



e-f@cts

Informationen
zum E-Business

Innovationspolitik, Informationsgesellschaft, Telekommunikation

Schwerpunkt

Sicherheit im E-Business: Risiken für alle Internetnutzer, Risiken für Unternehmen; Sicherheitsmaßnahmen für jedes IT-System, Sicherheitsmaßnahmen für Unternehmen.

► ab Seite 1

Fakten & Zahlen



► ab Seite 3

E-Business-ABC

Aktive Inhalte, ActiveX, Browser, Cache, Cookie, History, Java, Javascript, SSL

► ab Seite 4

Praxis & Technik

Virenschutz und
Browser-Sicherheits-Tipps

► Seite 6

Sicherheit im E-Business

Das Internet ist ein offenes Netz, an dem jeder teilnehmen kann. Das macht seinen „Charme“ aus. Der Nachteil dabei ist: Es gibt keine Aufsicht oder Kontrollinstanz, die für Sicherheit sorgt. Für die Sicherheit ist jeder Nutzer selbst verantwortlich.

Mit Sicherheit ist dabei in erster Linie der sichere Transport und die sichere Speicherung von Daten gemeint. Aber auch die angeschlossenen Rechner können bei Sicherheitsproblemen in Mitleidenschaft gezogen werden.

Gefahren drohen dabei übrigens nicht nur von außen. Gerade in Unternehmen entstehen Sicherheitsprobleme auch von innen. Dies wird immer wieder übersehen und führt – bei noch so großem Bemühen um Unverwundbarkeit – zwangsläufig zu Lücken in den Sicherheitsvorkehrungen.

Risiken für alle Internetnutzer

Viren: Ein Computer-Virus ist ein Programm, das z. B. per E-Mail, Download oder den Austausch von Disketten in einen Computer gelangt,

sich dort festsetzt und meist Datenbestände verändert oder löscht. Erstmals hat der „I-LOVE-YOU-Virus“ vor nicht allzu langer Zeit einer breiten Öffentlichkeit deutlich gemacht, wie groß ein solcher Schaden sein kann, sowohl bei privaten PCs als auch in großen Unternehmensnetzen.

Trojanische Pferde: Ein Trojanisches Pferd ist ein Programm, das – nicht erkennbar – in ein für Nutzer attraktives „Wirtsprogramm“ eingebettet ist. Dieses „Wirtsprogramm“ wird beispielsweise zum Download angeboten oder als Anhang an E-Mails verschickt. Öffnet man dieses „Wirtsprogramm“, wird die verdeckte Software gestartet und richtet Schaden auf der Festplatte oder im Netz eines Nutzers an.

Kein Schutz gegen aktive Inhalte: Gerade so genannte Standardsoftware (z. B. Internet-Explorer als Browser) wird unnötigerweise dadurch zur „Zeitbombe“, dass vorhandene Sicherheitsoptionen nicht genutzt werden – beispielsweise die Option, aktive Inhalte (Java, JavaScript, ActiveX) fremder Internetseiten nicht zuzulassen (s. Praxis & Technik, S. 6). Aktive Inhalte sind

Sicherheit im E-Business



Inhalt

Schwerpunkt

Sicherheit im E-Business: Risiken für alle Internetnutzer, Risiken für Unternehmen; Sicherheitsmaßnahmen für jedes IT-System, Sicherheitsmaßnahmen für Unternehmen.

► ab Seite 1

Fakten & Zahlen



► ab Seite 3

E-Business-ABC

Aktive Inhalte, ActiveX, Browser, Cache, Cookie, History, Java, Javascript, SSL

► ab Seite 4

Praxis & Technik

Virenschutz und Browser-Sicherheits-Tipps

► Seite 6

Computerprogramme, die in Internetseiten bereits enthalten sind oder beim Betrachten einer Internetseite automatisch nachgeladen werden: Sie können gezielt zu dem Zweck erstellt worden sein, vertrauliche Daten des Benutzers auszuspionieren.

Ungeschützte Kommunikation: Alle Arten der Kommunikation über das Internet sind anfällig für „Lauscher“ – aus technischen Gründen, vor allem aber auch wegen der Sorglosigkeit der Kommunikationspartner. E-Mails werden heutzutage gerne als das moderne Pendant zur Briefpost genutzt. Dabei kann eine E-Mail aber eigentlich nur mit dem Versenden von Postkarten gleichgesetzt werden, die mit Bleistift geschrieben sind. Die Technik macht es möglich, dass jeder sie mitlesen und verändern, womöglich sogar aufhalten kann, ohne dass dies nachweisbar wäre.

Fehlende Identifikation: Woher wissen Sie, wer Ihr Gegenüber – bei E-Mails oder bei Webseiten im Internet – ist? In offenen Netzen wie dem Internet stehen hinter Namensangaben nicht unbedingt die damit assoziierten Personen oder Institutionen. Beispiel: Unter www.xy-bank.com findet sich nicht unbedingt die XY-Bank. Ebenso sind Absenderangaben bei E-Mails leicht zu fälschen.

Fehlendes Bewusstsein, mangelnde Information: Fast immer kommen mehrere Gründe dafür zusammen, dass z. B. Viren, Trojanische Pferde oder aktive Inhalte tatsächlich Schäden anrichten können. Wären sich Nutzer der konkreten IT-Sicherheitsprobleme bewusst und wüssten sie mehr darüber, wie sie sich vor drohenden Gefahren schützen könnten, so würde eine Vielzahl der bekannten Schäden ausgeschlossen.

