Von der Krise zum Vertrauen in wenigen Stunden: So wurde Rapid7 zum Security-Sommelier

Was würden Sie tun, wenn Sie herausfinden, dass Ihre Kunden mit Spam belästigt werden, der ihrer Organisation entstammen soll? Ein Horrorszenario für jeden IT-Experten; eines, dass ein Datenleck mit drastischen Auswirkungen auf Ruf und Finanzen anzeigen könnte. Der erste Schritt einer sorgfältigen Reaktion ist der Einblick in die wichtigsten Systeme. Aber wie? Dieser Herausforderung sah sich Liberty Wines vor Kurzem gegenüber. Dank InsightIDR und der schnellen Reaktion von Rapid7 auf eine ernsthafte Sicherheitswarnung ist alles gut ausgegangen.

Der Angriff

Der Cyber-Angriff wurde Anfang 2016 durchgeführt, als IT-Manager Tom Brown auf einer Reise nach Osteuropa war. Nach seiner Rückkehr berichtete ihm sein Team von einem GAU im E-Mail-System: Kunden riefen an und berichteten, dass sie E-Mails von Liberty Wines mit einem ungewöhnlichen Anhang erhielten, der sich als bösartig herausstellte. Gleichzeitig wurde das Team von einer Flut von Fehlermeldungen überschwemmt, die auf fehlgeschlagene Zustellungsversuche hindeuteten. Tom Brown musste sicher gehen, dass es sich hierbei nicht um ein internes Datenleck handelte – deshalb rief er die Experten von Rapid7 zu Hilfe.

Liberty Wines ist ein kleines, aber weltweit operierendes und mehrfach ausgezeichnetes Weinhandelsunternehmen mit Hauptsitz in London. Als IT-Manager betreut Brown 130 Endpoints – eine Mischung aus Desktop-PCs, Smartphones und Laptops, sowie Hosted-Server für E-Mails und einige Server vor Ort. Mit einem Vertriebsteam, das sich von der ganzen Welt aus in das Unternehmensnetzwerk einwählt, und einer bunten IT-Landschaft, wird ihm nie langweilig.

Brown nutzte die Software von Rapid7 schon in der Vergangenheit und kennt Rapid7 als führendes Unternehmen im Security-Bereich. Er hatte zuvor den Bedarf identifiziert, Benutzeranmeldungen und –verhalten aufzuzeichnen und zu analysieren, konnte aber nichts Passendes finden. Außer von Rapid7 gab keine Lösung, die von einem kleinen Betrieb wie Liberty Wines bis zum Einsatz im Großunternehmen skalierte. Die Architektur des InsightIDR-Systems erlaubt den Einsatz in jeder Größe, vom Umfang aber auch von den Einstiegskosten her. Er hatte eine Live-Demo arrangiert, war begeistert und stellte ein Budget zur Installation im nächsten Geschäftsjahr bereit. Die Angreifer hatten aber andere Pläne.

Zurück zum Geschäft

Die Zeit war nun ein kritischer Faktor. Brown kaufte und installierte InsightIDR schnell, um die Transparenz und Tools zu erhalten, die er benötigte, um mit der aktuellen Krise umzugehen. InsightIDR ist eine integrierte Lösung zur Erkennung und Untersuchung, die Analytiken für Nutzerverhalten, Erkennung von Endpoints und eine grafische Suche in Protokollen verbindet, um eine Kompromittierung schnell und effektiv zu finden und einzudämmen. Das Team von Rapid7 arbeitete über drei verschiedene Zeitzonen hinweg eng mit Brown zusammen, um das Problem zu beseitigen. Dank des Quick Start Service von Rapid7 begann das Produkt praktisch sofort mit der Sammlung und Analyse von Verhalten, um Liberty Wines die Echtzeit-Informationen zu bieten, die zur zuverlässigen Identifikation der Kompromittierung benötigt werden.

Die Lösung durchsuchte die Systeme nach horizontaler Ausbreitung, Privilegien-Eskalation, ungewöhnlicher Nutzung von Zugängen für Dienste, Anmeldungen von ungewöhnlichen Orten und Geräten aus usw. Glücklicherweise gab es keinerlei Hinweise auf derartige Aktivitäten. Es entstand der Verdacht, dass die bösartigen Aktivitäten von einem Kunden ausgingen. Die Hacker hatten eine echte E-Mail von Liberty Wines kopiert und sie einschließlich eines bösartigen JavaScript-Anhangs massenweise an Millionen Internet-Nutzer versendet.

