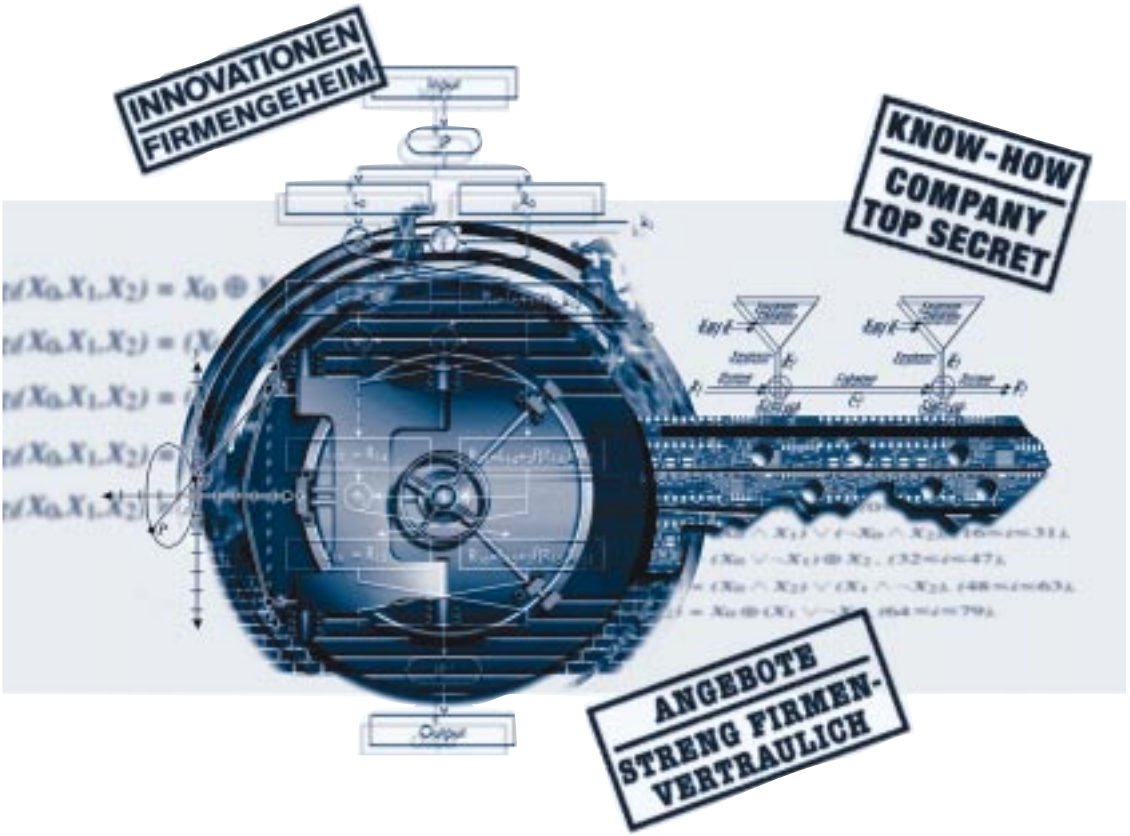


IT-Sicherheit – ein Thema, das uns alle angeht

ROHDE&SCHWARZ

IT-Sicherheit – ein Thema, das uns alle angeht

Fast täglich können wir aus der Presse erfahren, dass es irgendwo jemanden gelungen ist, in ein fremdes Computersystem einzudringen. Manchmal zum Spaß, öfter aber, um einen Geschäftsvorteil zu erlangen oder sogar, um gezielt Unheil anzurichten. Die Grauzone der Computerkriminalität dürfte außerdem erheblich sein – was jedoch nicht Wunder nimmt, wenn man bedenkt, dass heutzutage alle Geschäftsprozesse auf Daten abgebildet und in Rechnern verarbeitet werden. Wer als Unbefugter Zugang zu vertraulichen Daten erlangt oder es gar schafft, sich frei in einem Firmennetzwerk zu bewegen, kann dem Unternehmen beliebig großen Schaden zufügen. Aber auch jenseits der Spionage-Szenarien, die viele von Ihnen für theoretisch und konstruiert halten mögen, birgt eine IT (Informations-Technik)-Umgebung Gefahrenpotenziale, die von ärgerlich bis existenzgefährdend reichen. Sei es, dass eine Festplatte kaputtgeht und mit ihr die ungesicherten Daten darauf, sei es, dass durch sorglosen Umgang mit Dateien aus unbekannter Quelle Viren ins System gelangen und ihre subversive Tätigkeit beginnen. Gerade bei diesem Beispiel wird deutlich, dass IT-Sicherheit nicht nur eine Frage der Technik ist, sondern auch der Menschen, die sich ihrer mehr oder weniger bewusst bedienen.