Risiken für Unternehmen

Wer E-Business-Komponenten einsetzt, will in der Regel ein breites Publikum erreichen. Das bedeutet: Auch im Internet stehen die „Türen“ für Kunden weit offen. Folge: Ein E-Business-Anbieter muss auch immer mit unerwünschten Besuchern rechnen. Dabei werden meistens die Gefährdungen von außen als größtes Sicherheitsproblem gesehen. Darüber dürfen aber auch die weniger spektakulären, aber meist häufige-

ren internen Sicherheitsprobleme nicht vernachlässigt werden.

Gefährdungen von außen: Über Hacker-Angriffe wird immer wieder in der Presse berichtet, insbesondere dann, wenn die Sicherheitsvorkehrungen großer Unternehmen von Einzeltätern überwunden wurden (Goliath- bzw. Robin-Hood-Effekt) und sich dies auch noch eindrucksvoll präsentieren lässt. Hierzu gehören beispielsweise Angriffe, bei denen

- Webserver gezielt überlastet werden (Denial-of-Service-Attacks);
- das Webangebot manipuliert wird, also die Internetdarstellungen eines Unternehmens verändert werden (oft mit ehrverletzenden, rassistischen oder sexistischen Aussagen);
- auf internen Servern gespeicherte Kundendaten gelesen und missbraucht werden;
- Dienstleistungen unberechtigt in Anspruch genommen werden.

Gefährdungen von innen: Mängel. Es wird gerne verdrängt, dass ein Großteil aller Sicherheitsprobleme hausgemacht ist und auf technischen Defekten, Irrtümern, Fahrlässigkeit und Fehlern eigener Mitarbeiter inklusive Management, aber auch externer Dienstleister beruht. Dazu kommt: Tagtäglich fallen Betriebssysteme aus, die weniger stabil sind, als die Hersteller versprechen, weil Anwendungen nicht miteinander kompatibel oder Benutzer oder gar Administratoren ungenügend geschult sind für den Umgang mit den hochkomplexen IT-Systemen.

Gefährdungen von innen: Manipulation. Leider kommt auch die Manipulation von IT-Systemen durch die eigenen Mitarbeiter immer wieder vor. Daten oder Systeme können aus verschiedenen Motiven manipuliert werden: aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, um sich persönliche Vorteile zu verschaffen oder schlicht zur persönlichen Bereicherung. Manipulationen werden dadurch erleichtert, dass die organisatorischen bzw. technischen Hürden niedrig sind und gleichzeitig das Risiko, entdeckt zu werden, gering ist.

Gefährdungen von innen: mangelndes Sicherheitsbewusstsein. Ein mangelndes Sicherheitsbewusstsein führt schnell zu einem mangelhaften Umgang mit IT-Sicherheit. Es



betrifft dann oft nicht nur einzelne IT-Sicherheitsprozesse, sondern nicht selten auch den gesamten IT-Betrieb. Häufig ist zu beobachten, dass zwar eine Vielzahl von organisatorischen oder technischen Sicherheitsverfahren vorhanden ist, diese jedoch durch den sorglosen Umgang mit der Technik wieder ausgehebelt werden. Ein typisches Beispiel hierfür sind die fast schon sprichwörtlichen Zettel am Monitor, auf denen alle Zugangspasswörter notiert sind.

Risiken für E-Business-Kunden

Kundendaten nicht vertraulich behandelt: Viele potenzielle Kunden sind wegen ihrer Sicherheitsbedenken zurückhaltend beim Thema E-Business. Oft erfragen E-Business-Anbieter sinnvolle, aber auch überflüssige Angaben von ihren Kunden. Auf Seiten der Kunden ist hier das erstaunliche Verhalten zu beobachten, dass sie einerseits (z. B. bei Gewinnspielen) eine Unmenge persönlicher Daten bedenkenlos weitergeben, andererseits aber von Bestellungen über das Internet zurückscheuen, weil sie ihre Adresse angeben müssen. Allerdings haben eben auch viele Kunden gerade beim E-Business schlechte Erfahrungen damit gemacht, dass ihre Kundendaten z. B. an andere Unternehmen weitergegeben wurden: Sie hatten einmal im Internet bestellt, und anschließend wurde sowohl ihr Briefkasten an der Haustür als auch ihr E-Mail-Postfach mit Werbepost überschwemmt.

Kundendaten nicht gesichert: Kunden befürchten (nicht zu Unrecht), dass ihre Daten zuweilen unsicher gespeichert oder unsicher in andere Untersysteme der EDV weiter geleitet werden (z. B. Rechnungswesen). Einige Händler gehen erfahrungsgemäß so fahrlässig mit Kundendaten um, dass diese von Hackern ohne Probleme gelesen werden können.

„Wolf im Schafspelz“ – „Spoofing“: Viele Kunden haben negative Erfahrungen mit „Spoofing“ gemacht. Ein Kommunikationspartner täuscht vor, jemand Anderes zu sein, und dies normalerweise nicht mit guten Absichten.

