

Všeobecné technické bezpečnostní požadavky

Všeobecné technické bezpečnostní požadavky mj. zahrnují výtah technických požadavků plynoucích z vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti, dále jen Vyhláška) [1] a [2], resp. [3] Všeobecné technické bezpečnostní požadavky jsou určeny pro interní potřebu Českých Radiokomunikací a. s. (dále jen CRA) a určených dodavatelů. Odkazy na části Vyhlášky jsou orientační. V řadě případů bylo znění uvedené ve Vyhlášce upraveno – konkretizováno – aby lépe odpovídalo podmínkám nasazení.

Předložené Všeobecné technické bezpečnostní požadavky odkazují na standardy a doporučení, např. DoD STIG, viz kap. 2, jejichž splnění je v uvedeném rozsahu povinné. V případě rozdílných požadavků v odkazovaných dokumentech a požadavků explicitně definovaných ve Všeobecných technických bezpečnostních požadavcích, musí být vždy provedena konfigurace dle Všeobecných technických bezpečnostních požadavků. Pokud příslušná technologie (zejména pokud se jedná o nově zaváděnou technologii nebo technologii nabízenou v rámci poptávkového řízení dodavatelem) některý z požadavků nesplňuje, je požadováno, aby byla prokazatelně upozorněna Skupina provozní a kybernetické bezpečnosti CRA, která rozhodne, zda a jak bude daná technologie v infrastruktuře CRA integrována.

V případě že je daná technologie dodávána, spravována, integrována apod. externím subjektem – dodavatelem – je požadováno, aby dodavatel stanovil kontaktní osobu pro oblast kybernetické bezpečnosti, která bude na straně dodavatele odpovědná za plnění bezpečnostních požadavků. Stanovená kontaktní osoba dodavatele bude garantovat jejich plnění a současně bude kontaktní osobou pro „Skupinu provozní a kybernetické bezpečnosti CRA“ a také kontaktní osobou pro testování a hlášení případných bezpečnostních nedostatků, jejichž řešení bude rovněž garantovat. Je požadováno, aby kontaktní osoba byla kvalifikována pro oblast kybernetické bezpečnosti alespoň dle zákona č. 181/2014 Sb. [4], nebo byla certifikována dle jiného bezpečnostního standardu (CCNP Security, ISACA, ...)

1 Požadavky dle vyhlášky č. 82/2018 Sb.

1.1 Hlava II., technická opatření

Číslo	Odkaz	Požadavek
1	§ 18	Důsledná segmentace jednotlivých částí systému tak, aby narušením bezpečnosti jedné části nedošlo k narušení bezpečnosti v části jiné. Jedná se zejména o správnou konfiguraci přístupových oprávnění jednotlivých částí návrhu.
2	§ 18	Správa bude prováděna výhradně z technologické části sítě CRA. Přímý přístup ke správě z internetu není přípustný. Vzdálený přístup (z technologické části sítě CRA), vzdálená správa (konfigurace, aktualizace, přenosy souborů, ...) musí být chráněna kryptografickými prostředky dle kap. 1.2. Přímý přístup z jiných, než technologických zařízení (vč. technologických notebooků) není přípustný – správa musí probíhat buď prostřednictvím nástroje pro centrální správu nebo přes terminálový (jump) server, resp. Privileged Access Management. Viz kap. 2, požadavky 4 a 5.
3	§ 19	nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, musí vynucovat pravidla: <ul style="list-style-type: none">▪ délky hesla alespoň

Číslo	Odkaz	Požadavek
		<ul style="list-style-type: none"> ▪ 12 znaků u uživatelů a ▪ 17 znaků u administrátorů a aplikací, ▪ umožňující zadat heslo o délce alespoň 64 znaků, ▪ neomezuující použití malých a velkých písmen, číslic a speciálních znaků, ▪ umožňující uživatelům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut, ▪ neumožňující uživatelům a administrátorům <ol style="list-style-type: none"> 1. zvolit si nejčastěji používaná hesla, 2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a 3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel a ▪ pro povinnou změnu hesla v intervalu maximálně po 18 měsících, přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie. ▪ Nástroj pro ověřování identity uživatelů a administrátorů může být zajištěn i jinými způsoby, než jsou uživatelské jméno a heslo dle požadavku 3, pokud bude zajištěno, že použitá opatření zajišťují stejnou nebo vyšší úroveň odolnosti. ▪ Identita uživatele a administrátora musí být spojena s konkrétní fyzickou osobou, generické identity (účty), např. administrator, admin, root, guest, ... jsou zakázány. Je zakázáno sdílení jedné identity více fyzickými osobami.
4	§ 20	<p>Musí být integrován nástroj pro řízení přístupových oprávnění, který zajistí řízení oprávnění</p> <ul style="list-style-type: none"> ▪ pro přístup k jednotlivým aplikacím a datům a ▪ pro čtení dat, pro zápis dat a pro změnu oprávnění. <p>Nástroj pro řízení přístupových oprávnění, musí zaznamenávat použití přístupových oprávnění a tyto ukládat do záznamu činností dle požadavku 7. Další požadavky na přístupová oprávnění viz kap. 2, požadavek 5.</p>
5	§ 21	<ul style="list-style-type: none"> ▪ Musí být integrován nástroj pro ochranu před škodlivým kódem zajišťující nepřetržitou ochranu koncových zařízení, zejména pak pracovních stanic a serverů. Povinnost platí bez ohledu na instalovaný operační systém a jeho výrobce. Je požadováno, aby použité antimalware řešení v posledním roce získalo alespoň 3× maximum bodů v testech, viz [5], záchytu malware („protection score“). Je požadována alespoň denní aktualizace signatur. Spolehlivost detekce nesmí po celou dobu životnosti klesnout pod 98 %. Databáze signatur musí obsahovat alespoň signatury detekované antimalware nástroji umístujícími se v žebříčku [5] v každém roce alespoň třikrát mezi osmi nejlepšími. ▪ Zařízením, na něž není instalace antimalware řešení možná, lze udělit Skupinou provozní a kybernetické bezpečnosti CRA výjimku. Jedná se především o proprietární řešení, resp. striktně účelová zařízení, bez možnosti instalace dalšího software. Výjimka musí být udělena prokazatelně, žádá o ni správce příslušné technologie. ▪ Není-li specifikováno jinak, antimalware řešení není předmětem dodávky příslušného řešení, za jeho provoz je odpovědný administrátor technologie na straně CRA dodávaná řešení musí být s antimalware řešením kompatibilní.

