

## Bezpečnost IT je problém, je imunitní systém řešení? (I.)

00:01 | [Reklama](#)

[Články](#) - [Sítě](#) - [Bezpečnost IT je problém, je imunitní systém řešení? \(I.\)](#)

---

Malware je problém, imunitní systém řešení. Silný imunitní systém to není jen dobrý základ pro vlastní zdraví, ale i zdraví firmy či úřadu. Pojdme se podívat na první účinný imunitní systém v oblasti IT bezpečnosti pro malé i velké organizace.

---

Můžete namítnout: „Bezpečnost je jen marketingová bublina komerčních společností, aby vytáhly co nejvíce peněz z klientů.“ nebo naopak „Nikdy nemůžeme být dobře ochráněni, nejlépe je všechno zakázat!“, což jsou krajní meze známého faktu, bezpečnost IT je špatně měřitelná a rizika v poslední době stále hůře identifikovatelná. Naproti tomu snahy útočníků jednoznačně vedou k cíleným a skrytým útokům a k finančnímu profitu.



Obrázek dokazuje, že od roku 2007 se změnilo mnohé:

- stále více je jasné, že lokální ochrany nestačí, že systémy si musí vyměňovat informace o útočnicích a agregovat tak zkušenosti nasbírané po celém světě. Mění se snaha z úrovně identifikace útoku na úroveň identifikace útočníků (známou z fyzického světa)
- firewalling na úrovni povolování portů a aplikační kontrola na základě signatur jsou jen základem, nikoliv bezpečnostním prvkem ochraňujícím kritická aktiva.
- již dávno neplatí, co je šifrované to je bezpečné, ale naopak, co je šifrované, to je nebezpečné.
- uživatelé vyžadují přístupné všechny služby internetu a nestarají se o bezpečnost. Web proxy a web cache musí nabízet bezpečnostní funkce a účinně řídit přístupy zaměstnanců.
- emailová bezpečnost to není jen spam, je to ochrana firemních web mailů (OWA, LNWA), ochrana mail serverů a smtp serverů v DMZ a vnitřní síti a ochrana samotné email komunikace šifrováním
- bezpečnost musíme řešit nejen na perimetru ale i uvnitř sítě pomocí systémů ochran před únikem informací (DLP), komplexních řešení managementu identit, šifrováním citlivých dat
- datová centra potřebují nejen dostupnost, ale i propustnost a bezpečnost. Kritická je schopnost detekce a prevence všech narušení při zajištění propustnosti na úrovni gigabitových nebo 10Gbps páteří a zajištění virtuálního záplatování.
- Důležitá je i vynutitelnost bezpečnostních politik, zajištění přístupových práv nejen uživatelů ale i systémů

Jak to tedy je? Pokud klapky z našich očí sejmeme, reálně vidíme, že hrozba existuje a také chápeme, že informatika by nám měla co nejlépe sloužit a nikoliv nás při práci omezovat a brzdit.

Pojďme se tedy podívat na účinné ochrany proti novým způsobům útoků a jaké úspory může, pro IT a celou organizaci, přinést nový komplexní imunitní systém McAfee

spojující Network Security a System Security. **McAfee Inc. po úspěšných akvizicích v uplynulých letech dnes představuje totiž největšího světového hráče v oblasti IT bezpečnosti s nabídkou komplexních ochran od desktopů, přes ochrany před únikem informací, IPS až po perimetr. K dispozici je tak skutečný imunitní systém.** Definujme si požadavky na moderní bezpečnostní koncepci organizace tak, aby poskytovaná imunita byla skutečně účinná. Začneme od perimetru.

**1. Identifikace útočníků je účinnější než snaha postihnout každý útok.** Ano opravdu, i v Internetu je identifikace útočníků možná. McAfee provozuje nejkomplexnější systém globálních reputací [TrustedSource.org](http://TrustedSource.org), disponuje detekční technologií Artemis a jako bezpečnostní specialista, provozuje výzkumné laboratoře AVERT s více než 300 zaměstnanci se středisky na všech kontinentech.

**2. Firewally - Účinné už není provoz zkontrolovat a propustit, ale zprostředkovat jeho předání bezpečnostními proxy.** Opět na současné scéně Enterprise fw unikátní přístup reflektující nové hrozby skryté v aktivních kódech a cílený způsob šíření. McAfee Enterprise firewall ([Sidewinder](#)) pracuje na principu aplikačních proxy bran. Díky této technologii neexistuje žádné přímé spojení mezi nedůvěryhodným prostředím (Internetem, extraktem, apod) a chráněnými segmenty sítí (DMZ, interní servery, datacentra, aj.). Proxy fw vždy terminuje provoz z neznáma, zkontroluje obsah, zda obsahuje pouze co má a sama proxy (interní proxy) naváže komunikaci dovnitř na důvěryhodný segment. Navíc je vše propojeno na systémy globálních reputací a výzkumné laboratoře AVERT, tak aby postihlo nejnovější typy útoků a disponuje i možností omezit pravidla dle politik GeoIP. Bezpečnostní brána v [7 modelových řadách](#) navíc dokáže ochránit kritické služby infrastruktury jako je DNS, FTP a SMTP tím, že na vlastní zabezpečené platformě provozuje tyto servery.

