

Požiadavky na informačné systémy a súvisiacu infraštruktúru v oblasti kybernetickej bezpečnosti

Platformy s operačným systémom Windows alebo Unix/Linux

Obsah

1	Účel dokumentu	1
2	Všeobecné požiadavky	1
3	Hardening	2
4	Logovanie	3
5	Požiadavky na aplikáciu	3
5.1	Proces prihlasovania do aplikácie	3
5.2	Heslá používateľov aplikácie	3
5.3	Logovanie	4
5.4	Sieťový profil aplikácie.....	4
6	Požiadavky na prevádzkovanie riešenia v prostredí LPS SR	4

1 Účel dokumentu

Tento dokument poskytuje zoznam požiadaviek v oblasti kybernetickej bezpečnosti na informačné systémy a súvisiacu infraštruktúru, ktoré sú do LPS SR dodávané a implementované na platformách s operačným systémom Windows alebo Unix/Linux.

Tento dokument by mal byť súčasťou špecifikácie technických požiadaviek pri obstarávaní systémov. Požiadavky uvedené v kapitole 6 majú byť predmetom rokovania o servisnej zmluve s dodávateľom riešenia.

2 Všeobecné požiadavky

- a) Riešenie musí využívať len také nastavenia TLS protokolov, kryptovacích algoritmov, kryptovacích kľúčov, hash funkcií a ostatných bezpečnostných komponentov a riešení, ktoré

sú podľa rozhodnutia relevantných inštitúcií (NIST, PCI SSC, NSA, NBÚ) považované za bezpečné.

- b) Riešenie musí pridelovať pre všetkých používateľov jednoznačný identifikátor na autentizáciu na vstup do informačného systému,
- c) Parametre silného hesla, ktoré je všeobecne používané v procese autentifikácie, sú: dĺžka silného hesla je minimálne desať znakov, heslo musí obsahovať veľké a malé písmená a číslice.

3 Hardening

Dodané riešenie

- a) musí byť inštalované na minimálnej potrebnej konfigurácii operačného systému, napríklad *Server Edition* alebo *Server Core*
- b) musí mať odinštalované všetky procesy a služby, ktoré nie sú nevyhnutne potrebné pre beh aplikácií riešenia
- c) musí mať deaktivované všetky implicitné procesy a služby, ktoré nie sú nevyhnutne potrebné pre beh aplikácií, vrátane
 - i. OS Windows Client for Microsoft Networks
 - ii. OS Windows File and Printer Sharing for Microsoft Networks
 - iii. OS Windows Link Layer Topology Discovery
- d) musí mať odstránené všetky nepotrebné systémové účty
- e) musí mať deaktivované všetky nepotrebné implicitné systémové účty
- f) musí mať aktívny lokálny firewall, ktorý je nakonfigurovaný na princípe „least privilege“ pre všetky aktívne služby prístupné cez sieť, vrátane implicitných služieb ako Microsoft RPC, DFS a podobne. Pravidlá lokálneho firewall-u musia byť doladené na minimálny možný rozsah počas fázy Site Acceptance Tests SAT.
- g) musí mať nastavené heslá všetkých účtov systému na hodnoty, ktoré spĺňajú parametre silného hesla, pozri bod 2c)
- h) musí mať zmenené heslá všetkých software komponentov systému z východných (default) hodnôt na heslá, ktoré spĺňajú parametre silného hesla, pozri bod 2c)
- i) v prípade operačného systému Linux, ktorý umožňuje aktivovať funkciu name-based mandatory access controls, napr. s využitím modulu AppArmor, musí byť takýto modul aktivovaný v móde *enforce* a všetky aplikácie systému prístupné cez sieť musia v ňom mať aktivovaný svoj bezpečnostný profil
- j) musí mať aktivovanú funkciu pre automatické odhlásenie (log-out) po definovanej dobe nečinnosti používateľa
- k) v prípade operačného systému Linux musí mať aktivovaný framework Linux Audit. Dodatočné špecifické pravidlá pre Audit (napríklad sledovanie prístupu ku konfiguračným súborom) môžu byť predmetom implementácie počas fázy Site Acceptance Tests SAT
- l) musí byť časovo synchronizované s určeným lokálnym NTP serverom
- m) v prípade, že súčasťou riešenia sú dodávané HW komponenty (napríklad servery), musia byť dodané s aktuálnymi verziami svojho software vybavenia (firmware)
- n) v prípade, že súčasťou riešenia sú dodávané HW komponenty (napríklad servery), všetky heslá pre ich firmware musia byť nastavené na hodnoty, ktoré spĺňajú parametre silného hesla, pozri bod 2c)
- o) by malo umožniť monitorovanie záťaže CPU, pamäte a diskového priestoru systému. V prípade prekročenia definovaných hodnôt záťaže by malo vytvoriť notifikáciu pre správcu systému.

