WHITEPAPER

5 MÖGLICHKEITEN, RISIKEN VON MOBILITY UND IOT ZU MANAGEN

Netzwerkrisiken reduzieren, indem Sicherheitsrichtlinien durchgesetzt werden

aruba
a Hewlett Packard Enterprise company

TechTarget | Custom Media

EINLEITUNG

Beschäftigte sind heute mobiler als je zuvor und es ist kein Ende des Wachstums der Konnektivität innerhalb und außerhalb der Arbeitsbereiche in Sicht. Einer Prognose von Gartner zufolge wird es im Jahr 2020 über 21 Milliarden vernetzte Geräte auf der Welt geben.[1] Andere Fachleute sagen, bis zu diesem Jahr wird es mehr Menschen mit einem Mobiltelefon geben, als Menschen die über fließend Wasser und ein Auto verfügen und dass der Internet-Datenverkehr die Zettabyte-Grenze überschreiten wird.[2]

Die Diskussion um die BYOD-Sicherheit ist eindeutig vorüber, da Organisationen bereits vor langer Zeit erkannt haben, dass sie, um konkurrenzfähig zu bleiben, so flexibel sein müssen, ihren Benutzern die Freiheit zur Verbindung unterschiedlicher Geräte zu gestatten, ob sie der IT-Abteilung gehören oder nicht. Die meisten Organisationen ermöglichen diese Flexibilität durch eine maßvolle Herangehensweise, wobei bestimmte Bedingungen erfüllt sein müssen, bevor das Gerät eines Benutzers auf sensible Daten zugreifen darf. Dazu zählen Bedingungen bezüglich des Status des Geräts, verwendete Authentifizierungsverfahren, die Sensibilität der Daten, auf die zugegriffen wird usw. Reife Organisationen entwickeln diese Anforderungen auf Basis gründlicher Risikobewertungen und kodifizieren sie anhand von offiziellen Richtlinien. Diese Richtlinien sollen das Netzwerk und die Daten auf Mobilgeräten und Internet-of-Things (IoT)-Geräten während der Übertragung und auf den Speicherplätzen schützen.

Doch ist dies nur ein Schritt zum Risikomanagement in diesem neuen Zeitalter von „Always on"-Mobilkonnektivitäts- und IoT-Initiativen. Richtlinien sind nur so gut wie die Mechanismen zu ihrer Durchsetzung. Und leider verfügen viele Organisationen nicht über die Technologie oder Prozesse, um Sicherheitsrichtlinien in konsequente Praxis umzusetzen, namentlich durch effektive und automatisierte Abläufe zu deren Durchsetzung. Um das Risiko von Datensicherheitslücken, die durch Mobilität und IoT entstehen, wirklich zu mindern, müssen Organisationen die folgenden fünf Schritte in Erwägung ziehen.

NICHTS ANDERES ZÄHLT, BIS SIE WISSEN, WER UND WAS VERSUCHT, EINE VERBINDUNG HERZUSTELLEN

Die meisten Organisationen können nicht jederzeit die Risiken quantifizieren, weil sie gemeinsam mit Netzwerkverbindungen nicht über die nötige Transparenz oder die Kontrollen verfügen. Ohne diese grundlegende Fähigkeit fällt es ihnen schwer, Richtlinien im Netzwerk durchzusetzen, Hinweise auf Kompromittierung festzustellen und zu verstehen, wie verwundbar sie gegenüber neuen Bedrohungen sind, die mit mobilen Benutzern und Apps oder dem Internet der Dinge einhergehen.

Organisationen benötigen eine automatisierte Möglichkeit für die Erfassung von allem, das eine Verbindung mit dem Netzwerk herstellt, während es versucht, eine Verbindung herzustellen.

Diese Funktion sollte Informationen darüber liefern:

- wer eine Verbindung herstellt;
- wie und mit welchem Gerät ein Benutzer versucht, eine Verbindung herzustellen;
- welche Ressourcen für das Gerät des Benutzers zugänglich sind;
- welche Risiken mit diesem speziellen Gerät oder dieser Datenzugriffsberechtigung verbunden sind.

