Technická a organizační opatření Českých Radiokomunikací

1. Organizace dokumentu a definice pojmů

V tomto dokumentu jsou popsány organizační a technická opatření přijatá CRA pro jednotlivé služby a produkty.

Není-li uvedeno jinak, mají definovaná slova a spojení použitá v tomto dokumentu následující význam:

„CRA“	znamená společnost České Radiokomunikace a. s.
„zákazník“	Každý kdo užívá službu poskytovanou CRA, na základě smlouvy.
„zákaznická data“ nebo „zákaznické údaje“	Data, nebo údaje, poskytnuté zákazníkem.
„CRA Serverhousing“	Služba CRA, definovaná ve smlouvě.
„datová centra“	Prostory určené pro umístění ICT technologií.
„cloudová infrastruktura“	Soubor IT a síťových technologií, potřebný pro poskytování cloudových služeb.
„CRA Business Cloud“	Služba CRA, definovaná ve smlouvě.
„CRA Media Cloud“	Služba CRA, definovaná ve smlouvě.
„virtualizační infrastruktura“	Infrastruktura poskytující výpočetní výkon a kapacitu pro ukládání dat, prostřednictvím virtualizační vrstvy.
„platforma“	Soubor IT prostředků, definovaný svým účelem.

2. Zabezpečení jako priorita

CRA vyvíjí maximální úsilí k tomu, aby infrastruktura, kterou nabízí a provozuje, byla maximálně bezpečná. Je to klíčové nejen pro nás a naše zákazníky, ale i pro stát. Bezpečnost našich služeb, a dostupnost, integritu a obnovitelnost zpracovávaných dat považujeme za důležitou prioritu a vysokou a přidanou hodnotu pro naše zákazníky.

Z našeho přístupu k bezpečnosti jako prioritě vychází bezpečnost datových center a telekomunikační infrastruktury. Na to navazují cloudové ekosystémy poskytující výpočetní výkon a specializované OTT/HbbTV aplikace. Každá z těchto nadstavbových platforem disponuje dalšími úrovněmi ochrany.

Z našeho pohledu se jedná o komplexní soubor opatření, kterému věnujeme mimořádnou pozornost. Zahrnuje fyzické, procesní a technologické prostředky.

3. Certifikovaná kvalita:

Certifikace společnosti CRA

Pro zajištění vysokého standardu bezpečnosti poskytovaných služeb se České Radiokomunikace a. s. certifikují. Příkladem takových certifikací jsou například mezinárodní standardy ISO/IEC 27001:2013 pro ICT služby, ICT cloudové služby, telekomunikační služby a rovněž služby spojené s televizním a rozhlasovým vysíláním. Ve stejných oblastech jsme byli certifikováni také podle ISO 9001:2008, ISO/IEC 20000-1:2011, ISO 14001:2004 a ISO 50001:2011 a osvědčení Národního bezpečnostního úřadu jak pro seznamování se s utajovanými informacemi, tak pro poskytování nebo vznik utajovaných informací ve smyslu zákona č. 412/2005 Sb. pro stupeň utajení „tajné“. To na naši společnost klade zákonné požadavky na zajištění jak fyzické, tak kybernetické bezpečnosti. Všechny certifikace už více než 10 let nepřetržitě udržujeme a pravidelně obnovujeme.

Jsme společnost kontrolovaná ze strany orgánů veřejné moci v oblastech krizového řízení, kybernetické bezpečnosti, ochrany osobního údajů a ochrany utajovaných informací. Pro datová centra provádíme audit TIA v souladu s normou TIA-942.

Certifikace zaměstnanců CRA

Klíčoví zaměstnanci jsou držitelé osvědčení fyzické osoby až do stupně utajení „tajné“. Expertní zaměstnanci jsou certifikováni výrobci na provozované technologie.

4. Fyzická infrastruktura a datová centra – CRA Serverhousing

Fyzická bezpečnost je společným jmenovatelem pro všechny služby a vede napříč produktovým portfoliem. Uplatňováním definovaných zásad fyzického zabezpečení chráníme umístěná zařízení našich zákazníků na našich objektech před neoprávněným zásahem, poškozením, nebo zcizením. Stejnou měrou chráníme i naše vlastní technologie, benefitů fyzického zabezpečení využívají jak přenosové technologie a vysílací systémy, tak i cloudové systémy, které tvoří základnu pro nadstavbové mediální služby typu OTT/HbbTV.

