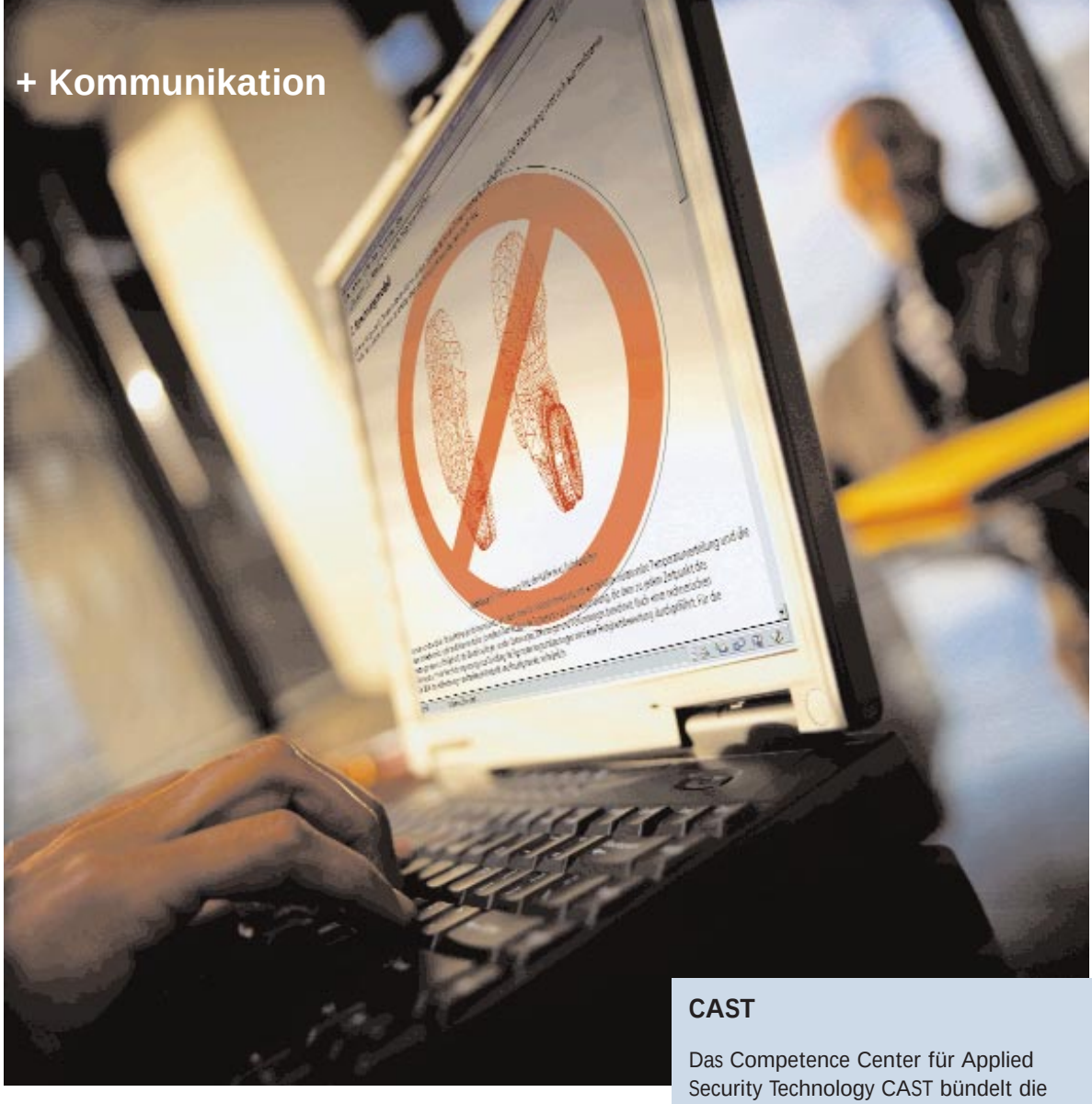


Sicher ins Netz

Früher schützten sich die Menschen mit dem Bau von dicken Stadtmauern und schweren Schlössern vor Einbrechern. Im Zeitalter des Internets sollen nun, elektronische Schützwälle und digitale Schlüssel wichtige Firmendaten und Informationen vor Diebstahl und Manipulation sichern.

