Bezpečnostní požadavky

Obecné požadavky

1. **[P]** Všechny komponenty základního systému musí být záplatovatelné a aktualizovatelné. Dodavatel je povinen poskytnout dostatečně bezpečné metody pro ověření a kontrolu integrity aktualizačních balíčků (např. kontrolní součty SHA-2 nebo balíčky podepsané certifikátem).
2. **[P]** Pro firmware a software musí být přijata dostatečná bezpečnostní opatření, aby byla zajištěna celková softwarová integrita (není možné neoprávněně změnit konfiguraci anebo zdrojový kód software).
3. **[P]** Systém a všechny jeho komponenty musí být před nasazením do provozu aktualizovány na poslední verzi vydanou výrobcem s ověřenou funkcionalitou výrobcem k datu nasazení do provozu. Navíc musí být instalovány nejnovější bezpečnostní záplaty a servisní balíčky s ověřenou funkcionalitou systému.
4. **[P]** Mělo by být možné, aby provozní personál, který provádí správu, instaloval záplaty a aktualizace.
5. **[P]** Instalace a odinstalace záplat a aktualizací nesmí být prováděna automaticky.
6. **[P]** Pokud systém umožňuje vyvolat aktualizaci online (přes počítačovou síť), pak musí:
    a. Buď být možné nastavit v systému vzdálené vlastní úložiště pro stahování aktualizací (např. update server, repositář SW, …)
    b. Anebo musí výrobce / dodavatel umožnit přístup k vlastnímu takovému online úložišti a potřebné informace, aby bylo možno provádět aktualizace přes proxy server zákazníka.
7. **[P]** U všech komponent základního systému musí být při dodávce proveden bezpečnostní hardening:
    a. smazání nepotřebných výchozích uživatelů a účtů,
    b. odinstalace nebo vypnutí nepotřebných programů a utilit,
    c. zakázání nepotřebných síťových protokolů,
    d. vypnutí nepotřebných nebo potenciálně nebezpečných služeb (telnet, RSH, …).
    e. Tyto komponenty budou odstraněny nebo, pokud to technicky není možné, trvale zakázány a zabezpečeny proti náhodné reaktivaci, pokud nemají vliv na funkci a bezpečnost systému. Zabezpečení a základní konfigurace všech komponent systému musí být zdokumentována.
8. **[P]** Veškerým aktivitám uživatelů ve všech komponentách systému musí předcházet jednoznačná autentizace. Autentizace musí být založena na použití jména a hesla nebo certifikátu.
9. **[P]** Procesy autorizace a autentizace musí být implementovány tak, aby byla zajištěna ochrana před neautorizovaným přístupem. Všechny komponenty systému musí mít funkční mechanismy, které umožní bezpečné a

reprodukovatelné přihlášení, odhlášení a přepínání uživatelů mezi sebou při plném provozu systému.

10. **[P]** Události v systému musí být evidovány do deníku událostí (log file). Záznamy událostí musí minimálně obsahovat datum a čas včetně specifikace časového pásma, typ činnosti, identifikaci technického aktiva, které činnost zaznamenalo, jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, jednoznačnou síťovou identifikaci původce a úspěšnost nebo neúspěšnost činnosti. Musí být zaznamenávaný minimálně tyto události (dle VKB č. 82/2018 Sb.):
    a. Přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
    b. Činnosti provedené administrátory,
    c. Úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
    d. Neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
    e. Činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
    f. Zahájení a ukončení činností technických aktiv,
    g. Kritických i chybových hlášení technických aktiv,
    h. Přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí.
11. **[P]** Se systémovými logy nelze manipulovat pomocí neprivilegovaného účtu.
12. **[P]** Po uplynutí předem naprogramovaného počtu (3-5) neúspěšných pokusů o přihlášení musí být zaznamenán log o neúspěšném opakovaném přihlášení do deníku událostí.
13. **[P]** Systémy musí podporovat logování a zasílání logů na centrální lokalitu standardizovaným protokolem (Syslog, Windows Event Log, atd.) nebo vyčítaní logů pomocí software na to určeným.
14. **[P]** Systémy musí podporovat řízení přístupů na základě skupin a rolí (Role Based Access model).
15. **[P]** Systémy musí podporovat správu účtů (zakládaní a rušení), správu oprávnění účtů (například právo zapisovat i číst anebo jen číst konfiguraci).
16. **[P]** Když není možné ověřit identitu uživatele pomocí vícefaktorové autentizace nebo kryptografických klíčů, musí ověření pomocí přihlašovacího jména a hesla splňovat pravidla (dle VKB č. 82/2018 Sb. v aktuálním znění):
    a. Musí být možné nastavit minimální délku hesla a komplexitu hesla
    b. Musí umožňovat délky hesla alespoň:
        i. 12 znaků u uživatelů a
        ii. 17 znaků u administrátorů a systémových účtů
    c. Povinná změna hesla musí být nastavitelná a vynutitelná
    d. Systém musí umožnit uživatelům změnu hesla, přičemž doba mezi dvěma změnami nesmí být kratší než 30 minut. Tento požadavek musí zajišťovat buď samotné zařízení nebo externí autentizační systém (např. LDAP, RADIUS, TACACS+).

