Ein Baustein für ein höheres Security Maturity Level

Veröffentlicht 01.04.2021 04:20, Dagmar Finlayson

Compromise Assessment kann ein wertvolles Tool darstellen, um die IT-Security von Kliniken neben traditionellen Maßnahmen wie Vulnerability Management oder Penetrations-Test zu erweitern. Damit können laufende oder vergangene Angriffe detektiert werden. Dennoch müssen sich Krankenhäuser darüber klar sein, dass nur ein ganzheitlicher Ansatz, der auf dem Zusammenspiel von Tools und Knowhow basiert, das Security Maturity Level dauerhaft anheben kann.

Unternehmen setzen in der Regel traditionelle Schutzmaßnahmen wie Vulnerability Management oder Penetrations-Tests gegen Cyberangriffe ein; diese sind allerdings immer schwieriger zu detektieren. Advanced Persistant Threats (APT) zum Beispiel nutzen eigene Tools mit unbekannten Signaturen, die ein IPS (Intrusion Prevention System) oder IDS (Intrusion Detection System) nicht erkennt.

Vulnerability Management oder Penetrations-Tests stellen Momentaufnahmen von der Sicherheit des Systems und der Konfiguration dar. Die Ergebnisse basieren beim Vulnerability Management überwiegend auf den Datenbeständen und beim Penetrations-Test auf dem Fachwissen der Tester. Ohne breites Knowhow und Qualität können die Ursachen von Angriffen nicht ermittelt werden. Penetrations-Test sind zudem invasiv. Da es zu Ausfällen und Mehrkosten kommen kann, sind sie mit hohen Risiken verbunden.

Beide Methoden zeigen nicht auf, ob vorhandene Schwachstellen bereits ausgenutzt wurden. Oft werden Zero-Day-Lücken übersehen: unbekannte Sicherheitslücken, die ausgenutzt werden können, um Schaden anzurichten. Auch einfache Konfigurationsfehler wie zu großzügige Berechtigungsmaßnahmen fallen durch das Raster: Im Active Directory von Windows finden sich häufig Accounts oder Gruppen mit diversen Berechtigungen und schlechten Passwörtern. Im Ernstfall kann darüber die komplette Infrastruktur kompromittiert werden.

Traditionelle oder präventive Maßnahmen reichen also nicht aus, um das Maturity-Level der IT-Security-Infrastruktur von Kliniken zu heben, Angriffe und akute Bedrohungen zu erkennen und darauf zu reagieren. Compromise Assessment kann hier eine wertvolle Ergänzung darstellen: Es ist darauf ausgelegt, Spuren von Angriffen zu finden, die sogenannten IOCs – Indicators of Compromise. Durch ihre Analyse und Bewertung werden kompromittierte Systeme und die zugrundeliegenden Schwachstellen entdeckt und daraus klare Handlungsempfehlungen abgeleitet. Die Ursachen werden in der Remediationsphase behoben und der gewünschte Soll-Zustand hergestellt, um laufende Angriffe zu beenden und künftige zu verhindern. Compromise Assessment ist dabei eine bewertende, keine präventive Disziplin in der IT-Security von Kliniken. Sie betrachtet die gesamte Infrastruktur und ermöglicht einen Blick in die Vergangenheit.

Die Spuren von laufenden und vergangenen Angriffen finden

Ein Angreifer hinterlässt zwangsläufig forensische Artefakte, die für die Auswertung herangezogen werden können. Dies können beispielsweise Log- und Dumpdateien von Angriffswerkzeugen, Dateien mit ungewöhnlichem obfuskiertem Inhalt, Werkzeuge zur Persistenzerzeugung oder schlicht Tools in untypischen Verzeichnissen oder spezifische Konfigurationsschlüssel sein. Es kann sich ebenso um ungewöhnliche Netzwerkverbindungen zu verdächtigen Servern, IP-Adressen und Ports handeln oder um Logdateien von Interaktionen, Anmeldungen und Prozessstarts. Die Anzahl und Vielfalt der in der Praxis detektierbaren IOCs ist dabei durchaus erschreckend.

Alleine das Tool THOR APT Scanner der Nextron Systems GmbH beinhaltet aktuell im Basisregelsatz beispielsweise ca. 18.000 IOCs in 26 verschiedenen Detektionsmodulen. Es wird weltweit von Threat Huntern und Incident Respondern geschätzt.

