stanice a rozsah pokrytí má vliv na kvalitu a rychlost komunikace. Bezdrátové technologie jsou více náchylné vůči rušení vnějších vlivů. Mobilní přístroje kromě mobility mají výhodu ve vlastním bateriovém zdroji napájení, kdy dokážou fungovat i několik dní bez připojení k elektrickému zdroji, v závislosti na využívání přístroje. Stejně tak jsou základové stanice vybaveny bateriovým napájením, které je začnou napájet v případě výpadku elektrického proudu.[20] Kromě mobilních telefonních přístrojů je u bezdrátové technologie potřeba také zmínit satelitní telefony. Tyto telefonní přístroje komunikují prostřednictvím telekomunikačních satelitů, které se nacházejí na oběžné dráze naší planety. Satelitní komunikační technologie funguje zcela nezávisle na lokálních pozemských telekomunikační sítích. Nevýhodou je nutnost přímého výhledu telefonního zařízení na oblohu pro komunikaci se satelitem. Jako další nevýhodu je třeba brát v potaz možné působení kosmických sil, které mohou narušit komunikaci, případně poškodit satelitní zařízení na oběžné dráze.[21] Telefonní technologie se stala v moderní společnosti nepostradatelnou formou pro komunikace. Zejména na poli mobilních telefonů, kdy právě skladnost, mobilita a jednoduchost ovládání těchto zařízení měla za následek masivní rozšíření těchto zařízení po celém světě a v souvislosti s tím také budování a vývoj bezdrátové telekomunikační infrastruktury.

2.2.3. Radiofonie

Díky technologickému pokroku a vývoji v oblasti radiových vln vznikla zařízení, která pro komunikaci nepotřebovala přímá propojení mezi sebou prostřednictvím kabelového připojení, tudíž nebylo nutné pro komunikaci budovat kabelovou infrastrukturu, která je více náchylná vůči mechanickému poškození či zničení. Průběh první a následně druhé světové války značně posunul vývoj v oblasti radiových technologií, neboť bylo potřeba rychle a efektivně předávat

[20] *Wikipedie: Otevřená encyklopedie: Mobilní telefon* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Mobiln%C3%AD_telefon&oldid=21536046
[21] *Wikipedie: Otevřená encyklopedie: Satelitní telefon* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Satelitn%C3%AD_telefon&oldid=21314099

informace mezi vedoucími důstojníky a frontovými liniemi. [22] Kabelová infrastruktura snadno podléhala nepřátelským útokům, což vedlo k vynálezu radiové vysílačky. Stejně jako v případě bezdrátové telegrafie a telefonie i zde máme vysílací zařízení, tedy základnovou stanici, ke které se radiostanice připojuje a prostřednictvím ní komunikuje s dalšími zařízeními anebo mohou radiostanice komunikovat přímo mezi sebou. Na rozdíl od telefonních přístrojů nemohou u radiových vysílaček uživatelé vysílat a zároveň přijímat informace naráz. Vždy může komunikovat pouze jedno zařízení, kdy komunikaci slyší všechny další radiostanice, které jsou připojeny do stejné radiokomunikační sítě. Po dobu, kdy jedno zařízení vysílá, nemůže další zařízení začít vysílat, dokud zařízení vysílání neukončí. Při tomto způsobu předávání informací je nutná komunikační kázeň, kdy účastníci komunikace jsou nuceni dodržovat určitá pravidla pro komunikaci a předejít tak k narušování vysílání. [23] Radiová komunikace je velice efektivní při koordinaci většího počtu účastníků, proto bývá využívána ozbrojenými silami, bezpečnostními a záchrannými složkami po celém světě. Radiokomunikační sítě těchto složek bývají oddělené od ostatních veřejných sítí, aby fungovali nezávisle v případě výpadku veřejných sítí. [24] Základové stanice jsou také vybaveny záložním bateriovým napájením pro případ výpadku elektrického proudu. Stejně tak mají mobilní radiostanice vlastní bateriový zdroj napájení, který jim umožňuje fungovat bez zdroje elektrického proudu i několik dní v závislosti na využívání přístroje. Při radiokomunikaci se radiostanice nejprve musí připojit k radiokomunikační síti. Toho lze docílit buď naladěním radiostanice na určitou frekvenci, na které vysílá základnová stanice anebo zvolením příslušného komunikačního kanálu, jsou-li takové kanály na radiostanici přednastaveny. V souvislosti s radiokomunikačními sítěmi je třeba zmínit, že radiokomunikační sítě bezpečnostních složek jsou chráněny šifrováním proti přístupu a odposlechu nepovolaných osob. Toho je dosaženo

---

[22] *Wikipedie: Otevřená encyklopedie: Telekomunikace* [online]. [cit. 10.03.2022]. Dostupné z https://cs.wikipedia.org/w/index.php?title=Telekomunikace&oldid=19883798

[23] *Wikipedia: The Free Encyclopedia: Radio* [online]. [cit. 10.03.2022] Dostupné z: https://en.wikipedia.org/w/index.php?title=Radio&oldid=1107386517

[24] *Ministerstvo vnitra České republiky: Technologie, struktura a služby sítě Pegas* [online]. [cit. 11.03.2022]. Dostupné z: https://www.mvcr.cz/soubor/technologie-site-pegas-pdf.aspx

přeprogramováním radiostanic, kdy nahráním specializovaného softwaru, se radiostanice může připojit do radiokomunikační sítě.

2.2.4. Hromadné sdělovací prostředky

Hlavním účelem hromadných sdělovacích prostředků je předání informace velkému počtu účastníků najednou. Za tímto účelem bylo vynalezeno rádio, tedy zařízení využívající radiových vln pro vysílání zvukových informací.[25] Následně se jako další sdělovací prostředek objevila televize, která na rozdíl od rádia dokázala kromě zvuku poskytnout i obrazový přenos. Pro hromadné sdělovací prostředky je charakteristické, že vysílají informaci pouze ven. Není skrze tato zařízení možno komunikovat s odesílatelem sdělení. Výhoda rádií spočívá v jejich mobilitě a vlastnímu bateriovému zdroji napájení. Naopak televize díky obrazovému přenosu může vizuálním znázorněním lépe vysvětlit obsah sdělení a zároveň i lépe zaujmou sledující účastníky. V případě rádia je zde vysílání prováděno výhradně bezdrátově, kdežto u televizního vysílání je přenos prováděn také prostřednictvím kabelového připojení. Právě kabelové připojení v tomto případě je schopno zajistit mnohem vyšší datový tok informací, což vede k velmi vysoké kvalitě obrazu na televizním zařízení.[26]

2.2.5. Počítačové sítě

Technologie počítačových sítí patří mezi nejnovější a nejmodernější způsob přenosu informací. Počítačová síť je vytvořena vzájemným propojením zařízení výpočetní techniky, nazývaných počítače. Tyto počítače jsou propojeny buď napřímo mezi sebou anebo prostřednictvím síťového prvku. Způsob propojení může být uskutečněn prostřednictvím kabelového anebo bezdrátového připojení. Počítače mohou při komunikaci vysílat a zároveň přijímat informace. Informace lze ukládat, archivovat a dále s nimi pracovat. Není zde limitován počet účastníků komunikace. Limity jsou pouze dány výkonem výpočetních zařízení a výkonem počítačové sítě. Největší počítačovou sítí na světě je nazýván internet. Jedná se o celosvětovou počítačovou síť, která vznikla propojením počítačových sítí. Zcela

[25] *Wikipedie: Otevřená encyklopedie: Rozhlas* [online]. [cit. 11.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Rozhlas&oldid=21392356
[26] *Wikipedie: Otevřená encyklopedie: Televize* [online]. [cit. 11.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Televize&oldid=21438634

jednoznačně je největší výhodou také rychlost přenosu informací, kdy tyto jsou mezi počítači přenášeny řádově v milisekundách či sekundách. Opět zde ale hraje roli kapacitní velikost přenášené informace a výkon výpočetních zařízení. Další výhodou počítačů je multitasking, tedy schopnost zpracovávat několik operací najednou. Některé operace mohou být plně automatizovány, tudíž zde nemusí být nutnost neustále přítomnosti obsluhy. Zpracovávané informace je možné si přečíst kdykoliv později. Dále je zde možnost dálkového přístupu k informacím z jiného zařízení. V souvislosti s dálkovým přístupem vyplývá nevýhoda ve zranitelnosti počítačových sítí. Díky vzdálené komunikaci a vzdálenému přístupu lze takovou síť napadnout a způsobit její vyřazení z provozu, kdy pak jednotlivé počítače nejsou schopny dále mezi sebou komunikovat. Dále je zde potřeba alespoň základních odborných znalostí v ovládání počítačového systému. Dnešní počítačové systémy nabízí pokročilá grafická rozhraní, která běžnému uživateli usnadňují jejich ovládání. Nicméně odborná znalost se týká také znalosti základních konfiguračních prvků systému, znalosti bezpečnostních hrozeb a jak se jim vyvarovat. Technologický vývoj v oblasti počítačových sítí nám v současné době poskytuje rozsáhlé možnosti v telekomunikaci. Nicméně právě tímto vývojem narůstá komplexnost této technologie, kdy právě složitost může vést k vytváření většího množství chyb, které může kdokoliv využít k možnému narušení počítačové infrastruktury, kdy následky takového narušení mohou být velmi nákladné.[27]

Kritická infrastruktura a telekomunikace v rámci civilizačního vývoje kráčejí společně ruku v ruce. Narůstající robustnost a komplexnost infrastruktury vyžaduje rychlý a efektivní způsob komunikace a zároveň rychlostí a efektivností telekomunikace dochází k dalšímu rozvoji infrastruktury. V současné době jsou informační technologie integrovány do všech součástí kritické infrastruktury. Technologický pokrok v informačních technologiích se promítá do předchozích komunikačních metod, které vznikly před vynálezem počítačové techniky, a tudíž takovou technologii ke své funkčnosti nevyžadovaly. V této souvislosti jde o modernizaci komunikačních způsobů, která vede ke zkvalitňování přenosu

[27] *Wikipedie: Otevřená encyklopedie: Počítačová síť* [online]. [cit. 11.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5&oldid=21440133

informací, zefektivnění správy a údržby zařízení prostřednictvím dálkového přístupu, zautomatizování procesů apod. Na druhé straně je to právě dálkový přístup a vzájemné propojení zařízení, které je vystavuje značné zranitelnosti.

3. Kybernetická bezpečnost

Kyberprostorem se nazývá virtuální prostředí, které je tvořeno informačními a komunikačními systémy, tedy počítačovými sítěmi a koncovými zařízeními v nich připojené. Vzájemným propojením těchto sítí je tvořen kyberprostor, nazýván také internet. Jedná se o digitální svět, který není hmatatelný, ale události v něm vznikající se promítají v reálném světě. Tímto vznikl nový trh v digitální podobě, který otevřel nové možnosti v oblasti komunikací, obchodu a služeb. Stejně tak otevřel možnosti v oblasti kriminálních aktivit.[28]

3.1. Kybernetické hrozby

Kybernetickou hrozbou rozumíme hrozící nebo trvající útok na informační a komunikační systémy. Cílem těchto útoků je neoprávněné vniknutí do systému za účelem jej narušit, ochromit, způsobit jeho disfunkci, přerušit komunikaci mezi účastníky anebo se zmocnit důležitých dat. Pachatelem těchto útoků (nazýván též „hacker“) je buď jedinec nebo organizovaná skupina. Důvodem těchto kybernetických útoků bývá především generování zisku vydíráním. Útočník pronikne do systému, odkud odcizí důležitá data a pak požaduje výkupné za jejich navrácení. Za útokem můžou být také politické či náboženské důvody, šíření poplašných zpráv a paniky, znevážení postavení státních orgánů a jejich důvěry vůči veřejnosti. Dále může být důvodem i konkurenční boj společností na trhu, kdy se získáním firemního know-how snaží konkurenční společnost získat strategickou výhodu. Důvodem může být také vojenský útok v případě válečného konfliktu, kdy se jedna strana snaží narušit obranyschopnost té druhé.[29]

Ať už je důvod pro kybernetický útok jakýkoliv, pro pachatele nebo skupinu pachatelů je typická velmi dobrá odborná znalost v oblasti informačních technologií. Pachatelé mají znalosti v oblastech programování a vývoji aplikací, v operačních systémech, v konfiguraci a správě počítačových sítí. Jedná se tedy o odborníka v těchto oblastech, což mu činí značnou výhodu oproti znalostem,