e. Systém nemůže umožnit použití dříve používaných hesel s pamětí alespoň 12 hesel. Tento požadavek musí zajišťovat buď samotné zařízení nebo externí autentizační systém (např. LDAP, RADIUS, TACACS+).
f. Systém musí uzamknout účet po 10 nebo méně neúspěšných pokusech o přihlášení.

17. **[P]** Heslo uživatelů nesmí být nikdy zobrazeno jako prostý text.
18. **[P]** Hesla nesmí být ukládána reverzibilním algoritmem.
19. **[P]** Systémy musí umožnovat změnu hesla pro uživatele. Změna hesla musí být možná pro všechny uživatele, samotnou změnu hesla musí být schopen provést minimálně administrátor systému.
20. **[P]** Platná změna hesla samotným uživatelem musí vždy vyžadovat platné přihlášení uživatele se starým heslem, zadání nového hesla a ověření platnosti identickým postupem.
21. **[P]** Systém musí podporovat kryptografii pro všechny síťové služby, u kterých to není v rozporu s jeho provozním hlediskem. Kryptografií jsou míněny prostředky šifrování a zajištění důvěrnosti a integrity přenášených dat mezi klientem a samotným systémem. Kryptografické prostředky (např. Certifikát s asymetrickým kryptografickým klíčem) musí být možné upravovat nebo nahrazovat (např. možnost nahrát vlastní certifikát podepsaný vlastní CA).
22. **[P]** Systémem musí být podporované dostatečně odolné kryptografické algoritmy a protokoly zabezpečení musí být systémem podporované s ohledem na aktuální nejlepší praktiky (best practice) v oblasti bezpečnosti ICT. Příkladem, nikoliv úplným výčtem může být:
    - Protokol TLS 1.2 a vyšší verze
    - Symetrická šifra AES-256 a vyšší
    - Asymetrická šifra RSA-3072 a vyšší
    - Hashovací funkce SHA-256 rodiny SHA2 a vyšší

    Podrobný seznam vyžadovaných doporučených a nežádoucích dosluhujících kryptografických algoritmů lze nalézt na stránkách NÚKIB viz https://www.nukib.cz/cs/infoservis/doporuceni/1843-doporuceni-v-oblasti-kryptografickych-prostredku-verze-2-0/ v aktuálním znění.

    Nesoulad s výše uvedenými doporučeními musí být řádně odůvodněn a zadavatelem schválen.

23. **[P]** Systém musí umožňovat bezpečnou práci s daty určité citlivosti oprávněnému uživateli (např. šifrováním v souborovém systému), pokud jejich důvěrnost není zajištěna jinými prostředky (systémovým firewallem, fyzickým přístupem, nutnou autentizací atd.)
24. **[P]** V případě, že je systém konfigurován / parametrizován vzdáleně (prostřednictvím počítačové sítě) nebo přes lokální rozhraní (např. sériový port), před samotnou konfigurací musí proběhnout autentizace. Pokud konfigurace /

parametrizace probíhá vzdáleně, musí být komunikace mezi klientem a systémem v šifrované podobě.

