

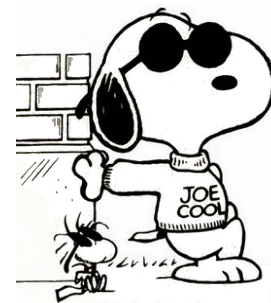
IDS, IPS bezpečnost



Lukáš Jakubík

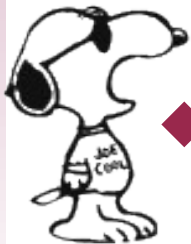
Narušení bezpečnosti

- ◆ **bezpečnost není stav, ale proces**
- ◆ **rozlišuje se mezi útokem a narušením**
 - ◆ **útokem** se myslí pokus o narušení
 - ◆ kdežto **narušení** je aktivní posloupnost odpovídajících událostí, které se záměrně snaží uškodit takovou měrou, že **systém se stává nepoužitelným**
- ◆ *firewall lze srovnat se zamčenými dveřmi*
- ◆ *IDS s alarmním systémem*
- ◆ *a IPS s hlídacími psy*
- ◆ *Jak ochrání alarm náš majetek?*



IDS – systém detekce narušení

- ◆ **IDS** (intrusion detection system) je systém, sada nástrojů, metod a zdrojů jak identifikovat a hlásit nežádoucí síťové aktivity
- ◆ nedetekuje samotné narušení, **pouze hlásí narušující aktivity**, nezabrání narušení, jen nás varuje
- ◆ není samostatné ochranné opatření, potřebuje další součásti k ochraně
- ◆ *I ten sebelepší alarm v autě vyžaduje, aby někdo vstal z postele a podíval se z okna, proč houká.*
- ◆ *Jak na pozorovanou událost pravděpodobně vedoucí k odcizení auta vlastně reagovat?*



IPS – systém prevence narušení

- ◆ **IPS** (intrusion prevention system) je monitorovací systém v síti, který **reaguje na narušující události podle předdefinovaných pravidel**
- ◆ IPS někdo považuje za nástupce IDS, jiní jako nutný doplněk k detektorům IDS
- ◆ IPS musí dokázat prosadit zabezpečení, reagovat na narušení
- ◆ *Rozmístění alarmů a senzorů na všechny okna, dveře, nákup bojových psů, je zbytečný, když je garáž otevřena a psy ze své ohrady ani nevyběhnou.*



IDS a IPS v praxi

- ◆ jsou nesrovnatelně efektivnější než člověk, avšak jen reagují na narušení, nedokáží průniku předejít
- ◆ všechno se zaznamenává
- ◆ nenahrazují člověka, odborníka, který je nastavuje a narušení vyhodnocuje
- ◆ principiálně se detekce dělá pomocí
 - ◆ databáze vzorků útoků, známých exploitů
 - ◆ statistického vyhodnocování
 - ◆ stavové, behaviorální analýzy
- ◆ příkladem IDS+IPS je **Snort**



Zdroje

- ◆ ENDORF, Carl – SCHULTZ, Eugene – MELLANDER, Jim. Detekce a prevence počítačového útoku. Praha: Grada Publishing 2005. ISBN 80-247-1035-8
- ◆ Wikipedia contributors. *Intrusion detection system* [Internet]. Wikipedia, The Free Encyclopedia; 2011-01-15, 18:32 UTC [cit. 2015-05-18]. http://en.wikipedia.org/w/index.php?title=Intrusion_detection_system&oldid=408058101.
- ◆ Obrázky převzaty z
 - ◆ http://www.astickerheaven4u.com/catalog/SnoopySleepingOnDoghouse_thumb.jpg
 - ◆ http://1.bp.blogspot.com/_mfvHDMw0Zlw/SwbZikviKvI/AAAAAAAAAK4/eIYw3EiOWTk/s320/snoopy-is-joe-cool-peanuts-254005_1024_768.jpg
 - ◆ <http://kruse-jensen.com/html/video2.html>
 - ◆ <http://www.fanpop.com/spots/peanuts/>

