

# EMM

CHRÁNIME VAŠE HODNOTY

## **AUDIT A BEZPEČNOSŤ V IT 2011**

**Optimalizovaný svet IT security**

### **Monitorovanie a ochrana súkromia zamestnancov**

Jozef Chebeň, CISA, CISM, CRISC

## 2/ Anotácia

-je bežným javom, že IKT vo vlastníctve firmy používa zamestnanec aj na súkromné účely

-je bežným javom, že firmy nasadia na ochranu bezpečnosti IKT monitorovacie a detekčné nástroje

-prezentácia z pohľadu zamestnávateľa popisuje riziká využívania firemných IKT na súkromné účely a riziká použitia monitorovacích a detekčných nástrojov

-prezentácia neanalyzuje právne aspekty použitia monitorovacích nástrojov

### Kde minú peniaze vaši zákazníci, keď vám zlyhá technika?

- jeden z Murphyho zákonov hovorí: "Všetko, čo neexistuje, funguje perfektne. A naopak." Ako je to u vás?
- zlyhanie komunikácie a spojenia nastáva práve v čase najintenzívnejšej prevádzky
- je to vždy, keď najviac potrebujete aby všetko fungovalo?
- koľko peňazí vás stoja 2 hodiny výpadku siete počas najväčšieho náporu zákazníkov?

**Vyhnete sa rizikám straty tržieb v predvianočnom období**

Ukážeme vám technológiu, pomocou ktorej rýchlo a jednoducho skontrolujete stav, funkčnosť a stabilitu siete vašej siete.

#### Chcete niečo viac?

Prevádzkové náklady na správu, údržbu IT a externé dodávky služieb až do 10-30%, investičné náklady na nákup a rozvoj IT až do 30% z ročného rozpočtu?

### Viete čo skutočne robia vaši zamestnanci v práci?

- štandardne zamestnanci venujú 20 až 40% svojho pracovného času zberu na internete
- viete aký softvér si zamestnanci nainštalovali na počítačoch vo firme bez vášho vedomia?
- najviac dát uniká z firmy vo chvíli, keď pracovník dostane výpoveď
- dodržiavajú vaši zamestnanci bezpečnostné smernice pri práci s citlivými dátami?

**Ušetriť na personálnych nákladoch môžete v priemere do 10 až 30%**

Chcete vedieť ako je na tom vaša firma?

**Príďte sa s nami naraňajkovať, radi vám povieme viac ...**

### 4 z 10 firiem minulý rok skrachovali kvôli úniku dát

- strihne vaša konkurencia na to, kedy vám nejaké dáta uniknú?
- koľko stojí vaše know-how?
- každá sieť je taká silná ako jej najslabší článok
- viete že zodpovednosť za používanie nelegálneho softvéru nesie vedenie?
- viete aký softvér je nainštalovaný na vašich PC? Myslíme aj ten čo uložia a nainštalujú vaši zamestnanci v rámci zábevy.

**Len vy viete, akú hodnotu majú vaše interné dáta**

**Chráňte sa pred krádežou a zneužitím výsledkov vašej práce !**

## 4/ Čo sa monitoruje bežne

- dochádzka zamestnancov  
(staré cvikačky, zošity, RFID, biometria, ...)
- pohyb zamestnancov v budove  
(prístupové systémy, PTV, ...)
- používanie služobných motorových vozidiel  
(čierna jazda vs. použitie PC...)
- korešpondencia  
(evidencia korešpondencie, pravidlá otváranie pošty – aj súkromnej...)

## 5/ Rizikové oblasti

- **únik údajov z vnútorného prostredia**  
(ponuky, zmluvy, interné predpisy, dokumentácia systémov, ...)
- **intrúzia údajov do vnútorného prostredia**  
(sw, fotografie, filmy, dokumenty, ...)
- **používanie zariadení na súkromné účely**  
(vybavovanie korešpondencie, komunikácia s rodinou, práca pre tretie strany, ...)
- **nelegálne aktivity (porušovanie zákona)**  
(porušenie autorských práv, porušenie etických noriem, trestná činnosť, ...)
- **zneužitie súkromných údajov**  
(súkromná korešpondencia, heslá, ...)

## 6/ **Limity**

- vnímanie vzťahu zamestnanec a zamestnávateľ

(zlý zamestnávateľ vs. dobrý zamestnanec, využívanie pracovného času, fajčiarske prestávky vs. vybavovanie si súkromných vecí – telefón, PC, ...)

- zákony chrániace zamestnanca a obmedzujúce práva zamestnávateľa

(ochrana osobných údajov, telekomunikačný zákon, využívanie pracovného času, fajčiarske prestávky vs. vybavovanie si súkromných vecí – telefón, PC, ...)

- všeobecná tolerancia kriminality a „jánošíkovej“ tradície

## 7/ **Prečo monitorovať, prečo sa chrániť**

- priame ekonomické straty
- strata konkurencieschopnosti
- poškodenie zdravia zamestnancov
- vyšetrovanie, trestné stíhanie
- poškodenie dobrého mena firmy

EMM

## 8/ Používané technológie

- IDS/IPS
- firewall
- content inspection
- access control (riadenie prístupu)
- DLP
- anomaly detection
- ...

EMM

## 9/ **Kontrolované technológie**

- elektronická pošta
- skype
- sociálne siete
- wifi, bluetooth
- prenosné nosiče údajov
- fotoaparáty a kamery
- mobilné zariadenia
- tlačiarne

**služobné aj súkromné**

EMM

## 10/ Opatrenia I

- definovať skutočné potreby komunikácie
- špecifikovať prístupové práva
- spravovať všetky zariadenia pripojené do IKT bez ohľadu na vlastníctvo
- striktná separácia firemných a súkromných údajov
- presadiť silné kontrolné mechanizmy vo všetkých zariadeniach

EMM

## 11/ Opatrenia II

- určiť pravidiel úhrady nákladov
- vynútiť zálohovanie údajov
- získať súhlas zamestnancov s aplikovaním bezpečnostných opatrení
- popísať dôsledky nedodržiavania opatrení

EMM

## 12/ Záver

- používanie firemných IKT na súkromné účely je rizikom pre zamestnanca aj zamestnávateľa
- zamestnávateľ by nemal akceptovať využívanie IKT na súkromné účely
- zamestnávateľ by mal zaviesť opatrenie na zisťovanie porušení
- zamestnávateľ by mal získať súhlas zamestnanca s aplikovaním monitorovacích nástrojov