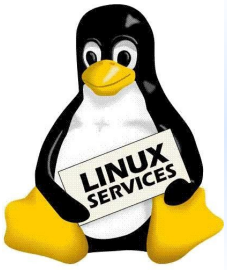


Linux Services

PORTFOLIO POSKYTOVANÝCH SLUŽEB

V OBLASTI KYBERNETICKÉ BEZPEČNOSTI


Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz

Obsah

Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz


Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz

Představení společnosti

Jsme freelancingová společnost složená ze samostatných a nezávislých ICT odborníků se sídlem v Praze. Máme více než dvacetiletou historii.

Nabízíme řešení v oblasti informačních systémů a zabezpečení, která jsou zcela nezávislá na dodavatelích, odpovídající zákonným normám ČR a EU, na bázi otevřených standardů a platných technických norem. Zabýváme se především analýzami, návrhem, dodávkou, instalací, konfigurací a servisem informačních systémů.

Naším cílem je poskytovat odbornou pomoc a podporu našim klientům v oblasti IT, navrhovat jim kvalitní a cenově dostupná výhodná řešení.

Při dodávkách hardware nabízíme výhradně špičkové a odzkoušené komponenty.

Jsme registrováni v Živnostenském rejstříku (http://www.rzp.cz) a v Obchodním rejstříku (http://www.justice.cz) pod IČ 12627721.

Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz

Nabízíme

- služby v oblasti zajištění kybernetické bezpečnosti dle metodik a standardů národních bezpečnostních autorit zemí EU (NBÚ, BSI), administraci a servis Informačních systémů
- poradenství ohledně provozování a bezpečnosti IS
- vypracování metodiky pro správu informačního systému (IS), sestavení požadavků na funkčnost IS, sestavení podkladů pro výběrová řízení na jednotlivé komponenty IS
- školení administrátorů IS s ohledem na platnou legislativu, doporučení národních autorit, platné standardy, ukázku legislativy členských zemí EU
- security zařízení IS (IDS/IPS, VPN Gateway, log collector, ticket system), která jsou na bázi open source

Správa informačních systémů

Provádíme servis a administraci jak celých informačních systémů, tak jejich vybraných částí.

Zákazníkům doporučujeme řešení na bázi obchodního modelu open-source, která zachovávají široké možnosti použití i spolehlivost, avšak umožňují ušetřit výrazné množství finančních prostředků a to jak při pořízení, tak při provozu softwarového vybavení.

Rádi bychom zdůraznili nabídku servisu s vedením on-line servisního deníku, do kterého může zákazník kdykoli nahlížet a zapisovat. To Vám umožňuje mít přesný přehled o tom, co se děje s Vašimi zařízeními a jaké změny a servisní zásahy jsme na nich prováděli.

Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz

Kybernetická bezpečnost

Jedná se o komplexní soubor povinností, zásad a pravidel, jež jsou závazná pro každého uživatele či provozovatele informačních technologií a systémů.

Gestorem oblasti kybernetické bezpečnosti je v ČR Národní bezpečnostní úřad (známý též pod zkratkou NBÚ). Stalo se tak usnesením vlády ze dne 19. října 2011 číslo 780 o ustanovení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. NBÚ následně vypracoval "Věcný záměr zákona o kybernetické bezpečnosti", jež vláda schválila v červnu 2012.

V této souvislosti je dobré připomenout, že i Trestní zákoník zná trestné činy související s neoprávněnými přístupy do informačních systémů, konkrétně § 230 nazvaný "Neoprávněný přístup k počítačovému systému a nosiči informací".

Legislativa

V současné době se jedná o již výše zmíněný "Věcný záměr zákona o kybernetické bezpečnosti". Paragrafové znění zákona by mělo být dostupné veřejnosti od léta 2013.

Metodika

Dle prohlášení ředitele NCKB (Národní centrum kybernetické bezpečnosti, odbor NBÚ), NCKB do vlastního zákona zapracuje odkazy na související normy a metodiky (například ISO 27032). Dále bude respektovat metodiky relevantní (například metodiky národních autorit členských zemí, NBÚ – Česká národní bezpečnostní autorita, BSI – Německá národní bezpečnostní autorita, EU Council – poradní orgán EU, NIST - National Institute of Standards and Technology USA atp.).

