

Bezpečnost intranetových aplikací

Karel Miko (miko@dcit.cz)

DCIT, s.r.o. (www.dcit.cz)



Hlavní body prezentace

- Fakta: historie a současnost
- Bezpečnost uvnitř podniku
- Kde jsou slabá místa intranetových aplikací?
- Kde leží řešení bezpečnosti Intranetu?
- Bezpečnost z hlediska manažera

Cílem příspěvku je ukázat význam bezpečnosti, která je často uvnitř podniku podceňována

Fakta: historie a současnost

Intranet: Jak vznikl? Co se tím rozumí?

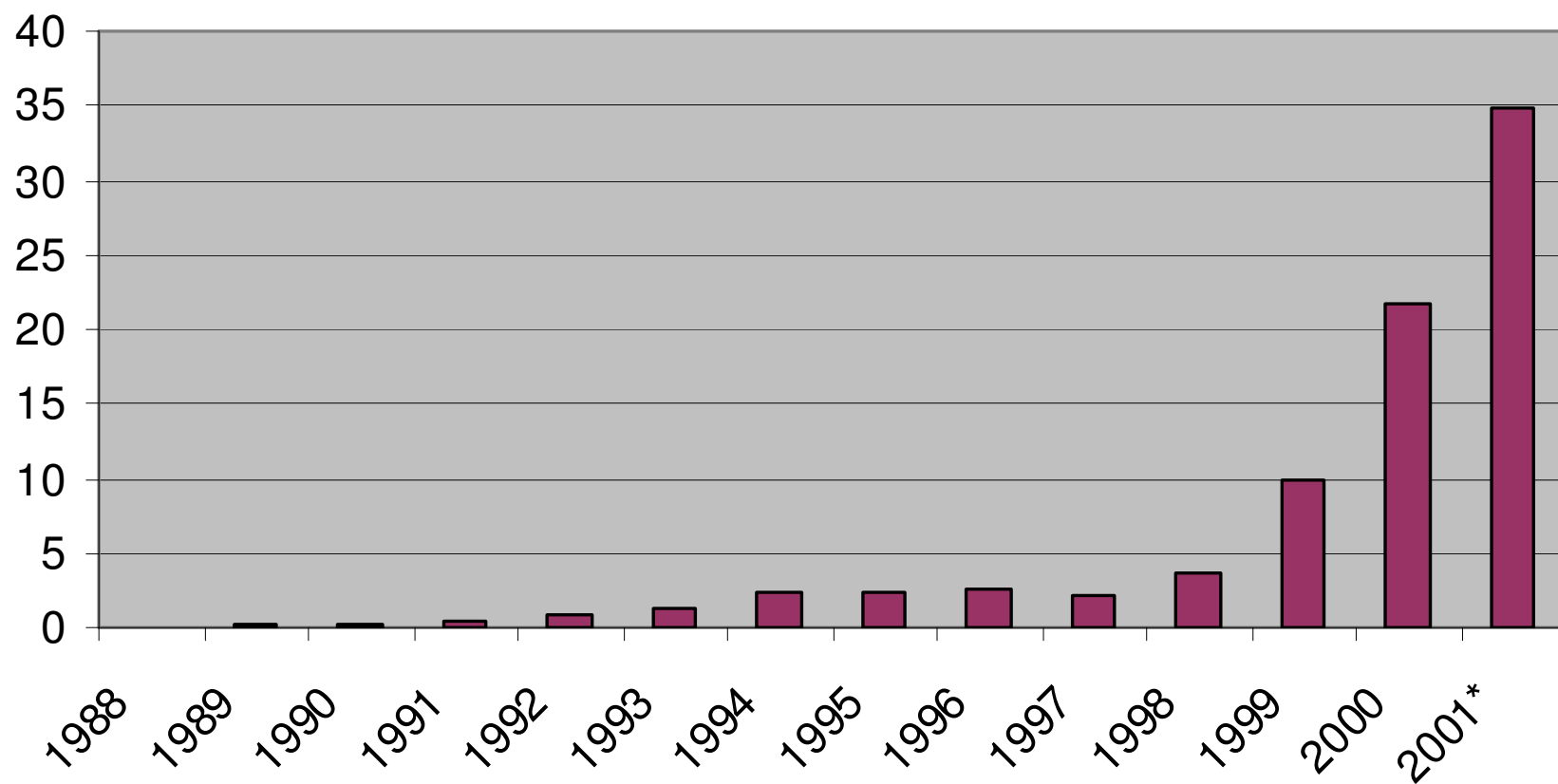
- není jednoduché najít přesnou definici
- pojem Intranet - zhruba polovina 90. let
- původní idea: „*Intranet = použití původně internetových technologií pro interní inf. systémy*“
- Intranetem se obvykle rozumí soubor vnitřních WWW aplikací přístupných širokému okruhu zaměstnanců
- z širšího hlediska lze pojem Intranet zobecnit na **veškeré vnitřní informační systémy** (často je WWW jejich jediným rozhraním)