WIRTSCHAFTSKRIMINALITÄT

Angriff aus dem All

Ungeniert schnüffeln vor allem die Amerikaner die deutsche Wirtschaft aus: Mit großem Aufwand und High-Tech durchforsten sie Telefonleitungen und Computernetze.

Lauschangriff auf Raten

Staatliche Kontrolle im Kampf gegen Kriminalität durch Industrie-Spionen

SPIONAGE

Die Wanze hat laufen gelernt

Der technische Fortschritt beunruhigt die Regierung: Sie prüft ein Handy-Verbot im Kabinettssaal, da die Telefone zum Lauschangriff mißbraucht werden können.

Weniger Einzellösungen, mehr integrierte Systeme sind gefragt

Das Vertrauen verschlüsselt sich

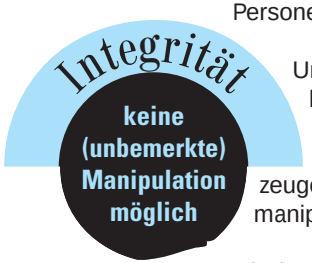
Microsoft hat Probleme, die uncodierte Software nicht hat

Diese kleine Broschüre soll Sie auf die wichtigsten sicherheitsrelevanten Aspekte aufmerksam machen. Denn Sicherheit kommt nicht von selbst – wir alle sind aufgefordert, täglich unseren Beitrag dafür zu leisten.

Die IT-Grundbedrohungen

Um eine gezielte Sicherheitspolitik für das Unternehmen formulieren zu können, werden zunächst die Informationen ausgewählt, die für das Unternehmen von Bedeutung und damit schutzwürdig sind. Die Maßnahmen, die dann für den Schutz dieser Informationen zu treffen sind, sollen drei Dinge sicherstellen: die Vertraulichkeit, die Integrität und die Verfügbarkeit der Daten. Die Verletzung einer dieser Sicherheitskategorien wird als Grundbedrohung für die IT-Sicherheit bezeichnet. Was versteht man nun unter diesen Begriffen?

Der Begriff der **Vertraulichkeit** ist unmittelbar verständlich. Bei Informationen, die als „firmenvertraulich“ oder gar „streng firmenvertraulich“ klassifiziert sind, ist dafür zu sorgen, dass eine Einsichtnahme nur festgelegten Personengruppen möglich ist. Zur Sicherstellung des Schutzes sind verschieden strenge Maßnahmen denkbar, vom Passwortschutz bis zum räumlich isolierten Archiv mit Personenzugang über Chipkarte.



Unter dem Begriff der **Integrität** sammeln sich Attribute wie unversehrt, vollständig, vertrauenswürdig. Bei „integren“ Daten kann man darauf bauen, dass sie genau in dem Zustand vorliegen, in dem ihr Erzeuger sie abgelegt hat, d. h. sie wurden weder unbefugt manipuliert noch durch technische Mängel verfälscht.

Mit der Gewährleistung der **Verfügbarkeit** wird zum einen erreicht, dass Daten nicht verloren gehen, etwa durch fehlende Datensicherung. Zum andern muß garantiert sein, dass der Anwender (und auch Daten verarbeitende Maschinen, z. B. in der Fertigung) in vernünftiger Zeit und störungsfrei an die Daten herankommt, um effizient arbeiten zu können.

Wie Daten bezüglich der drei Sicherheitsziele im Einzelnen klassifiziert werden, zeigt die Doppelseite 8/9.

Unsere Sicherheitsziele

Um den Bedrohungen der IT-Sicherheit zu begegnen, wurden für die Rohde & Schwarz-Firmengruppe drei Sicherheitsziele defininiert. Das erste Ziel ist das Hauptziel, aus dem sich die Unterziele und Schutzmaßnahmen ableiten. Es nennt die Grundbedrohungen und verpflichtet alle Mitarbeiter zur Teilnahme an ihrer Abwehr:

1. **Das Unternehmen Rohde & Schwarz schützt die Unternehmensdaten in Bezug auf Bedrohungen der Vertraulichkeit, Integrität und Verfügbarkeit.**

Ziel Nummer zwei ist zugleich eine wesentliche Voraussetzung zur Erreichung des Hauptziels. Es reglementiert den Zugang zu vertraulichen Daten:

