ČD-TELEMATIKA

Internetové služby

ČDT-MONITOR

Služba ČDT–MONITOR umožňuje získat zákazníkovi přehled o bezpečnostních incidentech na jeho internetové konektivitě. Prostřednictvím speciálních sond je monitorován jeho internetový provoz a sebraná data jsou vyhodnocována metodami detekujícími bezpečnostní rizika. S tímto produktem získává zákazník rychlý přehled o bezpečnostních rizicích ve své síti (útoky proti počítačům v síti, skenování počítačů, generování spamu atd.), což mu umožňuje rychle reagovat a minimalizovat jejich dopady na uživatele.

www.cdt.cz

ČD - Telematika a.s. **Korespondenční adresa** Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz, poptavka@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938

ČD-TELEMATIKA

ČDT-MONITOR

Použité metody

- **Telnet** – zvýšené použití služby Telnet. Detekuje veškeré spojení, včetně pokusů o spojení na TCP port 23, a pro jednotlivé IP adresy počítá počty těchto spojení;
- **SSHDICT** – pokusy o uhodnutí uživatelského jména/hesla, případně přihlášení podvrženým certifikátem ke službě SSH. Metoda je schopna rozpoznat úspěšný/neúspěšný útok;
- **OUTSPAM** – odesílání nebo pokusy o odesílání zvýšeného počtu e-mailů z konkrétních IP adres;
- **SCANS** – různé typy scanování sítě a způsoby provedení. Součástí detailů je počet unikátních scanů, zpráva o případné odpovědi scanované IP adresy a seznam dotčených portů. Indikuje zavirované IP adresy v síti;
- **DNSQUERY** – zvýšený počet DNS dotazů z konkrétních IP adres;
- **DNSANOMALY** – podezřelá komunikace DNS provozu;
- **BLACKLIST** – kontrola provozu (podle přiřazených filtrů) a rozpoznání komunikace s IP adresami uvedenými na blacklistu;
- **RDP Dictionary Attacks** – rozpoznává pokusy o uhádnutí uživatelského jména a hesla do služby RDP. Slovníkové útoky jsou široce rozšířenou a oblíbenou metodou pro získání neautorizovaného přístupu do počítačového systému.
- **REFLECTDOS Amplificated DoS attack** – detekuje DoS útoky, které využívají ke svému zesílení nedostatků některých služeb. Umožňují vygenerovat pro specifický požadavek několikanásobně větší odpověď, a to k jejímu odeslání na podvrženou zdrojovou IP adresu požadavku (např. prostřednictvím nezabezpečených NTP serverů).

Hlavní výhody

- včasné odhalení rizikového provozu v internetové konektivitě
- snížení zátěže na aktivních prvcích provozovatele sítě
- další rozvoj obchodních aktivit velkoobchodních partnerů směrem ke koncovým zákazníkům

Komu je služba určena

- lokální poskytovatelé internetu
- velké a střední společnosti
- státní správa a samospráva

Služba je poskytována jako doplňková služba k přístupu do sítě internet, poskytované společností ČD - Telematika.

Ukázka reportu

Period: 2012-11-04 00:00:00 - 2012-11-05 00:00:11

LOW priority events

ID	Timestamp	Type	Detail	Source	Targets	NetFlowSource
#143974	2012-11-04 21:06:27	SCANS	horizontal TCP SYN scan (attempts with response: 1, attempts without response: 108, targets: 96, port list: 62999, 9442, 80, 443)	[redacted]85	31.128.83.158, 46.40.87.201, 46.211.194.39, 66.30.111.208, 67.166.129.224, 68.49.31.43, 76.89.91.117, 77.122.119.153, 77.122.165.20, 78.88.192.245, ...	TS 06/4
#143976	2012-11-04 21:06:59	SCANS	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 111, targets: 109, port list: 62999, 9442)	[redacted]130	31.41.151.7, 46.47.193.9, 46.118.40.90, 46.118.145.129, 46.118.239.65, 46.119.114.138, 46.164.158.6, 46.214.53.72, 46.233.19.61, 60.52.94.230, ...	TS 06/4
#143997	2012-11-04 21:16:33	SCANS	horizontal TCP SYN scan (attempts with response: 1, attempts without response: 120, targets: 119, port list: 62999, 9442)	[redacted].130	31.147.124.123, 46.49.26.183, 46.49.31.168, 46.118.43.17, 46.119.9.50, 46.119.26.147, 46.172.233.1, 46.214.100.5, 50.81.219.64, 62.129.39.74, ...	TS 06/4

www.cdt.cz

ČD - Telematika a.s. Korespondenční adresa Pod Táborem 369/8a | 190 00 Praha 9 | tel.: +420 972 225 555 | e-mail: cdt@cdt.cz, poptavka@cdt.cz
Sídlo společnosti Pernerova 2819/2a | 130 00 Praha 3 | IČ: 61459445 | DIČ: CZ61459445 | vedená u Městského soudu v Praze, spisová značka B 8938