Das Rapid7-Team rekonstruierte und analysierte die fragliche Malware, um sicher zu gehen, dass Liberty Wines nicht betroffen war. In Verbindung mit der Echtzeit-Transparenz durch InsightIDR war Brown in der Lage, eine klare und detaillierte grafische Zeitachse der Ereignisse für die Vorstände von Liberty Wines aufzuzeichnen und die Kunden über die genaue Situation zu informieren. Nexpose, die führende Schwachstellen-Management-Lösung von Rapid7, wurde außerdem darauf angesetzt, jegliche potenziellen Schwachstellen im Aufbau der IT-Sicherheit bei Liberty Wines zu identifizieren.

Beständiges Vertrauen

Tom Brown war begeistert von der Geschwindigkeit und Genauigkeit, mit welcher der Störfall untersucht wurde. Rapid7 konnte InsightIDR innerhalb von Stunden in die Umgebung von Liberty Wines integrieren. Diese Geschwindigkeit ist im Fall einer möglichen Datenschutzverletzung unerlässlich, denn je länger ein Angreifer sich innerhalb eines Systems aufhält, um so größer ist der potenzielle finanzielle und indirekte Schaden.

„InsightIDR ist ein großartiges System. Es gibt Ihnen ein beruhigendes Gefühl, da es jegliches verdächtiges Verhalte im Netzwerk abfängt, bevor Sie es anderweitig entdecken," sagt Brown. „Die meisten IT-Manager akzeptieren, dass irgendjemand am Ende doch durchbricht, dass es irgendeine Lücke gibt. Deshalb geht es darum, schnell herauszufinden, wo die Lücke ist, und

„InsightIDR ist ein großartiges System. Es gibt Ihnen ein beruhigendes Gefühl, da es jegliches verdächtiges Verhalte im Netzwerk abfängt, bevor Sie es anderweitig entdecken."

„Sie denken anders über verschiedene Dinge. Die IT wird stets mit verschiedenen Anforderungen konfrontiert, aber dank Nexpose und InsightIDR habe ich die Möglichkeit, dem Kunden zu sagen: ‚Es geht so nicht, denn das ist nicht sicher.'"

schnelle Abhilfe zu schaffen. Das ist die Aufgabe von InsightIDR. InsightIDR half mir zudem, unsere Anwender jeden Tag besser zu verwalten."

Obwohl es kein Anzeichen für ein Datenleck gab, zeigte die neue Transparenz über Nutzer und Endpoints Liberty Wines einige Bereiche auf, in denen Maßnahmen nötig waren, insbesondere bei der Sicherheit der Benutzerkonten. Der gesamte Prozess zur Verwaltung des Personals von Liberty Wines ist jetzt effizienter und sicherer dank der granularen Transparenz, die InsightIDR bietet. Sie erlaubt Tom Brown zu sehen, wenn ein Anwender beispielsweise geschäftliche e-Mails von einem nicht verwalteten mobilen Gerät abruft oder sich aus dem Ausland einwählt. InsightIDR und Nexpose, die Schwachstellen-Management-Lösung von Rapid7, haben Tom Brown geholfen, ein effektiverer IT-Manager zu werden, wie er selbst sagt.

„Sie denken anders über verschiedene Dinge. Die IT wird stets mit verschiedenen Anforderungen konfrontiert, aber dank InsightIDR habe ich die Möglichkeit, dem Kunden zu sagen: ‚Es geht so nicht, denn das ist nicht sicher.'"
Tatsächlich war Tom Brown dank Nexpose der erste, der beziffern und nachweisen konnte, dass alte, nicht produktive Server, die aus Referenz-Gründen weiter betrieben wurden, ein großes Sicherheitsrisiko darstellten. Mit der Unterstützung der Geschäftsleitung konnte er die alten Server komplett abschalten und damit dieses Risiko eliminieren.
Mit diesen Ergebnissen verwundert es kaum, dass Tom Brown die Partnerschaft zwischen Liberty Wines und Rapid7 ausbauen möchte. Für die neue Website hat er bereits das Budget für einen Penetration Test bereit gestellt, damit die Seite „bombensicher" ist, wenn sie live geht. Und er plant darüber hinaus weitere Investitionen in Rapid7 Security Awareness Training.
Der Zwischenfall mag kein Datenleck gewesen sein, aber dank der umfassenden Reaktion von Rapid7 ist Liberty Wines jetzt in der Lage, die Verwaltung des Personals und die Sicherung der IT-Bestände in einer effektiveren, proaktiven Weise durchzuführen. Das ist etwas, worauf wir alle anstoßen können.

RAPID7