



Co vše může zahrnovat problematika bezpečnosti v souvislostech dnešního informačního světa? O tom všem je tento článek. Budeme se věnovat propojení soukromého a pracovního života i současným výzvám, jako jsou mobilita, sociální sítě a cloud computing. Projdeme jednotlivé bloky bezpečnosti, tedy elektronickou, fyzickou a informační bezpečnost i řízení identity. V závěru se zaměříme na síťovou bezpečnost a roli poskytovatele informačních a telekomunikačních služeb.

Soukromý a pracovní svět

Každý z nás žije v našem produktivním věku nejméně dvě odlišné role a dalo by se říci, že i dva životy. První role se zaměřuje na pracovní svět a naší profesi, kdy za pomoci ICT nástrojů vykonáváme naše povolání. Zařízení jako mobilní telefon nebo počítač připojený k internetu jsou již nedílnou součástí našeho života. Zajímavou otázkou je, kolik procent lidí používá stejný počítač nebo mobilní telefon zároveň pro soukromý život?

Dá se předpokládat, že naprostá většina uživatelů ICT nástrojů je zvyklá používat mobil a počítač i další nástroje pro komunikaci jak s partnery v práci, tak se svými přáteli a rodinnými příslušníky. Prolínání privátních a komerčních světů je tedy zejména díky ICT prostředkům realitou, což ale představuje významné bezpečnostní riziko.

Zaměstnavatel by si ideálně představoval, že jeho ICT infrastruktura bude používána výhradně pro práci a zaměstnanci jsou v soukromém životě zvyklí se se stejnými ICT nástroji věnovat zábavě a volnočasovým aktivitám. ICT infrastruktura a její používání má velké pozitivní dopady na naše životy, ale její používání představuje z pohledu ochrany komerčních aktiv ohromnou bezpečnostní hrozbu.

Současné ICT trendy a výzvy

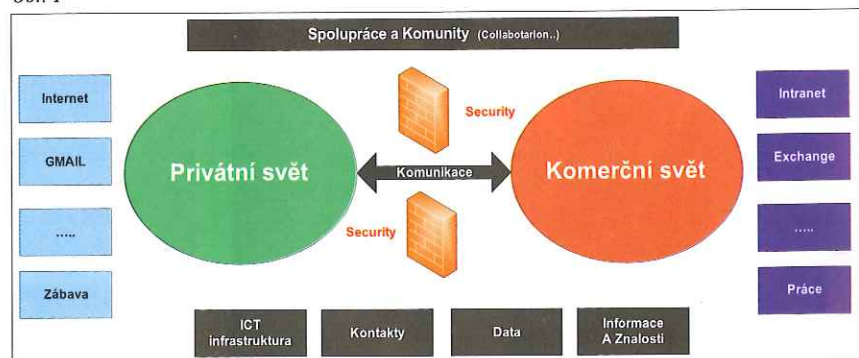
Mobilita a širokopásmový networking

Za posledních několik let se dramatickým způsobem zvětšilo geografické pokrytí celé naší planety mobilními a fixními sítěmi, takže pokud dnes máme dostatek finančních prostředků, není problém se připojit k internetu a ostatním síťovým zdrojům kdykoliv a kdekoliv.

Sociální sítě

Toto je fenomén, který nelze ignorovat, a ať už si o Facebooku myslíme cokoliv, tak naši přátelé, blízké komunity nebo i vlastní děti nás dříve či později přesvědčí, že nelze stát

Obr. 1



mimo. Zajímavou otázkou bylo a asi stále je, jaký je význam sociálních sítí pro komerční aktivity firem a zda se dají prostřednictvím těchto sítí vydělat peníze či jinak působit na firmy.

Mým osobním názorem jako autora tohoto článku je, že sociální sítě už nyní mají a do budoucna budou mít stále významnější vliv i pro korporace. Jako příklad bych uvedl aktivity firemních úseků zaměřených na vztahy k veřejnosti (PR, public relations). Dříve si tyto útvary stanovily komunikační strategii a pak cíleně prostřednictvím médií komunikovali a budovali image svojí společnosti. V době sociálních sítí se povědomí o konkrétních firmách šíří samovolně skoro virálním, a tedy těžko kontrolovaným způsobem přes jednotlivé komunity a jejich sdílené zkušenosti. Toto si komerční firmy uvědomují, a proto se již objevují první nástroje a použití tzv. social miners – tedy aplikací, které jsou připojeny do důležitých sociálních sítí a vyhledávají zde klíčová slova, témata a diskuse, na která PR útvary reagují a tak mohou zpětně působit na komunity a povědomí o své firmě.