Číslo	Odkaz	Požadavek
		<ul style="list-style-type: none"> Je požadováno, aby veškerá zařízení, která budou na straně dodavatele a jeho subdodavatelů využita v souvislosti s dodávkou pro CRA (vč. zařízení v jeho majetku), byla vybavena funkčním antimalware řešením shodných vlastností, jako je uvedeno v první odrážce tohoto požadavku.
6	§ 22	<p>Musí být integrován nástroj pro zaznamenávání činností informační infrastruktury, resp. informačních systémů, jejich uživatelů a administrátorů, který zajistí:</p> <ul style="list-style-type: none"> sběr informací o provozních a bezpečnostních činnostech, zejména: <ul style="list-style-type: none"> typ činnosti, datum a čas (SEČ/SELČ), identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a identifikace místa činnosti (IP adresa), úspěšnost nebo neúspěšnost činnosti a ochranu získaných informací před neoprávněným čtením nebo změnou.
7	§ 22	<p>Dle požadavku 6 bude zaznamenáváno mj.:</p> <ul style="list-style-type: none"> přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů, činnosti provedené administrátory, úspěšné i neúspěšné manipulace s účty, oprávněními a právy, neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému, zahájení a ukončení činností technických aktiv, kritických i chybových hlášení technických aktiv a přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí <ul style="list-style-type: none"> Záznamy činností budou uchovávány nejméně po dobu 18 měsíců. Nejméně jednou za 24 hodin bude provedena synchronizace jednotného systémového času.
8	§ 24	<p>Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí – je požadováno automatické odesílání událostí (zaznamenány jsou činnosti dle požadavku 7) ihned po jejich vzniku (po prokazatelném souhlasu Skupiny provozní a kybernetické bezpečnosti CRA nejpozději do 5 minut, dle [3], resp. [6]) do systému pro ukládání protokolů událostí (log management) protokolem Syslog ve verzi dle RFC 3164 [7] nebo RFC 5424 [8], šifrovaně, viz [9]. Obsahová část musí být ve formátu daného původce (raw) nebo ve formátu LEEF (Log Event Extended Format) [10]. V případě že není podporován, pak ve formátu CEE (Common Event Expression) [11] nebo CEF (Common Event Format) [12]. Jiný formát je přípustný pouze s prokazatelným souhlasem Skupiny provozní a kybernetické bezpečnosti CRA. Je požadováno dodání podrobného popisu každého z polí zasílaných událostí pro konfiguraci syntaktického analyzátoru (parser) SIEM QRadar.</p>
9	§ 25	<p>Je požadováno provádění bezpečnostních testů zranitelnosti (v případě nově dodávaných technologií nebo technologií spravovaných dodavatelem je provádí dodavatel), a to před uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.</p> <p>Je požadováno v rámci aplikační bezpečnosti zajistit trvalou ochranu</p>

Číslo	Odkaz	Požadavek
		<ul style="list-style-type: none"> ▪ aplikací a informací dostupných z vnější sítě před neoprávněnou činností, porušením provedených činností, kompromitací nebo neautorizovanou změnou a ▪ transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.
10	§ 26	<p>Pro používání kryptografické ochrany je stanoveno zajistit:</p> <ul style="list-style-type: none"> ▪ úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu a ▪ pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat. <p>Je požadováno používat kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a průkaznou identifikaci osoby za provedené činnosti.</p> <p>Dodavatel (v případě nově dodávaných technologií nebo technologií spravovaných dodavatelem) nebo správce příslušné technologie CRA ve všech ostatních případech:</p> <ul style="list-style-type: none"> ▪ stanoví pro používání kryptografických prostředků systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů, a ▪ používá odolné kryptografické algoritmy a kryptografické klíče dle kap. 1.2.

1.2 Minimální požadavky na kryptografické algoritmy

Je povoleno použití pouze kryptografických algoritmů uvedených v rámci kap. 1.2. Současně platí, že z algoritmů uvedených v kap. 1.2 je povoleno používat pouze algoritmy považované v době dodávky nebo významné úpravy (např. upgrade) dané technologie za bezpečné. Minimální požadavky na kryptografické algoritmy vychází z doporučení v oblasti kryptografických prostředků Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) [13].

Níže jsou uvedeny dvě kategorie kryptografických algoritmů, které jsou označeny jako „schválené“ a „dosluhující“.

Schválené kryptografické algoritmy (Approved, Recommended, Future) jsou algoritmy, které smí být bez omezení použity v rámci nových projektů a současně i projektů již realizovaných, na nichž probíhají úpravy.

Dosluhující kryptografické algoritmy (Legacy) jsou algoritmy, u kterých je zakázáno je používat u nových projektů. Přípustné je jejich využití pouze tehdy, byly-li v daném projektu použity před platností těchto Požadavků. Použití „Dosluhujících kryptografických algoritmů“ musí být výslovně a prokazatelně schváleno Skupinou provozní a kybernetické bezpečnosti CRA. Je požadováno, aby algoritmy této kategorie v systémech CRA nebyly přítomny po r. 2023.

Preferované algoritmy a délky klíče jsou v kap. 1.2.1–1.2.4 vyznačeny tučně, pořadí určuje preferenci použití daného algoritmu.

1.2.1 Symetrické algoritmy

- Schválené blokové a proudové šifry (Je požadováno preferovat použití blokových šifer před proudovými).

1. **Advanced Encryption Standard (AES)** s využitím délky klíčů 128, 192 a **256** bitů.
4. Twofish s využitím délky klíčů 128 až 256 bitů.
5. **Camellia** s využitím délky klíčů 128, 192 a **256** bitů.

6. **Serpent** s využitím délky klíčů 128, 192, **256** bitů.
7. SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů.
8. ChaCha20 s délkou klíče 256 bitů a se zatížením klíče menším než 256 GB.