Intranet - inspirace Internetem

- záměrem bylo zcela nepochybně převzít z internetových technologií to „pozitivní“
- Intranet ovšem přejal také řadu negativních aspektů internetových technologií - mimo jiné také řadu nedostatků v oblasti bezpečnosti
- bezpečnostní problémy - téma této prezentace
 - jsou známe především z oblasti Internetu (často bývají medializované - viz nedávný CodeRed)
 - zcela logicky je třeba s nimi počítat i v Intranetu (ve vlastním zájmu je většina firem nezveřejňuje)

Statistika - bezpečnostní incidenty

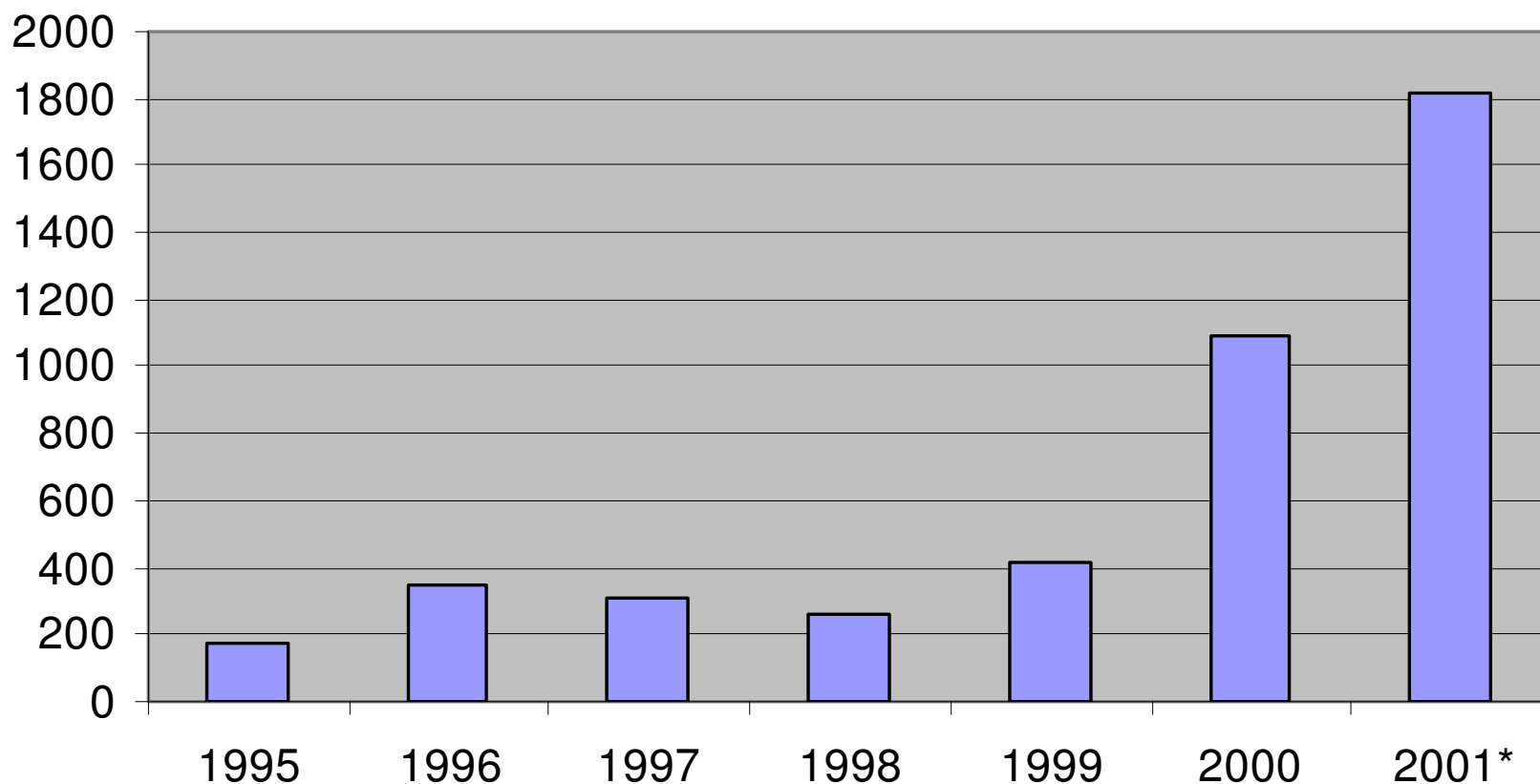
Vývoj počtu evidovaných incidentů (v tisících)



