

Netzwerksicherheit

Mangelnde Sicherheit ist ein Spiel mit dem Feuer



Mehr denn je zuvor verlassen sich Unternehmen jeder Grösse auf ihre Netzwerke bei der Abwicklung sämtlicher Aspekte ihres Geschäfts – von der internen und externen Kommunikation über Bestandskontrolle, Abrechnung und Vertrieb bis hin zum Handel mit externen Partnern. Gerade KMU sind aus den verschiedensten Gründen allzu häufig nicht für eine ausreichende Netzwerksicherheit besorgt – was durchaus zu einem Spiel mit dem Feuer werden kann.

Roland Zulliger

Im IT-Kontext steht der Begriff Sicherheit für den Einsatz von Soft- und Hardware, um via Netzwerk miteinander verknüpfte Computer-Systeme vor internen und externen Gefahrenquellen wie Viren, Würmern, Informationsdiebstählen und Hackerangriffen zu schützen. Sicherheit von Netzwerken hat sich zu einem erfolgskritischen Faktor in Unternehmen entwickelt. Auch für die meisten KMU ist es von eminenter Bedeutung, ihre Firmendaten adäquat zu schützen.

Kosten versus Schaden

Die finanziellen Verluste, die Unternehmen durch unbefugten Zugriff auf ihre Daten erleiden, sind so hoch, dass sie in keinem Verhältnis zu den Kosten leistungsfähiger Sicherheitslösungen stehen. Oder mit anderen Worten: Es ist viel einfacher und vor allem günstiger, Ungemach in der IT bereits im Vorhinein zu verunmöglichen, statt im Nachhinein in mühseliger und kostenaufwändiger Arbeit die Datenstruktur wieder

herzustellen. Und trotz aller Anstrengungen – eine Gewähr für den Erfolg solch nachträglichen Bemühungen gibt es nicht. Daten können unwiderruflich verloren gehen, der Schaden kann bleibend angerichtet sein.

Die Sünden vieler KMU

Mit der zunehmenden Verknüpfung und der Anbindung von Infrastrukturen, die bis vor wenigen Jahren noch als gänzlich computerfremd galten, werden Netzwerke immer vielfältiger. Damit verbunden werden auch die Angriffsmöglichkeiten mannigfaltiger, die sich längst nicht mehr nur auf Software von Personalcomputern beschränken. Umfassender werden somit auch die Auswirkungen eines Angriffs, sind doch mehr als nur ein oder einige wenige Computer betroffen, sondern eine gesamte Infrastruktur. Im Extremfall liegt nach einem punktuellen Angriff ein ganzes Unternehmen danieder.

Untersuchungen haben gezeigt: Trotz einer wachsenden Sensibilisierung wird in vielen KMU nach wie vor nicht ausreichend für

Netzwerksicherheit gesorgt. Die Gründe dafür sind vielfältig: Es gibt Stimmen, die behaupten, kleine Unternehmen wären weniger anfällig für Sicherheitsangriffe. Dies ist ein Trugschluss, denn gerade die grossen Unternehmen bauen ihre Netzwerksicherheit aus, was zur Folge hat, dass Hacker und andere Personen mit böswilligen Absichten ihre Aufmerksamkeit auf kleine und mittel-grosse Unternehmen lenken.

Demgegenüber ist es eine Tatsache, dass für viele Unternehmen die Netzwerksicherheit





zu komplex ist und einen zu grossen Ressourcenaufwand erfordert, um sich damit wirkungsvoll auseinander zu setzen. Für andere ist die Netzwerksicherheit ein weiterer Kostenfaktor, der das Unternehmenswachstum angeblich nicht vorantreibt. Wer allerdings das Thema aus einer anderen Perspektive betrachtet, sieht die Netzwerksicherheit als unerlässliche Voraussetzung für die Kontinuität des Geschäfts und nicht als ein IT-Problem an. Netzwerke sind für Unternehmen zu einem wesentlichen Bestandteil ihrer Geschäftstätigkeit geworden; deshalb ist eine Sicherheitsstrategie genauso wichtig wie eine Vertriebs- und Marketingstrategie.

Gefahr nicht unterschätzen

Die Dynamik der Bedrohungslage ist nicht zu unterschätzen: Die Gefahren für die Daten und Ressourcen wachsen beinahe täglich. Und immer werden neue Arten von

Angriffen entwickelt. Diese verbreiten sich immer mehr und können auch immer einfacher gestartet werden. Zum einen liegt das an der Allgegenwart des Internets. Bereits heute sind Millionen von Geräten in das Internet eingebunden und täglich werden es mehr. Damit haben Hacker auch immer leichteren Zugriff auf Schwachstellen im System. Das gigantische Ausmass und die Omnipräsenz des World Wide Web haben ausserdem dazu geführt, dass Hacker ihr Wissen weltweit austauschen können. Sucht man im Internet nach Begriffen wie «hack», «crack» oder «phreak», findet man Tausende von Sites, die vielfach einen böserartigen Code oder gar Tools zur Verwendung dieses Codes enthalten.