▪ Dosluhující blokové a proudové šifry

1. Triple Data Encryption Standard (3DES) s využitím délky klíčů 112 bitů, omezené použití jen se zatížením klíče menším než 10 MB. Doporučeno je použití jedinečného klíče pro každou zprávu.
2. Blowfish s využitím minimální délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB.
3. Kasumi s využitím délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB.

▪ Schválené módy šifrování s ochranou integrity (schválené módy šifrování musí používat schválené a současně preferované blokové šifry)

1. CCM
2. EAX
3. OCB1 a OCB3, preferováno OCB3 před OCB1
4. GCM s noncí dlouhou 96 bitů a s tagem dlouhým 128 bitů, nejpozději po 2^{32} hodnotách nonce musí dojít k výměně klíče.
5. ChaCha20 + Poly1305 se zatížením klíče menším než 256 GB.
6. Složená schémata typu „Encrypt-then-MAC“.

Poznámka: Schémata typu „Encrypt-then-MAC“ musí používat k šifrování pouze šifrovací módy uvedené v následujícím odstavci a k výpočtu MAC pouze schválené módy pro ochranu integrity. Inicializační vektor (nebo nonce) musí být součástí vstupu pro výpočet MAC.

▪ Módy šifrování (jejich samostatné použití je dosluhující, ale schválené je jejich použití ve složených schématech typu „Encrypt-then-MAC“; schválené módy šifrování musí být používány pouze se schválenými a současně preferovanými blokovými šiframi)

1. CTR
2. OFB
3. CBC (rovněž CBC-CS)
4. CFB

Poznámka: Pro použití v rámci schváleného složeného schématu typu Encrypt-then-MAC musí tyto módy používat pouze schválené blokové šifry. Módy CBC a CFB musí být použity s náhodným, pro útočníka nepředpověditelným, inicializačním vektorem. Při použití módu OFB se pro daný klíč nesmí opakovat hodnota inicializačního vektoru. Při použití módu CTR se pro daný klíč nesmí opakovat hodnota čítače. V případě použití CBC módu k šifrování bez ochrany integrity je třeba ověřit odolnost proti útoku na padding CBC módu.

▪ Schválené módy pro šifrování disků (schválené módy šifrování musí být používány pouze se schválenými a současně preferovanými blokovými šiframi)

1. XTS – délka jednotky dat (sektoru) nesmí přesáhnout 2^{20} bloků šifry (v případě šifry se 128bitovým blokem je to zhruba 16 MB)
2. EME2 (Encrypt Mix Encrypt V2)

▪ Schválené módy pro ochranu integrity (musí být používány pouze se schválenými a současně preferovanými hašovacími funkcemi)

1. **LMS (pouze pro ochranu integrity firmware a software)**
2. **XMSS (pouze pro ochranu integrity firmware a software)**

3. HMAC se schválenou hašovací funkcí
 4. EMAC
 5. CMAC
 6. UMAC s délkou tagu 64 bitů
- Dosluhující módy pro ochranu integrity
 1. HMAC-SHA1
 2. CBC-MAC-X9.19, omezené použití jen se zatížením menším než 10^9 MAC, v kombinaci s šifrou používající délkou klíče 256 bitů

1.2.2 Asymetrické algoritmy

- Schválené algoritmy pro technologii digitálního podpisu
 1. **CRYSTALS-Dilithium úrovně 5 (resp. Dilithium 5) implementovaný dle standardu NIST.**
 2. Dilithium SPHINCS+, Falcon (v kombinaci s algoritmy viz body 3–6 níže)
 3. Digital Signature Algorithm (DSA) s využitím délky klíčů 3 072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více.
 4. Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 256 bitů a více.
 5. Rivest-Shamir-Adleman Probabilistic Signature Scheme (RSA-PSS) s využitím délky klíčů 3 072 bitů a více.
 6. Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 256 bitů a více.
- Dosluhující algoritmy pro technologii digitálního podpisu
 1. Digital Signature Algorithm (DSA) s využitím délky klíčů 2 048 bitů, délky parametru cyklické podgrupy 224 bitů.
 2. Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů.
 3. Rivest-Shamir-Adleman Probabilistic Signature Scheme (RSA-PSS) s využitím délky klíčů 2 048 bitů.
 4. Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 224 bitů.
- Schválené algoritmy pro procesy dohod na klíči a šifrování klíčů
 1. **CRYSTALS-Kyber úrovně 5 (resp. Kyber-1024) implementovaný dle standardu NIST.**
 2. Kyber-k768 (v kombinaci s algoritmy viz body 5–11 níže)
 3. FrodoKEM-1344 a FrodoKEM-976 (v kombinaci s algoritmy viz body 5–11 níže)
 4. McEliece-8192128, McEliece-6688128, McEliece-460896, McEliece-8192128f, McEliece-6688128f, McEliece-460896f (v kombinaci s algoritmy viz body 5–11 níže)
 5. Diffie-Hellman (DH) s využitím délky klíčů 3 072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více.
 6. Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 256 bitů a více. U nových projektů je požadováno používat délky klíčů 384 bitů.
 7. Elliptic Curve Integrated Encryption System – Key Encapsulation Mechanism (ECIES-KEM) s využitím délky klíčů 256 bitů a více. U nových projektů je požadováno používat délky klíčů 384 bitů.
 8. Provably Secure Elliptic Curve – Key Encapsulation Mechanism (PSEC-KEM) s využitím délky klíčů 256 bitů a více. U nových projektů je požadováno používat délky klíčů 384 bitů.
 9. Asymmetric Ciphers and Key Encapsulation Mechanism (ACE-KEM) s využitím délky klíčů 256 bitů a více.

10. Rivest Shamir Adleman – Optimal Asymmetric Encryption Padding (RSA-OAEP) s využitím délky klíčů 3 072 bitů a více.
11. Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 3 072 bitů a více.
- Dosluhující algoritmy pro procesy dohod na klíči a šifrování klíčů
 1. Diffie-Hellman (DH) s využitím délky klíčů 2 048 bitů, délky parametru cyklické podgrupy 224 bitů.
 2. Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 224 bitů.
 3. Elliptic Curve Integrated Encryption System – Key Encapsulation Mechanism (ECIES-KEM) s využitím délky klíčů 224 bitů.
 4. Provably Secure Elliptic Curve – Key Encapsulation Mechanism (PSEC-KEM) s využitím délky klíčů 224 bitů.
 5. Asymmetric Ciphers and Key Encapsulation Mechanism (ACE-KEM) s využitím délky klíčů 224 bitů.
 6. Rivest Shamir Adleman – Optimal Asymmetric Encryption Padding (RSA-OAEP) s využitím délky klíčů 2 048 bitů.
 7. Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 2 048 bitů.

