Warum Unternehmen heute mehr denn je konvergente Sicherheit benötigen

Das Thema Cybersicherheit ist mittlerweile zu einem globalen Problem geworden und rückt deshalb immer stärker in den Mittelpunkt. Erst kürzlich wurde das Thema auf Betreiben von US-Präsident Biden und dem russischen Präsidenten Putin ganz oben auf die Tagesordnung des Genfer Gipfels 2021 gesetzt. Angesichts der Tatsache, dass die Zahl der Ransomware-Angriffe im März letzten Jahres um fast 150 % gestiegen ist und in der ersten Hälfte des Jahres 2021 ein Anstieg um 102 % zu verzeichnen war, sind die weitverbreiteten Sorgen durchaus berechtigt.

Versäumnisse bei der Cybersicherheit führen zunehmend zu schwerwiegenden Auswirkungen in der physischen Welt, wo sowohl kritische Infrastrukturen als auch das Leben von Menschen gefährdet sind. Nehmen Sie zum Beispiel den Hack des Wasserwerks in Florida im Jahr 2021. Eine Netzwerkverletzung wurde schnell zu einem physischen Angriff, der die Wasserversorgung einer Stadt mit einer gefährlichen Laugenkonzentration zu vergiften drohte.

Trotzdem betreiben viele Unternehmen ihre Teams für Cybersicherheit und physische Sicherheit nach wie vor als getrennte Bereiche, die bei der Krisenbewältigung kaum oder gar nicht zusammenarbeiten.

Was ist die Lösung? Da cyber-physikalische Bedrohungen immer mehr zunehmen, ist es für Unternehmen von strategischer Bedeutung, beiden Teams die nötige Basis für eine formelle Zusammenarbeit zu bieten. Das führt laut der U.S. Cybersecurity and Infrastructure Security Agency (CISA) zu integrierten Lösungen für die Cybersicherheit und die physische Sicherheit, die resilienter und besser ausgestrattet sind, Bedrohungen zu erkennen, zu verhindern, abzumildern und darauf zu reagieren.

Wie konnte es dazu kommen?

Bislang sind in den meisten Unternehmen die Teams für die physische Sicherheit und die Cybersicherheit voneinander unabhängig. Das liegt zum Teil an dem relativen Alter der beiden Verfahren. Die physische Sicherheit hat eine lange Geschichte, während die Cybersicherheit vergleichsweise neu ist.

Dataminr

Aber dank der zunehmenden Verwendung von IoT- und IIoT-Geräten, der Verlagerung von Systemen in die Cloud und der Verbreitung von sozialen Medien und intelligenten Geräten ist die Notwendigkeit einer branchenübergreifenden Sicherheitskonvergenz größer denn je.

Einige Beispiele für cyber-physische Risiken sind offensichtlicher, wie der Ransomware-Angriff auf das irische Gesundheitssystem im Mai 2021. Er führte zu einem systemweiten IT-Ausfall, der eine reale und unmittelbare Bedrohung für die Patienten darstellte. Oder der bereits erwähnte Angriff auf die Wasseraufbereitungsanlage in Florida.

Andere Beispiele sind nicht so offensichtlich, stellen aber dennoch ein erhebliches Risiko dar. Zum Beispiel die jüngste Zunahme von Angriffen auf mit dem Internet verbundene industrielle Kontrollsysteme (ICS), insbesondere solche, die kritische Infrastrukturen betreiben – von Wasseraufbereitungs- und Gasanlagen bis hin zu Zügen und Ampelsystemen. In einigen Fällen nutzen Hacker Sicherheitslücken in den Zugangskontrollen zu den Anlagen aus und können so Malware installieren, die das gesamte Netzwerk eines Unternehmens kompromittiert. Software für den Fernzugriff zur Steuerung von ICS und Heizungs-, Lüftungs- und Klimaanlagen sind ebenfalls häufige Einfallstore für Angriffe, die sowohl die Cybersicherheit als auch den physischen Bereich betreffen.

Der Ruf nach besserer Kontrolle über konvergierende Bedrohungen

Vorausschauende Unternehmen verschmelzen zunehmend ihre Teams für Cybersicherheit und physische Sicherheit, um ihre Sicherheitslage insgesamt zu verbessern. Die Verschmelzung der beiden Bereiche ist jedoch noch nicht das vorherrschende Modell für Sicherheitsoperationen. Einige Experten warnen davor, dass Unternehmen mit getrennten Teams blinde Flecken im Betrieb und eine schwächere Sicherheitslage riskieren. Wenn beispielsweise eine neue Bedrohung auftaucht, konzentrieren sich die Sicherheitsexperten oft nur auf ihren Zuständigkeitsbereich und wissen kaum etwas darüber, was auf der anderen Seite des Hauses passiert. So können die Teams für Cybersicherheit und physische Sicherheit aufkommende Bedrohungen nicht ganzheitlich betrachten.

