

## INHALT

### Aus dem Kompetenz-Center.

Die Landesinitiative »secure-it.nrw« offeriert Firmen, Bürgern und Behörden jetzt neue Informationsangebote zum Thema IT-Sicherheit: **Seite 2**

### Risikofaktor Festplatte.

Beim Ausmustern alter Rechner befinden sich auf der Festplatte oftmals noch vertrauliche Informationen. Wie Firmen richtig vorgehen: **Seite 3**

### So wird IT-Sicherheit erfolgreich.

„Vorbild sein, Mitarbeiter motivieren, Freiräume schaffen“, empfiehlt Top-Berater Willy Schmider Firmenchefs: **Seite 4**

### Frauen kaufen gern im Web.

Wie Online-Händler die kaufkräftige Zielgruppe zu Kunden machen: **Seite 4**

## AKTUELLES STICHWORT

### +++ Pharming +++

Mit dem so genannten Pharming verschaffen sich Kriminelle vermehrt Zugriff auf onlinegeführte Firmenkonten. Der Trick: Auch wer bei Überweisungen die korrekte Web-Adresse seiner Bank eintippt, landet auf einer getürkten Webseite. Dort erfassen die Cybergauner Passwort, PIN oder TAN.

Angriffsziel sind immer die so genannten Domain Name Server (DNS). Sie sorgen für die richtige Adressierung von Internetsites. Ein eingeschleustes Schadprogramm (Trojaner) verändert unbemerkt die mit der eingegebenen bank.de-Adresse verbundene IP-Kennziffer.

### So schützen sich Firmen:

1. Firewall so konfigurieren, dass sie keine unbekanntes Adressen ungeprüft durchlässt.
2. Wenn Firewall-Anbieter auf Sicherheitslücken hinweisen, sofort Patches aufspielen.
3. Virens Scanner aktuell halten – so gelangen keine schädlichen Codes auf die Festplatte.

**Achtung: Bei unberechtigten Abbuchungen kann die Schwachstelle auch beim Service-Provider oder bei der Bank sein.**

## Sicherheitstraining für Surfer

**Kluge Firmen schulen ihre Mitarbeiter für den sicheren Umgang mit Internet und E-Mail – und profitieren selber kräftig davon.**

„Internet und E-Mail sind für unser Unternehmen die wichtigsten Kommunikationswerkzeuge“, stellt Thomas Knorr fest, „sei es beim Kontakt mit Kunden, für die Informationsrecherche oder um weltweit gute Geschäfte zu machen.“ IT-Sicherheit ist für den kaufmännischen Leiter der Bühler Technologies GmbH nicht nur eine Frage der Technik: Ein externer Trainer hat die Bühler-Belegschaft in einer eintägigen Schulung fit für die elektronische Welt gemacht.



### Technik ist nicht alles

Bühler stellt in Ratingen seit mehr als 30 Jahren Komponenten und Systeme für die Fluidtechnik und die Prozessgasanalyse her. Kunden sind weltweit unter anderem chemische Werke, Kraftwerke und die Lebensmittelindustrie. Für den wirksamen IT-Schutz nach außen sorgt Wolfgang Mattern, bei Bühler verantwortlich für den EDV-Bereich, mit Firewall, Spam-Filter und einem Virenschutzprogramm. Aber auch er weiß: „Technik allein kann nicht alle Gefahren bannen – noch wichtiger sind die Wachsamkeit aller Mitarbeiter und richtiges Handeln in kritischen Situationen.“

