Breach Detection – finden Sie die Nadel im Heuhaufen

Unternehmen müssen heute davon ausgehen, dass ihre Systeme bereits infiltriert sind oder sie Opfer einer opportunistischen oder gezielten Attacke werden. Heutzutage braucht es neue, mitdenkende Sicherheitsmodelle.

Ernesto Hartmann,
Head of Security Operations, Member of the Management, InfoGuard AG

Hackerangriffe und andere IT-Sicherheitsvorfälle sind nicht nur ärgerlich, sie können auch enorme Kosten und einen riesigen Imageschaden mit sich bringen – und die Bedrohung für sensible Firmendaten durch Cyberangriffe nimmt stetig zu. Gründe sind unter anderem eine Professionalisierung der Werkzeuge und Methoden von Hackern. Aber auch der Umstand, dass dank Bitcoin schnell aus einem Angriff Kapital geschlagen werden kann, was die Anzahl der opportunistischen Attacken massiv erhöht hat. Unternehmen müssen heute davon ausgehen, dass ihre Systeme bereits infiltriert sind. Sie dürfen sich deshalb nicht allein auf Sicherheitsmethoden am Perimeter verlassen. Gelingt es einem Angreifer, in ein Unternehmensnetzwerk einzudringen, kann er sich unbemerkt völlig frei bewegen und unbehelligt Daten klauen. Deswegen braucht es heutzutage neue Sicherheitsdispositive bei welchen die Prevention gesteigert wird und auch die Detektion und Reaktion auf Angriffe miteinbezogen werden. Um bei einer Attacke schnell reagieren zu können, sind Unternehmen gut beraten, wenn sie auf ein Security Operations Team mit geeigneten Werkzeugen zurückgreifen können.

Nur wer Hacker versteht, kann sich auch richtig schützen

Professionelle und erfahrene Hacker sind darauf bedacht, ihre Attacken stets zu modifizieren, um die Aufdeckung zu erschweren. Deswegen wird die Malware permanent verändert oder verschlüsselt, um sicher zu stellen, dass sie keiner bekannten elektronischen Signatur entspricht. Angreifer sind so zwar in der Lage, die Erscheinung der Malware neu zu verpacken, nicht aber das Ziel der Angriffe: nämlich das Ausspionieren, die Verbreitung oder den Datendiebstahl in Netzwerken der Opfer. Diese Verhaltensweisen sind elementar und von grundlegender Bedeutung für eine Attacke - und sie lassen sich beobachten. Hier schlägt die Stunde der Cyber Defence. Sie umfasst die Erkennung von Infiltrationen, die Gruppierung anhand des Angriff-Fortschritts und die Reaktion auf den Angriff.

Falls der Angriff weit fortgeschritten ist, muss man davon ausgehen, dass nicht nur ein einzelnes System betroffen ist. Deshalb braucht es zur Verteidigung technologische Unterstützung in Form einer zentralen Security Intelligence Plattform, wie beispielsweise IBM QRadar und entsprechenden Agenten auf den Endgeräten. Sie sammelt automatisch alle Informationen aus den Infrastrukturkomponenten, vergleicht diese mit externen Threat Feeds und untersucht sie in Echtzeit auf Angriffe. Ergänzt wird dieses System mit Breach Detection Systemen, welche den Datenverkehr mit Hilfe von Data Science, maschinellem Lernen und Verhaltensanalysen durchsuchen und auswerten. Wird ein Angriff erkannt – oder befindet sich ein Angreifer bereits im internen Netz, muss das Cyber Defence Team jederzeit in der Lage sein schnell zu reagieren, indem beispielsweise auf jedem Endgerät eine Analyse gestartet werden kann. Dazu braucht es retrospektive Informationen, welche beispielsweise Systeme wie von Tanium permanent aufzeichnen. Mit diesen Informationen kann sich ein Analyst schnell ein Bild der im Angriff involvierten Prozesse machen. Nur so lässt sich die gesamte Infrastruktur flächendeckend nach «Indicators of Compromice» (IOC), wie Prozess-, File-Hashes, Directory Pfade oder involvierte externe IP-Adressen durchsuchen. Unternehmen welche nur auf präventive Sicherheit bauen, werden APT-Angriffe nicht erkennen können und setzen sich einem erheblichen Risiko aus.

In der heutigen Cyber Security Welt ist jeder Tag ein «Zero Day»

Eine effiziente und zuverlässige Cyber Security muss auf verschiedenen Lösungen und Ansätzen, wie Perimeter Security, Sandboxes und Malware-Protection aufbauen. Immer kombiniert mit Cyber Defence Services, wie APT Detection & Response, Cyber Threat Intelligence und der systematischen Analyse von Bedrohungen mittels SIEM- und Incident Response. Nur so lässt sich die Nadel im Heuhaufen finden und beseitigen.