

Monitorovanie aktivít zamestnancov na pracovných staniciach

*e*FOCUS

..nie je honom na čarodejnice, ale nástrojom

Jaroslav Oster, Info consult, s.r.o.

Pár myšlienok na úvod



*Môžeme rozsiahať diskutovať o
pojme počítačová kriminalita
viac bulvárny pojem než
odborne vyjasnená
problematika*

- objem počítačovej kriminality má narastajúcu tendenciu
- za rok 2014 – sa 48% podnikateľských subjektov stretlo s podvodom
- od roku 2011 je to nárast o 19%
- podiel interných/externých páchatel'ov je 49:51 (%)

Opatrenia

Firemné prostredie/kultúra

Organizačné
opatrenia

Technologické
opatrenia

Jasné pravidlá
(smernice)

Cyklické vzdelávanie
zážitkovou formou

Monitorovanie/audit
činností

EndPoint Security



Monitorovanie – primárna motivácia

- nepracovné aktivity zamestnancov
 - nepohodlný/problematický zamestnanec
 - nárast spotrebných nákladov
- prvý interný bezpečnostný incident
 - únik informácií
 - príspevok na sociálnej sieti
- doporučenie spracovateľa BP
- a ďalšie dôvody



Monitorovanie – oblasti monitoringu

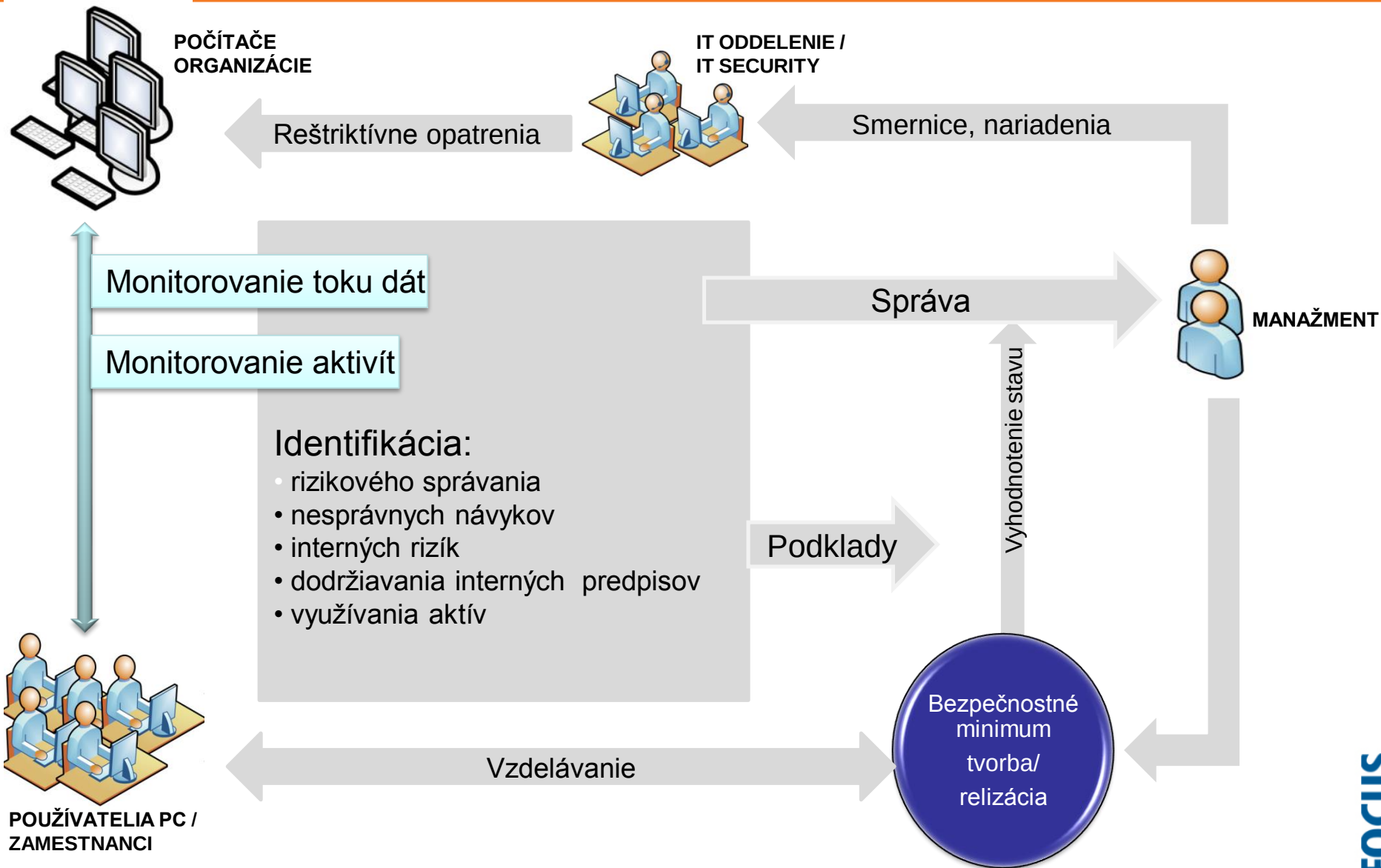
- prístupy k OS/aplikáciám
- modifikácie nastavení systému
- používanie dát
- export dát
- hraničné stavy udalostí
- neoprávnené aktivity
- komunikácia
- internetové aktivity