4 Logovanie

Dodané riešenie

- a) musí zabezpečiť dostatočnú diskovú kapacitu pre uchovávanie systémových a aplikačných logov pre podnikom stanovenú dobu, minimálne však 6 mesiacov
- b) musí zabezpečiť prístupové práva k súborom s log záznamami limitované na minimum
- c) musí umožniť konfiguračne nastaviť integráciu logovania aplikácie do logger framework operačného systému (napríklad syslog pre riešenia na platforme Unix/Linux)
- d) musí mať na úrovni operačného systému aktivované generovanie log správ obsahujúcich informácie o udalostiach ako úspešné a neúspešné pokusy o prihlásenie používateľa do systému, pokusy o eskaláciu privilégií, zastavenie/spustenie služby, vytvorenie/odstránenie používateľa alebo skupiny používateľov
- e) musí mať aktivovanú konfiguráciu pre posielanie systémových a aplikačných logov pre vybrané kategórie správ v móde prenosu syslog, Windows Event Forwarding (WEF) alebo MSE (Microsoft Security Event) na externý log server

5 Požiadavky na aplikáciu

5.1 Proces prihlasovania do aplikácie

V prípade, že aplikácia implementuje svoju databázu používateľov a proces ich autentifikácie pri prihlasovaní do aplikácie, aplikácia musí spĺňať nasledovné požiadavky:

- a) Aplikácia musí zabezpečovať, aby pri prihlasovaní neboli zobrazované žiadne systémové alebo aplikačné identifikátory, pokiaľ nebude proces prihlasovania dokončený
- b) Aplikácia musí zabezpečovať, aby bolo možné nastaviť varovný text pre neoprávnené používanie aplikácie (napríklad pred prihlásením používateľa do aplikácie)
- c) Aplikácia musí zabezpečovať, aby pri prihlasovaní sa nezobrazovali žiadne nápomocné informácie. V prípade neúspešného prihlásenia aplikácia nesmie uvádzať, ktorá časť prihlasovacích údajov je nesprávna
- d) Aplikácia musí zabezpečovať, aby sa pri zadávaní hesla nezobrazoval jeho text
- e) Aplikácia musí zabezpečovať, aby sa po definovanej dobe nečinnosti uskutočnilo automatické odhlásenie používateľa (idle timeout)
- f) Aplikácia musí zabezpečovať, aby sa po definovanom počte neúspešných pokusov o prihlásenie používateľa jeho účet uzamkol
- g) Aplikácia by mala zabezpečovať, aby sa po prihlásení zobrazil dátum a čas predchádzajúceho úspešného prihlásenia.

5.2 Heslá používateľov aplikácie

V prípade, že aplikácia implementuje svoju databázu používateľov a proces ich autentifikácie pri prihlasovaní do aplikácie, aplikácia musí spĺňať nasledovné požiadavky:

- a) Aplikácia musí umožňovať všetkým používateľom nastavovanie svojich vlastných hesiel
- b) Aplikácia musí umožňovať pravidelnú zmenu hesla a nastavovať časový interval na vynútenie zmeny hesla
- c) Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla
- d) Aplikácia musí pri zmene hesla vyžadovať dvakrát zadanie nového hesla.
- e) Aplikácia musí pre ukladanie hesiel používať štandardné a bezpečné hash algoritmy

- f) Aplikácia musí mať nastavené heslá všetkých účtov systému na hodnoty, ktoré spĺňajú parametre silného hesla, pozri bod 2c)
- g) Aplikácia by mala vyžadovať zmenu hesla po prvom prihlásení.

5.3 Logovanie

- a) Aplikácia musí zaznamenávať do svojich logov nasledujúce udalosti:
 - štart alebo reštart aplikácie s informáciou o software verzii spúšťanej aplikácie a načítaných konfiguračných súboroch
 - V prípade, že aplikácia implementuje svoju databázu používateľov a proces ich autentifikácie pri prihlasovaní do aplikácie, aplikácia musí zaznamenávať do svojich logov nasledujúce udalosti:
 - o úspešné a neúspešné prihlásenie a odhlásenie používateľa do aplikácie
 - o úspešné a neúspešné vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny
 - o žiadosť používateľa o zmenu hesla v aplikácii
- b) Aplikácia by mala zaznamenávať do svojich logov nasledujúce udalosti:
 - zmeny konfigurácie aplikácie
 - chybové a iné závažné udalosti aplikácie

Zápis aplikačného logu by mal obsahovať nasledujúce polia:

