Smlouva o dílo a o poskytování služeb "Implementace Service Desk a ITIL procesů"
Příloha č. 3 - Požadavky na bezpečnost
Identifikace a autentizace
Před přiřazením uživatelského jména nebo jiných identifikačních mechanismů přístupu k aplikaci, musí uživatelé projít registrační procedurou, která potvrdí jejich totožnost způsobem, který je nezaměnitelný a personalizovaný.
Každý uživatel musí mít vlastní uživatelské jméno, sdílení přístupových údajů více uživateli není dovoleno. Stejně tak každé uživatelské jméno musí mít právě jednoho vlastníka zodpovědného za jeho použití.
Obrazovka pro zadání přístupových údajů (resp. jakékoliv zobrazení před ověřením identity uživatele) musí poskytnout jen nezbytné minimum informací (neposkytují informace z operačního systému, informace o organizaci, neveřejné informace apod.).
Uživatelský účet musí být automaticky zablokován při 3 a více po sobě následujících neúspěšných pokusech o přihlášení minimálně na 30 minut nebo do zásahu administrátora.
Musí být definované procedury pro generování, distribuci a změny hesel.
Iniciační heslo uživatele nebo heslo předávané při jeho resetu (např. z důvodu zapomenutí uživatelem) musí být vždy různé a náhodné (a nesmí odpovídat uživatelskému jménu, ani z něj být odvozeno); při nastavování nebo resetování hesla nesmí být použito stejné. Uživatel musí být donucen systémem si iniciační (nebo resetované) heslo při prvním použití změnit.
Aby byla garantována důvěrnost a integrita hesel, musí být předávána jiným komunikačním kanálem, než k nim příslušná uživatelská jména. Hesla nesmí být předávána v otevřeném textu přes veřejné/externí sítě.
Změna hesla musí být vynucena, pokud nebylo změněno v posledních 3 měsících. Uživateli musí být umožněna změna hesla kdykoliv. Opakovaná změna hesla ale nejdříve po 30 minutách. Mechanismus pro změnu hesla (bez ohledu na to zda uživatel mění heslo o své vůli, nebo je změna vynucena) musí splňovat následující:
· hesla nesmí být při zadávání (ani v jiných případech) viditelná (např. se nahradí definovaným znakem)
· před změnou hesla musí být vyžadováno zadání stávajícího hesla
· nové heslo musí být požadováno zadat dvakrát (jako prevence překlepů)
· opakování libovolného z posledních 12 použitých hesel nesmí být dovoleno
· délka a další požadované parametry hesla musí být ověřeny před zapsáním změny (pokud nové heslo nevyhovuje, musí být uživatel upozorněn a vyzván z úpravě nového hesla)
Při použití uživatelských certifikátů musí být definovány procedury pro registraci, generování, obnovu, revokaci a likvidaci těchto certifikátů.
Řešení dodavatele musí být schopno integrace do systému centralizovaného ověřování (například systémy založené na protokolech LDAP, ...) v operačním systému i v aplikacích, které jsou nezbytné pro jeho fungování, při ověřování, autorizaci a logování činnosti uživatelů a při správě hesel s cílem

jednoznačně identifikovat totožnost osoby, která provádí přístup. Preferována je integrace s AD prostředím.
Řízení přístupu
Každý uživatel systému musí být jednoznačně identifikován svým uživatelským jménem. Uživatelem se rozumí osoby nebo procesy (služby), které k systému přistupují.
Je preferováno řízení přístupu založené na uživatelských rolích proti diskrétnímu přidělování a kontrole oprávnění uživatelských jednotlivým účtům. Informační systém musí řídit přístup nejen uživatelů, ale i všech dalších systémů a aplikací, které k němu přistupují. Systém musí logovat jak přístupy autorizovaných uživatelů, tak neautorizované (anonymní) přístupy i pokusy o neoprávněný přístup.
Hesla musí být chráněna před zneužitím neoprávněným uživatelem. Při vytváření nového účtu je uživateli dočasně přiděleno heslo, které je povinen neprodleně změnit.
V případě použití certifikátů pro přístup k systému jsou povoleny certifikáty vydané Důvěryhodnými Certifikačními Autoritami.
Uživatelské jméno a heslo předávané po síti musí být vždy šifrované. Stejně tak musí být šifrované staré i nové heslopři procesu jeho změny uživatelem (dobrovolném i vynuceném). Pro autentizaci je možné použití externích systému jako Kerberos či adresářových služeb jako LDAP nebo AD apod.
Informační systém nesmí uživateli zobrazovat funkce a volby, ke kterým uživatel není autorizován (nemá přístup).
Zřizování skupinových účtů a sdílení uživatelských účtů není dovoleno.
Řešení musí umožňovat implementaci přístupových profilů tak, aby byla pro každého uživatele použita příslušná úroveň oprávnění.
Řešení musí obsahovat minimálně dvě různé správcovské role – supervizor, který může nastavovat parametry v rámci aplikačního prostředí a administrátor, který je oprávněn provádět změny konfigurace systému, upgrady SW apod.
Dodavatel je povinen po akceptaci informovat o všech mechanismech v řešení, které umožňují obejití síťové a bezpečnostní infrastruktury (back door), a znemožnit jejich použití.
Logování
Systémový a/nebo aplikační bezpečnostní log musí zaznamenávat úspěšné i neúspěšné události minimálně v rozsahu:
• přihlášení a odhlášení
• informace o vypnutí/restartu systému

