Gutes Risiko-Management zum Überleben

Netzwerksicherheit

Gutes Risiko-Management zum Überleben

In den letzten 35 Jahren hat sich die Netzwerksicherheit genau wie die Computerumgebung verändert. Durch neue Technologien und neue Bedrohungen sind die Anforderungen an die Netzwerksicherheit immer komplexer geworden.

Vor fünfzehn Jahren konnten Gefahren dadurch gebannt werden, dass man sich auf einzelne Punkte konzentrierte. Heute sind sich IT-Profis zunehmend der Tatsache bewusst, dass man zwar eine Tür verriegeln kann, Eindringlinge jedoch stattdessen eine andere, unverriegelte Tür finden. Der Trick, Eindringlingen das Handwerk zu legen, liegt in der Minimierung des Risikos.

Strikte Abschirmung und Blockierung

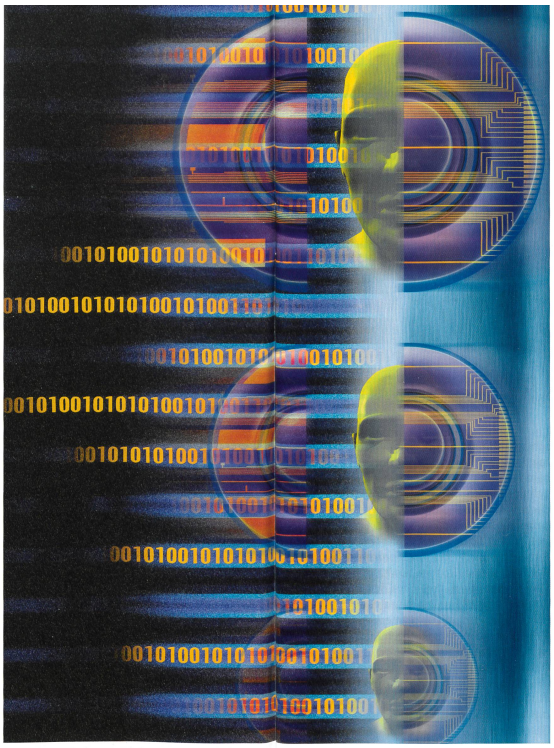
Die Ursprünge der Netzwerksicherheit liegen in physischen Sicherungsmassnahmen der späten 60er- und 70er-Jahre. Diese Periode der physischen Sicherungen war sozusagen die Vorzeit der Netzwerksicherheit. Während dieser Zeit ging es Computerprofis hauptsächlich darum, zu verhindern, dass Eindringlinge mit physischer Gewalt in Gebäude und Einrichtungen einbrachen und vertrauliche Informationen stahlen. Computersysteme verfügten zumeist nur über einen einzigen Zugangscode und waren daher relativ leicht zu knacken. Dann begannen Regierungsbehörden damit, neue Techniken zu entwickeln, um über physische Sicherheitsbeschränkungen hinaus wichtige Informationen zu schützen.

Problemsuche und -behebung

Durch die dramatischen Änderungen in Computerumgebungen während der 80er- und frühen 90er-Jahre wurden an die Netzwerksicherheit neue und höhere Anforderungen gestellt. Zuerst wandelten sich die Computer von proprietären, «dummen» Mainframe-Terminalsystemen zu Client-Server-Modellen mit Windows- oder UNIX-Betriebssystem. Durch die weitverbreitete Verwendung derselben Betriebssysteme wurden viele Unternehmen ein leichtes Ziel für Hacker, welche die Sicherheitslücken dieser Systeme ausnutzten.
Durch die wachsende Zahl der Internet-Benutzer wurden Netzwerke immer empfindlicher für Angriffe. Systemintegrität, Denial-of-Service-(DoS)Angriffe und Systemverfügbarkeit wurden die Topthemen der Sicherheitsexperten. Langsam kristallisierte sich die Form der Netzwerksicherheit heraus, wie wir sie heute kennen. Kommerzielle Softwarehersteller begannen, sich am wachsenden Markt der Netzwerksicherheit mit einzelnen Produkten zu Firewalls, Verschlüsselung und Antivirenlösungen zu beteiligen.

Auswerten und Verwalten

Heute hat die Netzwerksicherheit in den meisten Unternehmen Priorität. Dies ist unter anderem der breiten Berichterstattung über Sicherheitsverletzungen wie beispielsweise die DoS-Angriffe im Februar zu verdanken. Praktisch jede Führungskraft in den Chefetagen hat sich der Herausforderung Netzwerksicherheit gestellt. Sicherheit wird nicht mehr nur als blosses Technologiethema angesehen, sondern es geht nun vielmehr um die Frage, inwieweit Sicherheit die Geschäftsfähigkeit, Kundenbindung und Aktionärszufriedenheit beeinflusst. Durch die Minimierung von Sicherheitsvorfällen können Unternehmen ihren guten Ruf wahren und unnötige Gerichtsprozesse sowie die Einmischung von Bundesbehörden vermeiden.
Die täglichen Geschäftsabläufe bedeuten ein Risiko für Unternehmensnetzwerke. Die schnelle Umsetzung neuer Internet-Programme, von webfähigen Anwendungen über Extranets zu E-Commerce, stellt die Netzwerksicherheit jedoch vor immer neue Herausforderungen.
Chief Information Officers (CIOs) werden damit beauftragt, wirksame Mittel zur Minimierung von Sicherheitsvorfällen zu finden. Sie stehen vor der Herausforderung, eine Sicherheitsarchitektur zu entwerfen, die Geschäftsziele mit Technologiefragen in Einklang bringt. Durch die Erstellung von Sicherheitsplänen ihrer Ressourcen, Schwachstellen und Risiken können IT-Experten Systeme wirkungsvoller schützen. Jedoch handelt es sich um keine leichte Aufgabe. Netzwerke sind ein Labyrinth von Anwendungen und Hardware und haben zahlreiche Schwachstellen. CIOs bauen auf die Mithilfe von Softwareherstellern, um Netzwerksicherheit effektiver überwachen und verwalten zu können.