Společnost CRA má v souladu s požadavkem na zajištění bezpečnosti datových center vypracovanou dokumentaci popisující systém opatření z oblasti fyzické bezpečnosti, která mají neoprávněné osobě zabránit nebo ztížit přístup k technologiím a datům umístěným v datových centrech společnosti, popřípadě přístup nebo pokus o něj zaznamenat. Rozsah opatření fyzické bezpečnosti je standardizován dle prováděcích předpisů Národního bezpečnostního úřadu a odpovídá druhé nejvyšší bezpečnostní třídě – BT3. Definovaná opatření fyzické bezpečnosti jsou aplikována v rámci celého objektu datového centra. Objekt, kde se nachází datové centrum, spadá do kritické infrastruktury státu. Z toho plyne povinnost splnění vyšších než běžných bezpečnostních a provozních standardů.

Zajištění fyzické bezpečnosti umístěných dat a technologií je realizováno jak na úrovni technologické (dvoufaktorové systémy řízení přístupu s jednoznačnou autorizací osob

(RFID + biometrika), kamerové systémy se záznamem, pohybová čidla, atd.), tak na úrovni personální (bezpečnostní služba a pracoviště dohledů bezpečnosti v režimu 24x7). Všichni pracovníci datového centra splňují požadavky NBÚ minimálně pro úroveň utajení „Vyhrazené“.

V rámci služby CRA Serverhousing datových center pracovníci CRA nespravují technologie zákazníků ani nemají přístup k jejich datům. Data o kontaktních osobách zákazníků jsou získávána pouze pro účel jednoznačné identifikace osob při vstupu do objektu a definovaných prostor. Tato data jsou sbírána a uchovávána plně v souladu s požadavky Úřadu pro ochranu osobních údajů. Technologie, na kterých jsou data uchovávána, jsou umístěny v prostorách s omezeným přístupem a se zvýšenou mírou ostrahy.

Naplnění a dodržování úrovně bezpečnosti a ochrany technologií a dat je pravidelně auditována nezávislými orgány a auditory. Konkrétně se jedná o Národní bezpečnostní úřad, Úřad pro ochranu osobních údajů, Ministerstvo průmyslu a obchodu, audit TIA na soulad s normou TIA-942.

5. Cloudová infrastruktura.

Cloudová infrastruktura je poskytována buď jako konečná služba našim zákazníkům, nebo je využívána, jako infrastruktura pro poskytování služeb s vyšší přidanou hodnotou, kde zákazník čerpá její benefity jen nepřímo, prostřednictvím jiné služby. Z důvodů diverzifikace provozu existují dva ucelené systémy, a to generický, infrastrukturní CRA Business Cloud a mediálně orientovaná platforma CRA Media Cloud Infrastructure.

5.1. Business Cloud

5.1.1. Přístup k fyzickému prostředí

Platforma CRA Business Cloud je provozována ve fyzicky odděleném prostředí (privátním sále) datového centra s řízeným přístupem. Přístup do tohoto sálu je omezen na vybrané zaměstnance poskytovatele, s tím, že přístupy další osob jsou přípustné pod dohledem a po schválení.

Prostor datového sálu je trvale sledovaný záznamovým zařízením.

Záznamy jsou uchovávány v souladu s platnou legislativou.

5.1.2. Přístup k virtualizační infrastruktuře

Platforma CRA Business Cloud je spravována interní skupinou poskytovatele, případně ve spolupráci s externím dodavatelem, který je povinen dodržovat pravidla zabezpečení ve smyslu článku 10 tohoto dokumentu. CRA implementuje řadu omezení v přístupu k virtualizační infrastruktuře. Přístup k virtualizační infrastruktuře neobsahuje přístup k zákaznickým datům.

Mezi tato bezpečnostní opatření patří:

- Omezení přístupu na zaměstnance poskytovatele a na přesně definované osoby zastupující dodavatele.
- Přístup k virtualizační infrastruktuře je umožněn pouze ze zabezpečených sítí poskytovatele.

