DER UMFASSENDE LEITFADEN ZUR AKTUELLEN BEDROHUNGSLANDSCHAFT

Der Übergang zur digitalen Wirtschaft erfordert sich schnell entwickelnde Netzwerke. Anwendungen, Daten und Dienste müssen schneller und in größeren Volumina an ein zunehmend vielfältigeres Spektrum von Benutzern, Domänen und Geräte übertragen werden. Damit Schritt zu halten, ist nur ein Teil der Herausforderung. Die grundlegende Frage ist: Wie bewahren Sie das Gleichgewicht zwischen diesen Möglichkeiten einerseits und den Risiken andererseits? Das IoT und cloudbasierte Anwendungen sowie Infrastrukturen führen dazu, dass Organisationen sich um eine Angriffsfläche kümmern müssen, die für die IT möglicherweise nicht einmal zu sehen ist.

Durch die steigende Zahl von spektakulären Datendiebstählen und das zunehmende Bewusstsein der Vorstände über ihre finanzielle Haftung hat sich Cyber-Sicherheit zu einer Risk Management-Aufgabe entwickelt. CISOs konzentrieren sich auf das Risiko-Management, welches mit der Verlagerung von Geschäftszielen und Prozessen einhergeht. Sie messen die Risiken von Geräten, Diensten und Protokollen, die sie implementieren müssen, um diese Ziele zu erreichen, formulieren ihre Risikotoleranz und erstellen schließlich einen Plan, um dieses Risiko zu minimieren. Dabei müssen folgende Probleme berücksichtigt werden:

- Der digitale Fußabdruck von Unternehmen und Personen hat sich deutlich erweitert, wodurch auch die potenzielle Angriffsfläche erheblich größer geworden ist.
- Alles kann zum Ziel werden und alles kann als Waffe dienen.
- Bedrohungen werden intelligent, können autonom agieren und sind immer schwieriger zu erkennen.

Teil der Herausforderung ist, dass das Problem nicht in einem völlig neuen Bereich aufgetaucht ist. Ihr IT-Team hat bereits Dutzende Sicherheitslösungen von einer Vielzahl von Anbietern bereitgestellt. Leider waren diese Tools nicht dafür konzipiert, die verteilten, grenzenlosen und zunehmend transienten Netzwerke zu schützen. Diese traditionellen Sicherheitstools agieren häufig isoliert voneinander, sie haben getrennte Konfigurations- und Management-Konsolen und erfordern eine langwierige manuelle Korrelation, um komplexe Angriffe zu erkennen und auf sie zu reagieren. Aus diesem Grund gelingt es zahlreichen neuen Bedrohungen, sich monatelang innerhalb der Netzwerke zu halten, bevor sie entdeckt werden.

Der Kauf neuer Hardware für Ihr Netzwerk, um einem neuen Netzwerksegment oder einem Bedrohungsvektor zu begegnen, ist keine vernünftige Strategie mehr. Dieser Ansatz birgt das Risiko, die bereits bestehende Komplexität der Umgebung weiter zu verstärken und damit die begrenzten verfügbaren Ressourcen für das Konfigurieren, Integrieren, Überwachen, Verwalten und Korrelieren dieser neuen Tools zu überfordern. Wie Ihre Netzwerke muss auch die Sicherheit neu gedacht werden.

In diesem White Paper werden die fünf neuesten Netzwerktrends untersucht und warum sie ein echtes Risiko für

WHITE PAPER

Ihr Unternehmen darstellen. Es werden Wege für die Implementierung einer neuen Sicherheitsstrategie aufgezeigt, die es Ihnen erlaubt, die Möglichkeiten der digitalen Wirtschaft vertrauensvoll zu nutzen.

1. DAS INTERNET DER DINGE (IoT)

Experten sagen voraus, dass bis 2020 für jeden Mann, jede Frau und jedes Kind weltweit 4,3 internetfähige Geräte vorhanden sein werden. Die Einnahmen durch das IoT werden für 2020 auf 300 Milliarden USD geschätzt, bei einer globalen Wirtschaftsleistung von 1,9 Billionen USD.

Es gibt drei verschiedene Gruppen von IoT-Geräten, von denen Ihr Unternehmen sehr wahrscheinlich mindestens zwei nutzt.

Das erste, das Consumer-IoT, umfasst alle verbundenen Geräte, mit denen wir am besten vertraut sind, wie Smartphones, Uhren und Autos sowie verbundene Geräte und Unterhaltungssysteme. Viele dieser Geräte gehören Ihren Mitarbeitern, Kunden und Gästen. Diese möchten die Geräte mit Ihrem Netzwerk verbinden, um ihre E-Mails und Kalender zu prüfen, auf das Internet zuzugreifen und mit anderen zu kollaborieren.

