

Address



http://www



Informationsbroschüre

Informationsbroschüre für Einsteiger

IT-Sicherheit: Themenfokus Website

www.ec-net.de
www.ecc-handel.de

Gefördert durch:



Bundesministerium
für Wirtschaft
und Technologie



Netzwerk Elektronischer
Geschäftsverkehr

aufgrund eines Beschlusses
des Deutschen Bundestages

Herausgeber

E-Commerce-Center Handel, Köln



E-Commerce-Center Handel

Text und Redaktion

Sonja Rodenkirchen,
ECC Handel –
E-Commerce-Center Handel, Köln

Andreas Duscha,
ECC Handel, Köln

Judith Halbach,
ECC Handel, Köln

**Grafische Konzeption
und Gestaltung**

Christian Bähr,
ECC Handel, Köln

Bildquelle

www.fotolia.de

Stand

Oktober 2010

Inhalt

1	Einleitung: Die Relevanz einer sicheren Website	04
2	Wussten Sie schon, dass	05
3	Sichere Übertragung von Daten und Zahlen im Internet	06
4	Datenschutz und Datensicherung	08
5	Weitere rechtliche Aspekte der Website-Gestaltung ...	12
6	Fazit	13
7	Quellen	14
8	Weiterführende Informationen	14
9	Sichere E-Geschäftsprozesse in KMU und Handwerk...	15



Die Relevanz einer sicheren Website



@ http://www

Einleitung

Über 90% der im Rahmen der Studie „Netz- und Informationssicherheit in Unternehmen 2009“ befragten 490 Unternehmen verfügen über eine Website. Mehr als 25% davon betreiben einen eigenen Online-Shop, mit dem sie nennenswerte Umsätze realisieren. Diese Zahlen machen deutlich, wie hoch die Bedeutung der eigenen Internetpräsenz für Unternehmen heutzutage ist. Doch der Umgang mit dem Internet birgt auch zahlreiche Gefahren. Das Unternehmen muss sich mit rechtlichen Themen auseinandersetzen, es muss Gesetze zum Datenschutz

beachten und vor allem für eine sichere Übertragung von Kundendaten und Zahlungen sorgen. Denn insbesondere der Sicherheitsaspekt ist aus Kundensicht ein entscheidender Faktor – ist sich der Kunde bei einer Online-Bestellung nicht sicher, dass seine Zahlung auch tatsächlich beim Empfänger ankommt oder seine Daten sicher übertragen werden, ist die Wahrscheinlichkeit sehr hoch, dass er den Kauf abbricht. Die sichere Website-Gestaltung nimmt somit aus rechtlicher Hinsicht, aber auch aus Kundenakquisitions- und Kundenbindungssicht einen hohen Stellenwert ein.

Wussten Sie schon, dass...

- ▶ ... 50 % der Unternehmen kein umfassendes Datensicherheitskonzept umgesetzt haben?
- ▶ ... jedes zehnte Unternehmen bereits Opfer eines erfolgreichen Angriffs auf die eigene Internetpräsenz wurde?
- ▶ ... 20 % der Betreiber von Online-Shops Daten nicht verschlüsselt übertragen?
- ▶ ... 50 % der Unternehmen ihren Online-Shop nicht haben zertifizieren lassen?
- ▶ ... beim nachlässigen Umgang mit Kundendaten eine Haftstrafe von bis zu zwei Jahren drohen kann?

Sichere Übertragung von Daten und Zahlungen im Internet

Bei vielen Kunden und auch Website-Betreibern ist die Angst vor Datenmissbrauch im Internet hoch. Sensible und persönliche Daten, wie die Konto- und Kreditkartennummer, müssen besonders geschützt werden. Der verschlüsselten Übertragung dieser Daten kommt daher insbesondere in Online-Shops eine große Bedeutung zu. Verschlüsselungsprotokolle oder Dienstleister im Bereich der Zahlungsverfahren bieten hierzu verschiedene Lösungen an, deren Gebühren von einer kostenlosen Open-Source-Software bis hin zu umsatzbasierten oder transaktionsabhängigen Provisionsmodellen reichen.