### Den Blick schärfen

Um das zu fördern, hat die Bühler GmbH ein internes Awareness-Training durchgeführt. Ziel: anhand von praktischen Beispielen aus dem Berufsalltag zu einem bewussten Handeln beim Surfen und Mailen anzuleiten. Mehr als 40 Angestellte aus Verwaltung, Vertrieb und Fertigung nahmen daran teil. „Es geht in der Hauptsache darum, was ein Mitarbeiter darf und was nicht“, berich-

tet Sicherheitstrainer Edgar Scholl. Aus seiner Erfahrung weiß er: „Quer durch alle Branchen und Hierarchien besteht immer noch ein großer Aufklärungsbedarf.“ Deshalb geht er in seinen Kursen gezielt auf die Bedeutung von Sicherheitsmaßnahmen ein und schärft dabei auch den Blick für juristische Fallen: „Wer beispielsweise eine Mailing-Liste versendet und alle Adressaten in das ‚An‘-Feld setzt, kommt schnell mit dem Gesetz in Konflikt.“

Für Bühler hat sich das Training gelohnt. „Die Kosten von etwa 2.000 Euro sind gut investiert“, resümiert Thomas Knorr, „bei uns ist sogar die Zahl der Probleme im Umgang mit Spam- und Phishing-Mails deutlich zurückgegangen.“

„Wir fördern ausdrücklich die Neugier unserer Mitarbeiter.“ Thomas Knorr (rechts, mit IT-Verantwortlichem Wolfgang Mattern) hat nichts dagegen, wenn die Bühler-Beschäftigten das Internet intensiv nutzen, um neue Ideen zu entwickeln.

## TIPPS FÜR DEN WORKSHOP

- Sicherheitstrainer Edgar Scholl rät, auf diese Punkte zu achten:**
- Maximal zehn Teilnehmer pro Schulung
  - Vorab den Workshop auf die im Unternehmen benutzten Programme abstimmen
  - Workshop in externen Räumlichkeiten oder samstags abhalten – schafft Abstand vom Alltag

## Neues aus dem Kompetenz-Center

Bei der IT-Sicherheit müssen Firmen, Bürger und Behörden stets auf dem aktuellen Stand sein. Die Initiative »secure-it.nrw« bietet eine Vielzahl neuer Informationsmöglichkeiten.

### Basiswissen: „Online – aber sicher!“

Wie Mitarbeiter ihren PC mit einfachen Mitteln und Vorsichtsmaßnahmen vor den potenziellen Gefahren im weltweiten Netz schützen, zeigt »secure-it.nrw« mit den Veranstaltungen „Online – aber sicher!“. Sie finden in Zusammenarbeit mit regionalen Partnern wie Banken, Sparkassen oder der Polizei an folgenden Terminen statt: 27. April in Siegen, 11. Mai in Paderborn und 16. Mai in Siegburg. Die Teilnahme ist kostenfrei. Anmeldung: [info@secure-it.nrw.de](mailto:info@secure-it.nrw.de)

### Kompaktwissen: Sichere Geldgeschäfte

Online-Banking kann Firmen dabei helfen, ihre Geschäftsprozesse zu rationalisieren und nachhaltig Kosten zu sparen. Die neue Broschüre „Geldgeschäfte – online und sicher“ der Initiative »secure-it.nrw« zeigt anhand

von Praxisbeispielen Einsatzmöglichkeiten für den elektronischen Bankverkehr auf und gibt Tipps zum sicheren Umgang. Jetzt vorbestellen: [info@secure-it.nrw.de](mailto:info@secure-it.nrw.de)

### Service: Infodienst per E-Mail

Ab der nächsten Ausgabe versendet die Landesinitiative »secure-it.nrw« den Infodienst auch per E-Mail. Vorteile für Firmenchefs: 1. Die digitale Ausgabe ist einige Tage eher im Unternehmen als die gedruckte Fassung. 2. Sie landet direkt in Ihrem PC. 3. Gute Tipps lassen sich firmenintern leicht an Mitarbeiter weiterleiten. Wenn Sie den Infodienst künftig als PDF beziehen wollen, melden Sie sich bitte an:

[info@secure-it.nrw.de](mailto:info@secure-it.nrw.de)



## IT-Sicherheitspreis NRW 2006: Jetzt bewerben

Gesucht wird innovative und alltagstaugliche IT-Sicherheit. Bewerben können sich mittelständische Firmen, nordrhein-westfälische Schulen und IT-Anbieter aus ganz Deutschland.