- Typ alebo kód aktivity/akcie (napr. autorizácia, vytvorenie, aktualizácia, zmazanie, akceptovanie požiadavky sieťového spojenia a pod.)
- Subsystem vykonávajúci aktivitu (napr. názov alebo identifikátor procesu, transakcie)
- Identifikátory subjektu na ktorom bola uskutočnená aktivita (napr. meno používateľa, meno počítača, IP adresa, MAC adresa a pod.)
- Identifikátory objektu na ktorom bola aktivita uskutočnená (napr. názvy súborov, identifikátor záznamu v tabuľke, meno používateľa, meno počítača, IP adresa, MAC adresa a pod.)
- Zmena (hodnota parametra pred a po uskutočnení aktivity)
- Dátum a čas vykonania akcie vrátane relevantných informácií o formáte a časovom pásme, ak nie sú v koordinovanom svetovom čase
- Výsledok úspešnosti aktivity (napr. či aktivita bola uskutočnená alebo zamietnutá)
- Opis/kód príčiny zamietnutia aktivity

5.4 Sieťový profil aplikácie

- a) Riešenie musí mať zdokumentovaný zoznam používanej sieťovej komunikácie s podrobnosťami o využívaných sieťových protokoloch (TCP/UDP porty a podobne)

6 Požiadavky na prevádzkovanie riešenia v prostredí LPS SR

V tejto časti sú uvedené požiadavky na prevádzkovanie riešenia v prostredí LPS SR, ktoré majú byť predmetom rokovania o servisnej zmluve s dodávateľom.

- a) Dodané riešenie musí umožňovať inštalovať a aktivovať publikované bezpečnostné aktualizácie operačného systému. V prípade, že bezpečnostná aktualizácia operačného systému by spôsobila nefunkčnosť aplikácie, musí dodávateľ riešenia zabezpečiť potrebné úpravy aplikácie tak, aby bolo možné publikovanú bezpečnostnú aktualizáciu operačného systému inštalovať a aktivovať. Časový rámec inštalácie a aktivácie bezpečnostnej aktualizácie je predmetom dohody dodávateľa a LPS SR.
- b) Dodané riešenie musí umožňovať inštalovať a aktivovať publikované bezpečnostné aktualizácie software komponentov (sw knižníc) tretích strán použitých v aplikácii. V prípade, že bezpečnostná aktualizácia týchto komponentov by spôsobila nefunkčnosť aplikácie, musí dodávateľ riešenia zabezpečiť potrebné úpravy aplikácie tak, aby bolo možné publikovanú bezpečnostnú aktualizáciu komponentov inštalovať a aktivovať. Časový rámec inštalácie a aktivácie bezpečnostnej aktualizácie je predmetom dohody dodávateľa a LPS SR.
- c) Dodané riešenie musí umožňovať prechod na vyššiu verziu operačného systému v prípade, že aktuálne používaná verzia operačného systému prestala byť podporovaná výrobcom operačného systému a v danej verzii sú publikované zraniteľnosti, pre ktoré už neexistujú bezpečnostné aktualizácie. V prípade, že prechod na vyššiu verziu operačného systému by spôsobil nefunkčnosť aplikácie, musí dodávateľ riešenia zabezpečiť potrebné úpravy aplikácie tak, aby bolo možné prechod na vyššiu verziu operačného systému realizovať. Časový rámec inštalácie a aktivácie novej verzie operačného systému je predmetom dohody dodávateľa a LPS SR.
- d) Dodané riešenie musí poskytovať bezpečnostné aktualizácie pre zraniteľnosti aplikácie, ktoré identifikuje samotný dodávateľ v rámci svojich interných bezpečnostných analýz. V prípade, že bezpečnostná aktualizácia by spôsobila nefunkčnosť aplikácie, musí dodávateľ riešenia zabezpečiť potrebné úpravy aplikácie tak, aby bolo možné bezpečnostnú aktualizáciu aplikácie inštalovať a aktivovať. Časový rámec inštalácie a aktivácie bezpečnostnej aktualizácie je predmetom dohody dodávateľa a LPS SR.
- e) Distribúcia bezpečnostných aktualizácií aplikácie sa musí uskutočňovať bezpečným spôsobom, prostredníctvom komunikačného kanála, ktorý zabezpečuje verifikáciu integrity a autenticity aktualizácie.
- f) v prípade, že súčasťou riešenia sú dodávané HW komponenty (napríklad servery), dodané riešenie musí umožňovať inštalovať a aktivovať publikované bezpečnostné aktualizácie pre software týchto HW komponentov. V prípade, že bezpečnostná aktualizácia týchto komponentov by spôsobila nefunkčnosť aplikácie, musí dodávateľ riešenia zabezpečiť potrebné úpravy aplikácie tak, aby bolo možné publikovanú bezpečnostnú aktualizáciu komponentov inštalovať a aktivovať. Časový rámec inštalácie a aktivácie bezpečnostnej aktualizácie je predmetom dohody dodávateľa a LPS SR.