Datum: 19.10.2016

Schweizer Fachzeitschrift für Sicherheit

SICHERHEITSFORUM

Sicherheitsforum
8127 Forch
043/ 366 20 20
www.mediasec.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 3'650
Erscheinungsweise: 6x jährlich

Themen-Nr.: 663.078
Abo-Nr.: 1095967
Seite: 32
Fläche: 77'635 mm²

Das Netzwerk schützen

Trotz unterschiedlicher Umgebungen haben Security-Verantwortliche meist die gleiche Sorge: Wie lässt sich heute ein Unternehmensnetzwerk umfassend schützen?

© depositphotos

Von Franz Kaiser

Die Frage nach dem Schutz wird von unterschiedlichen Faktoren beeinflusst, die effiziente und grenzenlose Lösungen erfordern. Mit Blick auf aktuelle Bedrohungen lassen sich fünf grosse Security-Bedenken ausmachen, die jede Branche gleichermassen beschäftigen.

1. Sicherheit von Cloud-Applikationen

Cloud-Computing-Entwicklungen sind kaum mehr aufzuhalten. Immer mehr Mitarbeitende nutzen öffentliche Cloud-Applikationen für arbeitsbezogene Themen. Diese Anwendungen reichen von E-Mail-Services wie Gmail über öffentliche Speicherdienste wie Dropbox bis hin zu Chat-Software wie WhatsApp auf mobilen Geräten. Es wird immer schwieriger, diese Applikationen zu sperren. Daher gehören das Applikationsmanagement sowie die Verminderung der Risiken zu den obersten Prioritäten für Sicherheitsverantwortliche.

Datum: 19.10.2016

Schweizer Fachzeitschrift für Sicherheit

SICHERHEITSFORUM

Sicherheitsforum
8127 Forch
043/ 366 20 20
www.mediasec.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 3'650
Erscheinungsweise: 6x jährlich

Themen-Nr.: 663.078
Abo-Nr.: 1095967
Seite: 32
Fläche: 77'635 mm²

2. Advanced Persistent Threats

Von allen aktuellen Sicherheitsbedrohungen zählen die Advanced Persistent Threats (APTs) zu den am meisten gefürchteten. Diese unterscheiden sich von anderen Bedrohungen aufgrund ihrer Raffinesse, ihres mehrstufigen Ansatzes, ihrer heimtückischen Natur und einer zielgerichteten Angriffsweise. APTs haben vertrauliche, geschäftskritische Informationen und persönliche Daten wie Kredit- und Patientenkarteninformationen im Visier. Somit sind nicht nur grosse Unternehmen, sondern auch Einzelpersonen mögliche Ziele.

3. Event Management

Data Logging, Reporting und Event Management gewinnen zunehmend an Bedeutung im Kampf gegen komplexe Bedrohungen (z. B. APTs) und gehören somit seit vielen Jahren zu den Aufgaben eines Systemadministrators. Trends wie intelligente Städte, das Internet of Things (IoT) und Big Data sind hier starke Treiber. Die Bedeutung lässt sich anhand des Wachstums auf dem Markt für Security-Informationen und Event Management (SIEM) erkennen, der laut dem Unternehmen MarketsandMarkets von 2,47 Milliarden US-Dollar im Jahr 2014 auf 4,54 Milliarden US-Dollar im Jahr 2019 ansteigen soll. Unstrukturierte Informationen über einen Angriff sind fast so bedeutungslos wie keine Informationen. Daher müssen zuerst alle Event-Logs von sämtlichen Netzwerk-, Server- und Security-Geräten konsolidiert und dann entsprechend analysiert werden, um zum gewünschten Ergebnis zu gelangen.

4. Compliance

Richtlinien und Standards gehören zum Alltag. Die Einhaltung dieser Richtlinien kann allerdings kostspielig und kompliziert werden. Security-Entscheider beschweren sich, dass Zeit- und Kostenaufwand von Compliance-Massnahmen zu hoch sind und die strategischen Geschäftsziele dadurch in den Hintergrund geraten.