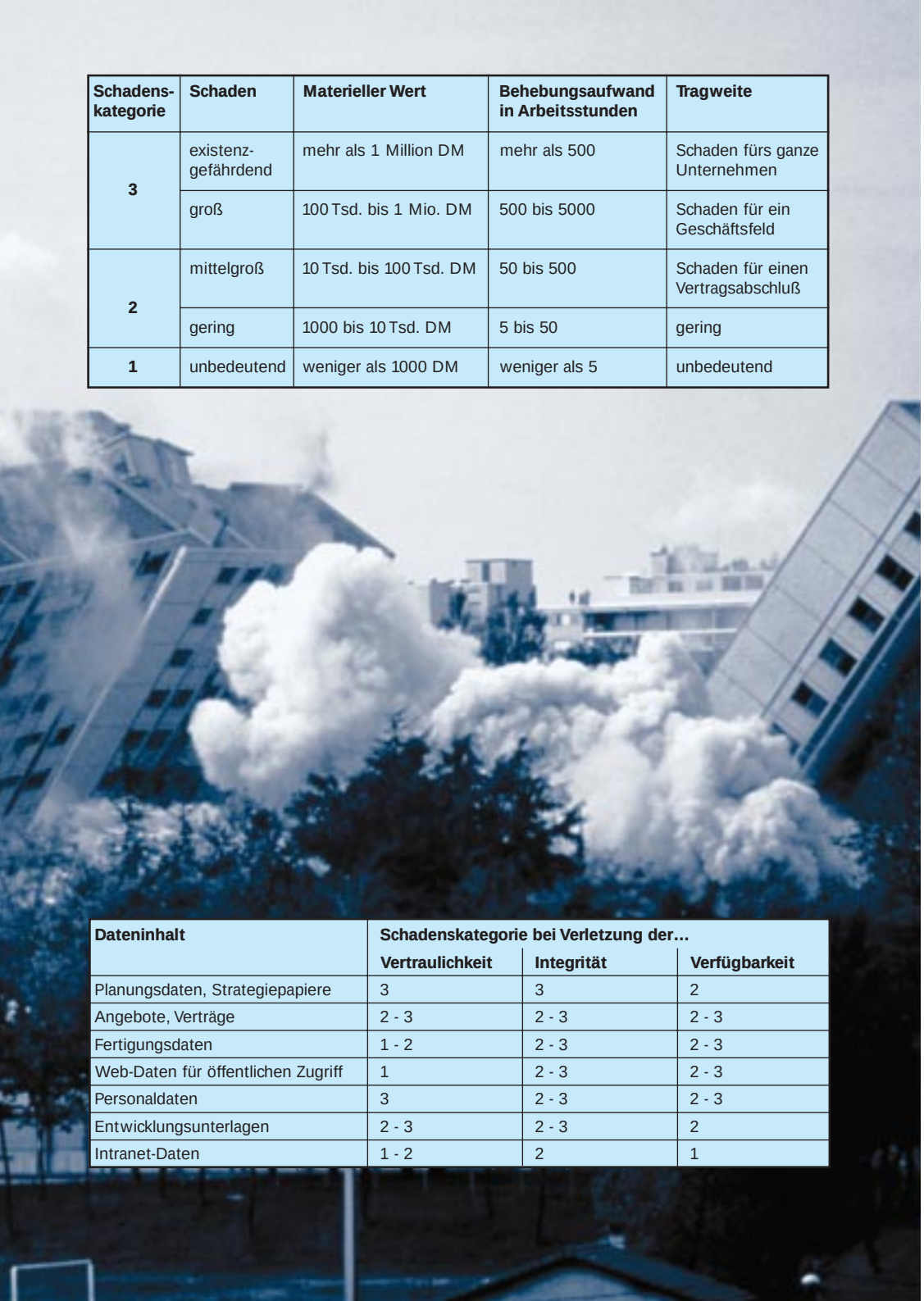
2. **Zugang zu schützenswerten Daten erhalten nur dazu berechtigte Personen. Zum Nachweis der Berechtigung ist eine Authentisierung erforderlich.**

Das dritte Ziel wiederum ist eine wichtige Maßnahme zur Erreichung des zweiten Ziels für den Fall, dass Daten über öffentliche Leitungen geschickt werden. Die internen Zugangsbeschränkungen reichen dann für einen sicheren Schutz nicht mehr aus und bedürfen der Ergänzung durch Datenverschlüsselungsverfahren:

3. **Vertrauliche Daten werden bei der Übertragung über öffentliche Netze vor unbefugter Kenntnisnahme geschützt.**

Diese Sicherheitsziele sind, wie das die Art von Gesetzestexten ist, sehr allgemein und müssen im Unternehmensalltag mit Leben erfüllt und in praktisch anwendbare Regeln überführt werden. Erste Anleitungen dazu geben die folgenden Seiten. Weitere Informationen finden Sie in den auf Seite 15 genannten Quellen.

