Compromise Assessments – sinnvoll oder Bauernfängerei?

Früherkennung von Schadsoftware

Das Eindringen von Schadsoftware rechtzeitig zu bemerken, etwa durch Compromise Assessments, wird für Unternehmen immer dringlicher. Doch was sind Compromise Assessments überhaupt, und was können sie leisten? Von Mario Emig und Christian Bohr

(Bild: Sikov/adobe.stock.com)

In puncto Cybersicherheit zählt das Jahr 2021 zu den schwärzesten der jüngeren Vergangenheit; die Anzahl von Cyberangriffen und Angriffsvarianten hat weltweit neue Rekordhöhen erreicht. Deutschland gehört neben den USA und Kanada zu den am häufigsten anvisierten Zielen von Cyberangreifern. Unternehmen müssen deshalb das Thema Früherkennung von Infektionen durch Schadsoftware noch ernster nehmen als bisher. Eine mögliche Methode dafür sind Compromise Assessments.

Ein Compromise Assessment ist die Untersuchung eines Netzwerks und seiner Geräte, um Sicherheitslücken, Schadsoftware und Anzeichen für unbefugten Zugriff zu entdecken. Konkret geht es darum, Angreifer ausfindig zu machen, die sich derzeit in der Unternehmensumgebung aufhalten oder in der jüngeren Vergangenheit dort aktiv waren. Wer die Wirksamkeit von Compromise Assessments im eigenen Unternehmen noch nicht erprobt hat, dem begegnen bei der ersten Auseinandersetzung mitunter kontroverse Auffassungen.

Eine dieser Thesen macht etwa den Bock zum Gärtner: *»Compromise Assessments sind schlecht, denn wenn etwas gefunden wird, habe ich einen schlechten Job gemacht«*. Dass Cyberangriffe die Reputation der IT-Abteilung und im Zuge dessen auch den Ruf des Unternehmens beschädigt, diese Befürchtung ist verbreitet und begründet. Allerdings greift die Sorge vor Früherkennung zu kurz, und Ignoranz schützt nicht vor dem Reputationsschaden selbst. Und der tritt in der Regel dann ein, wenn öffentlich bekannt wird, dass das Management verantwortungslos oder fahrlässig mit dem Thema IT-Sicherheit umgegangen ist oder gar keine IT-Sicherheitsstrategie verfolgt hat. Compromise Assessments belegen vielmehr, dass IT-Leiter oder Geschäftsführer ihrer Sorgfaltspflicht nachkommen und alles daransetzen, die IT-Infrastruktur und die digitalen Assets zu schützen. Das gilt erst recht, seit der Corona-bedingte Digitalisierungsschub das Risiko von Cyberangriffen drastisch weiter erhöht hat.

Die Auffassung *»Compromise Assessments bringen nichts; bei uns finden sie sowieso nichts«* negiert die Experteneinschätzung, dass 98,9 Prozent der Unternehmen kompromittiert sind – und zwar ohne es zu wissen. Wer heute glaubt, sein Unternehmen sei bestens gegen Cyberattacken geschützt, bei dem kann sich ein Hacker trotzdem längst eingenistet haben. Aktuellen Studien zufolge treiben Angreifer im Schnitt rund elf Tage unbemerkt in den Unternehmensnetzwerken ihr Unwesen, manchmal bleiben sie sogar über Monate unentdeckt. Dadurch entstehen Kosten, die das bis zu Zehnfache des IT-Budgets betragen können. Nach den bisherigen Erfahrungen gibt es bislang kein Compromise Assessment, das ohne Findings endete.

Einem Missverständnis sitzt die Ansicht auf, dass *»Compromise Assessments in kürzester Zeit Abhilfe bringen, wenn eine Infektion vorliegt«*. Durch ein Compromise Assessment erhält das Unternehmen eine qualifizierte Bewertung seiner momentanen Sicherheits- und Risikolage sowie Klarheit über etwaige schon länger existierende Kompromittierungen. Compromise Assessments sind damit der Wegweiser dafür,

wo die IT-Sicherheitsstrategie noch nicht so wasserdicht ist, wie sie sein sollte. Sie sind nicht die Lösung. Diese liegt in der anschließenden Konzeption und Umsetzung entsprechender Maßnahmen, um die aktuellen Sicherheitslücken zu schließen.

Ist diese Früherkennung damit nur ein Feuerlöscher: *»Compromise Assessments sind nur sinnvoll, wenn ein Breach klar auf der Hand liegt«*? Mitnichten. Compromise Assessments nutzen dem Unternehmen auch, wenn es sich bisher erfolgreich gegen Cyberattacken gewehrt hat. Aber nur, weil das bis gestern der Fall war, muss das nicht morgen auch noch so sein. Das Ziel von Compromise Assessments ist es, durch regelmäßiges Überprüfen der unternehmensweiten Systeme Hackern früher auf die Spur zu kommen, als das ohne Früherkennung gelingen könnte. Finden sich dann wirklich keine Indikatoren für eine Kompromittierung, kann sich das Unternehmen sicher sein, dass sich – aktuell – niemand hinter seinem Rücken an seinen wertvollen Daten und Systemen zu schaffen macht.

