Flash disky a USB zařízení – dobrý sluha, ale špatný pán informačního systému

Autor : Martin HANZAL,
Chief Executive Officer
E-mail : martin@sodatsw.cz

SODATSW spol. s r. o.; Horní 32; Brno; Czech Republic

www.usbpodkontrolou.cz
www.sodatsw.cz

Problém USB

- Přes USB rozhranní je možné připojit libovolné zařízení
- USB flashky jsou k dispozici za cca 200,- Kč za 4GB
- USB flashky umí použít téměř každý uživatel

Situace v organizacích

- Většina organizací nemá vytvořenou politiku pro používání USB zařízení
- Cestou není obecné zakázání používání USB zařízení
- Organizace do budoucna musí zavést řízení používání USB zařízení

Hlavní motivace

Informace zveřejněné Gartnerem, že 95% útoků na informační systémy organizací znamenající ztrátu pro organizaci je prováděno vlastními zaměstnanci

Jak postavit plot ...

... kolem IS organizace

Proč je zapotřebí plot?

- Přes USB flashky je možné zanést do IS škodlivý kód
- Přes USB flashky je možné během krátké doby vynést většinu informací informačního systému
- K provedení útoku není zapotřebí žádných speciálních dovedností

Největší čtyři chyby v uvažování organizací

- „Všechna data organizace jsou v databázi na serveru ...“
- „Nemůžeme přece omezovat uživatele v práci zbytečně složitým systémem ...“
- „Uživatelé - odpovědnost za to, co se děje s daty mají správci IT ...“
- „Správci – za data a práci s nimi odpovídají uživatelé ...“

Data na serverech

- Klientské aplikace pracující s daty na serverech umožňují jejich export do souborů na jakýkoli disk (i výměnný)
- Mnoho dokumentů je pouze součástí mailů či lokálních souborů
- Uživatelé si u sebe uchovávají daleko více dat, než potřebují

Omezování uživatelů

- Tento mýtus vzniká při neexistenci jednoznačné bezpečnostní politiky organizace
- V prostředí IS přece nemůže panovat anarchie
- IS organizace se musí používat z jasným cílem

Uživatelé a odpovědnost

- Uživatelé si myslí, že za všechno odpovídají správci IT
- Správci IT zabezpečili již dříve celé prostředí proti většině hrozbám
- Uživatelé musí vykonávat svoji práci a ne se zabývat nějakými omezeními

Správci IT a odpovědnost

- Mnohdy správci IT nedokáží prosadit prostředky, které jsou nezbytné pro bezpečnou práci v IS
- Když nastane incident, tak vinu nesou právě správci IT
- Při incidentu nikoho nezajímá, že na to dříve správci upozorňovali

A přitom …

Řídit práci s USB zařízeními je stejně jednoduché jako provozovat antivir nebo jiný podobný systém

Tři úrovně řízení USB

- Monitoring – detailní vytváření logů o používání USB zařízení a pohybu souborů mezi IS a USB flashkami
- Restrikce – řízení přístupu pouze k důvěryhodným USB zařízením
- Ochrana obsahu – kryptografická ochrana přenášený souborů

Monitoring

- Identifikuje používání USB
- Je možné určit potřebná USB pro IS
- Lze zjistit pohyb dat mezi IS – jak dovnitř, tak ven
- Celkově umožňuje správě IS se zorientovat
- Tlak na odpovědnost uživatelů

Restrikce

- Zabrání použití nebezpečných USB zařízení
- Prevence před zavlečením škodlivých kódů
- Prevence před zcizením interních dat
- Mnohdy velmi těžké definovat politiku restrikcí

Ochrana obsahu

- Šifrování souborů ukládaných na USB flashky
- Možnost použití USB flashek pouze v rámci IS organizace
- Zabezpečení přenosu souborů

Jak problém řeší Windows

- Monitoring není součástí OS
- Velmi jednoduché restrikce lze nastavit přes GPO
- Pohled na restrikce – černá/bílá
- Prostředky OS nelze použít na ochranu přenášených souborů

Řešení ve Windows do budoucna

- Zavedení UAC ve Windows Vista může být směrem k zamezení vkládání souborů do IS, ale prakticky je zatím nepoužitelné
- UAC neřeší a v budoucnu řešit nebude přenos souborů z vnitřního IS ven
- Windows 7 v této oblasti nedozná změn

Pro koho je zavedení USB pod kontrolou přínosem?

- Vedení organizace
- Správu bezpečnosti
- Správu IT
- Loajální zaměstnance
- Sabotéry

A nezapomeňte ...

že 95% útoků na informační systémy organizací znamenající ztrátu pro organizaci je prováděno vlastními zaměstnanci

Díky za pozornost

Autor : Martin HANZAL,
Chief Executive Officer
www.usbpodkontrolou.cz
E-mail : martin@sodatsw.cz