---

[28] *Správa.sítě.eu: Co je to kyberprostor* [online]. [cit. 15.07.2022]. Dostupné z: https://www.sprava-site.eu/kyberprostor/

[29] *Wikipedie: Otevřená encyklopedie: Počítačová kriminalita* [online]. [cit. 15.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_kriminalita&oldid=20758707

který má běžný uživatel. Pro své útoky a vniknutí do informačních systémů využívá bezpečnostních děr a neznalostí nebo neopatrností uživatelů těchto systémů. Pro své útoky vytváří škodlivé programy, nazývanými malware (z anglického názvu „malicious software“)[30]. Tento škodlivý software se pak prostřednictvím počítačové sítě snaží dále šířit a napadat informační systémy. Pro vytvoření škodlivého software postačí pouze počítačové zařízení a prostředí pro vývoj aplikací, kdy některá vývojová prostředí jsou k dispozici zdarma a volně ke stažení. Dále je zapotřebí internetového připojení, které bývá dostupné prostřednictvím volně přístupných bezdrátových sítí. V podstatě jedinou větší překážkou pro útočníka je odborná znalost v informačních technologiích. Není ovšem nutné, aby útočník vytvořil škodlivou aplikaci přímo sám. Existují různé internetové stránky, na kterých lze takovéto aplikace sehnat včetně návodů a postupů k případnému kybernetickému útoku. Tyto internetové stránky jsou nazývány „dark weby“.[31] Jedná se o počítačovou síť, která není běžně dohledatelná internetovými vyhledávači a vstup do takové sítě je možný prostřednictvím specifického programu nebo jiným druhem autorizace. V zásadě se však jedná o legální síť, neboť tato síť bývá vytvořena za účelem vytvoření anonymity a tím dokáže poskytnout bezpečnější sdílení dat při internetové komunikaci. Na druhou stranu právě snaha o anonymitu a nepodléhání žádným autoritám dává těmto počítačovým sítím živnou půdu pro vývoj nelegální činnosti. Za pomocí odborných znalostí v oblasti počítačových sítí se pachatel také snaží zakrýt svou digitální stopu a odhalit tak místo odkud provedl útok. Kybernetické útoky může útočník provádět i ze země, se kterou Česká republika nemusí mít dobré diplomatické vztahy a tamní orgány činné v trestním řízení nemusí být ochotny spolupracovat při vypátrání pachatele.

Kybernetický útočník se při vniknutí do systému snaží najít nejslabší článek, který v mnoha případech tvoří uživatel. Útočník se lstivými metodami pokouší z uživatele vylákat citlivé údaje například v podobě přístupových hesel. Za tímto

[30] *Eset.cz: Co je malware? Jak se zbavit malwaru?* [online]. [cit. 15.07.2022]. Dostupné z: https://www.eset.com/cz/malware/#co-je-to-malware
[31] *Wikipedia, The Free Encyclopedia: Dark web* [online]. [cit. 15.07.2022]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Dark_web&oldid=1106032026

účelem je útočník při vytváření kybernetické hrozby schopen se přímo kontaktovat s obětí.

3.1.1. Phishing

Phishing je metoda, kterou se útočník snaží získat citlivá data za pomoci elektronické komunikace. Komunikace probíhá přes e-mail nebo prostřednictvím služeb pro přímé zasílání zpráv tzv. „instant messaging“ (například aplikace Messenger od společnosti Facebook). Příkladem může být nedávné šíření takové falešné komunikace prostřednictvím právě zmíněné aplikace Messenger.[32] Uživateli přišla do této aplikace zpráva s internetovým odkazem. Po rozkliknutí odkazu se otevřela podvodná internetová stránka, která se tvářila jako oficiální stránka společnosti Facebook a žádala uživatele o zadání přihlašovacích údajů. Tímto způsobem tak získal útočník velké množství přihlašovacích údajů a zároveň tyto účty zneužil k dalšímu šíření podvodných zpráv, což více umocnilo rychlost šíření tohoto podvodu, neboť uživatel, kterému přišla zpráva od přátelského kontaktu, nepředpokládal klamavé jednání. V případě phishingu je nutné věnovat pozornost přijímané zprávě, například spisovnosti, skloňování slov apod. Dále je třeba věnovat pozornost adrese odesílatele, kdy na základě názvu e-mailové lze pojmout podezření, že se jedná o podvod. Zvýšenou opatrnost je třeba dbát při zadávání osobních údajů na webových stránkách. Bližším pohledem na podvodné webové stránky lze najít grafické nesrovnalosti oproti skutečným, stejně tak v názvu stránky lze zjistit nesouhlasné údaje.[33]

3.1.2. Vishing

V případě vishingu se útočník snaží získat citlivé údaje prostřednictvím telefonního hovoru. S touto podvodnou metodou se lze nejčastěji setkat v bankovním sektoru. Útočník se po telefonním spojení s uživatelem vystupuje jako pracovník banky a uživatele informuje o smyšlené události, že bankovní účet uživatele byl napaden. Pro ochranu peněz před smyšleným odcizením útočník navrhne přesun peněz na záložní účet, kdy se jedná o účet útočníka. Uživatel poté

---

[32] *Svět Androida: Na tom videu jsi ty?* [online]. [cit. 16.07.2022]. Dostupné z: https://www.svetandroida.cz/na-tom-videu-jsi-ty-utok-zprava-messenger/

[33] *Eset.cz: Co je phishing?* [online]. [cit. 16.07.2022]. Dostupné z: https://www.eset.com/cz/phishing/

prostřednictvím internetového bankovnictví přesune své finance na účet útočníka, kdy se jedná o účet v bance v zahraničí, která striktně neposkytuje žádné informace ke svým bankovním účtům ani ke svým klientům. Jako adekvátní řešení proti tomuto problému je nesdělování žádných osobních informací po telefonu, případně takový hovor ihned ukončit.[34]

V případě výše uvedených metod není vyloučeno, že útočník nevyužije těchto metod zároveň s nasazením škodlivého programu do systému uživatele. V poslední době bývají kybernetické útoky sofistikovanější, kdy se útočníci především prostřednictvím elektronické a telefonické komunikace snaží vnutit škodlivý software, který si důvěřivý uživatel dobrovolně nainstaluje.

3.1.3. Počítačové viry

Definice počítačového viru vznikla na základě totožného chování škodlivého programu s biologickým virem. Stejně jako v případě biologického viru, který se snaží u živých organismů šířit se a napadat buňky v těle, také v případě počítačového viru se tento snaží šířit a napadat soubory v počítačovém systému. Počítačové viry se šíří prostřednictvím aplikací nebo dokumentů, kdy do těchto souborů je vložen zdrojový kód škodlivého softwaru, kdy po spuštění aplikace nebo otevření souboru dochází k infikování počítačového systému virem. Pro počítačové viry je specifické, že se dokážou šířit bez vědomí uživatele. Uživatel systému si zpočátku vůbec nepovšimne, že je systém napaden. Přítomnost virů se v dalších fázích může projevovat v pomalejších reakcích operačního systému na interakci uživatele. Postupně se stávají viditelné změny v nastavení sytému, mohou se objevovat grafické chyby v rozhraní systému, zvýšení hluku počítače v důsledku vyššího využívání technického vybavení počítače a tím i zvýšení chladících systémů jednotlivých součástí. Při napadení virem také dochází ke ztrátám či zašifrování dat. Některé počítačové viry se však nemusí vůbec nijak viditelně projevovat. Naopak se snaží svoji přítomnost zatajit, sledovat zařízení a zaznamenávat komunikaci uživatele, kdy tyto informace jsou dále předávány útočníkovi. Počítačové viry jsou schopny se integrovat do spouštěcí sekvence operačních systémů, kdy se tak snaží předejít kontrolám antivirových programů

[34] *Česká spořitelna a. s.: Vishing* [online]. [cit. 16.07.2022]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/vishing

tím, že spustí škodlivý kód při spouštění systému v době, než dojde ke spuštění antivirového programu.[35]

3.1.4. Počítačové červy

Podstata počítačového červa spočívá ve vyhledávání zranitelností operačních systémů, kdy těchto zranitelností se snaží využít ke vniknutí a následnému napadání souborů a šíření se. Počítačový červ se oproti viru liší tím, že není součástí žádného programu. Zdrojový kód není vložen do žádné aplikace a není vyžadováno spuštění aplikace ke spuštění škodlivého kódu. Počítačový červ se šíří samostatně bez nutnosti hostitelské aplikace prostřednictvím počítačových sítí, kdy se postupně snaží napadat jednotlivá zařízení, která jsou k síti připojena. Nejčastější formou šíření červa je e-mailová komunikace nebo internetové stránky, kdy v případě otevření obsahu e-mailové zprávy nebo otevřením internetových stránek dochází k napadení operačního systému. Stejně jako v případě viru, také při nakažení operačního systému červen může dojít ke smazání dat, k jejich zašifrování nebo k jejich zneužití. Počítačový červ je schopen se dále šířit prostřednictvím e-mailových zpráv zasílanými kontaktům, které jsou uloženy v napadeném systému. Může také využít zranitelností v operačním systému k otevření takzvaných zadních vrátek, tedy umožnit volný přístup útočníkovi k datům uživatele a k ovládání systému.[36]

3.1.5. Scareware

Škodlivost tohoto softwaru spočívá především v zastrašování uživatele. Ve většině případů je samotný scareware neškodný. Při prohlížení internetových stánek nebo při otevření obsahu e-mailu se uživateli objeví varovná zpráva, že jeho počítač je napaden a následně je odkázán ke stažení škodlivého programu. Samotné nebezpečí spočívá právě při stažení takového programu, kdy se může jednat o škodlivý software umožňující přístup útočníkovi do operačního systému a sledovat tak uživatele, případně zneužít jeho data uložená v počítači. V některých

---

[35] *Wikipedie: Otevřená encyklopedie: Počítačový virus* [online]. [cit. 16.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus&oldid=21448963

[36] *Wikipedie: Otevřená encyklopedie: Počítačový červ* [online]. [cit. 16.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv&oldid=18815487

případech se může jednat o software, který nemá žádnou funkci, pouze se snaží zastrašit uživatele. Scareware může být spojen dohromady s phishingem či vishingem. Podvodná zpráva o napadení operačního systému bývá doplněna telefonním číslem, kdy po vytočení telefonního čísla se uživatel spojí s útočníkem, který se snaží z uživatele získat citlivé údaje.[37]

3.1.6. Spyware

Spyware je škodlivý software, který sbírá uživatelské údaje, data o prohlížení internetových stránek a uživatelská hesla, kdy tyto údaje posílá tvůrci spywaru. Nejčastěji je spyware součástí aplikace, kterou si uživatel dobrovolně nainstaluje. Většinou se jedná o multimediální aplikace, které slouží ke stahování či přehrávání multimediálního obsahu většinou nelegálním způsobem. Spyware po instalaci napadne regulérní programy především internetové prohlížeče, kdy těmto změní nastavení, kdy především vypne některé zabezpečovací prvky. V nejvíce případech změní výchozí webovou stránku a vyhledávací moduly za alternativní, které slouží tvůrcům ve sbírání dat. Dále se mohou uživateli zobrazovat v grafickém prostředí další nástrojové lišty či ikony neznámých aplikací na ploše systému nebo se mohou neustále zobrazovat reklamy. Spyware se také projevuje pomalejším načítáním operačního systému a jeho pomalejšími reakcemi na interakci uživatel. Projevuje se zdlouhavým spouštěním aplikací, především internetových prohlížečů a výrazným zpomalením internetového připojení.[38]

3.1.7. Adware

Tento škodlivý software se projevuje zobrazováním reklam. Adware se do operačního systému dostane společně s aplikací, kterou si uživatel dobrovolně nainstaluje. Sám o sobě adware není přímo nebezpečný. Nesbírá ani nikam nezasílá citlivé údaje uživatele, jeho účelem je pouze zobrazování reklam za účelem generování zisku pro vývojáře aplikace, se kterou byl adware nainstalován. Nicméně tyto reklamy mohou být v některých případech velmi obtěžující a mohou značně narušovat práci uživatele. Některá adware mohou

---

[37] *Wikipedia, The Free Encyclopedia: Scareware* [online]. [cit. 17.07.2022] Dostupné z: https://en.wikipedia.org/w/index.php?title=Scareware&oldid=1102495324

