Cisco Leitfaden zur Problemlösung

Echter Mehrwert im IT-Bereich: zehn wichtige Ratschläge zum Thema Sicherheit in Ihrem Unternehmen

In einem Unternehmen kommt man um das Thema Sicherheit nicht herum. Die Sicherheit Ihrer Informationen, Ihrer Geschäftsräume und Ihrer Kundendaten mag nicht das primäre Ziel Ihres Unternehmens sein, sollte für Sie aber dennoch höchste Priorität haben. Eine echte Herausforderung angesichts der Fülle an Informationen, von denen längst nicht alle essenzieller Natur sind. Immer wieder müssen fachfremde Entscheidungen getroffen und Fragen wie die folgende beantwortet werden: „Mir wurde gesagt, ich bräuchte eine Firewall. Aber bei Windows ist bereits eine Firewall installiert. Brauche ich trotzdem eine zusätzliche?“

In diesem Leitfaden möchten wir Ihnen einige Bereiche näherbringen, die Ihrer Aufmerksamkeit bedürfen, und Ihnen Informationen an die Hand geben, die Sie mit hoher Wahrscheinlichkeit im Rahmen Ihrer Tätigkeit benötigen. Darüber hinaus sprechen wir auch Probleme an, die über den rein technischen Aspekt hinausgehen.

Zehn wichtige Ratschläge

1. Antiviren-Software:

Antiviren-Softwarepakete sind äußerst praktisch, doch nicht alle bieten den optimalen Schutz. Vermutlich ist Ihnen bekannt, dass eine Antiviren-Software stetig über eine Datenbank Informationen zu möglichen Sicherheitsbedrohungen einholt (weswegen die regelmäßige Aktualisierung Ihrer Software unabdinglich ist).

Gleichzeitig hat dies aber auch zur Folge, dass die Antiviren-Software Ihr System nur vor den Viren schützen kann, über die Informationen vorliegen. Aus diesem Grund empfiehlt Cisco®, neben einer Antiviren-Software zusätzlich den Einsatz eines sogenannten Intrusion Prevention Systems (IPS). Im Gegensatz zu einer herkömmlichen Antiviren-Software greift ein IPS auf umfassendere Informationen zurück und überwacht darüber hinaus auf Ihrem Computer installierte Software auf auffälliges Verhalten. Ein IPS überprüft Ihr System also nicht nur auf bekannte Viren, sondern stoppt auch die Ausführung von Codes, die durch vermutlich von Ihnen unbeabsichtigte Aktivitäten (z. B. das Löschen anderer Dateien, Durchsuchen Ihrer Kundendatenbank etc.) auffallen. Sicherheitsexperten bezeichnen dies als „Day-Zero-Angriff"; also einen Angriff, der Schwachstellen oder Sicherheitslücken eines Programms ausnutzt, bevor sie vom Hersteller bemerkt und behoben werden. Unsere Lösung kann diese Angriffe abwehren, da sie Ihr System auf Auffälligkeiten anstatt auf bekannte Codes untersucht.

Es gibt verschiedene Arten von IPS: Host-basierte und Netzwerk-basierte IPS. Ein Netzwerk-basiertes IPS befindet sich am Zugangspunkt Ihres Netzwerks. Ein Host-basiertes IPS befindet sich dagegen auf Ihrem Notebook und bietet Ihnen so auch unterwegs den gewohnten Schutz.

2. Firewall:

Es reicht nicht aus, einfach irgendeine Firewall einzusetzen. Die Auswahl sollte mit Bedacht getroffen werden. Manche Firewall-Lösungen sind im Betriebssystem integriert, andere auf separaten Rechnern im Netzwerk installiert.

Entscheidender ist aber, hinsichtlich welcher Kriterien die Firewall Ihr System überwacht. Viele Firewalls überprüfen das Netzwerk auf potenzielle Angriffe und erfüllen damit eine wesentliche Anforderung. Unsere Lösungen bieten darüber hinaus auch Schutz auf Anwendungsebene, d. h. sie erkennen Codes, die möglicherweise ein auffälliges Verhalten von individuellen Programmen auslösen. Außerdem sollten Sie über eine Firewall verfügen, die nicht auf Ihrem Computer, sondern auf einem anderen Rechner, Router o. ä. installiert ist, der als Gateway in Ihrem Netzwerk fungiert. Ist dieses Gateway der einzige Zugangspunkt zum Netzwerk, ist die Implementierung einer Schutzfunktion unbedingt anzuraten. Wir bieten zu diesem Zweck Produkte mit unterschiedlichen Sicherheitsstufen an.

