Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 81 (2003)

Heft: 5

Artikel: Sperrgebiete für Datendiebe

Autor: [s. n.]

DOI: https://doi.org/10.5169/seals-876645

Sicherheitskonzepte

Sperrgebiet für Datendiebe

Computerkriminalität, Sicherheitsverstösse und Systemausfälle verursachen weltweit Schäden in Milliardenhöhe und bedrohen ganze Unternehmen in ihrer Existenz. Mit einem ganzheitlichen Konzept lassen sich die Risiken minimieren.

Vorsicht, Viren! Sircam, Code Red, Nimda, Badtrans und Goner hiessen einige der Übeltäter, die in den letzten Monaten die IT-Welt in Atem hielten. Als neuste Schädlingsvariante infizieren jetzt so genannte Flash-Viren, die sich in bunten Animationsbildchen verstecken, die PCs ahnungsloser Surfer.

Antivirensoftware reicht nicht

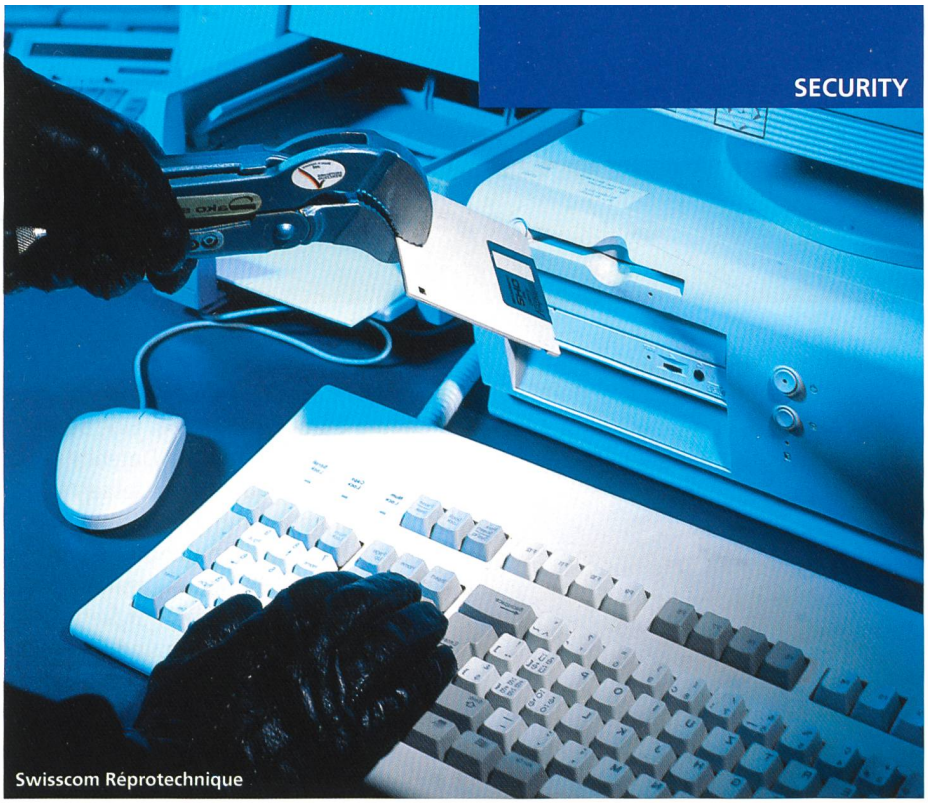
Mehr als die Hälfte der im Rahmen des «2001 Information Security Industry Survey» befragten 2500 IT-Professionals aus Unternehmen und Behörden in aller Welt hatte eine Web-Server-Attacke zu beklagen. Würmer, Trojanische Pferde und andere bösartige Programme infizierten 90% der Organisationen, obwohl 88% bereits Antivirensoftware installiert hatten. Doch damit allein sei es noch nicht getan, warnt die Professorin Dr. Dorothy Denning, Direktorin des Georgetown Institute for Information Assurance (GIIA) in Washington D.C.: «Wie effizient technologische Hilfsmittel sind, hängt immer von der Qualität der Produkte ab und auch davon, ob sie fachgerecht installiert und eingesetzt werden.»
Durch die Vernetzung von Mitarbeitern, die an verteilten Standorten, zu Hause oder von unterwegs aus arbeiten, sind Unternehmen gegenüber Angriffen aus dem Cyberspace verwundbarer geworden. Die weltweiten Verluste durch Computerkriminalität schätzen die Londoner Marktforscher von Datamonitor plc auf 15 Mia. US-$ pro Jahr. Gleichzeitig steckt aber jedes zweite Unternehmen weniger als 5% des IT-Budgets in die Sicherheit seiner Netze. Dabei entstehen im Ernstfall schnell Schäden in Millionenhöhe, abgesehen vom nicht wieder gut zu machenden Vertrauensverlust bei Geschäftspartnern und Kunden.
Es sind keineswegs nur Eindringlinge und Spione, die Firmennetzen zu schaffen machen. Viele Sabotageakte werden von den eigenen Mitarbeitern verübt – oft unwissentlich, manchmal auch vorsätzlich. Laut einer Studie der New Yorker Unternehmensberatung Pricewaterhouse Coopers LLP werden 58% der Sicherheitsverletzungen durch autorisierte, 24% durch nicht autorisierte Mitarbeiter sowie weitere 13% durch Ex-Angestellte begangen. Hacker oder Wettbewerber spielen dagegen nur eine untergeordnete Rolle.
Es ist also höchste Zeit, dass Verantwortliche die Risiken und Gefahren wirklich ernst nehmen. Eine Umfrage der Computer Sciences Corporation (CSC) unter 1000 IT-Managern internationaler Unternehmen belegt immerhin, dass ein Umdenken eingesetzt hat: Sicherheit ist im letzten Jahr auf Platz zwei der Prioritätenliste vorgerückt. Dennoch zeigen sich die wenigsten Betriebe ausreichend gewappnet: «Fast die Hälfte der Technikvorstände hat noch gar kein Sicherheitskonzept umgesetzt», bemängelt Joseph Stafford, Vice President CSC Global Information Security Services in Annapolis Junction (US-Staat Maryland).