Die Landesinitiative »secure-it.nrw« startet in diesem Jahr erneut einen Wettbewerb um innovative Produkte, Lösungen und Anwendungen für mehr IT-Sicherheit. Zielgruppe: mittelständische Firmen und IT-Anbieter. Außerdem vergibt die Initiative einen Preis an Schulen für kreative Projekte zu IT-Sicherheit und Datenschutz.

### Checken Sie hier Ihre Chancen ... ... als Anwender

- Wir schützen unsere Geschäftsdaten erfolgreich vor Manipulation und Verlust.
- Wir haben durch den Einsatz sicherer Informationstechnologie wirtschaftliche Vorteile.
- Unsere Lösung lässt sich auch in anderen Unternehmen umsetzen.

### ... als Anbieter

- Wir bieten innovative, mittelstandsgerechte IT-Sicherheitsprodukte oder Sicherheitslösungen an.
- Wir haben mittelständische Kunden, die unsere IT-Sicherheitsleistung erfolgreich nutzen.



Jetzt die Bewerbungsunterlagen im Internet abrufen:  
[www.secure-it.nrw.de](http://www.secure-it.nrw.de)

„Es ist ein hervorragendes Ziel von secure-it.nrw, IT-Sicherheitstechnologien in die Anwendung zu bringen.“

Professor Helmut Reimer, Geschäftsführer TeleTrust Deutschland e.V.

Die Gewinner erhalten eine Auszeichnung des Innovationsministeriums NRW und der Initiative »secure-it.nrw«, wertvolle Sachpreise und werden in einer Best Practice-Broschüre veröffentlicht. Bewerbungsschluss für Schulen ist der 26. Juni 2006, für Unternehmen der 30. Juni 2006. Die Preisverleihung findet auf dem „5. IT-Sicherheitstag NRW“ im November 2006 statt.

## TIPPS

**Money-Maker im Web.** Ein neues Bezahlverfahren namens „Giropay“ bringt Online-Händlern mehr Umsatz, schützt vor Zahlungsausfall und gibt Käufern mehr Sicherheit. Der Kunde überweist den Betrag nämlich wie beim Online-Banking über die Website seiner Bank.

[www.giropay.de](http://www.giropay.de)

**Passwort auf Abruf.** Firmen können sich jetzt davor schützen, dass Unbefugte an wichtige Passwörter kommen. Ein vom Fraunhofer-Institut SIT entwickeltes Computerprogramm generiert für jede geschützte Anwendung eine sichere Zugangskennung. Die Installation des „Passwordsitters“ in Firmen-Datenbanken bietet auch Geschäftschancen für IT-Dienstleister. [www.passwordsitter.de](http://www.passwordsitter.de)

**Update für den IT-Grundschutz.** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sein IT-Grundschutzhandbuch umstrukturiert und um neue Bausteine erweitert. [www.bsi.de/gshb/deutsch/etc/change2005.htm](http://www.bsi.de/gshb/deutsch/etc/change2005.htm)

## TERMINE

**24. bis 28.04.**  
**Secure Automation in Hannover.** Ausstellungsbereich zum Thema Sicherheit in der Industriekommunikation auf der Hannover Messe. [www.hannovermesse.de](http://www.hannovermesse.de)

**26. und 27.04.**  
**OWL-Security in Detmold.** IT-Sicherheits-Congress-Messe mit Themen wie IT-Recht, Risikoversorgung oder Vertragsgestaltung. [www.owl-security.de](http://www.owl-security.de)

**27.04.**  
**Online – aber sicher! in Siegen.** Kostenfreie Informationsveranstaltung der Initiative »secure-it.nrw« zum Thema IT-Sicherheit. Weitere Termine dieser Veranstaltungsreihe: **11.05. Paderborn, 16.05. Siegburg.** [www.secure-it.nrw.de](http://www.secure-it.nrw.de)

