

DIE BEDROHUNG IST REAL!

Mögliche IT-Sicherheitsrisiken und Szenarien zu Schadensfällen

Zwischen der Größe eines Unternehmens und der Bedrohung der IT-Sicherheit besteht kein direkter Zusammenhang. Das bedeutet, dass Internetrisiken und Cyberschädlinge alle Unternehmen gleichermaßen gefährden können – also auch Ihres. Das Problem: Die Verantwortlichen sind sich dieser Risiken häufig nicht bewusst.

So ist z. B. kaum bekannt,

... dass im Büroalltag das Internet im Schnitt bis zu 40 Prozent missbräuchlich genutzt wird.

... 55 Prozent der Benutzer ihr Passwort mindestens einmal und neun Prozent jedes Mal aufschreiben.

... 40 Prozent mit Mitarbeitern oder Bekannten ein gemeinsames Passwort benutzen.

Mangelndes Sicherheitsbewusstsein oder eine fehlende Sicherheitspolitik im Unternehmen kann neben finanziellen Einbußen auch eine Reihe weiterer Schäden nach sich ziehen. Dass diese Risikopotenziale keine graue Theorie, sondern eine ganz reale Bedrohung sind, zeigen die nachfolgend dargestellten Szenarien aus realen Schadensfällen der letzten Jahre in Europa und den USA.

Wissen Sie, was diese Übeltäter schon alles angerichtet haben?



DER FAKTOR MENSCH

Was wäre, wenn...

- ... ein Mitarbeiter Betriebsgeheimnisse stiehlt und mit Ihrem Knowhow zur Konkurrenz geht?
- ... ein Angestellter persönliche Daten (z.B. Personal- und Finanzinformationen) von einem Server stiehlt und diese an Marketing-Unternehmen verkauft oder sie für Betrugereien verwendet?
- ... komplette Datensätze über vermögende Kunden auf CD-ROM in der Redaktion einer Zeitung landen?
- ... ein Angestellter eines IT-Dienstleisters im Rahmen seiner Arbeit Zugang zu unterschiedlichen Datenbanken von Kreditunternehmen hat, Informationen von ca. 30.000 Konten stiehlt und anschließend inklusive der Kreditkartennummern an Interessenten für 60 US-Dollar pro Datensatz verkauft?
- ... ein ehemaliger Mitarbeiter das Computernetzwerk der Firma hackt, Daten löscht und einen Server außer Betrieb setzt, der für die ausländischen Geschäfte des Unternehmens von größter Wichtigkeit ist?
- ... ein Wurm in das Netzwerk eingespielt wird und durch die Infizierung auf den Bildschirmen der Mitarbeiter plötzlich Bilder mit pornographischem Inhalt zu sehen sind?
- ... ein Alkoholsünder bei der Vorladung kurz allein gelassen wird und dieser über einen nicht gesperrten Computer seine Alkoholfahrt aus dem Zentralrechner der Polizei löscht?
- ... zwei Männer sich als Computertechniker ausgeben und mit zwei Werkzeugtaschen ausgerüstet am Sicherheitsschalter mit falschen Namen vorstellen, um nach Feierabend angeblich Wartungsarbeiten an Servern durchzuführen, aber stattdessen einen Server mit wichtigen Informationen stehlen?
- ... der Computer-Support durch eine simple Verwechslung von Datenträgern das gesamte Data Warehouse einer Bankenkette löscht?

PORNOGRAPHIE AM ARBEITSPLATZ

Was würde es bedeuten, wenn...

- ... durch ihre Mitarbeiter Hardcore-Pornographie auf der Firmen-Festplatte gespeichert oder sogar über das Internet ausgetauscht wird?
- ... Minderjährige, also etwa Praktikanten oder Auszubildende, innerhalb des Unternehmens mit Pornographie konfrontiert werden?
- ... Sie, bei erlaubter privater Nutzung, durch Bereitstellung der Internet- und E-Mail Zugänge rechtlich selbst zum Telekommunikationsanbieter geworden sind?
- ... dem Arbeitnehmer bei entsprechenden Verstößen nicht eindeutig nachzuweisen ist, dass ihm die in der Richtlinie zur privaten Nutzung von E-Mail und Internet aufgestellte ausdrückliche Anweisung bekannt war?

ONLINE-BETRUG

Was wären die Folgen, wenn...