Die anderen beiden, das kommerzielle IoT und das industrielle IoT, bestehen aus Dingen, die die meisten normalen Verbraucher nie zu sehen bekommen. Das kommerzielle IoT umfasst beispielsweise Lagerbestandsprüfung, Geräteverfolgung und verbundene medizinische Geräte. Das industrielle IoT umfasst verbundene Zähler und Pumpen, Pipeline-Überwachung, Fertigungsflächen und automatisierte industrielle Kontrollsysteme. Durch die IoT-Implementierung erhalten Sie Zugriff auf kritische Echtzeitinformationen, die Produktivität und Effizienz wird verbessert und Sie verschaffen sich einen echten Wettbewerbsvorteil.

Die Security-Herausforderungen des IoT sind jedoch erheblich und gehen in die Tiefe und die Breite. Bei der Konzeption vieler IoT-Geräte wurden Sicherheitsfragen außer Acht gelassen. Sie verfügen häufig über schwache Authentifizierungs- und Autorisierungsprotokolle, einfach nutzbare Software und Firmware, schlecht gestaltete Kommunikationssysteme und wenig bis gar keine konfigurierbaren Sicherheitsfunktionen. Viele sind „headless“ (ohne Bildschirm), das heißt, Sie können auch keine Sicherheitsclients auf ihnen installieren oder Updates bzw. Patches nutzen.

Infizierte oder kompromittierte IoT-Geräte können Malware verbreiten und sensible Daten stören oder stehlen. Wie im vergangenen Herbst zu sehen war, können anfällige IoT-Geräte als Waffen verwendet werden und massive Geschäftsunterbrechungen und Denial-of-Service-Angriffe durchführen. Und wenn Ihre IoT-Geräte mit Betriebssystemen interagieren, wie etwa Fertigungsumgebungen oder kritische Infrastrukturen, können die Folgen einer Kompromittierung verheerend sein.

2. ÜBERGANG ZUR CLOUD

Laut Forbes werden in den kommenden Jahren 92 % der Rechenlasten von Cloud-Rechenzentren verarbeitet und nur noch 8 % weiterhin von traditionellen Rechenzentren. Die Möglichkeit die Kapital- und Betriebskosten durch den Kauf von Hardware-Infrastruktur und Software Tools ist ein zentraler Faktor bei der Einführung von Cloud-Computing. Dies gilt insbesondere, wenn Organisationen in die Zukunft schauen und die sich abzeichnenden Datenvolumina berücksichtigen, die sie verarbeiten müssen, um auf dem digitalen Marktplatz weiter zu bestehen.

Die meisten CEOs und CIOs nennen jedoch gleichzeitig Sicherheit als vorrangigen Faktor, der sie vom Wechsel zu einem umfassenden Cloud-basierten Modell abhält. Die Ausweitung Ihres Netzwerks in die Cloud vergrößert zwangsweise auch Ihre potenzielle Angriffsfläche. Die größte Sorge ist, dass die Cloud häufig ein schwarzes Loch für die IT-Teams darstellt. Sie können ihre Daten nicht sehen, nicht nachvollziehen, wo sie gespeichert werden, wer auf sie zugreift oder ob ihre lokalen Sicherheitsprotokolle angemessen durchgesetzt werden, wenn die Daten ihre Umgebung verlassen.

Wie beim IoT gibt es auch eine Vielzahl verschiedener Clouds. Public Clouds existieren außerhalb Ihrer lokalen Domäne und bieten eine Reihe von Diensten, vom einfachen Speicherplatz über Cloud-basierte Anwendungen oder On-Demand-Rechendienste bis zu vollständigen Plattform- und Infrastrukturlösungen, einschließlich Consulting, Design, Integration, Anwendungsentwicklung und Software-Dienste. Private Clouds erweitern Ihr traditionelles Netzwerk durch virtuelle Geräte und ermöglichen es Ihnen, Gemeinkosten und Ressourcen besser zu verwalten und gleichzeitig zahlreiche IT-Funktionen zu automatisieren, die früher manuelle Eingriffe erforderten.

Nahezu alle Cloud-Anbieter stellen eine Vielzahl von Sicherheitslösungen und SLAs bereit, die Ihr geistiges Eigentum schützen. Vor dem Übergang zur Cloud müssen jedoch weiterhin eine Reihe von Sicherheitsproblemen berücksichtigt und verstanden werden.