[38] *Wikipedie: Otevřená encyklopedie: Spyware* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Spyware&oldid=21189528

změnit výchozí webovou stránku v internetovém prohlížeči. Sice se adware nesnaží zneužít uživatelova data ani nijak zásadním způsobem narušit řádný chod systému, ale stále se může jednat o potencionální hrozbu, která může vytvořit zranitelnost v systému.[39]

3.1.8. Trojský kůň

Pojmenován podle řecké báje, kdy se řečtí bojovníci schovali do dřevěného koně, aby dobyli Tróju zevnitř. Počítačový trojský kůň je škodlivý software, který se snaží dostat do operačního systému a převzít kontrolu zevnitř. Trojský kůň může být samostatná aplikace nebo může být do stávající aplikace přidán. Některé trojské koně si uživatel přímo instaluje dobrovolně do stávajících aplikací, kdy aplikováním trojského koně do programu se tak může vyhnout zaplacení aplikace, kdy po aplikaci trojského koně si aplikace myslí, že bylo za její užívání řádně zaplaceno. Na rozdíl od počítačového viru se trojský kůň nedokáže dále šířit svojí kopií na další zařízení v počítačové síti. Za tímto účelem bývají vytvářeni počítačoví červi, kteří mohou na napadeném zařízení trojského koně nainstalovat.[40]

3.1.9. Ransomware

Ransomware je vyděračský software. Tento druh škodlivého softwaru při napadení operačního systému v něm zašifruje data, kdy následně útočník požaduje zaplacení výkupného za dešifrování dat. Zašifrování dat probíhá za užití šifrovacího algoritmu, kdy klíč k dešifrování dat má k dispozici pouze útočník. Obnovení dat v případě sofistikovanějšího šifrovacího algoritmu je bez dešifrovacího klíče velmi obtížné, téměř nepravděpodobné. Ransomware také dokáže zablokovat přístup k operačnímu systému zašifrováním všech oddílů na disku, kdy po startu systému se uživateli pouze zpřístupní možnost uhradit výkupné pro obnovení přístupu. Ransomware se šíří prostřednictvím e-mailu a infikovaných souborů. Velmi často se šíří prostřednictvím maker v aplikacích

[39] *Wikipedie: Otevřená encyklopedie: Adware* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Adware&oldid=20917505
[40] *Wikipedie: Otevřená encyklopedie: Trojský kůň* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Trojsk%C3%BD_k%C5%AF%C5%88_(program)&oldid=21212708

kancelářských balíků. V současné době se jedná o nejnebezpečnější škodlivý software.[41]

3.1.10. Denial of service

Denial of service je druh kybernetického útoku, jehož účelem je vyřazení internetových stránek nebo služeb z provozu. Princip tohoto útoku spočívá ve vyslání velkého množství dotazů v jeden okamžik na počítačový server, na kterém jsou internetové stránky nebo služby provozovány. Počítačový server takový nápor dotazů v jeden okamžik nezvládne zpracovat, čímž dojde k výpadku serveru a znepřístupnění internetových stránek nebo služeb. Útočník k tomuto způsobu útoku využívá počítačů, které jsou napadeny škodlivým softwarem, kdy prostřednictvím tohoto softwaru zasílá dotazy z napadeného počítače na server. Uživatel počítače nemusí vůbec tušit, že jeho zařízení je zapojeno do takového útoku. Cílem tohoto typu útoku bývá většinou výpadek zařízení poskytující internetovou službu, nelze však ale vyloučit možnost, že se útočník tímto způsobem bude snažit najít zranitelná místa ke vniknutí do systému a nasazení škodlivého softwaru či získání dat.[42]

V této části kapitoly byl uveden výčet v současné době nejčastějších a nejnebezpečnějších hrozeb, na které lze v kyberprostoru narazit. Škodlivý software lze kategoricky rozdělit podle způsobu útoku, šíření a následném nedovoleném chování v operačním systému. Přesto je každý škodlivý software svým způsobem unikátní, kdy jednotlivé škodlivé programy mají svá konkrétní pojmenování, kterými je lze individuálně identifikovat. Každý z těchto škodlivých programů značí autorův rukopis. V případě složitějších škodlivých programů a sofistikovanějších útoků může docházet ke kombinaci jednotlivých kategorií, čímž se potenciální hrozba zvyšuje.

3.2. Kybernetické útoky na zdravotnická zařízení

Zdravotnická zařízení jsou v současnosti plně závislá na počítačové infrastruktuře. Veškeré lékařské operace, skladové hospodářství lékařských

[41] *Wikipedie: Otevřená encyklopedie: Ransomware* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Ransomware&oldid=21367664
[42] *Wikipedie: Otevřená encyklopedie: Denial of service* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Denial_of_service&oldid=21395675

potřeb a léků, databáze pacientů včetně jejich lékařských anamnéz jsou digitálně zpracovávány a ukládány na tato zařízení. Závislost na počítačové infrastruktuře znamená riziko, které může mít zásadní dopad na životy pacientů v případě vyřazení této infrastruktury z provozu. Počet kybernetických útoků na zdravotnická zařízení v současné době začíná narůstat, kdy některé z těchto útoků byly natolik úspěšné, že byly schopny vyřadit počítačovou infrastrukturu nemocnic i na několik týdnů a způsobit závratné škody na majetku v hodnotách milionů korun a ohrozit životy mnoha pacientů.[43]

V prosinci roku 2019 došlo ke kybernetickému útoku na Nemocnici Rudolfa a Stefanie v Benešově. Jednalo se o škodlivý program ransomware, který byl součástí makra v elektronickém dokumentu kancelářského balíku Microsoft Office, který byl přílohou phishingového e-mailu. Makra v kancelářských balících usnadňují práci s dokumenty při výpočtech, úpravách textu apod. Jedná se o regulérní funkci, kterou útočník zneužívá pro implementaci a šíření škodlivého softwaru. Po stažení a následnému otevření dokumentu, uživatel povolil spouštění maker, kdy tímto povolením se spustil škodlivý kód, který umožnil stažení trojského koně Emotet do počítačového systému. Trojský kůň Emotet je schopen rozšiřovat své schopnosti pomocí škodlivých modulů, které jsou do něj nahrávány. Emotet následně nainstaloval škodlivý software Trickbot, který následně zavedl do systému ransomware Ryuk, který zašifroval data s požadavkem na výkupné za dešifrování dat a obnovení přístupu do systému. Tento kyberútok způsobil nemocnici škodu ve výši 59 milionů korun a k plnému provozu počítačové sítě došlo až po necelých třech týdnech. Naštěstí nedošlo k ohrožení pacientů ani k žádnému úniku dat.[44]

V lednu roku 2020 byl proveden kybernetický útok na Nemocnici následné péče v Horažďovicích. Za tímto útokem stál ransomware Buran. Tento ransomware se šíří phishingem skrze podvodné e-mailové zprávy nebo prostřednictvím vzdáleného přístupu do počítačového systému nebo skrze

---

[43] *Idnes.cz: Nemocnice jsou pro hackery stále snadným cílem. Útoků přitom přibývá* [online]. [cit. 21.07.2022] Dostupné z: https://www.idnes.cz/zpravy/domaci/kyberneticky-utok-hacker-nemocnice-zabezpeceni.A210203_141638_domaci_knn

[44] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 22.07.22]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

zranitelnosti zastaralého a v současné době již nevyvíjeného prohlížeče Internet Explorer. Po vniknutí do operačního systému je schopen se usadit v registrech operačního systému Windows, dále je schopen získat oprávnění na úrovni administrátora, kdy s oprávněním na této úrovni je schopen vymazat veškeré zálohy a body obnovení systému. Nakonec zašifruje veškerá data, kdy dešifrovací klíč odešle na server útočníka, který následně začne požadovat výkupné za dešifrování. Tímto kybernetickým útokem byla napadena část počítačové infrastruktury uvedeného nemocničního zařízení, kdy došlo ke zneužití a ztrátě některých dat. Škoda byla vyčíslena na 150 tisíc korun. K plné obnově počítačové infrastruktury došlo po týdnu.[45]

V březnu roku 2020 byla kybernetickým útokem zasažena počítačová síť Fakultní nemocnice v Brně. Opět se jednalo o ransomware, který byl součástí dokumentu kancelářského balíku Microsoft Office. V tomto případě útočník zneužil funkci propojování a vkládání objektů (OLE). Tato funkce umožňuje propojování dat mezi dokumenty a aplikacemi. Infikovaný dokument byl přílohou e-mailové konverzace, kdy v příloze byl označen jako lékařské zprávy pacientů. Po stažení a spuštění dokumentu došlo k napadení systému ransomwarem Defray777, který způsobil zašifrování dat na lokálních i síťových úložištích. Tento kybernetický útok ochromil nemocnici natolik, že byla přerušena většina operací a akutní pacienti museli být převezeni do okolních nemocnic. Nemocnice přišla o spoustu důležitých dat a dokumentů a trvalo jí více než rok, než byl systém obnoven do plného provozu. Škoda byla vyčíslena na stovky milionů korun.[46]

Ke konci března roku 2020 se stala obětí kybernetického útoku Psychiatrická léčebna v Kosmonosech. V tomto případě se jednalo o ransomware Dewar. Tento ransomware se podobně jako v předchozích případech šíří prostřednictvím e-mailové komunikace, kdy je součástí příloh obsahující soubory kancelářského balíku Microsoft Office, dokumentů ve formátech pdf, archivních souborů nebo může být součástí spustitelných souborů. Po infikování systémů došlo opět k zašifrování dat se žádostí o výkupné za dešifrování. Došlo tak ke ztrátě některých dat a záloh zdravotnického zařízení, kdy plné obnovení všech

[45] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 22.07.22]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

[46] Tamtéž

systémů trvalo přibližně měsíc. K ohrožení pacientů nedošlo, léčebna měla lékařské údaje o pacientech evidované také v papírové podobě.[47]

Cíl útoku	Datum zjištění	Malware	Dopad na infrastrukturu	Způsobená škoda
Nemocnice Rudolfa a Stefanie v Benešově (444 lůžek)	11. 12. 2019	Emotet TrickBot Ryuk	Ztráta kontroly nad systémem, nefunkčnost IT služeb	59 milionů korun
Nemocnice následné péče v Horažďovicích (140 lůžek)	Leden 2020	Buran	Zneužití a ztráta některých dat	150 tisíc korun
Fakultní nemocnice v Brně (1889 lůžek)	12. 3. 2020	Defray777	Ztráta kontroly nad systémem, nepřístupná data pacientů	Stovky milionů korun
Psychiatrická léčebna v Kosmonosech (600 lůžek)	27. 3. 2020	Dewar	Zašifrování a ztráta dat	Není známo

Tabulka č. 2 - Souhrnný přehled úspěšných útoků na zdravotnická zařízení[48]

Zhodnocením všech uvedených útoků na zdravotnická zařízení zjišťujeme stejný či podobný postup, kterým útočník pronikne do počítačové infrastruktury těchto zařízení. Prostřednictvím e-mailové komunikace rozesílá podvodné zprávy, ve kterých se nachází dokumenty kancelářského balíku Microsoft Office. Uvnitř těchto dokumentů jsou vložena makra, která obsahují škodlivý kód, kdy po otevření těchto dokumentů a aktivaci maker dojde ke spuštění škodlivého kódu, který následně stáhne vyděračský malware ransomware do systému, který se postupně rozšíří počítačovou sítí do dalších zařízení, ve kterých zašifruje veškerá

[47] *Aktuálně.cz.: Další kybernetický útok za nouzového stavu: Hackeři napadli psychiatrickou nemocnici* [online]. [cit. 22.07.2022]. Dostupné z: https://zpravy.aktualne.cz/domaci/kosmonosy-utok-koronavirus/r~188929ec732511ea9d74ac1f6b220ee8/

[48] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 22.07.22]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

data a omezí přístup do těchto systémů s následnou žádostí o zaplacení výkupného. Nemocnice se v tu chvíli stávají ochromeny a nemohou vykonávat svoji lékařskou činnost nebo je tato činnost výrazně omezena, čímž mohou být pacienti vystaveni ve vážné ohrožení života. Zároveň tím vzniká škoda v milionech korun, kdy tyto částky by jinak mohly být použity na modernizaci a nákup nového lékařského vybavení.[49]

