ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

F8

Fakulta informačních technologií
Katedra počítačových systémů

Bakalářská práce

Analýza bezpečnosti počítačové sítě

Michal Franc

Květen 2020
Vedoucí práce: Ing. Jiří Dostál, Ph.D.

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Analýza bezpečnosti počítačové sítě
Student:	Michal Franc
Vedoucí:	Ing. Jiří Dostál, Ph.D.
Studijní program:	Informatika
Studijní obor:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce letního semestru 2020/21

Pokyny pro vypracování

Zanalyzujte současný stav počítačové sítě společnosti T.J. Sokol Kolín - Atletika.
Zaměřte se především na slabá místa z hlediska počítačové bezpečnosti a architektury počítačové sítě.
Proveďte analýzu skutečných požadavků na provoz sítě.
Na základě analýzy navrhněte opatření, která odstraní nalezené bezpečnostní problémy a zároveň vyhoví požadavkům na provoz v síti.
Vybraná opatření implementujte a ověřte v reálném provozu.

Seznam odborné literatury

Dodá vedoucí práce.

prof. Ing. Pavel Tvrdík, CSc.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 2. února 2020

/ Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 2373 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo“), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené.

V Praze dne 3. 6. 2020

Abstrakt / Abstract

Tato práce se zabývá analýzou počítačové sítě společnosti T. J. Sokol Kolín – Atletika. Důraz je kladen především na kybernetickou bezpečnost. Během analýzy je postupováno podle standardu The Penetration Testing Execution Standard. Pro identifikaci a kategorizaci hrozeb je použita metodika STRIDE. Na analýzu je navázáno návrhem a implementací opatření na odstranění nalezených bezpečnostních slabin. Konkrétní řešení se zabývá především segmentací sítě, řízením přístupu, správou identit a monitoringem sítě.

Hlavním výsledkem je zvýšení bezpečnosti počítačové sítě společnosti T. J. Sokol Kolín – Atletika. Na základě této práce můžou další společnosti v podobné situaci zvýšit bezpečnost své sítě.

Klíčová slova: síťová bezpečnost, analýza počítačové sítě, penetrační testování, monitoring sítě, informační bezpečnost

This thesis deals with T. J. Sokol Kolín – Atletika company computer network security analysis. The emphasis is on cybersecurity. The analysis part proceeds using The Penetration Testing Execution Standard. The thesis uses method STRIDE to identify security threats. After analysis, the work continues with the suggestion and implementation of measures to eliminate the discovered threats. The solution is mostly based on network segmentation, access management, identity management, and network monitoring.

As a result, the T. J. Sokol Kolín – Atletika company network is better secured. Based on the thesis, similar companies can secure their networks such as.

Keywords: network security, computer network analysis, penetration testing, network monitoring, cybersecurity

Title translation: Computer Network Security Analysis

/ Obsah

Výpisy / Obrázky

Úvod

Nejen bezpečnost počítačových sítí, ale kybernetická bezpečnost obecně je velmi aktuálním tématem. V dnešní době se čím dál více spoléháme na infrastrukturu, která na to není připravena. Situace se pomalu zlepšuje a o kybernetické bezpečnosti se často mluví, i přesto zůstává spousta systémů nezabezpečena nebo zabezpečena jen minimálně.

I sportovní kluby potřebují ke své činnosti alespoň částečně využít počítače. Většinou ale nemají zaměstnance zabývající se touto problematikou. Nejen z těchto důvodů vychází nízká motivace investovat do zlepšení a zabezpečení infrastruktury. Práce se zaměřuje na počítačovou síť konkrétního sportovního oddílu, může však posloužit jako inspirace či návod i dalším oddílům v podobné situaci.

Práce se zabývá analýzou počítačové sítě. Důraz je kladen především na kybernetickou bezpečnost. Jedním z cílů je identifikace slabých míst jak z pohledu bezpečnosti, tak z pohledu architektury počítačové sítě. Dalším cílem je odstranění těchto nalezených slabin.

Nejdříve práce analyzuje současný stav počítačové sítě a požadavky na její provoz. Na tuto analýzu je navázáno modelem hrozeb a analýzou bezpečnostních slabin. Další část je věnována návrhu opatření na odstranění objevených bezpečnostních slabin. Nakonec následuje implementace vybraných opatření a ověření proveditelnosti této implementace.

Kapitola 1
Cíl práce

Hlavním cílem bakalářské práce je odstranění bezpečnostních slabin počítačové sítě společnosti T. J. Sokol Kolín – Atletika. Podružným cílem je nabídnout inspiraci pro řešení bezpečnosti v počítačových sítích s podobným provozem.

Mezi dílčí cíle patří analýza stavu počítačové sítě a identifikace slabých míst z pohledu kybernetické bezpečnosti a architektury počítačové sítě. Dále je cílem analýza požadavků na provoz a návrh opatření pro eliminaci slabých míst. Důležité je, nejen aby navržená opatření řešila nalezené slabiny, ale aby také reflektovala definované požadavky. Následně budou vybraná opatření implementována a funkčnost implementovaných opatření ověřena v reálném provozu.

Kapitola 2
Analýza síťové infrastruktury

Tato kapitola se zabývá analýzou současného stavu infrastruktury. Analýza je rozdělena na sběr informací, modelování hrozeb a definici požadavků na provoz.

Samotná analýza je velice podobná penetračnímu testování. Z toho důvodu bylo postupováno podle standardu „The Penetration Testing Execution Standard“ (PTES) [1]. PTES pokrývá průběh celého penetračního testování. Pro účely této práce byly využity především první čtyři kapitoly tohoto standardu, které pokrývají fázi před testováním, sběr informací, modelování hrozeb a analýzu zranitelností.

2.1 Aktuální stav

Následující část se zabývá sběrem informací o infrastruktuře a mapováním aktuálního stavu. V rámci přípravy na testování jsou zodpovězeny otázky související s testováním infrastruktury. Poté jsou ujasněny cíle, kterých se tato analýza týká. A následně je prezentován průběh analýzy infrastruktury rozdělený do několika tematických celků.

2.1.1 Příprava testování

Infrastruktura společnosti je kritická vzhledem k několika hlavním činnostem, přesto společnost nemá o infrastruktuře přehled. Cílem testování je zjištění aktuálního stavu za účelem zmapování situace a odhalení bezpečnostních slabin. Společnost nemusí splňovat konkrétní bezpečnostní standard.

Samotné testování by nemělo omezovat provoz sítě. Aktivní testy je možné provádět v dopoledních hodinách.

Rozsah testování odpovídá přibližně 10–20 zařízení. Výsledky testování mohou být zkresleny firewallem nacházejícím se na hranici LAN a WAN. V případě získání přístupu k nějakému zařízení je možné provést kompletní výčet zranitelností a pokusit se o eskalaci oprávnění.