1.2.3 Algoritmy hašovacích funkcí

- Schválené hašovací funkce SHA-2
 1. SHA-256
 - 2. SHA-384**
 3. SHA-512
 4. SHA-512/256
- Schválené hašovací funkce SHA3
 1. SHA3-256
 - 2. SHA3-384**
 3. SHA3-512
 4. SHAKE128
 5. SHAKE256
- Ostatní schválené hašovací funkce
 1. Whirlpool
 2. BLAKE2
- Dosluhující hašovací funkce
 1. SHA2 s délkou výstupu 224 bitů (SHA-224, SHA-512/224)
 2. SHA3-224
 3. RIPEMD-160

1.2.4 Algoritmy pro bezpečné ukládání hesel

- Schválené algoritmy (Musí být použita sůl náhodně vygenerovaná pro každé heslo. Délka soli musí být alespoň 128 bitů, tedy 16 bajtů. Délka výstupu – tagu – musí být alespoň 256 bitů, tedy 32 bajtů. Je požadováno volit parametry maximální možné v dané aplikaci.)
 1. Argon2 s funkcí Argon2id a parametry alespoň $t = 1$, $m = 2^{21}$ (pro zařízení mající alespoň 2 GB RAM) a $t = 3$, $m = 2^{16}$ (pro zařízení s pamětí velikosti 64 MB–2 GB).

2. Scrypt s parametry alespoň $N = 32\,768$ (tedy 2^{15}), $r = 8$, a $p = 1$.
3. PbKDF2 s počtem iterací alespoň 100 000 a schválenou hašovací funkcí SHA-2.

2 Další požadavky

1. Všechny operační systémy dodané (resp. používané) v rámci řešení musí být certifikovány dle CC EAL 4 a výše (Common Criteria, resp. ISO/IEC 15408-1:2009, resp. aktuální verze) [14], musí být uvedeny v rámci certifikovaných produktů, viz [15]. Po prokazatelném schválení Skupinou provozní a kybernetické bezpečnosti CRA je možné pro řešení použít i novější verzi certifikovaného produktu, která dosud certifikovaná není, u níž lze ale předpokládat, že certifikovaná v budoucnu bude. Novější – dosud necertifikovanou verzi – lze použít pouze tehdy, pokud je platná certifikace systému, jehož je nová verze následovníkem a současně je předchůdce nasazované verze plně podporován výrobcem. Platí, že všechny operační systémy a další software musí dále splňovat:
 - aktuálně podporován výrobcem, jsou pro CRA dostupné pravidelné aktualizace po dobu alespoň následujících 5 let od integrace do prostředí CRA
 - řešení zálohování alespoň v rozsahu stanoveném v [16]
2. Operační systémy a další software dodávaný (resp. použitý) v rámci řešení musí být nakonfigurován dle – v době dodání (nebo významného upgradu) – aktuálních DoD STIGs (Department of Defense Security Technical Implementation Guides), viz [17] dle profilu „Mission Critical Classified“. Pro rámcovou orientaci je možné použít portál [18]. Rozhodná je podoba dle [17]. V případě nutných konfiguračních výjimek musí být tyto projednány a prokazatelně schváleny CRA. Dodavatel je povinen v rámci nabídky řešení a poté znovu před předáním řešení uvést seznam dodávaného software, pro který STIG není dostupný (u interně realizovaných projektů předkládá správce příslušné technologie CRA).
3. Veškerý software, který je potřebný pro provoz a správu dodávaného řešení a není přímou součástí operačního systému, resp. Linuxové distribuce – např. skripty, knihovny, podpůrné nástroje atd. – je považován za předmět dodávky (musí splnit veškeré definované požadavky, vč. požadavků na technickou podporu, bezpečnostní aktualizace atd.), nejedná-li se o software explicitně uvedený jako zajišťovaný ze strany CRA. Veškerý takto dodávaný software musí být podrobně a kompletně specifikován v nabídce a technické dokumentaci. Jeho požití musí být prokazatelně schváleno Skupinou provozní a kybernetické bezpečnosti CRA. Příkladem takového software jsou balíky z repozitáře EPEL (Extra Packages for Enterprise Linux), software/skripty z GitHubu, Python Package Index (PyPI), kontejnery z Docker Hubu apod.
4. Operační systémy a další software dodaný (u nových projektů) nebo použitý v rámci řešení musí být integrován se zavedenými nástroji centrální správy CRA (Microsoft Active Directory, Microsoft System Center Configuration Manager, Foreman/Ansible). V případě, že to není z libovolného důvodu možné, bude navržen a předložen k prokazatelnému schválení Skupině provozní a kybernetické bezpečnosti CRA návrh řešení správy / centrální správy realizovaného řešení. Řešení správy / centrální správy musí umožnit konfiguraci operačního systému a dalšího software alespoň v rozsahu požadavků definovaných v kap. 1.1 a kap. 2 požadavek č. 2, tedy v rozsahu stanoveném v aktuálních DoD STIGs a také centrální instalaci aktualizací a bezpečnostních oprav. Přímá manuální konfigurace běžných síťových zařízení, pracovních stanic, serverů apod. není přípustná. Do produkčního režimu smí být uvedené technologie nasazeny výhradně prostřednictvím centrální správy, resp. automatizačních prostředků, vč. produkční konfigurace – ta nesmí být nikdy upravována manuálně. Vývojová, testovací a produkční prostředí musí být jasně definována a striktně oddělena.
5. Řešení přístupových oprávnění, vč. přístupových oprávnění centrální správy, musí být v souladu s NIST RBAC (Role-based access control [19; 20]), resp. „Microsoft Enterprise access model“ [21].

