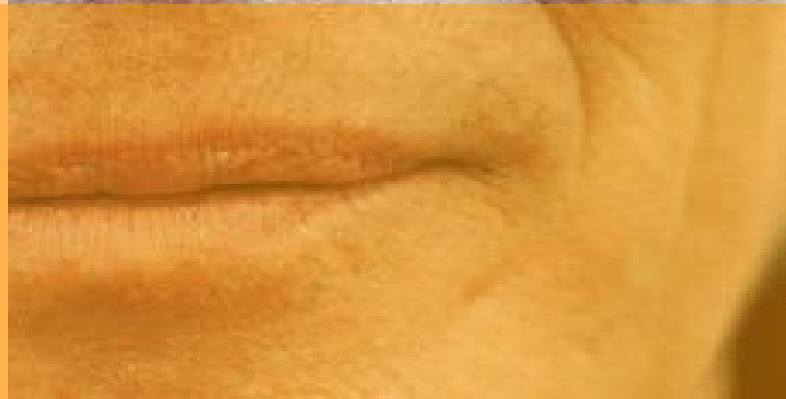
Let‘s talk about ...

IT Protection against External Attacks



Gerhard Hackl
SBS ORS SEC
Siemensstrasse 92
A-1210 Wien
Tel: +43 (0) 51707 24800
Fax: +43 (0) 51707 59390
Email: gerhard.hackl@siemens.com

Agenda

1. Informačná bezpečnosť a jej nutnosť

3. Útoky z vonkajšieho prostredia

5. Bezpečnostné opatrenia

7. Best Practice – ukážka z praxe

gerhard.hackl@siemens.com

„Eine Lüge ist schon um die halbe Welt gerast, während sich die Wahrheit noch die Schuhe bindet !“

Mark Twain

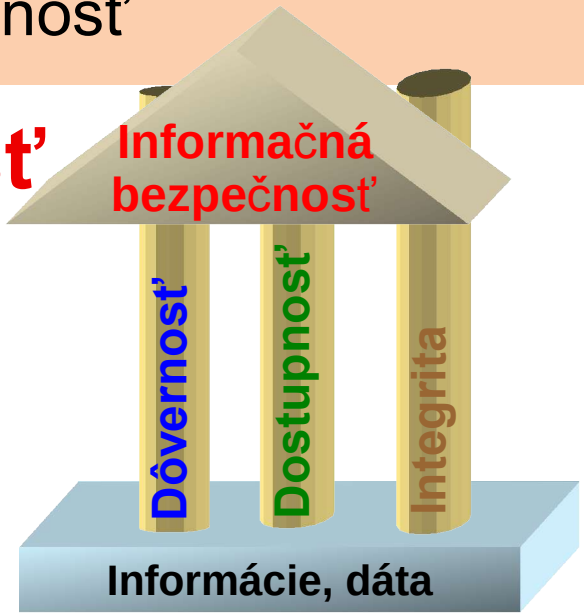
gerhard.hackl@siemens.com

Informačná bezpečnosť a jej nutnosť

Informačná bezpečnosť

nám slúži na zabezpečenie

- dôvernosti
- dostupnosti
- integrity



„Prečo“ informačná bezpečnosť ?

- aby len opravnené osoby mali prístup ku konkrétnym informáciam (dôvernosť)
- aby bol zaručnený spoľahlivý a včasný prístup k informáciam pre oprávnené osoby (dostupnosť)
- aby bola zaručená ochrana informácií pred ich neoprávnenou modifikáciou (integrita)

gerhard.hackl@siemens.com

Informačná bezpečnosť a jej nutnosť

Informačná bezpečnosť	Dôvernosť	Dostupnosť	Integrita
Typ narušenia	Krádež dát	Web-stánka Nie je k dispozícii	Neoprávnená manipulácia dát
Útoky	Hacking Vírusy	DoS-útoky Chyba softvéru	Špionáž Hacking
Dôsledky	Porušenie zákona o ochrane dát Strata dobrého mena	Prerušenie prevádzky Strata zákazníka	Strata dát Strata obratu

gerhard.hackl@siemens.com

Informačná bezpečnosť a jej nutnosť

Zamestnanci

Intranet

- Dokumenty
- Workflow
- Elektronický archív
- Elektronická kancelária
- Knowledge Management