Wettrüsten

Eine durchdachte Abwehrstrategie beginnt bei der Analyse, welchen Gefahren das Unternehmen überhaupt ausgesetzt ist. «Sicherheit ist kein Produkt, sie ist ein Prozess», betont Bruce Schneier, Technikchef und Mitgründer von Counterpane Internet Security Inc. im kalifornischen Cupertino. Was heute als bedenkenlos gelte, könne morgen schon ein Risiko darstellen. «Letztlich ist das ein Wettrüsten, bei dem die Angreifer alle Vorteile auf ihrer Seite haben», entgegnet Schneier allzu blauäugigen Firmenchefs, die meinen, es sei mit der Installation einer Firewall getan.

Drei Säulen der IT-Sicherheit

Bei Siemens hat man die Notwendigkeit eines umfassenden Ansatzes schon lange erkannt. Mit Hilfe strategischer Partner bietet der Konzern weltweit Analyse, Beratung und Umsetzung aus einer Hand. «IT-Sicherheit beginnt beim Rauchmelder und hört bei der Biometrie auf», beschreibt Christian Ernst, Director Security bei Siemens Business Services in Nürnberg, die Bandbreite der Thematik. Als wichtigste Kriterien nennt er:


Swisscom Réprotechnique

Viele Sabotageakte werden von den eigenen Mitarbeitern verübt; oft unwissentlich, manchmal auch vorsätzlich.

- Vertraulichkeit: Schutz vor unbefugtem Zugriff
- Integrität: Schutz vor unbemerkter Verfälschung
- Verfügbarkeit: Zugriff innerhalb eines definierten Zeitraums von Daten

Christian Ernst warnt explizit davor, nach dem Schrecken des 11. Septembers 2001 in Aktionismus zu verfallen und punktuelle Sicherheitslösungen einzusetzen. «Mit Einzelmassnahmen ist es nicht getan», betont der Experte. «Unternehmen brauchen ein ganzheitliches Konzept.» Siemens nimmt die Informationssicherheit deshalb nicht nur unter technischen, sondern auch unter organisatorischen Aspekten unter die Lupe. Dabei komme es auf jedes Detail an, denn eine IT-Infrastruktur sei nur so sicher wie ihr schwächstes Glied, betont Roberto Pillmaier: «Eine umfassende Schwachstellenanalyse ist die Grundvoraussetzung zur Bestimmung der Ist-Situation, um die optimal anzuwendenden Sicherheitsstandards bis hin zum Risikomanagement zu entwickeln», so der Principal Consultant bei Siemens Trusted Networks & Applications in München.

