6. 4. 2007

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Chraňte svoje data

V elektronické podobě ukládáme stále větší množství dokumentů a informací a je tedy na místě zabývat se ochranou dat a privátních datových sítí. Bez přístupu k veřejné datové síti INTERNET si naši práci už nedokážeme ani představit. Na INTERNETU získáváme informace a činíme dostupné ve vymezené míře i informace své, přes INTERNET obsluhujeme svoje účty u bankovních domů a komunikujeme. Komunikace přes veřejnou datovou síť je vlastně předávání informací mezi účastníky sítě.

Tato komunikace probíhá přes jednotlivé porty příslušné technologie, kterých je k dispozici více jak 65 000 a každá jednotlivá služba využívá svůj protokol a svoje porty. Tyto porty jsou pak jakousi vstupní branou do počítače nebo serveru. Útoky přes veřejnou datovou síť se soustředí na nalezení otevřeného portu tzv. skenováním portů. Útočníci pro skenovaní portů využívají celé robotické infrastruktury a skenují libovolné i vybrané účastníky kde je zaznamenán provoz a hledají bezpečnostní díry a otevřené porty. Zde je tedy i odpověď na otázku proč zrovna já bych mněl být napaden. Nebezpečí napadení je tedy vystaven každý kdo je do veřejné datové sítě připojen bez rodílu. INTERNET je veřejná datová síť to znamená že má k ní přístup každý ať má dobré či špatné úmysly. Stále vzrůstající počet nekalé činnosti, trv. Počítačové kriminality, v rámci veřejné datové sítě INTERNET nás nutí přemýšlet co udělat pro to, aby nebyly vykrádány, nebo ničeny naše chráněné databáze.

Obecně vzato své byty a domy též chráníme stále lepšími zámkovými systémy a totéž platí o ochraně dat u počítačů, serverů umístěných v privátních datových sítích, přičemž množina osob schopná ohrozit váš dům či byt je nesrovnatelně menší s množinou, která je schopna ohrozit vaše data. Samozřejmě, že ochrana dat něco stojí a je třeba tedy pečlivě vážit jaké hodnoty ochraňuji. Ze zkušenosti mohu potvrdit, že škody po napadení mají mnohdy fatální dopad na fungování poškozeného. Určitě je nutné vážit poměr nákladů za ochranu svých dat k jejich ceně pořízení, ale i ze platí že lepší prevence oproti problémovému stavu, než jeho následné řešení, protože náklady na následné řešení kolize jsou téměř vždy nesrovnatelně vyšší, o ztrátě dobrého jména v případě že jsou zcizena nebo poškozena i cizí chráněná data ani nemluvě.

Co tedy udělat pro to, abychom byli chráněni. Především je nutností používat průběžně aktualizovaný antivirový program a další security software i nastavení zabezpečení operačního systému přiměřeně topologii a vlastnostem privátní datové sítě. Považuji rovněž za nutné dbát zásad bezpečného chování při surfingu a obsluze pošty i aplikací.

Vlastní ochranu před neoprávněným průnikem do vaší privátní datové sítě, tedy k vašemu datovému úložišti, serveru či počítači, z veřejné datové sítě zabezpečuje firewall.

Firewall je v podstatě jakýmsi zámkem k vašim datům a datovým sítím. Existují firewally softwarové instalované na vašich počítačích a serverech sdílející jednotný operační systém i hardwarové, samostatná zařízení určena k tomuto jedinému účelu vybaveny specifickým operačním systémem. Tato zařízení nejen blokují nepovolenou komunikaci, ale i kontrolují povolený provoz. Vždy doporučujeme při ochraně dat kombinovat různé operační systémy a ochranu v různých úrovních, aby bylo učiněno přiměřené maximum možného k ochraně. Moderní hardwarové firewally určené k ochraně datových sítí, umožňují mimo základních funkcí i využití dalších služeb při zabezpečené

komunikaci. Tato zařízení prošla svým vývojem a jsou dnes na trhu hardwarové firewally plnící celé spektrum požadovaných funkcí a v dostupných cenách. Faktem však zůstává že tato zařízení na rozdíl od personálních softwarových firewallů vyžadují odbornou obsluhu a to samozřejmě něco stojí. Faktem též zůstává, že hodnoty, celou privátní datovou síť, které chráníme hardwarovýcm firewalem jsou nepoměrně vyšší. Mohu tedy jen doporučit touto problematikou se zabývat a učinit to přiměřené maximum možného k ochraně dat, protože zítra již může být pozdě……

Petr Jelínek
autor je výkonným ředitelem společnosti Daxta Communications a.s.

Další články:

- Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022
- Základní právní aspekty smart kontraktů - část 2.
- Úvod do práva smart kontraktů - část 1.
- Streamování počítačových her z pohledu práva
- Právní změny v oblasti e-commerce: přísnější pravidla pro objednávková „tlačítka“ v e-shopech
- QUO vadis 2019?
- Současná evropská rozhodovací praxe ve věcech omezovaní internetového prodeje a konec geo-blockingu
- Režim Safe Harbour v rámci poskytování hostingových služeb
- Live streaming programů po internetu a povinnost šíření (must carry) ve světle judikatury Soudního dvora Evropské unie
- Poučovací povinnost advokáta a odpovědnost za škodu při výkonu advokacie
- Novela zákona o ochranných známkách