V místě společnosti jsou k dispozici tři bezdrátové sítě včetně jedné veřejné. K veřejné síti se lze připojit bez autentizace. Ostatní sítě jsou zabezpečeny pomocí WPA2 a autentizace probíhá pomocí hesla. V době testování pravděpodobně nebude připojeno mnoho zařízení (odhadem maximálně pět).

2.1.2 Upřesnění cíle

Základní zmapování infrastruktury bylo provedeno pomocí utility `nmap`. Konkrétně pomocí příkazu `nmap 192.168.1.0/24 -sn` byla nalezena aktivní zařízení v síti. Seznam nalezených zařízení je k vidění ve výpisu 2.1. Cílem testování jsou tato nalezená zařízení.

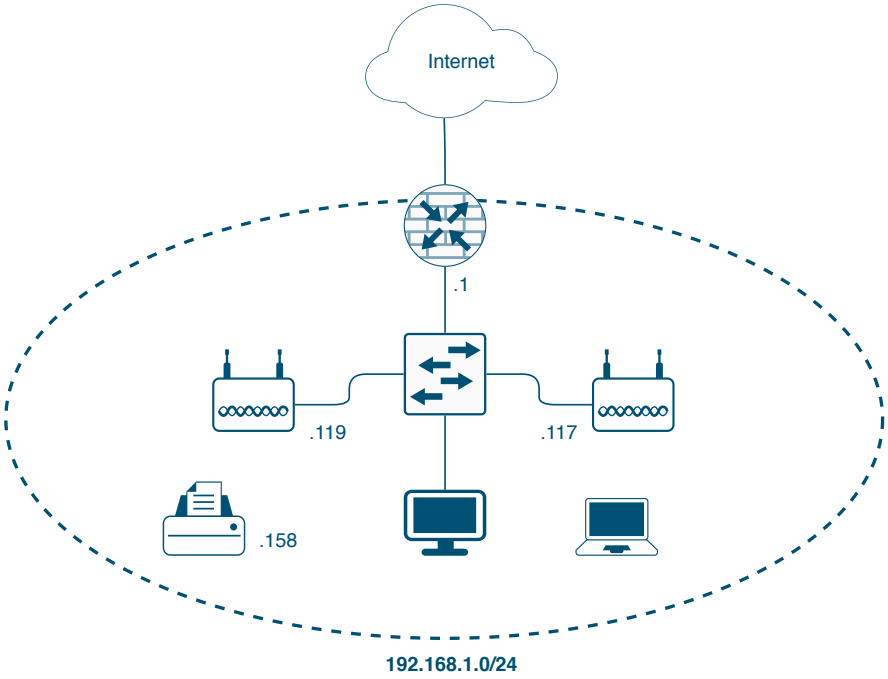
Dále pomocí utility `airodump-ng` byla ověřena přítomnost bezdrátových sítí. Program objevil přítomnost tří bezdrátových sítí patřících do dané infrastruktury. Výpis 2.2 zobrazuje informace získané programem (zkráceno o některé sloupce a sítě, které nepatří do infrastuktury).

```
Nmap scan report for 192.168.1.1
Host is up (0.0051s latency).
MAC Address: 00:0C:42:00:00:00 (Routerboard.com)
Nmap scan report for 192.168.1.117
Host is up (0.0035s latency).
MAC Address: 68:72:51:00:00:00 (Ubiquiti Networks)
Nmap scan report for 192.168.1.119
Host is up (0.0063s latency).
MAC Address: 04:8D:39:00:00:00 (Unknown)
Nmap scan report for 192.168.1.125
Host is up (0.033s latency).
MAC Address: 3C:F8:62:00:00:00 (Intel Corporate)
Nmap scan report for 192.168.1.158
Host is up (0.044s latency).
MAC Address: A8:6B:AD:00:00:00 (Hon Hai Precision Ind.)
```

Výpis 2.1. Základní scan sítě

```
ESSID               Cloaked Encryption
Atleticky Stadion 2 No      OPN,None
OnlineAtletika      No      WPA2,AES-CCM
Atletak-Press       No      WPA2,AES-CCM
```

Výpis 2.2. Aktivní bezdrátové sítě (zkráceno)



Obrázek 2.1. Aktuální stav počítačové sítě

2.1.3 Informace z otevřených zdrojů

Informace z otevřených zdrojů (OSINT, Open Source Intelligence) umožňují získat přehled o dané společnosti a o testované infrastruktuře.

Jedním z hlavních zdrojů takových informací jsou webové stránky společnosti. Přestože webové stránky jsou hostovány mimo infrastrukturu a nejsou tedy předmětem testování, z hlediska OSINT však mohou být získaná data přínosná. Metada publikovaných dokumentů mohou poskytovat informace, jako jsou jméno autora, datum, geolokační data, umístění souboru atd.

Dále se získáváním informací souvisí mapování infrastruktury. Data získaná v tomto kroku jsou velice podobná datům získaným při upřesňování cíle a také datům rozebíraným v následující části. Na diagramu 2.1 je zachycen aktuální stav infrastruktury odpovídající získaným informacím.

2.1.4 Identifikace zařízení

Skenování otevřených portů nám umožňuje získat základní přehled o aplikacích běžících na daných zařízeních. Pomocí dalších technik lze určit konkrétní aplikace, které na otevřených portech naslouchají. Ve výpisech 2.3 a 2.4 lze nahlédnout na výsledky získané pomocí technik „port scanning“ a „banner grabbing“.

Výsledky například ukazují na přítomnost routeru na adrese `192.168.1.1`. Data správně odhalují, že se jedná o zařízení „MikroTik RouterBOARD“. Na routeru běží pouze služby určené pro administraci tohoto zařízení.

Dále byla objevena tiskárna na adrese `192.168.1.158`. Na této tiskárně běží webová aplikace pro administraci tiskárny na portech 80 (HTTP) a 443 (HTTPS). Dále byly nalezeny služby pro přijímání dokumentů k tisku pomocí FTP a e-mailu. Také mimo jiné byla odhalena služba jetdirect (custom raw port) umožňující uživateli vytisknout veškerá data odeslaná na port 9100.