25. **[P]** Systém nesmí obsahovat neměnitelné účty nebo fixní servisní účty. Pokud takové účty jsou vyžadovány z provozního hlediska, nesmí umožňovat neoprávněný přístup anebo musí umožňovat autentizaci v souladu s dalšími bezpečnostními požadavky.
26. **[P]** OS a systém musí podporovat centralizovaný nástroj pro správu a ověření identity uživatelů, administrátorů, aplikací a jiných systémů a centralizovaný nástroj pro řízení přístupových oprávnění (centrální autentizace a autorizace).
27. **[P]** V případě operačního systému musí být možné nastavit BIOS/EFI/firmware heslo pro zabránění modifikace zavaděče či bootovacího pořadí.
28. **[P]** Systém s autentizací musí umožnit definovat minimálně 10 správcovských účtů.
29. **[P]** Pokud systém obsahuje alespoň základní operační systém, musí se v něm nacházet uživatelsky konfigurovatelný firewall.
30. **[P]** Systém musí ověřovat validitu všech přijatých zpráv ze všech rozhraní (kontrola syntaxe, datového formátu, rozsahu hodnot, atd.). Systém nesmí být ovlivnitelné poškozenými nebo deformovanými zprávami a zachovává si bezpečný stav i během nepředvídaných stavů selhání. Když systém selže, nesmí být ovlivněna důvěrnost nebo integrita.
31. **[P]** Rozhraní (LAN, USB, RS-232, atd.) systému musí být možné správcovsky deaktivovat. Při dodání systému je za deaktivaci nevyužitých rozhraní zodpovědný dodavatel.
32. **[P]** Systém nesmí být možné vypnout vzdáleně bez přihlášení (autentizace a autorizace).
33. **[P]** Musí být možná synchronizace reálného času.
34. **[P]** Systém a všechny jeho části budou nastaveny v souladu s volně dostupnou metodikou CIS (Center for Internet Security) minimálně do úrovně Level 1. Pokud pro některou část není dostupná metodika CIS, platí ostatní bezpečnostní požadavky. V případě, že je kterýkoliv požadavek metodiky v rozporu s provozním hlediskem, tato výjimka bude i s odůvodněním řádně zdokumentována.
35. **[NP]** Musí být možné vypnout automatické přihlášení do nouzového/single user/recovery režimu.
36. **[NP]** Musí být implementována funkce návratu do stavu před provedením upgradu (downgrade function).
37. **[NP]** Systém a komponenty musí být možné aktualizovat výhradně prostřednictvím digitálně podepsaných balíčků. Podepisovací standard (kryptografický algoritmus) musí být specifikován v nabídce.
38. **[NP]** Systém musí podporovat protokol 802.1X.
39. **[NP]** Systém musí umožnit dvoufaktorovou autentizaci.
40. **[NP]** V systému se musí nacházet dostatečné rezervy výpočetních prostředků pro aktualizaci bezpečnostní funkcionality (rezervy pro kryptografické algoritmy a zabezpečovací komunikační protokoly).

41. **[NP]** Systém musí být vybaven softwarovou ochranou pro detekci malware, exploitingu a jiných škodlivých aktivit, pokud je takový SW pro navržený operační systém dostupný a v dané aplikaci smysluplný. Provoz takové ochrany může být vyžadován bez nutnosti pravidelných aktualizací s ohledem na provozní hledisko a dostupnost systému.

Požadavky na dodavatele a dokumentaci

- Dodavatel musí sdělit verzi a vydání operačního systému a užívaných komponent (např. verzi SSH serveru/Web serveru) a umožnit zákazníkovi kontrolu bezpečnostních parametrů. [P]
- V případě odhalení kritické zranitelnosti je po dodavateli systému požadováno dodání opravných balíčků, a to jak pro operační systém, tak i pro aplikace a další komponenty. [P]
- Dodavatel musí prokázat, zda má své vlastní řízení informační bezpečnosti i bezpečnostní pravidla a opatření s odpovídající úrovní reportingu, včetně možností provádění auditů. [P]
- Dodavatel musí dát skupině E.ON možnost přiměřeného, individuálního a z ekonomického hlediska rozumného vlivu na jeho informační bezpečnost a provádění auditů a je povinen zajistit tento audit i u subdodavatelů. [P]
- Dodavatel je povinen v rámci dokumentace pro poskytované řešení zpracovat logovací příručku pro systémové, bezpečnostní a aplikační logy s popisem a vysvětlení jednotlivých událostí. [P]
- Dodavatel je povinný dodržovat v rámci řešení RFC a IEC standardy protokolů a na případné customizace upozornit a detailně je popsat.[P]
- Dodavatel je povinen v rámci dokumentace zpracovat komunikační matici poskytovaného řešení v následujícím rozsahu (Source IP(s), Destination IP(s), Source port(s) range, Destination port(s), L7 Protocol) e.g. [P]

Src. IP(s)	Src. Port(s)	Dst.IP(s)	Dst. Port(s)	L7 Proto
1.1.1.1	Any	2.2.2.2	445	SMB
2.2.2.2	Any	3.3.3.3	3389, 443	RDP,HTTPs

- Dodavatel má certifikaci dle ISO/IEC 27001. [P]
- Výrobce systému dodá výsledek penetračních testů celého systému. [NP]
- v případě, že jsou penetrační testy součástí dodávky a jsou hrazeny dodavatelem v rámci nabízeného řešení, je dodavatel povinen zpřístupnit kompletní výsledky testů objednateli. [P]