Obrázek č. 4 - Snímek dialogového okna ransomware požadující výkupné[50]

Na obrázku č. 4 je znázorněn snímek dialogového okna z počítačového systému, který byl infikován vyděračským malwarem WannaCry. Tento malware v roce 2017 infikoval počítače po celém světě, kdy se jedná o neznámější ransomware.[51] Na snímku je vidět upozornění, že důležitá osobní data uživatele byla zašifrována, kdy dále jsou uvedeny pokyny pro provedení platby, pokud si uživatel přeje svá data získat zpět. V levé části se nachází časomíra, kdy ve

[49] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 22.07.22]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

[50] *Wikipedia, The Free Encyclopedia: WannaCry ransomware attack* [online]. [cit. 22.07.2022] Dostupné z: https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&oldid=1106987274

[51] Tamtéž

vyděračském textu je upozornění, že v případě nezaplacení požadované částky do tří dnů, dojde k její navýšení a v případě neuhrazení výkupného do sedmi dnů, přijde uživatel o všechna data. Zobrazená časomíra může mít v mnoha případech značný psychologický efekt na poškozeného, který z obavy ze ztráty dat částku raději uhradí. Není ovšem nijak zaručeno, že po uhrazení částky dojde ke zpřístupnění zašifrovaných dat. V žádném případě nelze doporučit výkupné zaplatit. Ve spodní části dialogového okna se nachází odkaz pro zaplacení výkupného ve formě virtuální měny Bitcoin. Virtuální měna bývá kybernetickými útočníky nejčastěji využívána, neboť se jedná o měnu, nad kterou nedohlíží žádná banka či jiná instituce. Útočníkovi tak tento druh měny poskytuje značnou anonymitu a lze tento druh měny vyměnit za reálné peníze. Je však stále nutno podotknout, že jedním z hlavních důvodů vytvoření virtuální měny byla ochrana osobních údajů osob při provádění plateb v kyberprostoru. Ačkoliv bývá virtuální měna využívána kybernetickými útočníky, stále se jedná o legální měnu, která je využívána při mnoha legálních obchodních transakcích.[52]

3.3. Opatření při kybernetickém útoku

Při kybernetickém útoku jednou z prvních věcí, které je třeba se vyvarovat je jakékoliv placení výkupného nebo jakkoliv se pokoušet navazovat kontakt s útočníkem. Stejně jako u klasického způsobu vydírání i zde je velmi malá pravděpodobnost, že by útočník po zaplacení zpřístupnil napadená data. Je mnohem větší pravděpodobnost, že by požadoval další výkupné anebo by jakoukoliv žádost o zpřístupnění dat ignoroval. Pokud se již daná organizace stala obětí kybernetického útoku, je třeba podniknout kroky k zabránění vzniku dalších škod, a to zejména zastavením šíření útoku a postupně obnovit systémy do funkčního stavu.

V případě napadení počítačového systému nebo vniknutí útočníka do počítačové sítě je v prvním případě nejdůležitější přerušit jakoukoliv komunikaci infikovaného zařízení s dalšími zařízeními v síti, zejména se servery, na kterých jsou ukládány zálohy. Nejrychlejší cestou je odpojením zařízení od počítačové sítě vyjmutím síťového kabelu nebo odpojením bezdrátového modulu. Zašifrovaná

[52] *Wikipedie: Otevřená encyklopedie: Bitcoin* [online]. [cit. 22.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Bitcoin&oldid=21588971

data přesunout z napadeného počítače na externí médium. Stále existuje pravděpodobnost, že data půjdou obnovit. Jakoukoliv komunikaci mezi dalšími zařízeními v síti zakázat nebo ji povolit jen na to nejnutnější minimum a na nejméně nutnou dobu.[53]

Dále je nutno zakázat přístup do sítě Internet všem dalším zařízením, aby došlo k zamezení odesílání interních dat k útočníkovi nebo k dalšímu pronikávání škodlivého kódu do počítačové sítě. Přístup do sítě Internet povolit nejnutnějším zařízením a opět jen na nezbytně nutnou dobu. Dále je třeba oddělit síť s lékařskými přístroji od zbytku počítačové sítě. Některé specializované přístroje vyžadují internetové připojení, zároveň však mohou být neaktualizované, zastaralé a tím pádem zranitelné. Doporučuje se tyto přístroje oddělit do samostatných sítí a komunikaci s jinými zařízení omezit jen na nejnutnější případy.

Jedním z dalších kroků je změna hesel uživatelských účtů s administrátorskými právy. Škodlivý software může při svém šíření zachytit heslo k takovému účtu, kdy útočník s administrátorskými právy může obejít některá bezpečnostní opatření a získat tak neomezený přístup k citlivým datům a aplikacím, případně převzít plnou kontrolu nad počítačovým systémem.

Zálohy přesunout na off-line média, např. externí disky a provést jejich kontrolu. Záloha přesunutá na off-line médium je tak chráněna proti šíření nakažlivého softwaru či zneužití ze strany útočníka. Je důležité, aby kritická data byla vždy zálohována na off-line médiích.

Upozornit zaměstnance na riziko napadení počítačové sítě a na nebezpečí plynoucí z phisingu a vishingu a na koho se mají případně obrátit. Může nastat situace, kdy útočník se bude snažit kontaktovat zaměstnance, kdy se bude vydávat za správce počítačové sítě a bude se snažit získat další citlivé údaje. Upozorněním lze zvýšit ostražitost zaměstnanců, kdy je také potřeba je srozumět, jakým způsobem během mimořádné situace mají postupovat a kterým činnostem se mají vyvarovat.

Zakázat používání maker v kancelářském balíku Microsoft Office. Používání maker lze zakázat v nastavení kancelářského balíku. Ke konfiguraci

---

[53] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 26.07.22]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

nastavení slouží aplikace Nástroj pro přizpůsobení Office, kdy za pomocí této aplikace lze měnit nastavení kancelářského balíku plošně na všech počítačích.

Nemazat data na infikovaných zařízeních. Počítačový systém si vede záznamy o svých činnostech a činnostech aplikací, kdy tyto záznamy jsou ukládány do tzv. „logů". V těchto logách jsou užitečné informace jako rozsah IP[54] adres, časové údaje, uživatelské údaje aj., kdy tyto informace jsou užitečné pro další vyšetřování ke způsobu útoku a rozsahu napadení.[55]

Zkontrolovat segmentaci počítačové sítě a komunikaci mezi jednotlivými segmenty. Na segmentované počítačové síti s řízenou komunikací mezi segmenty lze zabránit dalšímu šíření nakažlivého softwaru.[56]

Zvýšit ochranu operačního systému zpřísněním bezpečnostního nastavení zakázáním spouštění nepovolených aplikací a spouštění neznámých příkazových skriptů. Operační systém Microsoft Windows disponuje takzvanými zásadami skupin (angl. „Group Policy")[57], kdy se jedná o nástroj pro hromadnou konfiguraci skupiny uživatelů a počítačových systémů s operačním systémem Windows. Tento nástroj umožňuje nastavovat druh oprávnění konkrétním uživatelům či konkrétní skupině uživatelů a dále povolení přístupu konkrétním aplikacím.

Mít vytvořený plán pro řízení činností organizace pro zajištění klíčových systémů při krizové situaci. [58] Takto vytvořený plán pomáhá vybudovat obranyschopnost při napadení, předvídat takovou situaci a mít připravené řešení při mimořádné události. Především by takovýto plán měl zahrnovat náhradní řešení během výpadku klíčových systémů, tak aby byla zaručena alespoň základní úroveň poskytovaných služeb. Nesmí se stát, aby výpadek počítačového systému zabránil přijmutí či léčbě pacienta.

Provést sken zranitelností v systémech, které jsou přístupné zvnějšku mimo organizaci. Sken zranitelností je automatizovaný proces, který se snaží najít

---

[54] Internet Protocol

[55] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 26.07.22]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

[56] *Techopedie: Co je to segmentace sítě* [online]. [cit. 26.07.22]. Dostupné z: https://cs.theastrologypage.com/network-segmentation

[57] *TechTarget: What is Group Policy?* [online]. [cit. 26.07.2022] Dostupné z: https://www.techtarget.com/searchwindowsserver/definition/Group-Policy

[58] *Wikipedie: Otevřená encyklopedie: Business Continuity Management* [online]. [cit. 26.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Business_Continuity_Management&oldid=19436136

slabá místa v sytému, která by mohla být zneužita ke kybernetickému útoku. Díky tomuto procesu lze odhalit nadbytečné procesy, které využívají přístupu k internetu, chyby v konfiguracích a zda jsou systémy aktualizované a neobsahují žádné zranitelnosti.[59]

Pokud se podařilo lokalizovat hrozbu, zabránit jejímu dalšímu šíření a odstranit zranitelná místa, následuje fáze obnovení systémů do původního funkčního stavu. Zcela nejjednodušším a nejefektivnějším způsobem je přeinstalace operačního systému s obnovením dat ze zálohy. Při nové instalaci operačního systémů dochází k formátování pevného disku, kdy při tomto procesu jsou vymazána veškerá data. Tento proces tak odstraní veškeré škodlivé soubory, které se na disku nachází. Jedná se nejbezpečnější způsob, jak se zbavit škodlivého softwaru. Díky obnově dat ze zálohy tak během procesu instalace dojde k nainstalování potřebných aplikací a ke konfiguraci nastavení systému, aby dané zařízení mohlo být opětovně nasazeno do pracovního prostředí. Právě v této fázi se projeví důležitost záloh, neboť řádně zálohovaná data tento proces výrazně usnadní a urychlí. Celková doba obnovení systémů od počátku kybernetického útoku do jeho odstranění se může značně lišit. Záleží na velikosti počítačové sítě a rozsahu rozšíření škodlivého softwaru. Plné obnovení tak může trvat od několika hodin až po několik týdnů. Jak je uvedeno v tabulce č. 2 finanční ztráty mohou být v jednotkách až stovkách milionů korun.

3.4. Bezpečnostní pravidla

Při budování kybernetické infrastruktury a její obsluze je třeba dbát základních bezpečnostních pravidel, které se týkají zabezpečení této infrastruktury před nedovoleným vniknutím. Stejně jako v případě budování klasické infrastruktury, také v kybernetické infrastruktuře je nutno stanovit základní pravidla pro ochranu informačních systémů a co nejefektivnější eliminaci hrozeb při jejich napadení. V přechozí kapitole byly uvedeny kroky vedoucí k odstranění škod vzniklých při napadení počítačového systému kybernetickým útokem. Tato část práce se bude zabývat bezpečnostními pravidly, které se snaží takovému útoku zabránit nebo mu předejít.

