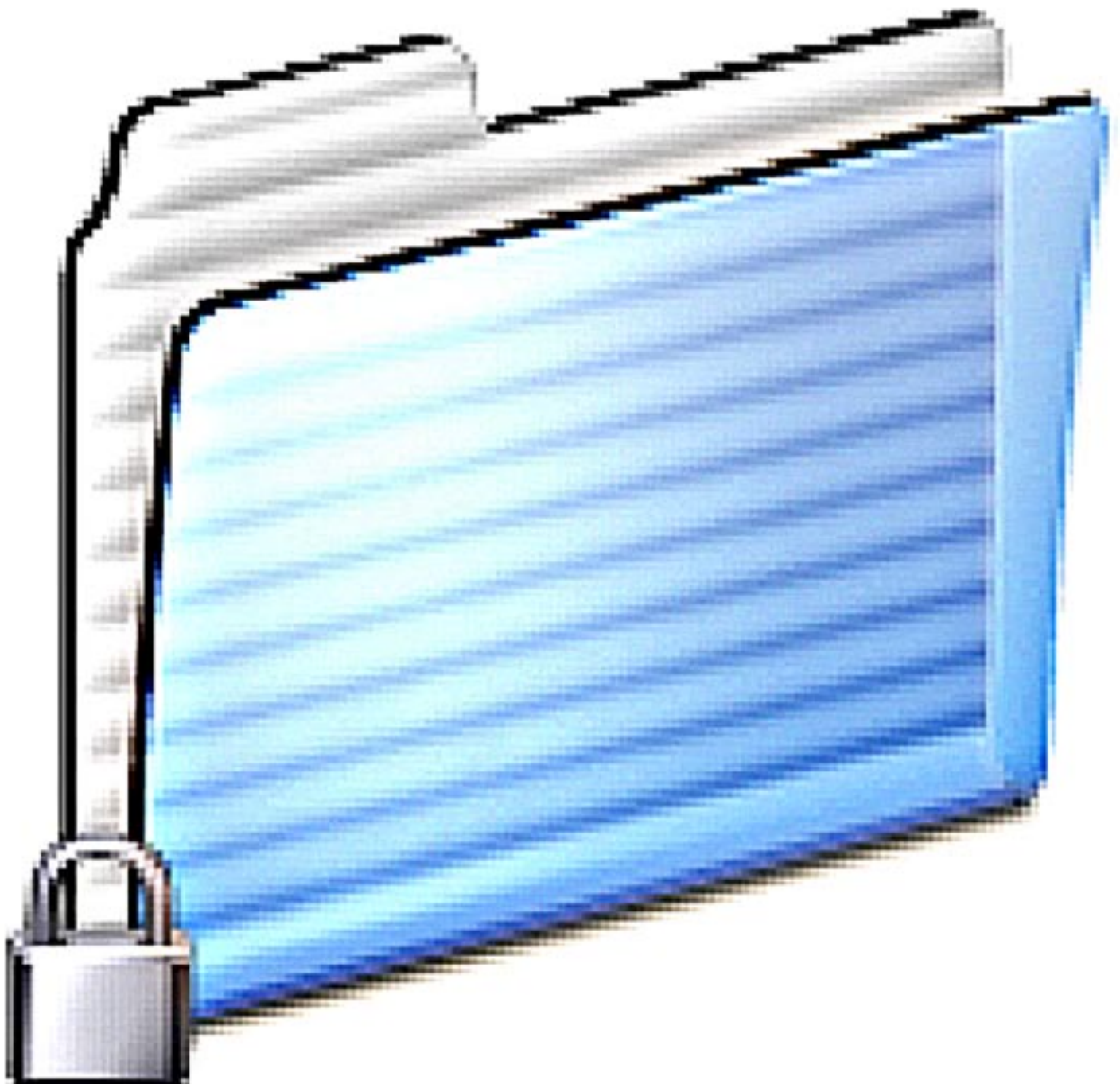


# Sicherheit – eine Aufgabe für alle

Früher konnten Unternehmen ihre Daten einfach abschotten, um sie abzusichern. Heute lasse sich ICT-Sicherheit dagegen nur mit einer strategischen Herangehensweise des gesamten Managements erreichen, sagt Eberhard von Faber, Leiter Strategie und Marketing für ICT-Security bei T-Systems. Zum Job des Sicherheitsexperten gehört es, Hackern und Spionen stets einen Schritt voraus zu sein. Sein Wissen gibt er als Honorarprofessor der Fachhochschule Brandenburg an die nächste Generation weiter.



