# Monitoring uživatelů – zkušenosti z praxe

## Proč monitorovat? Kde monitorovat? Příklady z praxe.

Autor: Martin Ondráček, Product Director
SODATSW spol. s r. o., Horní 32, Brno, Czech Republic

sodat sw

Efektivita a bezpečnost informací

# O nás - SODATSW spol. s r.o.

- Ryze česká společnost vyvíjející software pro správu a bezpečnost pracovních stanic
- Dodavatel a integrátor bezpečnostních řešení pro IT
- Více než 15 let tradice v oboru
- 50 000 instalací v České republice, jednička ve svém oboru v ČR
- Zákazníci z oblasti státní správy, bankovního sektoru, komerční sféry i školství
- Microsoft Partner, ISO 9001:2008, ISO 27001:2006, Osvědčení  NBU pro přístup k utajovaným informacím stupně DŮVĚRNÉ

# Jakou má souvislost monitoring aktivit uživatelů a bezpečnost?

- Bezpečnost informačních technologií je vždy jen na takové úrovni, na jaké je jejich nejslabší článek.
- Tím je obvykle koncový uživatel.
- Bez ohledu na úroveň povědomí způsobují závažné bezpečnostní incidenty.
- Účelem bezpečnostního monitoringu je především poznání bezpečnostního stavu (skutečných hrozeb a slabin).
- Součástí norem např. ČSN ISO/IEC 27001, ČSN ISO/IEC 17799/27002.

