Computerworld

Netzwerksicherheit im Zeitalter von Generation Y

2020 stellt die sogenannte Generation Y die Hälfte der Belegschaft. Für CIO und Netzwerk-Administratoren bedeutet dies eine Reihe neuer Herausforderungen, um die Unternehmens-IT abzusichern.

» Von Franz Kaiser, Fortinet, 28.02.2017 08:10.

Das Netzwerk eines Unternehmens zu sichern, ist einer der härtesten Jobs in der IT-Branche. Es ist auch jene Aufgabe, die sich mit dem Vormarsch der Generation Y zunehmend schwieriger gestaltet.

Denn die Generation Y, zu der Personen im Alter von ca. 20 bis Mitte 30 zählen, dominiert global immer mehr das Arbeitsleben. Bis zum Jahr 2020 wird diese demografische Gruppe die Hälfte der berufstätigen Bevölkerung weltweit ausmachen.

Mit dem Ausdruck «Generation Y» verbindet man vieles, zum Beispiel: Sie «teilt» gerne auf sozialen Netzwerken . Sie gibt sich nicht mit schlechten Benutzererfahrungen zufrieden. Sie will einen flexiblen Arbeitsansatz und – sie zieht schnell weiter, wenn sich ihre Erwartungen nicht erfüllen.

Diese Eigenschaften werden die Kultur des zukünftigen Arbeitsplatzes definieren und die Stabilität der Netzwerksicherheit vieler Unternehmen auf eine harte Probe stellen.

Mit folgenden drei Herausforderungen werden sich CIO, CSIO und IT-Netzwerkadministratoren in Sachen Generation Y besonders konfrontiert sehen.

Nächste Seite: 1. Social Media

1. Social Media

Blockieren oder nicht? Geht es um die Nutzung von Social Media durch eigene Mitarbeiter am Arbeitsplatz, haben sich Unternehmen schon mit dieser Frage beschäftigt.

Soziale Medien: Der Umgang mit ihnen muss gelernt sein, auch in Firmen © IMWF

Eine Studie des HR-Software-Anbieters CareerBuilder belegt, dass 37 Prozent der Arbeitgeber Social Media als einen der grössten Produktivitätskiller am Arbeitsplatz betrachten, gleich nach dem Mobiltelefon und SMS (55 Prozent), der Nutzung des Internets (41 Prozent) und Klatsch und Tratsch (39 Prozent). Drei von vier Arbeitgebern zufolge gehen täglich zwei oder mehr Stunden an Produktivität verloren, weil die Arbeitnehmer abgelenkt sind.

Aus der Perspektive der Netzwerksicherheit betrachtet ist Social Media ein Vektor für Malware und eine Angriffsfläche für Social Engineering. Wie viele Links, die in gutem Glauben geteilt werden, enden damit, dass sie die Nutzer auf kompromittierte Websites leiten? Und selbst wenn die Mitarbeiter soziale Kanäle auf professionelle Art und Weise nutzen, sind ihre Freunde und Kontakte in keinerlei Hinsicht dazu verpflichtet.

Auf Netzwerk-Level ist es einfach, Social-Media-Seiten zu sperren oder die Nutzung zu beschränken. Statische URL-Filter in Web-Filtersoftware können bestimmte URLs blockieren oder überwachen. Die Möglichkeit, nach Kategorien zu filtern, kann ganze Gruppen von Websites blockieren. Aber das bedeutet nicht, dass CIOs damit beginnen sollten, soziale Netzwerke am Arbeitsplatz zu blockieren.

Ein besserer Ansatz ist es, noch einmal genau hinzusehen, wie die Netzwerksicherheit im Ganzen verstärkt werden kann. Dabei sind eine klare Social-Media-Politik und Schulungen für die Mitarbeiter ein guter Start. Zum Beispiel sollten die Mitarbeiter im Verkauf an die Sicherheits- und Geschäftsrisiken erinnert werden, die aufkommen können, wenn sie sich bei ihren Kunden vor Ort über soziale Kanäle wie Facebook an ihrem Standort anmelden.

Die wichtigste Schutzmassnahme ist jedoch eine robuste, vielschichtige Sicherheitsinfrastruktur. Damit stehen Sie auf der sichereren Seite - sicherer, als wenn Sie sich darauf verlassen müssen, dass Ihre Mitarbeiter bei ihren Klicks auf ihren Social-Media-Konten niemals auf Abwege geraten.

Nächste Seite: 2. Die Sicherheitsschichten kennen

2. Die Sicherheitsschichten kennen

Vielschichtige Sicherheit, bei der verschiedene Securitylayer kombiniert werden, um Daten, Geräte und Menschen zu schützen, ist heute weit verbreitet. Dies gewährleistet, dass Angriffe, die auf verschiedene Quellen verübt werden – etwa auf das Netzwerk, die Applikation, das Gerät oder die Benutzerebene – erkannt und gestoppt werden können, bevor sie sich ausbreiten. Es ist auch eine effektive Massnahme gegen verschiedene Arten von Bedrohungen.

Die Generation Y ist mobil: Entsprechende BYOD-Konzepte gilt es daher zu beachten

Durch die Anforderungen der Generation Y ändern sich die Gewohnheiten im Arbeitsleben. CIOs sollten daher genau planen , wie jede einzelne Sicherheitsschicht gestaltet werden muss.