Gute Tools und breites Wissen um Angriffe schnell zu erkennen

Studien belegen, dass es in der Regel zwei bis drei Monate dauert, bis ein Angriff überhaupt entdeckt wird. Der Schaden wird mit jedem Tag, an welchem der Angreifer unentdeckt bleibt, größer. Über Compromise Assessment kann die Zeit zur Erkennung eines erfolgreichen Angriffs im besten Fall auf wenige Tage reduziert werden. Üblicherweise werden Angriffe kurz nach Beginn der Analyse entdeckt, weil mit den Events der höchsten Hitrate begonnen wird. Maßgeblich dafür ist eine Summe an Tagen, welche sich aus der Scandauer und dem Beginn der Analyse zusammensetzt. Dieser Zeitraum kann je nach Scankonfiguration, Größe des Systems und Anzahl zurückgelieferter Events stark variieren. Eine ungefähre Kenngröße ist eine Woche, da die Scandauer zwischen wenigen Minuten und mehreren Tagen betragen kann und im Anschluss direkt mit der Analyse begonnen wird. Man sortiert die Events nach Schweregrad und beginnt mit den schwerwiegendsten. Allerdings können auch Events mit einem niedrigen Schweregrad Indikatoren für einen Angriff darstellen. Deswegen ist es wichtig, dass die Analysten ein breites Wissen über den Aufbau und die Funktionsweise der Systeme besitzen: Das Ergebnis der Analyse kann nur so gut sein, wie es das Know-How der Analysten zulässt. Die Tools und das zugrundeliegende Regelwerk der IOC-Scanner geben die richtige Richtung vor, die Hinweise müssen dann richtig gedeutet und in Zusammenhang gebracht werden.

Die Notwendigkeit von Continuous Compromise Assessment

Auch wenn ein Compromise Assessment Scan Klarheit über laufende und vergangene Angriffe bringt und einen tiefen Einblick liefert - er bleibt eine Momentaufnahme. Jede Änderung an den Systemen eines Krankenhauses kann Angriffsvektoren beheben, aber eben auch neue schaffen. Deswegen ist ein Continuous Compromise Assessment sinnvoll: Das Scannen nach Angriffsspuren und Analysen auf wiederkehrender Basis. Der initiale Scan ist dabei recht aufwändig, da eventuell Millionen forensischer Artefakte untersucht werden müssen, was mehrere Tage in Anspruch nehmen kann. Die Folgescans und -auswertungen sind bedeutend einfacher, da nur die Änderungen durchleuchtet werden müssen.

Ein Compromise Assessment Scan allein verkürzt nicht die Zeit, bis ein Angriff erkannt wird. Das geschieht nur, wenn alle Maßnahmen aus vorhergehenden Scans umgesetzt und in regelmäßigen Abständen die Systeme erneut gescannt werden. Diese Maßnahmen müssen priorisiert, zeitnah umgesetzt und verfolgt werden, damit das Sicherheitslevel langfristig steigt. Dabei kann es sich zum Beispiel um das Einführen eines zentralisierten Log-Managements oder gar SIEM handeln, das Abändern der Domain Policy und das Einführen eines Berechtigungsmanagements. Es ist auch sinnvoll, Systeme auszutauschen, wenn diese zu alt sind oder der Hersteller den Support eingestellt hat. So können Kliniken ihre Prozesse optimieren und ein Sicherheitslevel erreichen, welches dazu beiträgt, dass neue Angriffe schneller behandelt oder verhindert werden können.

Fazit

Compromise Assessment ist eine exzellente Disziplin, um laufende oder vergangene Angriffe auf Kliniken zu erkennen, zu bewerten und durch entsprechende Maßnahmen in Zukunft zu verhindern. Es kann die IT-Security eines Krankenhauses sinnvoll erweitern, ist alleine aber nicht ausreichend, um dessen Security Maturity Level zu erhöhen. Denn Compromise Assessment ist eine passive Disziplin und muss manuell durchgeführt werden. Erst in Kombination mit anderen Tools und Maßnahmen entsteht ein Kosmos, welcher das gesamte Sicherheitslevel widerspiegelt.

Autor:

Christoph Lemke, Security Consultant SECUINFRA

Kurzvita Christoph Lemke, SECUINFRA:

Christoph Lemke hat bis März 2017 Technische Informatik an der Beuth Hochschule für Technik in Berlin studiert und startete im April 2017 bei SECUINFRA als Cyber Defense Analyst. Seitdem beschäftigt er sich hauptsächlich mit der Erkennung, Analyse und Abwehr von Cyber Angriffen basierend auf SIEM-Lösungen und dem Bereich Digital Forensics. Innerhalb diverser Projekte hat Christoph Lemke bereits erfolgreich die Detektions-Fähigkeiten von SIEM-Infrastrukturen verbessert. Seine Erfahrungen aus den Bereichen Digital Forensics und Incident Response sind dabei in die Entwicklung von SIEM Use-Cases zur Identifkation von selbst herausfordernden Angriffen (sog. Advanced Persistent Threats) eingeflossen.

Quelle Bild: pixapay/TheDigitalArtist