T-Systems Czech Republic

Bezpečnost nejen informačních systémů

ISSS 2009

5. – 7. dubna 2009

T Systems

O společnosti T-Systems

- Zákazníci: korporátní zákazníci především z mezinárodních skupin a oblasti veřejné správy, průmyslu a zdravotnictví
- Tržby: cca €8.8 mld.
- Zaměstnanci: cca 45.400 (více než 700 v České republice)
- Portfolio: Telekomunikační služby, systémová integrace, transformační outsourcing, komplexní ICT řešení...
- Mezinárodní zastoupení: pobočky ve více než 20 zemích světa, celosvětové pokrytí
- Významní partneři: SAP, Intel, Microsoft, Cisco, EMC², Alcatel-Lucent
- Pozice: # v TOP5 na českém trhu IT služeb
  # 4 na evropském trhu ICT

  nejlepší řešení bezpečnostních služeb v Evropě

  (dle studie Current Analysis 2008)

ISSS 2009

Bezpečnost nejen informačních systémů

- Jaká je role uživatele a jaký má vliv lidský faktor na celkovou bezpečnost informačního systému?

Security Consulting

Risk Management, Audits and Penetration

- Komplexnost ICT infrastruktury vzrůstá jak s velikostí organizace tak v souvislosti s novými bezpečnostními trendy.
- Pomocnou ruku nabízí systém bezpečnostních analýz, autorizovaných penetračních testů, strukturovaných průzkumů (auditů) ve společnosti, které v kombinaci s dalšími opatřeními můžeme přinést výrazně lepší ochranu.
- Získané poznatky jsou předány ve formě dokumentace obsahující podrobné analýzy rizik s vhodnými protiopatřeními zodpovědným osobám ve společnosti.
- Dokumentace obsahuje především organizační, administrativní, fyzickou, infrastrukturní a personální oblast bezpečnosti, které jsou uzpůsobeny vnitřním požadavkům dané společnosti, jejím procesům a legislativě.

Security Consulting

Process Design and Implementation

- ICT bezpečnost není pouze záležitostí použitého hardwaru nebo softwaru, nebo nejnovějších technologických inovací.
- Konstrukce bezpečnostně-souvisejících procesů je minimálně stejně rozhodující. Dokonce i nejchytřejší, velmi sofistikované IT řešení bezpečnosti může být ohroženo bez adekvátního plánování, koordinace, realizaci a kontroly.
- T-Systems analyzuje, navrhuje, optimalizuje a provádí zabezpečení IT procesů a odpovídajících organizačních struktur, s cílem vytvořit vysoce efektivní a vysoce transparentní prostředí pro řízení bezpečnosti.
- Naše činnost je založena na národních i mezinárodních bezpečnostních norem včetně principů ISMS (Systém managementu bezpečnosti informací).

Security Consulting

Security ICT Architecture Design and Implementation

- Organizace nutně potřebuje umět reagovat na nové situace, tak aby bylo dosaženo specifikovaného standardu udržitelné ochrany.
- Nejlepším způsobem vytváření informační infrastruktury je využít zkušeností prokazatelně bezpečných ICT modelů a architektury již při jejím plánování.
- Naši architekti a designéři IT využijí své bohaté zkušenosti, které vám pomohou provádět zodpovědná rozhodnutí o budoucí podobě vaší strategie informačních systémů.
- Nabízíme vám plnou transparentnost nákladů s ohledem na bezpečnost už od nejnižší vývojové fáze.
- Tím zajišťujeme, že budete schopni provádět své interní a obchodní procesy v celé komplexnosti účinně a efektivně, ať už zítřek přinese cokoliv.

Security Consulting

Security and Vulnerability Management Solutions

- Přes firewally, po antivirové mechanismy až po detekci průniků: to je reálná a efektivní ICT bezpečnost pro podniky v současné době. Ale ochrana tohoto druhu přináší své vlastní problémy – například pokud jde o sledování a řízení bezpečnosti a příslušné nastavování konfigurace.

- Vzhledem k rostoucímu přívalu dat z nejrůznějších logů může představovat vážné potíže identifikovat a reagovat na kritické události. S naší pomocí budete schopni identifikovat vaše skutečné bezpečnostní problémy a oddělit je od těch méně významných.

- Naše služby zahrnují moduly pro vypracování bezpečnostních politik a organizačních manuálů. Pomáháme s identifikací podnikových aktiv, a s provedením analýzy rizik a jejich hodnocení, dokážeme nastínit vhodná ochranná opatření a rozvíjet popisy procesů a provozních modelů včetně školení.