Monitorovanie – oblasti očakávaní

- prevencia
- merateľnosť efektivity využívania aktív
- spätná väzba
- bezpečnostné výstupy
- bezpečnostné reakcie (alerty)

Monitorovanie – očakávaný prínos



Preventívny dosah

už len informácia o zavedení = prínos

-30% 

- zníženie nepracovných aktivít
- zníženie aktivít vykazujúcich charakter nemorálnosti, protiprávnosti až kriminálneho správania
- dodržiavanie interných noriem
- zníženie rizika zneužívania aktív zamestnávateľa

Zákonník práce – informovanie je bez diskusie povinné



Meranie efektivity

- pracovné/nepracovné aktivity
 - sociálne médiá a iné formy „relaxácie“
 - aktívny používateľský čas
- využívanosť aktív – najmä aplikačné programové vybavenie

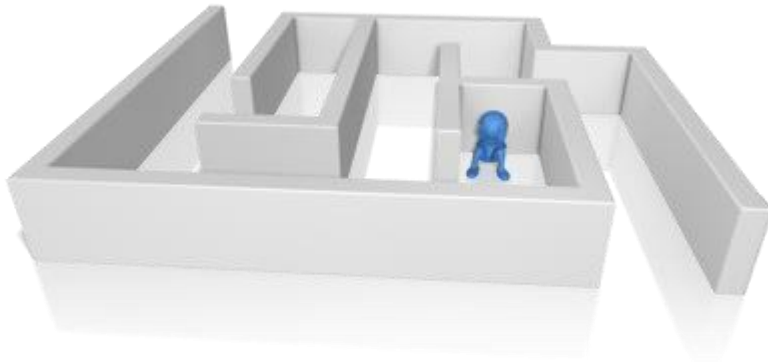


Spätná väzba a bezpečnosť

- prehľad o chovaní používateľov
- operatívna znalosť o prípadných kriminálnych aktivitách
- používanie výmenných médií
 - použitie USB kľúčov ako rizikového prvku
 - vynášanie dát mimo perimetra organizácie
- dátové toky na úrovni pracovnej stanice
- podklady pre rozhodovacie procesy
 - disciplinárne konania

Security education

STANDARD



- všeobecne známe princípy/poznatky
- cyklicky opakované, šablóna
- metóda: môžeš – nemôžeš
- fiktívne situácie

Základné črty:

- povinné školenie ako mnoho iných
- často „aby bolo“
- nepochopenie
- neakceptácia