Bezahlen über das Internet: Es gibt diverse Verfahren, die zur Zahlungsabwicklung über das Internet entwickelt wurden, die meisten befinden sich aber noch im Stadium von Pilotversuchen. Andere, vielversprechende Verfahren wie Cyber

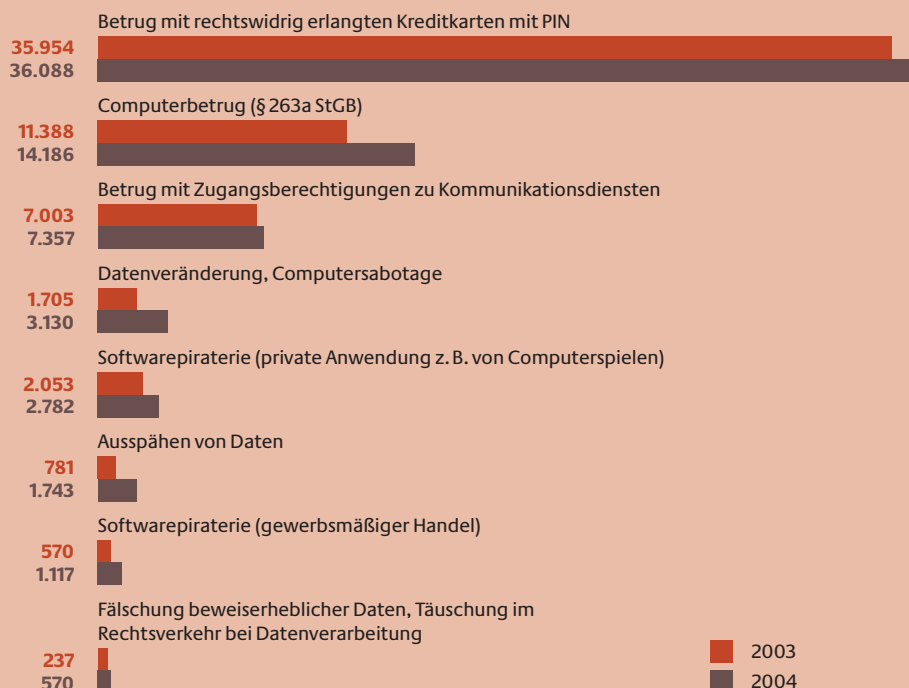
Cash oder ecash wurden bereits wieder eingestellt. Es wird noch eine Zeitlang dauern, bis sich die ersten Verfahren „internetweit“ etabliert haben. Bis dahin müssen Händler auch Zahlungsverfahren als Übergangslösungen anbieten, die weniger sicher sind als die speziell für den Electronic-Commerce entwickelten Verfahren: wie im herkömmlichen Versandhandel per Kreditkarte, per Nachnahme, Lastschrift oder Überweisung. Wichtig: Unternehmen sollten ihren Kunden anbieten, in jedem Fall personenbezogene Daten verschlüsselt zu senden (SSL). (Weitere Informationen hierzu in ef@cts 13 „Zahlungsverkehr im Internet“).

Angriffe abwehren

Virenschutzprogramme: Virenschutzprogramme überprüfen Datenträger auf eventuelle Computer-Viren. Eine solche Überprüfung sollte sowohl die am Arbeitsplatz benutzten Datenträger als auch sämtliche Datenträgerzugänge (z. B. Internet, E-Mail) umfassen.

Gefahren drohen nicht nur von außen. Gerade in Unternehmen entstehen Sicherheitsprobleme auch von innen. Dies wird immer wieder übersehen und führt zu Lücken in den Sicherheitsvorkehrungen.

Fälle von Computerkriminalität



Sicherheit im E-Business



E-Business-ABC

Aktive Inhalte

Computerprogramme, die in Internetseiten bereits enthalten sind oder beim Aufenthalt auf einer Internetseite automatisch nachgeladen werden. Häufig ist bei einem Klick auf einen Link nicht klar ersichtlich, dass damit ein aktiver Inhalt gestartet wird. Aktive Inhalte können gezielt zu dem Zweck erstellt worden sein, vertrauliche Daten des Benutzers auszuspiönieren. Die wichtigsten Beispiele für aktive Inhalte sind „Java“, „JavaScript“ und „ActiveX“.

Vorsicht: Es gibt immer wieder neue und andersartige Computer-Viren, so dass ältere Virenschutzprogramme mit der Zeit ihre Wirksamkeit verlieren, da sie nur die zu ihrem Entstehungszeitpunkt bekannten Computer-Viren berücksichtigen. Daher müssen sie regelmäßig (eigentlich täglich) aktualisiert werden. Virenschutzprogramme sind im Handel erhältlich oder können aus dem Internet heruntergeladen werden.

Auch die Verwendung der digitalen Signatur kann dem Virenschutz dienen (s. Sicherheitsmaßnahmen in Unternehmen, S.5): Wenn nämlich E-Mails immer mit einer „digitalen Signatur“ elektronisch unterschrieben wären, wüssten die Empfänger, wer ihnen was gesendet hat – immerhin 99 Prozent aller Massen-Viren erreichen die Empfänger mit gefälschten Absendern und zweifelhaften Inhalten.