Úrad

Internet

- Elektronická komunikácia
- WWW - Prezentácia
- Online - formuláre
- Virtuálna Pošta
- Virtuálna kancelária

**Občania,
podniky,
administratívy,
oznamy, tendre,
E-Billing**

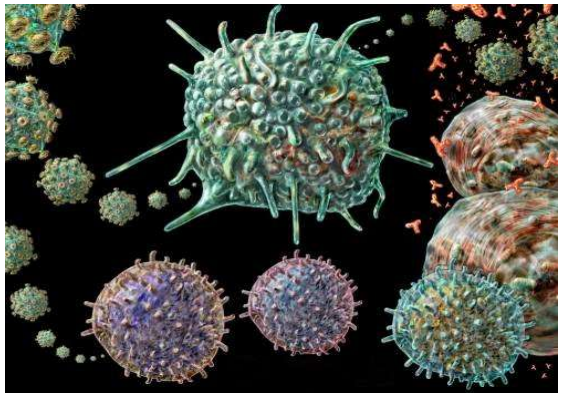
gerhard.hackl@siemens.com

Útoky z vonkajšieho prostredia

Reálny svet	→	Cyberspace
Vojna	→	Information Warfare
Terorizmus	→	Cyberterrorism
Blokády, zátarasy	→	Denial-of-Service-Attacks
Vandalizmus	→	Webpage Defacement
Demonštrácie	→	Hacktivism
Špionáže	→	Cyber e-Spionage
Kriminalita	→	Cybercrime
Protesty	→	Mailbombing
Biologické zbrane	→	Computer Viruses

gerhard.hackl@siemens.com

Narušenie it-bezpečnosti v slovenských podnikoch (2003)



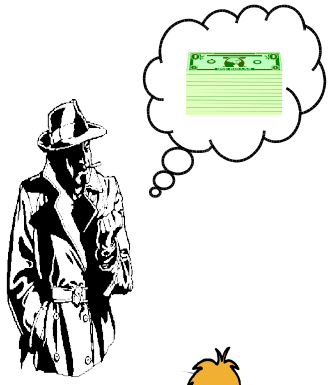
Zdroj: WU-Wien

gerhard.hackl@siemens.com

Útoky z vonkajšieho prostredia

Attachements

VPN



Rozptyľovacie taktiky

Vírusy

Downloads z Internetu

DoS útoky

Businesspartner

Hacking

SPAM

Pishing

gerhard.hackl@siemens.com

Útoky z vonkajšieho prostredia *(príklady)*

Vírus trápi švédsku zdravotnú poisťovňu

- Ochromenie celej prevádzky švédskej zdravotnej poisťovne (23. Jún 2004)
- Väčšia časť počítačov s operačným systémom Windows je napadnutá a ochromená vírusom
- Výpadok individuálnych internetových služieb ako aj informačného telefónu zdravotnej poisťovne
- Typ a pôvod virusu nebol k dňu napadnutia známi

Sasser

- Tento červ spôsoby zrútenie napadnutých počítačov
- DoS elektronického hlasovacieho zariadenia v slovenskom parlamente v Bratislave

gerhard.hackl@siemens.com

Útoky z vonkajšieho prostredia *(úroveň hrozieb)*

Riziká na pracovisku

- Otvárajú nevyžiadanú poštu a jej prílohy bez toho, aby si overili zdroj a skontrolovali obsah mailu
- Inštalujú softvér z neoverených zdrojov (víry, spyware, ...)
- Používajú slabé a ľahko uhádnuteľné heslá