Z toho mj. plyne požadavek, aby všechny části řešení a také uživatelé vždy používali nejmenší možná oprávnění umožňující danou činnost vykonat. Je zakázáno provozovat části řešení s oprávněním privilegovaných účtů, zejména pak generických (administrator, root apod.) V případě že je nezbytná výjimka, je požadováno její prokazatelné schválení Skupinou provozní a kybernetické bezpečnosti CRA.

6. Pokud je software, resp. operační systém, provozován na fyzickém hardwaru, je požadováno šifrování všech integrovaných úložišť (disků, diskových polí, ...) Požadavky na kryptografické algoritmy, viz kap. 1.2. Pokud bude zvoleno řešení šifrování úložišť odlišné oproti v CRA zavedenému (Linux Unified Key Setup – LUKS, resp. Microsoft BitLocker), musí zvolené řešení odpovídat stejným požadavkům na certifikaci jako operační systém, viz kap. 2, požadavek č. 1. Současně musí být zvolené řešení diskutováno se Skupinou provozní a kybernetické bezpečnosti CRA a prokazatelně Skupinou provozní a kybernetické bezpečnosti schváleno.
7. Pokud je software, resp. operační systém, provozován na fyzickém hardwaru, musí být aktivován UEFI (Unified Extensible Firmware Interface) Secure boot. UEFI musí být konfigurováno v souladu s doporučením [22].
8. Lhůty pro odstranění bezpečnostních chyb a zranitelností jsou stanoveny v kap. 5. Za nahlášené dle kap. 5 se mj. považují také všechny chyby v softwaru/technologii, jež jsou evidovány ve veřejně dostupných databázích – mj. např. CVE (Common Vulnerabilities and Exposures) [23], NVD (National Vulnerability Database) [24] apod.
9. Všechny dodané (použité) operační systémy, zařízení, software a technologie musí mít plně integrovanou podporu přihlašování prostřednictvím MS Active Directory, popřípadě LDAP (včetně šifrovaných verzí uvedených protokolů) – dle přesné specifikace v zadání, popř. bude zodpovězeno na dotaz.
10. Všechna dodaná (použitá) zařízení, technologie a software musí mít plně integrován standard IEEE 802.1X dle [25], výjimky musí být prokazatelně schváleny Skupinou provozní a kybernetické bezpečnosti CRA.
11. Dodavatel (u interně realizovaných projektů každý člen realizačního týmu) je povinen dodat řešení vyvinuté a navržené v souladu s aktuálními technickými a zejména bezpečnostními standardy a doporučeními (např. [26; 27]) a vyhnout se používání technologií zastaralých nebo se známými zranitelnostmi.
12. Veškeré instalační balíky dodávaného software budou předány CRA, vč. balíků závislých (nejsou-li součástí operačního systému nebo software již v CRA zavedeného). K jejich instalaci a provozu nebude vyžadováno internetové připojení (není-li to jejich výslovným účelem). Po předložení přesného výčtu požadovaných závislostí a prokazatelném schválení Skupinou provozní a kybernetické bezpečnosti lze instalovat software z veřejně dostupných zdrojů (např. PyPI, kontejnery z Docker Hubu apod.), avšak výhradně prostřednictvím lokálního repozitáře CRA prostřednictvím zavedené technologie „Sonatype Nexus Repository“ [28].
13. V případě webových projektů (mj. projektů využívajících HTTP/HTTPS, Hypertext Transfer Protocol) nebo projektů, kde je to dle Skupiny provozní a kybernetické bezpečnosti CRA účelné, je dodavatel povinen spolupracovat na integraci s webovým aplikačním firewallem (WAF) CRA. Mj. musí být projekt navržen tak, aby jasně odděloval interní/administrátorskou část a část zákaznickou/uživatelskou. Jasným oddělením se rozumí oddělení na úrovni architektury, rolí, částí projektu atd. – v případě jednoduchých projektů alespoň na úrovni URL (Uniform Resource Locator). Je požadováno, aby byl na webovém aplikačním firewallu a dalších technologiích omezen přístup definovaným skupinám uživatelů k interním částem projektu (např. administrátorským).

14. Řešení musí být navrženo tak, aby pro svoji funkci nevyžadovalo internetové služby třetí strany. V případě webových projektů se jedná např. o písma, JavaScript knihovny apod. Tyto musí být integrovány přímo v rámci řešení, resp. musí být užívaná jejich lokální kopie. Výjimkou jsou analytické nástroje, jsou-li výslovně žádanou součástí projektu (zejména webového), které – pokud jsou implementovány – musí být implementovány tak, aby jejich nedostupnost neohrozila funkčnost celého řešení.
15. U nových projektů je požadováno, aby řešení využívající jako uživatelské rozhraní webovou aplikaci bylo navrženo tak, aby ke své plné funkčnosti nevyžadovalo žádné doplňky prohlížeče, zejména pak Adobe Flash (s ohledem na to, že jeho vývoj a údržba byla v roce 2020 ukončena [29]) a Microsoft Silverlight (vývoj a podpora ukončena v říjnu 2021 [30]).
16. Softwarová řešení provozovaná na serverech musí mít jednoznačně definovaný front end a back end. Jednotlivé celky musí být umístěny ve stanovených demilitarizovaných zónách (DMZ).
17. Demilitarizované zóny sdružují zařízení tvořící jeden logický síťový bezpečnostní celek s definovanými vstupy a výstupy (komunikační protokoly). Komunikace v rámci DMZ je přípustná pouze v relevantních případech a výhradně v rozsahu dle definované komunikační matice (zahrnuje mikrosegmentaci na úroveň Isolated VLAN v rámci PVLAN, Private VLAN). Komunikace mezi jednotlivými DMZ musí vždy procházet přes firewall s aktivní hloubkovou paketovou inspekci, resp. systémem prevence průniku (IPS, Intrusion Prevention System). Komunikační matice pro systémy komunikující v rámci jedné DMZ může zahrnovat pouze IP adresy, komunikační matice zahrnující systémy s komunikací (v libovolném směru) i mezi jednotlivými DMZ, musí zahrnovat (kromě IP) adres také informace o komunikačním protokolu a TCP/UDP portech. Průchody přes firewall musí být protokolovány do SIEM, viz kap. 1.1, požadavky 6–8 v rozsahu alespoň zdrojová a cílová IP adresa, zdrojový a cílový TCP/UDP port, identifikace komunikačního protokolu, časová značka zahájení a ukončení spojení, identifikace zdroje protokolu (např. IP adresa nebo hostname příslušného firewallu), informace, zda bylo spojení povoleno nebo zamítnuto.
18. Architektura řešení (vč. umístění částí do jednotlivých DMZ) musí být před zahájením projektu spolu s projektovou dokumentací (vč. komunikačních matic) schválena Skupinou provozní a kybernetické bezpečnosti CRA.
19. V souladu s varováními vydávanými Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) dle § 12 zákona č. 181/2014 Sb. [4] bude rozhodnuto o účasti dodavatelů řešení označených NÚKIB jako rizikových, na úrovni statutárního orgánu CRA. Aktuálně jde o řešení obsahující technické nebo programové prostředky následujících společností, včetně jejich dceřiných společností:
 - Huawei Technologies Co., Ltd., Šen-čen, Čínská lidová republika [31]
 - ZTE Corporation, Šen-čen, Čínská lidová republika [31]
20. Dodavatel je povinen spolupracovat na integraci s bezpečnostními prvky instalovanými v CRA – jedná se zejména o přesnou specifikaci použitých síťových protokolů, komunikujících IP adres a TCP/UDP portů pro konfiguraci průchodů firewallu.
21. Veškerá komunikace spojená s kybernetickou bezpečností bude vždy mezi komunikujícími uzly šifrovaná bez dešifrování při přenosu (end-to-end šifrování). V případě e-mailové komunikace jsou přípustné jak technologie S/MIME (preferováno), tak PGP/GPG. Přípustné kryptografické algoritmy viz kap. 1.2.
22. Není přípustné ukládat popisy, dokumentaci, software atd. související s kybernetickou bezpečností na servery mimo kontrolu dodavatele nebo CRA. Bez prokazatelného souhlasu Skupiny provozní