- Logování veškeré aktivity prováděné v rámci virtualizační infrastruktury.
- Monitoring virtualizační infrastruktury prostřednictvím dohledových systémů poskytovatele.
- Přístupy třetích stran k virtualizační infrastruktuře jsou možné pouze po schválení interní autoritou poskytovatele. Tato schválení jsou evidována. Přístupy jsou asistovány zaměstnanci poskytovatele.
- Přístupová práva jsou nastavena pouze oprávněným a relevantním zaměstnancům.
- Je nastavena konkrétní politika hesel vycházející z aktuální nejlepší praxe na trhu.
- Je vyžadována změna hesla v předem nastaveném intervalu.

5.1.3. Přístup k datové struktuře

Přístup k datové struktuře platformy CRA Business Cloud, včetně zákaznických dat, je možný pouze skrze virtualizační platformu. Aktivity v této platformě podléhají omezením uvedeným v článcích 4.1.1 a 4.1.2 tohoto dokumentu.

Abychom zamezili přístupu k datovým strukturám platformy, implementovali jsme nad rámec výše uvedených omezení tato bezpečnostní opatření:

- Dohled na úrovni fyzických spojení s infrastrukturou.
- Jsou implementovány nástroje řízení přístupu na úrovni fyzické infrastruktury.
- Data jsou na fyzické úrovni šifrována a dostupná pouze v prostředí platformy.
- Změny v přístupu k infrastruktuře je možné pouze po schválení administrátorem platformy.
- Aktivity administrátorů jsou logovány.
- Prostředí je monitorováno.
- Přístupy jsou podmíněny přístupem k virtualizační platformě.

5.1.4. Řízení přístupu ke službám platformy

Přístup ke službám platformy slouží uživatelům platformy v jejím efektivním využívání. Pro řízení přístupu jsou implementovány nástroje řízení přístupu izolované pro tuto jedinou platformu.

Pro zajištění bezpečnosti při přístupu ke službám platformy jsou implementována tato opatření:

- Přístup je možný pouze z vyhrazených sítí či za použití VPN připojení.
- Každý přístup je omezen pouze na prostředí jediného zákazníka.
- Přístup je omezen na konkrétní vyjmenovaná prostředí daného zákazníka.
- Změna rozsahu přístupu je možná pouze po autorizaci administrátorem platformy a to pouze v rozsahu prostředích tohoto zákazníka.
- Je nastavena konkrétní politika hesel vycházející z aktuální nejlepší praxe na trhu.
- Je vyžadována změna hesla v předem nastaveném intervalu.
- Aktivity uživatelů jsou logovány.
- Prostředí je monitorováno na fyzické i virtuální úrovni za účelem bezpečného poskytování služby. Jedná se o monitoring technického stavu infrastruktury.

5.1.5. Kontrola přenosu dat

Platforma CRA Business Cloud má implementována opatření směřující k zabezpečení přenosu dat, včetně zákaznických dat, za účelem řízení kvality a bezpečnosti služby.

Tato opatření jsou:

- Izolace sítí sloužících pro řízení platformy, a to na úrovni L2 (LAN, VLAN).
- Využití šifrování pro přístup k řízení platformy.
- Využití systému IPS/IDS k ochraně přístupového bodu.
- Dohled infrastruktury.
- Zaznamenávání chování celkového systému v čase na úrovni přenosu dat.
- Analýza záznamů při neočekávaném chování.
- Žádné opatření se netýká samotného obsahu dat.

5.1.6. Šifrování osobních dat

Využíváním blokových systémů v rámci CRA Business Cloud, jako interní infrastruktury pro běh aplikací obsahujících osobní údaje, CRA zabezpečuje šifrování všech zde uložených dat. Data se tím pádem stávají „nečitelná“ pro všechny osoby, které nejsou oprávněny mít k nim přístup,“ tj. pro všechny osoby, které nemají k dispozici příslušné přístupové klíče.

5.1.7. Řízení dostupnosti

Platforma CRA Business Cloud je vytvořena s cílem zajistit vysokou míru dostupnosti celé platformy.

