Kybernetický zákon: Využijte naplno open source nástroje

Někdy bývá problém přeložit politicko-právní jazyk zákona o kybernetické bezpečnosti do jazyka srozumitelného technické komunitě. Přinášíme vysvětlení požadavků daných příslušnými paragrafy a zároveň nastiňujeme jejich praktické řešení za použití open source nástrojů.

JAROSLAV KODET

§ 16 Fyzická bezpečnost

Využití open source softwaru pro zajištění fyzické bezpečnosti je možné zejména při realizaci pultů centrální ochrany včetně kamerových přehledových systémů.

Pro tento účel lze využít nástroje určené pro dohled síťových prvků (Icinga, Nagios a další), doplněné o rozhraní pro odpovídající čidla, propojené s programy pro přenos a zachycení obrazového signálu z bezpečnostních kamer.

§ 17 Nástroj pro ochranu integrity komunikačních sítí

V tomto paragrafu se řeší pravidla pro komunikaci mezi vnitřní a vnější sítí, segmentace sítě, použití demilitarizovaných zón a pravidla pro bezpečný přístup z vnější sítě do vnitřní sítě, jakož i pravidla blokování nežádoucího provozu mezi jednotlivými segmenty.

Nástrojem pro ochranu integrity komunikačních sítí se tady rozumí vhodně navržená topologie sítě včetně použití síťových prvků umožňujících požadovanou segmentaci sítě a filtraci provozu mezi jednotlivými prvky.

Použitá zařízení pro dosažení těchto požadavků představují ethernetové switche, routery a firewally.

Pokud nelze zajistit segmentaci sítě pomocí VLAN na upravovatelném přepínači, je možné ji zabezpečit prostřednictvím několika menších nemanagovatelných switchů, z nich každý realizuje jednu fyzickou LAN.

[Pro praktické ověřování identity uživatelů nabízí komunita open source dostatek softwaru kompatibilního se svými komerčními protějšky.]

Ačkoli open source nástroje jsou nepochybně schopné zastat úlohu všech těchto prvků, jejich použití je limitované skutečností, že jsou zpravidla uskutečňované na plnohodnotném počítači – tedy poměrně energeticky náročném zařízení.

V roli routerů a firewallů lze samozřejmě použít malá miniPC, založená na úsporných platformách ARM nebo PPC, osazená vhodným operačním systémem, například OpenWRT či dd-WRT. Použitelnost těchto zařízení ovšem je limitována několika faktory, jimiž jsou počet ethernetových rozhraní (na tomto parametru závisejí maximální počet segmentů sítě), výkon CPU (na tomto kritériu závisí datová prostupnost prvku) a také velikost operační paměti nebo cache.

Určitou výjimku pak tvoří tuzemské routery Turris (*turris.cz*), jejichž výrobce slibuje vysokou bezpečnost (mj. díky firmwaru, který byl navržen s ohledem na dosažení maximálního možného zabezpečení) a rovněž nízký elektrický příkon. Turris existuje ve variantách první a druhé série, pro příští rok se připravuje úplně přepracovaná varianta Omnia (*omnia.turris.cz*).

Softwarové routery/firewally:

- `www.ipcop.org/`
- `ipfire.org/`

Ethernetový switch pro virtualizované prostředí:

- `openvswitch.org/`

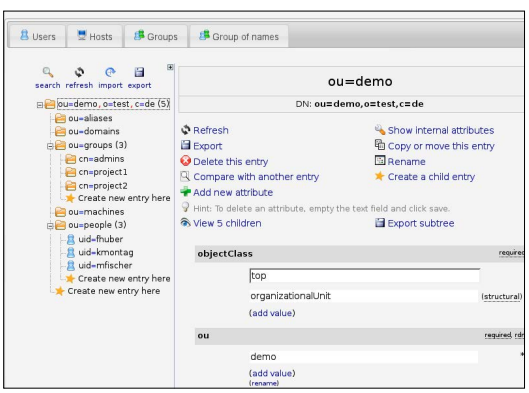
§ 18 Nástroj pro ověřování identity uživatelů

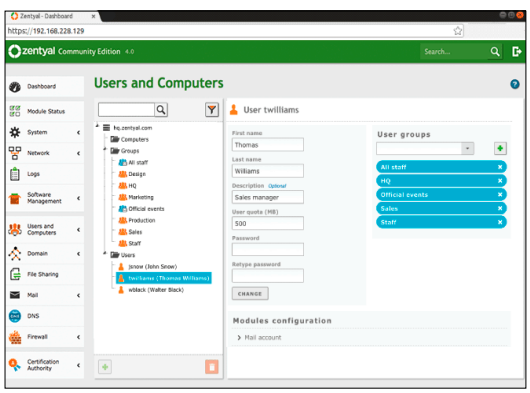
Možnost využití nástroje pro ověřování identity uživatelů je integrální součástí všech běžně používaných operačních systémů.

