Príloha č. 2

TECHNICKÁ ŠPECIFIKÁCIA INFORMAČNÉHO SYSTÉMU CARDIS

1. Vývoj a prevádzka informačného systému CARDIS

1.1. Informačný systém CARDIS je komplexný softvérový nástroj určený na podporu činnosti sociálnych služieb a je navrhnutý s dôrazom na bezpečnosť, spoľahlivosť a súlad s medzinárodnými štandardmi. Tento systém vyvíja a zároveň ako jediná prevádzkuje spoločnosť Chytrá organizace s.r.o., so sídlom Ostravská 94/57, 748 01 Hlučín, Česká republika, IČO: 04728629 (ďalej len „Spoločnosť"). Spoločnosť zodpovedá za celý životný cyklus systému – od návrhu architektúry a vývoja softvéru, cez správu serverovej infraštruktúry, až po technickú podporu. Všetky procesy prebiehajú v súlade s certifikáciou ISO/IEC 27001:2023, ktorou je Chytrá organizace s.r.o. držiteľom, čo zaručuje vysoký štandard informačnej bezpečnosti a ochrany dát.

2. Informačná bezpečnosť – certifikácia ISO/IEC 27001

2.1. Spoločnosť je držiteľom medzinárodnej certifikácie ISO/IEC 27001:2023, ktorá potvrdzuje zavedenie a udržiavanie systému riadenia informačnej bezpečnosti (ISMS) v súlade s aktuálnymi normami.

2.2. Certifikácia bola vydaná dňa 10. 12. 2024 a je platná do 09. 12. 2027.

2.2.1. Registračné číslo certifikátu: 1225/2024/SC/BI

2.2.2. Certifikačná autorita: Systémové certifikace s.r.o., Lipová 433, Svinov, 721 00 Ostrava, Česká republika

Certifikácia zahŕňa nielen zabezpečenie technickej infraštruktúry, ale aj procesné riadenie, školenie zamestnancov, riadenie prístupov a krízové scenáre.

3. Primárne dátové centrum – Ostrava (České Radiokomunikace a.s.)

3.1. Primárna infraštruktúra sa nachádza v dátovom centre Českých Radiokomunikácií v Ostrave, kde Spoločnosť prevádzkuje vlastný 1/2 rack (22U). Rack je fyzicky zabezpečený vlastným zámkom, prístup majú iba tri osoby (konateľ, riaditeľ a hlavný programátor) pomocou čipovej karty a individuálneho kódu k alarmu.

3.2. Dátové centrum je:

3.2.1. nepretržite fyzicky strážené a monitorované,

3.2.2. napojené na centrálny pult ochrany, Hasičský záchranný zbor a Políciu ČR,

3.2.3. umiestnené v nezáplavovej a bezletovej zóne,

3.2.4. napájané dvoma nezávislými vetvami z ČEZ,

3.2.5. pripojené viacerými trasami optických vlákien do sietí NIX a SIX.

3.3. Sieťová infraštruktúra zahŕňa dva oddelené switche – jeden pre verejné IP adresy (10Gbit), druhý pre internú správu (1Gbit) – a záložný tretí switch. Perimetrickú ochranu, aktívne VPN a aplikačnú bezpečnosť zabezpečuje firewall novej generácie WatchGuard.

3.4. Použité servery značiek HPE a Lenovo ThinkSystem majú redundantné napájanie, SSD/NVMe disky v poli RAID 5, 10Gbit sieťové karty a vzdialenú správu (iLO/iDRAC). Fyzické kontroly prebiehajú mesačne, vzdialené dvakrát mesačne. Stav infraštruktúry je monitorovaný s upozorneniami cez e-mail. V rámci lokality je pripravený záložný server pre prípad zlyhania primárneho uzla.

4. Záložné dátové centrum – Brno

4.1. Záložná infraštruktúra je prevádzkovaná v dátovom centre v Brne s rovnakými bezpečnostnými a prevádzkovými parametrami ako v Ostrave. Spoločnosť tu využíva 1/4 rack (10U) vybavený nasledujúcimi prvkami:

4.1.1. 1Gbit switch,v

4.1.2. server HPE DL360 Gen10 s virtualizovaným prostredím,

4.1.3. NAS úložisko Synology s kapacitou 64 TB.

4.2. Dáta z Ostravy sú do Brna replikované online. Záložné prostredie je prístupné iba na čítanie a slúži na exporty a núdzové obnovy.

