heute.de computer

heute-Nachrichten
- Startseite
- Schlagzeilen
- Politik
- Magazin
- Wirtschaft
- Computer
- Sport
- Wetter
- Börse

ZDFmediathek

Sendung verpasst?
Jetzt ansehen

- ZDF heute
- ZDF heute journal
- ZDF heute nacht

Sendungen von A-Z

Service
- Podcast-Angebot
- heute-Telegramm
- Bildschirmschoner
- PDA-Angebote
- WAP-Dienste
- Newsletter
- RSS-Angebot
- Nachrichtenbanner
- Sidebar
- heute als Startseite

Das Passwort pappt am Monitor

Sicherheitskongress Secure 2008: Wie gefährdet sind deutsche Unternehmen?

von Alfred Krüger und Volker Heil

ZDF, mev [M]

Schadprogramme, kriminelle Hacker, Datenspionage - deutsche Unternehmen wissen sich zu schützen. Schutzprogramme gehören überall zum Standard. Die "Schwachstelle Mensch" bleibt außen vor. Ein Sicherheitskongress in Bad Homburg zeigt die Gefahren auf.

Drucken Versenden 03.06.2008 [Archiv]

Deutschlands Unternehmen haben technisch aufgerüstet. Die gebetsmühlenartig vorgetragenen Warnungen vor Cyberkriminellen und den Gefahren aus dem Internet sind mittlerweile auch in den letzten deutschen Chefetagen angekommen. Antivirensoftware gehört überall zum Standard. Firewalls kontrollieren den ein- und ausgehenden Datenverkehr, und E-Mail-Filter sollen dafür sorgen, dass in den elektronischen Postfächern der Mitarbeiter nur erwünschte E-Mails landen.

"Technik löst nicht die Probleme"

Entsprechend hoch ist die "gefühlte" Sicherheit. 98 Prozent der Entscheidungsträger schätzen die IT-Sicherheit in ihrem Unternehmen als ausreichend oder besser ein. Das ergab eine Untersuchung des US-Sicherheitsunternehmens Websense. Mehr als die Hälfte der befragten deutschen Unternehmen hielt die eigene Firma sogar für ausgesprochen gut geschützt. Ein Viertel glaubte gar, komplett gegen Netzangriffe jeglicher Art gerüstet zu sein.

IT-Löcher auf dem Gang
- Datenfalle Kopierer

Die Wirklichkeit sieht völlig anders aus, sagen Sicherheitsexperten. Technische Schutzmaßnahmen bleiben vielfach wirkungslos. Wichtige Passworte etwa, die den Zugriff auf sensible Kundendatenbanken regeln sollen, werden auf Notizzettel geschrieben, die gut sichtbar am Monitor befestigt werden. E-Mail-Anhänge werden nach wie vor bedenkenlos geöffnet. Schutzsoftware wird kurzerhand abgeschaltet, wenn sie zu oft Alarm schlägt. Und in den Arbeitspausen bleibt der eingeschaltete Rechner vielfach ohne Aufsicht.

"Natürlich kann Technologie eine Menge dazu beitragen, die Sicherheit zu erhöhen", sagt Bruce Schneier, US-Experte für Computersicherheit. Aber allein mit Technik seien die Probleme nicht zu lösen. Man sollte deshalb nicht immer nur in ständig neue Schutzprogramme investieren, sondern darüber nachdenken, "wie man Menschen davon abbringen kann, falsche Dinge zu tun, und wie man ihnen helfen kann, das Richtige zu tun".

Kleine Firmen sind Schulungsmuffel

"Viele Sicherheitsvorfälle werden nicht durch organisationsfremde Angreifer, sondern durch unsachgemäßes Verhalten eigener Mitarbeiter hervorgerufen", sagt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Aufklärung tut not, erklären Experten und fordern schon seit längerem regelmäßige, praxisorientierte Mitarbeiterschulungen zu allen relevanten Sicherheitsthemen. Nur in Sicherheitsfragen geschulte Mitarbeiter wüssten, wie sie sich in sicherheitskritischen Situation zu verhalten hätten.