Riziká v administrácií

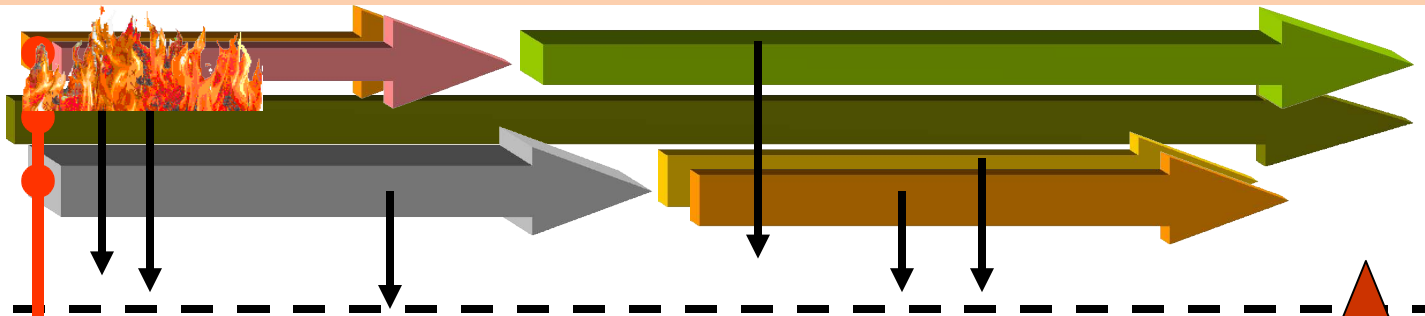
- Pripojenie nedostatočne zabezpečených systémov na Internet
- Neinštalujú opravy na známe bezpečnostné chyby
- Firewally nemajú nastavené pravidlá, ktoré by zakázali nebezpečnú premávku dnu aj von z organizácie
- Nedostatočne aktualizujú antivírovú ochranu alebo ju nepoužívajú v potrebnej miere

Riziká v manažmente

- Často nechápu vzťah medzi predmetom podnikania a informačnou bezpečnosťou
- Neuvedomujú si, akú majú hodnotu informácie a dobré meno ich organizácie
- Prideľujú nevyškolených ľudí na úlohy spojené so zabezpečovaním informačnej bezpečnosti spoločností a neposkytujú im ani dostatok času na školenia a zaučenie do úlohy

gerhard.hackl@siemens.com

Scenár e-Mail



Procesy

Operatívne/ Podpo-rujúce

Objekty

Digitálne (IT)

