DCIT

Ľudský faktor – najslabší článok bezpečnosti (internetové služby)

Autor: Martin Zajíček
(zajicek@dcit-consulting.sk)

DCIT Consulting, http://www.dcit-consulting.sk

CONSULTING
D C I T

Obsah prednášky

DCIT

1. Vnímanie problematiky prostredníctvom výsledkov prieskumov

2. Skutočnosť

3. Prejavy

4. Možnosti minimalizácie dopadov

CONSULTING DCIT

1. Vnímanie problematiky 1

DCIT

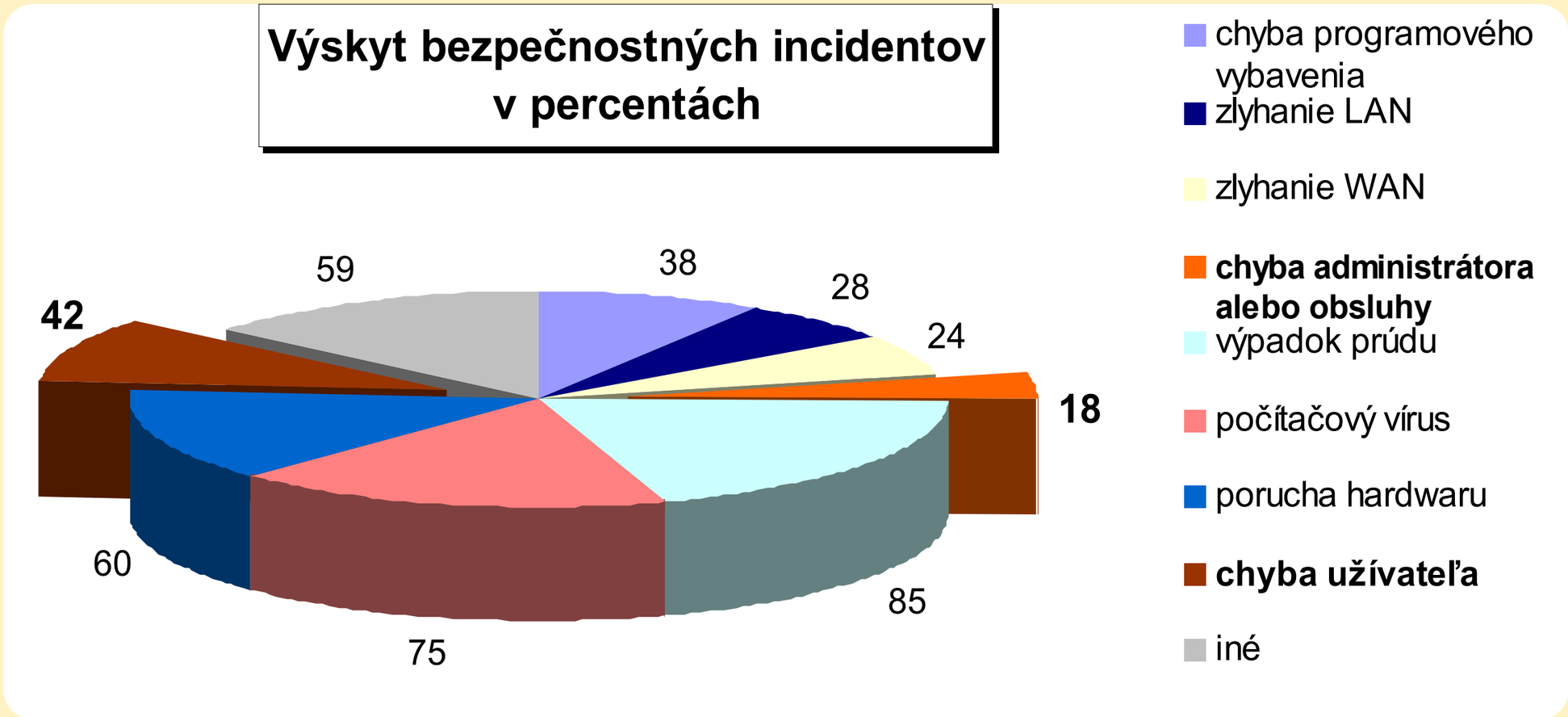
Zdroje:

- **PSIB SR ´04**, KPMG Slovensko, DSM-data security management, NBÚ -
  - historicky prvý prieskum v SR

- **PSIB ČR ´05**, Ernst & Young, DSM-data security management, NBÚ -
  - historicky už 4. prieskum opakujúci sa každé dva roky (prvý bol zrealizovaný v roku 1999)