Mnoho užitečných informací lze také získat pomocí protokolu „Simple Network Management Protocol“ (SNMP). Aktivní SNMP lze zjistit například pomocí nástrojů ze sady Net-SNMP. Pomocí utility `snmpwalk` byla zjištěna možnost komunikace pomocí SNMP se dvěma zařízeními. Ukázka získaných dat je k vidění ve výpisu 2.5.

```
iso.3.6.1.2.1.1.1.0 = STRING: "RouterOS RB433"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.14988.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (85628200) 9 days, 21:51:22.00
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "RB_Atletak"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 78
iso.3.6.1.2.1.2.1.0 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
```

```
iso.3.6.1.2.1.1.1.0 = STRING: "Brother NC-8300w"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.2435.2.3.9.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (76990460) 8 days, 21:51:44.60
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "BRWA86BAD6E32D7"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.10.3.1.1
```

Výpis 2.5. Ukázka údajů získaných pomocí SNMP

```
Nmap scan report for 192.168.1.1
Host is up (0.021s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE        VERSION
23/tcp   open  telnet         Linux telnetd
2000/tcp open  bandwidth-test MikroTik bandwidth-test server
2221/tcp open  ssh            MikroTik RouterOS sshd (protocol 2.0)
8291/tcp open  unknown
Service Info: OS: Linux; Device: router;
              CPE: cpe:/o:linux:linux_kernel, cpe:/o:mikrotik:routeros
```

```
Nmap scan report for 192.168.1.117
Host is up (0.017s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE    VERSION
80/tcp    open  http       lighttpd 1.4.39
443/tcp   open  ssl/https?
10001/tcp open  tcpwrapped
50122/tcp open  ssh        Dropbear sshd 2016.74 (protocol 2.0)
50123/tcp open  telnet
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 192.168.1.158
Host is up (0.011s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        Brother/HP printer ftpd 1.13
23/tcp    open  telnet     Brother/HP printer telnetd
80/tcp    open  http       Brother/HP printer httpd 1.20
443/tcp   open  ssl/http   Brother/HP printer httpd 1.20
515/tcp   open  printer
631/tcp   open  http       Brother/HP printer httpd 1.20
9100/tcp  open  jetdirect?
54921/tcp open  pop3       Brother MFC-7360N pop3d
Service Info: Device: printer
```

Výpis 2.3. Výsledek skenování otevřených portů

2.2 Model hrozeb

ISO/IEC 27000 [2] definuje hrozbu jako potenciální příčinu nežádoucího incidentu, který může vyústit v poškození systému nebo organizace. Model hrozeb tedy umožňuje identifikovat tyto hrozby a zařadit do infrastruktury taková bezpečnostní opatření, která tyto hrozby eliminují.

Tato práce nejdříve definuje aktiva v počítačové síti a poté využívá metodiky STRIDE k identifikaci hrozeb. STRIDE, akronym pro „Spoofing“, „Tampering“, „Repudiation“, „Information Disclosure“, „Denial of Service“ a „Elevation of Privilege“, byla navržena tak, aby pomáhala identifikovat typy útoků používaných proti softwaru [3]. Útoky na software však s útoky na počítačovou síť a na jednotlivé systémy souvisí. Zároveň lze síťové útoky kategorizovat stejným způsobem. Metodika je tedy vhodná i pro účely této práce.

```
Nmap scan report for 192.168.1.1
Host is up (0.0045s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
2000/tcp open  cisco-sccp
|_banner: \x01\x00\x00\x00
8291/tcp open  unknown
MAC Address: 00:0C:42:00:00:00 (Routerboard.com)
```

```
Nmap scan report for 192.168.1.119
Host is up (0.029s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
| banner: \xFF\xFD\x01\xFF\xFD\x1F\xFF\xFD!\xFF\xFB\x01\xFF\xFB\x03\x0D\x
|_0D\x0ANetis(WF2419)-V1.2.29433,2014.08.29 12:30.\x0D\x0A(none) login:
53/tcp open  domain
80/tcp open  http
MAC Address: 04:8D:39:00:00:00 (Unknown)
```

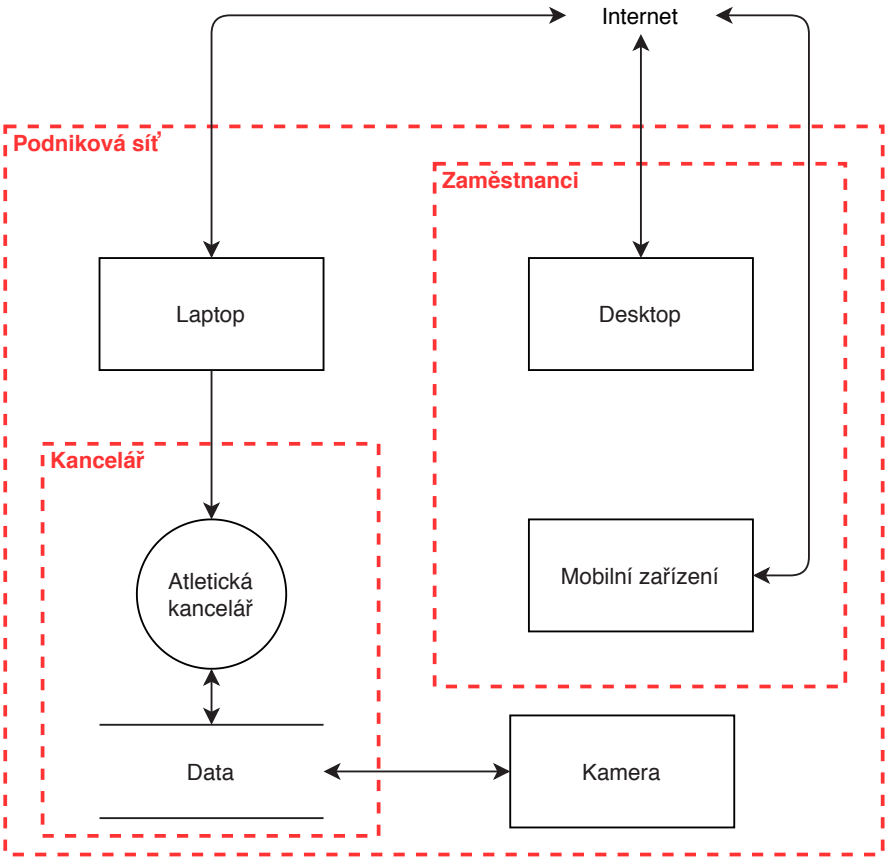
```
Nmap scan report for 192.168.1.158
Host is up (0.0080s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| banner: 220 FTP print service:V-1.13/Use the network password for the I
|_D if updating.
23/tcp   open  telnet
|_banner: \x1B[2J\x1B[1;1f\xFF\xFB\x01\xFF\xFB\x03\xFF\xFD\x03
80/tcp   open  http
443/tcp  open  https
515/tcp  open  printer
631/tcp  open  ipp
9100/tcp open  jetdirect
MAC Address: A8:6B:AD:00:00:00 (Hon Hai Precision Ind.)
```

Výpis 2.4. Informace získané pomocí techniky banner grabbing

2.2.1 Aktiva

Na diagramu 2.2 je vyobrazena podniková síť vzhledem k modelování hrozeb. Funkční síť sestává z následujících systémů:

- Laptop – jsou přenosná podniková koncová zařízení používaná personálem.
- Desktop – jsou podnikové stolní počítače používané personálem.
- Mobilní zařízení – jsou vlastní koncová zařízení vlastněná a používaná personálem.
- Atletická kancelář – představuje software a proces zaznamenávání výsledků a získávání a udržování informací o závodnících.
- Kamera – označuje souhrn zařízení sloužících k zaznamenávání a zpracování měřených dat.
- Data – je úložiště uchovávající data týkající se závodů atd.