3. Mitarbeiter:

Neben technischen Aspekten dürfen auch andere Faktoren, die ein Sicherheitsrisiko für Ihr Unternehmen darstellen können, nicht außer Acht gelassen werden. Im Folgenden sind einige Beispiele aufgeführt, bei denen Daten verloren gingen oder der Datenschutz gefährdet war:

- Nach Einführung einer strikten Richtlinie, mit der die Zugriffsrechte auf elektronisch gespeicherte Daten geregelt werden, wird diese Sicherheitsvorschrift nicht auf ausgedruckte Dokumente übertragen, die häufig in Zügen oder Hotels liegenbleiben.
- Mitarbeiter werden nicht ausreichend dazu angehalten, ihre Bildschirme auszuschalten, wenn sie nicht an ihrem Schreibtisch sitzen. Besucher haben so die Möglichkeit, vertrauliche Daten und Informationen zu lesen. (Hier sollte auch angemerkt sein, dass Bildschirmschoner unnötig Strom verbrauchen und schon lange keinen effektiven Schutz mehr darstellen.)
- Was längst bekannt sein sollte, wird doch immer wieder missachtet: Der Name Ihres Hundes oder Partners oder ein Teil Ihrer Anschrift ist kein sicheres Passwort. Dasselbe gilt für „passwort".
- Das Fehlen einer allgemein gültigen, verständlichen Richtlinie, die festlegt, was für die Netzwerksicherheit getan werden muss, wer dafür zuständig ist und welche Maßnahmen bei Nichteinhaltung getroffen werden. Nehmen Sie Ihre Mitarbeiter ernst, und behandeln Sie sie mit Respekt. So werden sie gerne ihren Beitrag leisten.
- Des Weiteren sollte die Richtlinie das willkürliche Herunterladen von Software ausdrücklich untersagen. In vielen Fällen richtet solche Software keinen Schaden an, kann aber zusätzliche Lizenzen erforderlich machen oder sich als Malware entpuppen.

4. Geräte:

Hier geht es um Sicherheitsprobleme, die von mobilen Geräten ausgehen. Im Verteidigungsministerium müssen Berichten zufolge mobile Geräte wie Mobiltelefone und MP3-Player am Eingang abgegeben werden, und man erhält sie erst beim Verlassen des Gebäudes zurück. Dies liegt mitnichten daran, dass diese Geräte die Mitarbeiter von der Arbeit ablenken könnten, sondern vielmehr an der Tatsache, dass Mobiltelefone, Kameras und ähnliche Geräte die Möglichkeit zur Datenspeicherung bieten. Ein iPhone 3G beispielsweise verfügt über 16 GB Speicherplatz. Über USB-Ports können diese Geräte an einen Computer angeschlossen werden. Besucher können auf diese Weise zum Beispiel Ihr Kundenverzeichnis auf ein beliebiges Speichermedium kopieren und mitnehmen. Auch Viren können über mobile Geräte in Ihr System eingeschleust werden.

Ein striktes Verbot von privaten mobilen Geräten möchten Sie jedoch nicht aussprechen. Es gibt aber andere Vorsichtsmaßnahmen, die Sie ergreifen können:

- Computer können so konfiguriert werden, dass sie USB-Geräte nicht erkennen.
- Eine intelligente Überwachungssoftware, wie sie in allen unseren Produkten integriert ist, erkennt auffällige Aktivitäten in Ihrem Netzwerk und informiert Sie darüber.
- Wenn Besucher sich an Ihrem Netzwerk anmelden und dabei ihre eigenen Notebooks verwenden, müssen diese vorher auf Viren überprüft werden und darüber hinaus den Sicherheitsvorschriften Ihres Unternehmens entsprechen. Unsere Lösungen unterziehen Gast-Computer beim Anmelden am Netzwerk einer umfassenden Prüfung auf bekannte Viren und auffällige Aktivitäten.