Auch unverschlüsselte Wireless-Netzwerke bieten heute mit der zunehmenden Verbreitung von Wireless-fähigen Computern relativ einfache Einstiegsmöglichkeiten für Eindringlinge. Bereits mit einer Dose Pringels-

Pommes-Chips lässt sich eine einfache, mobile Empfängerstation bauen, mit der man offene Netzwerke suchen kann. Auf Kosten anderer im Internet zu surfen ist dabei noch das kleinste mögliche Übel: Die Schäden reichen vom einfachen Datendiebstahl bis hin zur vorsätzlichen Zerstörung von Netzwerkeinstellungen und der Torpedierung der Geschäftstätigkeit.

Strategisches Kernelement

Die Sicherheit eines Netzwerks ist eines der elementarsten Kernelemente einer langfristigen Strategie zur Aufrechterhaltung der operationellen Prozesse eines Unternehmens. Mit zunehmendem Ausbau der IT-Infrastruktur muss daher in selbem Masse auch die IT-Sicherheit das gesamte Unternehmen durchdringen. Netzwerke werden heute oft noch wie eine Burg geschützt: Mit einer Mauer drum herum, die Eindringlinge abhalten soll. Nur: Netzwerke sind nicht unbedingt mit Burgen gleichzusetzen, sondern bilden dezentrale, verteilte Einheiten, die miteinander verbunden sind. Und wo keine Burg ist, nutzt auch eine Mauer nicht viel.

Fazit

Moderne Sicherheitskonzepte müssen demnach anders gestaltet werden. Statt Sicherheit nur an einem Punkt zu bieten, gehen die Lösungen heute in die Tiefe. Denn alles kann zum Ziel von Angriffen werden:





Tipps

IT-Sicherheit

Die folgenden Tipps können helfen, einen wirksamen Plan für die Netzwerksicherheit zu entwickeln und Unterstützung für den Einsatz dieses Plans zu erhalten.

- Das Augenmerk nicht ausschliesslich auf den Return on Investment (ROI) richten. Gleichermassen den Return on Value (ROV) beachten: An die möglichen verheerenden Folgen denken, die eine Sicherheitsverletzung haben könnte, wie beispielsweise Umsatzverluste oder rechtliche Auseinandersetzungen mit Kunden.
- Nie davon ausgehen, dass Angriffe auf die Netzwerksicherheit nur von aussen erfolgen. Selbst treue Mitarbeiter können ungewollt die Sicherheit kompromittieren;
- Sicherheitsprobleme nicht lösen, indem man Flickwerk betreibt, sondern eine ganzheitliche Sicherheitsstrategie einsetzen, die lückenlos alle Sicherheitsbereiche abdeckt. Bei der Entwicklung und Implementierung von Sicherheitsstrategien integriert arbeiten und sich dabei auf Technologie, Schulung, Standortsicherheit usw. konzentrieren.
- Das Gleichgewicht finden zwischen Sicherheit und Nutzbarkeit. Je sicherer das Netzwerk, desto schwieriger ist unter Umständen seine Nutzbarkeit.

Router, Switches, Hosts, Netzwerke, Applikationen, Informationen, Management Tools – nichts bleibt von Attacken verschont. Ständig entstehen neue Angriffsarten, die durch ein einzelnes Gerät nicht mehr abgeblockt werden können. Sicherheit muss daher auf mehreren Ebenen ansetzen und durch das gesamte Netzwerk hindurch wirken. ■



Fragen

Roland Zulliger
Sales Manager KMU
Cisco Systems Switzerland
Tel. 044 878 93 07
rzulliger@cisco.com
www.cisco.ch

Anzeige

Voice over IP: Sprache und Daten über dasselbe Netz.



sunrise 1com managed – für einen optimalen Kommunikationsfluss zum fixen Monatstarif.

Sprache und Daten über ein einziges Netz – das belebt die Geschäftsprozesse von KMU mit 10 bis 200 Mitarbeitenden. Mit sunrise 1com managed ist der Umstieg auf eine neue Voice over IP Telefonanlage mit geringen Investitionskosten möglich. Sie bezahlen einen festen Preis pro Anschluss, Mitarbeitenden und Monat: ¹⁾ Installation, Betrieb und Wartung der Anlage sind inbegriffen. sunrise 1com managed lässt sich mit Optionspaketen erweitern. Und ermöglicht neue, integrierte Sprach- und Datenanwendungen, die ein einziges IP-Netz nutzen.

¹⁾ Weitere Kosten, die z. B. für Gesprächsgebühren anfallen können, werden nach Aufwand verrechnet.