K zajištění této dostupnosti jsou implementována tato opatření:

- Redundance na úrovni jednotlivých fyzických prvků infrastruktury.
- Částečná redundance celků infrastruktury na globální úrovni a to do geograficky odděleného datového centra.
- Automatické procesy využití redundantních prvků s využitím automatického Fail-Over či Round-Robin/Load Balanced mechanismu.
- Monitoring všech prvků infrastruktury.
- Pravidelné vyhodnocování využívaných zdrojů a řízení změn rozsahu za účelem efektivního nakládání s prostředky a kontrolou funkčnosti automatického nahrazení části prostředků.
- Pravidelné vyhodnocování dohodnuté úrovně služeb a vzniklých incidentů.
- Pravidelné pořizování datových záloh do geograficky odděleného datového centra.
- Zálohujeme vždy celou infrastrukturu a data uchováváme v zašifrované podobě, po dobu definovanou ve smluvní dokumentaci se zákazníkem.

5.1.8. Dohled

Platforma CRA Business Cloud je v mnoha úrovních monitorována. Abychom zajistili znalost přesného stavu celé platformy, implementovali jsme tato pravidla pro monitoring:

- Provozní parametry platformy (např. dostupnost, výkonnost, disponibilní prostředky, síťové služby apod.) jsou v režimu 24x7 monitorovány on-line nástroji poskytovatele s okamžitým zobrazením stavu v rámci dohledového centra.
- Kritické incidenty klíčových prvků platformy jsou on-line sdíleny s dohledovými centry výrobců těchto prvků a automaticky vytváří incidentní případ.
- Monitoring je implementován na úrovních:
    - Fyzické infrastruktury – stavu jednotlivých prvků a jejich komponent.
    - Přenosové infrastruktury – stavu jednotlivých spojení v rámci infrastruktury, jejího využití a přehled o nenadálých situacích v rámci těchto spojení.
    - Virtualizační infrastruktury – stavu jednotlivých virtualizovaných objektech platformy a sledování nenadálých či neočekávaných stavů.
- Je pravidelně vyhodnocován stav klíčových prvků s cílem předejít neočekávaným incidentům.

5.2. CRA Media Cloud Infrastructure

5.2.1. Přístup k fyzickému prostředí

Platforma CRA Media Cloud Infrastructure je provozována v datovém sále s řízeným přístupem. Přístup do tohoto sálu je omezen na vybrané a autorizované osoby poskytovatele a vybrané a autorizované osoby zákazníků poskytovatele a provádí se pod dohledem.

Přístup k platformě je zabezpečen standardní zabezpečovací technickou datového sálu a je omezen pouze na zaměstnance poskytovatele. Přístup na fyzické úrovni je logovaný.

5.2.2. Přístup k virtualizační infrastruktuře

Platforma CRA Media Cloud Infrastructure je spravována interní skupinou poskytovatele a implementuje řadu omezení v přístupu k virtualizační infrastruktuře. Přístup k virtualizační infrastruktuře neobsahuje přístup k zákaznickým datům.

Mezi tato bezpečnostní opatření patří:

- Omezení přístupu na zaměstnance poskytovatele.
- Přístup je omezen pouze z interních sítí poskytovatele.
- Logování veškeré aktivity prováděné v rámci infrastruktury.
- Monitoring virtualizační infrastruktury prostřednictvím dohledových systémů poskytovatele.

5.2.3. Přístup k datové struktuře

Přístup k datové struktuře platformy CRA Media Cloud Infrastructure, včetně zákaznických dat, je možný pouze skrze virtualizační infrastrukturu. Aktivity v této infrastruktuře podléhají omezením uvedeným v článcích 4.2.1 a 4.2.2 tohoto dokumentu.

Abychom zamezili přístupu k datovým strukturám platformy, implementovali jsme nad rámec výše uvedených omezení tato bezpečnostní opatření:

- Dohled na úrovni fyzických spojení s infrastrukturou.
- Změny v přístupu k infrastruktuře je možné pouze po schválení administrátorem platformy a za fyzického přístupu k infrastruktuře.

- Aktivity administrátorů jsou logovány.
- Prostředí je monitorováno.
- Přístupy jsou podmíněny přístupem k virtualizační infrastruktuře.