Security Consulting

Problémy

- Je zvolení bezpečnostní technologie prioritní otázkou při návrhu bezpečnostní ICT architektury?
- Je nutné měnit původní informační systém nebo aplikace pouze kvůli změně?
- Počítá proces implementace bezpečnosti informací s aktivní účastí budoucích uživatelů systému?
- Jak probíhá seznámení uživatelů s plánovaným konečným stavem nastavení informačního systému?
- Zahrnují penetrační testy a audity také metody sociálního inženýrství a nestandardní chování uživatelů informačního systému?
- Zaručuje zavedení mezinárodních bezpečnostních standardů v organizaci reálné zvýšení bezpečnosti informačního systému?
- Rozumí uživatelé nově nastaveným procesům informačního systému a jsou s nimi ztotožněni?

Security Consulting

Řešení a doporučení

- Řešením při vytváření bezpečnosti informačních systémů je neimprovizovat a nesnažit se spoléhat pouze na zvolení bezpečnostní technologie.
- Stanovte si již na začátku bezpečnostní cíle vašeho informačního systému a konzultujte je s odborníky, budete ušetřeni nepříjemnostem.

Crypto Services

Safe Access Control

- Safe Access Control je systém pro úplné a komplexní řízení přístupu k síti.
- Bez ohledu na způsob připojení koncových bodů k síti, služba Safe Access Control zjišťuje a vyhodnocuje jejich stav z hlediska nastavených pravidel, zajišťuje optimální přístup k síti, a v případě potřeby zjednává nápravu a průběžně sleduje změny stavu koncových stanic.
- Každá IP zásuvka je otevřenou branou do vašeho informačního systému a my zaručíme, že se do něj připojí jen ti správní uživatelé a dostanou se jen do těch částí sítě, které stanoví bezpečnostní pravidla.

Crypto Services

Safe Desktop and Laptop

- Obavy o bezpečnost nezanikají při našem odpojení se z internetu nebo vypnutím počítače.
- Je velice alarmující, jak vzrůstá riziko krádeže dat nebo celého zařízení.
- Naše bezpečnostní služby ochrání vaše systémy před takovými bezpečnostními hrozbami a riziky – díky šifrování disků nebo rovnou celého operačního systému, využitím čipových karet pro identifikaci nebo kontejnerové šifrování, při kterém se automaticky ukládají data do virtuálního zabezpečeného prostředí.

Crypto Services

Safe Storage

- Safe Storage je bezpečnostní řešení v rámci celého životního cyklu pro vaše heterogenní datová úložiště nebo pásková zálohovací zařízení bez narušení součastných aplikací, infrastruktury, klientů, serverů nebo uživatelského workflow.
- Ukládání dat na úložiště s rychlým přístupem ze sítí může být citlivým a zranitelným místem vaší infrastruktury.
- Naše řešení kombinuje bezpečné systémy kontroly přístupu, autentizace, šifrování a bezpečného přihlášení k ochraně vašich dat.

Crypto Services

Safe Communication

- Řešení od společnosti T-Systems vám bude elektronicky podepisovat nebo šifrovat e-maily, dokumenty v libovolné elektronické podobě, s jediným kliknutím myši nebo zcela automaticky.
- Můžete si ověřit původ dat nebo šifrovat a dešifrovat důležité dokumenty či komunikaci a další aktiva ve vaší společnosti.
- Silné kryptografické principy autentizace, autorizace, komunikačních protokolů a šifrování zabezpečují odolný a bezpečný systém ochrany informací.

Crypto Services

Problémy

- Jakým způsobem řeší bezpečnost informačního systému životní cyklus hesel?
- Umožňuje informační systém svým uživatelům vzdálený přístup ke svým datům, aplikacím nebo elektronické poště?
- Může si uživatel informačního systému odnést na USB klíčence nebo jiném datovém médiu kompletní data organizace?
- Zaručí heslem chráněný spořič obrazovky počítač autentizaci uživatele nebo ruší v práci?
- Uživatel informačního systému nemá právo si změnit ani pozadí na obrazovce, je to správně?
- Pozná informační systém, kdo a jakým prostředkem přistupuje k interní síti a kam ho může pustit?
- Znamená ztracený nebo ukradený počítač riziko bezpečnost informací?