Nová koncová zařízení

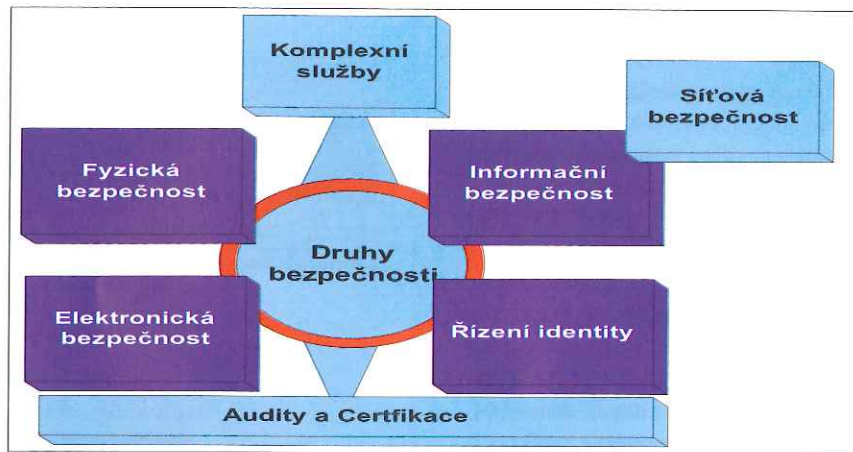
Poslední roky jsme svědky toho, jak firmy jako Apple mění náš svět a způsob, jak se v něm pohybujeme. Mobily iPhone doslova válčují trh a další zařízení jako Apple TV nebo iPad2 už jsou na cestě, aby nám změnily život. Koncept tabletu a dotykových displejů byl akceptován širokým portfoliem výrobců nejen hardwaru, ale i softwaru, a tak i Google a jeho operační systém Android umožňuje přinášet konkurenci a nové inovativní služby do našich životů.

Cloud computing

Představuje nejen vděčné téma pro probíhající konference po celém světě, ale také přináší nový obchodní model ve vztahu zákazník a operátor. V cloudu se jedná principiálně o pokročilou formu outsourcingu, kdy si zákazník namísto vlastní infrastruktury, platformy nebo softwaru kupuje službu, která je typicky provozována v internetu mimo fyzické hranice konkrétní firmy daného zákazníka (IaaS – infrastructure as a service, PaaS – platform as a service, SaaS – software as a service).

Bezpečnost a internet

S internetem padají bariéry trhu i geografická omezení. Toto je velký přínos pro rozvoj podnikání i kvalitu našich životů. Zároveň se ale problematika bezpečnosti v otevřeném světě stává důležitější a také stále složitější. To, že chceme data zároveň sdílet i chránit,



Obr. 2

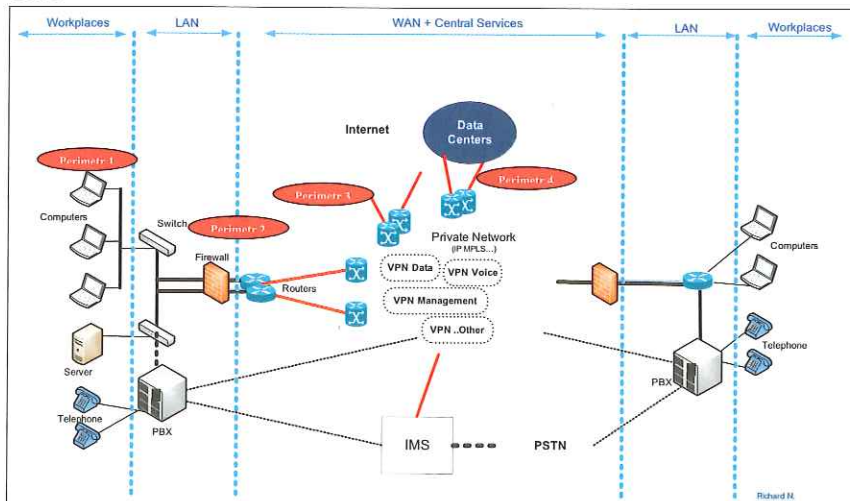
je velká výzva pro IT odborníky, firmy i samotné uživatele.