• import a export dat
• změny v metodě zabezpečení (včetně změn v nastavení logování)
Řešení dodavatele musí podporovat možnost vzdáleného logování do Logmanageru (případně SIEM).
Neúspěšné pokusy o autentizaci musí být logovány.
Zahájení a ukončení uživatelské relace musí být logováno.
Řešení musí zaznamenávat všechny akce uživatelů privilegovaných účtů (administrátoři a operátoři s právem konfiguračních změn).
Auditní mechanismus nesmí dovolit uživatelům a administrátorům modifikovat auditní záznamy.
V případě pokusu o neautorizovaný přístup nebo modifikaci auditních záznamů musí být o této události vygenerován záznam do logu.
Síťová bezpečnost
Komunikace mezi jednotlivými síťovými zónami a komunikace přes veřejné sítě musí být šifrována (povolené šifrovací algoritmy a délky šifrovacích klíčů stanoví Vyhláška o kybernetické bezpečnosti č. 82/2018). Je preferováno šifrování na základě certifikátů.
Bezpečnost software/aplikací
Všechny zranitelnosti dodané aplikace musí být ošetřeny do 2 měsíců od vydání oficiální bezpečnostní záplaty, resp. doporučeného postupu pro minimalizaci rizika zneužití.
Změny v aplikaci musí probíhat řízeně. Musí být minimalizovány a realizovány standardními postupy (nová verze balíčku, oficiální patch apod.).
Automatické odhlášení privilegovaného uživatele (administrátora, supervisora) musí být nastaveno po 15 minutách nečinnosti.
Bezpečnost webových aplikací
Identifikace a autentizace:
• Přístup ke zdrojům (stránky, soubory apod.) musí být podmíněn autentizací s výjimkou takových, které jsou deklarovány jako veřejné. Konkrétně přístup k osobním údajům bude umožněn pouze uživatelům, kteří byli jednoznačně identifikováni a ověřeni. Uživatelé musí být jednoznačně identifikováni a ověřeni aplikací, není povolen přístup generických (defaultních) uživatelů a sdílených účtů
• Všechny autentizační mechanismy musí být implementovány na straně serveru