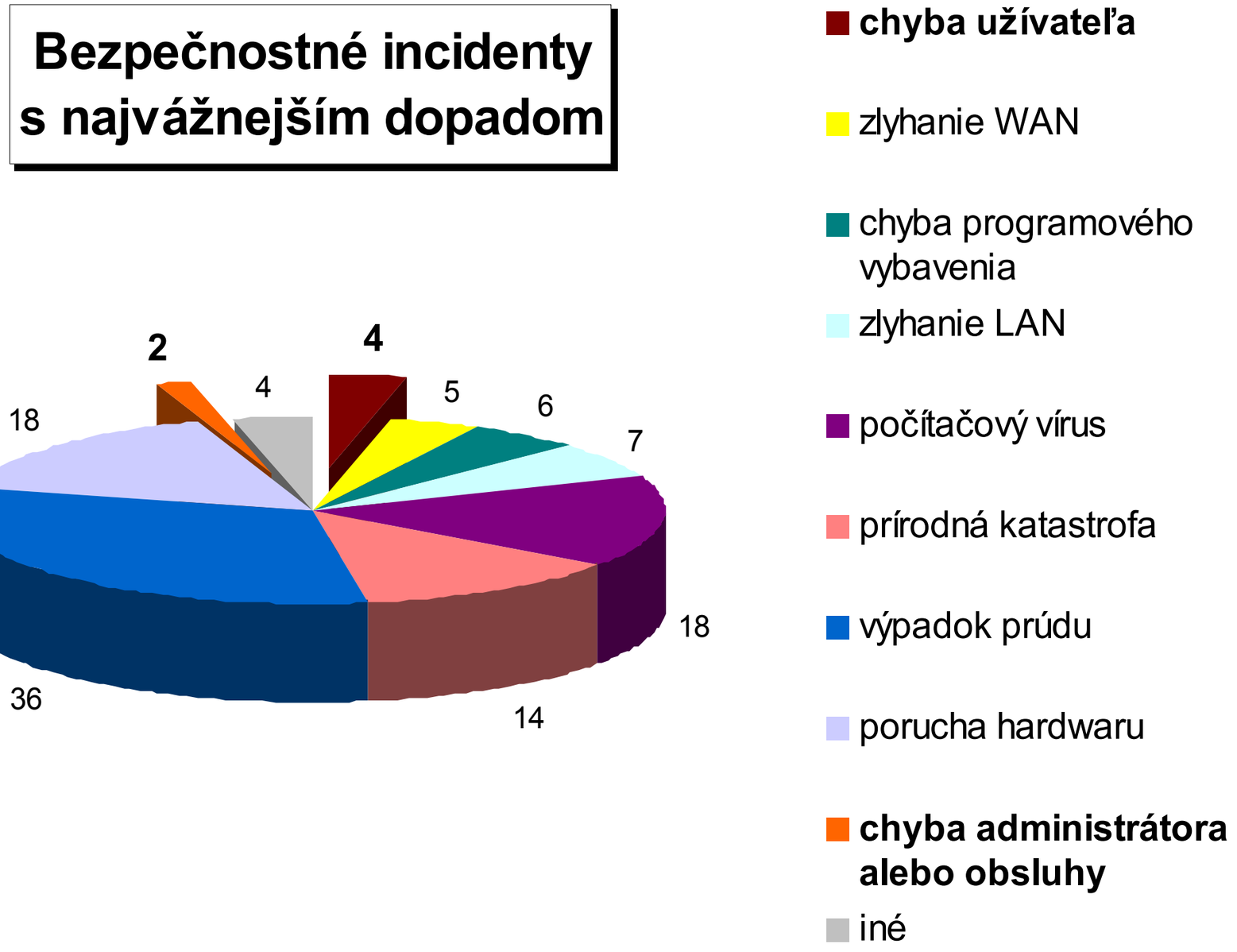
CONSULTING DCIT

1. Vnímanie problematiky 2



Zdroj: PSIB SR '04

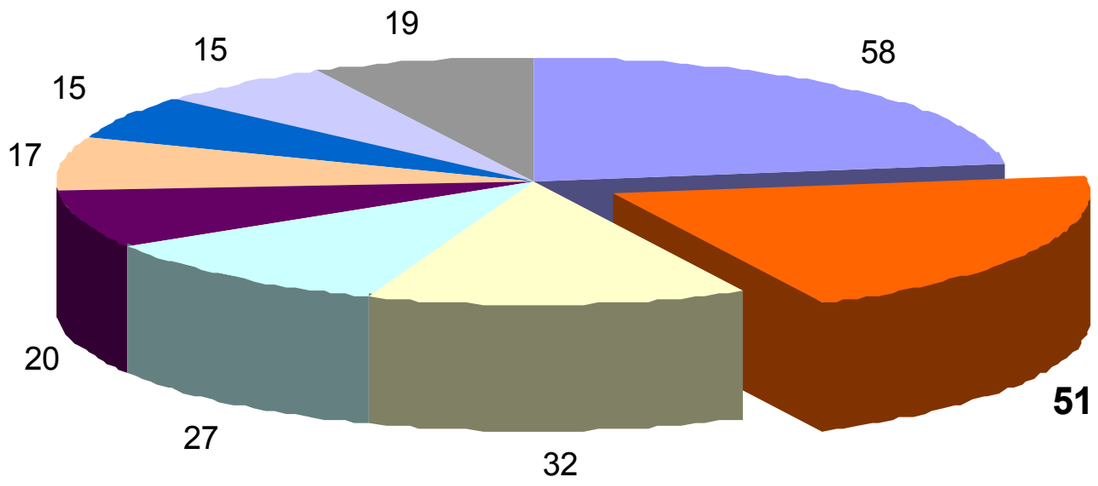
1. Vnímanie problematiky



Zdroj: PSIB SR '04

1. Vnímanie problematiky

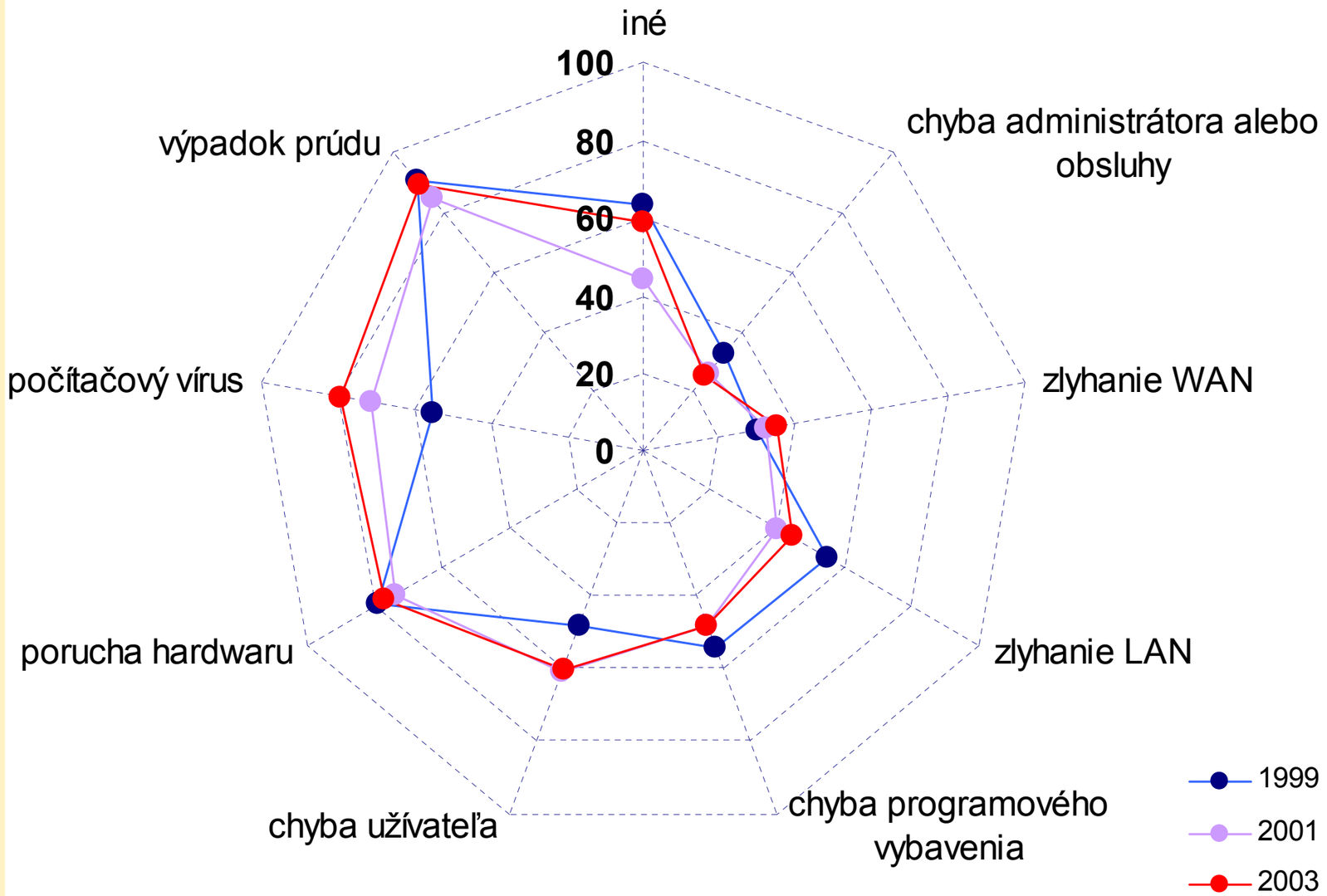
Najväčšie hrozby z hľadiska informačnej bezpečnosti