Homebanking, Online-Shopping, elektronische Post sekundenschnell verschicken, per Mausklick mit Kunden oder Geschäftspartner rund um den Globus in Verbindung treten, Behördengänge am heimischen Computer erledigen - das Internet macht es möglich. Doch das weltumspannende Netz birgt auch neue Risken und Gefahren: Es ist auch ein Einfallstor für Datendiebe, Betrüger oder Saboteure. Erst vor wenigen Wochen setzte das per E-Mail verschickte Virus »I love you« weltweit zahlreiche Firmennetze außer Betrieb. Geschätzter Schaden: Etwa fünf Milliarden DM. Schon wenige Monaten zuvor hatten »Hacker« gezeigt, wie anfällig das Internet

CAST

Das Competence Center für Applied Security Technology CAST bündelt die Kompetenzen des Fraunhofer-Instituts für Graphische Datenverarbeitung IGD, der TU Darmstadt und des Institut für Sichere Telekooperation GMD-SIT im Bereich der Sicherheit moderner Informationstechnologien. Es ist ein offenes Netzwerk, an das industrielle Partner sowie eine Reihe von kleinen und mittleren Unternehmen angeschlossen sind. Die Ziel des CAST-Forums ist es, neue Technologien und Know-how aus der Forschung in die Praxis zu umzusetzen. Das CAST Forum bietet Aus- und Weiterbildungen, Consulting, Evaluierung von Sicherheitskonzepten und -technologien, sowie den Austausch und Zugang zu Forschung und Entwicklung in diesem für die Industrie so wichtigen Bereich an.

Ansprechpartner:
Dr. Christoph Busch
Telefon: 0 61 51/155 -147
Telefax: 0 61 51/155 - 4 99
E-Mail: busch@igd.fhg.de

gegen Attacken von außen ist. Sie legten bedeutende Internet-Unternehmen wie den Suchdienst Yahoo, den Online-Auktionär eBAY, das elektronische Versandhaus amazon oder das E-Commerce Unternehmen Buy.com für mehrere Stunden lahm. Mittlerweile hat auch die Bundesregierung erkannt, dass die Sicherheit im Netz eine »Schlüsselfrage für jede moderne Volkswirtschaft« ist. Deshalb hat Innenminister Otto Schily sogar eine TaskForce zu diesem Thema gebildet. Zudem informieren das Bundesinnenministerium, das Bundeswirtschaftsministerium und das Bundesamt für Sicherheit in der Informationstechnik unter der Internet-Adresse http://www.sicherheit-im-internet.de/, wie Firmendaten oder E-Mails vor unberechtigten Zugriffen geschützt werden können.

»Leitungsfähige Sicherheitssysteme werden für die moderne Informations- und Kommunikationsgesellschaft immer wichtiger«, betont Prof. José Encarnação, Leiter des Fraunhofer-Instituts für Graphische Datenverarbeitung IGD in Darmstadt. Daher hat das IGD im vergangenen Jahr gemeinsam mit TU Darmstadt und dem Institut für Sichere Telekooperation GMD-SIT das Competence Center für Applied Security Technology CAST gegründet. Ziel des Forums am im Zentrum für Graphische Datenverarbeitung e.V. (ZGDV) ist es, neue Sicherheitstechnologien schneller und effektiver in die Wirtschaft zu transferieren.

castforum.de/

»Ein Zugang zum Internet ist wie ein Haus an einer großen, verkehrsreichen Straße. Viele Menschen kommen an diesem Haus vorbei und nicht alle haben lautere Absichten. Bei der riesigen Anzahl an Firmen, Organisationen und Einzelpersonen, die sich im Internet tummeln, muss man mit Angriffen rechnen«, beschreibt CAST Geschäftsführer Dr. Christoph Busch die Situation im World-Wide-Web. »Wir helfen Unternehmen, ihre Daten vor unberechtigen Zugriffen oder Manipulationen zu schützen.«

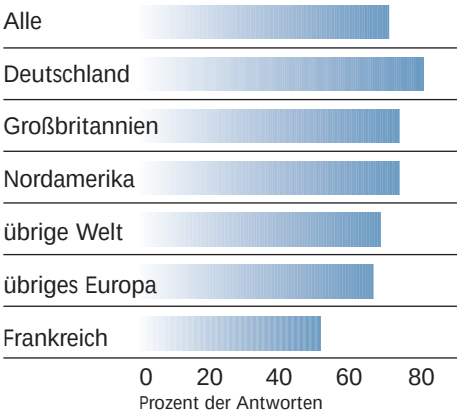
So stellt das CAST zum Beispiel in Workshops neue Technologien und Sicherheitssysteme vor, die elektronische Daten vor Diebstahl oder Missbrauch sichern: Eine Möglichkeit, unbefugte Zugriffe auf Firmennetze zu verhindern, sind Firewalls. Während früher dicke Stadtmauern, Städte vor ungewollten Eindringlingen abschirmten, sichern heute elektronische Schutzwälle, Firewalls, Rechner vor Raubrittern aus dem Internet ab. Firewalls lassen nur eine kleine Auswahl von Internet-Anwendungen zu, kontrollieren Datenströme und verweigern Unbefugten den Zugriff auf Firmenrechner. Doch wie leistungsfähig sind die bisher angebotenen Firewall-Systeme? Welches System ist für meine Anforderung geeignet? Antworten auf diese Fragen gibt das Firewall Technology Center im CAST. Dort werden kommerzielle Firewall-Systeme getestet und Anwendern verschiedene Architekturen demonstriert. So können sie sich selbst ein Bild von den Vor- und Nachteilen der einzelnen Systeme machen.

