

Sicherheitsprobleme bei www.microsoft.ch - fatale Reaktionen auf Portscans

Viele Unternehmen reagieren auf Hackerangriffe durch automatische Mechanismen. Auch die Firewall der schweizer Niederlassung von Microsoft führt solche Reaktionen durch – mit fatalen Folgen.

Viele Hersteller von IDS (Intrusion Detection Systems) werben damit, dass ihre Produkte in der Lage sind, gängige Firewalls als Reaktion auf einen Angriff umzukonfigurieren. So lässt sich die Checkpoint Firewall durch ein IDS wie Real Secure komfortabel über das OpSec-Protokoll umkonfigurieren. Viele Watchguard-Administratoren erreichen durch das „Block Intruder“-Feature, dass Angreifer schon bei einem Portscan auf eine schwarze Liste gesetzt werden. Jedwede zukünftige Kommunikation zwischen einem hier gelisteten System und dem Internet wird dann unterbunden.

Eine Analyse der Server der Schweizer Niederlassung von Microsoft zeigt ein überraschendes Ergebnis: Scannt man www.microsoft.ch, so ist das http-Protokoll auf www.microsoft.ch scheinbar nicht aktiv.

```
[root@comserv /root]# nmap -P0 www.microsoft.ch
```

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
```

```
All 1528 scanned ports on www.microsoft.ch (195.141.103.58) are: filtered
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 1035 seconds
```

```
[root@comserv /root]#
```

Der Verdacht liegt nahe, dass das scannende System bereits zu Beginn des Portscans auf eine Blacklist gesetzt und so der http-Verbindungsaufbau von Microsofts Firewall unterbunden wurde. Dieser Verdacht ließ sich leicht bestätigen, denn von einem anderen Rechner aus war die Webpage nach wie vor erreichbar.

Problem 1: Wer muss draußen bleiben?

Möchte eine Firewall einen potentiellen Angreifer aussperren, so werden sämtliche TCP/IP-Pakete mit dessen IP-Adresse einfach verworfen. Die Blacklist beinhaltet nun zu blockierenden IP-Adressen, von denen aus Portscans auf das Unternehmen durchgeführt wurden. Problematisch ist diese Vorgehensweise, wenn mehrere Personen unter der selben IP-Adresse auftretet und so viel zu viele Systeme von einem Blacklist-Eintrag betroffen sind.

Problem 2: IP-Spoofing und D.o.S.

Während die Folgen des ersten Problems noch akzeptiert werden können, hat ein weiteres Problem fatale Konsequenzen: Ein Angreifer kann auch fremde Adressen als Absender seiner TCP/IP-Pakete eintragen (IP-Spoofing). Als Folge gerät dann ein fremdes System auf die Blacklist des gescannten Unternehmens. Dies wurde unter Anwendung der „Decoy“-Option des Scanners nmap (www.insecure.org) bei www.microsoft.ch verifiziert: Eingewählt über AOL scannen wir Microsoft mit einer falschen IP-Adresse; in diesem Fall 209.221.165.176.

```
nmap -sS -P0 -D217.81.153.176 www.microsoft.ch
```

Danach versuchten wir, von 217.81.153.176 eine Verbindung auf den Webserver von MS zu öffnen, was wie erwartet nicht gelang: Die Firewall von Microsoft hatte zugeschlagen und ein „unschuldiges“ System ausgesperrt.

Ein blockierter Angreifer kann nun den Spieß umdrehen: Er könnte beispielsweise damit beginnen, die IP-Adressen von wichtigen Mailservern in die Blacklist von Microsoft einzutragen. Manche Firewall-Lösungen lassen sich mit folgendem Befehl empfindlich stören:

```
nmap -sS -P0 -D127.0.0.1 www.zielsystem.de
```

Fazit

Ohne Personalaufwand und ohne Verzögerung automatisiert auf Angriffe angemessen zu reagieren - das klingt verführerisch. Zieht man solche Techniken aber ernsthaft in Betracht, muss man mögliche unerwünschte Folgen zuvor genau analysieren. Die Blockierung eines „unerwünschten“ Systems durch die Firewall kann durchaus sinnvoll sein – man sollte sich nur sicher sein, dass man das richtige System erwischt. Und das ist bei Portscans (mit der Ausnahme des von Hackern selten eingesetzten TCP-Connect-Scans) nicht möglich. Für ernst zu nehmende Angriffe ist aber der Aufbau einer Verbindung nötig. Und dies ist (mit Ausnahme von Blind Spoofing Attacken) nur mit authentischen IP-Adressen möglich.

Sebastian Schreiber <Schreiber@SySS.de>