**10.05.**  
**IT-Trends Sicherheit in Bochum.** Lassen Sie sich von »secure-it.nrw« zum „IT-Sicherheitspreis NRW 2006“ beraten. [www.it-trends-sicherheit.de](http://www.it-trends-sicherheit.de)

## ■ Datensicherheit: Risikofaktor Festplatte

**Firmen gehen oftmals unbewusst ein hohes Risiko ein: Auf ihren Festplatten verbergen sich zuhauf Geschäftsgeheimnisse. Beim Ausmustern alter PCs oder bei Reparaturarbeiten können diese leicht in falsche Hände geraten.**

Um zu erkunden, wie gründlich Firmen, Institutionen und Privatleute beim Löschen ihrer Daten vorgehen, hatten Softwareexperten unlängst im Internet 100 gebrauchte Festplatten ersteigert. Die Überraschung war groß: Fast alle Datenträger konnten sie problemlos auslesen. Sie fanden darin Berichte über Umsatz- und Marktanteile, Strategiepapiere, Geschäftskorrespondenz mit dem Vermerk „streng vertraulich“ und sogar Patienteninformationen einer Krankenkasse.

### Langlebige Projektgeheimnisse

Schuld daran sind zum einen unvorsichtige Mitarbeiter: Untersuchungen ergaben, dass nach Ablauf eines Projekts zirka 90 Prozent der dabei entstandenen Dateien nie wieder geöffnet werden, aber dennoch auf der Festplatte verbleiben. Ein großes Risikopotenzial steckt zudem

in automatisch ablaufenden Speichervorgängen: Viele Anwendungsprogramme erzeugen so genannte temporäre Dateien, die nach Beendigung des Programms zwar gelöscht werden, aber weiterhin auf der Festplatte präsent sind. So erstellt beispielsweise das Windows-2003-Server-Betriebssystem regelmäßig Schattenkopien und lagert sie in einem speziellen Speicherbereich.

### Verwirrende Funktionen

Wichtig zu wissen: Funktionen wie Löschen, Formatieren oder das Verschieben der Dateien in den Papierkorb zerstören nicht die Dokumente, sondern tilgen nur den Verweis darauf. Die Dateien selbst bleiben so lange lesbar, bis sie vollständig überschrieben sind.

Firmen sollten deshalb vor dem Verkauf ihrer PCs die Festplatte überschreiben.



**Auf fast jeder Festplatte befinden sich zwischen 30 und 70 Prozent Datenmüll. Regelmäßige Reinigung sorgt für mehr Sicherheit.**

## ■ Putzplan für die Festplatte

**In Unternehmen verdoppelt sich jährlich der Datenbestand auf den Festplatten. Ein Fünf-Stufen-Plan schafft rechtzeitig Ordnung.**

**Dokumente verschlüsseln.** Eine Funktion dafür ist in Windows XP enthalten. Dateien lassen sich zwar wieder herstellen, sind aber nicht mehr lesbar.

**Datenträger reinigen.** Lässt sich in Windows XP einfach mit dem Hilfsprogramm „Datenträgerbereinigung“ erledigen. Löscht temporäre Dateien.

**Versteckte Dokumente löschen.** Tools wie TweakNow (kostenlos im Internet) räumen Registerdateien auf, löschen Cookies oder Internet-Verlaufsdateien, räumen den Papierkorb auf. Dateien

mit der Endung .tmp, .bak oder .sik kann man problemlos löschen.

**Festplatte aufräumen.** Regelmäßig die Windows-Funktion „Defragmentieren“ nutzen. Sie setzt vorher auf der Festplatte verteilte Dokumententeile wieder zusammen. Dabei werden auch an diesen Stellen zuvor gelöschte Dateien endgültig unlesbar. Zusatzvorteil: Der Zugriff auf Dateien wird schneller.