Obrázek 2.2. Model podnikové sítě

2.2.2 Podvržení identity

Podvržení identity (Spoofing) je vydávání se za něco či někoho jiného [3].

Z hlediska podvržení identity je problémové použití softwaru třetí strany pro vzdálený přístup některými uživateli. V takovém případě je autentizace založena na znalosti číselného kódu a není svázána s konkrétním uživatelem. Tomu lze zamezit nasazením vlastního řešení VPN.

Obecně, co se týče uživatelů, absence autentizace v rámci této infrastruktury znemožňuje jakoukoli identifikaci konkrétní osoby.

2.2.3 Pozměnění dat

Výsledkem pozměnění dat (Tampering) je nějaká neoprávněná změna v paměti, na disku nebo na síti [3].

V tomto případě je velice problémová práce s Atletickou kanceláří. Uživatel není vůči aplikaci autentizován ani autorizován. V důsledku může kdokoli, kdo se ke Kanceláři připojí, měnit libovolně data. Vzhledem k tomu, že aplikace samotná autentizaci nepodporuje, je možné této hrozbě předejít povolením připojení pouze vybraným zařízením či autentizaci na úrovni spojení se serverem.

2.2.4 Popření transakce

Při popření transakce (Repudiation) útočník či uživatel popírá (klamavě i čestně) zodpovědnost za provedenou akci [3].

Tuto hrozbu lze obecně eliminovat zavedením autentizace v kombinaci se zaznamenáváním každé provedené akce. V tomto případě je potřeba autentizovat jak uživatele,

tak zařízení. Zaznamenávat provedené akce je potřeba na systémové úrovni v podobě logování i na síťové úrovni v podobě monitorování provozu.

V souvislosti s infrastrukturou společnosti hrozí popření transakce především v případě práce s Atletickou kanceláří i v případě práce na jednotlivých pracovních stanicích, kde uživatelský účet není svázán s konkrétní osobou.

2.2.5 Únik informací

Únik informací (Information Disclosure) znamená umožnění nějaké osobě prohlížet data, která není oprávněna prohlížet [3].

Se všemi dříve popsanými hrozbami hrozí i únik informací. Zároveň dříve popsaná řešení v kombinaci s principem nízkých oprávnění zamezuje v existenci i této hrozby.

Navíc komunikace s Atletickou kanceláří není šifrovaná. Tato skutečnost znamená, že každý, kdo je k síti připojen, může tuto komunikaci odposlouchávat.

2.2.6 Odepření služby

Při útoku typu odepření služby (Denial of Service) jsou zdroje potřebné k poskytování služby využívány takovým způsobem, že je služba nepřístupná regulérnímu uživateli [3].

Současná infrastruktura například umožňuje útok na DHCP server, kdy útočník vyplýtvá dostupné adresy a tím zabrání regulérnímu zařízení v získání konfigurace pro své síťové rozhraní.

2.2.7 Zvýšení oprávnění

Neautorizované zvýšení oprávnění (Elevation of Privilege) znamená povolení uživateli provést akci, ke které není autorizován [3].

Tato hrozba většinou souvisí s konkrétními zranitelnostmi nebo chybnou konfigurací jednotlivých systémů. Konkrétní případy této hrozby nebyly v infrastruktuře identifikovány.

2.3 Provozní požadavky

Požadavky na provoz jsou rozděleny na bezpečnostní požadavky a na skupiny požadavků odpovídající provozovaným činnostem.

2.3.1 Bezpečnostní požadavky

Bezpečnostní požadavky jsou nadefinovány tak, aby jejich splnění vedlo k snížení dopadu současných hrozeb a zároveň předcházelo vzniku dalších hrozeb při zavádění nových služeb.

Vylepšená infrastruktura by měla splňovat následující:

- Počítačová síť bude oddělena od internetu firewallem.
- Počítačová síť bude segmentována.
- Aplikace poběží na individuálních virtuálních strojích (co aplikace, to VM).
- Aplikace poběží s nejnižším možným oprávněním.
- Každý uživatel bude mít vlastní účet s nízkými oprávněními.
- Uživatelské účty budou centrálně spravovány a pravidelně auditovány.
- V síti bude nasazen IDS/IPS.
- Zdroje budou dostupné pouze v rámci lokální sítě.
- Stálým zaměstnancům bude umožněno připojení z internetu pomocí VPN.

2.3.2 Závody

Během závodů je nejdůležitější zajistit stabilní propojení Atletické kanceláře a počítačů v poli. To vyžaduje pokrytí celého stadionu dostatečně silným signálem Wi-Fi.

Dále je vhodné alespoň částečně zavést správu identit. Je však potřeba vzít v potaz nestabilitu uživatelů.

Cílová kamera vyžaduje propojení s vyhodnocovací stanicí s rychlostí řádově v Gb/s. To je dáno přenosem velkého objemu obrazových dat a na rychlosti tohoto přenosu závisí rychlost vyhodnocování výsledků.

Během větších závodů je důležitá i rychlost připojení k internetu (především pro účely streamingu).

Na stadionu je poskytováno i veřejné připojení, to však nesmí omezovat provoz v lokální síti, ani připojení do internetu.

2.3.3 Tréninky

Trenéři se během tréninků obejdou bez počítačů, do sítě se tedy připojuje pouze veřejnost. Z toho vyplývá absence speciálních požadavků.