- Kann ich meine Daten auf ihrer Übertragung zwischen Cloud-Umgebungen sehen und verfolgen?
- Wie verhindere ich, dass meine Daten bei nicht zugelassenen Cloud-Service Providern gespeichert werden?
- Welche Tools sind verfügbar, um meine Richtlinien unabhängig vom Speicherort meiner Daten konsistent durchzusetzen?
- Kann ich schadhaften Datenverkehr, der aus meiner Cloud-Umgebung kommt oder dorthin eingedrungen ist, sehen und entsprechende Reaktionen ergreifen?

Das schwächste Glied für die Cloud-Sicherheit ist jedoch nicht in seiner Architektur zu finden, sondern in den Millionen Geräten, die auf Cloud-Ressourcen zugreifen. Cloud-Sicherheit hängt davon ab, wie kontrolliert wird, wer in das Netzwerk gelangt und in welchem Umfang diesen Teilnehmern vertraut wird. Es ist zu erwarten, dass mehr Angriffe auf Endgeräte zu verzeichnen sein werden, die auf Cloud-Anbieter und ihre Daten abzielen.

3. RANSOMWARE

Wenngleich mehr Geld und Ressourcen als jemals zuvor aufgewendet werden, gelingt es ausgeklügelten Angriffen weiterhin, die Abwehrmechanismen von Organisationen zu überwinden und damit in die Schlagzeilen zu gelangen. Dies liegt zum einen daran, dass die Angreifer immer intelligenter vorgehen und daher schwieriger zu entdecken sind. Zum anderen liegt es aber auch an der menschlichen Natur. Irgendeine Person in Ihrem Unternehmen wird dazu verleitet, auf einen infizierten Link oder Anhang zu klicken, wodurch ein Schadcode in Ihr Netzwerk eindringen kann – unabhängig davon, wie oft vor solchen Möglichkeiten gewarnt wird.

Der Hauptgrund für die meisten Cyber-Angriffe ist finanzieller Natur. Dies wird ganz besonders anhand der dramatischen Zunahme von Ransomware deutlich. Einige Experten gehen davon aus, dass die Gesamtkosten durch Ransomware für 2016 eine Milliarde Dollar überstiegen und dieser Erfolg sehr wahrscheinlich weiteres Wachstum befeuert.

Natürlich ist es nicht völlig neu, dass große Vermögenswerte als Geisel gehalten werden. Es ist jedoch auch das Aufkommen eines neuen besorgniserregenden Trends in diesem Bereich zu beobachten. Ransomware-as-a-Service ermöglicht es Cybercrime-Neulingen, praktisch ohne jegliche technische Schulung oder Kompetenzen tätig zu werden. Neue, Cloud-basierte „Franchise-Angebote“ bieten Zugriff auf komplexe Hacking- und Ransomware-Tools im Tausch gegen eine niedrige Vorauszahlung und kombiniert mit einer späteren Erfolgsbeteiligung. So sagen Experten voraus, dass Ransomware weiterhin exponentiell zunehmen wird, auch weil sie in der Lage ist, kosteneffizient auch auf kleinere Organisationen in weniger traditionellen Märkten abzuzielen.

Während Organisationen weiterhin breit angelegte Angriffe auf Ziele mit einem hohen Wert, wie Rechenzentren oder Kommunikationssysteme, durchführen werden, werden wahrscheinlich auch gezielte Angriffe auf geistiges Eigentum oder sensible oder persönliche Daten und deren Geiselnahme zunehmen.

Es ist auch zu erwarten, dass die geforderten Lösegeldzahlungen wesentlich ansteigen. Die Folgen für die betroffenen Organisationen gehen jedoch weit über den Geldwert hinaus. Öffentlich durchgeführte Ransomware-Angriffe können das Vertrauen von Verbrauchern untergraben und den Markenwert senken. Und für einige Organisationen kann eine mangelnde Vorbereitung auf derartige Angriffe auch rechtliche Folgen haben.

4. SSL-VERSCHLÜSSELTE DATEN

Der Umfang des Datenverkehrs, den moderne Netzwerke übertragen und verarbeiten müssen, überfordert bereits in vielen Fällen die genutzten Sicherheitsgeräte. Die Herausforderung für die IT-Sicherheit ist jedoch nicht auf das Volumen des Datenverkehrs beschränkt. Da viele dieser Daten sensibel oder geschützt sind, muss der Verkehr auch mittels Maßnahmen wie SSL-Verschlüsselung gesichert werden.