sicherheit-im-internet.de/

»Firewalls sind jedoch kein Allheilmittel, sondern nur ein Baustein eines umfassenden Sicherheitskonzepts«, erläutert Busch, der am IGD auch die Abteilung Sicherheitstechnologien für Graphik- und Kommunikationssysteme leitet. Andere Sicherungssysteme müssen die elektronische Schutzwälle ergänzen, um einen effektiven Schutz zu bieten. Verschlüsselungen - kryptographische Algorithmen, die die Daten unleserlich machen - verhindern zum Beispiel, dass Dritte elektronisch gespeicherte Geschäftspapiere oder via E-Mail verschickte Verträge lesen oder verfälschen können. Ähnlich wie beim Fernsehsender Premiere kann nur derjenige, der den richtigen Schlüssel besitzt, die so gesicherten Programme beziehungsweise Dokumente anschauen. Bei diesen Public-Key Infrastrukturen (PKI) erhält jeder Teilnehmer zwei Schlüssel: Einen privaten, mit dem digital signieren und für ihn personifiziert verschlüsselte Dokumente öffnen kann und einen öffentlichen Schlüssel (Public Key), der frei verteilt werden kann, um die durch den Teilnehmer vorgenommen digitale Signatur von jedermann verifizieren zu können. »Public Key Kryptosysteme machen es möglich, Daten authentisch und vertraulich zu speichern und zu übertragen. Diese Sicherheits-Technologie ist ein wichtiger internationaler Standard«, sagt der IGD-Wissenschaftler.

Das Internet revolutioniert auch den Vertrieb von Musik, Bildern und Videos. Ein Knopfdruck genügt, und schon können sich Internet-Nutzer Bilder von Fotoagenturen, den aktuellen Hit ihrer Lieblingsgruppe oder Videodaten herunterladen. Häufig wird dabei jedoch gegen Urheberrechte verstoßen. Eine Möglichkeit, die illegale Nutzung von multimedialen Daten zu vermeiden, sind digitale Wasserzeichen. Anders als das Wasserzeichen im Papier, das man sehen kann, ist das digitale Wasserzeichen unsichtbar. Es besteht aus kleinen, mit dem Auge nicht wahrnehmbaren Veränderungen der Frequenzen der Signale von Bild-, Video- und Audiodaten. Die Multi-Media Daten werden mit einem unsichtbaren Code versehen. So lässt sich der Urheber immer feststellen. Unsichtbare und robuste Wasserzeichen

Wurden Sie gehackt?
Umfrage bei 2700 Sicherheitsexperten



Quelle: PriceWaterhouseCoopers, Juli 99

werden zum Beispiel bei TALISMAN eingesetzt, einem vom Thomson CSF, dem IGD und neun weiteren Partnern entwickelter Mechanismus für den Urheberrechtsschutz digitaler Videodaten. Das System wurde erstmals bei der Fußball Weltmeisterschaft 1998 eingesetzt. Dort wurden alle von der European Broadcasting Union zu den nationalen Sendern übertragenen Sendungen mit einem digitalen Wasserzeichen versehern. »Mit digitale Wasserzeichen können aber auch Firmendaten geschützt werden. Sie erschweren die Industriespionage«, führt Busch aus. Wichtige und vertrauliche Informationen werden einfach mit einem unsichtbaren Code versehen. Geraten die Firmengeheimnisse in fremde Hände, so kann der Eigentümer das Wasserzeichen auslesen, die Information rekonstruieren und den Dieb überführen.

bsi.de/

Online-Banking, virtuelle Rathäuser, Geschäfts- und Kundenkontakte rund um den Globus - das Internet bietet zahlreiche neue Möglichkeiten. Doch erst wenn E-Commerce und Datentransfer via Internet vor Diebstahl und Manipulation wirklich sicher sind, werden Verbraucher und Firmen die Möglichkeiten auch umfassend nutzen.
Birgit Niesing