Zdroj: PSIB SR '04

DCIT

Výskyt bezpečnostných incidentov za posledných šesť rokov

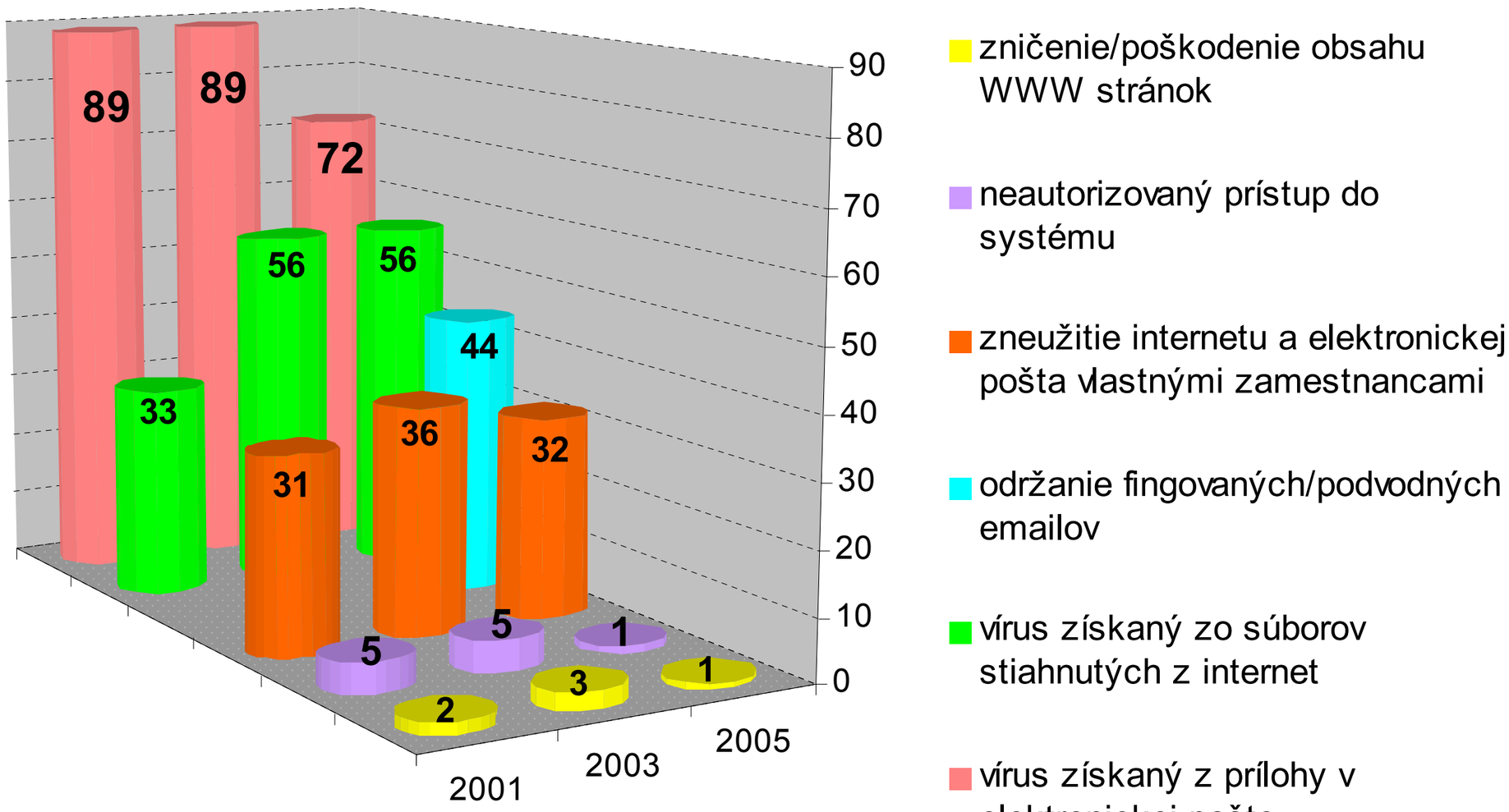


Zdroj: PSIB ČR '05

CONSULTING DCIT

1. Vnímanie problematiky

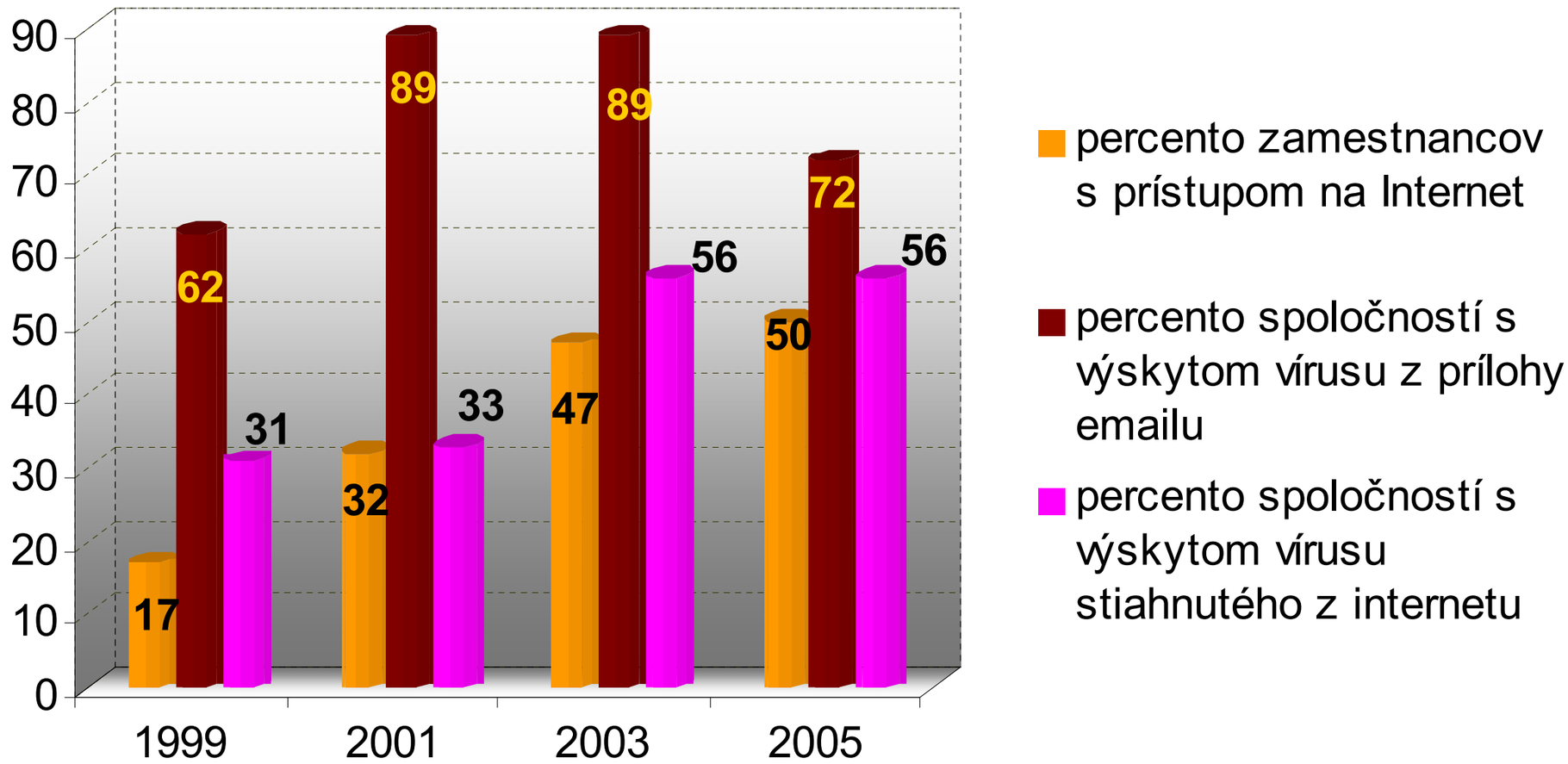
Výskyt bezpečnostných incidentov v súvisloti s využívaním internetu