a kybernetické bezpečnosti CRA není přípustné jakékoli jejich sdílení se třetí stranou. CRA pro potřebu přenosu většího množství dat, než je vhodné přenášet e-mailem, provozuje systém pro výměnu dat s dodavateli, do něhož bude dodavateli umožněn přístup [32].

23. S šifrovacími klíči certifikáty a dalšími kryptografickými prostředky smí být nakládáno výhradně v rámci infrastruktury CRA, a to pouze prostřednictvím prostředků určených CRA. Nikdy nesmí – bez prokazatelného souhlasu CRA – opustit úložiště stanovené CRA. Pokud není úložiště ze strany CRA specifikováno, je dodavatel povinen o specifikaci prokazatelně požádat.

3 Požadavky na technologie provozované mimo CRA

Do kategorie technologií provozovaných mimo CRA patří především softwarové služby poskytované externími firmami, tedy outsourceovaný software – tzv. cloudové služby. Jsou rozlišovány 2 typy těchto služeb – kritické a nekritické. Službu jako kritickou označuje Skupina provozní a kybernetické bezpečnosti CRA a označení je součástí požadavků na dodavatele, resp. zadání dané zakázky a následně i smlouvy. Jako kritické jsou obvykle označovány služby, na nichž závisí provozní bezpečnost CRA. Pokud není uvedeno níže jinak, není pro dodavatele nekritických služeb povinné plnění požadavků uvedených v kap. 1 a 2.

3.1 Požadavky na nekritické cloudové služby

1. Pokud se jedná o projekt s webovým rozhraním, je požadován bezchybný průchod testy dle OWASP Web Security Testing Guide v4.2 [33], prokázaný certifikací od certifikačního orgánu. Certifikována musí být aktuální hlavní verze dodávané cloudové služby, ne starší než 1 rok.
2. Certifikace společnosti, která cloudovou službu vyvinula a spravuje dle ČSN ISO/IEC 27000 [34] v aktuálním znění, popřípadě jiného obdobného bezpečnostního standardu, prokázaná platnou certifikací od certifikačního orgánu.
3. Certifikace (osvědčení) cloudové služby vydané subjektem pro vydávání osvědčení (certifikačním orgánem) nebo čestné prohlášení, kterým subjekt (správce, zpracovatel, výrobce atd.) prokazuje zajištění souladu s požadavky nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR) [35].
4. Všechny vrstvy cloudové služby počínaje fyzickým hardwarem (včetně uchovávaných dat) musí být umístěny v rámci Evropské unie.
5. Při ukončení služby, musí být veškerá data shromážděná v souvislosti s poskytovanou službou – včetně dat uživatelů (tedy dat vložených, popř. vytvořených uživateli) – předána CRA ve standardizovaném formátu a následně musí být na straně dodavatele bezpečně a neobnovitelně zlikvidována.

3.2 Požadavky na kritické cloudové služby

Je-li cloudová služba označena jako kritická, je navíc k požadavkům popsaným v kap. 3.1 požadováno, aby:

1. byla služba (řešení) provozována v rámci datového centra připojeného do projektu FENIX [36] nebo aby s daným datovým centrem měly CRA přímé síťové propojení (peering),
2. služba (řešení) byla připojitelná (a následně po uzavření smlouvy připojena) na on-premises SIEM CRA (QRadar) a povinně byly monitorovány činnosti dle kap. 1.1, číslo 6, 7 a byl splněn požadavek 8,
3. byla veškerá uložená data šifrována algoritmy dle kap. 1.2,
4. služba (řešení) plnila na všech svých vrstvách všechny požadavky dle kap. 1 a 2, s výjimkou požadavku č. 2 z kap. 1.1.

4 Metodiky testování

- U webových projektů jsou bezpečnostní (penetrační) testy prováděny dle OWASP Web Security Testing Guide v4.2 [33].
- Obecná metodika testování systémů je stanovena v rámci Technical Guide to Information Security Testing and Assessment (NIST SP 800-115), [37].

5 Bezpečnostní opravy, akceptovatelná bezpečnostní rizika a metodika stanovení stupně ohrožení zranitelností

Metodika stanovení stupně ohrožení zranitelností v softwarovém řešení je postavena na metodice „Common Vulnerability Scoring System (CVSS), Base Score“ [38] publikované organizací FIRST.org, Inc. Výpočet stupně ohrožení je prováděn dle [39]. Stupeň ohrožení danou zranitelností je stanovován vždy bez bezpečnostních prvků ve vlastnictví CRA.