Scharfer Beobachter:  
Hacker und Spione  
auszuspähen, ist  
die Aufgabe Eberhard  
von Fabers.



## Eberhard von Faber Von Sicherheit fasziniert

**Eberhard von Faber beschäftigt sich schon seit 17 Jahren mit der Frage, wie sich ICT-Systeme sicherer machen lassen.**

Der 1962 in Potsdam Geborene hat in Ilmenau Elektrotechnik studiert und dann in theoretischer Festkörperphysik promoviert. Sein Promotionsthema: elektronische Eigenschaften von Halbleiter-Grenzflächen, ein Grundlagenbereich der Chipproduktion. Nach Studienabschluss begann von Faber 1992 seine Laufbahn als Entwickler für Sicherheitssysteme und als Security Consultant. Drei Jahre später stieg er beim Systemhaus Debis ein, für das er in Bonn die Prüfstelle IT-Sicherheit aufbaute und jahrelang leitete. Seit 2001 arbeitet er für T-Systems. Dort ist von Faber heute Leiter Strategie und Marketing ICT-Security. Neben seinem Job behielt er immer auch allgemeine gesellschaftliche Entwicklungen im Blick. So veröffentlichte er 1998 das Buch „Die Zeit verstehen, Zukunft meistern“, in dem er naturwissenschaftliche Theorien, wie etwa die Chaosforschung, und Prinzipien der biologischen Evolution auf gesellschaftliche Phänomene bezog. Von Faber sammelt alte Rechner und Rechenmaschinen, seine Kollektion reicht von einem Rechenschieber aus seiner Schulzeit über den legendären Ur-Heimcomputer Sinclair ZX80 bis zu einem von ihm selbst gelöteten und programmierten Rechner aus den achtziger Jahren.

■ Wenn Industriespione und Hacker, Schadsoftware und Programmfehler nur auf eine Gelegenheit warten, um Daten stehlen oder beschädigen zu können, gilt es zu antizipieren, welche Angriffsszenarien besonders im Internetverkehr auf Unternehmen und deren IT-Netze zukommen. Bei der kontinuierlichen Fortentwicklung intelligenter Abwehrsysteme setzt die Deutsche Telekom besonders auf die Forschungsarbeit ihrer Geschäftskundentochter T-Systems. Dort sorgt ein Team von Sicherheitsprofis rund um den Strategiechef Eberhard von Faber dafür, dass neueste Sicherheitssysteme Spione und Hacker zur Verzweiflung bringen.

„Als ich 1992 in das Thema Sicherheit einstieg, war alles noch recht übersichtlich“, erinnert sich von Faber. Damals steckten World Wide Web und Vernetzung noch in den Kinderschuhen. Nutzer reichten ihre Anliegen oft noch bei Rechenzentren ein, in denen eine Elite Großrechner und Daten verwaltete. Unternehmen, die Geräte und Inhalte absichern wollten, mussten diese einfach nur nach außen abschotten.

Das geht heute nicht mehr: IT-Systeme müssen offen bleiben, weil mobile Mitarbeiter, Kunden und Zulieferer rund um den Globus Zugang zu den Daten eines Unternehmens brauchen. Außerdem steckt die IT-Intelligenz dezentralisiert in vielen kleinen Geräten. Zugleich ist der digitale Datenstrom stark angeschwollen, weil die Daten fast aller Geschäftsprozesse in der Wirtschaft durchgängig digitalisiert sind. „Früher wurde die rote Mappe mit den vertraulichen Daten nur im Unternehmen über den Flur getragen – heute laufen dieselben sensiblen Daten über öffentlich zugängliche IP-Verbindungen und müssen entsprechend sicher abgeschirmt werden“, sagt von Faber.