Zdroj: PSIB ČR '05

DCIT

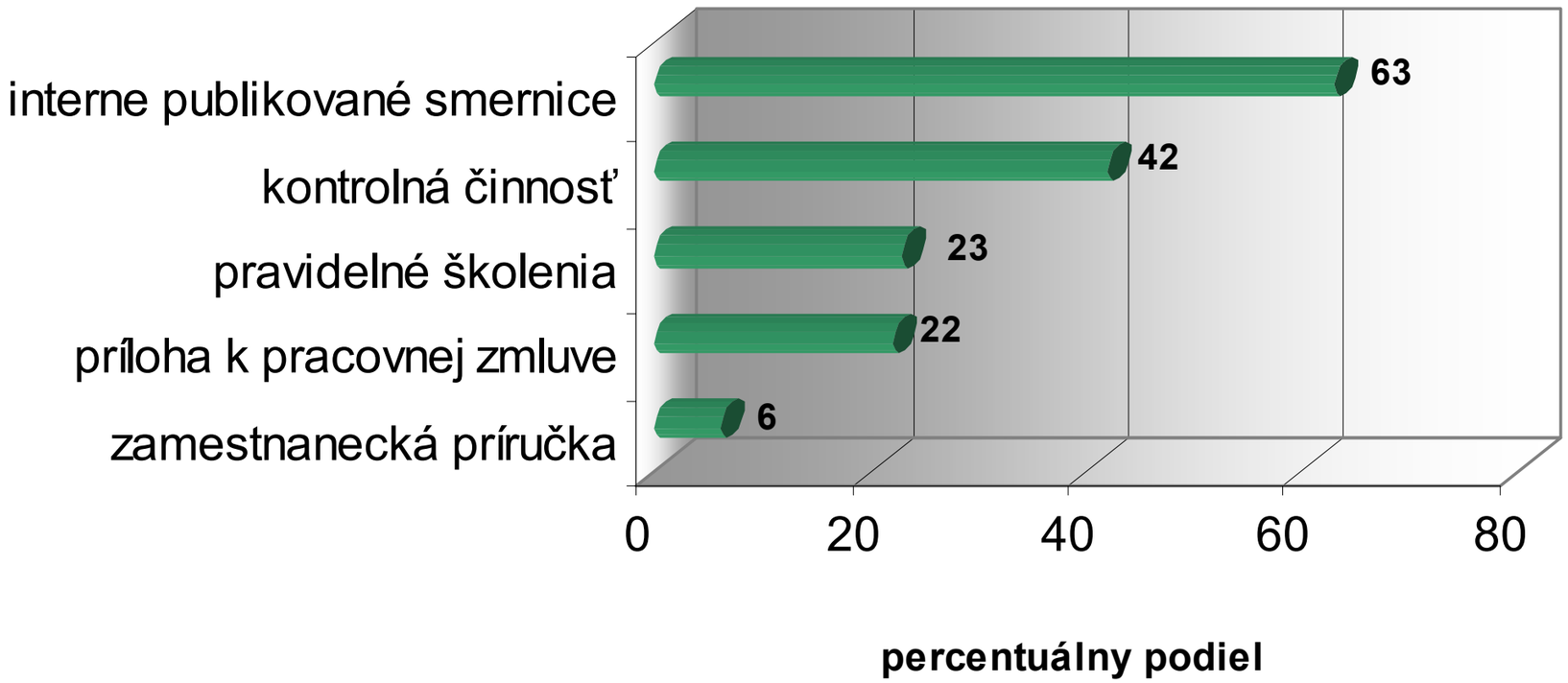
Percento zamestnancov s prístupom na internet a rast počtu vírusov stiahnutých z internetu



Zdroj: PSIB ČR '05

CONSULTING DCIT

Formy, ako prispievajú organizácie ku zvyšovaniu bezpečnostného vedomia svojich zamestnancov



Zdroj: PSIB SR '04

2. Skutočnosť 1

DCIT

Kde sa môže problém s ľudským faktorom objaviť

- Dodávatelia IS
- Vlastní užívatelia (správcovia IT, užívatelia)
- Externí užívatelia (klienti)

CONSULTING DCIT

2. Skutočnosť 2

DCIT

Dodávatelia IS

- tvorba WWW aplikácií, ktoré trpia známymi slabinami - SQL Injection, Cross site scripting (XSS), URL tampering, Cross site tracing (XST), Session hijacking, atď.
- nevhodná implementácia riešenia (default nastavenia služieb WWW, SQL servera a ďalších)

CONSULTING DCIT

2. Skutočnosť 3

DCIT

Vlastní užívatelia (správcovia IT, užívatelia), externí užívatelia (klienti)

- správa IT – dôsledky neznalosti problematiky a/alebo pohodlnosti
  - využívanie administrátorských práv pri bežnej práci
  - absencia auditovania a jeho kontroly
  - absencia reálneho riadenia užívateľských práv
  - absencia viacvrstvovej ochrany (víry, spyware a ďalší malware)
- užívatelia
  - žiadna alebo slabá znalosť hrozieb = naivita

CONSULTING DCIT

Príklad - phishing

DCIT

NCUA Home | Search | Privacy Policy & Accessibility | Site Map | Contact Us

National Credit Union Administration

Share Insurance | Resources for Credit Unions | Resources for Consumers | News | Search

Account Info Verification

Dear FCU holder account,

As part of our security measures, we regularly screen activity in Federal Credit Unions (FCU) network.
We recently noticed the following issue on your account: A recent review of your account determined that we require some additional information from you in order to provide you with secure service. Case ID Number: PP-065-617-349 For your protection, we have limited access to your account until additional security measures can be completed. We apologize for any inconvenience this may cause. Please log in to your FCU account to restore your access as soon as possible.