zdroj: www.cert.org

Statistika - bezpečnostní slabiny

Vývoj počtu zveřejněných slabin v inf. systémech



zdroj: www.cert.org

Z hlediska Intranetu jsou zajímavá některá další statistická čísla

- 2001 CSFI/FBI Computer Crime and Security Survey
 - neautorizované použití interního systému 64% respondentů
 - vážný incident ve vnitřní síti přiznalo 59% respondentů
 - zaměstnanec jako pravděpodobný zdroj útoku 76%
- PSIB 2001 PricewaterhouseCoopers, DSM
 - vlastní uživatele označilo jako hlavní hrozbu 49%
 - incident v důsledku selhání uživatele zaznamenalo 61% respondentů
 - přes 40% společností bylo postiženo bezpečnostním incidentem s prokazatelnými finančními dopady



Bezpečnost uvnitř podniku

Hlavní hrozby z hlediska Intranetu

- falešný pocit „bezpeční domova“
- nedůsledná údržba a dohled nad interními systémy
- podcenění vnitřního nepřítele - zaměstnance (důvěřuj ale prověřuj)
- v Intranetu jsou používány zcela totožné technologie jako na Internetu (např. WWW servery) (tj. stejné slabiny, stejné metody průniku, ...)
- útok zevnitř: malá pravděpodobnost - velký dopad
- v rozsáhlých sítích (stovky/tisíce uživatelů) je velmi obtížné kontrolovat každého

Kdo je útočníkem

- zaměstnanec mající úmysl škodit (zaměstnanec ve výpovědní lhůtě, neprověřený nový pracovník, ...)
- neznalý zaměstnanec - tzv. „social hacking“
- zaměstnanec nevědomě zneužitý k útoku
- hacker (z uvedených bodů nejméně časté)

Co je cílem útoku

- získat informace (ne nutně pro potřeby útočníka)
- provést nějakou operaci jménem někoho jiného
- pozměnit data ve prospěch svůj (či jiného)
- získat (pro někoho) konkurenční výhodu



Způsob provedení útoky

- metody totožné jako u internetových průniků (tzn. řadu „návodů“ lze najít na Internetu)
- interní útoky obvykle vyžadují delší přípravu
- nezanechat viditelné stopy (obtížně dohledatelné)

Následky útoku

- ztráta konkurenční výhody
- poškození zákazníka
- poškození práv vlastních zaměstnanců
- negativní vliv na image podniku
- v konečném důsledku finanční ztráta

Slabiny v systémech

- slabiny v systémech byly, jsou a budou
- některé slabiny byly zveřejněny po 5 a více letech
- současné systémy a aplikace jsou čím dál více sofistikovanější a složitější (vyšší výskyt chyb)

Extranet - komunikace s partnery

- Intranetové aplikace jsou často otevírány směrem k zákazníkům a partnerům
- to přináší zcela nové (až překvapivé) hrozby
- často jsou extranetová řešení spouštěna pod tlakem termínů (příp. konkurence)



Nové generace útoků

- spolu s velmi dynamickým vývojem IT technologií jdou kupředu i nástroje a metody hackerů
- agresivita útoků stoupá (např. útoky obcházejí technická opatření zneužitím důvěřivých uživatelů)
- nový fenomén - automatické útoky - např. CodeRed = robot napadající všechny napadnutelné servery v dosahu, z těchto pak napadá další a další
- rostoucí výpočetní síla např. zjednodušuje tzv. uhodnutí hesla (schopnost člověka pamatovat si delší heslo bohužel neroste)

Kde hledat slabá místa intranetových aplikací?