Software, Dáta

Mail

Fileserver

Domain Controller

Aplikácia „xy“

Intranet Server

Hardware

Sieť

Server

Clients

Fyzikálne

Infra-štruktúra

HKL(S

Napájanie

Vedenie/ lapájan

Budova

Výrobné stroje

Organi-začné

Osoby

Manažment Vedenie

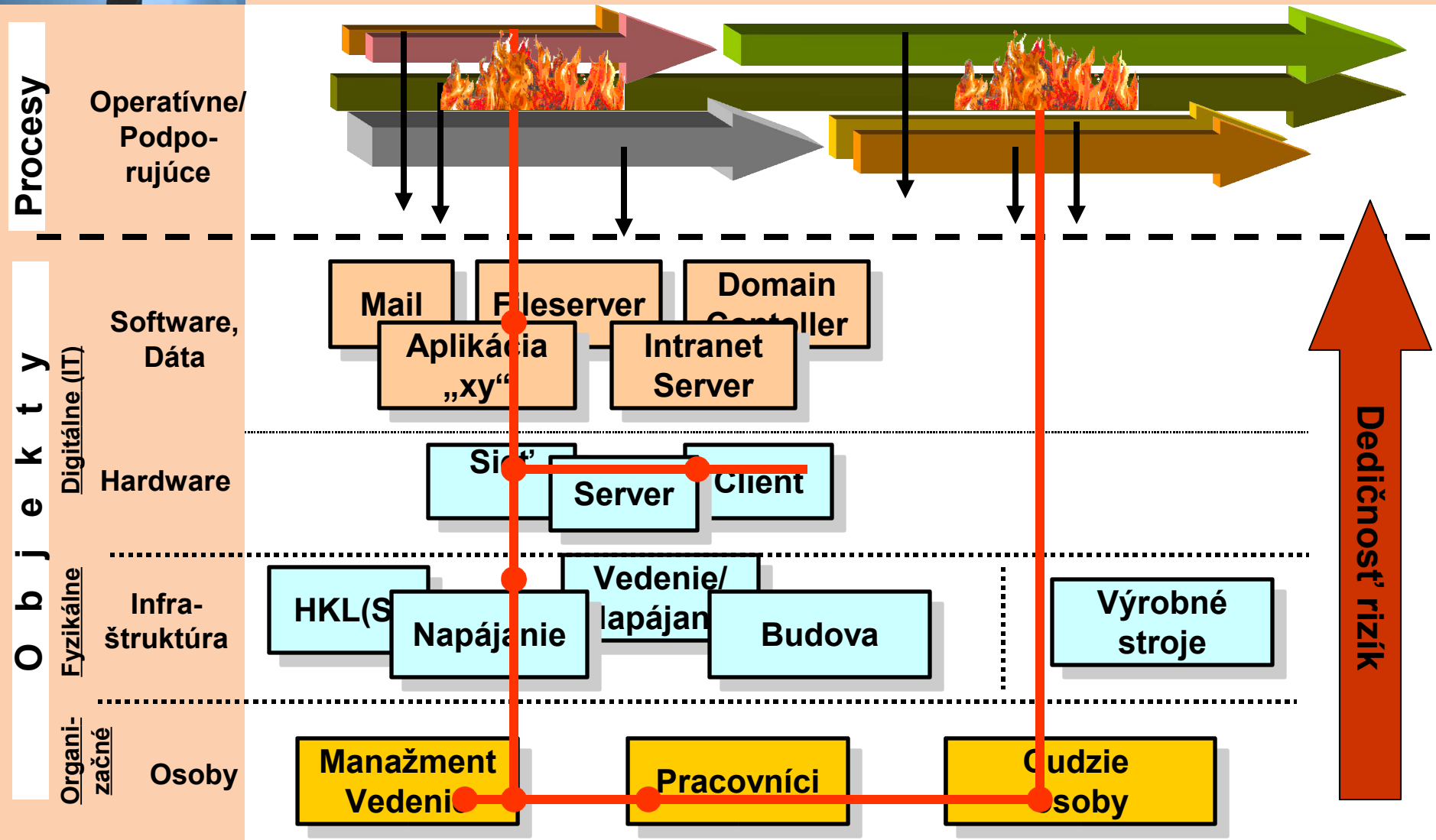
Pracovníci

Cudzie osoby

Dedičnosť rizík

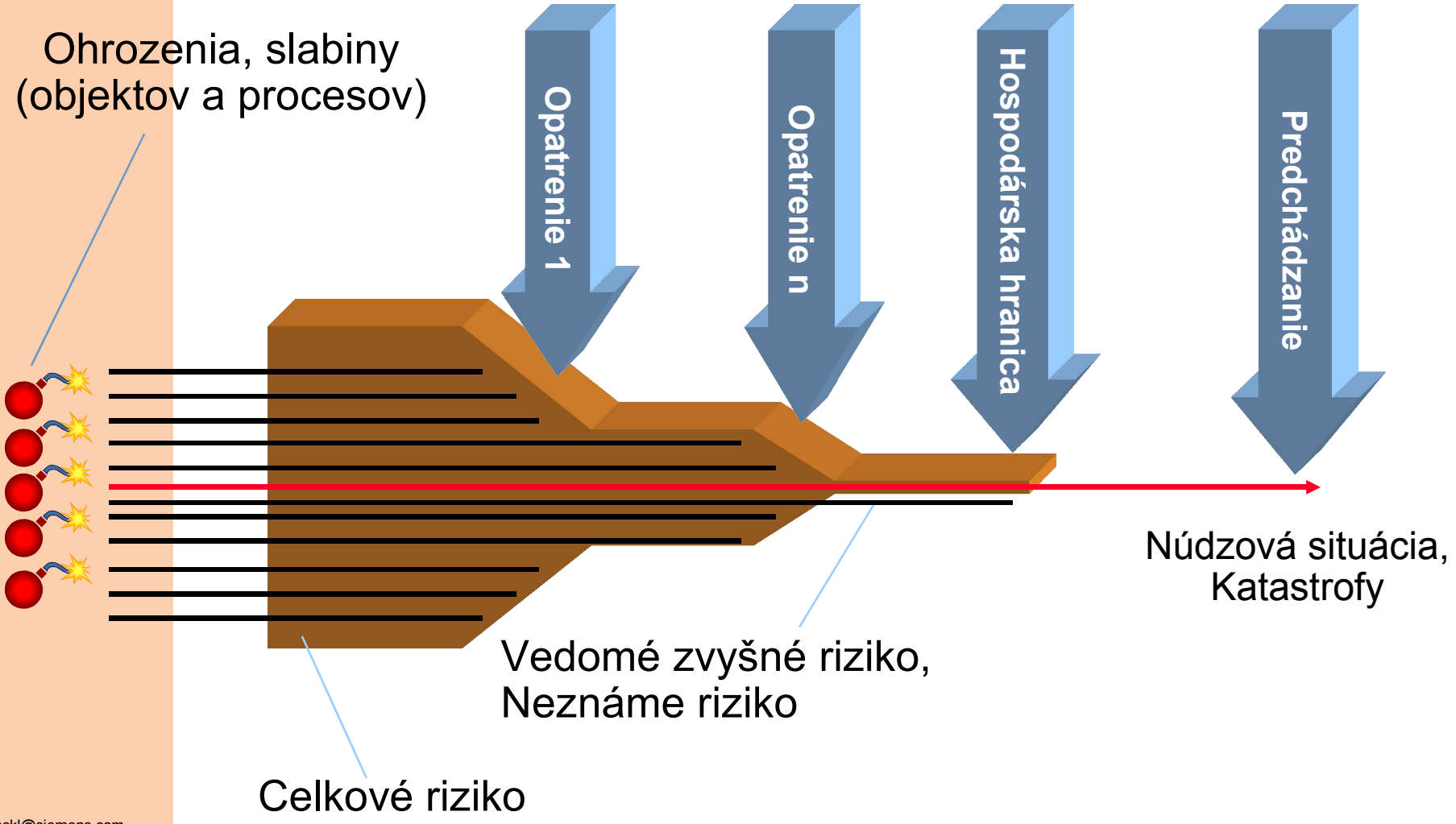
gerhard.hackl@siemens.com

Scenár DoS



gerhard.hackl@siemens.com

Bezpečnostné opatrenia



gerhard.hackl@siemens.com

Phishing