You must click the link below and fill in the form on the following page to complete the verification process.

Click here to update your account

In accordance with NCUA User Agreement, your account access will remain limited until the issue has been resolved. Unfortunately, if access to your account remains limited for an extended period of time, it may result in further limitations or eventual account closure. We encourage you to log in to your FCU account as soon as possible to help avoid this. We thank you for your prompt

About NCUA

The National Credit Union Administration (NCUA) is the independent federal agency that charters and supervises federal credit unions. NCUA, backed of the full faith and credit of the U.S. government, operates the National Credit Union Share Insurance Fund (NCUSIF) insuring the savings of 80 million account holders in all federal credit unions and many state-chartered credit unions. During the 1990s and into the 21st century, credit unions have been healthy and growing. Credit union failures remain low and the Share Insurance Fund maintains a healthy equity level. The National Credit Union Administration (NCUA) is comitted to maintain a safe environment for over 80 million account holders in all federal credit unions and many state-chartered credit unions. Protecting the security of holders account and of the Federal Credit Unions (FCU) network is our primary concern.

CONSULTING DCIT

Príklad - phishing

Príklad - phising

citibank

Serial EM202-16

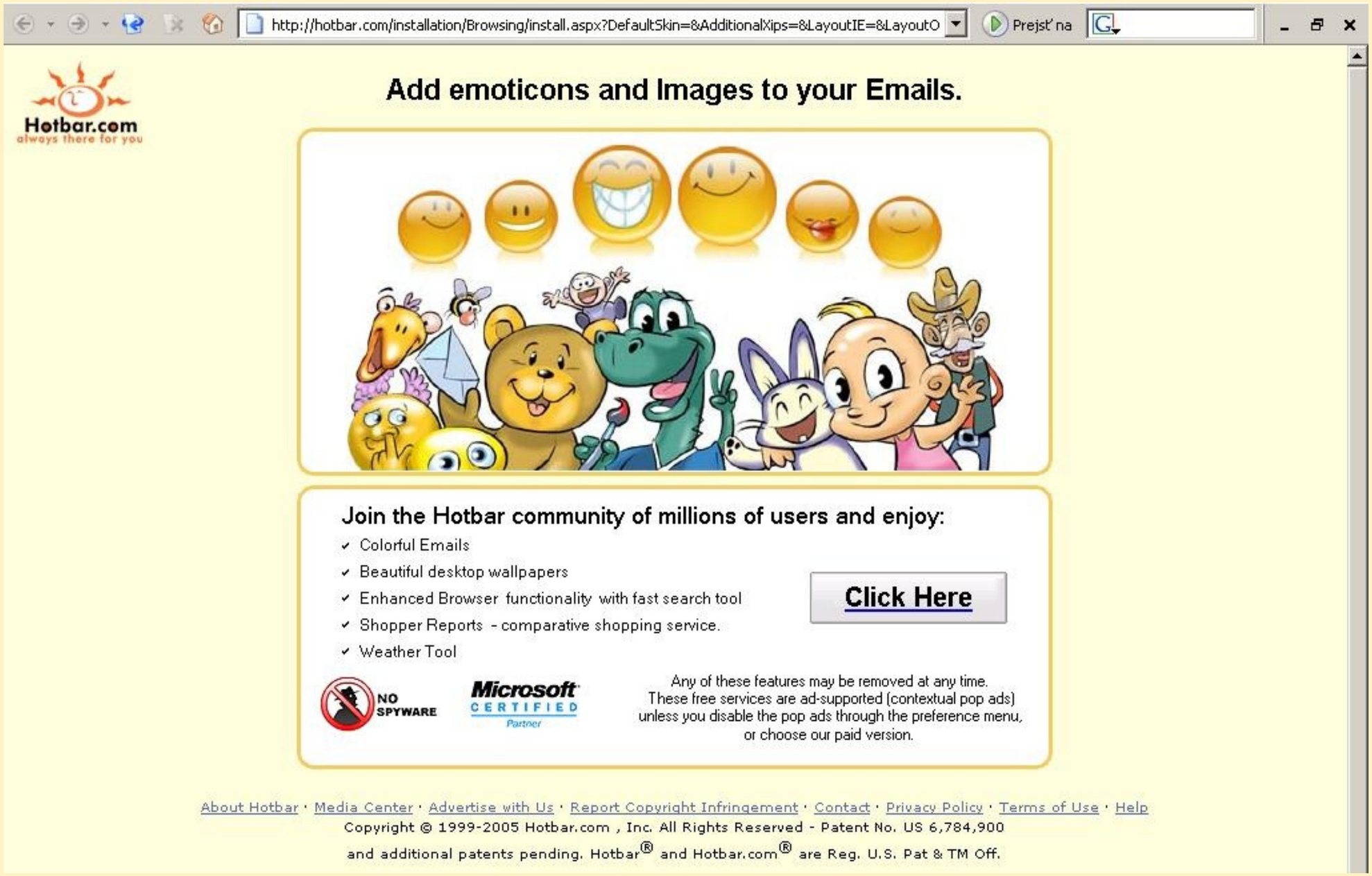
Vážený kliente Citibank Online®,

03/02/2006 na Váš běžný účet byl přijat převod v cizí měně na částku ve výši 2000 . Se shodou s *spotřebitelským souhlasem CitiBank® online* , je potřeba potvrdit tento převod pro jeho úspěšné zařazení na Váš běžný účet. **Pro potvrzení platby** Vás prosím o návštěvu programu ovládání Vaším účtem CitiBank® online a dále postupujte podle předloženého návodu. V případě nepřijetí potvrzení v průběhu 48 hodin, bude částka vracena odesílateli.

Pro vstup do programu CitiBank® online, **klikněte sem** >>>

S pozdravem
Služba CitiBank® Alerting Service

Príklad


http://hotbar.com/installation/Browsing/install.aspx?DefaultSkin=&AdditionalXips=&LayoutIE=&LayoutO
Prejsť na
Hotbar.com
always there for you
Add emoticons and Images to your Emails.
Join the Hotbar community of millions of users and enjoy:
Colorful Emails
Beautiful desktop wallpapers
Enhanced Browser functionality with fast search tool
Shopper Reports - comparative shopping service.
Weather Tool
Click Here
NO SPYWARE
Microsoft CERTIFIED Partner
Any of these features may be removed at any time.
These free services are ad-supported (contextual pop ads)
unless you disable the pop ads through the preference menu,
or choose our paid version.
About Hotbar · Media Center · Advertise with Us · Report Copyright Infringement · Contact · Privacy Policy · Terms of Use · Help
Copyright © 1999-2005 Hotbar.com , Inc. All Rights Reserved - Patent No. US 6,784,900
and additional patents pending. Hotbar® and Hotbar.com® are Reg. U.S. Pat & TM Off.

