

# Informacinės technologijos – grėsmė verslui

Audrius Lučiūnas

**UAB „Informacijos saugos sprendimai“**

[www.isec.lt](http://www.isec.lt)

2007 metų kovas



## Turinys

1. Kur dingsta duomenys?.....	3
2. Situacija Lietuvoje .....	4
3. Apie mus .....	5

## 1. Kur dingsta duomenys?

Kalbėkim atvirai: informacinės technologijos Jums nepadės laimėti konkurencinės kovos. Bet, nenaudodami jų, Jūs, be jokios abejonės, tą kovą pralaimėsit. Taip, informacinės technologijos tapo neatsiejama bet kokio verslo svarbia dalimi: jos padeda suvaldyti milžiniškus duomenų srautus, sudėlioti viską į vietas ir greitai surasti, ką kur padėjot. Šiandien žmogus per dieną gauna daugiau informacijos, nei viduramžiais valstietis gaudavo per visą savo gyvenimą. Taigi duomenys vaidina svarbų vaidmenį mūsų šiandienos gyvenime, o informacinės technologijos vaidina svarbų vaidmenį tuos duomenis valdant Jūsų verslo procesuose. Visiems, rodos, viskas aišku: investuok į informacines technologijas, naujas programas, techninę įrangą, darbuotojų mokymus kaip visu tuo naudotis, kurk, saugok, tinkamai apdorok terabaitus savo, konkurentų ir klientų duomenų ir Jūsų verslą galbūt aplankys palaima. O galbūt ir ne! Jei į visa tai pažvelgsite ne tik kaip į galimybę lengvai ir tinkamai valdyti informaciją, bet ir kaip į galimybę ją lengvai prarasti. Tos pačios informacinės technologijos leidžia greitai ir paprastai Jūsų informaciją sunaikinti ar tiesiog pasisavinti.

Tyrimų kompanijos Gartner Group, IDC, DTI, Source ir Meta Group pateikia tokius faktus, kaip pradingsta duomenys:

- nuo 40% iki 80% svarbių duomenų saugomi darbo kompiuteriuose;
- 6% stacionarių darbo kompiuterių per metus netenka duomenų;
- 32% duomenų prarandami dėl vartotojų kaltės;
- 10% nešiojamų kompiuterių kasmet yra pavagiama;
- 15% nešiojamų kompiuterių kasmet sugenda arba yra sugadinami;
- 3% duomenų netenkama dėl stichinių nelaimių;
- 7% duomenų netenkama dėl virusų ar panašių kenkėjiškų programų;
- 14% duomenų prarandama dėl netinkamai veikiančios programinės įrangos;

ir t.t.

Tai tik keletas skaičių iš įvairių kompanijų tyrimų, kur visai arba beveik visai nepaminiti įsilaužėliai ir nesąžiningų darbuotojų veiksmai, vaidinantys nemažą vaidmenį, stabdant Jūsų įmonės veiklą. Netinkamai prižiūrimos sistemos, įsilaužimai į Jūsų įmonės tinklą, darbuotojų kerštas – visa tai dar keli, tačiau toli gražu ne visi būdai prarasti duomenis.

Dar įdomesni skaičiai pasekmių, kurių sulaukia kompanijos, praradusios informaciją ar sutrikus jų verslo procesams:

- 70% įmonių pasitraukia iš verslo po didesnio duomenų praradimo;
- 80% įmonių bankrutuoja per dvejus metus, jei per 24 valandas nesugeba atstatyti savo verslo procesų.

Ar Jūsų įmonė daro bent jau svarbiausių duomenų kopijas? Ar nors kartą bandė, kaip tuos duomenis iš tų kopijų pavyksta atstatyti? Deja, bet pavyksta ne visuomet. Duomenų praradimas nebūtinai reiškia jų sunaikinimą. Iš svarbios informacijos gali nebelikti jokios naudos, jei ji staiga tapo vieša arba atiteko konkurentams. Atlyginimu nepatenkintam darbuotojui į USB įrenginį nukopijuoti kelis gigabitus informacijos nėra sudėtinga, kaip ir nesudėtinga tą USB įrenginį pamesti ar kažkam perduoti. Tokiu atveju Jūs galite nesunkiai tapti 70% grupės nariu.

Jei sutriko Jūsų įmonės verslo procesai, o Jūs juos sugebėjote atstatyti per dvi dienas, vieną tokį sutrikimą galbūt sugebėsite paaiškinti ir klientus išsaugosite. Jei nekreipsite dėmesio į kilusių sutrikimų šaltinius, jie būtinai pasikartos. Pasikartojus turbūt įgausite nepatikimos kompanijos įvaizdį, ir Jūsų klientai Jus paliks. Jei nesutvarkysite ir nenumatysite bent didžiosios dalies galimų verslo procesų sutrikimų priežasčių, turbūt ir Jūs per dvejus metus būsite priimti į 80% grupę.