Z již výše zmíněné řady ISO 27000 pak připomínáme následující ISO normy:

- ISO/IEC 27031:2011 (Business Continuity)
- ISO/IEC 27032 (Cybersecurity)
- ISO/IEC 27033 (Network Security)
- ISO/IEC 27034 (Application Security)
- ISO/IEC 27035:2011 (Incident Management)
- ISO/IEC 27036 (Supplier Relationships)
- ISO/IEC 27037 (Guidelines for identification, collection, acquisition and preservation of digital evidence)
- ISO/IEC 27039 (IDS)
- ISO/IEC 27040 (Storage Security)
- ISO/IEC 24762:2008 (Disaster Recovery)

Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz

Implementační scénáře

Vycházejí z již výše uvedené metodiky a ISO standardů. Každý scénář by měl zahrnovat:

- Topologické schema systému
- IP adresní plán
- Rozpis všech zařízení (rozpis HW)
- Komentované konfigurační soubory (parametry, jejich zdůvodnění)
- Zdůvodnění použitých technologií, služeb, aplikací, operačních systémů
- Zdůvodnění použitého HW
- Blokové a procesní schema systému

Popis jednotlivých security zařízení

Jedná se o zařízení potřebná pro vyhodnocování provozu informačního systému a dále pro zefektivnění správy celého systému. Toto vyhodnocování má pravidelné intervaly, provádí jej administrátor, který jednotlivá vyhodnocení zapisuje do provozního deníku. Kontrolu vyhodnocování provádí security officer, který může hodnocení doplnit (bezpečnostní incidenty, jejich vyhodnocení a náprava, doporučení apod.).

Jako podklady pro vyhodnocování slouží zejména:

- logy jednotlivých zařízení a aplikací
- hlášení o bezpečnostních incidentech
- výstupy od dodavatelů
- hlášení od uživatelů

Zařízení pro sběr a vyhodnocování logů (Log collector)

Jedná se o samostatné zařízení určené pro sběr a vyhodnocování logů (ve formátu syslog), které je součástí určité DMZ zóny nebo vnitřní LAN sítě. Vlastní vyhodnocování logů pak provádí automat na základě předem daných šablon. Obsluha má samozřejmě možnost se k jednotlivým logům vracet a zpětně je podrobně analyzovat. Vlastní rozesílání upozornění na „podezřelé“ logy se děje pomocí e-mailu nebo SMS. Celé zařízení je možné provozovat na bázi open source a to s nekomerční licencí GPL.

Ukázka výstupu z automatického vyhodnocování logů na log collectoru:

```
Security Alerts
=-=-=-=-=-=-=-=-=
Nov 29 01:02:21 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:173.75.247.118) detected.
Nov 29 01:02:30 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:173.75.247.118) detected.
Nov 29 01:02:47 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:93.205.134.211) detected.
Nov 29 01:02:50 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:93.205.134.211) detected.
Nov 29 01:02:56 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:93.205.134.211) detected.
Nov 29 01:03:41 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:88.161.175.163) detected.
Nov 29 01:03:45 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:88.161.175.163) detected.
Nov 29 01:04:18 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:79.193.29.170) detected.
Nov 29 01:04:20 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:79.193.29.170) detected.
Nov 29 01:04:26 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:79.193.29.170) detected.
Nov 29 01:04:48 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:77.3.157.72) detected.
Nov 29 01:04:51 192.168.1.1 PING-FLOODING flooding attack from WAN (ip:77.3.157.72) detected.
```