Možné dopady?

- únik dát
- zneužitie, zneprístupnenie infraštruktúry (SPAM, „zombie“, trójske kone, červy)
- v prípade zmanipulovaných transakcií reklamačné konania
- a ďalšie

Možnosti minimalizácie-všeobec.

DCIT

Mať systém riadenia bezpečnosti inform.

- zmapovať inf. aktíva, definovať vlastníka dát, vytvoriť kategórie, postupy a zodpovednosti

Zvyšovať bezpečnostné povedomie interných i externých užívateľov

Na technickej úrovni

- GPO, prípadne lokálna aplikácia opatrení
- viacvrstvové ochrany (AV)
- úprava konfigurácie, alternovanie WWW klientov
- ovládanie užívateľských práv
- monitorovanie a spracovávanie logov !!!

CONSULTING DCIT

Možnosti minimalizácie - konkr.1

DCIT

Dodávatelia IS

- súčasťou implementačného projektu IS má byť nezávislé preverenie treťou stranou – audit/preverenie aplikácie, penetračný test

Vlastní užívatelia

- monitorovanie a pravidelné spracovávanie logov !!!
- automatizovaná pravidelná aktualizácia OS i aplikácií
- minimalizovať rozsah užívateľských práv (používanie skupín Users, Power Users, využitie GP)

CONSULTING DCIT

Možnosti minimalizácie - konkr.2

DCIT

Vlastní užívatelia - pokračovanie

- konfigurácia WWW a email klientov (obmedzenie povolených príloh, ďalšie parametre použitím Resource kitu k MS Office balíku, obmedzenie ActivX komponentov) i na centrálnej úrovni (emailový server, proxy server)
- zvážiť používanie alternatívnych WWW a email klientov
- pretestovať pozornosť užívateľov
- pri užívateľoch s mobilnými zariadenia zvážiť použitie osobných firewallov
- venovať sa problematike spyware

CONSULTING DCIT

Možnosti minimalizácie - konkr.3

DCIT

Vlastní užívatelia - pokračovanie

- venovať sa aj svojim klientom (oboznámenie s hrozbami, priebežné informovanie o nových hrozbách, poskytnúť konkrétne doporučenia)

CONSULTING
D C I T

Možnosti minimalizácie - konkr.4

DCIT

Group policy (GP) - podrobnejšie

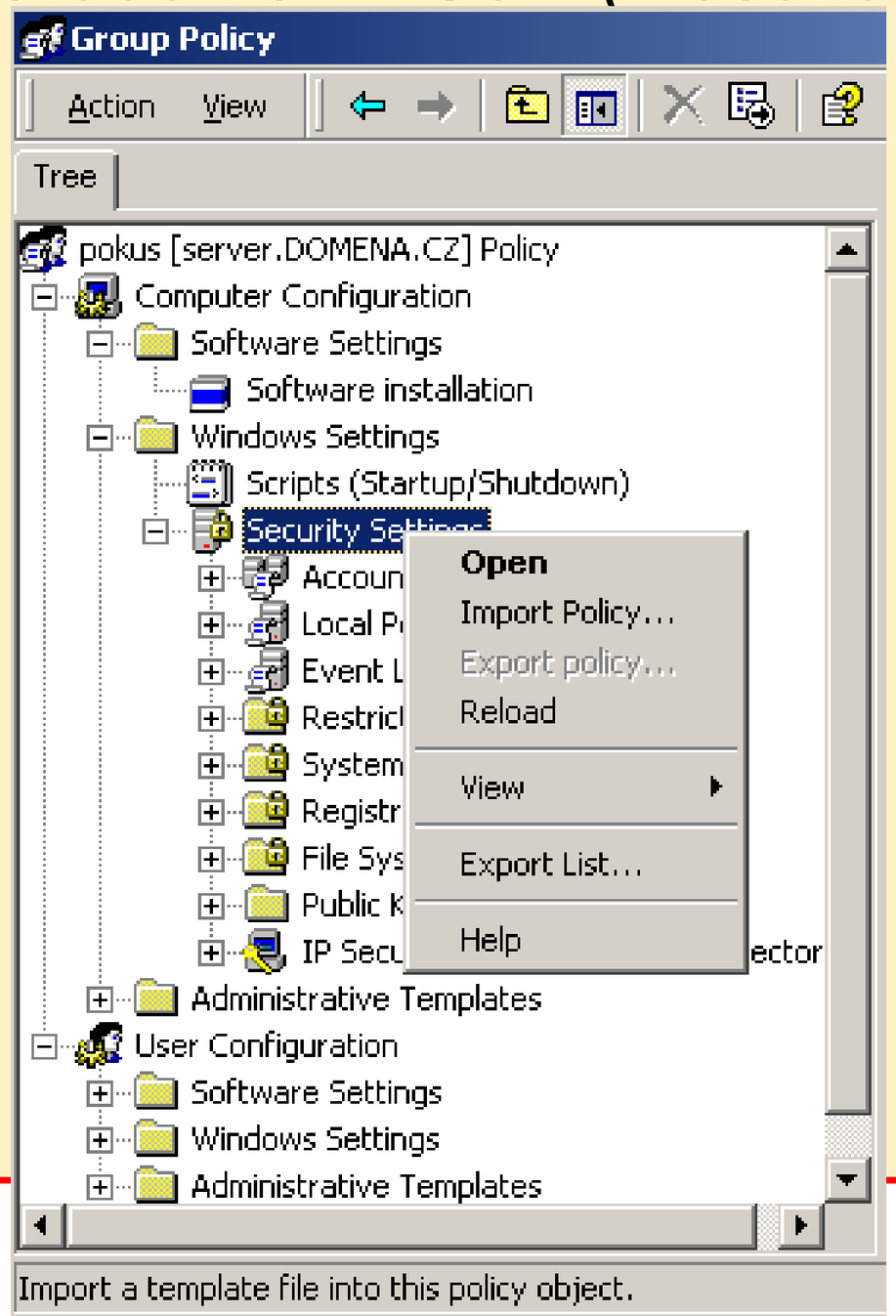
- GP (skupinové politiky) – definujú užívateľské a počítačové nastavenia pre celé skupiny užívateľov a počítačov
- možnosti – inštalácia aplikácií, práca so skriptami (logon/logoff, start-up, shutdown), nastavenie systému (plocha, ponuky, IE), politiky zabezpečenia, atď.
- Kombináciou lokálnej GPO, Site-based GPO, Domain based GPO a OU-based GPO (org. jednotky) je možné vytvoriť tzv. efektívnu politiku

Možnosti minimalizácie - konkr.5

DCIT

Group policy (GP) – podrobnejšie (pokrač.)