5.2.4. Řízení přístupu ke službám platformy

Přístup ke službám platformy slouží uživatelům platformy v jejím efektivním využívání. Pro řízení přístupu jsou implementovány nástroje řízení přístupu izolované pro tuto jedinou platformu.

Pro zajištění bezpečnosti při přístupu ke službám platformy jsou implementována tato opatření:

- Přístup je možný pouze z vyhrazených a schválených sítí
- Změna rozsahu přístupu je možná pouze po autorizaci administrátorem platformy
- Aktivity uživatelů jsou logovány
- Prostředí je monitorováno na fyzické i virtuální úrovni za účelem bezpečného poskytování služby. Jedná se o monitoring technického stavu infrastruktury.

5.2.5. Kontrola přenosu dat

Platforma CRA Media Cloud Infrastructure má implementováno sledování přenášených dat za účelem řízení kvality a bezpečnosti služby.

Tato opatření jsou:

- Izolace sítí sloužících pro řízení platformy, a to na úrovni L2 (LAN, VLAN).
- Využití šifrování pro přístup k řízení platformy.
- Dohled infrastruktury.
- Analýza přenosu dat při neočekávaném chování.

5.2.6. Řízení dostupnosti

Platforma CRA Media Cloud Infrastructure je vytvořena s cílem zajistit vysokou dostupnost provozovaných aplikací.

K zajištění této dostupnosti jsou v rámci platformy implementována tato opatření:

- Redundance na úrovni kritických prvků infrastruktury.
- Izolace jednotlivých částí infrastruktury vedoucí k minimalizaci tzv. lavinového afektu.
- Využití redundantních prvků s využitím mechanismu Fail-Over mechanismu.
- Dohled všech prvků infrastruktury.
- Pravidelné vyhodnocování využívaných zdrojů a řízení změn rozsahu za účelem efektivního nakládání s prostředky.
- Pravidelné vyhodnocování SLA jednotlivých služeb.

5.2.7. Dohled

Platforma CRA Media Cloud Infrastructure je na mnoha úrovních monitorována. Abychom zajistili znalost přesného stavu celé platformy, implementovali jsme tato pravidla pro monitoring:

- Provozní parametry platformy (např. dostupnost, výkonnost, disponibilní prostředky, síťové služby apod.) jsou v režimu 24x7 monitorovány on-line nástroji poskytovatele s okamžitým zobrazením stavu v rámci dohledového centra.
- Monitoring je implementován na úrovních:
  - Fyzické infrastruktury – stavu jednotlivých prvků a jejich komponent.
  - Přenosové infrastruktury – stavu jednotlivých spojení v rámci infrastruktury, jejího využití a přehled o nenadálých situacích v rámci těchto spojení.
  - Virtualizační infrastruktury – stavu jednotlivých virtualizovaných objektech platformy a sledování nenadálých či neočekávaných stavů.

6. Zabezpečení dat při přenosech v telekomunikační síti

Pro přenos dat, včetně zákaznických dat, využíváme především uzavřenou, izolovanou síť ve vlastnictví CRA. Standardně není třeba data v této síti šifrovat. Tento způsob přenosu dat lze, s ohledem na standardy na trhu, považovat za bezpečný a díky tomu lze považovat za důvěryhodnou síť. Pakliže to konkrétní zákaznická aplikace vyžaduje, lze pro přenos dat po síti využít standardních šifrovacích end-to-end prostředků. V takovém případě jsou veškeré klíče spravovány ze strany zákazníka. Pro přenos mimo naši fyzickou a virtuální síť využíváme vždy šifrování. Šifrování přenosu je proces, kdy je celý provoz, včetně užitečného obsahu zpráv zašifrován na vstupu a rozšifrován na výstupu.

Pro řízení přístupu našich administrátorů do CRA síťových prvků využíváme autorizační mechanismy (AAA), které jsou v naší správě. Máme nastaveny mechanismy pro management poskytovaných práv, jejich rozsah a validitu k dané osobě.