IDS/IPS

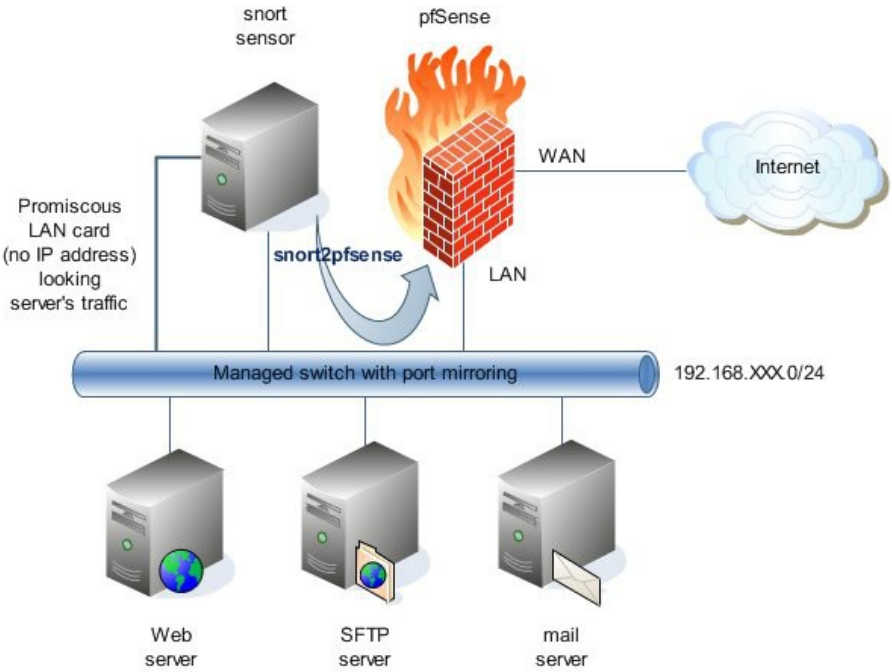
IDS/IPS (Intrusion Detection System /Intrusion Prevention System) je systém detekce a prevence síťových útoků. Může být použit pro ochranu konkrétního počítače či nasazen na internetové bráně a chránit tak celou lokální síť, která je přes tuto bránu připojena k Internetu. Analyzuje veškerou síťovou komunikaci, v níž rozpoznává a blokuje známé typy útoků (například port scanning, DoS aj.) a rovněž analyzuje určité podezřelé aktivity, čímž může zabránit i dosud neznámým typům útoků.

Intrusion Detection System (systém pro odhalení průniku) je obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity.

Intrusion Prevention Systems (systémy pro prevenci průniku) jsou zařízení přímo podporující zabezpečení kybernetického prostoru. Hlavní funkcí je identifikace škodlivé činnosti, zaznamenávání informací o jejím průběhu, její nahlašování (např. odesláním logů na log collector), případně blokování. Hlavní rozdíl oproti IDS systémům je ten, že IPS je zařazen přímo do síťové cesty. Může provádět vyvolání poplachu, filtrování škodlivých paketů, násilné resetování spojení či blokování provozu z podezřelé IP adresy. Všechny tyto úkony často provádí ve spolupráci s firewallem. Také umí defragmentovat proudy paketů, předcházet problémům s řazením TCP paketů a čistit nežádoucí přenos včetně nastavení síťové vrstvy.