Tyto nástroje bývají zpravidla široce konfigurovatelné a modulární, tak aby vyhovovaly požadavkům kladeným na takový nástroj zákonem o kybernetické bezpečnosti (ZKB).

Pro praktické ověřování identity uživatelů nabízí komunita open source dostatek softwaru kompatibilního se svými komerčními protějšky. Jde například o:

- FreeRADIUS (`freeradius.org`)/RADIUS





◄ Příklady open source správy adresářové struktury LDAP ►

- OpenLDAP (openldap.org)/Microsoft AD, Oracle Internet Directory
- Kerberos (www.gnu.org/shishi)
- OpenDiameter (sourceforge.net/projects/diameter)

Všechny tyto nástroje poskytují prostředky pro vynucení určené složitosti hesla, jakož i dalších atributů požadovaných ZKB, buď samy o sobě prostřednictvím login.conf, nebo s využitím externích mechanismů jako cracklib a slovníků oblíbených „hesel“.

§ 19 Nástroj pro řízení přístupových oprávnění

Nástroje typu „správa uživatelů a skupin“, ve spojení s nástroji pro nastavování atributů a oprávnění k souborům a adresářům, jsou implementované ve všech moderních operačních systémech (MS Windows, Linux, *BSD, komerční Unixy). Doporučují se nástroje pro centralizovanou správu přístupových oprávnění, komunikující s centrálním AAA (Authentication, Authorisation, Accounting) serverem.

§ 20 Nástroj pro ochranu před škodlivým kódem

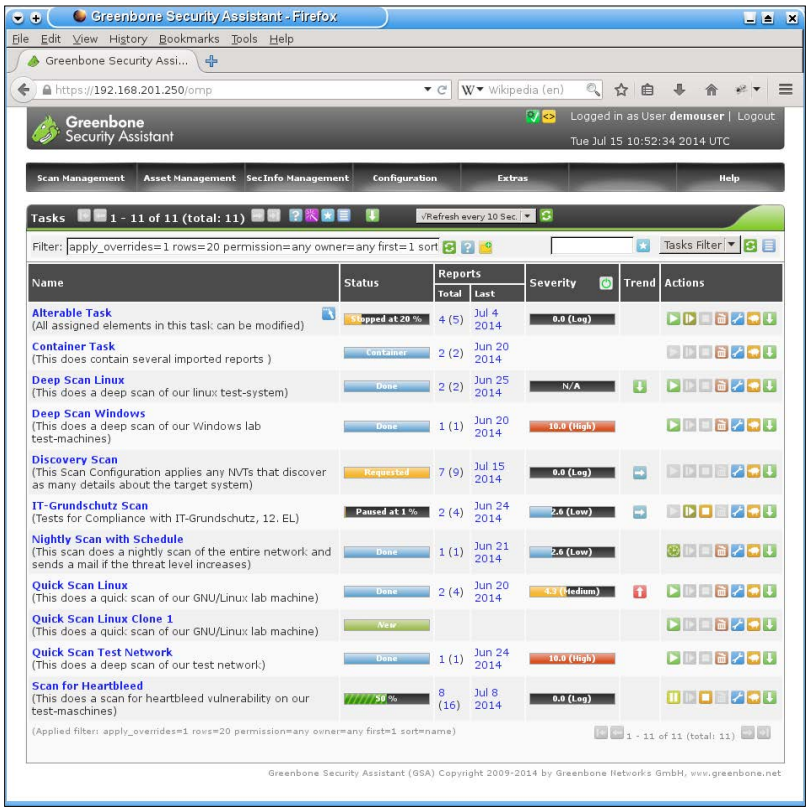
Obvykle se předpokládá, že operační systémy unixového typu (včetně Linuxu a *BSD) jsou vůči napadení škodlivým kódem o něco odolnější než MS Windows. To je do značné míry pravda, nicméně pokud není nástroj pro ochranu před škodlivým kódem implementovaný i na těchto platformách, které se často nasazují jako internetové servery, hrozí nebezpečí, že se tyto servery budou (ač třeba samy z principu infikované být nemohou) podílet na šíření infekce mezi klienty, kteří z nich získávají data – například přes stažený dokument infikovaný škodlivým kódem. Na straně serverů se proto doporučuje používat software pro identifikaci škodlivého softwaru, zejména pro kontrolu proudu dat získávaných ze serveru klienty.

1 Ochrana před škodlivým softwarem šířeným prostřednictvím e-mailu: je důležitá proto, že jde o jeden z nejvýznamnějších vektorů šíření škodlivého softwaru. Ochrana bývá řešena prostřednictvím e-mailového proxy serveru, který je schopen vykonávat kontrolu obsahu zpráv včetně komprimovaných příloh, ideálně včetně šifrovaných. Na unixových/linuxových serverech se pro tento účel používá kombinace softwaru Postfix, Amavis, ClamAV, SpamAssassin, Razor.