Es kann eine Herausforderung sein, das Fachwissen von Führungskräften und Teams für Cybersicherheit und physische Sicherheit zu integrieren. Oft gibt es kulturelle und fachliche Unterschiede zwischen den beiden, was dazu führt, dass sie die Welt sehr unterschiedlich sehen. Solche Unterschiede können die Kommunikation behindern oder sogar zu Fehlkommunikation führen. Das sind zwei der größten Probleme, mit denen Unternehmen konfrontiert sind, die noch keine soliden Prozesse entwickelt haben, um die Zusammenarbeit zwischen diesen beiden wichtigen Teams zu fördern.

Hinzu kommen logistische Hürden und ein mangelndes Verständnis auf der Führungsebene, warum die Sicherheitskonvergenz nicht länger ein schönes Extra ist, sondern ein absolutes Muss.

Wenn Sicherheitsteams ihre Kräfte bündeln

Wenn Teams für Cybersicherheit und physische Sicherheit eng zusammenarbeiten, ergeben sich daraus viele Vorteile:

- Eine stärkere, ganzheitlichere Sicherheitsposition
- Schnellere Erkennung und Bewertung von und Reaktion auf Bedrohungen, die sowohl in den Cyberbereich als auch in den physischen Bereich fallen
- Bessere Kommunikation und gemeinsame Nutzung von Informationen und Technologien
- Gesteigerte Effizienz und bessere Ergebnisse

Zwar wird jedes Unternehmen die zunehmende Konvergenz von physischen und Cyberrisiken anders handhaben und darauf reagieren, aber Echtzeitinformationen sind das Herzstück ihrer Fähigkeit, dies zu tun. Unternehmen müssen sicherstellen, dass alle Sicherheitsteams gleichberechtigten Zugang zu Echtzeitdaten über aufkommende und potenzielle Risiken haben, unabhängig davon, wo oder wie die Bedrohung ihren Anfang nimmt, und einen klaren Prozess dafür schaffen, wann und wie diese Informationen übermittelt werden und welche Stakeholder sie erhalten sollen.

Die Fähigkeit, diese cyber-physischen Ereignisse und Risiken so früh wie möglich zu erkennen, ist von entscheidender Bedeutung. Aus diesem Grund verlassen sich die Geschäftskunden von Dataminr auf Dataminr Pulse, um die frühesten Signale von Ereignissen mit großer Auswirkung und aufkommenden Risiken zu erkennen.

Als Colonial Pipeline im Mai 2021 von einem Ransomware-Angriff betroffen war, alarmierte Dataminr Pulse unsere Kunden einen Tag vor den großen Medien über die damit verbundenen Netzwerkprobleme. Und Pulse berichtete auch weiterhin über den Vorfall, während er sich entwickelte, und lieferte den Kontext, den unsere Kunden brauchten, um fundierte Entscheidungen zu treffen.

In dem Maße, wie die Technologie voranschreitet und immer mehr in unsere Arbeits- und Lebensweise integriert wird, ist mit einer Zunahme von cyber-physischen Bedrohungen wie dem Angriff auf die Colonial Pipeline zu rechnen. Um solchen Risiken einen Schritt voraus zu sein und sie effizient einzudämmen, müssen Sicherheitsverantwortliche – unabhängig von ihrem Fachgebiet oder Schwerpunkt – sicherstellen, dass ihre Teams zusammenarbeiten und gemeinsam Informationen, Tools, Fähigkeiten und Ressourcen nutzen, um Bedrohungen abzuwehren.

Erfahren Sie mehr über die Leistungsfähigkeit der Echtzeitwarnungen von Dataminr Pulse und sehen Sie sich dieses On-Demand-Webinar an, um mehr über die Notwendigkeit der Sicherheitskonvergenz zu erfahren.

Al Bowman ist ein Enterprise Account Manager bei Dataminr. Bevor er zu Dataminr kam, entwickelte, etablierte und leitete er das Intelligence Services Center von Deloitte in London. Davor diente er in der britischen Armee, wo er zuletzt als Direktor des globalen Risiko- und Aufklärungszentrums tätig war.

Dataminr