CUSTOMIZED

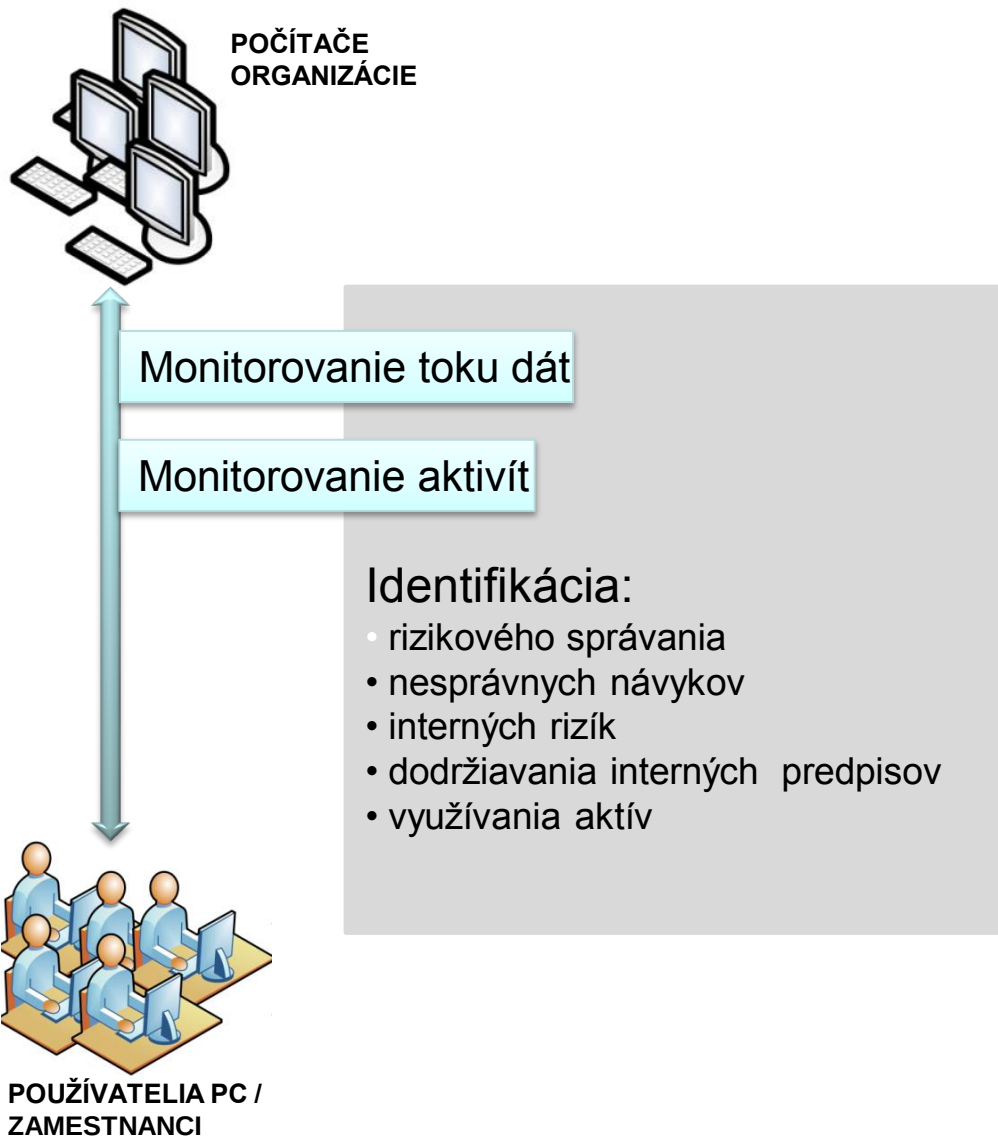
- všeobecne známe princípy/poznatky
- východisko z vlastného prostredia
- metóda: analyzujeme **naše** chyby



Základné črty:

- riešenie reálnych problémov
- nekreujeme „štábne cvičenie“
- pochopiteľnosť
- akceptácia

Security education



CUSTOMIZED

- všeobecne známe princípy/poznatky
- východisko z vlastného prostredia
- metóda: analyzujeme **naše** chyby

Podklady



Základné črty:

- riešenie reálnych problémov
- nekreujeme „štábne cvičenie“
- pochopiteľnosť
- akceptácia

Vždy rozvážne



SW/HW keylogger, keygrabber



15:20 – 15:40

Právny rámec monitorovania emailov zamestnanca
JUDr. Ing. Miroslav Chlipala, PhD., advokát a spoločník

Myšlienka na záver

Zadania majiteľov, štatutárov, manažérov
nie vždy korešpondujú s legislatívou

Nestaňte sa páchatelom trestnej činnosti preto,
aby ste preházali páchanie priestupku či
porušenia interných predpisov.

Ďakujeme za pozornost



**Systémy
ochrany
dát**