7. Ochrana perimetru

- Síťová infrastruktura společnosti je chráněna jak na úrovni perimetrů, tak interních segmentačních firewallů.
- Pro inspekci HTTP/HTTPS provozu a ochranu před aplikačními útoky využíváme specializovaný nástroj Web Application Firewall.
- Pro zajištění dostupnosti služeb je infrastruktura CRA vybavena ochranou před DDoS útoky, která snižuje rizika spojená se zahlcením nevalidním provozem.
- Všechny síťové bezpečnostní prvky jsou nepřetržitě monitorovány zaměstnanci CRA v režimu 24x7.
- Klíčové prvky jsou v režimu vysoké dostupnosti (HA).

8. Detekce a správa incidentů zabezpečení informací

Společnost CRA disponuje bezpečnostním týmem CSIRT (Computer Security Incident Response Team) s názvem CRA CSIRT. Tento tým je veden u GÉANT/TF - CSIRT Trusted Introducer ode dne 9. listopadu 2016.

9. Správa účtů

9.1. Řízení a kontrola přístupu/ správa účtů

Přístup k zákaznickým datům je umožněn pouze osobám, které je potřebují k zajištění činností vyplývajících ze smlouvy, a to pouze v nezbytně nutném rozsahu (princip Need-To-Know). Přístupy k systémům (účtům) z nezabezpečeného prostředí jsou vždy kontrolovány a v takovém případě přenos dat je vždy šifrován. Dle zákona o kybernetické bezpečnosti máme implementovanou politiku hesel. Veškeré systémy mají svého administrátora, který přiděluje uživatelské přístupy. Minimální požadavek na přístup do systémů je uživatelské jméno a heslo, některé systémy používají pro přihlášení model dvou faktorové autentizace. Přihlašování do webových aplikací probíhá přes zabezpečený protokol https.

9.2. Skupiny uživatelů:

- Administrátoři

Administrátoři služeb mají přístup pouze k vymezené skupině činností, přičemž je zachován princip oddělení rolí administrátora a auditora.

Přístup do systémů mají pověření pracovníci CRA, nebo dodavatele, kterým je vygenerováno pro přístup uživatelské jméno a heslo. Veškeré aktivity těchto uživatelů v systémech jsou logovány a vyhodnocovány v souladu s interními směrnicemi.

- Zákazníci

Zákazníci obdrží přístup do systémů na základě podepsané smlouvy k dané službě. Některé systémy umožňují zákazníkovi vytvářet další uživatele/role v systému. Pro tyto účty platí stejná pravidla pro kontrolu, správu účtu a logování aktivit.

- Koncoví uživatelé služeb

Účty jsou zřizovány na základě registrace ve front-end aplikacích. Každý uživatel je autorizován pomocí jména a hesla. Heslo splňuje bezpečnostní standardy pro bezpečná hesla. Používají se pouze šifry, které jsou v daném čase doporučené k používání Uživatelům je umožněna správa účtu, obnova účtu probíhá některou ze standardních autorizačních metod, například zasláním linku na asociovaný e-mail uživatele. Rozsah dat požadovaných pro vytvoření účtu, je řízen podmínkami služby od zákazníků. Přístup a možnost vytvořit heslo dostane osoba uvedená na smlouvě služby. U vybraných služeb si může, pro zvýšení bezpečnosti přístupů, uživatel aktivovat dvou faktorovou autentizaci.

9.3. Ověřovací kód

Ověřovacím kódem pro změnu poskytovatele služby přístupu k internetu je tzv. *ID služby* uváděné zejména v příslušné Technické specifikaci služby (dílčí smlouvě), není-li ve smluvní dokumentaci výslovně stanoveno jinak.

10. Zabezpečení subdodavatelů

CRA může najmout subdodavatele za účelem poskytování služeb jejím jménem. Tito subdodavatelé budou smět zákaznická data získat pouze za účelem poskytování služeb a zákaznické podpory, k jejichž poskytování se zavázali, a nebudou smět tato data používat za jakýmkoli jiným účelem. CRA zůstávají odpovědné za dodržování souladu s povinnostmi stanovenými v těchto podmínkách svými subdodavateli. Zákazník již dříve

souhlasil s tím, že CRA smí přenést zákaznická data a údaje o podpoře k subdodavatelům podle popisu v těchto podmínkách.