Crypto Services

Řešení a doporučení

- Řešením může být jedna čipová karta, díky které odstraníme většinu potíží.
- Může s potiskem sloužit pro identifikaci v organizaci, pro potřeby fyzické bezpečnosti z hlediska přístupu do vyhrazených prostorů nebo pro účely detailní docházky.
- Může vyřešit bezpečné přihlášení do informačního systému, jeho aktivitu a nebo pro potřeby generování klíčů šifrovací relace komunikace.
- Uživatel informačního systému tak má ve výsledku pouze jednu čipovou kartu s většinou čtyřmístným pinem, který si navíc může měnit tak, aby si jej snáze zapamatoval.

Managed Firewall

Popis služby

- T-Systems vám pomáhá čelit problémům ICT bezpečnostní infrastruktury – s bezpečným přístupem do sítě, firewally, antiviry, antispamem a dalšími filtry, detekčními a prevenčními nástroji, bezpečnostním managementem a monitoringem, a také komponenty pro mobilní a bezpečnou komunikaci.
- Navíc dodáváme odborné poradenství při tvorbě a realizaci bezpečného ICT prostředí a infrastruktury informačních a komunikačních technologií.
- Formou outsourcingu či převzetí, můžeme a dokážeme převzít plnou odpovědnost za provoz vašeho bezpečnostního řešení.

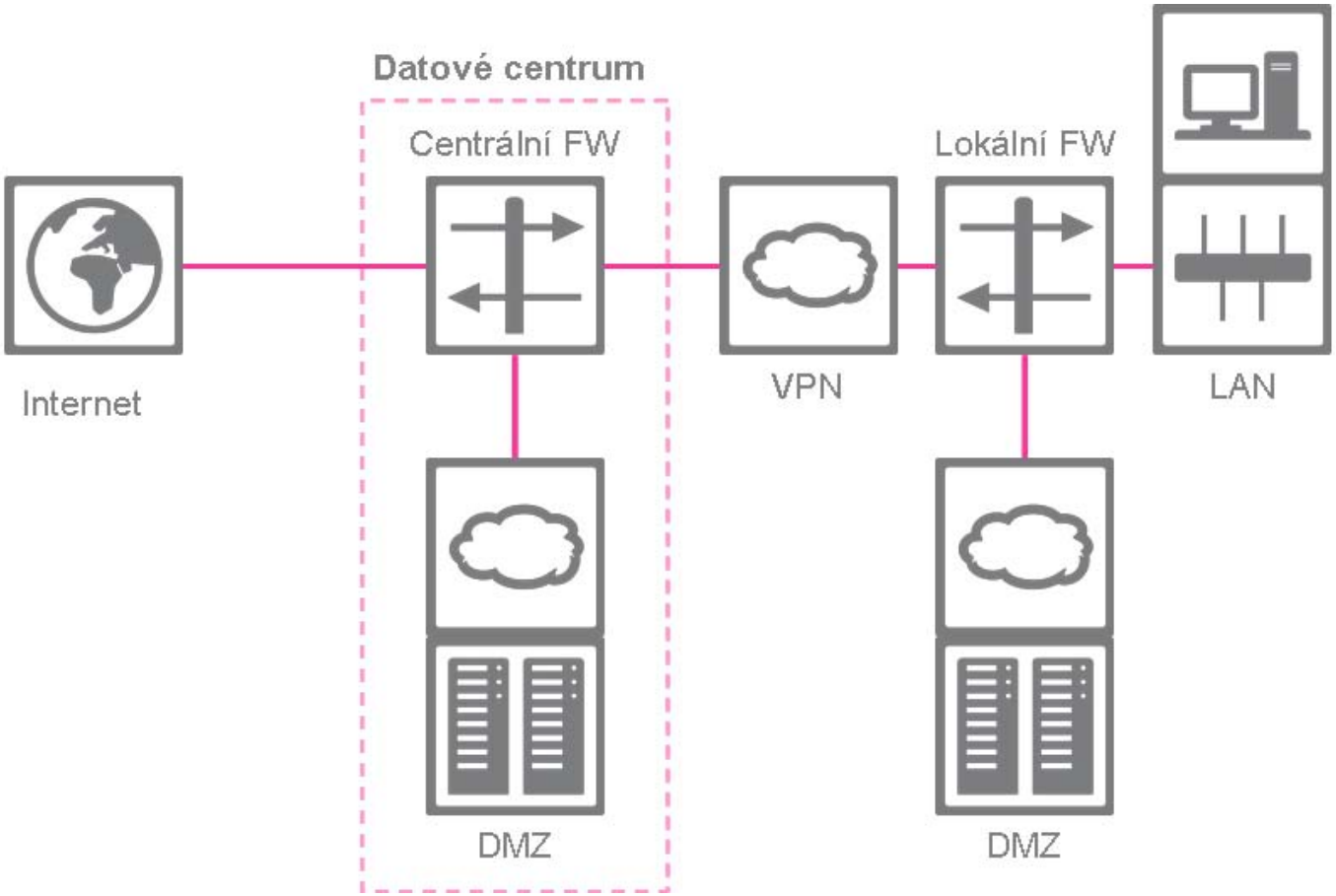
Managed Firewall

Typy služeb

- Firewall
- IPS/IDS
- Antispam
- Antivirus
- Web Filtering
- Security management
- Security monitoring a reporting
- AAA