Transport Layer Security (TLS)

Das gängigste Verfahren zur Verschlüsselung von Daten ist Transport Layer Security (TLS). Es ist besser bekannt unter seinem Vorgängernamen Secure Sockets Layer (SSL). Bei TLS handelt es sich um ein Verschlüsselungsprotokoll zur sicheren Übertragung von Daten im Internet. Der große Vorteil von TLS ist, dass es in jedem Standard-Browser, wie bspw. Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome, integriert ist und Kunden daher keine weitere Software installieren müssen. Aufgrund des Verschlüsselungsvorgangs können Außenstehende den Inhalt weder lesen noch verändern. Internet-Seiten, die mit dem TLS-Ver-

fahren arbeiten, erkennt man daran, dass die URL mit https:// anstatt mit http:// beginnt. Außerdem wird in allen gängigen Browsern ein verriegeltes Schloss-Symbol in der unteren Leiste angezeigt. Für die Übertragung der verschlüsselten Informationen sind sogenannte digitale Zertifikate notwendig, die die Identität des Website-Betreibers feststellen, um zu verhindern, dass eine gesicherte Verbindung zu einem Anbieter aufgebaut wird, der sich als jemand anderer ausgibt. Erst die finale Prüfung des Zertifikates gewährleistet eine sichere Übertragung von Daten. Um die Zuverlässigkeit und Integrität dieser Zertifikate im Rechtsverkehr sicherzustellen, unterliegen die Aussteller der Zertifikate der Aufsicht der Bundesnetzagentur. Auf den Seiten der Bundesnetzagentur findet sich eine Liste der Zertifikataussteller, darunter beispielsweise VeriSign oder TC TrustCenter.





Extended-Validation-SSL (EV-SSL)

Seit einiger Zeit nutzen immer mehr Webseitenbetreiber Extended-Validation-SSL-Zertifikate (EV-SSL), also „Zertifikate mit erweiterter Überprüfung“. Diese sollen Internetnutzern ermöglichen, noch schneller zu erkennen, ob sie sich auf vertrauenswürdigen Seiten befinden und sie so besser vor Phishing-Versuchen schützen. Denn auch Betrüger haben es aufgrund einer teilweise zu lockeren Vergabe von SSL-Zertifikatengeschafft, sich eine angeblich sichere Verbindung zu erschleichen. Bei EV-SSL-Zertifikaten wird daher in der Adresszeile des Browsers zusätzlich ein Feld angezeigt, in dem Zertifikats-

und Domaininhaber im Wechsel mit der Zertifizierungsstelle eingeblendet werden. Des Weiteren wird je nach verwendetem Browser die Adresszeile (teilweise) grün eingefärbt. Um die größere Sicherheit zu gewährleisten, ist die Ausgabe an strengere Vergabekriterien gebunden. Dies bezieht sich vor allem auf eine detaillierte Überprüfung des Antragstellers, wie bspw. ein Rückruf durch die Zertifizierungsstelle zur Feststellung der Identität und der Geschäftsadresse. Kunden von EV-SSL sind beispielsweise eBay oder der Zahlungsdienst PayPal.



Zahlungsverfahren im Überblick

Grundsätzlich minimiert der Einsatz verschiedener Zahlungsverfahren das Risiko eines Kaufabbruchs. Bei der Einführung neuer Zahlungsverfahren sollten jedoch immer Chancen und Risiken abgewogen werden – da sich die Zahlungsverfahren hinsichtlich ihrer Sicherheit und Kosten unterscheiden. In die Vollkostenanalyse mit einbezogen werden sollten Paymentkosten, Kosten für Personal, Mahnwesen, Forderungsausfall, verzögerte Geschäftsprozesse, Lagerhaltung und Retourenmanagement.

Die Zahlungsverfahren werden in drei Kategorien eingeteilt. Klassisches E-Payment: Überführung von Offline-Payment hin zu Online-Payment, z. B. Nachnahme, Rechnung, Vorkasse, Kreditkarte, Lastschrift. Modernes E-Payment: Paymentlösungen, die speziell für den Online-Handel etabliert wurden, z. B. Direktüberweisungsverfahren (Sofortüberweisung.de, Giropay), E-Mail-Verfahren oder E-Wallets (PayPal, ClickandBuy). Mobile Payment (M-Payment): Bezahlverfahren speziell für Mobiltelefone.

Datenschutz und Datensicherung

Von Kunden erhobene Daten müssen im Unternehmen vor Missbrauch geschützt (Datenschutz) und besonders gesichert (Datensicherung) werden. Wird dies nicht beachtet, können nicht nur ein Imageverlust und die Abwanderung von Kunden, sondern auch Geldbußen sowie Haftstrafen von bis zu zwei Jahren drohen. Unternehmen sind daher gut beraten, sich mit den relevanten Gesetzen in diesem Bereich, wie beispielsweise dem Bundesdatenschutzgesetz und dem Telemediengesetz, ausführlich auseinander zu setzen.