---

[59] *TEMPEST a.s.: Vulnerability Scanning* [online]. [cit. 26.07.2022]. Dostupné z: https://www.tempest.sk/skenovani-zranitelnosti-5e4.html

Analyzováním údajů z kybernetických útoků na zdravotnická zařízení v České republice lze vyvodit závěr, že jedním z nejslabších míst počítačového systému je samotný uživatel. Ve všech případech se ransomware dostal do počítačové sítě prostřednictvím souboru kancelářského balíku Microsoft Office, kde škodlivý kód byl uložen v makru, který následně otevřením souboru a spuštěním makra uživatel aktivoval. Právě neznalost a neinformovanost uživatele může vést k úspěšnému kybernetickému útoku, proto nejčastěji útočník cílí přímo na uživatele. K většímu zabezpečení počítačové sítě v první řadě patří vzdělávání zaměstnanců o kybernetické bezpečnosti, o hrozbách a jak se jim vyvarovat. Nelze ani opomenout ochranu osobních údajů a vyvarovat se jakémukoliv sdělování citlivých údajů, zejména přístupových jmen a hesel. Pravidelné školení zaměstnanců zvýší povědomí o kybernetických hrozbách a tím pádem přispěje k větší kybernetické bezpečnosti. Školení by se mělo také vztahovat na správce počítačové sítě ke zjišťování nových informací, nových technologií, nových hrozeb za účelem prohlubování kvalifikace a zvýšení obranyschopnosti při odstraňování nově objevených zranitelností.[60]

Dalším velmi významným zabezpečením je segmentace počítačové sítě. Segmentace umožňuje rozdělit počítačovou síť do menších segmentů takzvaných podsítí, kdy v každé podsíti lze nastavit přístupová oprávnění do daného segmentu či možnost regulovat komunikaci mezi segmenty. Segmentace sítě zabraňuje dalšímu šíření kybernetického útoku, kdy díky rozdělení sítě a regulaci komunikace lze útok limitovat a uzavřít jej pouze na jednom segmentu a ochránit tak zbylé další části. Počítačovou síť lze segmentovat podle pracovních oddělení například účetní oddělení, personální oddělení apod. Do samotného segmentu lze zvlášť připojit některá lékařská zařízení, která mnohdy bývají softwarově zastaralá a plná zranitelností. Bez segmentace se může útočník při vniknutí pohybovat bez omezení po celé síťové infrastruktuře.[61]

Dále do bezpečné sítě patří regulace uživatelských účtů. Moderní operační systémy umožňují regulovat oprávnění jednotlivých uživatelů či skupin uživatelů. V zásadě lze uživatele rozdělit do dvou skupin. Tou první skupinou je běžný

---

[60] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 26.07.2022]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

[61] Tamtéž

uživatelský účet. Jedná se o účet s omezeným přístupem, kdy takovýto uživatel má pouze omezená práva, nutná jen k výkonu své činnosti. Takovýto účet nemůže zasahovat zásadním způsobem do konfigurace operačního systému, nemůže instalovat žádné aplikace a v rámci počítačové sítě může vstoupit jen do těch částí systému, kam má povolen přístup. Uživatel má k výkonu své činnosti již přednastavené prostředí včetně aplikací, které pro svoji činnost potřebuje. Tímto způsobem lze zabránit jakémukoliv neodbornému zásahu do operačního systému či počítačové sítě. Druhou skupinou uživatelských účtů jsou účty s administrátorskými právy, který používají výhradně správci počítačové sítě. Jedná se o privilegovaný účet, který může mít přístup ke všem počítačovým systémům, sítím a datům. Privilegované účty lze také regulovat, kdy i takovýto účet může mít omezen přístup do některých částí sítě či datům. Tento typ účtu by měl používat pouze odborník a obecně platí zásada používat takovýto účet jen po dobu nezbytně nutnou, pouze k provedení dané operace. Kompromitování administrátorského účtu může mít velký dopad na všechny systémy v celé organizaci. Doporučuje se pravidelně měnit hesla u všech uživatelských účtů. K vyššímu zabezpečení lze využít dvoufázového ověření při přihlašování uživatele, kdy se uživatel přihlásí do systému pomocí přístupového jména a hesla a dále svou identitu potvrdí například kódem, který mu je během přihlášení zaslán na mobilní telefon. Tento způsob přihlašování by měl být využíván u privilegovaných účtů, především u těch, které mají přístup k zálohám.[62]

Jedním z nejvýznamnějších prvků bezpečné sítě je zálohování. Zálohy dat obsahují vždy citlivé údaje a důležité informace dané organizace a jedná se o jeden z hlavních cílů útočníka. Kompromitování záloh má nejzávažnější dopad, je tedy velmi důležité při zálohování dodržovat doporučená bezpečnostní opatření pro vytváření záloh. Doporučuje se při zálohování dodržovat pravidlo 3 – 2 – 1, tedy mít alespoň tři kopie na dvou různých zařízení, kdy jedno zálohovací médium by se mělo nacházet mimo organizaci. Mít jednu nebo více záloh na off-line úložišti. Zálohování má být pravidelné, jejich funkčnost by měla být pravidelně

[62] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 27.07.2022]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

kontrolována a testována. Dalším doporučením je pro přístup k zálohám mít zvlášť vytvořený administrátorský účet, který bude sloužit jen pro účely zálohování.[63]

Pravidelná aktualizace operačního systému je bezesporu dalším prvkem bezpečné sítě. Aktualizace přinášejí do systému řadu nových funkcí a obsahují bezpečnostní záplaty, které opravují zranitelnosti. Aktualizovány by měly být také nainstalované aplikace, především ty, které vyžadují přístup k internetu. Vyvarovat se užívání zastaralých a nepodporovaných operačních systémů. Takovéto systémy po ukončení vývoje nedostávají žádné bezpečnostní záplaty. Často se stává, že takovéto systémy bývají nadále využívány. Důvod bývá spojován s nákupem licence novější verze operačního systému, kdy s tímto bývá spojen také nákup nového hardwaru, kdy starý hardware již nemá výkon potřebný pro plynulý chod nové verze operačního systému. Dalším důvodem může být nekompatibilita nové verze s některým zařízením nebo s některým softwarem. Pokud je přesun na novou verzi operačního systému spojen s finanční náročností, lze se poohlédnout po některých alternativních operačních systémech, které jsou k dispozici volně ke stažení zdarma. Pokud však není možné zastaralý systém nahradit, je nutno takovéto zařízení umístit do oddělené počítačové sítě a komunikaci s tímto zařízením omezit na nezbytné minimum.[64]

Dalším bodem do bezpečnosti patří antivirové programy. Antivirový software obsahuje databázi virů, kdy při své činnosti prohledává soubory v počítači a porovnává nalezené výsledky s virovou databází. Moderní antivirové programy jsou schopny také detekovat podezřelou aktivitu, kdy analyzují podezřelé chování programu za účelem zjištění, zda se jedná o hrozbu či nikoliv. Antivirový program běží neustále na pozadí systému, kdy ve většině případů svou činností nijak neruší uživatele při práci. Při své činnosti kontroluje běžící procesy, soubory na úložištích, soubory stahované do počítače z internetu a také kontroluje

---

[63] *NÚKIB: Ransomware: doporučení pro mitigaci, prevenci a reakci* [online]. [cit. 27.07.2022]. Dostupné z: https://www.nukib.cz/download/publikace/navody/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf

[64] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 27.07.2022]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

připojená externí zařízení (např. USB disky). Pro svoji činnost musí být antivirový program pravidelně aktualizován, aby virová databáze byla vždy aktuální.[65]

Pro monitoring komunikace v počítačové síti slouží bezpečnostní brána firewall. Brána firewall umožňuje hlídat komunikační provoz jak zvenčí, tak i uvnitř počítačové sítě. Umožňuje oddělit od sebe počítačové sítě a stanovuje pravidla pro komunikaci mezi nimi na základě nadefinovaných pravidel. Brány firewall jsou schopny detekovat útoky, kdy podobně jako v případě antivirů analyzují příchozí spojení a v případě zjištění pokusu o neoprávněné vniknutí se snaží útok zablokovat. Firewall řídí komunikaci oběma směry, tedy příchozí i odchozí komunikaci. Rozlišujeme dva typy firewallů. Prvním typem je síťový firewall, kdy se jedná o samostatné technické řešení a slouží jako první flitr pro příchozí komunikaci. Druhým typem je personální firewall, který je nainstalován na koncových počítačích. Také bezpečnostní brána firewall musí být pravidelně aktualizována.[66]

Provádět pravidelnou kontrolu počítačové sítě, monitoring komunikací, kontrolu aplikací, které mají přístup k internetu. Zejména se zaměřit na služby, které jsou otevřené do veřejných sítí. Jedná se především o služby pro vzdálený přístup, které slouží administrátorům pro správu počítačové sítě na dálku, kdy tímto způsobem lze ušetřit čas a pohonné hmoty, než by se musel správce počítačové sítě dostavit na místo osobně. Na druhou stranu právě prostřednictvím těchto služeb se snaží útočník vniknout do organizace. Proto je doporučováno ponechat spuštěné jen služby potřebné pro chod organizace a zbylé nepotřebné služby vypnout. Dále je třeba vést dokumentaci sítě a kontrolovat aktuálnost všech síťových zařízení. Zastaralá a neaktualizovaná síťová zařízení představují další bezpečnostní riziko.[67]

V případě výpadku počítačové sítě ať už v důsledku kybernetického útoku či jiného incidentu je nutno mít vypracovaný náhradní krizový plán. Takovýto plán by měl zahrnovat postupy v případě výpadků počítačových systémů, náhradní

---

[65] *Wikipedie: Otevřená encyklopedie: Antivirový program* [online]. [cit. 27.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Antivirov%C3%BD_program&oldid=20781273

[66] *Wikipedie: Otevřená encyklopedie: Firewall* [online]. [cit. 27.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Firewall&oldid=19597290

[67] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 27.07.2022]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

způsoby komunikace a předávání informací a jejich zaznamenávání. Nelze, než doporučit mít v takových případech připraveny v papírové podobě tiskopisy a formuláře, které by reflektovaly elektronickou podobu a mohly tak dočasně nahradit elektronickou evidenci. Mít v záloze náhradní počítačová zařízení, která by měla být přednastavená a především aktualizovaná, aby mohla v co nejkratší době nahradit infikovaná či poškozená zařízení. Plán by měl také zahrnovat krizový management, tedy proškolené pracovníky pro řízení organizace při krizové situaci. Měl by obsahovat kontakt na tyto pracovníky a definovat postup pro řešení krizové události. Organizace by si měla určit důležitost svých dat a systémů a v případě výpadku si určit, která data a systémy by měly být obnoveny jako první.[68]

[68] *NÚKIB: Ransomware: doporučení pro mitigaci, prevenci a reakci* [online]. [cit. 27.07.2022]. Dostupné z: https://www.nukib.cz/download/publikace/navody/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf

4. Makra v elektronických dokumentech

Jak již bylo uvedeno v předchozí kapitole této práce, makra jsou oficiální funkcionalitou obsažená v aplikacích kancelářských balíků, která umožňují automatizovat různé procesy při práci v těchto aplikacích. Jako příklad využití maker lze uvést zpracování přijatých dat, následné vypracování grafů a rozeslání výsledků prostřednictvím e-mailového klienta dalším osobám bez nutnosti jakýchkoliv manuálních úprav a zásahů ze strany uživatele. V rámci této práce se autor zaměřil na kancelářský balík Microsoft Office, který společně s platformou Microsoft Windows patří mezi nejrozšířenějších software na osobních počítačích po celém světě.

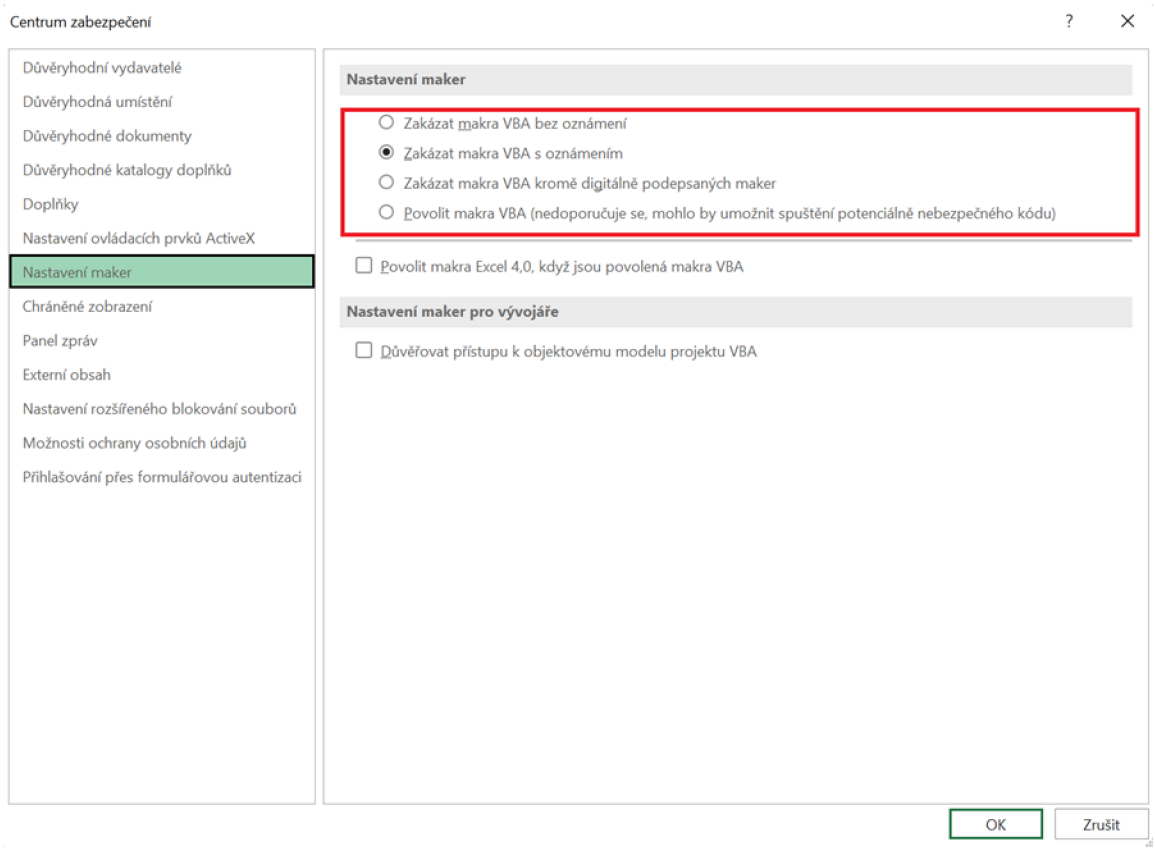
Poprvé se makra objevila v roce 1992 v tehdejším tabulkovém procesoru Excel 4.0 vyvinutém společností Microsoft pro tehdejší operační systémy Windows 3.0 a Windows 3.1. V tehdejší verzi aplikace Excel se soubory obsahující makra označovaly jako XLM soubory, čímž se tento typ maker nazývá XLM makra. V následující verzi Excel 5.0 byla XLM makra nahrazena makry vytvořenými v modernějším programovacím jazyku Virtual Basic for Applications (zkráceně „VBA“), který je používán dodnes. Zatímco XLM makra fungují jen v aplikacích Excel, makra vytvořená ve VBA fungují ve všech aplikacích sady Microsoft Office. Současná VBA makra nabízejí mnohem více funkcí oproti původním XLM makrům. Stále však XLM makra nabízejí mnoho funkcí, které jim umožňují přístup do rozhraní současných verzí Windows.[69]