Požadavky na bezpečnostní testování

- Před nasazením komponenty nebo celého systému proběhne bezpečnostní testování. Bezpečnostní testování může být vyžadováno i v případě aktualizace projektu nebo jiných významných konfiguračních změn.
- Bezpečnostní testování může být prováděno jednorázově, před nasazením produktu do provozu nebo v pravidelných i nepravidelných intervalech v souladu s plány a požadavky na kybernetickou bezpečnost.
- Bezpečnostní testování může zahrnovat:
    - sken zranitelností,
    - bezpečnostní a penetrační testy,
    - porovnání aktuálního stavu bezpečnosti testovaného řešení se zadanými bezpečnostními požadavky, dokumentací a požadovanou bezpečnostní metodikou.

Dodavatel je zejména povinen:

- zabezpečit přímé přístupy, práva a oprávnění k celé dodávané infrastruktuře dle požadavků testovacího týmu (např. kompletní sudo u linuxových systémů, admin práva na windows, root); tyto požadavky budou bez zbytečného odkladu poskytnuty před zahájením testů;
- poskytnout potřebnou dokumentaci a dle možností, požadavků a v souladu se smluvními a licenčními ujednáními mezi dodavatelem a objednavatelem i zdrojové kódy, klíče a certifikáty k danému řešení;
- umožnit skenování zranitelností před provedením penetračních testů;
- dodavatel před testováním poskytne kompletní seznam HW a SW prvků prověřovaného řešení včetně provozovaných verzí jednotlivých SW komponent (operační systémy, firmware, SW) a další technické údaje k řešení (např. adresace, architektura systému);
- testování může způsobit selhání testovaného prostředí, a na základě toho musí být dodavatel připraven provést jeho případné obnovení (až na úrovni disaster recovery); případná nedostupnost systému způsobená v průběhu bezpečnostního testování se nezapočítává do stanovených parametrů dostupnosti služby stanovených v SLA;
- po dokončení testování je dodavatel bez zbytečného odkladu povinen vrátit všechna nastavení (účty, přístupy apod.) do původního stavu, pokud se s objednatelem nedohodne jinak;
- v projektu dodávky a implementace řešení vyhradit zdroje pro součinnost při bezpečnostním testování;

Objednatel je zejména povinen:

- oznámit dodavateli, jak bude bezpečnostní testování probíhat a co bude předmětem testování;
- v případě pravidelných skenů informovat dodavatele o jejich termínech;

Obecné informace k bezpečnostnímu testování:

- testování musí proběhnout před začátkem platnosti servisních smluv;
- řešení nálezů z bezpečnostního testování je vyjmuto ze servisní smlouvy (servisní smlouva nebude pro tyto případy platit);
- bezpečnostní testování musí být uzavřeno před uvedením do pilotního provozu, tj. ověření, že nálezy byly odstraněny nebo akceptovány objednavatelem;
- bez uzavřeného bezpečnostního testování nebude řešení převzato do produkčního provozu;
- v rámci poskytnutí součinnosti při bezpečnostním testování musí být v projektu dodávky a implementace vyhrazeny dostatečné/přiměřené zdroje na straně dodavatele;
- bezpečnostní testování může vycházet z metodik CIS, případně jiných bezpečnostních metodik;

V případě použití operačního systému Windows nebo jednoho z distribuce Linuxu, jsou vyžadovány i následující požadavky:

- **Požadavky na systémy s OS Windows:**
    - Uživatel se nesmí přihlásit s účtem Microsoft account. [P]
    - Musí být možné vypnout všechny služby volající API třetích stran (Skype, WiFi sync atd.). [P]
    - Musí být možné vypnout anonymní SID / překlad adres. [P]
    - Musí být možné zakázat anonymní enumeraci SAM účtů. [P]
    - Musí být možné vynutit neaplikování přístupových práv "Everyone" pro anonymní účty. [P]
    - Musí být možné vypnout lokální systémový NULL session fallback. [P]
    - Musí být možné nastavit Windows firewall pro všechny profily (doména, privátní, veřejný). [P]
    - Musí být možné nastavit Windows firewall pro všechny profily na blokování příchozího síťového provozu. [P]
    - Musí být možné nainstalovat a použít Microsoft baseline security analyzer. [P]
    - Uživatelé / aplikace nesmí mít privilegium "Systém". [NP]
    - Lokálně musí být možné se přihlásit jenom s privilegiem Administrátor. [NP]
    - Uživatel s privilegiem Guest se nesmí přihlásit ani jako služba, dávkový soubor, lokálně nebo přes RDP. [NP]
    - Účet guest musí být možné vypnout. [NP]
    - Musí být možné nastavit časovou lhůtu, po které je přístup uzamčen a vyžaduje reautentizaci. [NP]
    - Named pipes nelze použít pro anonymní účty. [NP]
    - Sdílené složky nesmí být možné připojit anonymně. [NP]
    - Musí být možné vynutit neukládání LAN manager hashů. [NP]
    - Musí být možné nastavit LAN manager autentifikační úroveň na NTLMv2 a explicitně odmítnout LM a NTLM. [NP]
    - Všechny svazky musí být možné používat na NTFS. [NP]
    - Musí být možné instalovat software na kontrolu integrity lokálních systémových souborů. [NP]
    - Lze konfigurovat oprávnění a přístup k registrům. [NP]