**Löschsoftware einsetzen.** Spezielle Programme überschreiben die auf der Festplatte gespeicherten Daten (auch einzelne Dokumente) mehrfach. Sie machen sie damit unleserlich. Üblich ist siebenmaliges Überschreiben, besser aber 35-mal. Software-Firmen wie Acronis, Steganos O&O-Software oder Ashampoo bieten solche Blankputzer an (zirka 30 Euro).

### ANLEITUNG

**Firmenchefs sollten feste Regeln für den Umgang mit alten Datenbeständen aufstellen – und deren Einhaltung kontrollieren.**

1. Klare Vorgaben machen, wie Datenmüll identifiziert und gelöscht wird. Kriterien könnten zum Beispiel sein: Altersstrukturen der Dateien oder Nutzungsintensität.
2. Festlegen, wie Datenmüll technisch entsorgt wird – zum Beispiel Löschen durch Überschreiben.
3. Eindeutig bestimmen, welcher Mitarbeiter für die Entsorgung des Datenmülls verantwortlich ist.
4. Verfahren einführen, die sicherstellen, dass im Rahmen von Projekten gespeicherte Dateien nicht zu Datenfriedhöfen führen – beispielsweise auf externem Datenträger archivieren.
5. Filterverfahren festlegen, die Datenmüll durch Spam-Mails verhindern.

### SERVICEPOINT

**Festplatten-Report:** Was die O&O-Software GmbH auf ersteigerten Festplatten alles gefunden hat. Link unter: [www.secure-it.nrw.de/infodienst.php](http://www.secure-it.nrw.de/infodienst.php)

## So wird IT-Sicherheit erfolgreich

„Die Verantwortung für IT-Sicherheit können Firmenchefs nicht einfach wegdelegieren“, sagt Managementberater Willy Schmider. Eine Handlungsanleitung für Chefs.

**Berater Willy Schmider: „Nur ein ganzheitlicher Ansatz führt zu mehr IT-Sicherheit im Unternehmen.“**

Willy Schmider weiß: „Investitionen in Technik sind nur der Anfang eines wirksamen IT-Sicherheitskonzeptes.“ Der Personal- und Managementberater – Partner der Unternehmensberatung Hetzel & Partner in Bonn – rät Firmenchefs deshalb, auf sieben Punkte zu achten.

- „Der IT-Zuständige des Unternehmens sollte jederzeit Zutrittsmöglichkeit zum Büro des Geschäftsführers haben. Wichtig ist auch, dass ihm der Chef Freiräume für notwendige IT-Sicherheitskonzepte schafft.“
- „Entscheidend ist auch, wie ein Unternehmen Mitarbeiter außerhalb der IT-Abteilung für Gefahren und Risiken im Umgang mit Daten sensibilisiert. Es muss ihnen mehr Eigenverantwortung übertragen.“
- „Wie das Management das Thema IT-Sicherheit anpackt, so wird es auch im Unternehmen gelebt: Chefs müssen deshalb gut informiert und Vorbild sein.“
- „Es kann für ein Unternehmen durchaus sinnvoll sein, die Position des IT-Verantwortlichen nicht mit einem reinen Techniker zu besetzen, sondern mit einem Querdenker.“
- „Die Informationstechnologie ist nur ein Hilfsmittel. Für deren Sicherheit muss das Management einen eigenen Schwerpunkt setzen.“
- „Beim Einsatz neuer IT-Lösungen alle Abteilungen in den Prozess einbeziehen. Das schafft bei Mitarbeitern mehr Akzeptanz.“
- „Rundumsorglos-Pakete sind keine Lösung für mehr IT-Sicherheit. Sie vermitteln den Nutzern eher den Eindruck, sich um nichts mehr kümmern zu müssen.“



### NEWS-TICKER

#### Frauen kaufen gern im Web

Online-Händler sollten sich stärker auf Frauen als Zielgruppe einstellen: Seit 2003 ist die Zahl der Europäerinnen, die im Netz einkaufen, von 17 auf 27,4 Millionen gestiegen. Eine Umfrage des Softwareanbieters Novomind verrät: 52,8 Prozent der Nutzerinnen ordern mit Begeisterung Kleidung und Sportartikel. Aber 42 Prozent der Käuferinnen klagt über technische Probleme während des Bestellvorgangs. Vor allem individuelle Servicefunktionen, die den Einkauf zum virtuellen Erlebnis machen, locken weibliche Kunden an.