Oblasti bezpečnosti

Otázku bezpečnosti můžeme rozdělit tematicky do následujících hlavních oblastí (viz obr. 2):

- **Fyzická bezpečnost** – jedná se o zabezpečení fyzického průniku ke chráněným aktivitám. Může se jednat o plot, dveře, závory, ale i ostrahu bezpečnostní agenturou a jejími zaměstnanci.
- **Elektronická bezpečnost** – především jde o jednotlivá elektronická čidla, senzory nebo kamerové systémy. Tato zařízení bývají zpravidla napojena na centrální dohledový systém, který umožňuje jednotlivé vstupy vyhodnocovat, korelovat a následně provést bezpečnostní akci.
- **Řízení identity** – zde se jedná autentizaci, autorizaci a další prostředky prokazování a správy identity většinou na základě přístupového jména, biometrických údajů nebo hesla s následným přidělením práv přístupu

Obr. 3



k jednotlivým bezpečnostně citlivým datům a systémům.

- **Informační bezpečnost** – toto je asi nejširší, ale také nejsložitější oblast, neboť se jedná o jednotlivé informační systémy, databáze, protokoly a další. Přičemž je typické, že komplexní systém informační bezpečnosti často zahrnuje jako subkomponenty jednotlivé prvky výše uvedených oblastí, jako je například elektronická bezpečnost nebo řízení identity. Velkou skupinou informační bezpečnosti, která je svým způsobem považovaná i za samostatnou oblast, je **síťová bezpečnost**, která je navázána na networking a o které budeme mluvit více do hloubky v následujících odstavcích.
- **Komplexní bezpečnostní služby** – zahrnují většinou na zakázku dodané služby, jako jsou bezpečnostní audity či penetrační testy často sloužící pro nastavení bezpečnostních procesů, které jsou později předmětem různých certifikací například v rámci ISO a další. Na trhu je celá řada firem, které se specializují na tyto komplexní služby.

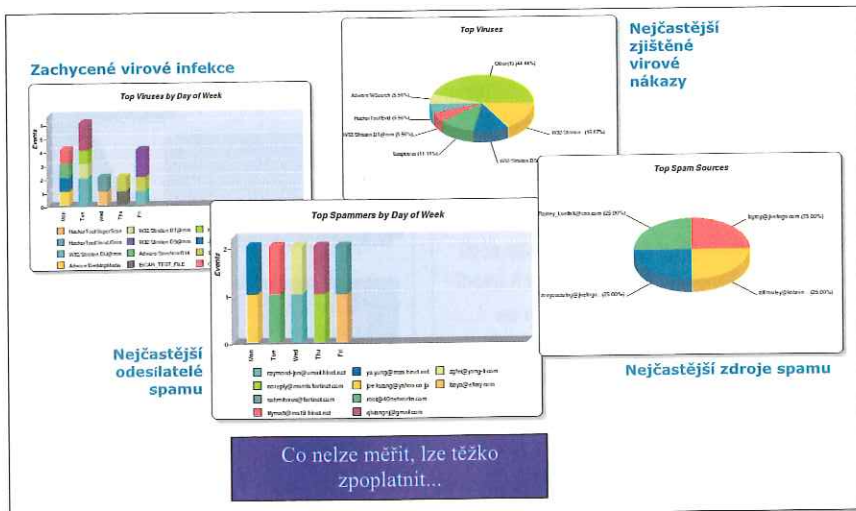
Pro větší názornost bych uvedl příklad zabezpečení datového centra, kde je použit mix všech uvedených oblastí. Datové centrum je objekt, ve kterém se koncentruje ohromné množství technických i finančních aktiv ve formě serverů, datových úložišť, networkingu a běžících aplikací (ERP, CRM, webových serverů atd.).

Pokud chcete vstoupit do sálů datového centra, hned na vstupu vás čeká bezpečnostní agentura, která se stará o přístup do objektu na základě prokázání identity a oprávnění ke vstupu. Tato agentura a ostraha sleduje buď přímo na místě nebo v centrále v rámci PCO (pult centralizované ochrany) stav elektronické bezpečnosti, typicky prostřednictvím kamer a čidel sledujících jednotlivé datové sály. Pokud návštěvník projde přes fyzickou i elektronickou ochranu, a prokáže tedy identitu opravňujícího ke vstupu, dostane se k jednotlivým serverům, které jsou chráněny prostředky informační bezpečnosti proti průniku jak z vnějšku (internet, VPNs, ...), tak zevnitř datového centra.