Von den 490 Unternehmen, die im Rahmen der jährlich durch das NEG durchgeführten Studie „Netz- und Informationssicherheit in Unternehmen 2009“ befragt wurden, gaben jedoch nur 50 % an, über ein umfassendes Datensicherheitskonzept zu verfügen. Des Weiteren hatten ebenfalls nur 50 % ihren Shop mit einem Gütesiegel wie beispielsweise Trusted Shops zertifizieren lassen. Auf der folgenden Seite finden Sie einige Hinweise und Tipps zum Thema Datensicherung und Datenschutz.

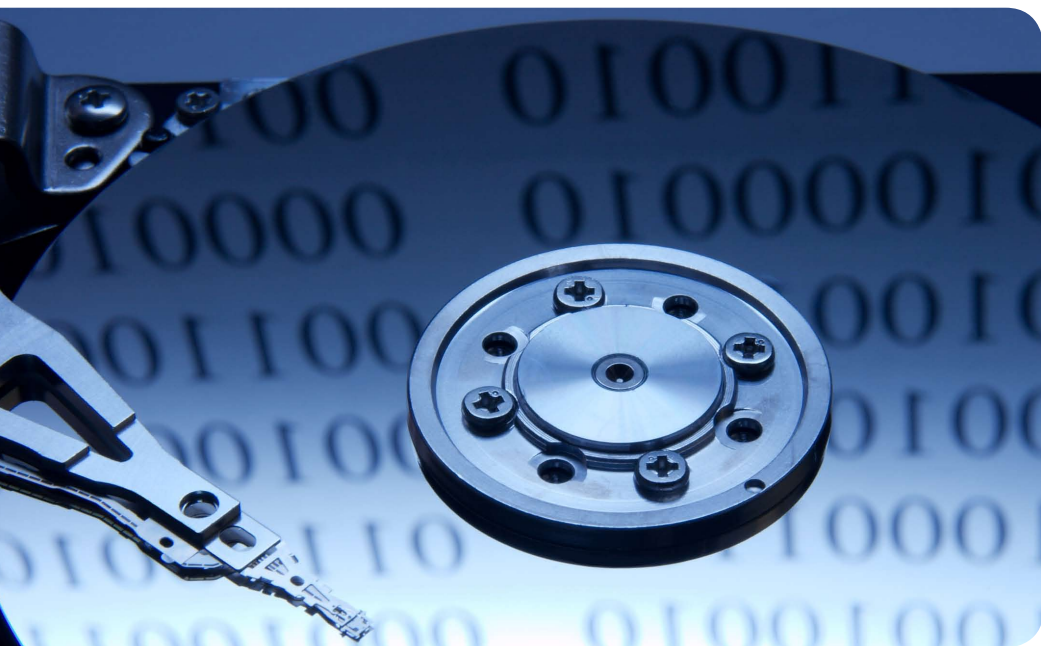


Was ist erlaubt?

- ▶ Grundsätzlich erlaubt ist die **Speicherung von sogenannten Bestandsdaten**, d. h. Unternehmen dürfen die Kundenadressen und Angaben, die zur Abwicklung des Bestellverhältnisses notwendig sind, speichern.
- ▶ Die **Verwendung von Kundenadressen zu Marktforschungszwecken, zur Werbung und für personalisierte Marketing-Maßnahmen** ist nur dann erlaubt, wenn sie durch eine explizite Einwilligung des Kunden (z. B. über das Anklicken eines Kästchens) autorisiert wurden.

Wo sollen die Daten gespeichert werden?

- ▶ Daten sollten auf separaten Rechnern gespeichert werden, die vom Internet abgekoppelt sind und damit besser vor Hackern geschützt werden können.
- ▶ Bandlaufwerke oder externen Festplatten sollten als zusätzliche Sicherungskopie eingesetzt werden.
- ▶ Doch auch bei der Speicherung von Kundennamen und Kontoprofilen auf Notebooks, Smartphones, mobilen Datenträgern und Papier müssen die Daten geschützt werden: Nicht nur das Internet kann Datenlecks verursachen.