- efektívna politiku, alebo tiež RSoP (Resultant Set of Policy)



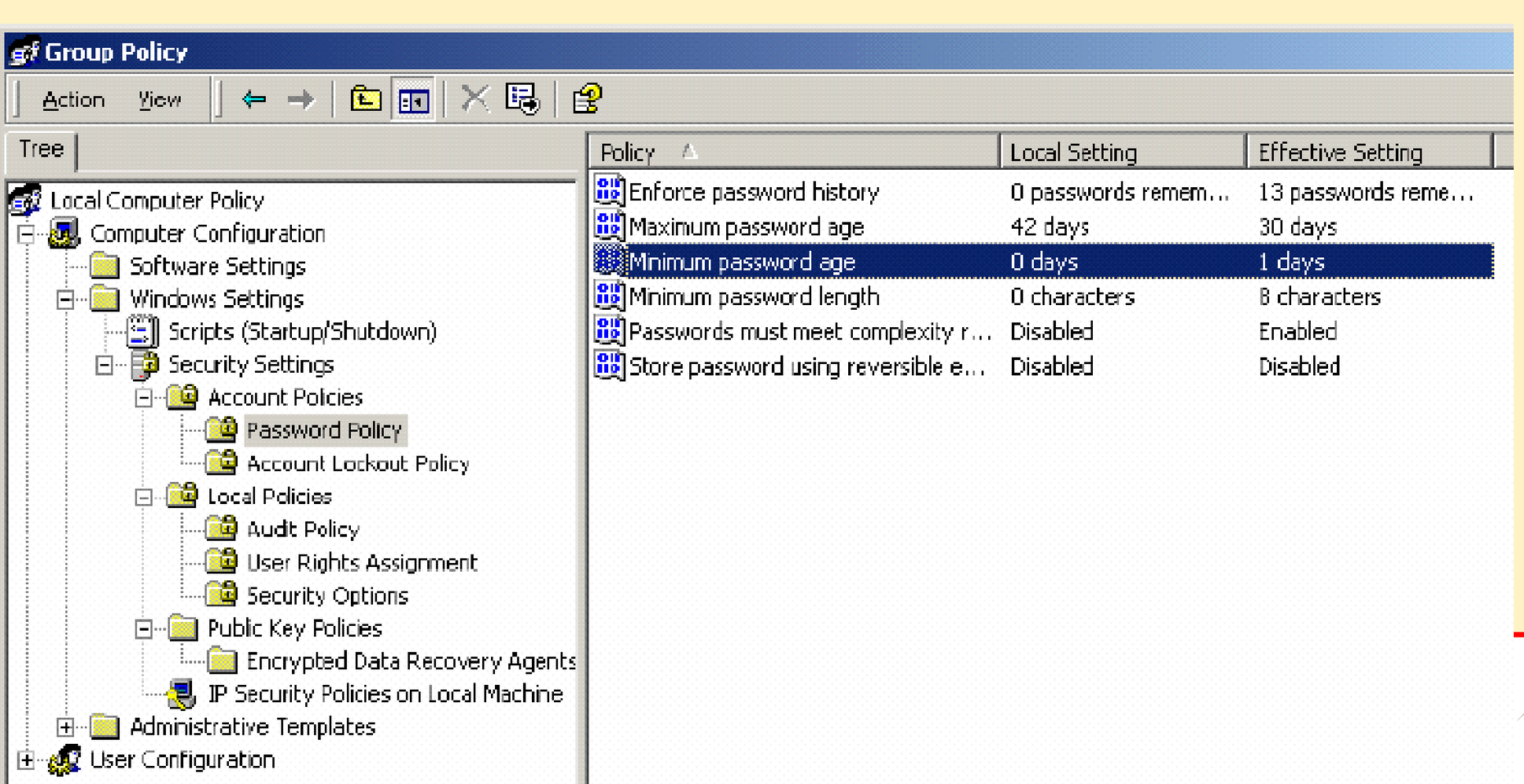
CONSULTING DCIT

Možnosti minimalizácie - konkr.5

DCIT

Group policy (GP) – podrobnejšie (pokrač.)

- čo je možné nastaviť/nastaviť:
  - nastavenia na úrovni GUI (kozmetika)
  - bezpečnostné nastavenia (Account Policy, Local Policies, EventLog, Services, Registry, File System, IPSEC, PKI)