Kapitola 3
Realizace

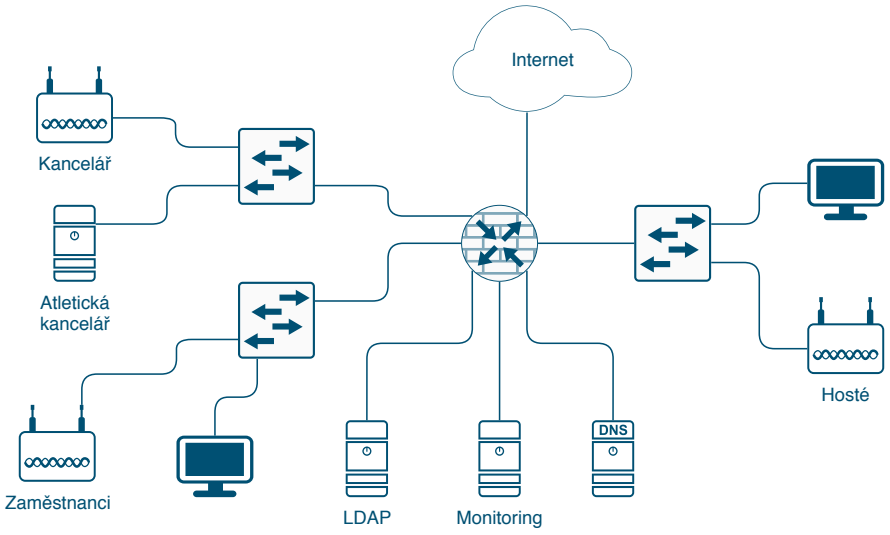
Tato kapitola se zabývá návrhem opatření, která řeší nalezené a dříve popsané slabiny zkoumané sítě. Nejdříve jsou popsána opatření týkající se infrastruktury počítačové sítě. Poté jsou řešena opatření, která jsou základem pro všechna následující opatření. Na společný základ je navázáno výběrem konkrétních řešení dílčích problémů.

Jako první je rozebráno řešení firewallu a detekce/prevence vniknutí. Na to je navázáno správou identit včetně dalších, s tím souvisejících, jmenných služeb. A v neposlední řadě je předvedeno řešení monitoringu sítě.

3.1 Infrastruktura

Z firemní sítě bude vyčleněno veřejné připojení. Samotná síť pak bude oddělena firewallem a rozdělena do několika segmentů. Konkrétně se jedná o segmenty pro zaměstnance, Atletickou kancelář a služby infrastruktury. V neposlední řadě bude jeden segment vyhrazen pro management sítě. Návrh infrastruktury je k vidění na diagramu 3.1.

Přístup mimo jiné zajistí několik access pointů připojených do odpovídajících segmentů. Pro zabezpečení komunikace bude nadále používáno WPA2. Do zaměstnaneckého segmentu bude umožněn přístup na základě znalosti hesla. Do segmentu atletické kanceláře bude umožněn přístup na základě znalosti hesla kombinován s filtrováním zařízení.



Obrázek 3.1. Navržená infrastruktura počítačové sítě

3.2 Příprava

Pro snazší oddělení jednotlivých služeb a správu serverů je použita virtualizace. Virtuální stroje vycházejí ze stejného základního obrazu stroje. Základ je postaven na OS Linux (Debian Buster), na kterém je provedena základní konfigurace. Projekt Debian

zároveň nabízí manuál Securing Debian [4], který provází základním nastavením systému s ohledem na bezpečnost.

Kromě hlavního síťového firewallu je připravena ochrana zařízení pomocí jednotlivých lokálních síťových firewallů. Pro konfiguraci firewallu na všech serverech je jednotně využita utilita Shorewall. Princip konfigurace je popisován v části 3.3.1. Firewall je nakonfigurován restriktivně, aby obraz systému byl ve výchozím stavu maximálně chráněný a zároveň aby obraz zůstal univerzální. Příchozí komunikace je zahazována. Výjimku tvoří povolení komunikace s monitorovacím serverem, SSH pro administraci a ICMP pro základní diagnostiku stavu zařízení. Při nasazení tedy musí být povolena komunikace podle potřeb konkrétního stroje.

K dispozici je připraven jeden lokální administrátorský účet pro základní nastavení a případné řešení problémů. Superuživateli je znemožněno se přihlásit vzdáleně i lokálně. Administrátoři mohou spravovat systém pomocí vlastního účtu definovaného ve službě LDAP. Způsob navázání na jmenné služby představí část 3.5.2. Privilegované operace mohou provádět s využitím příkazu `sudo`.

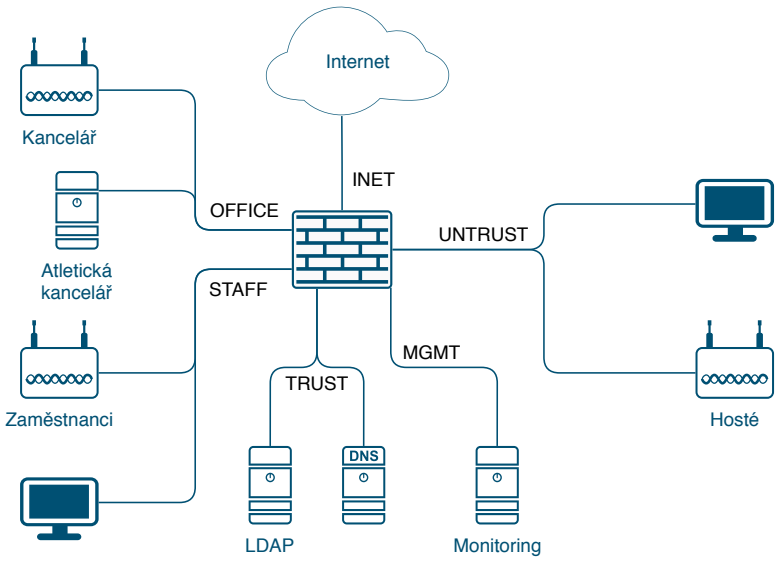
3.3 Ochrana sítě

Na hranici sítě bude nasazen firewall v kombinaci se systémem detekce (prevence) průniku (IDS/IPS). Vzhledem k tomu, že tímto zařízením projde většina komunikace, je takové umístění ideální. Navíc tato kombinace umožňuje IDS ovlivňovat chování firewallu.

Vybrané řešení spoléhá na kombinaci utility Shorewall a IDS Suricata. Shorewall slouží k manipulaci s pravidly firewallu. Suricata poté analyzuje provoz a dále omezuje chování firewallu na základě získaných dat.

3.3.1 Firewall

Shorewall dělí konfiguraci na části týkající se síťových rozhraní, zón, politik a pravidel. Diagram 3.2 zobrazuje rozdělení sítě do zón. Takto navržené zóny jsou poté nakonfigurovány ve firewallu.