Produkt Managed Firewall

Obrázek



Managed Firewall

Problémy

- Víte jak dlouho trvá pracovní stanici uživatele než nabootují všechny „anti“ programy nebo update operačního systému a dalších přidaných aplikací a jak ji zatěžují?
- Znemožňujete svým zaměstnancům přístup k Internetu a myslíte si, že je to správně?
- Je způsob monitorování vašeho komunikačního prostředí v souladu s platnou legislativou?
- Myslíte si, že každý soubor s koncovkou exe je virus?
- Je vaše ICT infrastruktura dostatečně bezpečnostně proaktivní, a jaká je potom doba reakce na bezpečnostní incident a jak se o něm dovíte?
- Víte jaká je povolená síťová komunikace ve vaší organizaci?
- Máte nepřetržitý systém sledování stavu bezpečnosti informačního systému?

Managed Firewall

Řešení a doporučení

- Řešením podobných problémů může být řízený přístup k Internetu přes soustavu bezpečnostních zařízení.
- Uživatel je seznámen například s tím, že od 9.00 hod do 12.00 a od 12.30 hod do 17.00 hod pracovní doby je blokován přístup na internetové stránky, které přímo nesouvisí s výkonem zaměstnání, mimo tento interval je pak blokován pouze nevhodný obsah.
- Stahování uživatelem je omezeno pouze třeba na 100 MB měsíčně a podléhá antivirové kontrole.
- Informace o typu (ne obsahu) internetové komunikace jsou uchovávány minimálně 3 měsíce ve formě použitelné jako důkazní materiál.
- V případě prohřešku ze strany zaměstnance přichází varování a teprve při dalším prokazatelném porušování pravidel jsou provedeny sankce.

SecureMail

Popis služby

- Jedním z nejdůležitějších typů komunikace je dnes elektronická pošta, která se stala nedílnou součástí jak osobního života tak pracovní činnosti.
- Přijímání a odesílání emailových zpráv je dnes stejnou samozřejmostí jako telefonování nebo faxování.
- Stinnou stránkou emailové technologie je prudký a neustálý nárůst nevyžádané pošty a s tím spojená rizika virové infekce, podvržených stránek, spyware a phishingu.

