Prevádzkové odporúčania na bezpečné používanie e-Testu

1. Všeobecné bezpečnostné princípy

Princíp udržania bezpečnosti systémov zaistí, že počas testovania nedôjde k neželanému narušeniu funkčnosti systému a narušeniu bezpečnosti spracovaných údajov. **Princíp použiteľnosti systému** – po aplikovaní bezpečnostných pravidiel bude systém použiteľný na bežné pracovné úlohy.

1.2 Základné pravidlá

Nasledujúci zoznam obsahuje **základné bezpečnostné pravidlá** na zaistenie bezpečnosti a ochrany údajov na počítačoch.

1. Všetci používatelia počítačov v učebniach sú poučení o základnej počítačovej bezpečnosti a pravidlách bezpečnosti IT školy.
2. Na počítačoch je nainštalovaný a pravidelne aktualizovaný antivírusový program. Požaduje sa mať zapnutý antivírusový program v aktuálnom čase testovania.
3. V operačnom systéme sú nainštalované všetky bezpečnostné aktualizácie vydané výrobcom. Aktualizácia má byť automatická. Nemajú sa používať operačné systémy bez existujúcej podpory výrobcu (napr. Windows XP).
4. Používatelia sú poučení, aby neotvárali na počítačoch žiadne podozrivé emaily a prílohy, ktorých obsah je podozrivý, resp. neznámy.
5. Používatelia majú prístup k počítačom len na úrovni bežných používateľov, bez možnosti získania administrátorských práv k systému.
6. Používatelia sa prihlasujú k systémom jedinečným menom a heslom. Identifikačné a autentifikačné údaje nesmú byť medzi používateľmi zdieľané.
7. Prístupové účty sú rozdelené na správcovské a používateľské. Na bežnú prácu a testovanie v rámci škôl sa používajú používateľské účty bez možnosti zmeny systémových nastavení a inštalácie aplikácií.
8. Exspirácia hesiel je najviac 12 mesiacov a automatická kontrola zabráni opakovaniu najmenej troch naposledy použitých hesiel.
9. Systémy by mali byť po inštalácii zálohované, aby bolo možné vrátiť sa k pôvodnej konfigurácii.
10. Šetrič obrazovky sa aktivuje do 15 minút a požaduje zadanie hesla pri obnove.
11. Zdieľanie v rámci siete je riadené a sú popísané pravidlá na zdieľanie súborov.
12. Na počítačoch nie sú nainštalované lokálne serverové riešenia (napr. IIS, Apache).
13. Všetky nepotrebné sieťové služby sú zakázané na úrovni lokálneho firewall-u.
14. Zmena používateľských hesiel môže byť realizovaná maximálne raz denne.
15. Systém, po piatich neúspešných pokusoch o prihlásenie, zablokuje prístup k účtu na definovaný čas (minimálne 15 minút).

2. Sieťové prostredie v testovacích miestnostiach

Testovanie prebieha na počítačoch pripojených do siete s prístupom na internet. Prípustný je akýkoľvek model zapojenia siete, pri ktorom je možné spravovať

a monitorovať sieťový prenos minimálne na úrovni základných pravidiel firewall-u na perimetri sieťového prostredia školy.

V sieti je nastavená rezervácia MAC adries pre jednotlivé počítače určené na testovanie a prideľovanie IP na základe tejto rezervácie.

V prípade, ak je v rámci školskej siete prevádzkovaných viacero učební, resp. podsietí (vrátane bezdrôtových sietí), konkrétna učebňa určená na certifikačné testovanie má byť oddelená v rámci separátneho segmentu siete bez možnosti priameho prístupu z iných segmentov. V rámci segmentu sú na úrovni centrálneho sieťového prvku zablokované všetky nepotrebné sieťové služby, vrátane ICMP služieb.

Ak nie je prístup medzi počítačmi riadený sieťovým zariadením, sú na úrovni počítačov nastavené pravidlá lokálnych firewall-ov zabraňujúce prístup z iných počítačov v rámci daného segmentu siete. Lokálne pravidlá zároveň majú blokovať všetky nevyužívané sieťové služby.

3. Aplikácia Offline testovanie

Na certifikačné testovanie sa používa **aplikácia Offline testovanie**. **Jej súčasťou je LockDown Browser**, ktorý sa správa rovnako ako klasický internetový prehliadač s výnimkou niektorých úprav a zabezpečenia (znefunkčnené ovládanie, blokovanie aplikácií, atď).