Obrázek 3.2. Rozdělení sítě do bezpečnostních zón

Politiky definují výchozí chování firewallu. Proto jsou nastaveny, na odmítání spojení a v případě komunikace ze zón untrust a internet jsou pakety rovnou zahazovány (výpis 3.1). Výjimkou je povolení komunikace ze zón untrust, staff a office do internetu. Vzhledem k tomuto nastavení pravidla poté slouží jako whitelist pro povolení konkrétní komunikace. Příkladem je třeba povolení SSH z management zóny nebo povolení připojení k DNS serveru v zóně trust (viz výpis 3.2).

```
#SOURCE          DESTINATION          POLICY     LOGLEVEL
untrust          inet                 ACCEPT
staff            inet                 ACCEPT
office           inet                 ACCEPT
untrust          all                  DROP       info
inet             all                  DROP       info
all              all                  REJECT     info
```

Výpis 3.1. Nastavení výchozího chování firewallu

```
#ACTION      SOURCE               DESTINATION
DNS(ACCEPT)  office               trust:<dns_srv_ip>
DNS(ACCEPT)  staff                trust:<dns_srv_ip>
DNS(ACCEPT)  mgmt                 trust:<dns_srv_ip>
DNS(ACCEPT)  $FW                  trust:<dns_srv_ip>
DNS(ACCEPT)  trust:<dns_srv_ip>   inet

SSH(ACCEPT)  mgmt                 office
SSH(ACCEPT)  mgmt                 staff
SSH(ACCEPT)  mgmt                 trust
SSH(ACCEPT)  mgmt                 $FW
```

Výpis 3.2. Ukázka pravidel firewallu

V nastavených pravidlech je akce povolení komunikace (`ACCEPT`) často nahrazena akcí `NFQUEUE`. Toto nastavení souvisí s integrací IDS a je vysvětleno dále.

3.3.2 Detekce/prevence průniku

Úkolem IDS Suricata je analýza probíhající komunikace na základě definovaných pravidel. Pro analýzu komunikace lze využít pravidel vytvářených různými výzkumnými týmy nebo lze vytvořit pravidla vlastní. Vzhledem k tomu, že IDS slouží jako nadstavba firewallu, je vhodnější nakonfigurovat všechna vlastní pravidla na firewallu. Tento přístup zajistí, že chování firewallu bude nastavováno pouze z jednoho místa a IDS bude dále analyzovat pouze povolenou komunikaci.

Jedním z možných způsobů integrace IDS Suricata s firewallem, který je využit v tomto řešení, je předávání pomocí speciální fronty. Tento způsob umožňuje filtrovat komunikaci na všech síťových rozhraních. Zároveň lze definovat, jaká komunikace bude pomocí IDS analyzována. Druhá možnost je nastavení do módu odposlechu. V takovém případě je IDS napojen na dvě síťová rozhraní na linkové vrstvě a stará se o analýzu a kopírování komunikace mezi rozhraními. Tato varianta ke své práci nevyžaduje nastavení firewallu.

Pro nastavení IDS Suricata do IPS módu stačí pouze spustit program s parametrem `-q <číslo fronty>`, který definuje, jakou frontu má IDS použít. Předávání vybraného

provozu je poté definováno pomocí pravidel firewallu. K uložení komunikace do fronty je použita akce `NFQUEUE`. IPS u všech takto předaných paketů rozhoduje, zda budou přijaty či zahozeny. Takové chování je možné zmírnit konfigurací „NFQ módu“ (výpis 3.3). Použití NFQ módu `repeat` umožňuje vrátit paket k vyhodnocení podle všech pravidel firewallu. Mód `route` předá vyhodnocený paket do jiné fronty.

```
nfq:
  mode: accept
```

Výpis 3.3. Nastavení NFQ módu aplikace Suricata

Informace o činnosti IDS lze získat několika způsoby. Suricata nabízí logování veškeré aktivity do systémového logu, logování vybraných informací ve formátu „Extensible Event Format“ (EVE) nebo logování do textových souborů. Výpis 3.4 ukazuje nastavení logování upozornění (fast log), statistik, zahozených paketů a komunikace specifických protokolů.

3.4 Certifikační autorita

Certifikáty umožňují jak utajení informace, tak ověření původu dat. Z těchto důvodů jsou základem šifrované komunikace.

Toto řešení používá privátní infrastrukturu veřejných klíčů (PKI). To umožňuje vystavit certifikáty na míru konkrétním potřebám společnosti. Pro ověření platnosti konkrétního certifikátu musí ověřovatel mít k dispozici certifikát kořenové certifikační autority (CA). V případě privátní PKI to znamená, že na každé zařízení musí být manuálně nainstalován kořenový certifikát. Popisované řešení je určeno pro použití v lokální síti, a tedy tato vlastnost není omezením.

Základ PKI je tvořen kořenovou a mezilehlou autoritou. Výpis 3.5 popisuje přípravu prostředí pro vytvoření autorit. Soubory CA jsou umístěny v adresáři `CADIR=/root/CA`. Práce s certifikáty je prováděna pomocí programu „OpenSSL“.

```
mkdir "$CADIR"
cd $CADIR
mkdir private newcerts crl certs intermediate
chmod 700 private
touch index.txt
echo 1000 > serial

mkdir intermediate/{certs,crl,csr,newcerts,private}
chmod 700 intermediate/private
touch intermediate/index.txt
echo 1000 > intermediate/serial
echo 1000 > intermediate/crlnumber
```

Výpis 3.5. Příprava certifikační autority

Výpis 3.6 zobrazuje postup vytvoření kořenové CA. Nejdříve je vygenerován privátní klíč kořenové CA. Poté následuje vytvoření „self-signed“ certifikátu autority.

V případě mezilehlé autority (výpis 3.7) je po vygenerování privátního klíče mezilehlé CA vytvořen požadavek na podepsaní certifikátu (CSR). CSR je poté předán kořenové autoritě k vytvoření certifikátu.

```
outputs:
  - fast:
      enabled: yes
      filename: fast.log
      append: yes
      filetype: regular

  - http-log:
      enabled: yes
      filename: http.log
      append: yes

  - dns-log:
      enabled: yes
      filename: dns.log
      append: yes
      filetype: regular

  - stats:
      enabled: yes
      filename: stats.log
      append: yes
      totals: yes
      threads: no
      null-values: no

  - drop:
      enabled: yes
      filename: drop.log
      append: yes
      filetype: regular

  - tls-log:
      enabled: yes
      filename: tls.log
      append: yes
```

Výpis 3.4. Nastavení výstupů IDS

```
cd $CADIR
openssl genrsa -aes256 -out private/ca.key.pem 4096
chmod 400 private/ca.key.pem

openssl req -config openssl.cnf \
    -key private/ca.key.pem \
    -new -x509 -days 3650 -sha256 -extensions v3_ca \
    -out certs/ca.cert.pem
chmod 444 certs/ca.cert.pem
```

Výpis 3.6. Vytvoření kořenového certifikátu

Výstupy předváděných příkazů jsou ovlivněny konfigurací jednotlivých autorit. Výpis 3.8 zobrazuje základní nastavení CA. Většina příkazů se týká adresářové struk-

```
cd $CADIR
openssl genrsa -aes256 \
    -out intermediate/private/intermediate.key.pem 4096
chmod 400 intermediate/private/intermediate.key.pem

openssl req -config intermediate/openssl.cnf -new -sha256 \
    -key private/intermediate.key.pem \
    -out intermediate/csr/intermediate.csr.pem

openssl ca -config openssl.cnf -extensions v3_intermediate_ca \
      -days 3650 -notext -md sha256 \
      -in intermediate/csr/intermediate.csr.pem \
      -out intermediate/certs/intermediate.cert.pem
chmod 444 intermediate/certs/intermediate.cert.pem
```