Nach einem solchen Stufenplan ging auch die Versicherungsgesellschaft «Hannover'sche Leben» vor. Mit einem Beitragsvolumen von 950 Mio. Euro (2000) ist der älteste deutsche Direktversicherer, 1875 gegründet als Preussischer Beamten-Verein, in seinem Segment klarer Marktführer. Zurzeit sorgen rund 430 Mitarbeiter in der Hauptverwaltung und den dezentralen Servicecentern für eine qualifizierte Beratung der Kunden. Damit der IT-Betrieb auch künftig reibungslos läuft, hat die Hannover'sche Lebensversicherung ihren Partner Siemens mit einer Sicherheits- und Schwachstellenanalyse beauftragt. Als Ergebnis präsentierte der Dienstleister einen Katalog, der Massnahmen zur Vermeidung von Schäden aufzeigt, die einen Teil- oder Totalausfall des Systems verursachen können.

Bauliche Vorkehrungen

Als Erstes wurde ein Back-up-Konzept entwickelt. Bislang begnügte sich die «Hannover'sche Leben» mit redundanten Systemen, die allesamt denselben Risiken ausgesetzt waren. Durch ein zweites, räumlich getrenntes Rechenzentrum lässt sich nun ausschliessen, dass ein Brand das gesamte Firmennetz lahm legen könnte. Vor der Inbetriebnahme wurden zahlreiche Schutzvorkehrungen getroffen, etwa der Einbau von Brandwänden, Rauchmeldern, Löschvorrichtungen, Zugangssperren, Alarmanlagen oder Notstromaggregaten. Auch vor Hitze, Staub, Blitzschlag, Hochwasser oder Elektrosmog müssen die Systeme abgeschirmt werden.

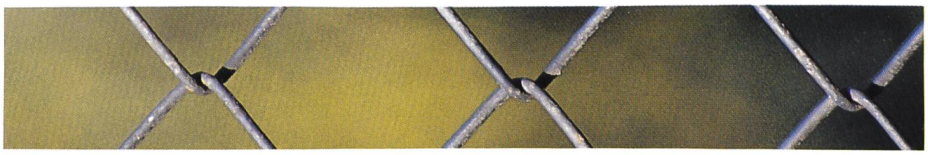
Notfallpläne

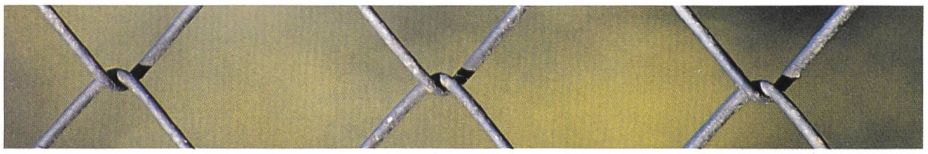
«Solche Umfeldrisiken sind häufig unterschätzte Gefahrenquellen», sagt Robert Schumann, Experte für physische Sicherheit und Notfallplanung bei Siemens Business Services in München, «denn was nützt ein ausgeklügeltes Sicherheitskonzept samt der neusten Technik, wenn ein Rechenzentrum in der Nachbarschaft einer Chemiefabrik steht, von der Gefahren ausgehen können?» Mit der Gewissheit, mögliche Störfaktoren ausgeschaltet zu haben, geben sich die Niedersachsen aber nicht zufrieden: Im zweiten Schritt führt die «Hannover'sche Leben» jetzt einen Notfallplan ein, der genau vorschreibt, wie in Problemsituationen zu verfahren ist, beispielsweise durch Umgehung des ausgefallenen Systems. Natürlich muss Sicherheit bezahlbar sein. Restrisiken sind nie auszuschliessen, doch sollten sie keine unabsehbare Katastrophe verursachen können. «Auf diese Art war es uns möglich, ein auf die Gefährdung abgestimmtes und zugleich wirtschaftliches Gesamtkonzept zur Sicherung unseres Rechenzentrumbetriebs umzusetzen», erklärt Uwe Oltrogge, Leiter Datenverarbeitung bei der «Hannover'schen Leben».