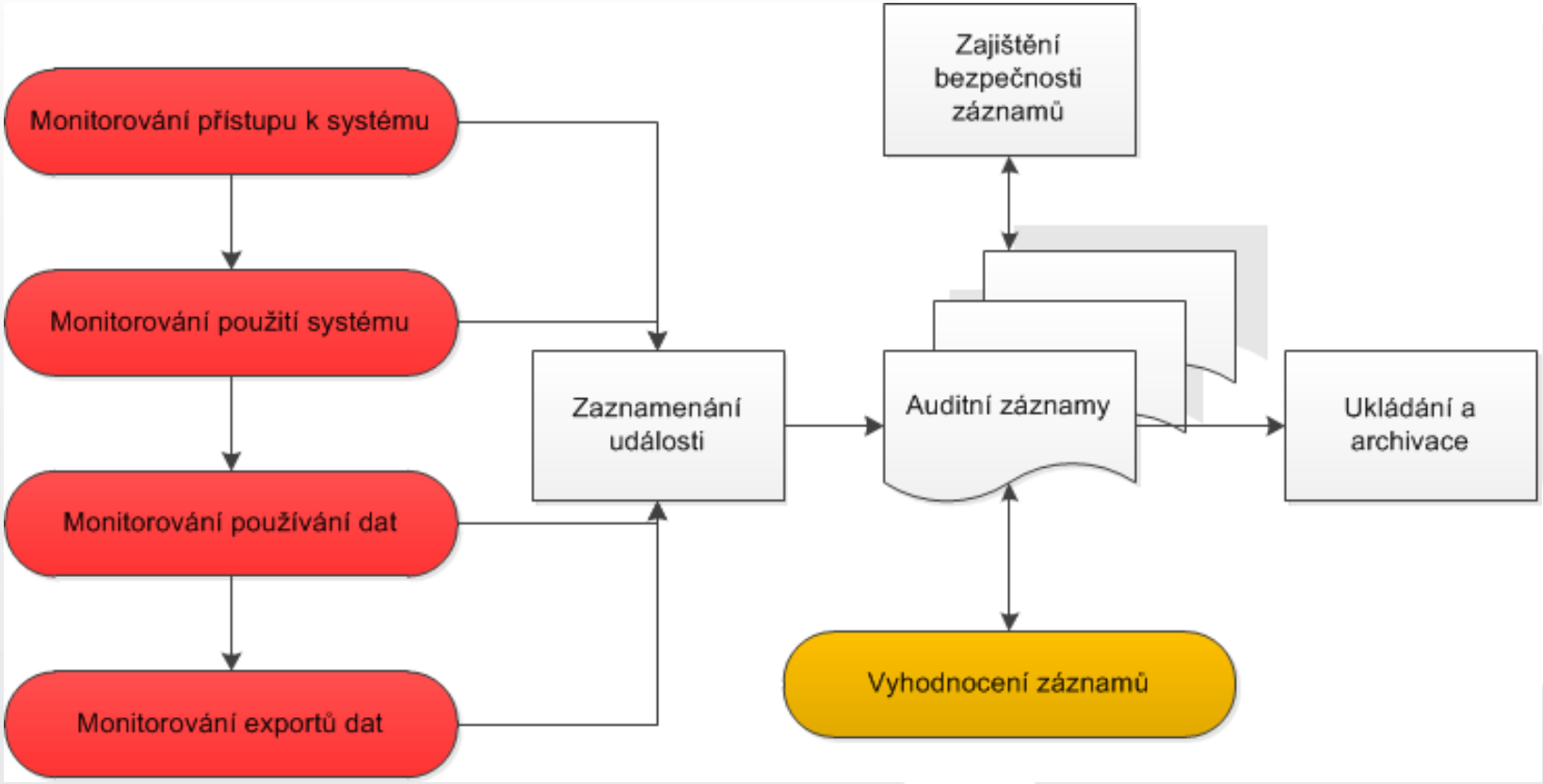
# Monitoring aktivit na koncové stanici

- Desktop/notebook u většiny pozic hlavní nástroj pro vykonávání pracovních povinností.
- Přímo nosič až 60% citlivých údajů organizace, ideální pro napadení sítě zevnitř.
- Uživatelé pracují s citlivými daty kritickými pro chod společnosti.
- Monitorování lze využít při úpravách bezpečnostní politiky, kontrole jejího dodržování a nastavení.
- Dokáže nejen zaznamenat, ale i upozornit na nebezpečné operace.

# Nežádoucí/nebezpečné aktivity

- Ne vždy lze přístup uživatele zcela zablokovat.
- Uživatelé zneužívají/využívají možností, které jim nemohly být odebrány.
- Incidenty jsou úmyslné i neúmyslné, vždy je jich ale mnoho a jsou vážné.
- Koncové zařízení zůstává jedním z největších rizik pro vnitrofiremní síť.
- Díky monitoringu máme záznamy/důkazy o bezpečnostních incidentech ze strany zaměstnanců.

# Model monitorování



# Reálný příklad č. 1

- Ministerstvo střední velikosti, podezření na úniky dat.
- Absence bezpečnostní politiky na periferie i internet.
- Důsledek: připojování obrovského počtu periferních zařízení na uživatele.
- Důsledek: kopírování obrovského množství dat – referátníky, smlouvy, zápisy, zprávy el. pošty.. Na periferie.
- Zároveň také absolutně běžná cesta souborů přes webové emailové klienty, 3 povolené webové prohlížeče, chaos…

# Reálný příklad č. 2

- Státní úřad s rozvětvenou strukturou, penetrační test údajně omezených periferií.
- Síťová politika restriktivní, údajně přísná politika i pro USB periferní zařízení – pouze výjimky pro některé uživatele.
- Důsledek: výjimka potvrzuje pravidlo, téměř všichni uživatelé mohou použít co chtějí.
- Důsledek: připojování nejen paměťových zařízení, ale i telefonů jako Access Point – tedy mimo politiku.
- Odhalen např. i flagrantní střet zájmů u jednoho z vedoucích lokální pobočky úřadu.

# Reálný příklad č. 3

- Bezpečnostní složka s oddělenými sítěmi.
- Citlivé či jinak klasifikované údaje nesmí opustit vnitřní síť, přenos po firemním USB.
- Důsledek: využívání i soukromých zařízení v obou sítích, odnášení velkého množství citlivých dat.
- Důsledek: absence odmazávání dat z USB (mají dostatečnou kapacitu) a vzhledem k absenci zabezpečení USB pak katastrofa při ztrátě zařízení.
- Odhalen např. i flagrantní únik klasifikovaných dokumentů, které nesmí nikdy opustit vnitřní síť.

# Reálný příklad č. 4

- Soukromá společnost čelící čínské výrobě plagiátů náhradních dílů.
- Absolutně nulová bezpečnostní politika, absence základních bezpečnostních principů vyjma fyzické bezpečnosti.
- Důsledek: přenášení kompletní projektové dokumentace na periferie techniků (co kdyby náhodou).
- Kopírování dokumentace na zařízení zákazníků v Rusku, ztráty dat obrovského rozsahu.

# Reálný příklad č. 5

- Městský úřad 3. kategorie o cca 150 zaměstnancích.
- Cílem zjištění využívání informačního systému a výpočetní techniky za účelem optimalizace.
- Zjištěno průměrné menší než 50% využití výpočetní techniky, ale pouze cca 35% účelně.
- Část uživatelů využívala techniku ke zcela nepracovním aktivitám typu soukromé emaily, brouzdání internetu, přehrávání videa či hraní her.
- Úřad mohl racionalizovat svůj běh, ušetřit na licencích i dříve požadovaném výkonném hardware.

# Obecná zjištění/závěry

- Zaměstnanci ignorují bezpečnostní principy a politiku (pokud existuje).
- Největším nebezpečím pro data jsou zařízení opouštějící perimetr – hlavně notebooky a USB zařízení.
- Monitorování poslouží nejen k odhalení incidentů, ale i jako psychologická prevence.
- Monitorování je třeba provádět buď systémově průběžně nebo alespoň testovat uživatele v dostatečných cyklech.

# Dotazy?

**Autor: Martin Ondráček, Product Director**
**SODATSW spol. s r. o., Horní 32, Brno, Czech Republic**

sodat sw

Efektivita a bezpečnost informací