Firewalls: Firewall bedeutet wörtlich „Feuerschutzwand“ oder „Brandmauer“. Es handelt sich hier um eine Hardware oder Software, die den Zugang zu internen Datensystemen etwa von Unternehmen (z. B. Intranets) beschränkt oder verhindert. Dabei ist auch zu prüfen, inwieweit das zu schützende Unternehmensnetz unterteilt werden kann, so dass nicht das gesamte Netz, sondern vielleicht nur ein geringer Teil mit dem Internet verbunden ist.

Angriffe erfassen: Intrusion Detection Systeme

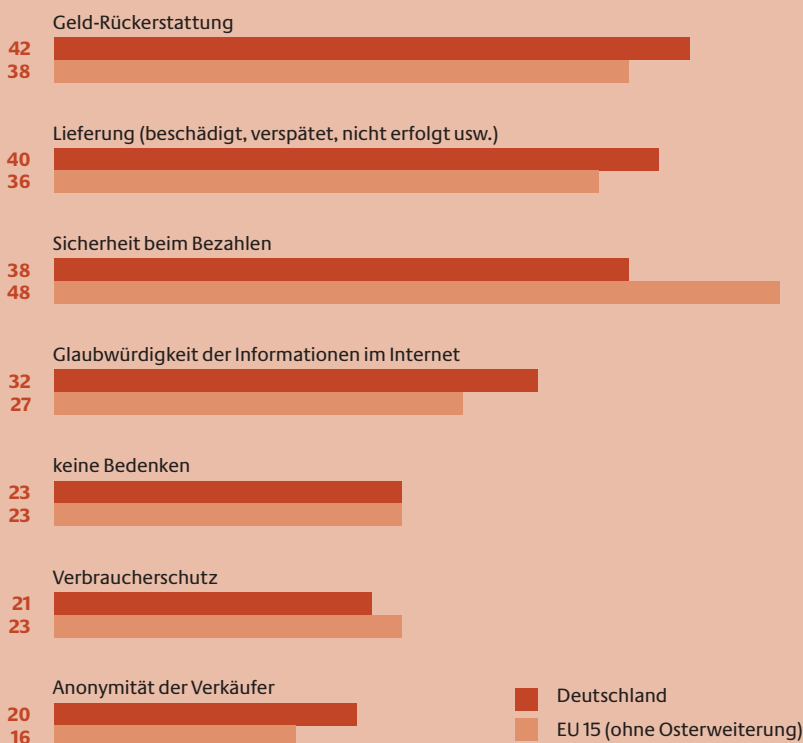
Hacker-Angriffe auf ein Netzwerk lassen sich erkennen: in den Zugriffs-Daten, die jede Firewall durch einen automatischen Firewall-Administrator protokolliert. Schwierig ist allerdings, eine Attacke in der Fülle der Daten und bei der Vielzahl und Komplexität der verschiedenen Angriffsmöglichkeiten zu entdecken. Intrusion Detection (ID) und Intrusion Response (IR) Systeme können hierbei helfen.

ID-Systeme unterstützen einen Firewall-Administrator dabei, einen Angriff aus einer großen Anzahl von Protokoll-daten herauszulesen. IR-Systeme dagegen dienen dazu, automatisch Gegenmaßnahmen einzuleiten, sobald ein Angriff erkannt wird. Zurzeit sind Intrusion Detection Systeme allerdings noch kein Allheilmittel gegen Angriffe von außen, sondern noch mit diversen Problemen behaftet, so dass sie auf keinen Fall als Ersatz für andere Sicherheitsmaßnahmen, sondern nur als Ergänzung für diese eingesetzt werden sollten.

Sowohl Firewalls als auch Intrusion Detection Systeme werden von Spezialanbietern verkauft. Welche Firewall bzw. welches Intrusion Detection System empfehlenswert ist und für bestimmte Unternehmen in Frage kommt, wird immer wieder von Fachzeitschriften getestet.

Bedenken gegen Internet-Kauf

Antworten in %





Angreifbarkeit vermindern

Verschlüsselung von Nachrichten

Bei der Online-Übertragung von Nachrichten sollten sich alle Kommunikationspartner darüber im klaren sein, dass unverschlüsselte Nachrichten während ihres gesamten Weges unbemerkt gelesen, geändert bzw. abgefangen werden können. Daher ist zu überlegen, ob die Nachrichten verschlüsselt und/oder digital signiert werden sollten. Auch innerhalb eines Unternehmens sollten alle sensiblen Geschäftsdaten vor den Augen Dritter durch Verschlüsselung geschützt werden. Besonders wichtig für die Verschlüsselung und z. B. für eine digitale Signatur:

- ▶ Ohne ein verwendetes Verschlüsselungsprogramm (Algorithmus) darf es nicht möglich sein, einen verschlüsselten Text zu rekonstruieren. Nicht in jedem Fall macht aber ein hochkomplizierter Schlüssel Sinn. „Nicht möglich“ bedeutet daher, dass der erforderliche Aufwand zum „Knacken“ des Schlüssels größer sein sollte als der Informationsgewinn, den man so erzielen könnte.
- ▶ Das Verschlüsselungsprogramm muss gut funktionieren. Leider sind viele der in Unternehmen eingesetzten Verschlüsselungssysteme von zweifelhafter Qualität. Einige Programme haben Konstruktionsfehler oder sind unverständlich.
- ▶ Die Schlüssel und der verschlüsselte Text dürfen nicht zusammen auf einem Datenträger gespeichert werden.
- ▶ Zur Verschlüsselung wird häufig SSL (Secure Socket Layer) eingesetzt. SSL hat den Vorteil, dass es in jedem Standard-Browser integriert ist und die Kunden keine weitere Software installieren müssen.
- ▶ Mit dem GNU Privacy Guard (GnuPG) und dem vom Bundesministerium für Wirtschaft und Technologie (BMWi) geförderten GNU Privacy Projekt (GnuPP) steht darüber hinaus eine freie Verschlüsselungssoftware zur Verfügung.