Nevinne pôsobiace emaily sú rozposielané rôznym príjemcom elektronickej pošty, pričom odosielateľ sa mylne vydáva za banku alebo inú inštitúciu. Príjemca pošty je vyzvaný zadať PIN/TAN kódy alebo iné osobné údaje na WWW-stránku, ktorej odkaz bol zadaný v emaily. Odkaz je samozrejme na pohľad autentický, čo nie je nijaký problém (email je totiž vo formáte HTML). Odkaz Vás však nasmeruje na stránku podvodníkov, ktorí takto neoprávnene získavajú osobné údaje.

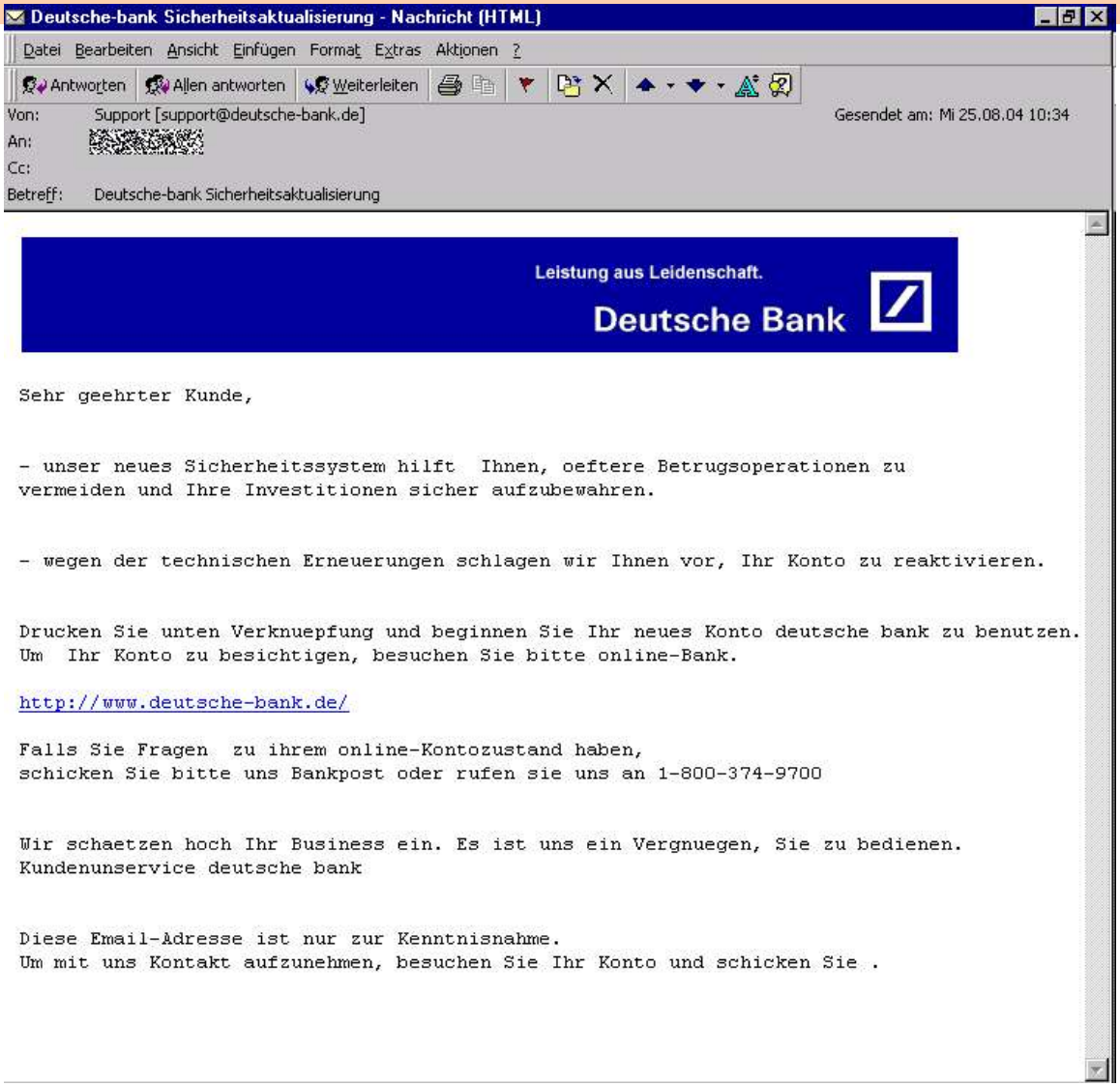
Na základe prieskumu (Gartner Group) v USA sa vzniknutá škoda Phishing útokov odhaduje za posledných 12 mesiacov na 2,4 Mrd. $.

