



Foto: Nick Benjaminsz

TenMinITs

In zehn Minuten zur IT-Sicherheit

Die IT-Sicherheit wird in kleinen und mittleren Unternehmen oft immer noch nicht richtig ernst genommen. Dazu zunächst drei Beispiele aus unserer Praxis: Bei einer eigenen Umfrage unter 98 schon größeren Mittelständlern glaubte die Hälfte, gut geschützt zu sein. Vierzig Prozent davon war aber gegen übliche Internet-Gefahren überhaupt nicht geschützt.

Bei einem kleineren Unternehmen mit sensitiven Daten war der Router zwischen Firmennetz und Internet vollständig offen, ein Zugriff vom Internet her war aufgrund des nicht geänderten Standardpasswortes jederzeit möglich.

Das dritte Beispiel hat eine besondere Tragweite. Einem uns bekannten Unternehmen mit 60 Mitarbeitern wurde die elektronische Personaldatei entwendet. In der Folge wurden die Know-how-Träger mit gezielten Angeboten zur Konkurrenz abgeworben. Diesen Aderlass hat das Unternehmen nicht überstanden.

Aus unseren Auswertungen wissen wir, dass auf typischen Internet-Rechnern pro Monat mehr als tausend unzulässige Zugriffsversuche stattfinden, mit denen wichtige System-Informationen ausgespäht werden sollen. Und der *Mydoom*-Wurm steckte zeitweilig in jeder dritten E-Mail Europas. Insgesamt also Grund genug, gerade im Mittelstand die IT-Sicherheit ernst zu nehmen.

IT-Sicherheit ist Chefsache. Denn nur die Unternehmensleitung kann die möglichen finanziellen Auswirkungen beurteilen. Sicherheitsmaßnahmen, die erkennbar notwendig sind, müssen von der Unternehmensleitung auch ergriffen werden, sonst droht (sogar persönliche) Haftung nach §§ 278 und 823 BGB, 43 GmbHG, 93 II AktG oder 266 StGB.

TenMinITs ist als „Management Summary“ gedacht, das in zehn Leseminuten die allerwichtigsten Fakten der IT-Sicherheit für ein mittelständisches Unternehmen zusammenstellt. Zehn Schutzmaßnahmen und zehn Praxistipps bilden die Basis einer Mini-IT-Sicherheit. Natürlich ist in zehn Minuten kein Sicherheitskonzept zu erstellen. Aber die ersten zehn Minuten können die effizientesten sein.

Notwendige Voraussetzung jeder Sicherheits-Maßnahme ist zunächst eine zumindest schematische Dokumentation der IT-Landschaft, gegliedert in

- Systeme, insbesondere solche, die sicherheits- oder ausfallkritisch sind,
- Netzwerktopologie mit sachgemäßen Vertrauensbeziehungen,
- Nutzergruppen mit ihren Kommunikationsprofilen

Anschließend sind in einer Risikoanalyse mögliche Schadensfälle zu klassifizieren (z.B. niedrig, mittel, hoch). Dabei kann es nicht darum gehen, jedes Risiko auszuschließen, denn totale Sicherheit gibt es nicht. Angemessene Schutzmaßnahmen sind aber umzusetzen und aktuell zu halten, siehe den nachfolgenden Katalog.



Foto: Lucian Binder

Minutes 1: Die 10 wichtigsten IT-Schutzmaßnahmen

- Physische Zugangskontrolle
- Zugriffskonzept, (starke) Authentifizierung, Logging
- (Starke) Verschlüsselung von sensiblen Daten
- Redundante Auslegung ausfallkritischer Komponenten (Platten, Lüfter, Netzteile, USV, Kühlung)
- Dokumentation, Schulung, Sicherheitsbewusstsein
- Tägliches Backup und Auslagerung ins Bankschließfach
- Schutz gegen Hacker (Firewall)
- Schutz gegen Viren, Würmer, Trojaner
- Schutz gegen Spam
- Intrusion Detection (Erkennung von Angriffsmustern)

Wer die folgenden Praxistips sämtlich befolgt, hat schon mehr als eine Mini-IT-Sicherheit erreicht.

Minutes 2: Die 10 wichtigsten Praxistips der IT-Sicherheit

- Spam sofort löschen, nie beantworten, keine namentlichen E-Mail-Adressen ins Web setzen
- Virenmusterdatenbank mindestens täglich updaten
- Nur starke Passwörter einsetzen (z.B. Satz ausdenken und die Anfangsbuchstaben der einzelnen Wörter nehmen)
- Software-Patches zeitnah einspielen

- Mit Memory-Sticks vorsichtig umgehen, Datenklau droht
- Die Sicherheit zur Chefsache erklären, Verpflichtungserklärungen von den Mitarbeitern einfordern
- Gesetze befolgen, z.B. Anbieterkennzeichnung im Web nach TDG, Datenschutz nach BDSG, UrhG zu Raubkopien
- Ein *Basis Security Audit* durchführen lassen (bringt Grundlage in die Sicherheit, kostet nur wenige Manntage Aufwand)
- Für die IT-Sicherheit ein Prozent des Umsatzes einsetzen
- Restrisiken bewusst machen, ggf. versichern (z.B. Betriebsunterbrechungsversicherung)

Für die IT-Sicherheit existieren komplexe und umfangreiche Kriteriensysteme und Standards (z.B. ISO 17799, BSI IT-Grundschriftbuch, Common Criteria, ITSEC). Für die (partielle) Anwendung solcher Systeme – das Grundschriftbuch mit seinen 59 Bausteinen von „Archivierung“ bis „Verkabelung“ ist in drei DIN-A4-Ordern untergebracht – muss ein mittelständisches Unternehmen mit 10 bis 100 Manntagen Aufwand rechnen. ■

Weitere einführende Informationen:

Bundesamt für Sicherheit in der Informationstechnik
www.bsi.de

Bundesministerium für Wirtschaft und Arbeit
www.mittelstand-sicher-im-internet.de

Interessengemeinschaft sicher vernetzte Wirtschaft
www.isvw.de

BITKOM Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V.
www.bitkom.org

Anmerkung: »Minutes« ist englisch für »Protokoll«.



Der Autor:
Dr. Kurt Brand
Pallas GmbH
Hermülheimer Str.10
D-50321 Brühl
Telefon: 02232 – 18 96-0
E-Mail: pr@pallas.com
Web: www.pallas.com