Angriffserkennung, Sicherungsmaßnahmen und Notfallplan

Angriffs- und Einbruchserkennung

Angriffe werden meist zu spät erkannt, wenn überhaupt. Viele Schutzmechanismen gaukeln Unternehmen eine Scheinsicherheit vor. Solange Schutzmechanismen nichts Auffälliges finden, wird auch keine Anomalie gemeldet.

Heutige Angreifer sind auf Informationen aus und sind nicht daran interessiert auffällig zu werden. Angriffe für die Informationsgewinnung sind nicht destruktiv wie Viren und andere Malware. Angriffe beschränken sich heutzutage nicht mehr allein auf außen, die Bedrohung von innen ist ebenso real.

Diese Angriffe geschehen im Verborgenen und so manches Unternehmen musste bereits miterleben, dass ein Konkurrenzunternehmen, z. B. in Übersee, ein Patent kurz vor Ihrer eigenen Patentveröffentlichung angemeldet hat (Stichwort Wirtschafts-kriminalität).

Sicherheitsmaßnahmen:

1. Integritätsprüfung (Integrität der Daten wird geprüft)
2. Signaturerkennung (bekannte Angriffssignaturen werden erkannt)
3. Zero-Hour-Schutz (bei bekannten Sicherheitslücken durch virtuelles Patching)
4. Patentierter verhaltensbasierter Security-Scanner (zur proaktiven Erkennung und Abwehr unbekannter Angriffe)
5. Anomalieerkennung (vom Normalbetrieb abweichende Operationen werden er-kannt)

Was tun bei einem erfolgreichen Angriff?

Wenn eine Anomalie erkannt wird, was auf einen **erfolgreichen** Angriff schließen lässt, ist es bereits zu spät. Genau wie bei einer Kompromittierung durch Malware, ist das System nicht mehr vertrauenswürdig. Folgende Maßnahmen sollten sofort durchgeführt werden:

1. Das Netzwerk ist sofort vom Internet zu trennen, um weitere Manipulationen zu verhindern

2. Wenn ein System kompromittiert wurde, können alle Daten (Programme, Informationen etc.) manipuliert, an Dritte weitergeben oder bereits (Passwörter usw.) bekannt sein.

3. Ein Backup des Systems und der Log-Dateien mit all ihren Daten ist zur späteren Analyse zu empfehlen.

3.1. Das System-Backup zur Analyse muss zwingend von einem sauberen Medium aus geschehen (Boot-CD)

3.2. Sämtliche Log-Dateien sind auf einem externen Medium zu sichern
   3.2.1. Firewall, IPS und IDS Log-Dateien
   3.2.2. Betroffene Server Log-Dateien
   3.2.3. Betroffene Workstation Log-Dateien

3.3. Analyse der Backups und der Log-Dateien
   3.3.1. Angriffsweg identifizieren
   3.3.2. Datenmanipulationen anhand der Prüfsummen vergleichen
   3.3.3. Wichtige Dateien, die nicht kompromittiert wurden, sind zu sichern
   3.3.4. Kompromittierte Systeme (Server, Workstation) sind zu ermitteln

3.4. Backups und Log-Dateien zur Beweissicherung (Betriebshaftpflicht) aufbewahren

4. Existiert ein sauberes Backup des Systems, sind folgende Maßnahmen zu treffen:
   4.1. Es muss garantiert sein, dass das Backup sauber ist
   4.2. Der Angriffsweg muss bekannt sein, damit eine erneute Kompromittierung ausgeschlossen werden kann
   4.3. Das saubere Backup auf die ermittelten kompromittierten Systeme zurück spielen
   4.4. Passwörter ändern

5. Existiert kein sauberes Backup des Systems, sind folgende Maßnahmen zu treffen:
   5.1. Der Angriffsweg muss identifiziert werden, damit eine erneute Kompromittierung ausgeschlossen werden kann
   5.2. Wenn kein sauberes Backup zum Vergleich (Prüfsummen) von Datenmanipulationen vorliegt, sind alle Dateien und Programme bei den ermittelten kompromittierten Systemen als nicht vertrauenswürdig zu betrachten
   5.3. Neuinstallation bei den betroffenen kompromittierten Systemen
   5.4. Passwörter ändern

Rösner-IT:

- ✓ sichert Ihre wichtigen Daten
- ✓ rekonstruiert bei Datenmanipulation
- ✓ untersucht Angriffe
- ✓ stellt Ihr System wieder her

Rösner-IT
EDV
IT-Security
Consulting & Service

Rösner-IT ♦ Lönsstr. 16 ♦ 48485 Neuenkirchen
Tel: +49 (0) 5973-90 06 52 ♦ Fax: +49 (0) 5973-90 07 98
E-Mail: info@roesner-it.com ♦ Web: www.roesner-it.com