Ochrana na straně poštovního serveru je první linií obrany, jejímž úkolem je zabránit doručení škodlivého obsahu do poštovních schránek uživatelů, a tím zabránit jejich nechtěnému otevření a následnému spuštění škodlivého kódu.

Velmi elegantním open source řešením e-mailové proxy, zajišťujícím ochranu před škodlivým softwarem, je projekt ASSP (AntiSpam SMTP Proxy, *sourceforge.net/projects/assp/*), umožňující komplexní konfiguraci chování mail proxy prostřednictvím webového rozhraní.

2 Ochrana před škodlivým softwarem šířeným prostřednictvím webu: Opět jde o první linii ochrany, v tomto případě uskutečňovanou nejlépe prostřednictvím filtrujícího a antivirového HTTP proxy serveru.



Grafické rozhraní nástroje OpenVAS, konkrétně seznam úloh bezpečnostních skenů.

[Velmi elegantním open source řešením e-mailové proxy, zajišťujícím ochranu před škodlivým softwarem, je projekt ASSP.]

Vhodným řešením je například projekt HTTP AntiVirus Proxy (havp.org) nebo www.cacheguard.com. I zde je nutné zajistit také odpovídající ochranu koncových pracovních stanic, protože šifrovaný provoz není možné v reálném čase skenovat v pozici „muže uprostřed“.

3 Dalším prvkem ochrany před škodlivým softwarem je blokování jeho síťového provozu, a to jak na úrovni datové infrastruktury, tak na úrovni „osobních firewallů“ koncových stanic. Pravidla síťové komunikace by se měla nastavit „paranoidně“, tj. povolit jen provoz nezbytný k fungování legitimního softwaru, vše ostatní zakázat.

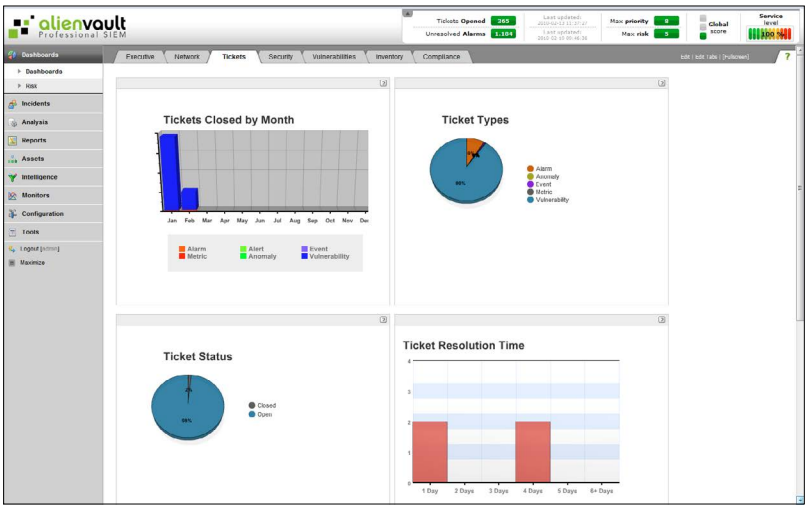
Opatření na straně serveru, proxy serveru či prvku síťové infrastruktury ale v žádném případě plně nenahrazuje ochranu proti škodlivému softwaru na koncových pracovních stanicích, zejména proto, že nemusí být vždy schopné zachytit šifrovaný provoz, který je dešifrován až na klientském programu.

§ 21 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

Nástroji pro zaznamenání činností KII (kritická informační infrastruktura), VIS (významná informační infrastruktura) a jejich uživatelů a administrátorů jsou systémové a aplikační logy.

Pro zajištění jejich použitelnosti pro případ vyšetřování kybernetických bezpečnostních incidentů je třeba zajistit synchronizaci času všech prvků KII a VIS pomocí protokolu NTP (Network Time Protocol), který je implementovaný na všech běžných operačních systémech.

Dále je třeba zajistit konfiguraci logovacích systémů (ať už unixových syslogů či Windows event-



SIEM řešení OSSIM/USM od firmy AlienVault

logů), tak aby obsahovaly všechny požadované náležitosti specifikované v jednotlivých odstavcích tohoto paragrafu.

Použitelnými open source nástroji jsou v tomto případě syslog, syslog-ng (`syslog-ng.org`) a rsyslog (`rsyslog.com`).

Bývají užitečné zejména v roli centralizovaných syslog serverů, na nichž se koncentrují veškeré relevantní logy ze všech prvků KIS na jednom místě.