GERÄTETRANSPARENZ MUSS MIT DER DURCHSETZUNG IM NETZWERK VERKNÜPFT SEIN

Zwar bietet der Markt eine Reihe von Werkzeugen für das Gerätemanagement, die einen gründlichen Einblick in den Sicherheitsstatus der Geräte erlauben, doch haben sie ihre Einschränkungen. Die Verwendung von Werkzeugen zur Verwaltung von Mobilgeräten oder Endpunkten ist nur ein Element einer soliden Mobilgeräte-Sicherheitsstrategie, da ihnen die Mittel für eine zuverlässige Durchsetzung im Netzwerk fehlen.

Organisationen müssen nicht nur erfassen können, welche Geräte mit ihrem Netzwerk verbunden sind, sondern auch in der Lage sein, den Zugriff aufgrund des Status dieser Geräte einzuschränken. Organisationen benötigen eine Möglichkeit, Kontextinformationen zu dem Gerät zu berücksichtigen, wie zum Beispiel den Status von Berechtigungseinstellungen im Gerät, ob das Gerät gerootet wurde, ob das Gerät über vollständig aktualisierte Anti-Malware-Software verfügt und ob das Gerät potenzielle Zeichen von Kompromittierung aufweist.

Transparenz in Bezug auf diese Kontextelemente ist ein entscheidender erster Schritt. Der nächste Schritt ist, sie

1 „Gartner: 21 Billion IoT Devices to Invade by 2020", InformationWeek, 10. Nov. 2015
2 „Phones Will Drive Internet Traffic Past the Zettabyte Mark This Year", Recode, 3. Feb. 2016

mit effektiven Mitteln für die Durchsetzung im Netzwerk zu verbinden, je nachdem, wie gut der Zustand des Gerätes den aktuellen Sicherheitsrichtlinien entspricht. Um Netzwerkressourcen besser zu schützen und Angriffe von riskanten Geräten zu verhindern, benötigen Organisationen automatisierte Zugriffskontrollen, die sicherstellen, dass Geräte, die die Anforderungen der Richtlinie nicht erfüllen, keine Verbindung mit dem Netzwerk herstellen können, solange sie nicht konform sind.

BENUTZER- UND UMGEBUNGSKONTEXT SIND ENTSCHEIDEND

Je mehr Kontext in die Zugriffskontrollen einfließt, desto detaillierter können die Richtlinien sein, die den Zugriff bestimmen. Der Gerätestatus ist wichtig, aber ebenso wichtig ist, wer den Touchscreen bedient, von wo aus die Benutzer verbunden sind und zu welcher Tageszeit sie verbunden sind.

Wenn Organisationen Richtlinien durchsetzen, müssen die Zugriffskontrollen nuanciert genug sein, um den Zugang zu Netzwerkressourcen auf Basis von Benutzerberechtigungen, Ort, Tageszeit und anderen Merkmalen zu kontrollieren. Darüber hinaus benötigen Organisationen eine Möglichkeit, verschiedene Geräte mit einem einzelnen Benutzer zu verknüpfen und transparente Durchsetzungsprozesse zu erstellen, die den Benutzerkontext im Fokus behalten. Derselbe Kontext kann dann dafür benutzt werden, das Verhalten von Benutzern und Einheiten im Netzwerk zu überwachen.

Und schließlich sollte die Zugriffskontrolle über eine zweckmäßig abgestimmte Automatisierung verfügen, die relevanten Kontext dafür nutzt, mit Mobilität verbundene Risiken zu minimieren.

KABELGEBUNDENE VERBINDUNGEN NICHT AUSSER ACHT LASSEN

Heute hängt mobile Sicherheit stark davon ab, wie gut Organisationen drahtlose Verbindungen absichern. Doch dürfen Organisationen die Bedeutung kabelgebundener Verbindungen nicht vergessen.