Poštová Banka *(Deutsche Postbank):*

- **Jeden zákazník si ešte včas všimol a stornoval neoprávnený prevod zo svojho konta v hodnote 9000 €.**
- **Neoprávnený prevod vo výške 12.000 € bol zistený pri internom bezpečnostnom audite.**
- **Títo zákazníci zadali na sfalšovanej internetovej stránke Poštovej Banky (Postbank) svoje prístupové kódy.**

gerhard.hackl@siemens.com

PHISHING – mylné zavádzanie zákazníkov



Deutsche-bank Sicherheitsaktualisierung - Nachricht (HTML)

Datei Bearbeiten Ansicht Einfügen Format Extras Aktionen ?

Antworten | Allen antworten | Weiterleiten

Von: Support [support@deutsche-bank.de]
Gesendet am: Mi 25.08.04 10:34
An: [redacted]
Cc:
Betreff: Deutsche-bank Sicherheitsaktualisierung

Leistung aus Leidenschaft.
Deutsche Bank

Sehr geehrter Kunde,

- unser neues Sicherheitssystem hilft Ihnen, oeftere Betrugsoperationen zu vermeiden und Ihre Investitionen sicher aufzubewahren.

- wegen der technischen Erneuerungen schlagen wir Ihnen vor, Ihr Konto zu reaktivieren.

Drucken Sie unten Verknuepfung und beginnen Sie Ihr neues Konto deutsche bank zu benutzen.
Um Ihr Konto zu besichtigen, besuchen Sie bitte online-Bank.

http://www.deutsche-bank.de/

Falls Sie Fragen zu ihrem online-Kontozustand haben,
schicken Sie bitte uns Bankpost oder rufen sie uns an 1-800-374-9700

Wir schaetzen hoch Ihr Business ein. Es ist uns ein Vergnuegen, Sie zu bedienen.
Kundenunservice deutsche bank

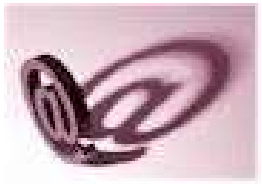
Diese Email-Adresse ist nur zur Kenntnisnahme.
Um mit uns Kontakt aufzunehmen, besuchen Sie Ihr Konto und schicken Sie .