Takto shromážděné logy se následně zpracovávají softwarem IDS/IPS/SIEM (viz další paragrafy) pro včasnou detekci kybernetických bezpečnostních incidentů, jakož i k omezení jejich dopadů a prevenci jejich opakování.

§ 22 Nástroj pro detekci kybernetických bezpečnostních událostí

Požaduje se nasazení intrusion detection systémů (IDS), a to jak v rámci vnitřní komunikační sítě, tak na serverech patřících do informačního systému KIS a komunikačního systému KIS.

K detekci kybernetických bezpečnostních událostí lze využít výstupů z mnoha softwarových nástrojů, například prohledávačů logů Logwatch (`logwatch.org`), Epylog (`fedorahosted.org/epylog`), intrusion detection systémů jako OpenVAS (`openvas.org`), Suricata (`suricata-ids.org`), Snort (`www.snort.org`) nebo Samhain (`la-samhna.de/Samoin`).

§ 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Do této kategorie spadají nástroje souhrnně nazývané SIEM (Security Incident and Event Management). Kromě mnoha komerčních řešení existují i open source řešení nabízející podobné funkcionality jako jejich komerční protějšky.

Častěji než u jiných kategorií softwaru zde dochází k tomu, že stejná firma nabízí zdarma nástroj jednodušší (respektive s nějakým způsobem omezenou funkčností) a komerčně pak komplexnější, s lepší zákaznickou podporou, nabízející více pohledů a větší komfort ovládání nebo vyhledávání.

Takto je tomu například u dvojice produktů od firmy AlienVault OSSIM/USM (`www.alienvault.com/free-downloads-services`). Dalšími open source nástroji, které mohou být užitečné, jsou OSSEC (`www.ossec.net/`) nebo logalyze (`www.logalyze.com`).

[Často se zapomíná na to, že open source software sámo sobě sice lze získat zdarma, ale komerční podpora k němu již bezplatná nebývá.]

§ 24 Aplikační bezpečnost

Aplikační bezpečnost se zajišťuje prostřednictvím penetračního testování zranitelností aplikací dostupných z vnější sítě pomocí nástrojů k tomuto účelu vhodných. Tyto nástroje testují aplikace na známé zranitelnosti, výsledkem je report včetně navrhovaných řešení.

K zajištění aplikační bezpečnosti se také využívají aplikační firewally například jako bezpečnostní moduly webserveru (`www.modsecurity.org`) nebo OWASP Web Application Firewall.

Z komerčních nástrojů pro testování aplikační bezpečnosti jde zejména o nástroj Nessus (`www.tenable.com/products/nessus-vulnerability-scanner`).

Jeho open source alternativou je pak projekt OpenVAS (`www.openvas.org/`).

§ 25 Kryptografické prostředky

Pro účely zajištění dostatečně odolného šifrování síťového provozu se používají knihovny OpenSSL (`openssl.org`), avšak je třeba mít zajištěnou jejich aktuálnost a správnou konfiguraci, tak aby se vyhovělo podmínkám této vyhlášky.

Je nutné sledovat aktuální zprávy o zranitelnostech a nevyhovující verze knihoven bez otálení upgradovat na varianty bez známých zranitelností. V tomto ohledu lze doporučit projekt bettercrypto (`bettercrypto.org`), který má administrátorům pomoci s co nejlepším zabezpečením jimi používaných služeb a používané kryptografie.

§ 26 Nástroj pro zajišťování úrovně dostupnosti

Pro dosažení předepsané úrovně dostupnosti lze použít clusterové a cloudové technologie vyvíjené jako open source (KVM, OpenStack), případně zajistit dostupnost náhradního aktiva v určeném čase prostřednictvím back-up/restore softwaru (`sourceforge.net/projects/bacula/`).

Komerční systémy vs. open source

Celkově je nutné konstatovat, že ačkoli teoreticky lze vyhovět všem požadavkům ZKB na technická opatření pomocí open source nástrojů, je nutné jejich nasazení uvážit ze všech hledisek, zejména na základě analýz rizik a nákladů spojených s jejich vlastnictvím.

Často se totiž zapomíná na to, že open source software sám o sobě sice lze získat zdarma, ale komerční podpora k němu již bezplatná nebývá. Stejně jako ke komerčním produktům je možné k nim někdy přikoupit podporu na bázi SLA, ale není to pravidlem.

Pokud není komerční podpora k dispozici, je organizace odkázána na podporu na komunitní bázi, případně na schopnosti administrátora těchto nástrojů.

Při náležité úrovni znalostí administrátorů však není třeba se open source řešení obávat, nicméně náklady na vyškolení administrátora též přispívají k navýšení celkových nákladů na vlastnictví. ■

Autor pracuje jako bezpečnostní analytik sdružení CZ.NIC, které provozuje Národní bezpečnostní tým Csirt.cz.