Sicherheitsmaßnahmen in Unternehmen

Keine „Monokulturen“

Unternehmens-Netzwerke sollten nicht an jeder Stelle mit derselben Standardsoftware ausgestattet sein: also keine „Monokulturen“, in der jeder einzelne Server und jeder PC von einem Virus befallen werden könnte. Dort, wo dennoch bekanntermaßen anfällige Software genutzt wird, sollten die bestehenden Sicherheitsmöglichkeiten aktiviert werden (s. Praxis & Technik, S.6).

Verbraucherfreundliche Technologien

Der Erfolg von E-Business-Unternehmen steht und fällt mit der Gewährleistung von Daten- und Verbraucherschutz. Daher sollten Internet-Händler ihre Internet-Angebote so gestalten, dass diese

Fortsetzung auf Seite 7

E-Business-ABC

ActiveX

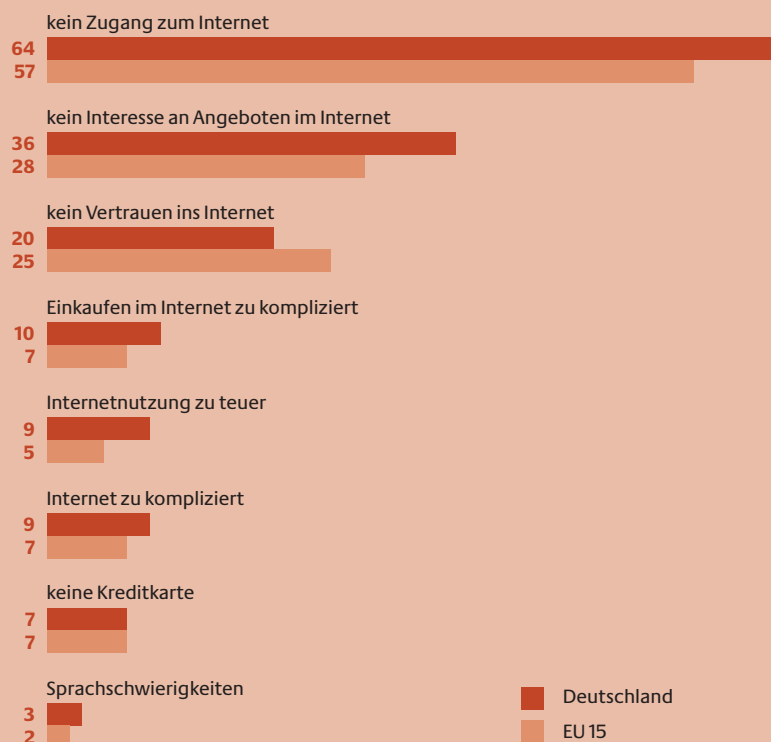
Mit Hilfe von ActiveX können interaktive Softwarekomponenten aus beliebigen Programmiersprachen in Webseiten eingebunden werden. Dadurch werden z. B. Multimedia-Effekte oder interaktive Objekte lebendig.

Browser

Software, mit deren Hilfe im Internet gesucht und Inhalte auf einem Monitor sichtbar gemacht werden können (z. B. Internet Explorer, Netscape-Navigator). Diese Browser können auch für die Nutzung von Multimedia-CDs verwendet werden.

Warum kaufen Sie nichts im Internet?

Antworten in %



Quelle: Eurobarometer 2004

Virenschutz und Browser-Sicherheits-Tipps

E-Business-ABC

Cache

Temporärer Zwischenspeicher auf der eigenen Festplatte, in dem Daten zu besuchten Webseiten abgelegt und griffbereit gehalten werden. Effekt: Wenn man eine vorher besuchte Webseite nochmals ansteuert, müssen die Originaldaten nicht nochmals vollständig vom Server der betreffenden Seite heruntergeladen werden.

Cookie

Hält die Zugriffe eines Nutzers auf bestimmte Internetseiten fest. Mit Hilfe dieser Protokolle lässt sich genau verfolgen, welche Vorlieben der betreffende Internetnutzer hat.

History

Die meisten Web-Browser speichern alle Internetadressen, die ein Benutzer besucht, intern in einer Liste ab. Mit Hilfe dieser Liste kann der Benutzer später bequem eine einmal besuchte Webseite wiederfinden und nutzen. Die Liste wird häufig „History“ oder „Verlauf“ genannt.

Java

Eine Programmiersprache, die zusammen mit einer Webseite übertragen und auf einem beliebigen Rechner (dessen Browser Java beherrscht bzw. zulässt) ausgeführt werden kann. Dadurch kann ein Anwender zu Hause Programme ausführen, die von einem fernen Rechner übertragen werden. Durch Java können Internetseiten multimedial und interaktiv gestaltet werden, z. B. durch Musik, Animationen, Videos.