Schadens-kategorie	Schaden	Materieller Wert	Behebungsaufwand in Arbeitsstunden	Tragweite
3	existenz-gefährdend	mehr als 1 Million DM	mehr als 500	Schaden fürs ganze Unternehmen
	groß	100 Tsd. bis 1 Mio. DM	500 bis 5000	Schaden für ein Geschäftsfeld
2	mittelgroß	10 Tsd. bis 100 Tsd. DM	50 bis 500	Schaden für einen Vertragsabschluß
	gering	1000 bis 10 Tsd. DM	5 bis 50	gering
1	unbedeutend	weniger als 1000 DM	weniger als 5	unbedeutend



Dateninhalt	Schadenskategorie bei Verletzung der…		
	Vertraulichkeit	Integrität	Verfügbarkeit
Planungsdaten, Strategiepapiere	3	3	2
Angebote, Verträge	2 - 3	2 - 3	2 - 3
Fertigungsdaten	1 - 2	2 - 3	2 - 3
Web-Daten für öffentlichen Zugriff	1	2 - 3	2 - 3
Personaldaten	3	2 - 3	2 - 3
Entwicklungsunterlagen	2 - 3	2 - 3	2
Intranet-Daten	1 - 2	2	1

Wie bei der Autoversicherung: Risikoklassen

Ob eine Datei, ein Dokument oder eine E-Mail besonders zu schützen ist – und wie – , hängt von dem Schaden ab, der dem Unternehmen zugefügt werden kann, wenn eine der zuvor beschriebenen Kategorien, also die Vertraulichkeit, die Integrität oder die Verfügbarkeit, gefährdet ist.

Je nach potenzieller Schadensgröße gibt es geeignete Maßnahmen, um die Information ihrem Wert entsprechend zu schützen. Das kann aber im Extremfall auch bedeuten, dass eine Information überhaupt nicht mit Mitteln der Informationstechnik verarbeitet oder transportiert werden darf.

Ein Beispiel:
Kann ein Angebot im zweistelligen Millionen-DM-Bereich nicht als verschlüsseltes Dokument übermittelt werden, weil das Empfängerland keine Kryptografie zulässt, muss evtl. mit Kurier gearbeitet werden.

Versuchen Sie, die in Ihrem Bereich zu verarbeitenden Daten einem materiellen Wert gegenüber zu stellen, so wie das in den Tabellen auf der linken Seite gezeigt wird. Dann können Sie auch einfacher die anzuwendenden Maßnahmen bestimmen, mit denen die Daten zu schützen sind.

Wenn Sie bei der Datenübertragung nicht sicher sind, ob mit verschlüsselten Leitungen gearbeitet wird, oder wenn Sie nicht wissen, wie man die Verschlüsselung herbeiführt, fragen Sie bitte bei den Abteilungen 3DV oder 4SG nach.

Was kann der Einzelne tun?

Zunächst gilt es zu erkennen, ob für bestimmte Daten ein erhöhter Schutz notwendig ist. Da in der Regel alle firmenrelevanten Daten der höheren Schadenskategorien auf Netzwerk-Servern liegen – und somit potenziell von jedem Rechner im Netz aus zugänglich sind –, bleibt für den/die Einzelne(n) vor allem die Aufgabe, dafür zu sorgen, dass kein Unberechtigter über den persönlichen Arbeitsplatz-Rechner Zugriff auf diese Daten bekommt. Dieser Schutz ist einfach zu erlangen, fordert er doch nur ein wenig Selbstdisziplin, siehe nächste Seite.

Ein weiteres Schlupfloch, durch das ein gewiefter Datenspäher sich den Netzzugang erschwindeln kann, tut sich auf, wenn am Arbeitsplatz-PC ein Modem direkt an einer Amtsleitung betrieben wird. Ein solcher Betrieb ist deshalb generell verboten. Der Datenaustausch mit der Außenwelt erfolgt bei Rohde & Schwarz über zentral administrierte Router und Firewall-Systeme. Ausnahmen davon bedürfen der Genehmigung.

Den Server-Administratoren kommt im Sicherheitsbereich besondere Verantwortung zu. Ob auf einem Server für Rohde & Schwarz existenzgefährdende Daten gespeichert sind, ist für den/die Verantwortliche(n) schwer zu erkennen. Man kann aber davon ausgehen, dass ein Schaden schnell die entsprechende Größenordnung erreicht. Das bedeutet, dass für die meisten Server die gängigen Schutzmaßnahmen zur Gefahrabwendung zu treffen sind, insbesondere Maßnahmen zur

- Zutrittsregelung zum Serverraum:
  Wer darf hinein? Wie erfolgt die Legitimation?