Zákazníci Poštovej Banky sa stali terčom útokov

Quelle: FTD

gerhard.hackl@siemens.com

PHISHING - opatrenia



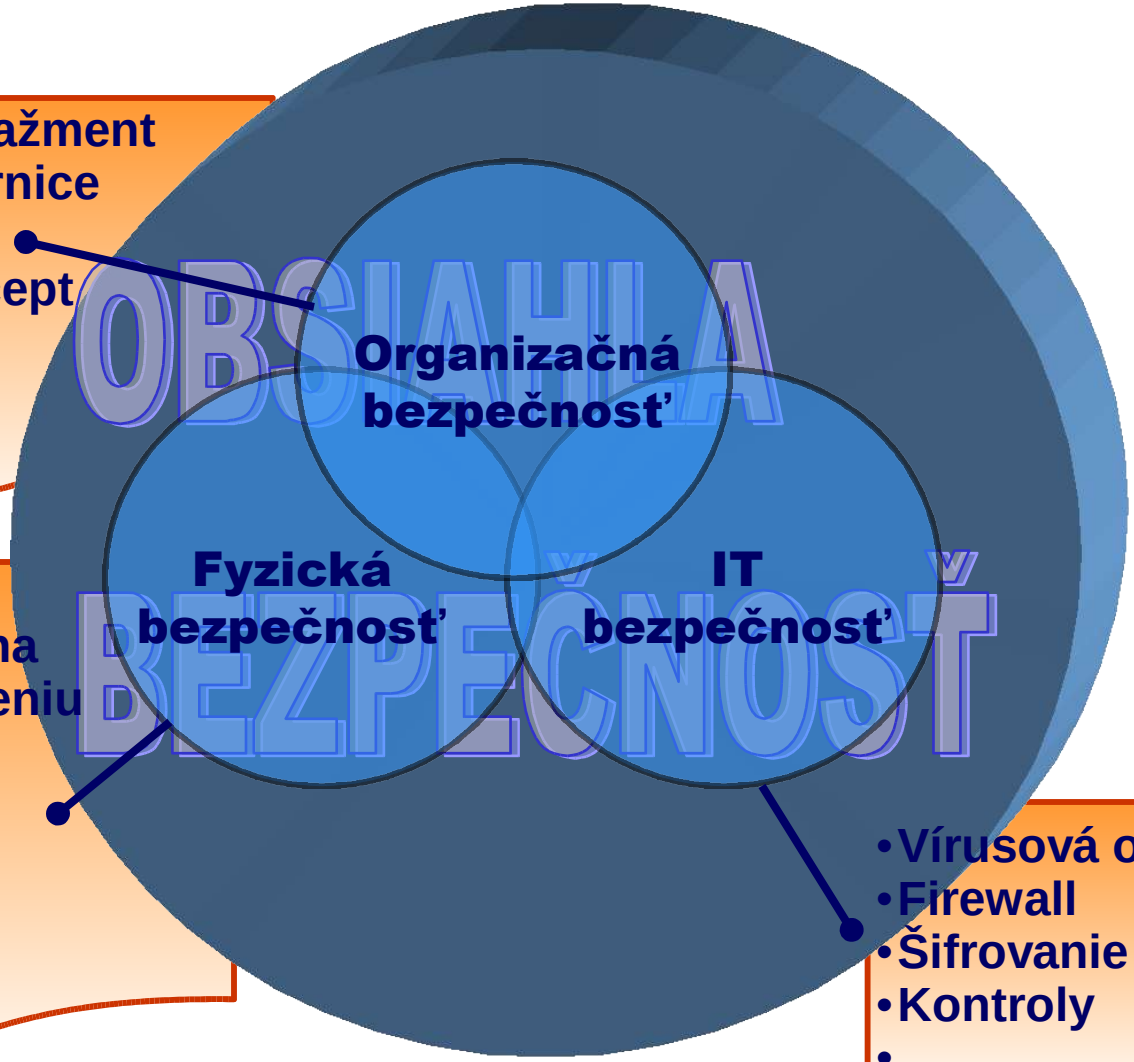
- Ignorujte odkazy v emailoch, ktorých skutočná adresa nie je overená!
- Neverte každému emailu, ktorý Vás bezprostredne vyzýva zadať Vaše osobné údaje finančného charakteru – buďte nedôverčivý!
- Dávajte si pozor na digitálny podpis – v prípade chýbajúceho digitálneho podpisu môže byť email sfalšovaný!
- Dávajte si pozor aby ste vždy mali inštalované najaktuálnejšie bezpečnostné updaty pre Váš prehliadač, keďže aj ich bezpečnostné diery (OPERA) umožňujú falšovanie pravých WWW-adries (URL)!

