Grow. With the leader.

Arrow ECS, a.s.

Bezpečnost provozu podnikových aplikací

Pohled na současnou situaci

- **Úzká návaznost na provoz a business**
  - Silný tlak na vývoj a včasné nasazení do provozu
- **Vzrůstající trend ve vystavování aplikací do prostředí webu**
- **Požadavky regulativů – PCI DSS**
- **Bezpečnost je řešena „až na posledním místě“**

Funkční aplikace ≠ Kvalitní aplikace

Jaké to má dopady?

- **Zvýšení nároků na aplikační vývoj z pohledu zajištění bezpečnosti**
- **Odhalení bezpečnostních slabin aplikace během auditu**
- **Úspěšně realizované útoky zvenčí**
- **Zpoždění při nasazení aplikace díky náročným bezpečnostním testům**

Trendy v zajištění aplikační bezpečnosti

- **Integrita a důvěrnost**
  - Zajistit ochranu kritických webových aplikací
  - Snížit nároky na aplikační vývoj
  - Zajištění souladu s bezpečnostními regulativy
- **Optimalizace dostupnosti**
  - Snadně a systémově pomocí infrastruktury zvýšit dostupnost služeb poskytovaných servery
  - Posunutí hranic výkonnosti systémů (serverů) a sítí
  - Rychlejší odezva aplikačních služeb vůči uživateli

Optimální strategie pro ochranu WEB aplikací

- Ochrana pouze proti známým zranitelnostem
- Obtížné vynutit v případě subdodávky kódu
- Kód je psán ve spěchu pod tlakem business požadavku

- Kontrola prováděna v periodických cyklech
- Kontrola pouze na známé útoky

- Nepřetržitá ochrana v režimu 24 x 7
- Okamžitá ochrana proti novým typům útoků
- Efektivní zajištění provozní bezpečnosti více aplikací

Představení webového aplikačního firewallu

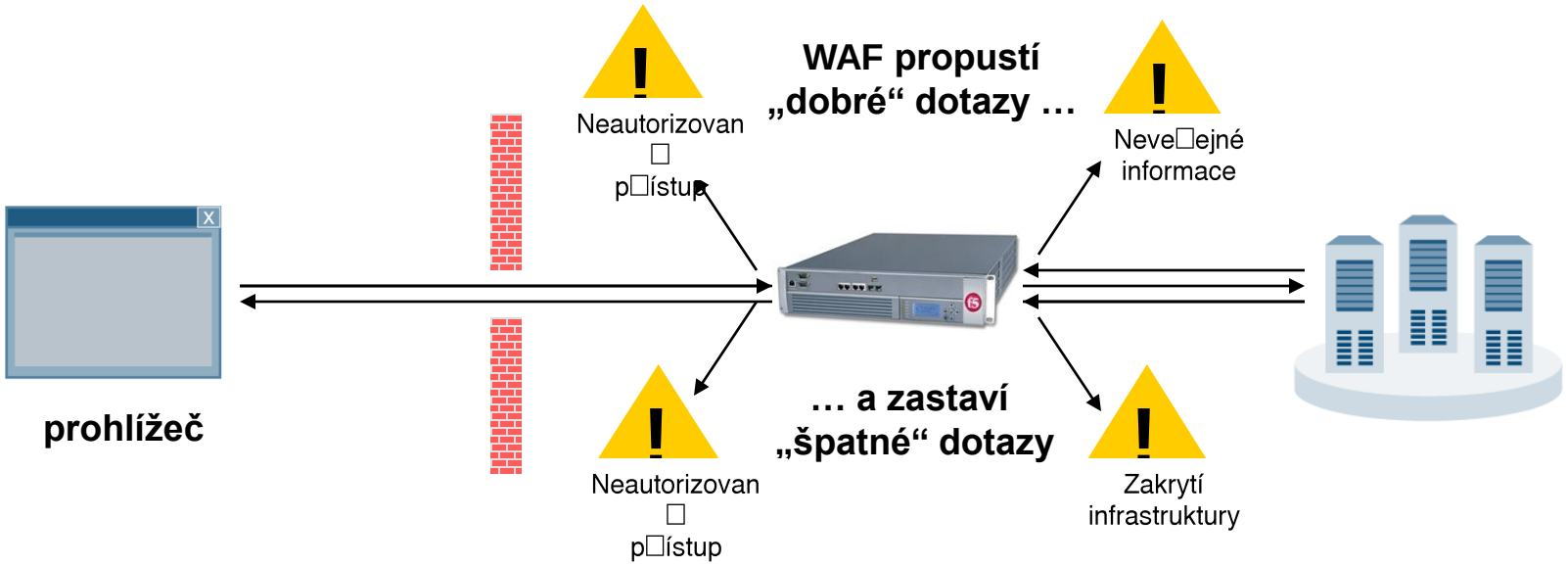
- **Pokrytí útoků, které klasické FW a IDP neřeší**
- ochrana/prevence HTTP provozu a logování
- rychlé řešení existujících chyb aplikace – workaround řešení
- „hardening“ webových aplikací

Jaké typy útoků neřeší tradiční security prvky?

	Application Firewall	*Network Firewall*	*IPS*
Known Web Worms	✓	Present	Present
Unknown Web Worms	✓	Present	Present
Known Web Vulnerabilities	✓	Present	Present
Unknown Web Vulnerabilities	✓	Present	Present
Illegal Access to Web-server files	✓	Present	Present
Forceful Browsing	✓	Present	Present
File/Directory Enumerations	✓	Present	Present
Buffer Overflow	✓	Present	Present
Cross-Site Scripting	✓	Present	Present
SQL/OS Injection	✓	Present	Present
Cookie Poisoning	✓	X	X
Hidden-Field Manipulation	✓	X	X
Parameter Tampering	✓	X	X

Princip ochrany pomocí WAF

Bezpečnost je řešena „až na posledním místě“



- Obousměrná inspekce:
  - Inbound: ochrana proti obecným i cíleným útokům
  - Outbound: „vyčištění“ obsahu a skrývání infrastruktury
- Držení aplikačního obsahu a kontextu
- Vysoký výkon, dostupnost, bezpečnost, nízké zpoždění
- Plná proxy, hloubková inspekce, založeno na politikách
- Pozitivní i negativní bezpečnostní model
- Centrální řídící bod aplikační bezpečnosti

Řešení od společnosti F5 Networks

… **komplexní řešení odstraňující nedostatky v provozu aplikací po síti, a tím poskytující**

Efektivní, dostupný a bezpečný provoz moderních podnikových aplikací

Řešení od společnosti F5 Networks

- **Víceúrovňové řešení ochrany provozu aplikace**
  - Vrstva L2-L4/TMOS
  - Ochrana protokolů HTTP, SMTP a FTP
  - Ochrana aplikační logiky (WAF)
    - Negative security model
    - Positive security model
  - Ochrana XML služeb

- **Integrace funkcí pro optimalizaci provozu aplikace**
  - Load Balancing
  - SSL offloading
  - Caching/Komprese
  - Optimalizace protokolu
  - IPv6
  - RateShaping

Děkuji za pozornost a přeji hezký zbytek dne

Jiří Petrásek
System Engineer
jiri.petrsek@arrowecs.cz

Arrow ECS, a.s.
Ostrava
Tvorkovských 5
709 00 Ostrava - Mariánské Hory
tel.: +420 597 488 811
fax: +420 596 622 486

Praha
Nagano Office and Technology Park,
Nagano III
U nákladového nádraží 10
130 00 Praha 3
tel: +420 266 109 211
fax: +420 283 840 236

www.soft-tronik.cz