5. Zálohovanie dát

5.1. Zálohovacia stratégia je navrhnutá s dôrazom na redundanciu, bezpečnosť a kontrolu integrity:

5.1.1. zálohovanie prebieha 4× denne (00:00, 06:00, 12:00, 18:00),

5.1.2. dáta sú ukladané na 4 NAS zariadenia umiestnené v oddelených lokalitách (2× Hlučín, Ostrava, Brno),

5.1.3. zariadenia nie sú dostupné z verejného internetu, sú chránené firewallom a prístupné iba z definovaných IP adries,

5.1.4. NAS servery majú redundantné napájanie, sú pravidelne aktualizované a monitorované, prebieha kontrola konzistencie a scrubbing,

5.1.5. prístup majú iba dve osoby (konateľ, hlavný programátor),

5.1.6. zálohy sú šifrované pomocou AES-256 a prenášané výhradne cez SSH,

5.1.7. všetky zálohy sú nemenné (immutable),

5.1.8. obnova záloh je testovaná týždenne,

5.1.9. retenčná doba záloh je 365 dní, zálohy sa denne rotujú.

6. Serverová prevádzka a monitoring

6.1. Všetky servery bežia na platforme Red Hat Enterprise Linux (RHEL), pričom systémové aktualizácie sú aplikované každých 14 dní. Systémová architektúra je chránená firewallom WatchGuard.

6.1.1. Verejne sú prístupné iba porty 80 (HTTP) a 443 (HTTPS).

6.1.2. Administratívny prístup (napr. SSH) a ping sú dostupné iba cez VPN.

6.1.3. Všetky prístupy cez SSH sú auditované, rovnako ako ostatné systémové udalosti.

6.2. Prevádzkový monitoring sleduje stav CPU, RAM, disku, sieťových rozhraní aj aplikačných služieb. V prípade incidentu sú odosielané notifikácie prostredníctvom SMS.

7. Technická špecifikácia IS CARDIS

7.1. Systém je vyvíjaný na technologickom stacku:

7.1.1. HTML5,

7.1.2. CSS3,

7.1.3. PHP,

7.1.4. JavaScript,

7.1.5. VueJS,

7.1.6. AJAX,

7.1.7. databáza MariaDB.

7.2. Systém beží na dedikovaných serveroch bez kvót na diskový priestor. Nasadzovanie aktualizácií prebieha mesačne v období 15.–25. dňa daného mesiaca, zvyčajne bez výpadku, s maximálnou dĺžkou do 1 minúty. Používatelia sú o aktualizáciách informovaní po prihlásení.

8. Zabezpečenie hesiel

8.1. Systém vynucuje silné politiky pre tvorbu hesiel:

8.1.1. Minimálna dĺžka hesla: 8 znakov.

8.1.2. Povinné prvky: malé a veľké písmená, číslice, špeciálny znak.

8.1.3. Heslá sú ukladané v hashovanej podobe.

8.1.4. Systém upozorňuje používateľa na slabé heslo a vyžaduje jeho zmenu do 30 prihlásení. Po prekročení tohto limitu je účet zablokovaný.

9. Zákaznícka podpora

9.1. Používatelia systému majú prístup k viacúrovňovej zákazníckej podpore:

9.1.1. Interný ticketovací systém – na bežné požiadavky, zmeny a chyby,

9.1.2. Telefonická podpora,

9.1.3. SMS podpora pre kritické incidenty.

10. Kompatibilita a sieťová komunikácia

10.1. Systémové požiadavky na prehliadač:

10.1.1. podporované: Google Chrome (odporúčané),

10.1.2. nepodporované: Mozilla Firefox, Apple Safari, Microsoft Edge, Internet Explorer.

10.2. Sieťová komunikácia:

10.2.1. všetky dátové prenosy prebiehajú výhradne cez HTTPS (port 443),

10.2.2. používa sa platný SSL certifikát vydaný dôveryhodnou autoritou,

10.2.3. nekompatibilné alebo nezabezpečené protokoly (napr. HTTP) nie sú systémom akceptované.

11. Interná bezpečnostná politika

11.1. Spoločnosť aplikuje vlastné interné bezpečnostné štandardy, ktoré reflektujú princípy ISO 27001 a zabezpečujú ochranu vývoja aj prevádzky systému:

11.1.1. Koncové zariadenia:

a) všetci zamestnanci používajú zariadenia s Apple macOS,

b) systémy sú chránené používateľským heslom a biometrickým overením (Touch ID),

c) aktívne šifrovanie disku pomocou FileVault.

11.1.2. Práva a prístupy:

a) prístup k zdrojovému kódu a vývojovým nástrojom majú výhradne programátori,

b) ostatní zamestnanci majú prístup len ku klientskému rozhraniu a testovacím inštanciám.

11.1.3. Kyberbezpečnostné vzdelávanie:

a) všetci zamestnanci absolvujú školenie v oblasti kyberbezpečnosti každý štvrťrok,

b) školenie zahŕňa testy znalostí, simulované phishingové útoky a obnovu hesiel.

11.1.4. Segmentácia siete:

a) interná sieť je rozdelená na vývojovú (pre prístup k testovacím a produkčným prostrediam) a návštevnícku (oddelená Wi-Fi),

b) operačné systémy Windows nie sú v internom prostredí povolené.