Zu den kostengünstigsten Sicherheitstechnologien für Unternehmen gehören virtuelle private Netze (VPN). Eine bislang einmalige Form hat Siemens bei der MediaLine Interactive Solutions AG in Chur realisiert, einem Spezialisten für CRM-Services (Customer Relationship Management). Sein Angebot reicht von der Pflege bestehender Kunden mit dem Ziel «Cross Selling» über die Beantwortung von Anfragen per Telefon, Fax, Brief, E-Mail oder Chat bis hin zur Online-Beratung während des Kaufvorgangs. «Wir machen nicht einfach Telefonanrufe, sondern wir generieren Umsatz», formuliert Vorstandschef Giacomo Rusconi seine Erfolgsstrategie.

Sicherer Fernzugriff

Vor diesem Hintergrund benötigen sowohl eigene Mitarbeiter als auch die Kunden den sicheren Fernzugriff auf die Datenbank von MediaLine. Gewährt wird





Datenintegrität

Kernfragen einer Schwachstellenanalyse

Schutzbedarf:
Welche Hard- und Software gibt es im Unternehmen? Für welche Anwendungen muss Hochverfügbarkeit garantiert sein? Sind wichtige Komponenten redundant vorhanden?

Zugangsschutz:
Gibt es bei allen Räumlichkeiten und Systemen eine wirksame Barriere gegen unerlaubtes Betreten beziehungsweise unautorisierten Zugriff (Türschlösser, PIN-Code, Passwort, Smartcard, biometrische Verfahren)?

Betriebssicherheit:
Sind die Räumlichkeiten und Systeme vor äusseren Einflüssen wie Hitze, Wassereinbruch, Blitzschlag oder Elektrosmog geschützt? Existiert eine Notstromversorgung?

Back-up und Recovery:
Werden regelmässig Sicherungskopien auf externen Medien angefertigt und an einem geeigneten Ort verwahrt? Gibt es Vorkehrungen, die eine Wiederherstellung verlorener Daten gestatten?

Sicherheitspolitik:
Existieren klar definierte Verantwortlichkeiten und Benutzerrichtlinien? Werden Schutzvorkehrungen gepflegt und kontrolliert? Ist festgelegt, welche Erstmassnahmen im Notfall zu ergreifen sind und wer benachrichtigt werden muss?

Kundendienst:
Mit welchem Netzbetreiber, Service Provider oder IT-Dienstleister arbeitet das Unternehmen zusammen? Können die Partner die erforderlichen Reaktionszeiten durch Service Level Agreements garantieren?

Qualifikation:
Welche Mitarbeiter gehen mit vertraulichen Daten um? Sind die Betreffenden ausreichend für die Problematik sensibilisiert? Wird das Personal regelmässig geschult?

er ihnen über ein Business Gateway von F-Secure Corp. aus Helsinki. Eine starke Verschlüsselung garantiert Datenintegrität, sämtliche Funktionen lassen sich zentral administrieren. Der Clou: Alle Verbindungen werden über die bestehende Firewall geleitet; das galt bis dato als undurchführbar. Dabei hat Siemens das Projekt samt Beratung und Feinkonzept in nur zehn Manntagen umgesetzt. «Seit nunmehr einem Jahr läuft die Lösung ohne jegliche Probleme», berichtet Klaus Schlösser, Solution Manager bei Siemens Trusted Networks & Applications in München.