Neue Technologien und neue Bedrohungen – die Netzwerksicherheit erfährt immer neue Herausforderungen.

Erhöhung der Netzwerksicherheit

Zwar ist es unmöglich, Sicherheitsvorfälle gänzlich zu verhindern, jedoch gibt es zur Verwaltung der Netzwerksicherheit einen bewährten und effektiven Ansatz. Dies sind die grundlegenden Schritte:

Verstehen der Zielsetzung

Man muss sich der Tatsache bewusst sein, dass ein Unternehmen nicht mehr sicher ist, sobald es an ein Netzwerk angeschlossen ist. Risiko-Management ist nicht gleich Risikovermeidung. Das Netzwerk wird nie zu 100% sicher sein. Manchmal sind die Kosten zur Beseitigung einer Schwachstelle grösser als die Kosten, die ein Angriff verursachen könnte. Daher bleibt dieser Teil des Netzwerks anfällig. In einigen Fällen gibt es für manche Schwachstellen keine Möglichkeit der Beseitigung. Bedrohungen entstehen schnell, Gegenmittel dagegen, wenn überhaupt, sehr langsam.

Durchführen von Sicherheitsüberprüfungen

Die Unternehmens-Ressourcen sollten genau bestimmt und dann festgestellt werden, durch welche Schwachstellen und Bedrohungen sie Gefahren ausgesetzt sind. Man muss sich mit der Wahrscheinlichkeit auseinandersetzen, mit der bestimmte Bedrohungen auftreten könnten. Der Umfang an Netzwerkressourcen, der durch bestimmte Angriffe oder Netzwerkausfälle verloren gehen könnte, sollte festgehalten werden. Es ist notwendig, die Ressourcen nach Prioritäten zu klassieren und kritische Systeme mit den besten Sicherheitsmassnahmen zu schützen.

Sicherheitsrichtlinien und -massnahmen

Nach einer Überprüfung des Netzwerks können IT-Experten fundierte Entscheidungen über Unternehmenssicherheitsrichtlinien und -massnahmen treffen. Die Ausarbeitung genauer Richtlinien und Massnahmen unterstützt IT-Experten dabei, aktiven Netzwerkschutz wirksam und kosteneffektiv zu betreiben.

Beste Schutzvorrichtungen für kritische Systeme

Für die meisten gefährlichen Schwachstellen bestehen bekannte Schutzmöglichkeiten. Zuerst sollte bestimmt werden, welche Systeme kritisch sind und welches deren Schwachstellen sind. Dann lässt sich herausfinden, welche Gegenmassnahmen für diese Schwachstellen die besten sind. Es lohnt sich, einen grossen Teil an Zeit und Ressourcen für kritische Systeme aufzubringen, um Verluste aufgrund von Sicherheitsvorfällen zu minimieren.

Grundlegende Sicherheitsvorrichtungen für nichtkritische Systeme

Hacker investieren nicht viel Zeit und Mühe, um diese Systeme zu knacken. Wenn ein Hacker die meisten Hintertüren verriegelt findet, wird er es wahrscheinlich woanders versuchen. Das Schliessen offensichtlicher Sicherheitslücken schreckt die meisten Eindringlinge ab.

Aktionsplan für den Fall eines Angriffs

Da Netzwerke niemals vollständig sicher sein können, müssen IT-Experten ausreichend auf einen Sicherheitsvorfall vorbereitet sein. Die Erstellung eines Aktionsplans stellt dabei eine lohnende Investition dar. Neben einem sicheren Netzwerk ist die Schadensreduzierung nach einem Sicherheitsvorfall eine der wichtigsten IT-Zielsetzungen. Dies beinhaltet die Implementierung von Frühwarnsystemen wie beispielsweise Intrusion-Detection-Systemen sowie die Sicherung kritischer Systeme und Daten.

Gewappnet für die Zukunft

Viele Unternehmen haben bereits damit begonnen, ihre Netzwerksicherheitsstrategien zu überarbeiten. Aktives Management und die Überwachung der Netzwerksicherheit werden langsam für jeden zur Selbstverständlichkeit. Im Zug der zunehmenden Bedrohungen der Netzwerksicherheit ist ein gutes Risiko-Management für das Überleben eines Unternehmens unabdingbar. Wenn Unternehmen die Netzwerksicherheit als Teil des aktiven Managements von Bedrohungen betrachten, sind sie für neue Herausforderungen im Bereich der Netzwerksicherheit gewappnet und können Verluste problemlos auf ein Minimum reduzieren. [4]

Symantec (Switzerland) AG
Grindelstrasse 6
CH-8303 Bassersdorf
Tel. 01 838 49 32
Fax 01 838 49 01
E-Mail: Heike_Faller@symantec.com