Virenschutz-Tipps

Besonders anfällig sind die Mail-Programme „Microsoft Outlook“, „Outlook 2000“ und „Outlook Express“, die auf rund 90 Prozent aller Computer installiert sind. Die Standardeinstellungen dieser Programme weisen Sicherheitslücken auf, so dass Viren „freie Bahn“ auf Ihren Rechner haben. Einige wenige Änderungen schließen die gravierendsten Sicherheitslücken.

Outlook, Outlook 2000 und Outlook Express: Deaktivieren Sie das „Vorschauenfenster“ und die „Autovorschau“. Diese finden Sie in Outlook 2000 unter dem Menüpunkt „Ansicht“; in Outlook Express unter „Posteingang“ und „Ansicht“; in Outlook Express unter „Ansicht“ und „Layout“. Stellen Sie Outlook über den Menüpunkt „Optionen“ und „Sicherheit“ von „Internet-Zone“ auf „Zone für eingeschränkte Sites“ um.

- ▶ Menüpunkt „Extras“ anklicken, „Optionen“ auswählen
- ▶ Reiter „Sicherheit“ anklicken
- ▶ Sicherheitszone „Eingeschränkte Sites“ auswählen
- ▶ „O.K.“ anklicken

Damit diese Sicherheitszone wirklich eingeschränkt ist, sollten Sie in der Windows Systemsteuerung die Einstellungen des Punktes „Eingeschränkte Sites“ überprüfen.

Windows Systemsteuerung:

- ▶ „Einstellungen“ und dann „Systemsteuerung“ anklicken
- ▶ „Internetoptionen“ anklicken
- ▶ Reiter „Sicherheit“ auswählen
- ▶ „Eingeschränkte Sites“ auswählen
- ▶ „Stufe anpassen“
- ▶ Hier sollten Sie alle Punkte deaktivieren, vor allem „AktiveX-Steuererelemente...“ und „Scripting/Active Scripting“. Rollen Sie die gesamte Liste herunter, um alle Punkte zu kontrollieren. Java, JavaScript oder ActiveX haben in E-Mails nichts zu suchen
- ▶ Zum Abschluss nochmals „O.K.“ anklicken

Browser-Sicherheits-Tipps

Fast alle Internetnutzer arbeiten mit dem Internet Explorer (IE) als Browser. Dieser bietet zwar eine Reihe von Sicherheitseinstellungen, die aber in der Regel vom Nutzer erst selbst aktiviert werden müssen.

Aktuelle Ausgabe besorgen: Besorgen Sie sich immer die aktuelle Version des Internet Explorers (IE). Sie garantiert, dass Sicherheitslücken, die zwischenzeitlich bekannt geworden sind, beseitigt wurden.

Hohe Sicherheitsstufe einschalten: Unter Extras/Internetoptionen/Sicherheit/Standardstufe sollten Sie die Sicherheitsstufe „Mittel“ einstellen (ist in der Regel so voreingestellt).

Alle Vorgänge kontrollieren: Sie sollten ausschließen, dass Ihr Computer etwas tut, was Sie nicht wollen oder von dem Sie nichts wissen. Klicken Sie bei allen Optionen unter Sicherheitseinstellungen, bei denen es möglich ist, den Punkt „Eingabeaufforderung“ an.

Aktive Inhalte ausschließen: Aktive Inhalte (ActiveX) bergen ein beträchtliches Risiko und sollten generell nur auf Bestätigung des Benutzers geladen und gestartet werden. Schließen Sie die Gefahrenquelle daher weitgehend aus. Gehen Sie nur dann auf Seiten mit aktiven Inhalten, wenn es nicht zu vermeiden ist (z. B. Ihrer Bank). Diese Seiten sollten Sie in die Rubrik „vertrauenswürdige Sites“ aufnehmen. Allerdings schließen Sie so viele Seiten zum Surfen aus, die nicht ohne diese Scripts funktionieren. Also bei Bedarf wieder aktivieren und anschließend das Deaktivieren nicht vergessen.

- ▶ Wählen Sie dafür unter Extras/Internetoptionen/Sicherheit/Stufe anpassen bei sämtlichen aktiven Inhalten die Option „Eingabeaufforderung“
- ▶ Nicht sichere bzw. unsignierte ActiveX-Elemente deaktivieren

Java: Java ist im Vergleich zu ActiveX relativ sicher. Deshalb können Sie es bei der voreingestellten hohen Sicherheit belassen. Wer auf Nummer sicher gehen will, sollte Java deaktivieren.