Integrierte Komponenten

Neben VPNs haben sich auch Smartcards zu einem multifunktionalen Sicherheitsinstrument entwickelt. Laut einer Analyse der US-Marktforscher von Frost & Sullivan Inc. soll die Zahl der weltweit genutzten Minicomputer im Chequekartenformat im Jahr 2004 bei 3,66 Mia. liegen. Das sind doppelt so viele wie im Jahr 2000. Auf diesem Gebiet besitzt Siemens eine langjährige Erfahrung und übernimmt jede gewünschte Dienstleistung von der Chiplieferung bis zum Personalisierungssystem. «Wesentlich ist ein umfassendes Konzept, das alle nötigen Komponenten integriert», unterstreicht Michael Stiegert, Solution Manager bei Trusted Networks & Applications in München.
Als Pionier für den Einsatz von Smartcards in einer PKI-Umgebung (vgl. Kasten) gilt die Universität Mannheim. Im November 2000 hat sie als erste deutsche Hochschule einen chipkartenbasierten Studentenausweis eingeführt, der durch eine PIN vor Missbrauch geschützt ist und mit seinem Kryptoprozessor eine Reihe von Anwendungen unterstützt. Über 10 500 Studenten und 11 000 externe Nutzer der Bibliothek, des Rechenzentrums und anderer universitärer Einrichtungen gebrauchen ihn nicht nur bei der Zutrittskontrolle zu Gebäuden und Räumen. «Mit der Verschlüsselungsmöglichkeit können die Studenten die Chipkarte auch dazu verwenden, ihr Semesterticket auszudrucken, bargeldlos in der Mensa zu bezahlen und vertrauliche

Schutzmechanismen

Sicherheitslösungen und ihre Funktionsweise

Firewall:
Schnittstelle zwischen privatem und öffentlichem Netz. Filtert den Datenstrom und prüft, welche Rechnersysteme und Benutzer miteinander kommunizieren dürfen.

Virenscanner:
Durchsucht alle Datenträger auf Muster bekannter Viren. Erkennt das Programm eine Übereinstimmung, schlägt es Alarm und versucht, die befallene Datei zu säubern oder wieder herzustellen.

Intrusion-Detection-System:
Überwacht das Firmennetz, erkennt Angriffe und Regelverletzungen, protokolliert kritische Ereignisse und leitet umgehend Gegenmassnahmen ein.

Virtuelles privates Netz:
Kommunikationsdienst, der in einem öffentlichen Netz ein kundenspezifisches Teilnetz bildet. Darüber lassen sich standortunabhängig verschlüsselte Verbindungen aufbauen, die wie interne Verbindungen behandelt werden und deren Bandbreite sich dynamisch konfigurieren lässt.

Smartcard:
Multifunktionale Chipkarte mit eigenem Betriebssystem, deren Mikroprozessor einfache Programme ausführen kann. Lässt sich als Träger des privaten Schlüssels und damit sowohl als Authentifizierungsmedium als auch zur Datenverschlüsselung einsetzen.

Public-Key-Infrastruktur:
Umgebung zur sicheren Abwicklung von Online-Transaktionen. Verwendet einen privaten Schlüssel (wird entweder auf der Smartcard gespeichert oder von ihr selbst erzeugt) und einen öffentlichen Schlüssel, der dem jeweiligen Geschäftspartner vorliegen muss. Ein Anwendungsbeispiel ist die digitale Signatur, bei der ein Absender sich mit seinem privaten Schlüssel authentifiziert und der Empfänger dies mit einem öffentlichen Schlüssel verifiziert.

Biometrischer Scanner:
Überprüft anhand körperlicher Merkmale wie Fingerabdruck oder Irismuster die Identität des Benutzers.

Mails zu verschicken», sagt Franz-Josef Jochem, Projektleiter an der Universität Mannheim.

Iris-Scan

Dennoch bringen Smartcards auch einen Nachteil mit sich – sie können verloren oder gestohlen werden. Darum setzt die australische Regierung in Canberra seit Oktober 2001 auf einen biometrischen Zugangsschutz für ihre Gebäude, den Siemens unter anderem gemeinsam mit Iris Australia Pty Ltd. aus Sydney entwickelt hat. Die Iriserkennung gilt als derzeit sicherstes Verfahren der Nutzerauthentifizierung auf Grund von Körpermerkmalen – sie bietet etwa sechs- bis achtmal so viele Variablen wie ein Fingerabdruck. Dabei wird das menschliche Auge mit einer speziellen Videotechnik aus einer Entfernung von maximal einem Meter aufgenommen. «Die Iriserkennung vereinfacht nicht nur das Sicherheitsmanagement», betont Greg McAnulty, Regional Director E-Business Services bei Siemens, «sie erhöht auch das Vertrauen der Anwender.» Damit ist dieses biometrische Verfahren unter anderem für den Einsatz bei Geldautomaten prädestiniert.