Tipps zum Datenschutz

- ▶ **Stellen Sie hohe Anforderungen an Kunden-Passwörter:** Lassen Sie Ihre Kunden Passwörter bilden, die Groß- und Kleinbuchstaben, Sonderzeichen sowie Zahlen sinnfrei zusammensetzen und länger als 8 Stellen sind. So vermeiden Sie, dass Kundenkonten leicht gehackt werden können.
- ▶ **Speichern Sie personenbezogene und nicht personenbezogene Daten in separaten Datenvorhaltungssystemen:** Falls vom Nutzer nicht anders gestattet, dürfen personenbezogene Kundendaten nur zur Erfüllung und Verwaltung eines Vertragsverhältnisses, wie die Abwicklung des Einkaufsvorgangs, gespeichert und genutzt werden. Nicht personenbezogene Daten dürfen in aggregierter Form auch für andere Zwecke, wie Marktforschung, verwendet werden.
- ▶ **Benennen Sie einen konkreten Ansprechpartner in Datenschutzfragen für Ihre Kunden:** Dieser Datenschutzbeauftragte kann zeitnah auf Fragen und Bedenken von Kunden reagieren.
- ▶ **Lassen Sie Ihre Website und Ihren Shop zertifizieren:** Berater und Zertifizierungsstellen entdecken Sicherheitslücken oft früher als die eigenen Leute. Auch externe IT-Dienstleister wie Callcenter, Zahlungsabwickler oder Hostingpartner, die Zugriff auf Kundendaten erhalten, sollten vor Vertragsschluss durch Sachverständige überprüft werden.
- ▶ **Schaffen Sie klare Regeln für die Zugriffsrechte auf Daten:** Das gilt für digitale Speichermedien gleichermaßen wie für Aktenordner. Diese Regeln müssen dokumentiert und eingehalten werden.

Weitere rechtliche Aspekte der Website-Gestaltung

Die zentrale Vorschrift im Internetrecht ist das Telemediengesetz, das umgangssprachlich daher auch „Internetgesetz“ genannt wird. Es legt beispielsweise fest, welche Angaben in einem Impressum zu finden sein müssen – je nach Rechtsform und Art des Anbieters sind unterschiedliche Angaben erforderlich. Außerdem werden zum Beispiel die Haftung für Internetseiten mit gesetzwidrigen Inhalten oder der Datenschutz beim Betrieb von Internetseiten und zur Herausgabe von Daten geregelt. Häufige Verstöße gegen das Telemediengesetz betreffen z. B. das Impressum, das Urheberrecht,

Links auf rechtswidrige Seiten oder die nicht autorisierte Verwendung von Marken und Logos. Jeder Internetseitenbetreiber muss sich daher mit diesem und weiteren Gesetzen auseinandersetzen und dazu im besten Fall auch rechtliche Beratung in Anspruch nehmen, um nicht in die Gefahr zu kommen, hohe Strafen zahlen zu müssen.





Fazit

Die sichere Gestaltung von Websites bezieht sich sowohl auf die Sicherheit der Datenübertragung und -speicherung als auch auf die Beachtung von rechtlichen Vorschriften. Da auf diesen Gebieten viele unterschiedliche Gefahren lauern, ist es für Unternehmen essentiell, sich mit den Themen auseinander zu setzen, Verantwortliche zu bestimmen, Konzepte zu erstellen und möglicherweise recht-

liche Beratung in Anspruch zu nehmen sowie ihre Seiten zertifizieren zu lassen. So gerüstet können Unternehmen und Kunden mit einem guten Gefühl im Internet in den Austausch treten.



Quellen

- ▶ Bundesnetzagentur 2010, [http://www.bundesnetzagentur.de/cln_1912/DE/Sachgebiete/QES/QES_node.html]
- ▶ Bundesverband Digitale Wirtschaft (BVDW) e.V., Online-Payment und Forderungsmanagement, 23.09.2010,
- ▶ Customer Relationship Management Portal (2007 erstellt, 2010 abgerufen), [http://www.crmmanager.de/magazin/artikel_1722_kunden-daten_datenschutz.html]
- ▶ Netz- und Informationssicherheit in Unternehmen 2009, [http://www.ecc-handel.de/netz_und_informationssicherheit_in_unternehmen.php]
- ▶ ECC Handel (2007 erstellt, 2010 abgerufen), [http://www.ecc-handel.de/datenschutz_1932301.php]
- ▶ Financial Times Deutschland, 2010. [<http://www.ftd.de/karriere-management/management/:sicherheit-im-unternehmen-ab-in-die-tonne-mit-kundendaten/50147362.html>]