Scripting: Scripting ermöglicht oft erst das Ausnutzen von Sicherheitslücken. Daher sollten Sie es deaktivieren. Dadurch gehen allerdings bei vielen Sites einige Funktionen verloren. Kompromiss:

- ▶ Deaktivieren Sie Active Scripting und nehmen Sie alle vertrauenswürdigen Sites, die Sie benötigen, in die Liste vertrauenswürdiger Sites auf
- ▶ Klicken Sie bei „Einfügeoperationen“ und „Java-Applets“ „Eingabeaufforderung“ an



Fortsetzung von Seite 5

sowohl möglichst wenig Risiken für die Benutzer beinhalten als auch einfach zu bedienen sind. Empfehlungen:

- ▶ E-Business-Nutzer sollten möglichst keine Cookies verwenden: Dateien also, die vom Internet-Browser automatisch angelegt werden und die dem Anbieter einer Homepage zur Wiedererkennung eines Online-Besuchers dienen. Wenn doch, sollten sie die Kunden über deren Inhalt und Zweck aufklären.
- ▶ E-Business-Anbieter sollten möglichst keine aktiven Inhalte auf Unternehmens-Seiten anbieten (z. B. Formulare oder Bilder in Java, JavaScript, ActiveX). Grund: Aktive Inhalte können auf verschiedene Weise Software enthalten, die Schäden verursachen oder Daten auf Kundenrechnern ausspionieren und Kunden „vergraulen“ kann.
- ▶ Jeder seriöse E-Business-Anbieter sollte für die Übermittlung aller personenbezogenen Daten die Möglichkeit anbieten, diese zu verschlüsseln.

Identifikation

Unternehmen sollten bei Bestellungen ihre Kunden einer Plausibilitätsprüfung unterziehen: Gibt es den Kunden überhaupt? Dies wäre wenig wahrscheinlich bei einem Kunden „Mickey Maus“. Stimmt die Adresse? Kaum möglich bei einer Adresse „Entenhausen“ etc. Im Zweifelsfalle: den Kunden anrufen.

Digitale Signatur

Nicht wenigen Online-Händlern ist eine fehlende rechtsverbindliche persönliche Unterschrift im Internet zum Problem geworden: angesichts etlicher Blindlieferungen und geplatzter Verkaufsverträge. Mit Hilfe der elektronischen Signatur nach dem Signaturgesetz ist es möglich, elektronische Dokumente (z. B. E-Mails) rechtsverbindlich zu unterschreiben.

Online-Nutzer, die die digitale Signatur nutzen wollen, erhalten von einer Zertifizierungsstelle einen verschlüsselten Unterschriften-Code auf einer besonders gesicherten Chip-Karte. Wollen sie nun elektronische Dokumente unterzeichnen, können sie sich über ein spezielles Kartenlesegerät am Computer einwählen, ausweisen und verschlüsselt unterschreiben.

Sicherheitsmanagement

IT-Sicherheit kann nicht ausschließlich mit technischen Sicherheitsmaßnahmen erreicht werden. Der Sicherheitsgedanke muss vielmehr alle Bereiche eines Unternehmens durchdringen: Rechte und Pflichten der Mitarbeiter, Zuständigkeiten, verbindliche Handlungsanweisungen, Diskretion etc. Hierzu gehört u. a. ein fundiertes IT-Sicherheitsmanagement, das für die sinnvolle Umsetzung und Erfolgskontrolle von IT-Sicherheitsmaßnahmen sorgt. In kleineren Betrieben reicht hier ein IT-Sicherheitsbeauftragter aus. In großen Unternehmen kümmert sich sinnvollerweise ein IT-Sicherheitsmanagement-Team um die vielfältigen Aufgaben zur Konzeption und Koordinierung der IT-Sicherheit.

Aufbau einer Sicherheitskultur

Um Sicherheitsschwachstellen auszuschließen, das Zusammenspiel aller Sicherheitsmaßnahmen zu garantieren und Fehler zu vermeiden, sollte jedes Unternehmen eine eigene IT-Sicherheitskultur schaffen. Deren Elemente sind:

- ▶ Vollständigkeit: Alle denkbaren Sicherheitseinstellungen für IT-Systeme werden eingerichtet und aktiviert.

E-Business-ABC

JavaScript

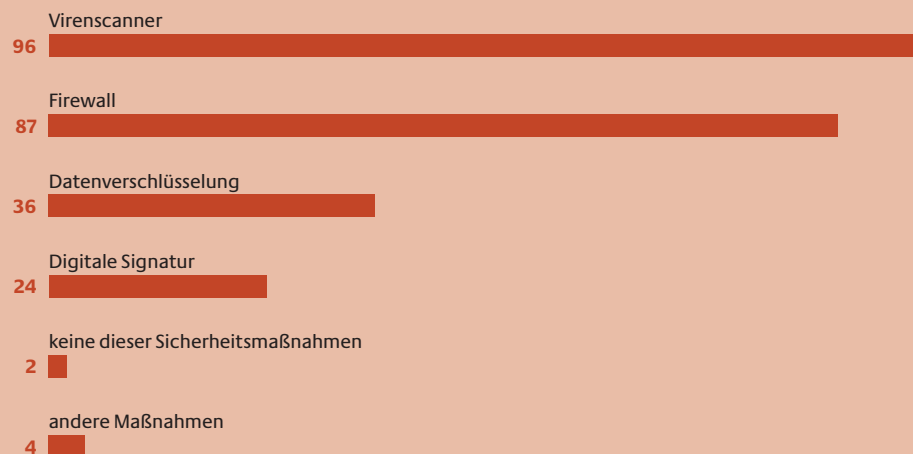
Eine Art „Mini-Programmiersprache“, mit der sich einfache Zusatzfunktionen auf Webseiten realisieren lassen. Der Code wird direkt in das HTML-Dokument geschrieben. Java-Script wird gerne mit Java verwechselt. Beide sind aber vollkommen verschieden.

SSL

Ein Protokoll, das verschlüsselte Kommunikation über das Internet erlaubt. SSL wird meist in der Kommunikation zwischen Web-Browsern und Servern verwendet.