#### Polizeistreife an der Kasse

Händler können sich jetzt besser vor Betrug per EC-Karte schützen: Immer mehr Polizeidienststellen melden die Daten aller als gestohlen oder verloren registrierten EC-Karten an eine zentrale Datenbank beim EHI-EuroHandelsinstitut in Köln. Das Institut gibt die Information direkt an die Kassensysteme der angeschlossenen Einzelhändler weiter. Wenn der Kunde mit einer als gesperrt gemeldeten Karte bezahlt, wird der Transaktionsvorgang automatisch abgebrochen. Die Teilnahme am Warnsystem kostet ab 120 Euro pro Jahr. Infos über [kuno@ehi.org](mailto:kuno@ehi.org)

#### Computer müssen zum Sicherheitscheck

Firmen sollten bei mobil oder stationär eingesetzten Kommunikationsgeräten regelmäßig die Sicherheitseinstellungen überprüfen. EDV-Spezialist Landseck hat herausgefunden, dass in 14 Prozent der untersuchten Unternehmen Mitarbeiter sicherheitsrelevante Einstellungen an ihren Computern verändert oder deaktiviert hatten.

#### Lange Leitung beim Internet-Call

Gerade einmal elf Prozent aller Kleinunternehmen telefonieren nach einer Studie der Marktforscher TechConsult übers Internet. Befürchtungen: Virenattacken legen auch die Sprachkommunikation lahm und Gespräche sind leichter abzuhören. Als Vorteile machen Nutzer aus: günstige Tarife, weniger Wartungskosten, schnelles Anrufen aus der Datenbank, Sprachdaten lassen sich direkt auf der Festplatte speichern.

#### Blickschutz für Laptops

Eine neue Monitorabdeckung schützt beim Arbeiten mit dem Laptop vor neugierigen Mitlesern. Winzige Mikrolamellen in der vom Technologiekonzern 3M entwickelten Folie blockieren den Einblick von der Seite. Einfach zu befestigen.

### IMPRESSUM

**secure-it INFODIENST**  
Sicherheit bei elektronischen Geschäftsprozessen  
Ausgabe 2/06

**Herausgeber:**  
Agentur »secure-it.nrw«  
bei der IHK Bonn/Rhein-Sieg  
Bonner Talweg 17  
D-53113 Bonn

Thomas Faber (V.i.S.d.P.)

Telefon: +49 (0) 2 28-22 84-184  
Telefax: +49 (0) 2 28-22 84-221

E-Mail: [info@secure-it.nrw.de](mailto:info@secure-it.nrw.de)  
Internet: [www.secure-it.nrw.de](http://www.secure-it.nrw.de)

**In Zusammenarbeit mit:**  
Fraunhofer-Institut Sichere Informations-  
technologie, Sankt Augustin (FhG),  
Medienpool Köln GmbH, Köln (mpk)  
Redaktionsbüro Alfred Preuß, Köln

**Redaktionsleitung:**  
Alfred Preuß

**Redaktion:**  
Jürgen Seidel (FhG)  
Ulrich Kalhöfer (mpk)  
Melanie Schmidt  
(Agentur »secure-it.nrw«)

**Layout und Grafik:**  
Medienpool Köln GmbH

Der secure-it INFODIENST erscheint vierteljährlich und wird unentgeltlich vertrieben.

Verbreitete Auflage 23.500 Exemplare.

Der nächste secure-it INFODIENST erscheint im 3. Quartal 2006.

gefördert vom:



Ministerium für Innovation,  
Wissenschaft, Forschung  
und Technologie des Landes  
Nordrhein-Westfalen