4.1. Povolování VBA maker

Kancelářský balík Microsoft Office nabízí několik možností pro povolování spouštění VBA maker v jednotlivých aplikací. Povolování spouštění maker se nachází v nastavení dané aplikace v sekci Centrum zabezpečení (viz obrázek č. 5). Povolit či zakázat spouštění maker lze nastavit pro každou aplikaci kancelářského balíku zvlášť. Při nastavování uživatelských oprávnění lze určit, kteří uživatelé mohou mít oprávnění ke změnám v Centru zabezpečení. Při nastavování spouštění maker je třeba především určit, zda uživatelé využívají

[69] *Outflank: Old school: evil Excel 4.0 macros (XLM)* [online]. [cit. 15.08.2022] Dostupné z: https://outflank.nl/blog/2018/10/06/old-school-evil-excel-4-0-macros-xlm/

dokumenty s makry ke své činnosti a pokud ano, tak ve kterých konkrétních aplikacích je využívají. Podle toho, kteří uživatelé, v kterých konkrétních aplikacích makra využívají, pak nastavení provést. Na obrázku č. 5 je zobrazen výčet některých možností pro nastavení maker. V tomto případě se jedná o nastavení maker v aplikaci Excel kancelářského balíku Microsoft Office 365.[70]

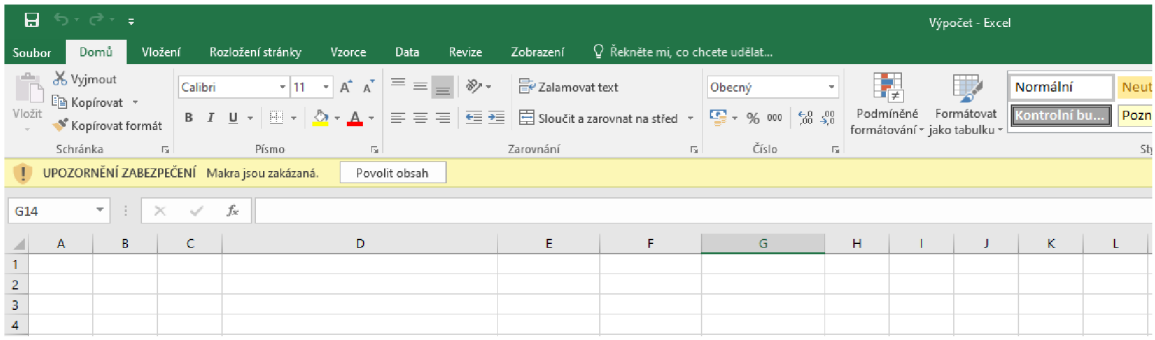


Obrázek č. 5 - Nastavení VBA maker

První z možností vyobrazených na obrázku č. 5 zakáže makra úplně, kdy při otevření dokumentu se zobrazí informační lišta s upozorněním, že dokument obsahuje makra bez možnosti povolit spouštění maker. Tuto možnost lze nastavit pro uživatele, které makra vůbec nepoužívají. Tím lze jednoznačně snížit riziko, že uživatel neznalý práce s makry nespustí škodlivý kód, který by se mohl nacházet v podvrženém dokumentu.[71]

[70] *Microsoft.com: Macros in Office files* [online]. [cit. 15.08.2022] Dostupné z: https://support.microsoft.com/en-us/office/macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6
[71] Tamtéž

Druhá možnost bývá výchozím nastavením, při kterém je spouštění maker zakázáno s oznámením. Při otevření dokumentu obsahující makra se zobrazí lišta s upozorněním na přítomnost maker a s nabídkou pro povolení spouštění maker (viz obrázek č. 6). Při tomto nastavení je dokument otevřen ve chráněném režimu, při kterém nedojde ke spuštění maker, dokud to uživatel sám nepovolí. V tomto případě je na každém uživateli, jestli povolí spuštění maker či nikoliv. Jak ukázala samotná praxe, toto nastavení je rizikové. Uživatel může jednoduše spustit škodlivý kód, který se může v makru nacházet. Tuto možnost lze doporučit pouze pro zkušené uživatele, kteří pracují s makry pravidelně a při práci s dokumenty zasílanými pouze od důvěryhodných osob.[72]



Obrázek č. 6 - Lišta s upozorněním na přítomnost maker

Třetí možnost povoluje pouze spouštění digitálně podepsaných maker. Při tomto nastavení se spustí pouze makra digitálně podepsaná důvěryhodným vydavatelem. U maker digitálně podepsanými nedůvěryhodným vydavatelem bude uživatel upozorněn, kdy makra se spustí pouze na povolení uživatele podobně jako v případě zákazu maker s oznámením. Makra bez digitálního podpisu se nespustí. Digitální podpis potvrzuje, od koho dokument s makry pochází a také, že v makrech nedošlo k žádným změnám. Při jakékoliv změně je nutno dokument znovu digitálně podepsat. Tím je zaručeno, že se souborem nikdo další nemanipuloval.[73]

Poslední možnost nedoporučuje ani samotný vydavatel softwaru. Automatické spouštění maker bez jakékoliv bezpečnostní regulace znamená

[72] *Microsoft.com: Macros in Office files* [online]. [cit. 15.08.2022] Dostupné z: https://support.microsoft.com/en-us/office/macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6
[73] Tamtéž

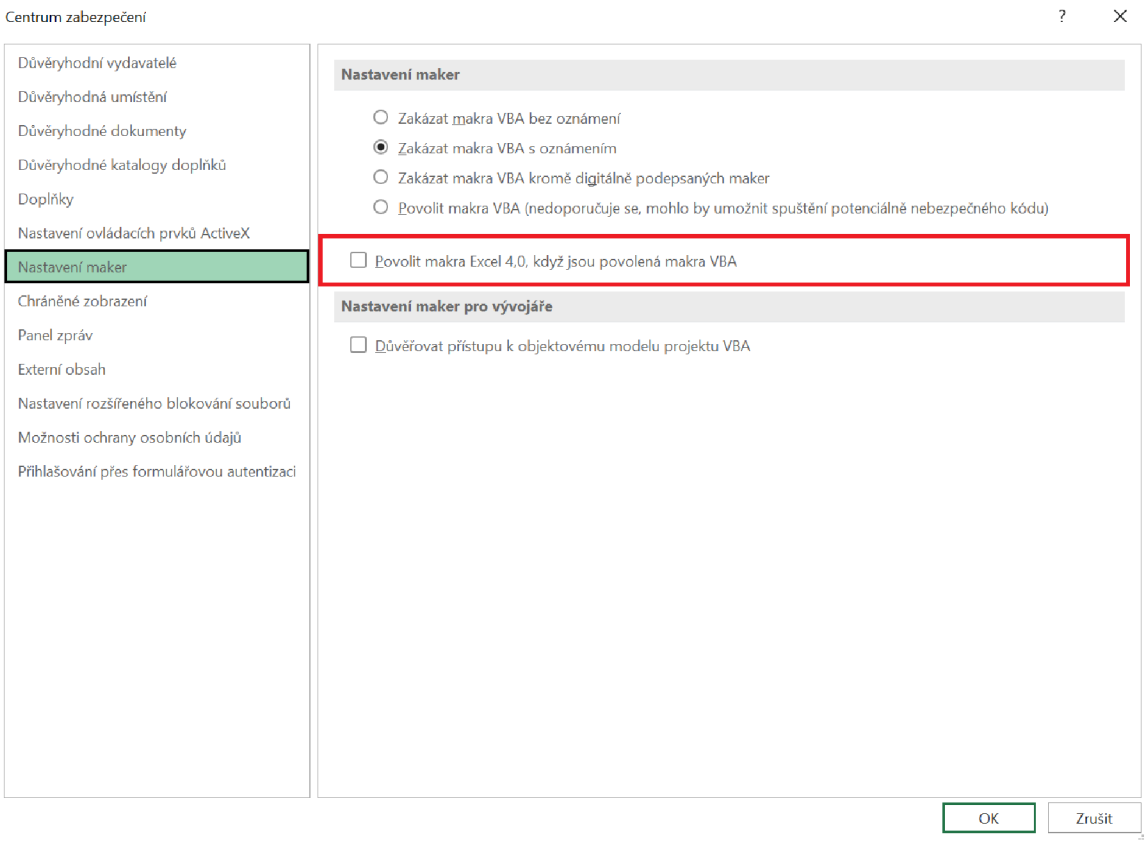
velmi vysoké riziko kybernetického útoku. Tuto možnost lze doporučit jen při práci s makry vytvořenými v dokumentech, které jsou posílány mezi uživateli v uzavřené vnitřní počítačové síti bez vnějšího přístupu.[74]

4.2. Povolování XLM maker

Ačkoliv jsou XLM makra dnes považována za zastaralou technologii, stále je lze díky zpětné kompatibilitě vytvářet a spouštět v současné verzi aplikace Excel. XLM makra mají velmi mnoho funkcí, díky kterým lze vytvářet a spouštět procesy také v současných verzích operačního sytému Windows. Tento zastaralý typ maker představuje v současné době větší bezpečnostní riziko oproti moderním VBA makrům. Jedním z důvodů je masivní rozšířením VBA maker, kdy XLM makra jsou dnes používána velmi minimálně, díky čemuž se moderní bezpečnostní systémy zaměřují především na kontrolu VBA maker. Všechna vytvořená makra jsou uložena v souboru dané aplikace. Způsob, kterým se XLM makra ukládají v souboru aplikace, je odlišný od způsobu ukládání VBA maker. Právě tento odlišný způsob ukládání způsobuje, že XLM makra se hůře analyzují moderním bezpečnostním systémům, čímž se z tohoto druhu maker stává zajímavý způsob pro šíření škodlivého kódu. V současných verzích kancelářského balíku Microsoft Office je tento druh maker zakázán a jejich spouštění vyžaduje zvláštní povolení, které musí v nastavení povolit sám uživatel. Povolit XLM makra lze stejně jako v případě VBA maker v nastavení aplikace Microsoft Office. Nabídka pro spouštění XLM maker se nachází pouze v aplikaci Excel (viz obrázek č. 7).[75]

[74] *Microsoft.com: Macros in Office files* [online]. [cit. 15.08.2022] Dostupné z: https://support.microsoft.com/en-us/office/macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6

[75] *Outflank: Old school: evil Excel 4.0 macros (XLM)* [online]. [cit. 15.08.2022] Dostupné z: https://outflank.nl/blog/2018/10/06/old-school-evil-excel-4-0-macros-xlm/