Diese Erkenntnis hat sich noch nicht überall herumgesprochen. Viele Unternehmen scheuen noch immer die regelmäßig anfallenden Schulungs- und Weiterbildungskosten und investieren lieber einmalig in vermeintlich kostengünstigere technische Schutzvorrichtungen. Das gilt besonders für Klein- und Mittelbetriebe. Hier werden die Mitarbeiter in Sicherheitsfragen meist allein gelassen.

Eine Umfrage des Netzwerks Elektronischer Geschäftsverkehr (NEG) hat ergeben: Jeder zweite Klein- und Mittelbetrieb ist ein ausgemachter Schulungsmuffel. "Viele Entscheidungsträger verengen das Thema Sicherheit auf den technischen Aspekt und betrachten es nicht als ganzheitliche Managementaufgabe", sagt Andreas Duscha, Projektleiter der NEG-Studie. Das eigentliche Sicherheitsrisiko sind demzufolge nicht die ungeschulten Mitarbeiter, sondern jene Chefs, die aus Kostengründen an der Mitarbeiterschulung sparen.

Am falschen Ende gespart

Solche Versäumnisse können schwer wiegende Folgen haben. Wird ein IT-Zwischenfall bekannt, leidet das Image eines Unternehmens ganz erheblich. Dies gilt besonders dann, wenn Kundendaten ausspioniert wurden und in falsche Hände geraten sind. Darüber hinaus drohen hohe finanzielle Einbußen. Mit anderen Worten: Wer bei der Mitarbeiterschulung spart, der zahlt am Ende drauf.

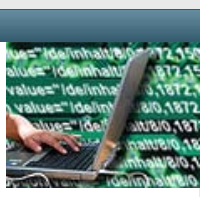
Die heute in Bad Homburg startende zweitägige Kongressmesse Secure 2008 wird sich mit diesen und ähnlichen Sicherheitsfragen beschäftigen. Der hochkarätig besetzte Kongress will einen Überblick geben über Trends, Anwendungen und Strategien zum Schutz der Unternehmens-IT vor Angriffen und Missbrauch.

Die Kunst der Täuschung

Eingeladen ist unter anderem der US-amerikanische Ex-Hacker und jetzige Sicherheitsexperte Kevin Mitnick. Mitnick gelang es in den 1990er Jahren mehrfach, in einige der am besten abgesicherten Computersysteme der Welt einzudringen. Dabei nutzte er konsequent die Methoden des sozialen Hackens und praktizierte die hohe "Kunst der Täuschung". Er erschlich sich trickreich das Vertrauen von Mitarbeitern und gelangte so an Passwörter und Zugangsdaten der geschützten Systeme.

"Es wäre naiv zu glauben, dass man allein durch die Installation einer Firewall vor möglichen Angreifern geschützt ist", sagt Mitnick. "Diese Annahme verleitet dazu, sich in Sicherheit zu wiegen. Aber der vermeintliche Schutz kann sich schlimmer auswirken als gar keine Sicherheitsmaßnahmen", so Mitnick. Denn für die Sicherheit in Unternehmen gelte: "Menschen sind das schwächste Glied."

Mehr zum Thema



- **IT-Sicherheit: Die Grenzen der Aufklärung**
  Fünf Jahre "BSI-für-Bürger"
- **Datenfalle Kopierer**
  Sicherheitslücke wird unterschätzt
- **Schwachstelle Mensch**
  Sicherheitslücken und leichtfertige Anwender bedrohen IT-Sicherheit
- **Von Ahnungslosigkeit bis "Wird-gutgehen"**
  Deutsche Unternehmen vernachlässigen IT-Sicherheit
- **Hackerparagraf: Mit einem Bein im Knast?**
  Sicherheitsexperten fürchten Kriminalisierungswelle

Externe Links
- **Secure 2008**
- **Netzwerk Elektronischer Geschäftsverkehr**
- **BSI: Die Lage der IT-Sicherheit in Deutschland 2007**

Das ZDF ist für den Inhalt externer Webseiten nicht verantwortlich

Drucken Versenden

zum Seitenanfang

Suche in ZDF.de

Das Unternehmen | ZDFwerbung | ZDFshop | Zuschauerservice | Barrierefreiheit | About ZDF | tivi für Kinder

ZDFinfokanal ZDFdokukanal ZDFtheaterkanal arte 3sat PHOENIX KiKA Deutschlandfunk Deutschlandradio Kultur