Tool zur Früherkennung? Oder Feuerlöscher im Schadensfall?

Wann ein Compromise Assessment sinnvoll ist

Compromise Assessment kommt mit forensischen Methoden Angreifern im System auf die Spur und kann so zu einer schnelleren Entdeckung von Incidents bzw. Sicherheitsvorfällen beitragen. Doch eignet sich dieser durchaus teure Ansatz auch für die Prävention? Durchaus: Denn Unternehmen erhalten einen Überblick, ob eine Kompromittierung vorliegt, können feststellen, ob Sicherheitsmaßnahmen greifen und gegensteuern.

Compromise Assessment spürt mit forensischen Methoden die Spuren von Hackerangriffen im System, die Indicators of Compromise (IOC), auf. Die eingesetzten Scanner entdecken jene Artefakte, die Angreifer hinterlassen und die ihr Verhalten aufzeigen: Technik, Taktik und Prozeduren (TTP). Damit können betroffene Systeme identifiziert und Gegenmaßnahmen eingeleitet werden.

Angreifer sind oft bekannte „Ransomware-Gruppen“, anders finanziell motivierte Gruppen oder APTs. Ransomware gelangt wegen Unachtsamkeit ins System, wenn Links in E-Mails mit Schadsoftware oder Makros in Excel angeklickt bzw. aktiviert werden. Die Angreifer sammeln Informationen, sichern sich Rechte und breiten sich aus. Dann wird das System verschlüsselt und die erpresserische Forderung gestellt.

Compromise Assessment: Nach dem Angriff oder präventiv?

In der Regel kommt Compromise Assessment dann zum Einsatz, wenn ein solcher Angriff bekannt wurde. Die IT-Experten stehen hier oft vor einem Chaos. Nun gilt es einen Plan aufzustellen und ihm zu folgen: Die Agenten werden für den Scan ausgerollt und die Systeme gescannt. Betroffene Bereiche können schnell identifiziert werden und die Untersuchung damit zielgerichtet erfolgen. Gerade bei großen Unternehmen mit vielen Rechnern ist es aber nicht sinnvoll, die forensischen Analysen auf jedem Gerät durchzuführen, was zu viel Zeit in Anspruch nehmen und enorme Kosten verursachen würde. Mit Compromise Assessment hingegen identifiziert man kompromittierte Systeme, welche anschließend forensisch untersucht werden können.

Dem Mandiant Report zufolge vergingen im Jahr 2020 im Durchschnitt 76 Tage vom Beginn eines Angriffs bis zu seiner Erkennung[1] – diese Zeitspanne kann mit Compromise Assessment stark reduziert werden.

Compromise Assessment ist aber nicht nur sinnvoll, wenn sich ein Angreifer im System befindet, sondern auch als Präventionsmaßnahme. Die Vorteile dabei: Die Methodik erlaubt einen Blick in die Vergangenheit, was mit klassischen IT-Security-Ansätzen wie z. B. EDR (Endpoint Detection and Response) nicht möglich ist. Viele Unternehmen nutzen zwar Antiviren-Software oder EDR; Compromise Assessment findet aber Spuren von Angriffen in den vermeintlich geschützten Systemen, indem forensische Artefakte in den Fokus genommen werden.

Das Problem bei gängigen Tools der Cyber-Sicherheit: Viele Unternehmen wägen sich im Glauben, man müsse sie nur installieren und dann erledigen sie die Arbeit. Doch dem ist nicht so. Tools brauchen Betreuung, sie müssen eingestellt und überwacht, Erkennungsregeln angepasst werden. Hier passieren schnell Fehler; mit Compromise Assessment entsteht die Möglichkeit, auch z. B. über Fehler in Erkennungsregeln der Tools hinaus Spuren für Cyberangriffe zu erkennen.

Compromise Assessment ist im Ad Hoc Einsatz als Momentaufnahme oder kontinuierlich als Continuous Compromise Assessment möglich. Bei letzterem werden die Systeme in regelmäßigen Intervallen gescannt – etwa einmal im Monat. Dann wird das Delta betrachtet: So lassen sich Spuren von Angreifern finden und die Möglichkeit zur zeitnahen Reaktion entsteht. Die Maßnahmen erlauben dann eine ebenfalls konstante Optimierung der Sicherheits-Infrastruktur.

Weitere Use Cases für Compromise Assessment

Compromise Assessment eignet sich auch zum Nachweis bei Audits, dass genug für die IT-Sicherheit getan wird und Vorfälle dokumentiert werden: Bei einer solchen präventiven Kontrolle kann schnell eine Aussage getätigt werden, ob ein Verdacht besteht bzw. aktive Verdachtsfälle vorhanden sind, eine Folgenabschätzung vorgenommen und der Incident Response Life Cycle angestoßen werden.