Wie sichern Mittelständler die Datenkommunikation zu Kunden/Lieferanten ab?

in % der befragten Unternehmen (Mehrfachnennungen möglich)



Sicherheit im E-Business



Impressum

Herausgeber:

Bundesministerium für Wirtschaft und Technologie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
info@bmwi.bund.de
www.bmwi.de

Redaktion:

Bernd Geisen, Regine Hebestreit
PID Arbeiten für Wissenschaft und Öffentlichkeit GbR
Menzenberg 9, 53604 Bad Honnef
Tel.: 02224 90034-0, Fax: 02224 90034-1
info@pid-net.de

Mitarbeiter dieser Ausgabe:

Stefanie Teufel, Torsten Esser
www.impulse.de
Isabel Münch
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Rahmenlayout:

Atelier Hauer + Dörfler, Berlin

Produktion:

PRpetuum GmbH, München

Bildnachweis:

MEV, Photodisc

Druck:

Druckerei Thierbach,
Mülheim an der Ruhr

Auflage: 10.000

Schwerpunkt der nächsten Ausgabe:
„Rechtsfragen beim E-Business“

Wenn Sie dazu Fragen oder Anregungen haben oder Fragen zu anderen Themen der e-f@cts, wenden Sie sich bitte an:

Bernd Geisen, Regine Hebestreit
PID Arbeiten für Wissenschaft und Öffentlichkeit GbR

- ▶ **Erreichbarkeit:** Zutritt (in Räume), Zugang (zu PCs oder Netzwerken), Zugriff (auf bestimmte Daten) zu den IT-Systemen werden begrenzt.
- ▶ **Zuständigkeit:** Wer ist wofür verantwortlich?
- ▶ **Qualifikation:** Das Personal wird für IT-Sicherheitsbelange sensibilisiert und so geschult, dass es in seinen Aufgabenbereichen maximale Sicherheit umsetzen kann.
- ▶ **Regelmäßigkeit:** Alle wichtigen Daten werden regelmäßig und sorgfältig gesichert (vor Verlust, aber auch vor unbefugtem Zugriff).
- ▶ **Standardsicherung:** Es wird ein zuverlässiger Schutz vor Viren und Trojanischen Pferden aufgebaut.
- ▶ **Verschlüsselung:** Alle wichtigen Daten werden verschlüsselt und digital signiert.
- ▶ **Isolierung:** Jeder Netzanschluss wird gesichert (z. B. durch Firewalls, Intrusion Detection Systeme).
- ▶ **Weitsicht:** Auch die Telekommunikationssysteme werden in die Sicherheitsbetrachtungen mit einbezogen (z. B. Sicherung von Telefonanlagen gegen Abhören, Sicherung der Datenübertragung per Telefonleitung).
- ▶ **Notfallvorsorge:** Was tun im Fall von Datenverlust?
Achtung: Häufig ist zu beobachten, dass zwar viele organisatorische oder technische Sicherheitsverfahren vorhanden sind, diese jedoch durch den sorglosen Umgang mit der Technik wieder ausgehebelt werden.

Sicherheits-Informationen für Kunden

Ob ein Online-Shop erfolgreich ist oder nicht, hängt nicht zuletzt vom Vertrauen der Kunden ab: Wie seriös ist der unbekannte Geschäftspartner „am anderen Ende der Leitung“, dem man sein Geld anvertrauen soll? E-Business-Anbieter sollten ihre Kunden daher darüber aufklären,

- ▶ was das Unternehmen leistet, um den Kunden und seine Daten bestmöglichst zu schützen;
- ▶ welche Möglichkeiten ein Kunde hat, um sich selbst zu schützen.

Kunden-Info: Was tut das Unternehmen?

Insbesondere sollte den Konsumenten erklärt werden, in welchem Umfang und wofür Daten über sie erhoben werden und wie diese vor Missbrauch geschützt werden. Beispiele: Wie sind personenbezogene Daten im Unternehmen geschützt? Falls Cookies verwendet werden, sollte man den Kunden darüber informieren, welchem Zweck sie dienen sollen und wie lange die damit ermittelten Informationen gespeichert werden. Dies entspricht übrigens auch den Forderungen des Teledienststedatenschutzgesetzes (TDDSG). Hier heißt es (§3 Abs. 5), dass „der Nutzer vor der Erhebung über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten ist“.

Selbstverständlich sollte jedes E-Business-Unternehmen seinen Kunden ausdrücklich die Möglichkeit anbieten, sensible Daten wie Bestellungen oder Zahlungsanweisungen verschlüsselt zu übermitteln.

Kunden-Info: Was kann der Kunde tun?

Kunden sollten immer die Möglichkeit haben, Techniken oder Methoden auszuschließen, bei denen sie erfahrungsgemäß Sicherheitsbedenken haben. Beispiel: Viele animierte Demonstrationen auf Webseiten verlangen aktive Inhalte wie JavaScript. Anstatt sicherheitsbewusste Kunden zu dieser Form der Demonstration zu „zwingen“, sollte man sie darauf hinweisen, dass für eine Demonstration JavaScript im Browser eingeschaltet sein muss, aber diese auch ohne JavaScript als einfache Bilderfolge betrachtet werden kann.