Gefahren drohen diesen sensiblen Daten in Unternehmen von innen und von außen. Und von Faber weiß, wovon er spricht.

Im Master-Studiengang Security-Management – einzigartig in der deutschen Hochschullandschaft – forscht und lehrt von Faber an der Fachhochschule Brandenburg, mit welchen Attacken auf ihre Datenschätze Unternehmen zukünftig rechnen müssen, welche Abwehrsysteme Unternehmen schon heute auf die Zukunft vorbereiten und wo in den Unternehmen die sinnvollsten Schnittstellen liegen, um die Datensicherheit nachhaltig zu machen.

Der 46-Jährige ist bei T-Systems für Strategie und Marketing im gesamten Bereich ICT-Security verantwortlich, also für Produkte und Dienstleistungen, die Informations- und Kommunikationstechnik (ICT) sicherer machen. Seine Instrumente sind Firewalls, Gateways und Tunnelverbindungen, die die IT-Systeme von Unternehmen und deren Daten und Ideen schützen.

### Umfassendes ICT-Security-Portfolio

Denn, so von Faber: „Ein totales Abschotten kann sich in Zeiten von globalem Sourcing, weltweitem Datenverkehr und weitverzweigten Lieferketten fast kein Unternehmen mehr leisten.“ Darum brauchen Datenetze ausgeklügelte Systeme, die den Verkehr an den Schnittstellen effizient kontrollieren und ihn trotzdem nicht behindern. Und in Zeiten globalen Wettbewerbs müssen Security-Systeme dafür Sorge tragen, dass Konstruktionsunterlagen und anderes geistiges Eigentum nicht unerlaubt abfließen.

Von Faber analysiert permanent Markt- und Technologietrends, schiebt Innovationsprojekte an und kümmert sich um das Vermarkten neuer Lösungen. „Vom Erkennen neuer Entwicklungen über das Umsetzen in ein entsprechendes Produkt bis zur Marktkommunikation ist das bei uns ein durchgängiger Prozess“, erklärt von Faber. Dazu gehört auch, dass er kürzlich 120 Unternehmen zu ihren Sourcing-Strategien befragt hat, sich beim Branchenverband BITKOM in der Arbeitsgruppe Sicherheit



engagiert und für neue Produkte schon mehrfach den TeleTrust-Innovationspreis verliehen bekam. So ist ein ICT-Security-Portfolio entstanden, das sich nahtlos entlang den Wertschöpfungsketten der unterschiedlichsten Branchen erstreckt. Es reicht von Produkten wie Managementsystemen für Identitäten und Zugriffsrechte sowie Lösungen für elektronische Signaturen bis zu Dienstleistungen wie etwa Risikoanalysen, Sicherheitskonzepten oder dem kompletten Betrieb von Sicherheitslösungen für Kunden. Mit dem Security-Portfolio schützt T-Systems die Daten und die Kommunikation von Unternehmen vor allen denkbaren Gefahren.

### Schaden durch Wirtschaftsspione

#### 20 Milliarden Euro

Doch Industriespione und Datendiebe gehen immer professioneller vor und führen technisch ausgefeiltere Angriffe aus. So entdeckten beispielsweise in Großbritannien kürzlich die Betreiber von Kreditkartenterminals, dass die Geräte schon bei der Herstellung in China oder beim Transport manipuliert worden waren. Über Mobilfunknetze übertrugen die Terminals Kreditkartendaten an eine Hackerbande im pakistanischen Lahore. „Eine solche Operation hätte früher nur ein nationaler Geheimdienst ausführen können“, kommentierte der US-Geheimdienstkoordinator Joel Brenner: „Das kann einem schon Angst machen.“ Die aufwendigen Aktionen lohnen sich. Der Staatssekretär im Bundesministerium des Innern, August Hanning, bezifferte die Verluste, die allein bei nationalen Unternehmen durch Wirtschaftsspionage entstehen, auf jährlich mehr als 20 Milliarden Euro.