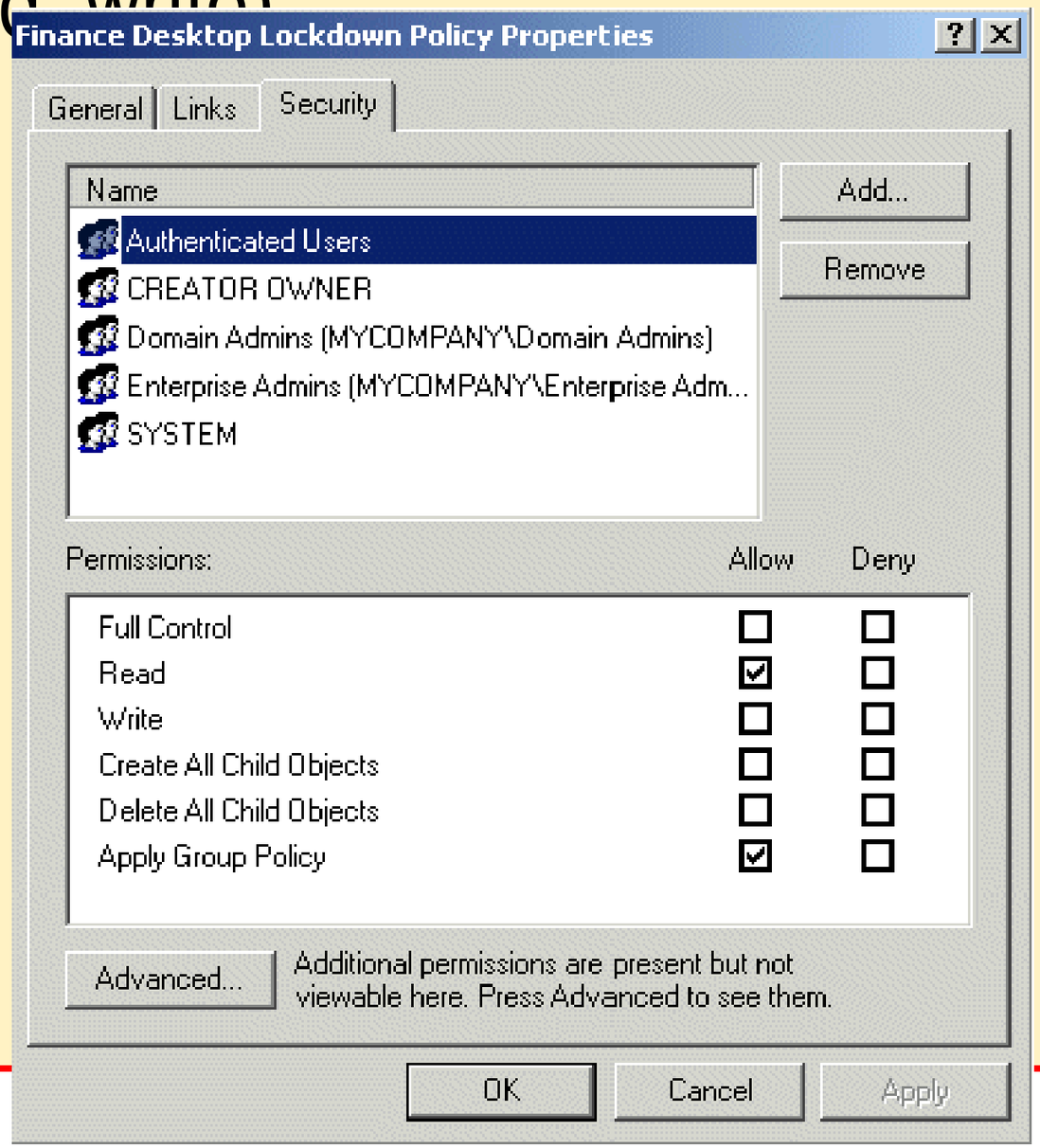
CONSULTING DCIT

Možnosti minimalizácie - konkr.6

DCIT

Group policy (GP) – podrobnejšie (pokrač.)

- pri GP je možné nastavovať ACL, právo Apply, možnosti filtrov (read, write)



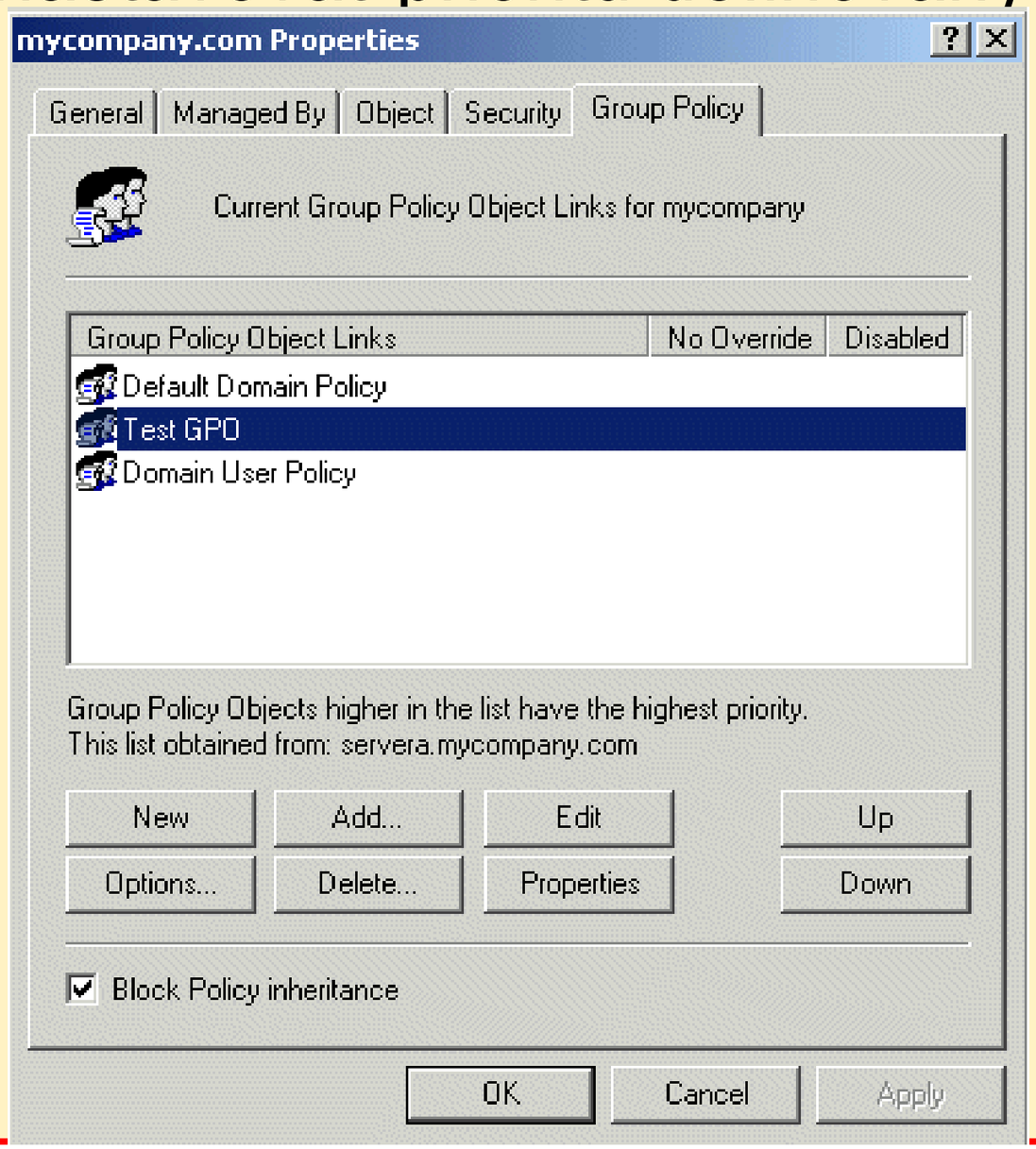
CONSULTING DCIT

Možnosti minimalizácie - konkr.6

DCIT

Group policy (GP) – podrobnejšie (pokrač.)

- pri GP je možné nastavovať prioritu definovaných politík



CONSULTING DCIT

Možnosti minimalizácie - konkr.6

DCIT

Group policy (GP) – podrobnejšie (pokrač.)

- táto oblasť má však aj svoje úskalia
- „nenávratnosť“ niektorých nastavení (potrebné špecifické reverzné politiky a „dekontaminačné“ kontajnery)
- špeciálne v rozsiahlych prostrediach sa môžu doménové GPO „vymknúť kontrole“

CONSULTING DCIT

Krátke resume

Existujú možnosti, ako čiastočne eliminovať ľudské činnosti, použitím existujúcich (vstavaných) riešení a ich kombinovaním. Akákoľvek činnosť v tejto oblasti a odklon od „default“ nastavení je pozitívna.

Niektoré z oblastí, ktoré zostali otvorené:

- sociálne inžinierstvo
- interný audit zameraný na IT (odd. auditu alebo bezp. manažér)

Zaver

DCIT

Otázky?

Martin Zajíček, zajicek@dcit-consulting.sk

CONSULTING
D C I T