Výpis 3.7. Vytvoření mezilehlého certifikátu

tury. Dále tato sekce nastavuje délku platnosti vystavených certifikátů a revokačních listů (`default_days` a `crl_default_days`), hashovací algoritmus, politiku podepisování, atd. Pro podpis mezilehlých certifikátů je použita striktní politika (viz výpis 3.9), podpisy koncových certifikátů uplatňují politiku volnější (viz výpis 3.10).

```
[ ca ]
default_ca = CA_default

[ CA_default ]
dir               = /root/CA
certs             = $dir/certs
crl_dir           = $dir/crl
new_certs_dir     = $dir/newcerts
database          = $dir/index.txt
serial            = $dir/serial
RANDFILE          = $dir/private/.rand

private_key       = $dir/private/ca.key.pem
certificate       = $dir/certs/ca.cert.pem

crlnumber         = $dir/crlnumber
crl               = $dir/crl/ca.crl.pem
crl_extensions    = crl_ext
default_crl_days  = 30

default_md        = sha256

name_opt          = ca_default
cert_opt          = ca_default
default_days      = 375
preserve          = no
policy            = policy_strict
```

Výpis 3.8. Základní nastavení CA

```
[ policy_strict ]
countryName             = match
stateOrProvinceName     = match
localityName            = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional
```

Výpis 3.9. Striktní politika vydávání certifikátů

```
[ policy_loose ]
countryName             = match
stateOrProvinceName     = match
localityName            = optional
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional
```

Výpis 3.10. Volná politika vydávání certifikátů

3.5 Jmenné služby

V počítačové síti jsou nasazeny služby DNS a DHCP. Pro správu identit je použita služba Lightweight Directory Access Protocol (LDAP). LDAP umožňuje uchovávat informace o zaměstnancích a provádět jejich autentizaci vůči používaným systémům. Výhodou LDAP je podpora napříč různými systémy a aplikacemi. S využitím této vlastnosti lze uživatelům podrobně nastavit oprávnění a poté je autorizovat k jednotlivým úkonům.

3.5.1 DHCP a DNS

Síťová rozhraní jsou automaticky nastavována pomocí protokolu DHCP (Dynamic Host Configuration Protocol). Pro tyto účely je využívána služba ISC dhcpd. Výpis 3.11 ukazuje základní nastavení vlastností DHCP serveru. K vidění jsou možnosti společné pro všechny zařízení vnitřní sítě.

```
option domain-name "atletika.kolin";
option domain-name-servers 192.168.2.2;

default-lease-time 86400;
max-lease-time 604800;

authoritative;
```

Výpis 3.11. Nastavení DHCP serveru

DNS server se poté stará o překlady jmen serverů v lokální síti. Vybrané řešení je postaveno na serveru BIND9, který se chová jako autoritativní pro doménu `atletika.kolin`.

3.5.2 Adresářové služby

Popisované řešení využívá implementaci „OpenLDAP“ protokolu LDAP a grafickou aplikaci „LDAP Account Manager“ pro snazší administraci uživatelských účtů.

Samotná manipulace s LDAP serverem poté probíhá pomocí utilit jako ldapsearch, ldapmodify, ldapadd atd. Data jsou vyměňována ve formátu LDAP Data Exchange Format (LDIF). Je tedy možné mít konfiguraci připravenou v souborech a na server nahrát pouze potřebné změny.

Nejdříve je provedena změna domény a nastaveno logování pomocí příkazů ve výpisu 3.12. Nastavení logování na úroveň 480 zajistí zaznamenávání průběhu vyhledávání, vyhodnocování přístupových práv a konfigurace. Navíc budou zaznamenány probíhající operace ve formě statistik.

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: 480

dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=atletika,dc=kolin
-
replace: olcRootDN
olcRootDN: cn=admin,dc=atletika,dc=kolin
```

Výpis 3.12. Základní nastavení serveru LDAP

Ve výpisu 3.13 lze nahlédnout na ukázku konfigurace přístupových práv. První pravidlo umožní uživatelům prohledávání všech uživatelských profilů a úpravu svých profilů. Administrátorům pak toto pravidlo umožňuje správu uživatelů. Pravidlo druhé umožňuje administrátorům práci se skupinami. A poslední pravidlo zakazuje vše, co nebylo povoleno dříve.

```
add: olcAccess
olcAccess: {2}to dn.children="ou=people,dc=atletika,dc=kolin"
        by dn.exact="cn=search,dc=atletika,dc=kolin" read
        by group.exact="cn=admins,ou=groups,dc=atletika,dc=kolin" write
        by self write
        by users read
-
add: olcAccess
olcAccess: {3}to dn.children="ou=groups,dc=atletika,dc=kolin"
        by dn.exact="cn=search,dc=atletika,dc=kolin" read
        by group.exact="cn=admins,ou=groups,dc=atletika,dc=kolin" write
-
add: olcAccess
olcAccess: {4}to * by * none
```

Výpis 3.13. LDAP – přístupová práva

Protokol LDAP podporuje šifrování komunikace pomocí protokolu TLS. Na straně serveru lze šifrování nastavit pomocí příkazů ve výpisu 3.14.

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/certs/ca.cert
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/certs/ldap.atletika.kolin.cert
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/certs/ldap.atletika.kolin.key
-
add: olcTLSVerifyClient
olcTLSVerifyClient: allow
```

Výpis 3.14. LDAP – nastavení použití certifikátů

3.6 Monitoring sítě

Monitorovací server pravidelně získává data ze zařízeních v síti a umožňuje tak administrátorům udržovat si přehled o dění v síti.

V této implementaci byl vybráno řešení Zabbix. Zabbix umožňuje monitoring od celé sítě přes servery až po jednotlivé služby. Sběr dat z monitorovaného zařízení probíhá pomocí Zabbix agenta, SNMP nebo IPMI. Alternativně je možné použít skenování otevřených portů, ICMP nebo spouštět příkazy přes SSH.

Zabbix umožňuje provádět autentizaci uživatelů s využitím LDAPu. Autorizaci poté server provádí sám. Granularita oprávnění umožňuje zcela detailní nastavení povolených akcí. Nevýhodou je chybějící možnost automatického importu uživatelů z databáze LDAP.