Quelle: FTD

gerhard.hackl@siemens.com

... Obsiahle bezpečnostné opatrenia...
Tri neoddeliteľné komponenty

- Bezpečnostný manažment
- Bezpečnostné smernice
- Analýza rizík
- Bezpečnostný koncept
- Pravidlá
- Kontrola kvality
- Audity
- ...



- Bezpečnostné zóny
- Protipožiarná ochrana
- Ochrana proti zatopeniu
- Ochrana prepätia
- Redundantná infraštruktúra
- Detekcia vlámania
- Kontrola prístupu
- Monitorovanie
- ...

- Vírusová ochrana
- Firewall
- Šifrovanie
- Kontroly
- ...

gerhard.hackl@si...

Bezpečnostné opatrenia

Ktorým bezpečnostným opatreniam chcú slovenské podniky v nasledujúcich 24-mesiacoch venovať svoju najväčšiu pozornosť?

IT bezpečnostné opatrenia	Priemer
Ochrana proti vírom,červom a trójskym koňom	1,82
Organizačné opatrenia *(napr. bezpečnostné smernice)*	2,20
Analýza rizík a slabých miest	2,22
Firewall	2,22
Bezpečnosť výpadku	2,22
Kontrola prístupu *(fyzické zabezpečenie)*	2,76
Právne aspekty informačnej bezpečnosti	2,78
Bezpečnostné podvedomie *(napr. školenia)*	2,86
Email – šifrovanie	3,08
Externý bezpečnostný audit	3,32

1 – najväčšia pozornosť
5 – najmenšia pozornosť

Zdroj: WU-Wien

gerhard.hackl@siemens.com

Best Practise
Stratégia

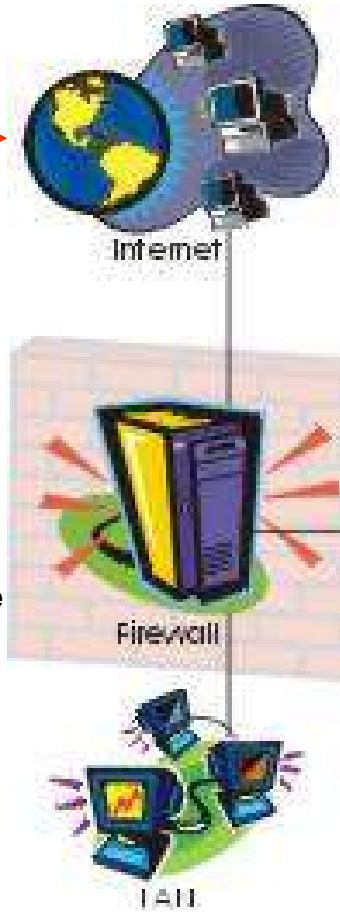
Governance	**Governance definuje štandardy, pravidlá a riešenia.**
Organizácia & Procesy	**-viaže na seba manažment, pracovníkov a poskytovateľov služieb. Integruje bezpečnostné funkcie do obchodných procesov a podporuje realizáciu potrebných opatrení.**
Povedomie	**Zväčšovanie povedomia je jeden z rozhodujúcich faktorov pre úspešnú informačnú bezpečnosť.**
Technika	**Technika preberá podpornú a nezastupiteľnú úlohu.**
Kontrola	**Obsiahla kontrola preverí efektívnosť opatrení.**
Partner	**Silný a kompetentný partner Vám zabezpečí pokojný priebeh prevádzky.**

gerhard.hackl@siemens.com

Flash Check

Externer Security Check z Internetu (FLASH CHECK)

Postupnosť



Pomocou externých útokov, podobným aké používajú hackeri pri prekonávaní firewallov, je celý systém firewallu (router, firewall a dmz) za pomoci Security scaneru ako aj ručných útokov, preskúmaný a prekontrolovaný na slabé miesta, čím sa odhalia eventuálne bezpečnostné diery.

gerhard.hackl@siemens.com

Ďakujem za Vašu pozornosť

Sicher ist,
dass nichts sicher ist,
selbst das nicht!

Joachim Ringelnatz

Gerhard Hackl

Siemens Business Services

Operational Related Services

Security

gerhard.hackl@siemens.com