## 2. Situacija Lietuvoje

Lietuvoje vyrauja nuomonė, kad apsaugoti įmonės informacinių technologijų sistemas nuo kompiuterinių įsilaužėlių (hakerių) pakanka įdiegti ugniasienę (angl. firewall) ir antivirusines sistemas. Namuose naudojamam kompiuteriui tai galbūt ir tinkamas minimalus saugumo sprendimas, bet tikrai ne įmonei. Pvz., nei ugniasienė, nei antivirusinė sistema neapsaugos tinklalapio, jei jame programuotojai paliko klaidų. Gan įprasta situacija, kai naudojama įranga būna netinkamai įdiegta, o visa informacinių technologijų sistemų ir tinklo architektūra yra pasmerkta grėsmei. Jei Jūs informacinių technologijų ūkį prižiūrinčio žmogaus ar įmonės paklaustumėte, ar jie savo darbą atlieka gerai, ar veikiančios sistemos yra saugios, ar tinkamai viskuo rūpinamasi, žinoma, kad sulauksit atsakymo „Taip“. Bet sakykit, ar Jūs prisipažintumėte esąs prastas meilužis?

Jūsų įmonėje dirbantys žmonės gali kelti ne ką mažesnę pavojų nei netinkamai naudojama techninė įranga. Jie gali tapti įsilaužėlio bendrininkais net patys to neįtardami. Asmeninis patekimo į įmonės vidinį tinklą rekordas yra 3 minutės. Būtent tiek laiko prireikė audito metu, kad įmonės darbuotojas, pats to nesuvokdamas, mane „išileistų“ į įmonės vidinį tinklą ir taptų mano „bendrininku“. Šiuo atveju visa techninė įranga buvo bejėgė, nors ir tinkamai prižiūrima. Esant realiam įsilaužimui, tokį darbuotoju pasinaudojusį įsilaužėlį susekti būtų praktiškai neįmanoma, o visi įkalčiai būtų nukreipti į darbuotoją. Norint išvengti tokių nesusipratimų, reikėtų ne tik diegti tinkamą techninę įrangą, bet ir šviesti darbuotojus, pvz., mokant juos atpažinti klastingas el. pašto žinutes, telefoninius skambučius, suklastotus tinklalapius ir t.t.

Jei vakarų šalyse, kur informacijos apsauga susirūpinta gerokai anksčiau nei pas mus, yra įprasta numatyti galimus verslo procesų sutrikimus, įvyksiančius sutrikus informacinių technologijų sistemoms, ir atitinkamai tam pasiruošti, sukuriant verslo tęstinumo procedūras, Lietuvoje į tai dėmesį kreipia tik

maža dalis įmonių. Dėl to Lietuvoje yra normalu gesinti kilusius „gaisrus“ ar, pvz., dėl sugedusio kompiuterio disko dalies funkcijų nevykdyti dvi savaites, po to dar du mėnesius vyti prarastą laiką, kol įmonė pilnai pasiekia savo įprastos veiklos tempą. Viso to pasekmė - įmonės veikla nepatenkinti klientai, dėl viršvalandžių pikti darbuotojai, dėmesys ne įmonės plėtrai, bet jos veiklos atstatinėjimui, rinkoje suprastėjusi įmonės reputacija ir dėl to kritusi akcijų vertė ir t.t. Sąrašą galite pratęsti patys.

Prastą situaciją Lietuvoje patvirtina ir pasaulinės antivirusinių sprendimų kūrimo bendrovės "F-Secure" atstovai, sausio 14-17 dienomis Helsinkyje vykusioje Tarptautinės parlamentarų informacinių technologijų asociacijos penktojoje Generalinėje asamblėjoje pareiškę, jog vieni iš daugiausia Europos elektroninėje erdvėje padarančių nusikaltimų yra Lietuvos gyventojai. O tai reiškia, kad mūsų šalyje arba labai daug kompiuterinių nusikaltėlių, arba esančias informacinių technologijų sistemas yra nesudėtinga panaudoti kaip tarpininkes, slepiant tikrąjį nusikaltimo vykdytoją.

Todėl kiekvieną dieną, naudodami informacines technologijas namie ar versle, būtinai atkreipkite dėmesį ne tik į tai, kokią naudą jos suteikia, bet ir kokius pavojus gali sukelti. Juk peiliu galima ir duoną raikyti, ir žudyti. Tad būkit atsargūs ir neleiskit, kad informacinės technologijos „nužudytų“ Jūsų verslą.

### 3. Apie mus

UAB "Informacijos saugos sprendimai" - 2006 metais įkurta kompanija, kurios pagrindinė veikla yra konsultacijos, mokymai ir auditas, susiję su informacijos apsauga. Kompanija yra nepriklausoma ir neatstovauja nei vienam programinės ar techninės įrangos gamintojui, todėl visuomet išlieka nešališka. Įmonėje dirba didelę patirtį turintys specialistai. Tai daug metų informacijos saugumu ir informacinėmis technologijomis besidomintys žmonės, konsultavę bei ruošę saugos politikas ir atlikę informacijos apsaugos auditus didžiosiose Lietuvos įmonėse. Kompanijos darbuotojai ne tik gerai išmano šiandien aktuales informacijos apsaugos standartus, hakerių metodus, bet turi patirties ruošiant su informacijos apsauga ir informacinių technologijų nusikaltimais susijusius įstatymus, kuriant incidentų valdymo tarnybą.

Kompanija laikosi savo etikos politikos - suteikti klientui tik aukščiausio lygio paslaugas.

Įmonė laikosi konfidencialumo principų net jei raštiškai nėra išipareigojusi to daryti.

Kompanijai svarbu sukurti vertę, todėl ji savo darbą vertina pagal klientui suteiktą naudą.

Daugiau informacijos apie įmonę bei jos teikiamas paslaugas galima rasti internete adresu <http://www.isec.lt>, el. paštu [info@isec.lt](mailto:info@isec.lt) arba telefonu +370 615 20288.