Ihre Vorteile:

- VoIP-Telefonanlage für 10 bis 200 Mitarbeitende mit Unified Communication (IP) und ISDN-/Analog-Anschlüssen, sunrise Services inklusive
- nur noch ein Netz für Sprach- und Datenkommunikation
- geringe Investitionskosten
- neueste Sicherheitsstandards
- Innovative Technologien wie Dualmode-Handys (GSM/WLAN) oder Video-Conferencing

Checkliste

Massnahmen für die Netzwerksicherheit

Jedes Unternehmen sollte über einen schriftlichen und gut durchdachten Plan für die Netzwerksicherheit verfügen. Die Beantwortung der folgenden Fragen kann dabei helfen, die eigenen Sicherheitsrichtlinien zu entwickeln.

1. Eine Bestandsaufnahme der bestehenden Sicherheitstechnologien machen: Werden die folgenden Sicherheitstechnologien eingesetzt?

- Firewall
- Virtuelle private Netzwerke (VPN)
- Intrusion-Prevention-Systeme
- Anti-Virus-Lösungen
- Sicheres Wireless-Netzwerk
- Anomaly Detection (Erkennung ungewöhnlicher Ereignisse)
- Identitätsmanagement
- Prüfung der Einhaltung von Sicherheitsrichtlinien

2. Die wichtigsten digitalen Vermögenswerte und die damit verbundenen Zugriffsmöglichkeiten identifizieren:

- Welche digitalen Vermögenswerte hat das Unternehmen?
- Wie hoch ist ihr Wert?
- Wo befinden sich diese Vermögenswerte?
- Wer hat Zugriff darauf und warum? Haben alle Mitarbeiter die gleichen Zugriffsrechte für das Netzwerk und die Anwendungen?
- Erstreckt sich der Zugriff auch auf Partner und Kunden?
- Wie wird der Zugriff kontrolliert, überprüft und überwacht?

3. Potenzielle Auswirkungen einer Sicherheitsverletzung einschätzen:

- Welche potenziellen finanziellen Auswirkungen hätte ein Netzwerkausfall, der auf Grund einer Sicherheitsverletzung verursacht wurde?
- Würde eine Sicherheitsverletzung die Lieferkette unterbrechen und, falls ja, inwieweit?
- Welche Auswirkungen hätte der Absturz der Website? Wie lange kann die Website nicht verfügbar sein, bevor dies für das Unternehmen wesentliche finanzielle Folgen hätte?
- Stehen auf der Website E-Commerce-Features zur Verfügung? Wie lange kann die Handelsschnittstelle nicht verfügbar sein, bevor dies für das Unternehmen wesentliche finanzielle Folgen hätte?
- Ist das Unternehmen gegen Cyberangriffe oder den Missbrauch von Kundendaten versichert? Wenn ja, ist der Versicherungsschutz angemessen?

4. Gegenwärtige und zukünftige Anforderungen einschätzen:

- Wie wird der Geschäftsplan in den nächsten Jahren aussehen?
- Wann wurden die Netzwerkgeräte das letzte Mal aktualisiert? Wann die Software und Virusdefinitionen?
- Welches Sicherheitstraining erhalten die Mitarbeiter?
- Wie wird sich das Unternehmenswachstum auf seine digitalen Vermögenswerte und deren Wert für das Unternehmen als Ganzes auswirken?
- Werden die Mitarbeiter, Kunden oder Partner in Zukunft verstärkt von entfernten Standorten aus auf diese digitalen Vermögenswerte zugreifen?

Business Excellence 2006

Die Schweizer Unternehmertagung vom 26. Oktober 2006 im KKL Luzern zum Thema «Zukunftskompetenz»

Agenda

12.00 Uhr **Networking-Lunch**



Alenka Ambroz, Moderation
Kommunikationsberaterin
ehemals Moderatorin „10vor10“

13.30 Uhr **Werner von Allmen**
Geschäftsleiter TQM Forum Schweiz
Eröffnung der Tagung



Anton Lauber
CEO Schurter AG
Präsident TQM Forum Schweiz



Prof. Dr. Dr. Franz Josef Radermacher
Leiter Forschungsinstitut für anwendungsorientierte Wissensverarbeitung Ulm



Ernst Uhlmann
Geschäftsleiter FELA Management AG
Visionär für das LSVA-System



Stefan Prebil
General Manager
Sandoz Pharmaceuticals AG

Verleihung Swiss Award for Business Ethics



Dr. Pierin Vincenz
Vorsitzender der Geschäftsleitung
der Raiffeisen Gruppe

18.00 Uhr **Apéro** und Gespräch mit den Experten

Swiss Award for Business Ethics

In Zusammenarbeit mit CASH verleiht das TQM Forum Schweiz im Rahmen der Business Excellence 2006 den Swiss Award for Business Ethics.



Medienpartner

CASH

KMU

Designed by Glasi Hergiswil

Anmeldungen

TQM Forum Schweiz
www.tqm-forum.ch Tel. 041 417 10 16
excellence@tqm-forum.ch

Das Kompetenzzentrum
für Business Excellence
TQM FORUM
SCHWEIZ