• Všechny autentizační mechanismy musí pracovat s chybami bezpečným způsobem (zachytávání, bezpečná správa výjimek apod.)
• Aplikace musí uživatelům kdykoliv umožnit bezpečnou změnu autentizačních údajů
• Pole pro hesla nesmí zobrazovat znaky prostého textu (např. je nahrazují hvězdičkou), funkce autocomplete nesmí být povolena
• Mechanismy pro hesla musí být nastaveny tak, aby splňovaly požadavky VKB
• Pokusy o přístup k aplikaci (úspěšné i neúspěšné) musí být logovány
• Hesla nesmí být ukládána v prostém textu, pouze jejich hashe. K heslům (jejich hashům) smí přistupovat pouze autentizační modul aplikace s omezeným přístupem
• Veškerý kód, který implementuje nebo používá autentizační mechanismy nesmí být ovlivnitelný škodlivým kódem (malicious code)
• Pokud při autentizačním procesu uživatel překročí definovaným maximální počet neúspěšných pokusů o přihlašování, musí být účet zablokován
• Aplikace musí zajistit bezpečný mechanismus obnovení zapomenutých hesel. Tzv. "bezpečnostní otázky" nejsou povoleny.
Řízení přístupu:
• Uživatelé smí mít přístup pouze k funkcím, odkazům, službám, zdrojům a informacím pro které mají definovaná přístupová oprávnění
• Veškeré mechanismy řízení přístupu musí být implementovány na straně serveru
• Pokusy o přístup k funkcím/modulům a datům aplikace (úspěšné i neúspěšné) musí být logovány
Bezpečnost komunikace:
• SSL/TLS musí být použito pro všechna připojení, která:
- vyžadují autentizaci uživatele
- souvisejí s procesem změny hesla
- odesílají nebo přijímají data/citlivé funkce
- souvisí se správou aplikace
• Všechna připojení k externím systémům zahrnujícím výměnu dat/citlivé funkce musí být autentizována
• Všechna připojení k externím systémům s funkcí výměny dat/citlivých funkcí musí používat účet s nastavenými minimálními potřebnými oprávněními
• Všechny autentizační údaje k externím systémům a aplikacím musí být uloženy šifrovaně v úložišti s omezeným přístupem (nikoliv ve zdrojovém kódu)
• SSL certifikáty používané servery musí být podepsané certifikačními autoritami rozpoznatelné prohlížeči tak, aby uživatelům umožnily přístup k aplikaci
• Chyby v SSL spojení nesmí umožnit nezabezpečené spojení
• Chyby v SSL spojení musí být logovány
• Musí být definována jednotná znaková sada (např. UTF-8) pro všechna spojení
• Přenos citlivých dat a/nebo osobních údajů musí být šifrován.
Kryptografie:
• Všechny kryptografické funkce pro ochranu citlivých informací v rámci aplikace musí být implementovány na straně serveru
• Všechny vygenerované hashe pro ukládání hesel musí mít přidánu "sůl" (řetězec dostatečné délky pro zabránění útokům slovníku nebo hrubou silou)
Další požadavky

• Aplikace musí být schopna zvládnout chybějící, nadbytečné nebo přejmenované parametry (např. korektně zahlásit chybu)
• Skrytá pole ("hidden files") smí být použita pouze pro sekvencování stránek, nikdy nesmí být použita pro přenos dat
• Logika aplikace musí být imunní proti pokusům o její obcházení (např. změna pořadí kroků, obcházení kroků apod.)
• Aplikace nesmí obsahovat/zobrazovat žádné informace, které by útočníkovi pomohly k plánování/realizaci útoku
Legal compliance
Veškeré informace musí být zpracovávány v souladu s právními požadavky na zabezpečení informací, zejména se:
• zákonem 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, včetně navazujících vyhlášek, zejména vyhláškou 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
• zákonem 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů
• nařízením EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (GDPR)
• nařízením EU 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS)
• vyhláškou 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
Řízení software
Aplikace/web musí být zabezpečený; pokud je založen na platformách třetích stran (např. Java, Flash apod.), musí být kompatibilní s novými verzemi těchto platforem, aby se zabránilo narušení bezpečnosti díky chybám v nich odhalených.
Aktualizace softwaru nesmí mít žádný vliv na funkčnost. Pro každou aktualizaci softwaru musí být připravený mechanismus pro vrácení do stavu před aktualizací.
Validace a integrita dat
V případě použití webového grafického rozhraní musí být vstupy dat (uživatelské i automatizované) ověřeny z pohledu správnosti (má-li být na vstupu číslo, nelze akceptovat písmeno) a integrity, je-li to technicky realizovatelné.
Bezpečnost Cloudových služeb

Cloudové služby musí splňovat požadavky na bezpečnost dle právních předpisů.
Hesla
Hesla nesmí být při zadávání (ani v jiných případech) viditelná (např. se nahradí definovaným znakem).
Před změnou hesla musí být vyžadováno zadání stávajícího hesla.
Nové heslo musí být požadováno zadat dvakrát (jako prevence překlepů).
Opakování libovolného z posledních 12 použitých hesel nesmí být dovoleno.
Délka a další požadované parametry hesla musí být ověřeny před zapsáním změny (pokud nové heslo nevyhovuje, musí být uživatel upozorněn a vyzván z úpravě nového hesla).