Ke komunikaci s monitorovanými zařízeními je využit Zabbix agent. Výměna dat mezi agentem a serverem je šifrovaná, šifrování probíhá za využití certifikátů. Výpis 3.15 ukazuje zabezpečení agenta a nastavení šifrované komunikace. Konfigurace zakazuje agentu běh s právy uživatele root a spouštění vzdálených příkazů. Komunikace je povolená pouze se serverem `nms.atletika.kolin` a je povoleno pouze šifrované spojení.

```
EnableRemoteCommands=0
LogRemoteCommands=1

Server=nms.atletika.kolin

AllowRoot=0
User=zabbix

TLSConnect=cert
TLSAccept=cert
TLSCAFile=/home/zabbix/zabbix_ca_file
TLSServerCertIssuer=<Atletika Kolin CA>
TLSServerCertSubject=<nms.atletika.kolin subject>
TLSCertFile=/home/zabbix/zabbix_agentd.crt
TLSKeyFile=/home/zabbix/zabbix_agentd.key
```

Výpis 3.15. Konfigurace Zabbix agenta

Kapitola 4
Ověření

Tato kapitola shrnuje nalezené slabiny testované infrastruktury a připomíná definované požadavky. Cílem kapitoly je ověření, zda vybraná opatření popisované slabiny odstranila a jsou-li uveditelná do reálného provozu.

Z hlediska provozu byly na infrastrukturu kladeny minimální požadavky. Konkrétní požadavky se týkaly pouze kvality připojení. V případě bezdrátového připojení nebyla vytvořena mapa kvality signálu, ale kontrola proběhla za běžného provozu na stanovištích, která odpovídají běžnému rozmístění rozhodčích v poli. Během celého testu nebyly hlášeny žádné problémy s připojením. V případě pevného připojení je vyžadována rychlost řádově v Gb/s pouze pro propojení cílové kamery a počítače pro obsluhu této kamery. Přímé propojení takových rychlostí dosahuje, při zapojení do stávající infrastruktury je rychlost o řád nižší. Vzhledem k tomu, že jak z technického, tak z bezpečnostního hlediska je přímé propojení cílové kamery a obslužného počítače nejlepším řešením, lze i tento požadavek považovat za splněný.

U zařízení byly vypnuty nepoužívané služby. To umožňuje zúžit případný vektor útoku. Výpis 4.1 například zobrazuje kontrolu otevřených portů u tiskárny Brother.

```
Nmap scan report for 192.168.1.3
Host is up (0.012s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE    VERSION
23/tcp    open  telnet     Brother/HP printer telnetd
80/tcp    open  http       Brother/HP printer httpd 1.20
443/tcp   open  ssl/http   Brother/HP printer httpd 1.20
515/tcp   open  printer
631/tcp   open  http       Brother/HP printer httpd 1.20
Service Info: Device: printer
```

Výpis 4.1. Kontrola otevřených portů u tiskárny

Další požadavky nebyly splnitelné na současné infrastruktuře. Před dokončením práce nebylo možné získat zařízení odpovídajících vlastností a možností. Vzhledem k faktu, že nové systémy budou virtualizovány, byla implementace, která není proveditelná na stávajícím hardwaru, vytvořena a otestována ve virtuálním prostředí. Tím je zároveň splněn požadavek na provoz aplikací na oddělených strojích.

Nasazení firewallu na hranici sítě v kombinaci s analýzou provozu splňuje požadavky na segmentaci lokální sítě, oddělení od internetu a detekci průniku.

Nasazení služby LDAP a webového rozhraní pro správu této služby umožňuje přehledně spravovat uživatelské účty, udržovat si potřebné informace o uživatelích a zařazovat je do skupin. Napojení uživatelských systémů na tyto služby pak umožňuje navázání práv na uživatelské skupiny a přihlašování uživatelů k těmto systémům. Tím jsou splněny veškeré požadavky na uživatelské účty.

Závěr

Hlavním cílem bakalářské práce bylo odstranění bezpečnostních slabin počítačové sítě společnosti T. J. Sokol Kolín – Atletika. Bezpečnostní slabiny byly úspěšně identifikovány. Následně bylo implementováno několik opatření na odstranění těchto slabin.

Nejdříve byl zanalyzován stav počítačové sítě. Pro postup byl využit The Penetration Testing Execution Standard. Proběhla identifikace zařízení v síti a přístupových bodů. Na základě získaných informací byl sestaven model hrozeb. K modelování hrozeb byla využita metodika STRIDE. Následně byly definovány požadavky na bezpečnost a na provoz. Konkrétně bylo požadováno oddělení lokální sítě od internetu firewallem a segmentace lokální sítě. Dále byly kladeny nároky na centrální správu identity a omezení privilegií. V neposlední řadě byl požadován systém pro monitorování lokální sítě a systém detekce/prevence narušení.

Dále proběhl návrh opatření pro eliminaci hrozeb. Konkrétně byla v rámci této práce vyřešena správa uživatelů pomocí jmenných služeb. Celkovou ochranu infrastruktury zajistilo nasazení firewallu v kombinaci se systémem prevence průniku. A v neposlední řadě řešení popisuje nasazení monitorovacího systému, což umožňuje udržovat si přehled o stavu počítačové sítě. Vybraná opatření byla implementována a ověřena ve virtuálním prostředí.

Nad rámec této práce bude následovat nasazení řešení pro vzdálený přístup. Následně proběhne vyhodnocení použitelnosti nasazených opatření v ostrém provozu. Ve výhledu je také nahrazení hesel za vhodnější formu autentizace.

Literatura

[1] *The Penetration Testing Execution Standard* [online]. Penetration Testing Execution Standard Group, 2014 [cit. 2020-03-23]. Dostupné z: http://www.pentest-standard.org/index.php/Main_Page.

[2] *ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary*. 5. Geneva: International Organization for Standardization, 2018.

[3] ADAM, Shostack. *Threat modeling: designing for security* [online]. 1. New York: John Wiley & Sons, Incorporated, 2014 [cit. 2020-04-21]. ISBN 9781118809990. Dostupné z: Proquestu.

[4] PEÑA, Javier Fernández-Sanguino. *Securing Debian Manual* [online]. 3.19. Debian Documentation Project, 2017 [cit. 2020-05-02]. Dostupné z: https://www.debian.org/doc/manuals/securing-debian-manual/index.en.html.

Příloha A
Seznam zkratek

CA	Certifikační autorita
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
OS	Operační systém
OSINT	Open Source Intelligence
PKI	Public Key Infrastructure
PTES	The Penetration Testing Execution Standard
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WPA2	Wi-Fi Protected Access 2

Příloha B
Obsah přiloženého média

- `readme.txt` ..... stručný popis obsahu média
- `src`
  - `conf` ..... zdrojové kódy implementace
  - `test` ..... zdrojové soubory analýzy
  - `thesis` ..... zdrojová forma práce ve formátu TEX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF