DFN-CERT Warnmeldungen und Cisco ASA: eine datenschutzfreundliche Kombination

Thomas Blaß und Prof. Dr. Rainer W. Gerling
Generalverwaltung
Max-Planck-Gesellschaft

Warnmeldung des DFN-Cert

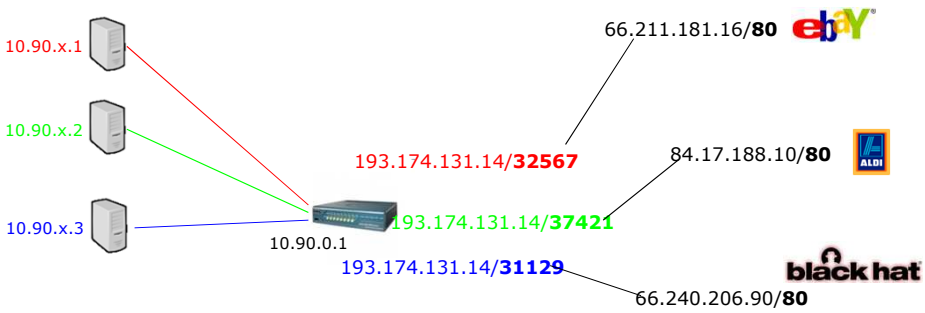
IP	Meldungstyp	Zuletzt gesehen
193.174.131.14	Bot	2010-01-29 13:46:04 GMT+0100

Details zu den Meldungen pro IP:

System: 193.174.131.14
Meldungstyp: Bot
Zeitstempel: 2010-01-29 13:46:04 GMT+0100 (Winterzeit)
Beschreibung: Auf dem System scheint eine Bot-Software betrieben zu werden, die versucht, einen HTTP- oder IRC-basierten Bot-Netz Control-Server zu erreichen.

TCP Quellport	Malwaretyp	Zeitstempel(GMT+0000)
1365	Torpig	2010-01-29 12:46:04
64414	Torpig	2010-01-29 12:28:46
2351	Torpig	2010-01-29 12:03:15
58659	Torpig	2010-01-29 07:54:58

Network Address Translation



- 10.90.x.1 -> 193.174.131.14/**32567**
- 10.90.x.2 -> 193.174.131.14/**37421**
- 10.90.x.2 -> 193.174.131.14/**31129**

- Momentaufnahme, deshalb ist die Uhrzeit relevant

Logging

- 10.90.x.1 -> 66.211.181.16/80
- 10.90.x.2 -> 84.17.188.10/80
- 10.90.x.2 -> 66.240.206.90/80
- Wir sehen, was die/der Beschäftigte aufruft!
  ➔ Probleme mit Personalvertretung

- 10.90.x.1 -> 193.174.131.14/32567
- 10.90.x.2 -> 193.174.131.14/37421
- 10.90.x.2 -> 193.174.131.14/31129
- Wir sehen **nicht**, was die/der Beschäftigte aufruft!
  - Erst die DFN-Cert Warnmeldung liefert die erforderliche Zusatzinformation

Datenschutzfreundliches Positiv-Logging

- Mit dem externen Zusatzwissen der Warnmeldung können wir den PC identifizieren
- Auswertungen, welche Web-Seiten aufgerufen werden, sind nicht möglich
- Original Log-Datei-Eintrag:

```
Feb  2 11:10:33 193.174.131.17 %ASA-6-305011: Built dynamic TCP translation
from intern:10.90.x.2/2551 to extern:193.174.131.14/29128
```

  - logging list DefaultFilter level warnings
    logging list DefaultFilter message 305011
    logging trap DefaultFilter
    logging host extern 193.174.x.y 17/1514

- Alle Geräte senden Ihre Log-Dateien an einen Log-Server (syslog)
  - Switches, Router, Firewalls usw.
- Aufbewahrungsdauer: ~~60~~ 20 Tage

MAX-PLANCK-GESELLSCHAFT | Rainer W. Gerling, 18. DFN Workshop | SEITE 5