- Pokud je Base Score větší nebo rovno 7, je v případě dodávky nového řešení takové řešení neakceptovatelné do odstranění zranitelnosti. V případě řešení již zavedeného jej lze provozovat pouze tehdy, je-li možné prostředky CRA snížit stupeň ohrožení danou zranitelností pod Base Score menší než 7, s požadavkem na odstranění zranitelnosti v termínu dle tohoto sníženého Base Score.
- V případě Base Score náležícího do intervalu od 3 do 7 musí být zranitelnost odstraněna nejpozději do 1 měsíce od identifikace nebo nahlášení dodavateli (u interně realizovaných projektů správci příslušné technologie v CRA). V případě nového řešení je toto akceptovatelné s výhradou a odstraněním zranitelnosti v uvedeném termínu.
- V případě Base Score menšího než 3 je požadováno odstranění zranitelnosti v rámci běžného vývojového (opravného) cyklu, nejpozději však do 6 měsíců od identifikace nebo nahlášení dodavateli. V případě nového řešení je toto akceptovatelné s výhradou a odstraněním zranitelnosti v uvedeném termínu.

Zranitelnost software, pro nějž existuje konfigurační standard STIG, viz kap. 2, požadavek 2, tedy software vyvinutý globálními dodavateli bez praktické možnosti ovlivnit dodávku bezpečnostní opravy lze ve stanovených lhůtách opravit rovněž přijetím mitigačních opatření definovaných výrobcem. Nejsou-li postupy vedoucí k mitigaci zranitelnosti k dispozici, je dodavatel (u interně realizovaných projektů správce příslušné technologie v CRA) povinen bez zbytečného odkladu, nejpozději do 2 pracovních dnů, problém prokazatelně konzultovat se Skupinou provozní a kybernetické bezpečnosti CRA.

Pozn.: V roce 2023 byla definovaná čtvrtá verze CVSS [40; 41]. Kvůli aktuálnímu stavu implementace v technologiích podporujících kybernetickou bezpečnost CRA zůstává zaveden výpočet stupně ohrožení zranitelností dle specifikace CVSS v3.1 [38].

6 Kvalifikační požadavky

6.1 Základní a profesní způsobilost

Je požadováno, aby dodavatel splňoval kvalifikační předpoklady ve smyslu § 74, odst. 1, a § 77 zákona č. 134/2016 Sb. [42].

6.2 Technická kvalifikace

Dodavatel doloží alespoň 2 referenční implementace nabízeného zařízení, které provedl samostatně v rozsahu stejném nebo větším, jako je popsáno v kap. 6.1, vč. kontaktu umožňujícího ověření předložené informace a prohlídku instalovaného řešení.

Bibliografie

- [1] Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). 21. 5 2018.
- [2] Národní úřad pro kybernetickou a informační bezpečnost. Doporučení na minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů. [Online] 10. 8 2016. [Citace: 30. 11 2020.] <https://www.govcert.cz/cs/informacni-servis/doporuzeni/2485-doporuzeni-na-minimalni-pozadavky-pro-logy-ktete-musi-byt-zajisteny-pro-spolehlivou-ex-post-analyzu-kybernetickych-bezpecnostnich-incidentu/>.
- [3] —. Doporučení na minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů. [Online] 10. 8 2016. [Citace: 30. 11 2020.] <https://www.govcert.cz/download/doporuzeni/container-nodeid-1259/logmngmntfinal.pdf>.
- [4] Česká republika. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.
- [5] AV-TEST GmbH. AV-TEST: The Independent IT-Security Institute. *The best Windows antivirus software for business users*. [Online] AV-TEST GmbH. [Citace: 8. 8 2023.] <https://www.av-test.org/en/antivirus/business-windows-client/>.
- [6] KENT, Karen a MURUGIAH, Souppaya. NIST SP 800-92: Guide to Computer Security Log Management. [Online] 13. 9 2006. [Citace: 30. 11 2020.] <https://csrc.nist.gov/publications/detail/sp/800-92/final>. NIST SP 800-92.
- [7] LONVICK, C. RFC 3164: The BSD syslog Protocol. [Online] 8 2001. [Citace: 14. 11 2021.] <https://datatracker.ietf.org/doc/rfc3164/>.
- [8] GERHARDS, R. RFC 5424: The Syslog Protocol. [Online] 3 2008. [Citace: 23. 10 2019.] <https://datatracker.ietf.org/doc/rfc5424/>.
- [9] MIAO, F., MA, Y. a SALOWEY, J. RFC 5425: Transport Layer Security (TLS) Transport Mapping for Syslog. [Online] 3 2009. [Citace: 23. 10 2019.] <https://datatracker.ietf.org/doc/rfc5425/>.
- [10] International Business Machines Corp. (IBM). LEEF overview. [Online] [Citace: 1. 5 2023.] <https://www.ibm.com/docs/en/qsip/7.4?topic=leef-overview>.
- [11] The MITRE Corporation. Common Event Expression (CEE). [Online] 28. 11 2014. [Citace: 20. 1 2021.] <https://cee.mitre.org/>.
- [12] Micro Focus International plc. ArcSight Common Event Format (CEF) Implementation Standard. [Online] 1 2020. [Citace: 20. 1 2021.] <https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Implementation-Standard/ta-p/1645557>.
- [13] Národní úřad pro kybernetickou a informační bezpečnost. Minimální požadavky na kryptografické algoritmy – Doporučení v oblasti kryptografických prostředků verze 3.0. [Online] 2. 8 2023. [Citace: 29. 11 2023.] <https://nukib.cz/cs/infoservis/doporuzeni/1988-doporuzeni-v-oblasti-kryptografickych-prostredku-verze-3-0/>.
- [14] Common Criteria Recognition Arrangement. ISO/IEC 15408-1:2009: Common Criteria (Evaluation Assurance Level - EAL). *CC/CEM Documentation*. [Online] [Cited: 11 28, 2023.] <https://www.commoncriteriaportal.org/cc/index.cfm>.
- [15] —. Common Criteria. *Certified Products*. [Online] [Cited: 11 28, 2023.] <https://www.commoncriteriaportal.org/products/index.cfm>.
- [16] Národní úřad pro kybernetickou a informační bezpečnost. Ransomware: Doporučení pro mitigaci, prevenci a reakci, verze 1.2. [Online] 22. 5 2023. [Citace: 26. 9 2023.] <https://www.nukib.cz/download/publikace/navody/RANSOMWARE%20-%20Doporuzeni%20pro%20mitigaci%20prevenci%20a%20reakci.pdf>.
- [17] Defense Information Systems Agency (DISA). Security Technical Implementation Guides (STIG). [Online] U. S. Department of Defense. [Citace: 14. 7 2020.] <https://public.cyber.mil/stigs/>.