Ungeschützte Kabelanschlüsse an öffentlich zugänglichen Orten sind häufig die Achillesferse einer ansonsten soliden Netzwerksicherheitsstrategie. Wenn ein Besucher einen öffentlichen Bereich betritt, das Netzwerkkabel eines Druckers oder eines IP-Telefons in einem Besprechungsraum ausstecken und einen Laptop anschließen kann und sofort freien Zugang erhält, ist das ein Problem.

ERSTELLEN SIE EINEN WIEDERHERSTELLUNGSPLAN, DER IN JEDEM SZENARIO FUNKTIONIERT

Eine herausragende Zugriffskontrolle ist eine Sache, doch muss eine Organisation auch über einen Plan oder über einen Workflow verfügen, um Probleme zu lösen, wenn etwas schief läuft. Einer der größten Fehler, den Organisationen machen, liegt darin, Technologie einzusetzen, um Netzwerkverbindungen von Geräten zu kontrollieren, aber keine automatischen Benachrichtigungen an Benutzer einzuführen, in denen ihnen mitgeteilt wird, warum ihnen der Zugriff verwehrt wird. Diese Art von Übersehen überschwemmt die Mitarbeiter von Helpdesks mit Störungstickets, verschwendet die Zeit der Benutzer und irritiert Führungskräfte.

Wenn Organisationen Zugriffskontrollen einführen, benötigen sie einen Plan und einen Prozess zur Optimierung des Workflows, nachdem ein Gerät gesperrt wurde. Das bedeutet, wenn möglich automatisch eine Wiederherstellung auszulösen. Das bedeutet, Benutzer über das Problem zu informieren, das die Sperrung verursacht hat. Das bedeutet, den Helpdesk und den IT-Support zu beteiligen. Und es bedeutet, Unterlagen oder andere Ressourcen bereitzustellen, die nötig sind, um die Benutzer bei einer möglichst schnellen Wiederherstellung zu unterstützen.

WIE ARUBA CLEARPASS HILFT

ClearPass bietet die Transparenz, Richtlinienkontrolle, Workflow-Automatisierung und Integration mit anderen Sicherheitsprodukten, die nötig sind, um diese fünf Schritte umzusetzen. Funktionsmerkmale sind unter anderem:

- Integrierte Profilerstellung, die Echtzeitdaten, wie zum Beispiel Gerätekategorien und Betriebssystemversionen, erfasst
- Authentifizierungsprozesse, die die Nutzung des Benutzer- und Gerätekontexts für die Durchsetzung erlauben
- Gemeinsame Kontextnutzung, die mit Drittanbietersystemen funktioniert. Zu diesen Systemen gehören zum Beispiel Firewalls, Endpoint-Management, Benutzer- und Verhaltensanalyse, Gerätemanagement sowie IT-Dienste, die akkurate Daten zu Benutzern und Geräten liefen, um die Wiederherstellungsworkflows zu verbessern.

Mit diesen Funktionen können Organisationen kontrollieren, auf welche Weise Benutzer und Geräte interne Ressourcen nutzen, ungeachtet der Rolle eines Benutzers, des Gerätetyps oder des Standorts, von dem aus eine Verbindung hergestellt wird.

FAZIT: ZUSAMMENFASSUNG

Wenn Organisationen sich daran begeben, alle diese Schritte zur Minderung der Mobilitätsrisiken umzusetzen, gibt es nicht eine einzige technologische, magische Wand. Organisationen benötigen ein ausgewogenes Ökosystem von Kontrollen, um alle Risikodimensionen zu erfassen. Sie müssen berücksichtigen, dass es gilt, detaillierte Netzwerkzugriffskontrollen und die Transparenz von Verbindungen mit IT-Orchestrierungsplattformen zur Wiederherstellung zu verbinden.

Dafür müssen Organisationen Lösungen implementieren, bei denen Integration an erster Stelle steht, um sicherzustellen, dass die Anbieter, die sie wählen, gut zusammenarbeiten und nahtlose Sicherheit bieten.