Weiterführende Informationen

- ▶ <http://www.ec-net.de/sicherheit>, Online-Portal des Netzwerks Elektronischer Geschäftsverkehr
- ▶ <http://www.bit.ly/it-sicherheit>, Themenspezifische Informationen des Verbundsprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“
- ▶ http://www.gesetze-im-internet.de/bdsg_1990, Bundesdatenschutzgesetz
- ▶ <http://www.gesetze-im-internet.de/tmg>, Telemediengesetz

Das Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“

Das Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Das Gesamtprojekt setzt sich neben dieser und zwei weiteren Einsteigerbroschüren insbesondere aus den nachfolgenden Tätigkeiten zusammen:

- ▶ Unter der Überschrift „Stammtische IT-Sicherheit“ wird eine Reihe regionaler „Unternehmerstammtische“ bundesweit etabliert. Die kostenfreien Stammtische sind ein Forum für Dialog und Information und bilden eine Plattform für den Austausch von Unternehmern untereinander.

- ▶ Die jährlich veröffentlichte Studie „Netz- und Informationssicherheit in Unternehmen“ zeigt auf, wie es um die Informationssicherheit in Unternehmen bestellt ist und wie leicht unternehmensfremde Personen an Geschäftsdaten kommen können. Die kompletten Berichtsbände finden Sie zum kostenlosen Download unter: <http://www.bit.ly/it-sicherheit>
- ▶ Kostenfreie IT-Sicherheitsratgeber bieten insbesondere KMU neutrale und praxisnahe Hinweise und Tipps, wo Sicherheitslücken bestehen und wie mit ihnen umgegangen werden sollte. Themenschwerpunkte sind u. a. „Basischutz für den PC“, „Sicheres Speichern und Löschen von Daten“, uvm. Download unter: <http://www.it-sicherheit.de>
- ▶ Aktuelle und neutrale Informationen zur Informationssicherheit werden Ihnen im Internet auf der Informationsplattform des NEG unter der Rubrik „Netz- und Informationssicherheit“ angeboten: <http://www.ec-net.de/sicherheit>



Fachhochschule Gelsenkirchen

Sebastian Spooen



ECC
E-Commerce Center Basal

Andreas Duscha



m/e/c/k
Sicherheit im Internet

Andreas Gabriel



Ekkehard Dierich



SAGeG
Kompetenzzentrum
Elektronischer Geschäftsverkehr
Dagmar Lange
(Konsortialführung)

Das Netzwerk Elektronischer Geschäftsverkehr

– E-Business für Mittelstand und Handwerk

Das Netzwerk Elektronischer Geschäftsverkehr (NEG) ist eine Förderinitiative des Bundesministeriums für Wirtschaft und Technologie. Seit 1998 unterstützt es kleine und mittlere Unternehmen bei der Einführung und Nutzung von E-Business-Lösungen.

Beratung vor Ort

Mit seinen 29 bundesweit verteilten Kompetenzzentren informiert das NEG kostenlos, neutral und praxisorientiert – auch vor Ort im Unternehmen. Es unterstützt Mittelstand und Handwerk durch Beratungen, Informationsveranstaltungen und Publikationen für die Praxis.

Das Netzwerk bietet vertiefende Informationen zu Kundenbeziehung und Marketing, Netz- und Informationssicherheit, Kaufmännischer Software und RFID sowie E-Billing. Das Projekt Femme digitale fördert zudem die IT-Kompetenz von Frauen im Handwerk. Der NEG Website Award zeichnet jedes Jahr herausragende Internetauftritte von kleinen und mittleren Unternehmen aus. Informationen zu Nutzung und Interesse an E-Business-Lösungen in Mittelstand und Handwerk bietet die jährliche Studie „Elektronischer Geschäftsverkehr in Mittelstand und Handwerk“.

Das Netzwerk im Internet

Auf www.ec-net.de können Unternehmen neben Veranstaltungsterminen und den Ansprechpartnern in Ihrer Region auch alle Publikationen des NEG einsehen: Handlungsleitfäden, Checklisten, Studien und Praxisbeispiele geben Hilfen für die eigene Umsetzung von E-Business-Lösungen.

Fragen zum Netzwerk und dessen Angeboten beantwortet Markus Ermert, Projektträger im DLR unter 0228/3821-713 oder per E-Mail: markus.ermert@dlr.de.



Netzwerk Elektronischer
Geschäftsverkehr