Síťová bezpečnost – topologie a perimetry

Jak jsme již popsali v odstavcích výše, síťová bezpečnost je podmnožinou bezpečnosti informační a váže se na komunikační infrastrukturu – tedy LAN, WAN a internetové sítě a aktivní prvky v těchto sítích působící. Na obrázku 3 je uvedena topologie komplexní sítě zákazníka, od jeho koncových zařízení přes LAN síť jedné pobočky propojené do VPN s následným přístupem do datového centra a internetu. V červených elipsách je pak na obrázku zachyceno umístění jednotlivých perimetrů bezpečnosti situovaných ve vrstvách do různých bodů sítě. Obecně se dá říci, že pravidlo více vrstev a perimetrů je plošně akceptovaným principem pro kvalitní ochranu proti bezpečnostním rizikům.

Perimetr 1 je umístěn na koncovém zařízení, jakým je typicky počítač nebo server. Zde má dnes již většina zařízení instalováno softwarové bezpečnostní řešení, jako je antivirový program. Perimetr 2 je umístěn na rozhraní lokální LAN sítě a jejího propojení do WAN sítě. Typicky je zde instalováno CPE plnící funkci firewallu (FW), intrusion detection and prevention system (IDS/IPS), případně další bezpečnostní funkce dle konceptu unified threat management (UTM) boxů. Perimetr 3 je umístěn na rozhraní privátní WAN sítě (např. IP MPLS) a jejího přístupu do internetu. Zde může být umístěn podobný UTM CPE box jako v perimetru 2, ideálně s rozšířenější bezpečnostní funkcionalitou



Obr. 4

a také od jiného výrobce. Perimetr 4 je fyzicky situovaný do datového centra, kde může být například součástí demilitarizované zóny (DMZ), která odděluje vnitřní prostředí aplikací od externího světa.

Funkcionality síťové bezpečnosti a jejich dostupnost

Většinu jsme již zmínili, nicméně pro přehlednost uvádím základní funkcionality síťové bezpečnosti:

- firewall,
- intrusion detection and prevention system (IDS/IPS),
- content filtr,
- NAT/PAT,
- antivir,
- antispam,
- VPNs,
- DMZ,
- eventuálně další dle potřeby jednotlivých firem.

Poskytovatel těchto služeb by měl firmám nabízet celou řadu řešení, které bude vždy odpovídat představám požadavkům konkrétního zákazníka. Jedním z obvykle nabízených produktů je řešení pro kompletní potřeby středních firem. Ty mají většinou požadavek na síťovou konektivitu (WAN, LAN, internet) plus bezpečnostní funkce (firewall, content filtr a další) a navíc řešení e-mailového serveru a správu koncových schránek uživatelů e-mailu. Takovéto řešení může být postaveno například na platformě Linux. Samozřejmostí je, že operátor poskytuje toto řešení formou služby a že zařízení je typicky umístěno v datovém centru poskytovatele.

Jinou volbou může být operátorské řešení specializované výhradně na oblast

bezpečnosti, a nemá tedy e-mailový server. Opět platí, že je výhodou, pokud jej operátor provozuje jako službu a snímá tak ze zákazníka starost o provoz a správu těchto zařízení. Každý poskytovatel by měl být dále schopen zákazníkovi poskytnout formou služby individuální řešení na míru.

V případě řešení bezpečnosti je vždy důležitá i analýza. Nabízený produkt by měl být schopen graficky prezentovat výstupy z jednotlivých sond. Obrázek 4 zachycuje příklad takového výstupu v produktu GTS Managed Security.

Závěr

Bezpečnost je důležitá a složitá věc, která zasahuje do našich každodenních soukromých i pracovních životů. Kvůli své složitosti pak zejména informační a síťová bezpečnost vyžaduje, aby se jí chopili odborníci, kteří mají k této problematice blízko. Problematiku ICT je nutné vnímat vždy komplexně, i proto by měl zákazník mít na své straně zkušeného poskytovatele těchto služeb. ■



Autor je ředitelem pro Managed Services ve společnosti GTS Czech.