5. Sicherung der Daten Ihrer Mitarbeiter im Heimbüro und unterwegs:

Ihr Netzwerk kann noch so gut abgesichert sein – wenn Informationen außerhalb Ihres Netzwerks ungesichert sind, ist der Datenschutz nicht mehr gewährleistet. Aus diesem Grund sollten Sie folgende Punkte beachten: Verbindungen zu Ihrem Netzwerk über das Internet sollten ausschließlich über ein sicheres VPN (virtuelles, privates Netzwerk) erfolgen, bei dem alle erforderlichen Sicherheitsfunktionen aktiviert sind. Auch die nichttechnischen Aktivitäten Ihrer Mitarbeiter sollten denselben Sicherheitsvorschriften entsprechen, die im Büro gelten. Wenn beispielsweise das Ausdrucken von Dokumenten oder das Übertragen von Dateien auf USB-Sticks im Büro untersagt ist, sollten Ihre Mitarbeiter dies auch im Heimbüro unterlassen.

Durch die Implementierung eines intelligenten Switching-Netzwerks im Büro und die Sicherung des Gateways mit den entsprechenden Cisco Produkten können viele dieser Ziele erreicht werden.

6. Drahtlose Netzwerke:

Zur Sicherung der Daten Ihrer Mitarbeiter im Heimbüro und unterwegs gehört auch, die Konfiguration Ihres internen und externen drahtlosen Netzwerks zu überprüfen. Wenn ein Notebook oder ein Smartphone ein Netzwerk findet und dieses als „gesichert“ angezeigt wird, heißt es noch lange nicht, dass der optimale Schutz bei diesem Netzwerk auch wirklich gegeben ist. Häufig bedeutet es nur, dass das WEP-Sicherheitsprotokoll aktiviert ist – eine Technologie, die mittlerweile veraltet ist und von jedem versierten Hacker problemlos umgangen werden kann.

Im Büro verfügt die Netzwerkausrüstung von Cisco über integrierte Sicherheitsfunktionen. Diese sind standardmäßig aktiviert und können von unseren Partnern konfiguriert werden. Außerhalb des Büros verwenden Ihre Mitarbeiter möglicherweise eigenes drahtloses Zubehör. In diesem Fall sollten Sie darauf bestehen, dass folgende Punkte gewährleistet sind:

- Ist ein WEP-Sicherheitsprotokoll aktiviert, sollte es auf WPA aktualisiert werden.
- Standard-Passwörter, die schon bei der Lieferung eingerichtet waren, sollten unbedingt geändert werden.
- Der Computer und der Netzwerk-Router verfügen über eine eindeutige Kennung, die sogenannte SSID (Service Set Identifier). Sie ist im Konfigurationsmenü des Routers aufgeführt und sollte unbedingt geändert werden. Außerdem sollten Sie die Übertragung der SSID deaktivieren, damit Ihr Computer nicht von Hackern gefunden werden kann.
- Deaktivieren Sie den automatischen Verbindungsaufbau zu WiFi-Netzwerken, sodass Benutzer sich nur mit vertrauenswürdigen Netzwerken verbinden können.
- Weisen Sie Ihren Geräten eine statische IP-Adresse zu. Andernfalls weist Ihr Netzwerk den Geräten diese Adressen nach dem Zufallsprinzip zu, was das Trennen eines Geräts vom Netzwerk erschwert.
- Wahrscheinlich verfügt Ihr Router über eine Firewall. Stellen Sie sicher, dass sie aktiviert ist – bei vielen Routern ist die Firewall nämlich standardmäßig deaktiviert.
- Schalten Sie das Netzwerk aus, wenn es längere Zeit nicht verwendet wird.

7. Hacking – wie groß ist die Gefahr?

Sie haben nun erfahren, wie Sie sich vor Hacker-Angriffen schützen und ungewolltes Eindringen in Ihr Netzwerk verhindern können. Aber wie wahrscheinlich ist es, dass Sie tatsächlich eines Tages Opfer eines Hacker-Angriffs werden? Bei vielen unserer Kunden handelt es sich um kleine und mittlere Unternehmen. Viele meinen, daher für Hacker von keinerlei Interesse zu sein.

Als sich hinter jedem Hacker noch ein Mensch verbarg, war diese Annahme vermutlich sogar richtig. Mittlerweile laufen viele Hack-Angriffe allerdings automatisiert ab. Stellen Sie sich den Hacker als Anführer einer Diebesbande vor, die in unbewachte Häuser einbricht, um herauszufinden, ob sich darin lohnende Beute befindet. In diesem Beispiel entsprechen die Häuser Computern und sehen einander sehr ähnlich. Die einzige Möglichkeit, herauszufinden, ob sich ein Einbruch lohnt, besteht also darin, sich Zugang zum Innern zu verschaffen.