Die Datenverschlüsselung scheint eine gute Idee zu sein. Selbst wenn Cyber-Kriminelle in Ihr Netzwerk eindringen, sind alle von ihnen abgefangenen oder gestohlenen Daten nutzlos. Aber was gut für Sie ist, kann auch gut für die Cyber-Kriminellen sein. Verschlüsselter Datenverkehr kann auch Malware, Netzwerksonden und bösartigen Datenverkehr verbergen. Der gesamte Datenverkehr muss daher geöffnet, überprüft, neu verpackt und dann versendet werden.

Das ist leichter gesagt als getan.

Die Untersuchung von SSL-Datenverkehr ist außerordentlich ressourcenintensiv. Aus diesem Grund verzeichnen die meisten am Markt erhältlichen Sicherheitsgeräte bei der Überprüfung von verschlüsseltem Datenverkehr große Leistungseinbußen – und das in einer Situation, in der Leistung wichtiger ist als jemals zuvor. Viele Organisationen ziehen es deshalb vor, kritischen Datenverkehr entweder nicht zu verschlüsseln oder verschlüsselten Datenverkehr nicht zu überprüfen. Beide Vorgehensweisen führen zu unnötigen Risiken in einer ohnedies komplexen Bedrohungslandschaft.

5. QUALIFIKATIONSLÜCKE BEI DER CYBER-SICHERHEIT

Als wäre das Problem nicht schon komplex genug, sehen wir uns auch noch einem weltweiten Mangel an qualifizierten Cyber-Sicherheitsexperten gegenüber. Schätzungen nach gibt es global bis zu einer Million unbesetzter Stellen. In einer neuen von der Information Systems Security Association (ISSA) und Analysten der Enterprise Strategy Group (ESC) durchgeführten Umfrage geben 70 % der Organisationen an, dass diese Kompetenzlücke auch auf sie Auswirkungen hat. 54 % der Organisationen berichten, dass ein Sicherheitsvorfall im vergangenen Jahr auf einen Mangel an Sicherheitsexperten oder Schulung zurückzuführen gewesen sei.

Es ist nicht möglich, seine IT-Sicherheit zu planen, zu implementieren, zu verwalten, zu beurteilen oder zu verbessern, wenn das zuständige Team keine Personen mit angemessene Sicherheitskompetenzen umfasst. Die zuständigen Mitarbeiter

müssen auch die kurz- und langfristigen Geschäftsziele kennen und in der Lage sein, die Auswirkungen von tiefgreifenden Änderungen innerhalb des Netzwerks auf die Sicherheit zu bewerten.

WAS IST ZU TUN?

Zur Erfüllung der neuen digitalen Geschäftsanforderungen müssen Organisationen und Unternehmen ihren herkömmlichen isolierten Ansatz für die Wahl und Bereitstellung von Sicherheitstools überdenken. Isolierte Sicherheitsstrategien erhöhen den Overhead, verringern die Transparenz und beschränken die Kontrolle.

Die modernen Sicherheitsanforderungen können nur durch einen Übergang zu einer ganzheitlichen Sicherheitsstrategie bewältigt werden. Komplexe Netzwerke erfordern schnelle Authentifizierung und Überwachung, interne Segmentierung zum automatischen Trennen und Überwachen sensibler Ressourcen, Integration und Automatisierung traditionell isolierter Sicherheitstechnologien sowie Cloud-basierte Sicherheitsdienste, die Geräte und Daten überall in Ihrem verteilten Ökosystem von Netzwerken verfolgen und verteidigen.

Eine integrierte Security Fabric hält das gesamte verteilte Netzwerk durch die sichere Verbindung von Endgeräten und IoT-Geräten mit lokalen Netzwerken und über die Cloud zusammen und sorgt für vollständige Transparenz. Sie synchronisiert Netzwerk- und Sicherheitsdaten, erweitert die Transparenz und automatisiert die Kontrolle über das gesamte Unternehmen, um komplexe Bedrohungen zu erkennen und abzuwehren.

DEUTSCHLAND
Feldbergstraße 35
60323 Frankfurt
Deutschland
Verkaufsabteilung:
+49 69 310 192 0

SCHWEIZ
Riedmuehlestr. 8
CH-8305 Dietlikon/
Zürich
Schweiz
Verkaufsabteilung:
+41 44 833 68 48

ÖSTERREICH
Wienerbergstrasse
7/D/12th floor
1100 Wien
Österreich
Verkaufsabteilung:
+43 1 22787 120

HEADQUARTER
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 (408) 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
905 rue Albert Einstein
06560 Valbonne
Frankreich
Tel.: +33 (0)4 8987 0500

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

LATEINAMERIKA
ZENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd.,
Suite 430
Sunrise, FL 33323
Tel: +1 954 368 9990

30. Januar 2017