Sind *»Compromise Assessments nur für große Unternehmen geeignet«*? Nein, die richtige Argumentationskette verläuft genau entgegengesetzt. Während weltweit agierende Konzerne massiv in ihre IT-Sicherheit investieren, fehlt kleinen und mittelständischen Unternehmen dafür häufig das Budget und/oder das Know-how. Entsprechend anfällig sind gerade sie – auch als Bestandteil von Lieferketten – für Cyberattacken aus dem Netz. Wer diesen Angriffen nicht schutzlos ausgeliefert sein oder gar das Ende seines Unternehmens riskieren will, für den führt kaum ein Weg an Compromise Assessments vorbei. Denn es trifft längst nicht nur die Großen: 2020 und 2021 wurden neun von zehn Unternehmen (88 Prozent) Opfer von Angriffen aus dem Cyberspace – darunter auch zahlreiche kleine und mittelständische Betriebe, die für Hacker viel leichtere Ziele sind.

Können und sollen Compromise Assessments den Fachkräftemangel kompensieren und sind eher *»etwas für schwach besetzte IT-Abteilungen mit einem kleinen Team«*? Compromise Assessments sind in kleineren IT-Abteilungen eine große Hilfe, aber wer will schon – unabhängig von der Größe – seine Ressourcen für die ineffiziente manuelle Identifikation von Malware oder für die Auswertung forensischer Spuren verschwenden? Inzwischen setzen immer mehr Unternehmen auf Compromise Assessments, auch und gerade, wenn sie eine Armada hoch qualifizierter IT-Experten beschäftigen. Denn diese Experten haben wahrlich Besseres zu tun: etwa die IT-Sicherheitsstrategie auf Basis der Findings im Compromise Assessment so weiterzuentwickeln, dass die Organisation kein lohnendes Ziel mehr für Angreifer ist.

Wer die These *»Compromise Assessments sind für verteilte IT-Landschaften ungeeignet«* vertritt, ist offenbar nicht über die Technologie informiert, auf der Compromise Assessments beruhen. Compromise Assessments können Unternehmen mit EDR-Lösungen (Endpoint Detection and Response) darin unterstützen, die Risiken der Homeoffice-Arbeitsplätze gezielt zu überprüfen und potenzielle Sicherheitsverletzungen konsequent zu beseitigen. Sie analysieren Daten und Prozesse in den Endgeräten und identifizieren anomales Verhalten oder Malware. Im Rahmen von proaktivem Threat Hunting werden nicht nur Alarme von EDR-Systemen untersucht, sondern Spezialisten suchen auch in vermeintlich sauberen Systemen nach entsprechenden Angreiferspuren. Denn selbst wenn ein System keine aktive Malware mehr enthält, könnte es in der Vergangenheit Opfer eines Angriffs geworden sein – und dadurch zum Sicherheitsrisiko für das gesamte Unternehmen werden.

Übrigens: Ein Compromise Assessment kann auch hilfreich sein, wenn Unternehmen die Verantwortung für neue Betriebsstandorte oder Abteilungen etwa nach einem Merger übernehmen und sicherstellen wollen, dass sie durch die Integration ihre existierende IT-Landschaft nicht gefährden.

Kein Allheilmittel, aber nicht zu unterschätzen

Compromise Assessments sind kein Allheilmittel und können traditionelle Sicherheitsmaßnahmen nicht ersetzen. Dennoch sind sie sinnvoll, denn Compromise Assessments finden Spuren erfolgreicher Angriffe, die von IPS (Intrusion Prevention Systems) und IDS (Intrusion Detection Systems) nicht erkannt worden und beim Vulnerability Management oder bei Penetrationstests unbemerkt geblieben sind. So unterstützen Compromise Assessments dabei, Lücken in der Detektionsfähigkeit vorhandener Sicherheitslösungen zu ermitteln und damit auch Investitionsbedarf besser zu begründen.

Wer sich einen Partner für Compromise Assessments sucht, sollte darauf achten, dass der Anbieter in der Lage ist, das Unternehmen nicht nur in der Umsetzung der Früherkennung, sondern auch in der Optimierung der IT-Sicherheitsstrategie zu begleiten. Der Kostenumfang von Compromise Assessments wird – je nach Anbieter – meist bestimmt von der Größe der zu untersuchenden Infrastruktur, der begleitenden Analysearbeit und der Anzahl der Endgeräte. Das Investment für ein Compromise Assessment liegt erfahrungsgemäß deutlich unter einem möglichen finanziellen Schaden, den unentdeckte Schadsoftware in Unternehmenssystemen anrichten kann – etwa durch Forderungen von Lösegelderpressern und eine Betriebsunterbrechung durch eine Ransomware-Attacke.

Übrigens: Weil sie einen dauerhaft besseren Schutz vor Cyberattacken anstreben und Sicherheit als kontinuierlichen Prozess begreifen, haben sich 90 Prozent der Auftraggeber von Controlware bislang dafür entschieden, das Compromise Assessment nach den ersten vier Wochen in den Regelbetrieb zu überführen. ak

Mario Emig
ist Head of Information Security bei Controlware.

Christian Bohr
ist Head of Managed Services Consulting bei Controlware.