- **Požadavky na systémy s OS Linux:**
    - Musí být možné vytvořit separátní partici pro /tmp s nastavením nodev, nosuid, noexec. [P]
    - Musí být možné vytvořit separátní partice pro /var, /var/log, /var/log/audit a /home. [P]
    - Musí být možné bind mountnovat /var/tmp na /tmp. [P]
    - Musí být možné nastavit příznak nodev pro /home. [P]
    - Musí být možné nastavit nodev, nosuid, noexec příznaky pro /dev/shm. [P]
    - Všechny world-zapisovatelné složky musí být možné nastavit sticky bit. [P]
    - U souboru /boot/grub2/grub.cfg nebo ekvivalentního musí být možné nastavení vlastnictví pro root a pouze root může soubor editovat. [P]
    - Pro zavaděč (Grub) musí být možné aktivovat heslo. [P]
    - Na systému nesmí být aktivovány legacy služby (např. telnet-server; rsh, rlogin, rcp; ypserv, ypbind; tftp, tftp-server; talk, talk-server). [P]
    - Musí být možné vypnout služby a aplikace startované v kontextu xinetd nebo inetd. [P]
    - Musí být možné vypnout xinetd. [P]
    - Musí být možné vypnout legacy služby (chargen-dgram, chargen-stream, daytime-dgram, daytime-stream, echo-dgram, echo-stream, tcpmux-server). [P]
    - Musí být možné vypnout/blokovat IP forwarding. [P]
    - Musí být možné vypnout/blokovat paketové přesměrování. [P]
    - Musí být možné vypnout/blokovat source routované pakety. [P]
    - Musí být možné vypnout akceptaci ICMP přesměrování. [P]
    - Musí být možné zapnout ignoraci broadcastů. [P]
    - Musí být možné aktivovat ochranu vůči Bad error message. [P]
    - Musí být možné aktivovat TCP/SYN cookies. [P]
    - Musí být možné používat SSH jenom ve verzi 2. [P]
    - Před nasazením do provozu musí být možno prověřit soubory pro PAM (/etc/pam.d/*). [P]
    - Na systém nesmí být aktivován X Windows systém. [NP]
    - Musí být možné vypnout X Font server. [NP]
    - Musí být možné omezit core dumpy. [NP]
    - Musí být možné zapnout Randomized Virtual Memory Region Placement. [NP]
    - Každý daemon musí mít nastavenou adekvátní umask. [NP]
    - Musí být možné explicitně vyjmenovat IP adresy v kontextu OS, které se můžou připojit k provozovaným službám. [NP]
    - Musí být možné nastavení logovací úrovně SSH na úroveň INFO. [NP]
    - Nesmí být možné se vzdáleně přihlásit jako root přes SSH. [NP]
    - SSH musí mít nastaveno PermitEmptyPasswords na No. [NP]

- Musí být možné instalovat a využívat AIDE. [NP]
- Musí být možné využívat SELinux a aplikační software má přítomná pravidla a nastaveny kontexty. [NP]
- Musí být možné využívat OSSec HIDS. [NP]
- Operační systém musí mít aktivováno auditování (auditd). [NP]
- Hesla musí být hashovaná SHA-512. [NP]
- Lze omezit root přihlašování na systémovou konzoli. [NP]

Legenda zkratek

API	Application programming interface
BIOS	Basic Input Output System
CIS	Center for Internet Security
HW	Hardware
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commisision
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
LM	Lan Manager
[NP]	Nepovinný
NTFS	New Technology Filesystem
NTLM	NT Lan Manager
OS	Operační systém
[P]	Povinný
PAM	Pluggable Authentication Modules
RDP	Remote Desktop
RFC	Request for Comment
RSH	Remote Shell
SAM	Security Account Manager
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SID	Security Identifiers
SLA	Service-level agreement
SSH	Security Shell
SW	Software
TCP	Transmission Control Protocol
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VKB	Vyhláška o kybernetickej bezpečnosti