Obrázek č. 7 - Povolení XLM maker v aplikaci Excel

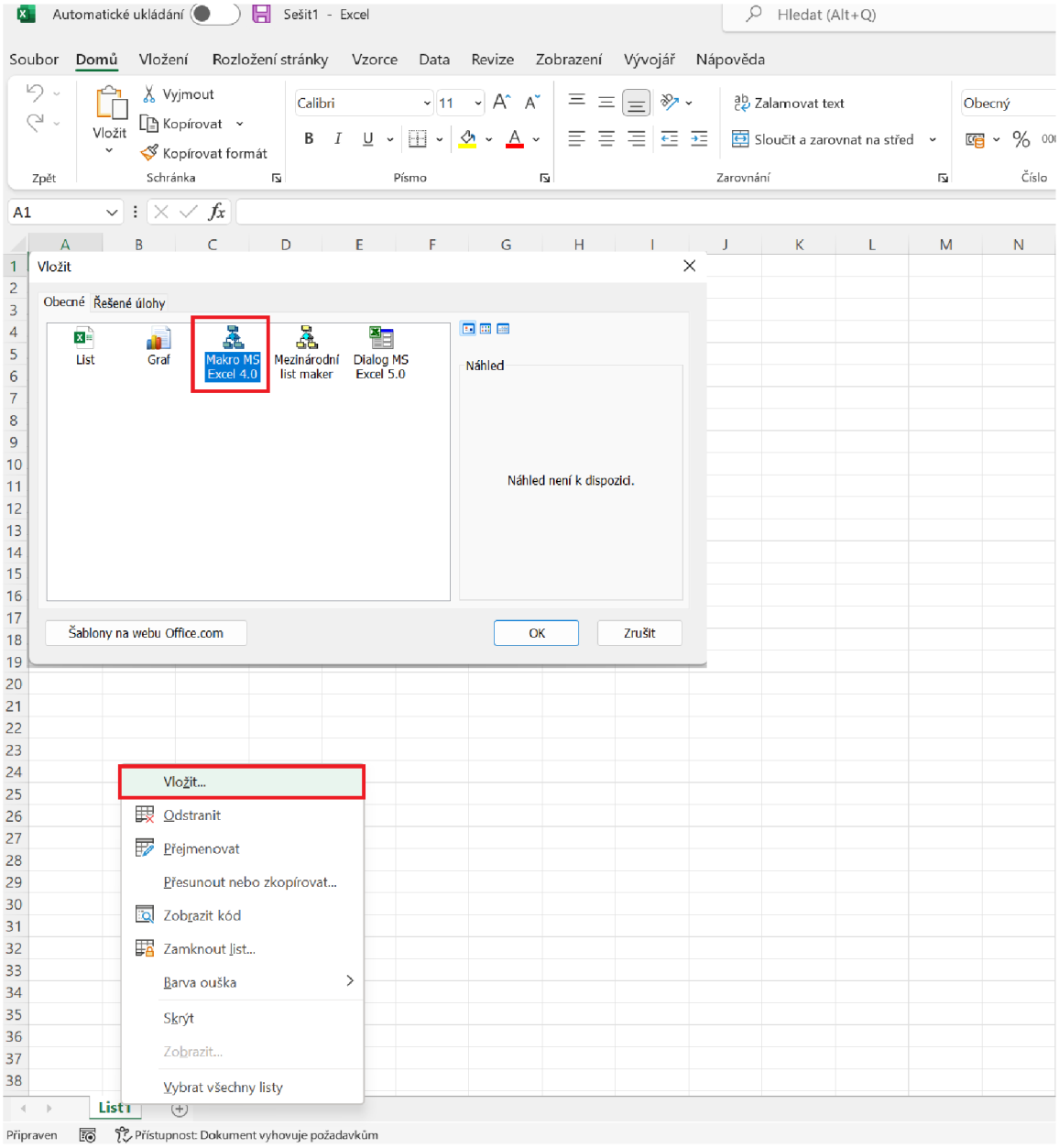
Jak je vidět na obrázku č. 7 ve výchozím nastavení je spouštění XLM maker zakázáno. V případě povolení tohoto typu maker jakékoliv další spouštění závisí na konkrétním nastavení povolení VBA maker.

4.2.1. Vytvoření XLM makra

V rámci této práce autor vytvořil jednoduché XLM makro k demonstraci některých možností, kterými disponuje tento typ maker. Jedná se o velmi jednoduché příkazy, které ze souboru aplikace Excel spustí některou ze systémových aplikací operačního systému Microsoft Windows. Makro bylo otestováno v kancelářském balíku Microsoft Office ve verzi 2021 nainstalovaném na platformě operačního systému Microsoft Windows ve verzi 11. Makra byla nastavena v režimu „zakázat s oznámením“, tedy při spuštění aplikace Excel bylo vyžadováno dodatečné povolení pro spuštění makra.

Po spuštění aplikace stačí kliknout v dolní část na název listu, následně levým tlačítkem myši vyvolat kontextové menu a vybrat položku „Vložit makro.“

Následně se objeví dialogové okno, ve kterém je nutno zvolit položku „Makro MS Excel 4.0.“ (viz obrázek č. 8).[76]



Obrázek č. 8 - Vložení XLM makra

[76] *Outflank: Old school: evil Excel 4.0 macros (XLM)* [online]. [cit. 15.08.2022] Dostupné z: https://outflank.nl/blog/2018/10/06/old-school-evil-excel-4-0-macros-xlm/

Tím se vytvoří samostatný list pro vytvoření XLM makra. Ve výchozím názvu bývá tento list pojmenován jako „Makro1.“ Do prvních dvou řádků v prvním sloupci stačí zapsat následující příkazy:[77]

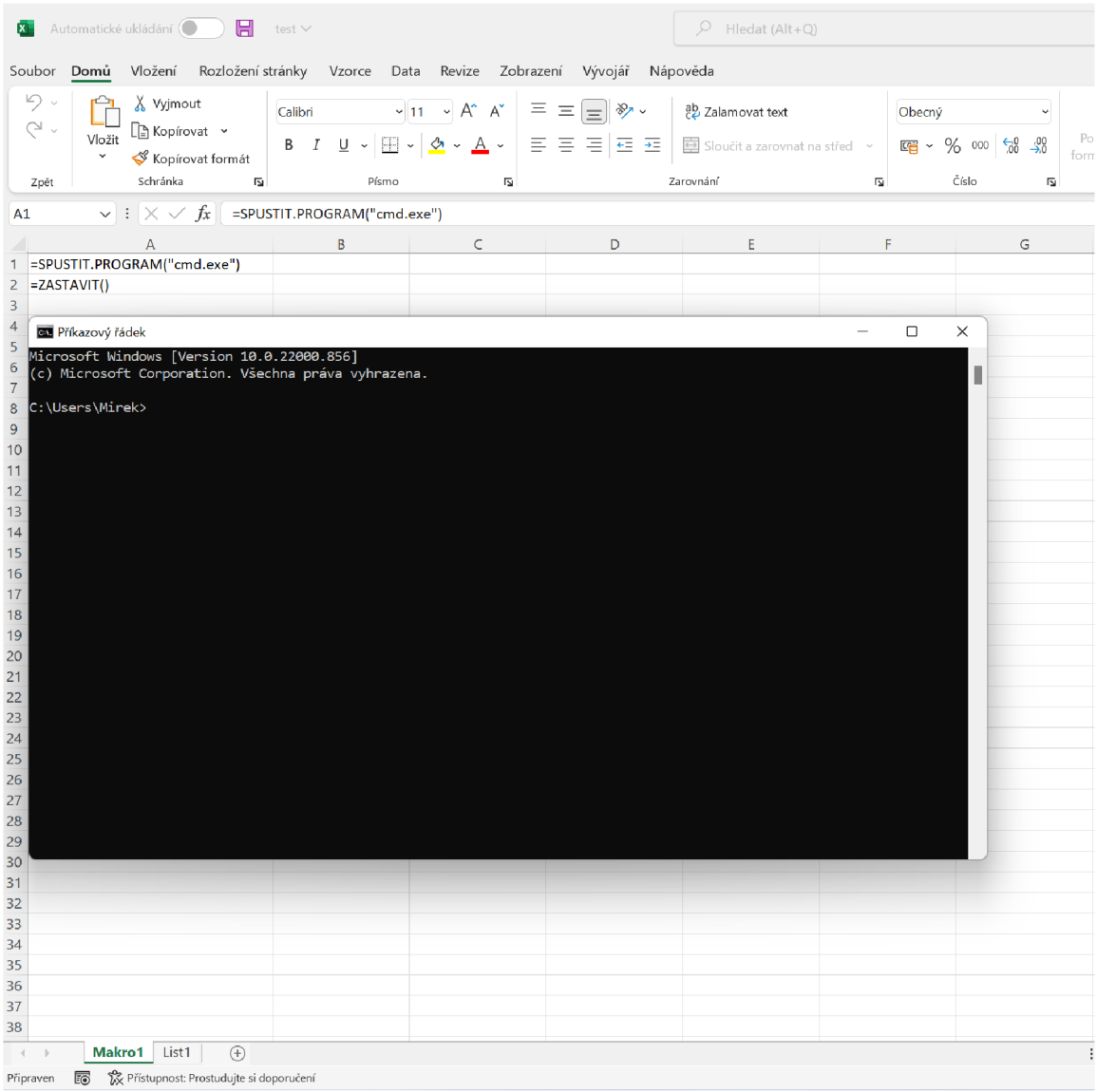
```
SPUSTIT.PROGRAM("cmd.exe")
ZASTAVIT()
```

Při spuštění makra první příkaz v tomto případě spustí systémovou aplikaci „Příkazový řádek“ (viz obrázek č. 9). Druhý příkaz makro následně zastaví. Prostřednictvím příkazového řádku může uživatel komunikovat s operačním systémem a zadávat mu různé operace.[78] Pro tvůrce škodlivého softwaru není problém takovýto příkaz doplnit dalšími parametry, kdy instrukce, které mohou být součástí těchto parametrů, následně příkazový řádek vykoná. Ačkoliv jsou výše uvedené příkazy v češtině, při otevření aplikace Excel v operačním systému, který má předinstalovaný cizí jazyk, dojde k automatickému překladu příkazů.

XLM makra jsou dnes považována za zastaralou technologii, která je v aplikaci Excel do současné doby zachována kvůli zpětné kompatibilitě. Stále však jsou tato makra schopna spouštět aplikace v operačním systému a vstupovat do jeho rozhraní. Stejně jako v případě VBA maker, také zde je riziko možného šíření škodlivého kódu, který díky této zastaralé technologii může uniknout detekci moderních bezpečnostních systémů. Vzhledem k tomu, že se jedná o zastaralou technologii, která představuje velmi velké riziko při používání, nelze jinak než doporučit nepoužívat tento typ maker a nepovolovat jejich spouštění.

[77] *Outflank: Old school: evil Excel 4.0 macros (XLM)* [online]. [cit. 15.08.2022] Dostupné z: https://outflank.nl/blog/2018/10/06/old-school-evil-excel-4-0-macros-xlm/

[78] *Wikipedie: Otevřená encyklopedie: Příkazový řádek* [online]. [citováno 15.08.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=P%C5%99%C3%ADkazov%C3%BD_%C5%99%C3%A1dek&oldid=21594357



Obrázek č. 9 - Spuštění příkazového řádku pomocí XLM makra

Závěr

Moderní počítačové systémy nám nabízí širokou škálu možností, díky kterým můžeme definovat bezpečnostní pravidla pro chování v daném systému. Tato pravidla jsou však určována podle uživatelů, který daný systém používají. V první řadě se vždy snažíme chránit uložená data, ke kterým uživatelé přistupují. V centru dění tak máme uživatele, kterému určujeme pravidla, ke kterým datům má přístup a rozsah jeho oprávnění. Musíme se tak zaměřit na uživatele samotného, neboť právě on je operátorem systému a mnohdy vstupním bodem škodlivého softwaru do systému.

Moderní bezpečnostní systémy jsou schopny v mnoha případech detekovat škodlivý kód a zvýšit tak bezpečnost systému. Nicméně na bezpečnostní systémy je třeba se dívat jako na pomocné nástroje a nelze se na ně úplně stoprocentně spoléhat. Útočníci se vždy budou snažit hledat způsoby, jak proniknout do systému, vyhledávat jeho slabiny a největší slabinou bývá právě uživatel. Neznalý uživatel je riziko pro celou počítačovou infrastrukturu. Proto by jedním z bodů pro kybernetickou bezpečnost mělo být vzdělávání uživatelů, upozornění na aktuální bezpečnostní hrozby a jak se těmto hrozbám vyvarovat.