Die «Security Fabric» als Lösungsweg: Diese unterschiedlichen Sorgen deuten darauf hin, dass nur ein ganzheitlicher Ansatz Abhilfe schaffen kann – eine «Sicherheitsfabrik», die Hardware, Software und Kommunikationsprotokolle mit interner Segmentierung in einer einzigen Architektur vereint. Kunden erhalten damit einen nahtlosen, umfassenden Schutz vor Bedrohungen über die komplette Angriffsfläche hinweg, die aufgrund von Cloud- und IoT-Technologien stetig wächst.

Vor allem die Cloud ist als eine Erweiterung des Unternehmensnetzes zu sehen. Betriebe brauchen eine Sicherheitsstrategie, die vorsieht, die grossen Datenmengen im grenzenlosen Netzwerk erkennen und kontrollieren zu können. Damit sind kabelgebundene sowie drahtlose Zugangspunkte, öffentliche und private Netzwerke, traditionelle wie auch cloudbasierte Infrastrukturen gemeint.

Um APTs wirkungsvoll zu bekämpfen, müssen Unternehmen über die Grenzen traditioneller Perimeter-Firewalls und üblicher mehrschichtiger Abwehrmechanismen hinausschauen. Eine effektive APT-Strategie erfordert den Einsatz einer sogenannten Internal-Segmentation-Firewalling (ISFW)-Architektur. Eine ISFW schränkt die Verbreitung von Malware zwischen unterschiedlichen Bereichen eines Unternehmens ein. Im Zusammenspiel mit Echtzeit-Bedrohungsintelligenz und APT-Erkennungstechnologien wie Sandboxing und End-

Datum: 19.10.2016

Schweizer Fachzeitschrift für Sicherheit

SICHERHEITSFORUM

Sicherheitsforum
8127 Forch
043/ 366 20 20
www.mediasec.ch

Medienart: Print
Medientyp: Fachpresse
Auflage: 3'650
Erscheinungsweise: 6x jährlich

Themen-Nr.: 663.078
Abo-Nr.: 1095967
Seite: 32
Fläche: 77'635 mm²

point-Security lassen sich APTs schnell erkennen und sperren. Ein weiterer Faktor bei der Bekämpfung von APTs ist ein guter Logging-Mechanismus, der den kompletten Datenverkehr im Netzwerk – sowohl intern als auch extern – erfasst und interpretiert. Eine Security Fabric, die Transparenz über Devices, Benutzer, Inhalte und ein- und ausgehende Daten sowie eine Analyse von Verkehrsmustern bietet, leistet hier Hilfestellung. Darüber hinaus kann eine «Fabric» den Logging-Prozess optimieren, indem eine Session nur einmal protokolliert wird. Das macht es einfacher, Muster im Netzwerkverkehr und damit die echten Bedrohungen zu erkennen.

Bezüglich Compliance setzen die meisten Security-Verantwortlichen bestimmte Methoden zur Risikominderung ein. Eine «Sicherheitsfabrik» mit ISFW zeigt ein detaillierteres Bild des aktuellen Compliance-Status und bewertet darüber hinaus den Sicherheitsgrad. Damit können Unternehmen besser verstehen, welche Bereiche des Netzwerkes besonders gefährdet sind, und in weiterer Folge entsprechende Massnahmen ergreifen.

Um die Sicherheitslage und Effektivität anderer Richtlinien und Prozesse zu verstehen, muss ein Security-Verantwortlicher wissen, was genau, zu welchem Zeitpunkt mit dem Netzwerk verbunden ist. Eine «Security Fabric» erkennt sämtliche Netzwerkressourcen, ermöglicht die Erstellung von Sicherheitszielen und überprüft die Richtlinien für alle «Fabric»-Knoten, um festzustellen, ob die für jedes Asset geeigneten Schutzmassnahmen umgesetzt werden.

5. Investitionsschutz

Eine «Sicherheitsfabrik» adressiert auch die fünfte Sorge eines Security-Verantwortlichen – nämlich Investitionsschutz. Eine solche Architektur wird von Grund auf so entwickelt, dass sie mit den wesentlichen Bestandteilen eines Netzwerkes arbeitet. Auch wenn sich die einzelnen Netzwerkkomponenten verändern, bleibt die solide Grundlage der «Fabric» relevant und wird das Unternehmen auch in Zukunft schützen. ■

FRANZ KAISER
Regional Vice President Alps bei Fortinet