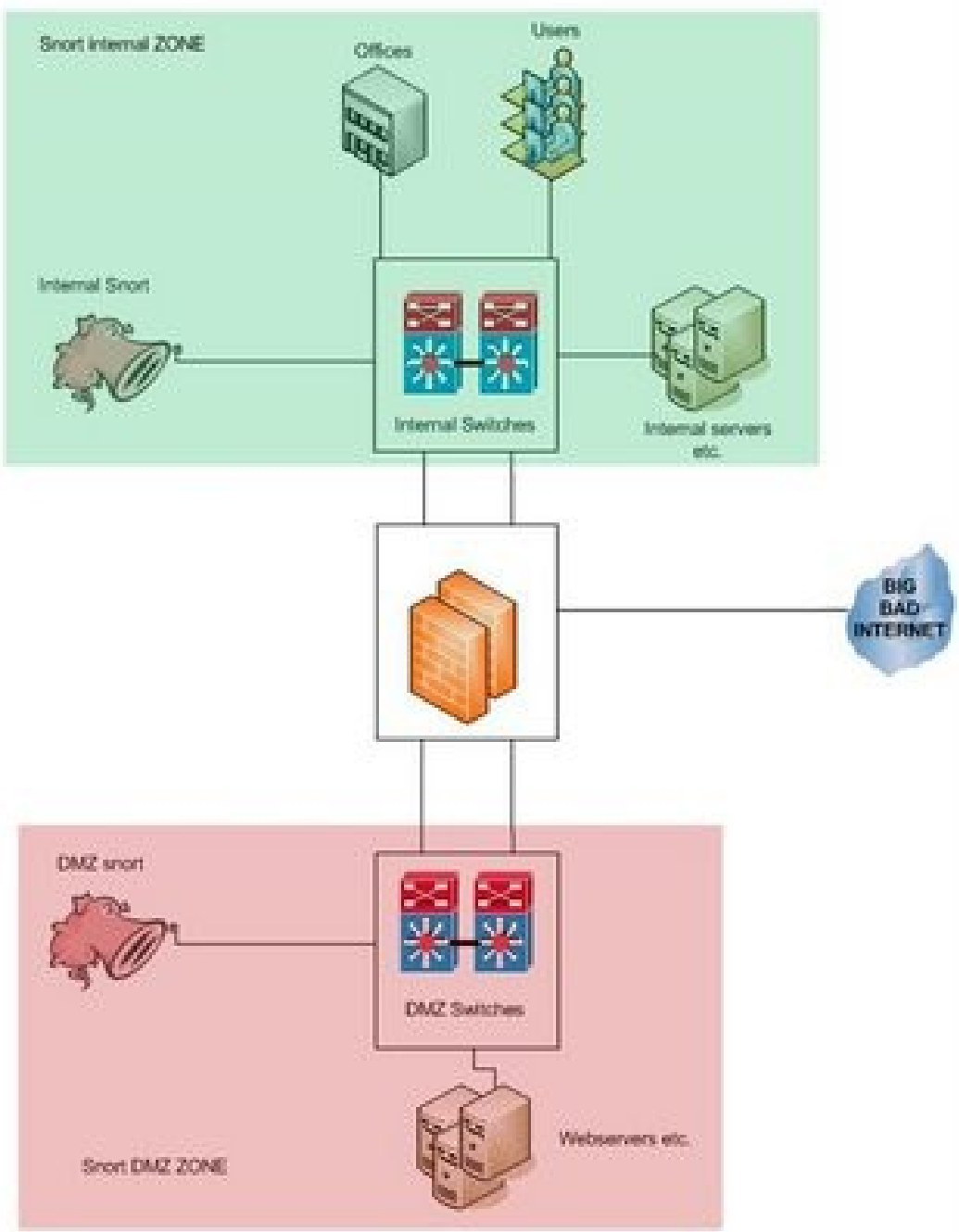
Celé toto zařízení je samozřejmě možné postavit na bázi open source. Zde konkrétně se jedná o programové vybavení zvané SNORT (www.snort.org), které využívají i národní bezpečnostní autority EU (např. BSI – německá národní bezpečnostní autorita, odkaz zde a zde).

Jedno z možných zapojení snort senzoru:



Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz

Jiné zapojení snort senzorů:



Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz

Ticket system

Tento systém je určen pro zefektivnění správy a provozu informačního systému. Uživatelé k systému přistupují skrze standardní www rozhraní a to pomocí svého www prohlížeče (Mozilla Firefox, Opera, Chrome, Konqueror, MSIE). Vlastní systém plně respektuje zásady „platform independent“ a proto není podstatné, jaký operační systém uživatel používá. Podstatné je, aby jeho www prohlížeč plně respektoval příslušné standardy (RFC, W3C).

Záleží na kázni a disciplinovanosti uživatelů informačního systému (uživatelé, administrátoři), tato kázeň spočívá v zadávání veškerých požadavků právě skrze ticket system. Veškerá lidská činnost (požadavky, řešení požadavků) je pak evidována v ticket systému a to včetně historie každého požadavku.

Jde o plně modulární systém běžící nad redakčním systémem Drupal. Veškeré licence jsou nekomerční (GPL, LGPL). Systém je možné napojit (skrze standardní API) na libovolnou aplikaci (např. rezervační systém, e-shop, campus web, multifunkční webový portál apod.).

Základní verze ticket systému zahrnuje následující funkčnost:

1. Zadávání, správa a přidělování jednotlivých tiketů
2. Stavy tiketů (nový, v řešení, čekající, uzavřený)
   a jejich priority (nízká, střední, vysoká, kritická)
3. E-mailové upozornění na nový tiket nebo na změnu stavu tiketu
4. Vyhledávání podle klíčových slov nebo obsahu (integrace s Drupal search)
5. Neomezený počet uživatelů (jinými slovy - co Váš HW unese)
6. Komentáře k tiketům

Praha duben 2013

Linux Services | Naskové 3, 150 00 Praha 5
+420 257 189 583 | www.linuxservices.cz | info@linuxservices.cz