Sinnvoll ist der Einsatz auch bei Firmenfusionen, wenn Netzwerke vereint werden. Über ein Ad Hoc Compromise Assessment beider können Kompromittierungen erkannt und vor der Öffnung beseitigt werden.

[1] Mandiant (2021): *M-Trends 2021*. Online verfügbar unter https://www.mandiant.com/sites/default/files/2021-09/rpt-mtrends-2021-4.pdf, zuletzt aufgerufen am 23.05.2022.

Erkenntnisse und Informationsgewinne

Mit Compromise Assessment gewinnen Unternehmen darüber hinaus wichtige Erkenntnisse über ihre Cyber-Security; es kann die Schwächen der Infrastruktur aufzeigen: Manche stellen fest, dass ihr Sicherheitsniveau vom State of the Art Level weit entfernt ist und dass sie bis dato blind im Netzwerk unterwegs waren. Oder, dass Assets, die inaktiv sein sollten, aktiv waren oder sich Skripte auf Laufwerken befinden, über die Angreifer Zugriff auf Admin-Rechte erhalten können. Ein weiterer möglicher Fund: In einer für alle zugänglichen Datei befinden sich Passwörter für Servicekonten. Auch Policy-Verstöße können erkannt werden, etwa wenn E-Mails trotz anderslautender Anweisung als Datei gespeichert oder wenn unerlaubt externe Geräte wie USB-Sticks angeschlossen werden.

Auch weitergehende Security-Konzepte mit Aufbau der Infrastruktur und Passwort Policies können gestartet und bestehende Maßnahmen wie Antivirenlösungen und deren Konfiguration überprüft werden. Damit können Unternehmen Schwachstellen ausmerzen, die Wahrscheinlichkeit künftiger erfolgreicher Angriffe verringern und ihr Sicherheitsniveau langfristig anheben.

Vorteile und Grenzen von Compromise Assessment

Compromise Assessment schafft Sichtbarkeit und erlaubt nach der Installation des Agents, der Server und der Analyse den Blick in die Vergangenheit. Gängige Lösungen wie EDR und SIEM erkennen Probleme erst mit der Installation – und zu diesem Zeitpunkt kann sich bereits ein Angreifer im Netzwerk befinden.

Hinter dem eingesetzten Scanner steht zudem eine große Community: Das hat den Vorteil, dass von Anfang an gute Regeln zur Verfügung stehen und der Scanner immer auf dem neuesten Stand ist. Bis neue Angriffspfade dagegen in einem EDR hinterlegt sind, kann mehr Zeit vergehen, da diese erst dem Hersteller bekannt sein müssen, er sie einbauen und für die Kunden ausrollen muss. Diese Zeit kann allerdings bei der Angriffserkennung entscheidend sein.

Compromise Assessment hat aber auch Grenzen. Es ist eine passive Disziplin, die nicht invasiv und automatisch ins System eingreift und sie ist auch kein Tool für Netzwerksicherheit. Die Scans müssen eingerichtet und manuell angestoßen werden. Gerade anfangs kann dabei Zeit vergehen: Für das Baselining erfolgt zunächst eine Bestandsaufnahme aller Systeme, die gescannt und bewertet werden. Daraus werden Maßnahmen abgeleitet und sie mit einem weite-

ren Scan überprüft. Auch die Auswertung erfordert Fachwissen und Personal und damit ebenfalls Zeit – Compromise Assessment ist keine Disziplin für die Schnellerkennung. Deswegen reicht es allein nicht aus, sondern ist eine sinnvolle Ergänzung etwa zu SIEM und EDR.

Als spezielle Disziplin erfordert Compromise Assessment auch eine gewisse Investitionsbereitschaft, denn es kann teuer werden. Unternehmen beginnen deswegen meistens mit einem Proof of Concept im kleinen Rahmen, sehen das Potenzial und rollen es dann in die Breite aus.

Fazit

Mit Compromise Assessment können Unternehmen ihr IT-Sicherheitsniveau konstant erhöhen. Angriffe und ihre Pfade können mit dem Blick in die Vergangenheit erkannt und der Schaden effizient behoben werden, da die betroffenen Rechner schnell eingegrenzt werden können. Doch auch wenn kein konkreter Angriff vorliegt, kann Compromise Assessment einen guten Überblick über die Schwachstellen des Systems bieten und auf dieser Basis Gegenmaßnahmen eingeleitet werden.

Autoren:

Christoph Lemke, Senior Cyber Defense Consultant

SECUINFRA

Leon Hormel, Cyber Defense Consultant

SECUINFRA

Weitere Informationen:

https://www.secuinfra.com/de/services/compromise-assessment/

Pressekontakt:

SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Mobile: +49 160 921 633 44

marketing@secuinfra.com