Im Internet wird dies von sogenannten „Bots“ erledigt und erfolgt über das „Port Scanning“. Hierbei kommen die Bots praktisch an die „Tür“ Ihres Netwerks im Internet und überprüfen, ob sie abgeschlossen ist. Das sollte sie natürlich sein.

(Dies gilt auch für Ihre richtigen Türen. Wir bieten Kameras an, die mit dem Internet verbunden und so von überall aus überwacht werden können. Viele Modelle verfügen über einen Bewegungsmelder, der Sie alarmiert, wenn ein Unbefugter sich einem Eingang nähert.)

8. Online-Geschäfte:

Wenn Ihre Geschäfte ausschließlich oder mehrheitlich über das Internet abgewickelt werden, müssen Sie Maßnahmen ergreifen, um vertrauliche Lager- und Kundendaten zu schützen. Die bereits genannten Punkte tragen zu diesem Ziel bei, aber es gibt noch weitere, auch nichttechnische Möglichkeiten zum Datenschutz. Beispielsweise sollten unverschlüsselte CDs nicht in öffentlichen Verkehrsmitteln liegengelassen werden. (Denken Sie daran, Ihre CDs zu verschlüsseln, damit Ihre Daten auch dann nicht gelesen werden können, wenn jemand den Passwortschutz umgeht.)

9. Wie zahlen sich diese Maßnahmen aus?

Viele kleine und mittlere Unternehmen legen gerade in finanziell angespannten Zeiten Wert darauf, dass sich Investitionen im IT-Bereich auszahlen. Im Sicherheitsbereich ist dieser Ansatz allerdings etwas problematisch, da es sich hier um immaterielle Werte handelt. Wenn Sie Schlösser an Ihren Türen anbringen, berechnen Sie nicht, nach welchem Zeitraum sie sich amortisiert haben; Sie wissen lediglich, welcher Verlust Ihnen bei einem Einbruch entstünde.

Es gibt jedoch auch bei Sicherheitsausgaben Investitionsrenditen, die einfacher zu ermitteln sind. Wenn Sie beispielsweise eine E-Commerce-Website betreiben und Ihren Kunden die Sicherheit ihrer Daten nicht gewährleisten können, werden die Kunden diesen Vertriebskanal nicht mehr nutzen. Wenn sich Besucher vor Ort an Ihrem Netzwerk anmelden und ihr Gerät dabei mit einem Virus infizieren, weil die Sicherheitseinstellungen Ihres Netzwerks nicht ausreichen, werden Sie Kunden verlieren. Und dies sind nur zwei Beispiele.

Die grundlegende Sicherheitsausrüstung ist dabei in der Regel sehr kostengünstig. Ein Wireless-Router mit Firewall und umfassenden Sicherheitsfunktionen schlägt für ein kleines Büro mit wenigen Mitarbeitern mit weniger als £ 150 zu Buche.

10. Outsourcing der Sicherheit:

Wenn Sie sich den Herausforderungen der Netzwerksicherheit nicht alleine stellen möchten, haben Sie die Möglichkeit, Ihre gesamte Sicherheitsinfrastruktur auszugliedern. Viele unserer Partner sind darauf spezialisiert, die Sicherheit in kleinen und mittleren Unternehmen zu erhöhen. Als Anbieter vom Fach profitieren sie von Kostenersparnissen und verfügen außerdem über umfassendes Know-how. Vertrauliche Daten außerhalb Ihres Netzwerks zu speichern und von qualifizierten und zuverlässigen Fachkräften verwalten zu lassen bietet kleinen und mittleren Unternehmen zusätzliche Sicherheit.

Wie wir schon anfangs sagten: In einem Unternehmen kommen Sie um das Thema Sicherheit nicht herum. Aber die grundlegende Ausrüstung für ein sicheres Netzwerk ist nicht allzu kostspielig. Und wenn Sie Unterstützung bei der Einrichtung benötigen, stehen wir oder unsere Partner Ihnen jederzeit mit Rat und Tat zur Seite.

Viel Erfolg!