Počítačové systémy jsou dnes součástí každé domácnosti, kdy drtivá většina obyvatelstva používá chytré mobilní telefony, využívá internetových služeb a mnohdy si pro svoji neznalost neuvědomují některá rizika. Velmi často tak dochází k zneužití osobních údajů, které útočník získá lstivými metodami, které mnohdy bývají známé.

Distribuce malware prostřednictvím maker není žádnou novinkou. Poprvé se tato metoda objevila ke konci dvacátého století. Do popředí se tato metoda dostala opět v souvislosti s ransomware. Tato metoda útoku úspěšně infikovala počítačové systémy po celém světe několik let předtím, než se objevila v nemocnicích v České republice. Vzhledem k napjatému rozpočtu nemocničních zařízení je velmi pravděpodobné, že počítačová infrastruktura bývá v těchto zařízeních zastaralá, kdy v rozpočtu má přednost lékařské vybavení. Toho si však je útočník vědom, a proto si takové zařízení vybírá.

Ovšem také znalý uživatel může udělat chybu a škodlivý kód spustit. Proto je potřeba nastavit bezpečnost takovým způsobem, aby odpovídala moderním

trendům a bezpečnostní systémy mohly sloužit jako další záchytný bod pro zastavení šíření malware a tím přispět k ochraně dat.

Investice do počítačové infrastruktury není jednorázová. Informační technologie se neustále vyvíjí. Vznikají stále nové funkce, dochází ke stále většímu propojování služeb a útočníci se vždy budou snažit najít nové způsoby ke kybernetickým útokům. Vzhledem k tomu, jak je v dnešním světě počítačová infrastruktura důležitá, nelze tedy usnout na vavřínech a při spravování jakékoliv organizace myslet na tento druh infrastruktury a jaký má na její chod vliv.

Seznam použité literatury

[1] *J.Kolouch, T. Zahradnický, A. Kučínský: Cyber security: Lessons learned from cyber-attacks on hospitals in the Covid-19* [online]. [cit. 27.07.2022]. Dostupné z: https://journals.muni.cz/mujlt/article/view/14463/12356

[2] *Ministerstvo vnitra České republiky, generální ředitelství Hasičského záchranného sboru České republiky: Krizové řízení při nevojenských krizových situacích.* [online]. [cit. 10.02.2022]. Dostupné z: https://docplayer.cz/21764430-Ministerstvo-vnitra-generalni-reditelstvi-hasicskeho-zachranneho-sboru-ceske-republiky.html

[3] *Česko: Ústavní zákon č. 110 ze dne 22. dubna 1998 o bezpečnosti České republiky*. In Sbírka zákonů České republiky. 1998, částka 39, s. 5386 [online]. [cit. 11.02.2022]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3146

[4*] Česko: Zákon č. 240 ze dne 28. června 2000 o krizovém řízení a o změně některých zákonů*. In Sbírka zákonů České republiky. 2000, částka 73, s. 3745 [online]. [cit. 11.02.2022]. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240

[5] *Generální ředitelství Hasičského záchranného sboru ČR: Integrovaný záchranný systém* [online]. [cit. 11.02.2022]. Dostupné z: https://www.hzscr.cz/clanek/integrovany-zachranny-system.aspx

[6] *Česko: Nařízení vlády č. 432 ze dne 22. prosince 2010 Sb. o kritériích pro určení prvku kritické infrastruktury*. In Sbírka zákonů České republiky. 2010, částka 149, s. 5623 [online]. [cit. 12.02.2022]. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=21413

[7] *Česko: Zákon č. 97 ze dne 25. února 1993 o působnosti Správy státních hmotných rezerv*. In Sbírka zákonů České republiky. 1993, částka 27 [online]. [cit. 12.02.2022] Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=2671

[8] *Wikipedie: Otevřená encyklopedie: Komunikace* [online]. [cit. 25.02.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Komunikace&oldid=21357436

[9] *Wikipedie: Otevřená encyklopedie: Telekomunikace* [online]. [cit. 05.03.2022]. Dostupné z https://cs.wikipedia.org/w/index.php?title=Telekomunikace&oldid=19883798

[10] *Wikipedie: Otevřená encyklopedie: Akustika* [online]. [cit. 05.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Akustika&oldid=20173963

[11] *Wikipedie: Otevřená encyklopedie: Kurýrní služba* [online]. [cit. 05.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Kur%C3%BDrn%C3%AD_slu%C5%BEba&oldid=20207260

[12] *Wikipedie: Otevřená encyklopedie: Zvířata během první světové války* [online]. [cit. 05.03.2022]. Dostupné z: https://cs.frwiki.wiki/wiki/Animaux_durant_la_Premi%C3%A8re_Guerre_mondiale

[13] *Wikipedie: Otevřená encyklopedie: Telegrafie* [online]. [cit. 10.03. 2022]. Dostupné z https://cs.wikipedia.org/w/index.php?title=Telegrafie&oldid=21426540

[14] *Wikipedie: Otevřená encyklopedie: Telefonie* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Telefonie&oldid=21610990

[15] *Wikipedie: Otevřená encyklopedie: Telefon* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Telefon&oldid=21409833

[16] *Wikipedie: Otevřená encyklopedie: Fax* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Fax&oldid=21254984

[17] *Wikipedie: Otevřená encyklopedie: Mobilní telefon* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Mobiln%C3%AD_telefon&oldid=21536046

[18] *Wikipedie: Otevřená encyklopedie: Satelitní telefon* [online]. [cit. 10.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Satelitn%C3%AD_telefon&oldid=21314099

[19] *Wikipedia: The Free Encyclopedia: Radio* [online]. [cit. 10.03.2022] Dostupné z: https://en.wikipedia.org/w/index.php?title=Radio&oldid=1107386517

[20] *Ministerstvo vnitra České republiky: Technologie, struktura a služby sítě Pegas* [online]. [cit. 11.03.2022]. Dostupné z: https://www.mvcr.cz/soubor/technologie-site-pegas-pdf.aspx

[21] *Wikipedie: Otevřená encyklopedie: Rozhlas* [online]. [cit. 11.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Rozhlas&oldid=21392356

[22] *Wikipedie: Otevřená encyklopedie: Televize* [online]. [cit. 11.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Televize&oldid=21438634

[23] *Wikipedie: Otevřená encyklopedie: Počítačová síť* [online]. [cit. 11.03.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5&oldid=21440133

[24] *Správa.sítě.eu: Co je to kyberprostor* [online]. [cit. 15.07.2022]. Dostupné z: https://www.sprava-site.eu/kyberprostor/

[25] *Wikipedie: Otevřená encyklopedie: Počítačová kriminalita* [online]. [cit. 15.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_kriminalita&oldid=20758707

[26] *Eset.cz: Co je malware? Jak se zbavit malwaru?* [online]. [cit. 15.07.2022]. Dostupné z: https://www.eset.com/cz/malware/#co-je-to-malware

[27] *Wikipedia, The Free Encyclopedia: Dark web* [online]. [cit. 15.07.2022]. Dostupné z: https://en.wikipedia.org/w/index.php?title=Dark_web&oldid=1106032026

[28] *Svět Androida: Na tom videu jsi ty?* [online]. [cit. 16.07.2022]. Dostupné z: https://www.svetandroida.cz/na-tom-videu-jsi-ty-utok-zprava-messenger/

[29] *Eset.cz: Co je phishing?* [online]. [cit. 16.07.2022]. Dostupné z: https://www.eset.com/cz/phishing/

[30] *Česká spořitelna a. s.: Vishing* [online]. [cit. 16.07.2022]. Dostupné z: https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat/vishing

[31] *Wikipedie: Otevřená encyklopedie: Počítačový virus* [online]. [cit. 16.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus&oldid=21448963

[32] *Wikipedie: Otevřená encyklopedie: Počítačový červ* [online]. [cit. 16.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv&oldid=18815487

[33] *Wikipedia, The Free Encyclopedia: Scareware* [online]. [cit. 17.07.2022] Dostupné z: https://en.wikipedia.org/w/index.php?title=Scareware&oldid=1102495324

[34] *Wikipedie: Otevřená encyklopedie: Spyware* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Spyware&oldid=21189528

[35] *Wikipedie: Otevřená encyklopedie: Adware* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Adware&oldid=20917505

[36] *Wikipedie: Otevřená encyklopedie: Trojský kůň* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Trojsk%C3%BD_k%C5%AF%C5%88_(program)&oldid=21212708

[37] *Wikipedie: Otevřená encyklopedie: Ransomware* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Ransomware&oldid=21367664

[38] *Wikipedie: Otevřená encyklopedie: Denial of service* [online]. [cit. 17.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Denial_of_service&oldid=21395675

[39] *Idnes.cz: Nemocnice jsou pro hackery stále snadným cílem. Útoků přitom přibývá* [online]. [cit. 21.07.2022] Dostupné z: https://www.idnes.cz/zpravy/domaci/kyberneticky-utok-hacker-nemocnice-zabezpeceni.A210203_141638_domaci_knn

[40] *Aktuálně.cz.: Další kybernetický útok za nouzového stavu: Hackeři napadli psychiatrickou nemocnici* [online]. [cit. 22.07.2022]. Dostupné z: https://zpravy.aktualne.cz/domaci/kosmonosy-utok-koronavirus/r~188929ec732511ea9d74ac1f6b220ee8/

[41] *Wikipedia, The Free Encyclopedia: WannaCry ransomware attack* [online]. [cit. 22.07.2022] Dostupné z: https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&oldid=1106987274

[42] *Wikipedie: Otevřená encyklopedie: Bitcoin* [online]. [cit. 22.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Bitcoin&oldid=21588971

[43] *Techopedie: Co je to segmentace sítě* [online]. [cit. 26.07.22]. Dostupné z: https://cs.theastrologypage.com/network-segmentation

[44] *TechTarget: What is Group Policy?* [online]. [cit. 26.07.2022] Dostupné z: https://www.techtarget.com/searchwindowsserver/definition/Group-Policy

[45] *Wikipedie: Otevřená encyklopedie: Business Continuity Management* [online]. [cit. 26.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Business_Continuity_Management&oldid=19436136

[46] *TEMPEST a.s.: Vulnerability Scanning* [online]. [cit. 26.07.2022]. Dostupné z: https://www.tempest.sk/skenovani-zranitelnosti-5e4.html

[47] *NÚKIB: Ransomware: doporučení pro mitigaci, prevenci a reakci* [online]. [cit. 27.07.2022]. Dostupné z: https://www.nukib.cz/download/publikace/navody/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf

[48] *Wikipedie: Otevřená encyklopedie: Antivirový program* [online]. [cit. 27.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Antivirov%C3%BD_program&oldid=20781273

[49] *Wikipedie: Otevřená encyklopedie: Firewall* [online]. [cit. 27.07.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Firewall&oldid=19597290

[50] *Outflank: Old school: evil Excel 4.0 macros (XLM)* [online]. [cit. 15.08.2022] Dostupné z: https://outflank.nl/blog/2018/10/06/old-school-evil-excel-4-0-macros-xlm/

[51] *Microsoft.com: Macros in Office files* [online]. [cit. 15.08.2022] Dostupné z: https://support.microsoft.com/en-us/office/macros-in-office-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6

[52] *Wikipedie: Otevřená encyklopedie: Příkazový řádek* [online]. [citováno 15.08.2022]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=P%C5%99%C3%ADkazov%C3%BD_%C5%99%C3%A1dek&oldid=21594357

Seznam obrázků

Obrázek č. 1 - schéma legislativy krizového řízení 10
Obrázek č. 2 - schéma orgánů krizového řízení ČR..... 13
Obrázek č. 3 - komunikační schéma 17
Obrázek č. 4 - Snímek dialogového okna ransomware požadující výkupné 39
Obrázek č. 5 - Nastavení VBA maker 50
Obrázek č. 6 - Lišta s upozorněním na přítomnost maker..... 51
Obrázek č. 7 - Povolení XLM maker v aplikaci Excel 53
Obrázek č. 8 - Vložení XLM makra 54
Obrázek č. 9 - Spuštění příkazového řádku pomocí XLM makra 56

Seznam tabulek

Tabulka č. 1 - odvětvová kritéria 15
Tabulka č. 2 - Souhrnný přehled úspěšných útoků na zdravotnická zařízení..... 38