Možná překvapivě jsou nejslabším místem bezpečnosti Intranetu uživatelé

- Intranet je především pro zaměstnance (zefektivní práci, usnadní přístup k informacím, ...)
- zaměstnanci ovšem nejvíce ohrožují resp. mohou ohrozit jeho bezpečnost
- uživatelé musí mít přístup do Intranetu a k informacím, aby mohli dělat svoji práci
- selhání lidského faktoru (tj. uživatele) lze jen obtížně zabránit, aniž bychom uživatele omezovali při práci

WWW servery jsou základním stavebním kamenem Intranetu

- v prostředí Internetu oblíbený terč hackerů
- průnik na Intranetový server má prakticky stejné atributy, stejný průběh, stejný „výsledek“
- intranetové servery obvykle nechrání firewally
- intranetové WWW aplikace jsou obvykle řádově složitější než internetové aplikace (jsou náchylnější na výskyt chyby)
- intranetové aplikace obvykle přistupují do provozních databází s velmi citlivými daty

Intranetové aplikace bývají obvykle poměrně rozsáhlá softwarová díla

- složitý systém - nezanedbatelná možnost chyby (i málo rozšířené systémy jsou napadnutelné)
- volba „solidního“ dodavatele/výrobce (zajištění bezpečnosti deklarují všichni)
- nutnost korektního nastavení systému
- administrace - uživatelské role a přístupová práva
- provoz a údržba systému (monitoring, kontrola)
- podpora systému ze strany výrobce (opravy, upgrady apod.)

Kde leží řešení bezpečnosti Intranetu?

Řešení bezpečnosti v rámci Intranetu

*Absolutní (100%) bezpečnost je meta,
ke které se lze jen blížit*

Bezpečnost Intranetu má dvě roviny

- Technická opatření
- Organizační opatření

**Bezpečnost nelze vyřešit jednorázovou
investicí, je to kontinuální činnost**

Volba technologie

- Intranet zahrnuje: WWW servery, nástroje pro tvorbu obsahu, intranetové aplikace aj.
- při výběru intranetových technologií je kritérium bezpečnosti často opomíjeno
- prakticky neustále probíhá rozšiřování Intranetu o nové komponenty
- většinu řešení od „solidních“ výrobců lze provozovat bezpečně
- nutnost odborné instalace a konfigurace
- potřeba pravidelné údržby a dozoru

Implementace a nasazování intranetových (WWW) aplikací

- často jsou intranetové aplikace speciálně vytvořené na míru konkrétním potřebám
- obvykle důraz na funkčnost nikoli na bezpečnost
- často je volena cesta „domácího“ vývoje
- změny intranetových WWW aplikací jsou prakticky soustavné a většinou nedůsledně kontrolované
- k průniku na intranetový server často stačí banální chyba ve zpracování jediné stránky (útočník si vystačí s běžným prohlížečem)



Stanovení pravidel, povinností a zodpovědností pro uživatele i správce

- bezpečnostní politika podniku
- provozní směrnice týkající se výpočetní techniky
- zakotvení do pracovního řádu, písemné ujednání

Formální „papírová“ pravidla vs. praxe

- zásady bezpečnosti je třeba uživatelům „prodat“
- význam osvěty a vzdělávání uživatelů
- kontrolní mechanismy (pravidelné, namátkové)
- prokazatelnost přestupků - postihy

Zajištění údržby systémů

- zodpovědnost vlastních správců i dodavatelů (např. při outsourcing) - reakční doby
- využívat podporu ze strany výrobců technologií

Reakce na incidenty

- přes veškerá opatření může incident vzniknout
- včasná detekce (monitorovací mechanismy)
- efektivní vyřešení incidentu (připravené scénáře)
- zjištění příčiny příp. viníka (nutnost zaznamenávání důležitých událostí v systému)

Bezpečnost z hlediska manažera

Definovat pravidla a povinnosti

- bezpečnostní politika, směrnice apod.

Zajistit bezpečnost IT technologií

- investice, která ochrání Vaše data

Bezpečnost v praxi

- pravidla, která nejsou vymáhána jsou neúčinná
- i špičkovou technologii lze provozovat „nebezpečným“ způsobem



Nasazení intranetových aplikací

- odborná instalace a konfigurace
- vyškolení uživatelů i administrátorů

Outsourcing údržby systému

- monitorování + reakce na incidenty
- instalace bezpečnostních oprav (záplat)

Nezávislá kontrola bezpečnosti

- penetrační (průnikové) testy
- bezpečnostní audity

Závěr



Dotazy?

Kontakt:

Karel Miko, miko@dcit.cz

<http://www.dcit.cz>