- [18] Network Frontiers LLC. STIG Viewer. [Online] Network Frontiers LLC. [Citace: 14. 7 2020.] <https://www.stigviewer.com/stigs>.
- [19] National Institute of Standards and Technology (NIST). Role Based Access Control (RBAC). [Online] National Institute of Standards and Technology (NIST), 22. 6 2020. [Citace: 8. 1 2024.] <https://csrc.nist.gov/projects/role-based-access-control>.
- [20] Red Hat, Inc. What is role-based access control (RBAC)? [Online] 5. 12 2023. [Citace: 9. 1 2024.] <https://www.redhat.com/en/topics/security/what-is-role-based-access-control>.
- [21] Microsoft Corporation. Enterprise access model (Active Directory administrative tier model). *Microsoft Security*. [Online] 3. 4 2023. [Citace: 10. 8 2023.] <https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model>.
- [22] National Security Agency / Central Security Service USA. UEFI Lockdown Quick Guidance. [Online] 3. 1 2020. [Citace: 12. 11 2021.] <https://media.defense.gov/2019/Jul/16/2002158050/-1/-1/0/CSI-UEFI-LOCKDOWN.PDF>.
- [23] The MITRE Corporation. Common Vulnerabilities and Exposures. [Online] The MITRE Corporation. [Citace: 19. 10 2017.] <https://cve.mitre.org/find/>.
- [24] National Institute of Standards and Technology (NIST). National Vulnerability Database. [Online] National Institute of Standards and Technology (NIST). [Citace: 19. 10 2017.] <https://nvd.nist.gov/>.
- [25] JEFREE, Tony, CONGDON, Paul a SEAMAN, Mick. IEEE 802.1X-2010: IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control. [Online] 5. 2 2010. [Citace: 6. 10 2020.] https://standards.ieee.org/standard/802_1X-2010.html.
- [26] International Organization for Standardization. ISO/IEC TS 17961:2013: Programming languages, their environments and system software interfaces – C secure coding rules. místo neznámé : International Organization for Standardization (ISO), 2013.
- [27] CHESNEY, Brad a BAAN, Steven. OWASP Developer Guide. [Online] 2014. https://www.owasp.org/index.php/OWASP_Guide_Project.
- [28] Sonatype Inc. Sonatype Nexus Repository. [Online] Sonatype Inc. [Citace: 7. 1 2024.] <https://www.sonatype.com/products/sonatype-nexus-repository>.
- [29] Adobe Inc. Flash & the Future of Interactive Content. [Online] 25. 7 2017. [Citace: 28. 11 2023.] <https://blog.adobe.com/en/publish/2017/07/25/adobe-flash-update>.
- [30] Microsoft Corporation. Ukončení podpory platformy Silverlight. [Online] 10 2021. [Citace: 13. 10 2021.] <https://support.microsoft.com/cs-cz/windows/ukon%C4%8Den%C3%AD-podpory-platformy-silverlight-0a3be3c7-bead-e203-2dfd-74f0a64f1788>.
- [31] Národní úřad pro kybernetickou a informační bezpečnost. Varování - použití technických nebo programových prostředků společností Huawei Technologies Co. a ZTE Corporation (č.j.: 3012/2018-NÚKIB-E/110). [Online] 17. 12 2018. [Citace: 3. 1 2019.] https://www.nukib.cz/download/uredni_deska/Varovani_NUKIB_2018-122-17.pdf.
- [32] České Radiokomunikace a. s. Cloud-Drive CRA. [Online] <https://cloud-drive.radiokomunikace.cz/>.
- [33] SAAD, Elie, a další. OWASP Web Security Testing Guide Version 4.2. [Online] 3. 12 2020. [Citace: 29. 11 2021.] <https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf>.
- [34] Česká agentura pro standardizaci. ČSN EN ISO/IEC 27000:2017 (369790): Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací. místo neznámé : Česká agentura pro standardizaci, 2017.
- [35] Evropská unie. EU 2016/679 (GDPR): Nařízení Evropského parlamentu a Rady (EU) 2016/679. 2018.
- [36] NIX.CZ zájmové sdružení právnických osob. Projekt FENIX. [Online] NIX.CZ zájmové sdružení právnických osob. [Citace: 1. 9 2016.] <http://fe.nix.cz/>.

- [37] SCARFONE, Karen, a další. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment. [Online] 10 2008. [Citace: 20. 10 2016.] <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>. NIST SP 800-115.
- [38] FIRST.org, Inc. Common Vulnerability Scoring System version 3.1: Specification Document. [Online] 6 2019. [Citace: 1. 12 2020.] <https://www.first.org/cvss/v3.1/specification-document>.
- [39] —. Common Vulnerability Scoring System version 3.1: Specification Document – Base Metrics Equations. [Online] 6 2019. [Citace: 1. 12 2020.] <https://www.first.org/cvss/v3.1/specification-document#7-1-Base-Metrics-Equations>.
- [40] —. Common Vulnerability Scoring System version 4.0: Specification Document. [Online] FIRST.org, Inc., 11 2023. <https://www.first.org/cvss/v4.0/specification-document>.
- [41] —. Common Vulnerability Scoring System version 4.0: Specification Document - Base Metrics. [Online] FIRST.org, Inc., 11 2023. [Citace: 28. 11 2023.] <https://www.first.org/cvss/v4.0/specification-document#Base-Metrics>.
- [42] Česká republika. Zákon č. 134/2016 Sb., o zadávání veřejných zakázek.