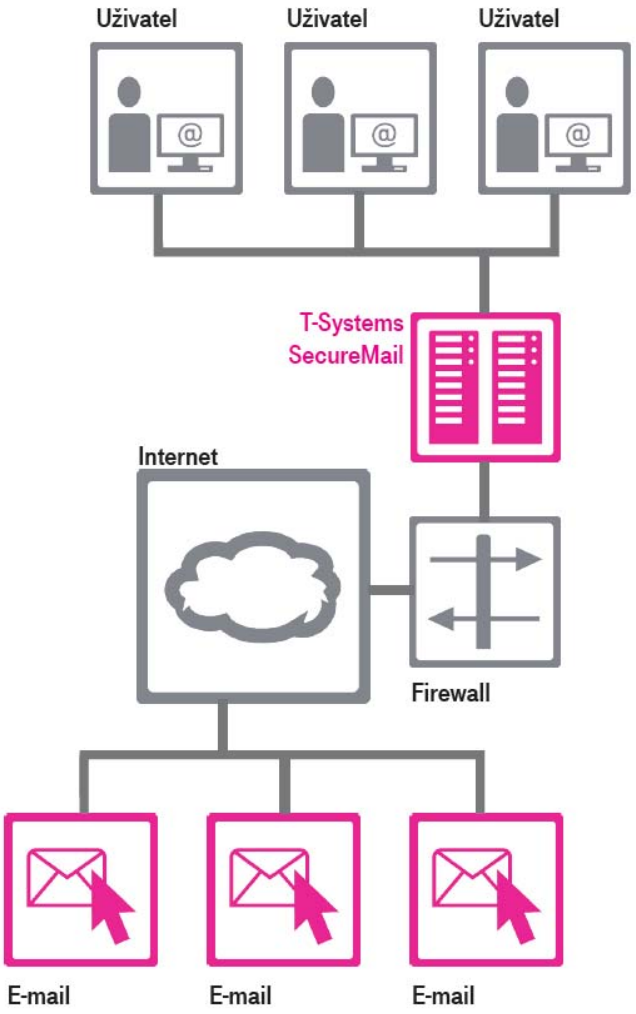
SecureMail

Celkový popis služby

- Kompletní zabezpečení emailové komunikace.
- Ochrana před nevyžádanou poštou.
- Ochrana před viry, červy a škodlivým kódem.
- Uživatelské karantény pro spam a další typy napadené pošty.
- Speciální bezpečnostní proaktivní filtry.
- Možnost detailního reportování a „online“ bezpečnostní sledování emailové komunikace.
- Ochrana příchozí, ale i odchozí pošty.

Produkt SecureMail

Obrázek



SecureMail

Problémy

- Jak zaručíte, že uživatelé informačního systému nebudou zavaleni nevyžádanou poštou?
- Jak sledovat nevhodný obsah mailů?
- Dokážete proaktivně reagovat na elektronickou poštu s virem nebo škodlivým kódem?
- Umí informační systém eliminovat pokusy o phishing?
- Jak zaručíte, že budete mít zpětně informace o veškeré emailové komunikaci?
- Dokáží uživatelé informačního systému rozlišit citlivost obsahu odesílaného respektive přeposílaného mailu?

SecureMail

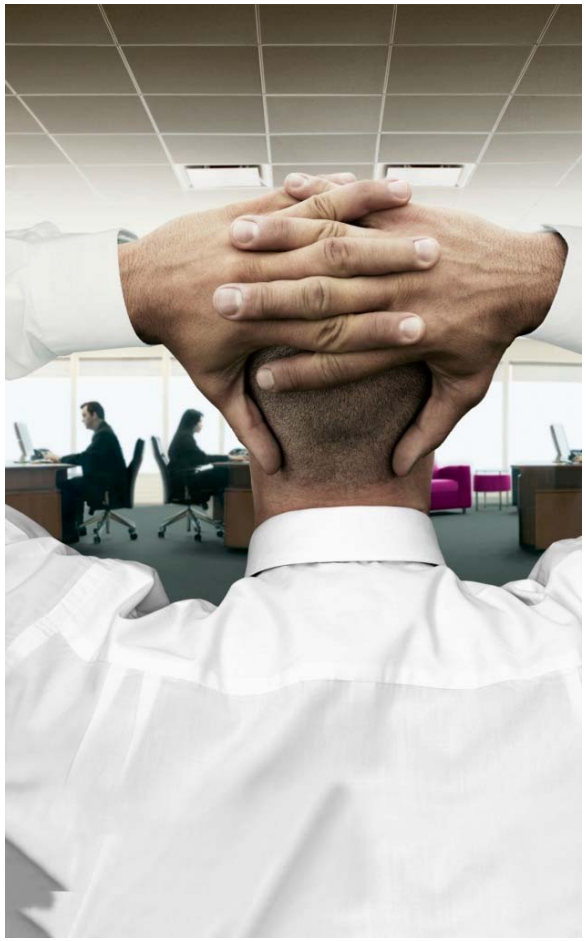
Řešení a doporučení

- Řešením problémů se zabezpečením elektronické komunikace může být automatické šifrování pošty.
- Uživatel informačního systému se potom nemusí starat o hesla nebo klíče, ale zároveň má jistotu, že jsou data chráněna.

ISSS 2009

T-Systems Czech Republic a. s.

- Společnost T-Systems Czech Republic si uvědomuje, že bezpečnostní aspekty se stávají nedílnou součástí každého ICT projektu, a proto přichází s ucelenou řadou bezpečnostních produktů a řešení, které Vám umožní nechat starosti s bezpečností na silného a důvěryhodného partnera.



T Systems

T-Systems Czech Republic a. s.

Vybrané bezpečnostní reference ze státní správy

- Ministerstvo průmyslu a obchodu (provoz a zabezpečení živnostenského rejstříků)
- Letiště Praha (zabezpečení privátní bezdrátové sítě)

ICT Security

Kontakt.

Mgr. Vlastislav Havránek

Commercial Product Manager
oddělení Commercial Product Management
divize Sales and Service Management

Tel: +420 236 099 436
Mobile: +420 739 384 754
email: Vlastislav.Havranek@t-systems.cz
www.t-systems.cz

Děkuji za pozornost...