Abhörsichere Handys

Sicherheit und Vertrauen spielen auch im Mobilfunk eine immer bedeutendere Rolle: Vor rund zwei Jahren entwickelten Siemens-Forscher ein Verfahren, das auf Knopfdruck eine geschützte Verbindung mit End-to-End-Verschlüsselung herstellt. Das Krypto-Handy «TopSec GSM» ist seit Mai 2001 auf dem Markt. Äusserlich und in der Funktionalität gleicht das «TopSec GSM» dem Businesshandy «S35i». Zum Aufbau einer mit 128 Bit verschlüsselten Verbindung über einen GSM-Datenkanal drückt der Benutzer einfach einen Softkey. Ein briefmarkengrosses Modul kodiert und verwürfelt die Informationen daraufhin so gründlich, dass selbst Geheimdienste nicht mithören können. Allerdings muss dazu auch der Gesprächspartner über ein passendes Handy oder ISDN-Telefon verfügen. Bislang hat Rohde & Schwarz, der Messtechnikspezialist aus München, etwa 1000 Krypto-Handys verkauft. Zielgruppe sind Manager von Topunternehmen sowie hochrangige Behörden- und Regierungsangestellte. 4

Quelle: IC-World, Siemens

I and C Kompakt

Obwohl das Risiko, Opfer einer Netzattacke zu werden, dramatisch gestiegen ist, verwenden Unternehmen nach wie vor nur einen Bruchteil ihres IT-Budgets für Sicherheitsmassnahmen.
Das Schutzschild für sensible Daten:
- Die drei Säulen der IT-Sicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit von Daten.
- Eine durchdachte Abwehrstrategie beginnt mit einer Gefahren- und Schwachstellenanalyse und leitet daraus die technisch möglichen und wirtschaftlich vertretbaren Massnahmen ab. Nur ein ganzheitliches Konzept sichert die gewünschten Standards.
- IT-Sicherheit ist ein Wettrüsten. Wegen der Dynamik der technischen Entwicklung müssen Verantwortliche ihr gegenwärtiges Konzept regelmässig überprüfen und überdenken.
- Zu den Standardlösungen zählen heute Firewalls, Virenscanner, Intrusion-Detection-Systeme, virtuelle private Netze oder chipkartenbasierte Authentifizierungs- und Verschlüsselungsmechanismen. Hinzu kommen als relativ neue Entwicklungen biometrische Erkennungsverfahren und Krypto-Handys für vertrauliche Mobilfunkkommunikation.
- Einzelne Sicherheitsprodukte und Schutzmechanismen dürfen keine Insellösung sein, sondern müssen ineinander greifen.

Summary

No-go Area for Data Thieves

Computer crime, security breaches and system failures cause billions of dollars worth of damage worldwide and threaten the existence of entire companies. Companies have become more vulnerable to attacks from cyberspace due to the networking of employees working at distributed sites, at home or while travelling. The market researchers at London-based Datamonitor plc estimate global losses as a result of computer crime to be 15 billion US dollars per year. Yet at the same time, one in two companies invests less than 5% of its IT budget in the security of its networks. And when the worst comes to the worst, millions of dollars worth of damage soon arise. According to a study carried out by New York business consultants Pricewaterhouse Coopers LLP, 58% of security breaches are carried out by authorised staff, 24% by unauthorised staff and a further 13% by former employees. By contrast, hackers and competitors play only a minor role. Siemens recognised the necessity of a comprehensive approach a long time ago. With the assistance of strategic partners, the company offers one-stop analysis, consultation and implementation on a global basis. The most important criteria are defined as confidentiality (protection against unauthorised access), integrity (protection against concealed fraud) and availability (access within a specified time period). It is important above all to keep these three criteria in mind when creating a no-go area for data thieves. The risks can only be minimised by means of a holistic concept.