Das Problem betrifft Unternehmen aller Größenordnungen und Branchen. „Kaum ein Unternehmen kann heute ausschließen, zu einem Ziel von Wirtschaftsspionage oder kriminellen Hacker-

„Unser Studiengang bezieht Sicherheit im Wirtschaftsleben ganzheitlich auf Unternehmenssicherheit und nicht nur auf Informationstechnik.“

Johanna Wanka,  
Wissenschaftsministerin von Brandenburg

angriffen zu werden“, sagt der T-Systems-Experte. Diesen neuen Herausforderungen sollten Unternehmen mit einer ganzheitlichen, strategischen Herangehensweise entgegentreten. „In diesem Prozess ist Informationssicherheit mehr als nur das Resultat von ein paar technischen Abwehrmitteln“, betont von Faber. Vielmehr sei sie das Ergebnis eines Konzerts aufeinander abgestimmter Maßnahmen in allen Organisationseinheiten, Prozessen und verwendeten Systemen: „ICT-Sicherheit fügt sich ein und wird so Bestandteil der Unternehmensführung.“

#### Investitionen zahlen sich aus

Die Sicherheit ist nicht kostenlos. Für Produkte, Beratungen und Umstrukturierungen werden zunächst Investitionen fällig. Vor allem kleine und mittlere Unternehmen können dabei auf automatisierte Managed Security Services zurückgreifen, also die Sicherheitsverantwortung an professionelle Anbieter auslagern. Deren Lösungen sind immer auf dem neuesten Stand, kostensparend und helfen den Nutzern, sich auf ihr Kerngeschäft zu kon-

zentrieren. So wird Komplexität beherrschbar und die Kosten lassen sich senken. „In jedem Fall sind die Kosten für ICT-Sicherheit ein Teil der allgemeinen Kosten für die Geschäftsbesorgung“, erklärt von Faber. Schließlich ist das reibungslose Funktionieren der Rechen- und Kommunikationssysteme die Voraussetzung dafür, dass das Unternehmen überhaupt Geschäfte machen kann – ICT-Risiken sind Geschäftsrisiken. Eben darum zahlt es sich von Faber zufolge für Unternehmen aller Größenordnungen aus, ICT-Sicherheit ernst zu nehmen und Geld in diesen Bereich zu investieren. Schließlich sind die Schäden im Ernstfall enorm: Geistiges Eigentum geht verloren, die Produktion gerät ins Stocken, die Reputation bei Kunden und Geschäftspartnern sinkt, die Motivation der eigenen Mitarbeiter schwindet.

#### Risk Management beim Vorstand ansiedeln

Weil Informationssicherheit derart wichtig ist, sollte ein eigenes Corporate Risk Management Office dafür verantwortlich sein, rät von Faber. Und das sei nicht in der IT-Abteilung am besten aufgehoben – sondern beim Vorstand.

Das neue Sicherheitsbüro sollte sich dabei von Faber zufolge am besten als Mittler zwischen der IT-Abteilung und den ausführenden Geschäftseinheiten verstehen: Es übersetzt technische Informationen von den IT-Abteilungen in Angaben zu geschäftlichen Risiken. Auf dieser Grundlage könnten die Geschäftseinheiten Entscheidungen treffen, welche die Sicherheitsmanager dann wieder in technische Anforderungen für die IT-Abteilung übersetzten.

So hat die Deutsche Telekom beispielsweise nach Erfahrung mit kriminellen Datendieben im Privatkundengeschäft Ende Oktober Dr. Manfred Balz zum neuen Vorstand für Datenschutz, Recht

FH Brandenburg:  
einzige deutsche  
Hochschule mit  
dem Studiengang  
Security  
Management.

und Compliance berufen. Der Jurist und sein neu geschaffenes Ressort sind zur Durchsetzung ihrer Strategien und Policies mit umfassenden Informations- und Kontrollrechten ausgestattet. Dabei hat die interne und externe Prävention von Datenmissbrauch bei der Deutschen Telekom und ihren Unternehmenstöchtern oberste Priorität. „Ich nehme jeden Manager und Mitarbeiter in die Pflicht, der mit dem Schutz und der Sicherheit von Kundendaten befasst ist“, so Manfred Balz.