Denken Sie beispielsweise an die Nutzung persönlicher Geräte am Arbeitsplatz. Laut einer Studie von McKinsey & Company erlauben ca. 80 Prozent der Unternehmen ihren Mitarbeitern, persönliche Geräte mit unternehmenseigenen Netzwerken zu verbinden. Zunehmend erwarten Mitarbeiter auch, dass sie darin von ihren IT-Abteilungen unterstützt werden - etwa, dass auf den persönlichen Geräten der Zugang zu Unternehmensapplikationen wie E-Mail und Kalender eingerichtet wird. Der BYOD-Trend (Bring Your Own Device) führt also zu einer Vielzahl neuer Sicherheitsbedrohungen.

Ein ganz besonderes Augenmerk sollten CIOs auf eine verbesserte Sicherheit auf Geräteebene legen. Der erste Schritt dabei ist, die Geräte selbst zu schützen, durch eine vorgeschriebene Kombination von Firewalls, Anti-Malware-Software, MDM-Lösungen (Mobile Device Management) und regelmässigen Patches. Eine BYOD-Kultur setzt Unternehmen auch deshalb Risiken aus, weil die intelligenten Geräte der Mitarbeiter aufgrund schlechter Passwörter gehackt werden könnten. Richtlinien und Schulungen zu sicheren Codes sind daher ein Muss.

Es können auch unsichere Gerätetypen definiert werden, denen der Zugang zu einigen Teilen des Netzwerkes verwehrt wird – wie etwa Mobiltelefonen. Auch Sessions sollten gesichert sein, etwa dadurch, dass einem Besuch unsicherer Websites durch den Nutzer vorgebeugt wird.

Ein weiterer wichtiger Punkt ist der Schutz der Benutzereben, um das steigende Risiko interner Bedrohungen so gering wie möglich zu halten. Aufgrund der Notwendigkeit, hier Sicherheit und Komfort in eine gesunde Balance zu bringen, ist diese Ebene oft diejenige, die am heikelsten zu handhaben ist. Es können auch eine Vielzahl von Authentifizierungsmethoden zur Erkennung des Netzwerknutzers eingesetzt und verschiedene Zugangslevel geschaffen werden. Die Mitarbeiter zu sensibilisieren und zu schulen ist auch hier unerlässlich.

Nächste Seite: 3. Schatten-IT bewältigen

3. Schatten-IT bewältigen

Mit dem Begriff Schatten-IT wird die Nutzung von Applikationen und Services, oftmals basierend auf einer Cloud, beschrieben, die vom Unternehmen nicht genehmigt sind. Da es in der Natur der Sache liegt, dass diese Schatten-IT unkontrolliert ausgeführt wird, stellt sie eine Sicherheitsbedrohung und eine Herausforderung an die Governance dar.

Schatten-IT wird mit der Generation Y virulent

Stellen Sie sich nur einmal das Szenario vor, in dem Mitarbeiter ihr Smartphone nutzen, um eine Datei zu öffnen. Es ist sehr wahrscheinlich, dass das Smartphone eine Kopie dieser Datei fertigen wird. Diese könnte dann an einen nicht genehmigten Online-Speicherort gesendet werden, wenn das Smartphone sein routinemässiges automatisches Backup ausführt. So bewegen sich ohne weiteres Ihre sicheren Unternehmensdaten an einen unsicheren Standort.

Auf die gleiche Art und Weise können sich sensible Unternehmensdaten an unsichere Standorte bewegen, und zwar durch die vielen Social Collaboration-Apps, die bei der Generation Y so beliebt sind.

Das Personal anzuweisen, die Nutzung nicht genehmigter Geräte und Applikationen zu stoppen, wird jedoch vermutlich nicht deren Ausbreitung im Unternehmen verhindern. Offen gesagt, trägt die Allgegenwärtigkeit von Smartphones dazu bei, dass die Mitarbeiter soziale Netzwerke und ihre persönlichen Cloud-Apps auch nutzen, ganz gleich, ob Sie dies mit Ihren Richtlinien verhindern möchten oder nicht.

Effektiver ist es, die Nutzer zu schulen und die entsprechende Technologie, beispielsweise Datenverschlüsselung, Zugriffskontrolle und Traffic-Überwachung zu implementieren, um das Problem in den Griff zu bekommen.

Aus einer anderen Perspektive betrachtet, geschieht die Nutzung der Schatten-IT dann, wenn Ihre Mitarbeiter mit den Lösungen, die ihnen das Unternehmen bietet, nicht glücklich sind. Es ist den CIOs vielleicht nicht möglich, die Mitarbeiter davon abzuhalten, für, sagen wir einmal, den Zweck der Collaboration, nach alternativen Apps zu suchen, aber sie können die Dinge in Schach halten, indem sie sich auf ihre Belange einstellen.

© Fortinet

Zum Autor

Franz Kaiser ist Regional Vice President Alps bei Fortinet

Neue Mediengesellschaft Zürich AG, Redaktion Computerworld, Kalanderplatz 5, CH-8027 Zürich, Schweiz
Phone: +41 44 387 44 44, Fax: +41 44 387 45 80