**3. WEB. Už dávno neplatí co je šifrované je bezpečné.** Webové proxy i firewally musí umožnit detekci nežádoucích kódů i v šifrovaném provozu. Uživatelé musí mít bezpečný přístup k potřebným zdrojům internetu, organizace ale musí zůstat chráněna jak před zavlečením nových hrozeb z webového brouzdání tak před únikem informací. Všechny tyto klíčové komponenty webové bezpečnostní brány poskytuje McAfee Web Gateway ([Webwasher](#))

- PROXY – pro příchozí a odchozí web provoz uživatelů
- Cache provázaná s bezpečností. Stále žádaná funkcionality webové cache musí být připravena pro prostředí dynamicky generovaného obsahu webu a doplněna o metody kontroly uloženého obsahu při aktualizaci signatur malware a virů aniž by byl přítom snížen výkon či znovu načítána celá cache.
- AntiMalware – skutečná kontrola aktivních kódů a skriptů v rámci http i https. Analýza potencionálního dopadu.
- Anti-Virus - tradiční modul pro detekci škodlivých kódů na základě aktualizace signatur virů a spywarů integrovaný pro vysoký výkon do web proxy.
- SSL Scanner, který umožňuje kontrolování šifrované komunikace uživatelů se zdroji na Internetu. Jen tak lze zabránit průniku heckerů, virů a dalšího škodlivého obsahu skrytého v SSL (https) provozu a ve spojení s DLP modulem zabraňuje i úniku citlivých informací přes tento šifrovaný provoz.
- URL filtrace. Automatizované řízení přístupu zaměstnanců ke zdrojům internetu

zajišťuje vyšší produktivitu i menší čerpání internetového pásma.

- Napojení na zmíněný Systém globálních reputací TrustedSource.org.
- [4 modelové řady](#) až s 4x300GB SAS pro caching

**4. Emailová bezpečnost to není jen spam**, je to ochrana firemních web mailů (OWA, LNWA), ochrana mail serverů a smtp serverů v DMZ a vnitřní síti a ochrana samotné email komunikace šifrováním. McAfee Email Gateway ([IronMail](#)) nabízí tyto ochrany pro kritický emailový provoz:

- **Anti-Spam & AntiPhishing** – přesná detekce díky kombinaci 12 metod
- **Dynamic Spam Classifier** – aktualizace algoritmů každých 20 minut
- **LDAP connection control**
- **Anti-virus & spyware chránící okno zranitelnosti**
- **Email IPS & Email firewall** pro ochranu email server a web mail portal v jednom řešení
- **TrustedSource** ochrana systémem globálních reputací
- **Funkce IMAGE analysis** – ochrana před obrázkovým spammem
- **Web Mail ochrany, vlastní proxy pro (OWA, LNWA)**
- **DLP – Ochrana před únikem informací** - předdefinované výrazy a validační algoritmy
- **Flexibilní šifrování B2B, B2C** + gateway to gateway v ceně řešení, volitelné gateway to klient šifrování s technologií push a pull pro klienty bez dešifrovacích programů

Na perimetru dnes článek o imunitním systému McAfee ukončíme. Bezpečnost musíme řešit ale i uvnitř sítě. V příštím dílu se tedy podíváme na řešení ochrany před únikem informací (DLP), systémy prevence narušení a managementu zranitelností, ale také na koncové stanice a vynutitelnost bezpečnostních politik organizace.

Článek pro vás připravili odborníci nadnárodní společnosti COMGUARD a.s. distributora IT Security řešení pro ČR, SR a UA. COMGUARD nabízí partnerům prodejní model Value Added Distribuce s plnou odbornou podporou od certifikovaných odborníků. Prodej distribuovaných řešení je realizován přes síť partnerů v ČR, SR a Ukrajině včetně 1st level supportu pro partnery a 2nd level supportu pro koncové zákazníky v lokálním jazyce a celé škály odborných služeb včetně provozu Autorizovaného školícího střediska McAfee.

## **Příště: Bezpečnost IT je problém, je imunitní systém řešení? (II.)**

**5. Bezpečnost** musíme řešit nejen na perimetru ale i uvnitř sítě pomocí systémů ochrany před únikem informací (DLP), systémy prevence narušení a managementu zranitelností, ale také na koncových stanicích, kde je důležitá vynutitelnost bezpečnostních politik organizace a snadná centrální správa.

**6. Datová centra** potřebují nejen dostupnost, ale i propustnost a bezpečnost. Kritická je schopnost detekce a prevence všech narušení při zajištění propustnosti na úrovni gigabitových nebo 10Gbps páteří a zajištění virtuálního záplatování. Výrobci software jen velmi zřídka stíhají reakce na bezpečnostní slabiny a vzájemná nekompatibilita provozovaných systémů a existujících patchů zranitelnosti jen nahrává. Virtuální záplatování zde pak pomáhá nejen bezpečnosti, ale i dostupnosti a eliminací šíření útoků i propustnosti.

**7. Centrální správa** musí být skutečně centrální a obsahovat i centrální reporting a monitoring, protože jen tak lze vyhodnocovat bezpečnostní události a kontinuálně upravovat nastavenou bezpečnostní politiku.

---

### **Další články z této rubriky**

Bezpečnost IT je problém, je imunitní systém řešení? (I.)

BGP - dynamické routování - 1 (úvod, administrativa)

Vyčerpání IPv4 adres: Co potom?

Internet se mění: Jak čelit vyčerpání IPv4 adres

Nagios + Centreon + MySQL - moduly pro Centreon

---

ISSN 1214-1267, (c) 1999-2007 [Stickfish s.r.o.](#)