Abwehrmechanismen gegen die Angriffe

Zielsetzung dieses Kapitels

In diesem Kapitel werden Maßnahmen beschrieben, mit denen sich die in diesem Projekt verwendeten Angriffsvektoren – EternalBlue (MS17-010) und Elasticsearch RCE (CVE-2014-3120) – verhindern oder zumindest deutlich erschweren lassen. Die Maßnahmen sind aus Sicht eines Administrators formuliert und decken sowohl technische als auch organisatorische Aspekte ab.

---

1. Abwehr von EternalBlue (MS17-010)

EternalBlue nutzt eine Schwachstelle im SMBv1-Protokoll von Windows. Der Angriff funktioniert nur, wenn SMBv1 aktiv ist und der Rechner nicht gepatcht wurde. Entsprechend gibt es mehrere Ansatzpunkte.

1.1 Patch-Management

Der wichtigste Schritt ist das Einspielen des Microsoft-Patches **KB4012212** (für Windows 7 und Server 2008 R2). Ohne diesen Patch bleibt das System dauerhaft anfällig, egal welche anderen Maßnahmen ergriffen werden.

In Unternehmen sollte ein fester Patch-Zyklus etabliert sein, damit kritische Sicherheitsupdates nicht monatelang liegen bleiben.

1.2 SMBv1 deaktivieren

Da EternalBlue ausschließlich SMBv1 angreift, ist das Abschalten von SMBv1 die wirksamste Gegenmaßnahme. Das geht per PowerShell:

powershell

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
```

Danach ist der Angriff wirkungslos, selbst wenn der Patch fehlt. SMBv1 wird heute ohnehin kaum noch benötigt – moderne Systeme nutzen SMBv2 oder SMBv3.

1.3 Port 445 einschränken

SMB sollte niemals direkt aus dem Internet erreichbar sein. Firewall-Regeln, die Port 445 nur für interne Subnetze erlauben, reduzieren die Angriffsfläche erheblich. In Kombination mit Netzwerksegmentierung wird verhindert, dass ein kompromittiertes System andere Systeme im Netz angreift.

1.4 Monitoring und IDS

EternalBlue erzeugt charakteristischen SMB-Traffic. Ein Intrusion Detection System wie Snort oder Suricata erkennt die typischen MS17-010-Pakete und kann Alarm auslösen. So lassen sich Angriffe früh erkennen, auch wenn sie nicht sofort erfolgreich sind.

---

2. Abwehr von Elasticsearch RCE (CVE-2014-3120)

Die Elasticsearch-Schwachstelle erlaubt die Ausführung von beliebigem Java-Code über dynamische MVEL-Scripts. Sie ist besonders gefährlich, weil keine Authentifizierung nötig ist.

2.1 Version aktualisieren

Die Schwachstelle betrifft ausschließlich Elasticsearch 1.1.x. Ein Update auf eine aktuelle Version behebt das Problem vollständig. Das ist die einfachste und wirksamste Maßnahme.

2.2 Dynamische Scripts deaktivieren

Falls ein Update nicht sofort möglich ist, können dynamische Scripts in der `elasticsearch.yml` abgeschaltet werden:

yaml

```
script.disable_dynamic: true
```

Damit ist die RCE über dynamische Scripts nicht mehr möglich. Der Funktionsumfang von Elasticsearch wird dadurch kaum eingeschränkt.

2.3 Authentifizierung aktivieren

Elasticsearch hat standardmäßig **keine** Authentifizierung. In Produktivumgebungen sollte das unbedingt geändert werden. Möglichkeiten:

- Reverse Proxy mit Basic Auth davor setzen (z. B. Nginx)
- X-Pack oder OpenSearch Security Plugin nutzen
- Elasticsearch nur an `localhost` binden, wenn kein externer Zugriff nötig ist

2.4 Netzwerkzugriff einschränken

Port 9200 sollte niemals aus dem Internet erreichbar sein. Nur Systeme, die Elasticsearch wirklich benötigen, sollten darauf zugreifen können. Firewall-Regeln und Netzwerksegmentierung sind hier die richtigen Werkzeuge.

2.5 Monitoring

Ungewöhnliche Anfragen an `/_search` mit `script`-Feldern sind ein Warnsignal. Logging und Alerting helfen, Angriffe früh zu erkennen, bevor sie erfolgreich sind.

---

3. Allgemeine Maßnahmen

Neben den spezifischen Maßnahmen gegen die beiden Angriffsvektoren gibt es allgemeine Prinzipien, die in jeder Umgebung gelten:

- **Least Privilege:** Dienste sollten nicht als Administrator laufen, sondern mit minimalen Rechten.
- **Regelmäßige Scans:** Schwachstellen-Scanner wie Nessus oder OpenVAS zeigen veraltete Dienste früh.

- **Patch-Management:** Ein fester Patch-Zyklus verhindert, dass Systeme monatelang verwundbar bleiben.
- **Netzwerksegmentierung:** Angriffe auf einen Host sollten nicht automatisch auf andere Hosts übergreifen.
- **Bewusstsein schaffen:** Administratoren sollten veraltete Dienste erkennen und nicht „läuft ja, also nicht anfassen“ denken.

---

4. Fazit der Abwehrmaßnahmen

Beide Angriffsvektoren lassen sich mit verhältnismäßig einfachen Mitteln verhindern. EternalBlue verschwindet durch das Abschalten von SMBv1 und das Einspielen des Patches. Elasticsearch RCE verschwindet durch ein Update oder das Deaktivieren dynamischer Scripts.

Das eigentliche Problem ist nicht die Technik, sondern die Zeit: Beide Dienste waren veraltet und ungepatcht. Ein sauberes Patch-Management und eine regelmäßige Überprüfung der eingesetzten Software hätten beide Angriffe von vornherein verhindert.

Revision #2
Created 29 September 2026 10:07:33 by Admin
Updated 29 September 2026 10:11:29 by Admin