#### Hohe Auszeichnung für T-Systems-Forschung

Die Ergebnisse seiner Forschung gibt von Faber als Honorarprofessor der Fachhochschule Brandenburg an die nächste Generation von Sicherheitsexperten weiter. Passend zu seinen Thesen von der neuen Rolle der ICT-Sicherheit ist der Studiengang nicht im Fachbereich Informatik angesiedelt, sondern zählt zu den Wirtschaftsstudiengängen.

T-Systems hat zusammen mit anderen Partnern, darunter SAP, bei Aufbau und Gestaltung des Studiengangs mitgewirkt. Erst Ende 2006 gerade auf den Weg gebracht, erhielt der Studiengang bereits die Auszeichnung mit dem Preis der Initiative „Deutschland – Land der Ideen“. Lob und Anerkennung bekommt von Fabers Hochschularbeit auch von politischer Ebene: So lobte Brandenburgs Wissenschaftsministerin Prof. Dr. Johanna Wanka, der deutschlandweit einmalige Studiengang beziehe „Sicherheit im Wirtschaftsleben ganzheitlich auf Unternehmenssicherheit und nicht nur auf den engeren Bereich der Informationstechnik“. Und eben das ist auch Eberhard von Fabers Ziel.

FLORIAN SIEVERS

★ **LINKS**  
[www.t-systems.de/datensicherheit](http://www.t-systems.de/datensicherheit)  
[www.t-systems.de/managed-security-services](http://www.t-systems.de/managed-security-services)

## Interview

# „Sicherheit muss der Strategie folgen“

Drei Fragen an den ICT-Security-Experten Carsten Casper,  
Research Director, Gartner Deutschland

#### Wie kann ein Unternehmen ermitteln, wie gefährdet es durch Angriffe auf die eigene ICT-Infrastruktur ist?

Das konkrete Gefährdungsniveau hängt von vielen Faktoren ab, unter anderem von der Branche, der Unternehmensgröße, dem Standort, dem Grad der Zentralisierung, dem Reifegrad der IT und der IT-Sicherheit sowie der Unternehmenskultur. Für eine genaue Einschätzung ist eine konkrete Risikoanalyse notwendig – am besten bezogen auf eine Applikation oder einen Geschäftsprozess.

#### Aus einer solchen Analyse werden sich konkrete Schutzmaßnahmen ergeben.

#### Wie sollten sich diese zur unternehmerischen Gesamtstrategie verhalten?

Informationssicherheit muss immer von der Strategie des Unternehmens abgeleitet sein und darf sich nicht danach richten, was sich die IT-Techniker als optimale und sicherste Lösung vorstellen. Geht das Unternehmen gern Risiken ein, muss die Informationssicherheit vor allem flexibel gestaltet sein. In regulierten Industriebereichen wie dem Finanz- oder dem Gesundheitssektor gilt das Gegenteil: Ausfälle können hier unter Umständen sogar Menschenleben kosten oder zumindest Millionen von Euro. Entsprechend konsequent muss auch die Informationssicherheit aufgestellt sein. In vielen

Fällen funktioniert die Kopplung von Unternehmensstrategie und Informationssicherheit über ein umfassendes Risikomanagement.

#### Wann rechnet es sich, ICT-Sicherheit an einen professionellen Anbieter auszulagern?

Das Outsourcing von Informationssicherheit ist kein Tabu mehr. Doch ein Unternehmen sollte zunächst wichtige Sicherheitsleistungen selbst erbringen. Denn: Ein späteres Auslagern funktioniert dann am besten, wenn man die extern erbrachte Leistung verstehen, kontrollieren und auch wertschätzen kann. Wann es sich genau rechnet, hängt ab von der Anzahl der eigenen Mitarbeiter, deren Fähigkeiten und vom Reifegrad der ausgelagerten Leistung. Große Unternehmen können die notwendige Skalierbarkeit häufig selbst erreichen und haben auch sehr spezielle Anforderungen, kleinere Unternehmen können sich auch gut auf Standardkonfigurationen einlassen.

„Informationssicherheit muss immer von der Unternehmensstrategie abgeleitet sein.“

Carsten Casper,  
Gartner Deutschland



FOTOS: PR