- ... Täter E-Mails verschicken, die Spendenaufrufen hilfstätiger Organisationen gleichen, um sich Kreditkartendaten zu beschaffen, die dann zu einer anderen Web-Seite, z.B. in Asien übermittelt werden?
- ... man auf einer gefälschten Webseite eines Billigfliegers vermeintlich ein Ticket bestellt und man seine Kreditkartendaten dort eingibt?
- ... Sie mittels so genannter Dialer beim Besuch von Internetseiten zu teuren Einwahlen umgeleitet werden?

HACKER

Welche Schäden können entstehen, wenn...

- ... Sie von krimineller Motivation angetriebenen Hacker-Banden - der so genannten "Cyber-Mafia" - angegriffen werden?
- ... ein Hacker, der Ihre Webseite gehackt hat, Ihre Nutzer und den gesamten E-Mail-Verkehr auf eine von ihm entwickelte Webseite umleitet?
- ... der PC eines Arztes unzureichend gegen Fremdzugriffe gesichert ist, so dass vertrauliche Patienteninformationen in einem lokalen Internet-Diskussionsforum veröffentlicht werden?
- ... ein IT-Experte das Computersystem eines Gesundheitszentrums hackt und dadurch Zugriff auf die Daten von hunderten von Patienten erlangt?
- ... ein Hacker ein Sicherheits-System eines Dienstleistungsunternehmens durchbricht, welches Transaktionen für Kreditinstitute abwickelt und Zugang zu ungefähr 5,6 Millionen Kreditkartenkonten erlangt?
- ... gängige Software-Tools zum Entschlüsseln von Passwörtern genutzt werden, um Zugang zu zentralen Linux und Solaris Servern von Universitäten zu erhalten?
- ... Ihre Homepage gehackt wird und die Hackergruppe veränderte oder neue Inhalte darauf bereitstellt?

SPAM-MAILS

Wollen Sie riskieren, dass...

- ... Ihr Firmencomputer von einer Spam-Gang unter fremde Kontrolle gebracht wird und dann, als sog. Spam-Relais, zum massenhaften Verschicken von Werbemails missbraucht wird?
- ... Mitarbeiter und Kunden weder E-Mails verschicken noch empfangen können, da Ihre Mail-Server Angriffsziel einer Spam-Attacke sind?
- ... Sie oder Ihr Unternehmens-Mailserver als Unschuldige auf den „Schwarzen Listen“ der Provider landen?

BÖSARTIGE SOFTWARE, VIRUS

Können Sie verantworten, dass...

- ... bei Ihnen kein automatisierter Update-Mechanismus eingerichtet ist, mit dessen Hilfe im Eilverfahren die Viren-Schutzprogramme auf allen Rechnern mit den neuen Viren-Signaturen aktualisiert werden können?
- ... Sie Ihr durch einen Internet-Wurm verseuchtes System bis zu mehrere Tage vom Netz nehmen müssen?
- ... ein Internet-Wurm jegliche E-Mail-Kommunikation unmöglich macht und die Mitarbeiter über eine persönliche Mitteilung darüber unterrichtet werden müssen, dass dieser Wurm Dritten den Zugriff auf ihre Computer und dadurch das Verändern oder Löschen von Dateien ermöglicht?
- ... Sie Mails mit den Betreffzeilen wie z.B. "Urgent Windows Update", "Important Windows Update" erhalten, die mit einem Link zum vermeintlichen Sicherheitsupdate versehen sind, welches jedoch mit einem Trojaner gespickt ist?
- ... Sie unschuldig verurteilt werden, weil ein heimlich eingeschleustes Programm auf Ihrer Arbeitsstation zum Download von pornografischen, zum Teil Minderjährige zeigenden, Bildern benutzt wurde?
- ... Ihr Außendienst-Mitarbeiter sein Laptop auch privat nutzt und zuhause über Modem ungeschützt eine Internetverbindung herstellt?

DATENVERLUST

Welche Konsequenzen hätte es, wenn...

- ... ein Hacker einen Datenverlust verursacht, so dass ein Backup eingespielt werden muss und alle Transaktions-Daten seit der letzten Sicherung verloren gegangen sind?
- ... ein Server durch einen Festplattendefekt ausfällt und die Daten vom Sicherungsband wieder eingespielt werden sollen, sich aber herausstellt, dass das Bandlaufwerk offenbar bereits längere Zeit defekt war und gar keine Daten auf die Sicherungsbänder geschrieben hatte?
- ... Ihr einziger Administrator durch einen schweren Unfall ausfällt und nicht mehr arbeitsfähig ist?
- ... ungesicherte Laptops, Datenträger oder Informationen gestohlen werden oder verloren gehen?