- physischen Sicherung:
  Verhinderung, Erkennung und Eindämmung von Brand- und Wasserschäden; Klimatisierung; Notstrom

- Datensicherung:
  angemessene Backup-Verfahren; Prophylaxe gegen mögliche Katastrophen-Schäden

Allgemeine Tipps und Verhaltensregeln

Arbeitsplatz
Wenn Sie Ihren PC-Arbeitsplatz verlassen, darf der Rechner bzw. das System nicht frei zugänglich sein. Aus diesem Grund ist der auf jedem PC im Netz angebotene Bildschirmschoner mit Passwortzwang („Anmelde-Bildschirmschoner“) zu verwenden. Dieser sperrt den Systemzugang, wenn in der vorgegebenen Zeit keine Eingabe erfolgt ist.

Passwörter
Wer mag schon ellenlange, unverständliche Passwörter, die man außerdem noch ständig ändern soll. Aber: Das Passwort ist und bleibt bis auf weiteres der wichtigste Zugangs- und Sicherheitsschlüssel zu IT-Systemen. Es soll folgende Eigenschaften aufweisen: Länge mindestens acht Zeichen; keine Trivialwörter (Wörter, die sich leicht erraten lassen) oder Datumsangaben, sondern eine Mischung aus Buchstaben, Zahlen und Sonderzeichen; keine Gruppenpasswörter.

E-Mail
Da die E-Mail-Korrespondenz mittlerweile mindestens so wichtig geworden ist wie der Telefonverkehr und demnach viele firmenvertrauliche Informationen über öffentliche Datennetze fließen, kommt dem Sicherheitsaspekt besondere Bedeutung zu. Bei E-Mails innerhalb des R&S-Konzerns, also im Notes-Verbund, wird generell empfohlen, die Verschlüsselungsoption von Notes zu nutzen, wenn der Empfänger nicht am eigenen Standort sitzt. Um auch den E-Mail-Verkehr zu Geschäftspartnern und Kunden verschlüsselt abwickeln zu können, wird eine ebenso praktikable wie sichere Lösung erarbeitet. Ob es sich im Einzelfall um eine E-Mail wichtigen Inhalts handelt, die verschlüsselt werden sollte, können Sie anhand der Schadenskategorien (s. S. 8/9) entscheiden.

Viren
Viren können einen einzelnen Rechner, die PCs einer Abteilung oder ein ganzes Netzwerk lahm legen. Zum Schutz dagegen laufen bei Rohde & Schwarz sowohl auf den Servern wie auch auf den Netz-PCs Antivirenprogramme im Hintergrund, die sowohl eingehende E-Mails samt Anhängen wie auch die Datenträger überwachen. Diese Tools sollten tunlichst nicht deaktiviert werden. Natürlich können die Schutz-

Allgemeine Tipps/ Weiterführende Informationen

programme nur Viren entschärfen, die ihnen bekannt sind. Deshalb gilt die Grundregel: nur Dateien von vertrauenswürdigen Quellen auf den eigenen Rechner lassen. Da wir selbst eine solche vertrauenswürdige Quelle sein wollen (und aus Haftungsgründen auch sein müssen), sind unbedingt auch alle Datenträger, die an Kunden und Geschäftspartner gehen, auf Virenfreiheit zu prüfen.

Mobiler Einsatz
Reisende, die mit dem Laptop unterwegs sind, haben dafür zu sorgen, dass der Rechner und seine Daten nicht in falsche Hände gelangen. Besonderer Passwortschutz (z. B. Boot-Passwort), Verschlüsseln von Dateien oder ganzen Laufwerken sind die möglichen Schutzmaßnahmen. Geeignete Tools dafür können bei 3DV erfragt werden.

Weiterführende Informationen

- IT-Sicherheitshandbuch
  Für die Rohde & Schwarz-Firmengruppe ist ein IT-Sicherheitshandbuch erarbeitet worden, das die IT-Sicherheitsbelange verbindlich regelt. Sie finden es als Notes-Datenbank im Datenbank-Katalog unter dem Stichwort „Sicherheit".

- R&S-Aushang
  Im Aushang wird ebenfalls eine Rubrik „IT-Sicherheit" eingeführt. Dort finden Sie Links zu entsprechenden Datenquellen.

ROHDE & SCHWARZ GmbH & Co. KG
Mühldorfstrasse 15
81671 München

Tel. 089 4129-0
Fax 089 4129-3777

www.rohde-schwarz.com

PD 757.5643.11