IT-Sicherheitstipp: Webseiten sicher betreiben

Einer aktuellen Studie des *Bundesministeriums für Wirtschaft und Technologie* (BMWi) in Zusammenarbeit mit dem *Netzwerk Elektronischer Geschäftsverkehr* (NEG) zu Folge sind knapp 93 Prozent aller kleinen und mittelständischen Unternehmen mit einer eigenen Website im Internet vertreten (Stand: 05/2011). Der überwiegende Anteil von 78 Prozent hat den Internetauftritt in Form einer kompakten Unternehmensdarstellung realisiert. Rund 14 Prozent der Befragten Unternehmen geben an, auf ihrer Website auch einen Online-Shop zu betreiben [1]. Die Handhabung von Benutzereingaben und die sichere Übertragung und Verwaltung sensibler Kundendaten erfordert eine besondere Beachtung von Sicherheitsvorkehrungen bei dem Betrieb von Webseiten. Öffentlich bekannte Fälle, wie Diebstähle von mehreren hunderttausend Kundendatensätzen, bis individuelle Schäden durch kompromittierte Online-Shops geben negative Beispiele dafür, dass der Sicherheit von Webseiten häufig nicht die Bedeutung beigemessen wird, die erforderlich ist.

Wählen Sie einen passenden und vertrauenswürdigen Anbieter aus

Webseiten repräsentieren das Unternehmen nach außen und sorgen häufig für den ersten Eindruck bei potentiellen Kunden. Besonders für solche Unternehmen, die keine eigene IT-Abteilung haben, ist es ratsam, ihre Webseiten an einen professionellen Dienstleister auszulagern. Für kleine Unternehmen bringt es viele Vorteile mit sich, wenn der Anbieter in der Nähe ist. Vertrauen Sie bei der Wahl eines Anbieters auch auf Empfehlungen aus Ihrem Umfeld.

Sofern Ihre Internetseite keine reine Visitenkarte ist, sondern dort auch unternehmensinterne Informationen oder Kundendaten hinterlegt werden sollen, empfiehlt es sich, ein professionelles Unternehmen mit der Erstellung zu beauftragen. **Ein Webdienstleister mit Erfahrungen im Bereich der IT-Sicherheit kann Sie optimal dabei unterstützen, beispielsweise einen geschützten Bereich innerhalb Ihrer Internetseite aufzubauen und so sensible Informationen wie Kundendaten oder Händlerpreislisten sicher zu verwalten.** Größere Webseiten werden üblicherweise mit Inhaltsverwaltungssystemen (engl.: *Content Management System*, kurz: CMS) realisiert. Ein CMS ermöglicht es auch Laien ohne Programmierkenntnisse, Internetseiten und Ihre Inhalte komfortabel anzulegen und zu bearbeiten ohne

bei jeder Änderung auf den Webdienstleister angewiesen zu sein. Darüber hinaus bietet ein CMS noch viele weitere Vorteile, die aber nicht Schwerpunkt dieses Tipps sein sollen.

Vor der Entscheidung für einen Anbieter sollten Sie die Sicherheitsvorkehrungen des Anbieters prüfen. Informieren Sie sich über die Art der Dokumentation und Versionsverwaltung, die der Anbieter einsetzt. **Die Dokumentation der IT-Infrastruktur ist die Basis für eine Absicherung Ihres Systems, ebenso wie der Einsatz einer Versionsverwaltung.** In einem Notfall hat der Anbieter dadurch die Gelegenheit, schnell zum letzten lauffähigen und integren Stand zurückzuspringen. Unter die Dokumentation fällt die Konfiguration aller Systemkomponenten, die Art der Vernetzung und die wichtigsten Kontaktdaten von Dienstleistern. Insbesondere wenn Cyberkriminelle den Webauftritt kompromittiert haben, ist es außerordentlich wichtig, mit Hilfe der Versionsverwaltung nachvollziehen zu können, welcher Stand integer ist und diesen wiederherzustellen.

Sensibilisieren Sie Ihre Mitarbeiter

Sensibilisieren Sie Ihre Mitarbeiter speziell für IT- und Informationssicherheit im Umgang mit Webseiten, sofern diese selbständig Inhalte einpflegen oder modifizieren. Bearbeitungsrechte für Mitarbeiter bergen ein Sicherheitsrisiko, da jeder Zugang ein Einfallstor für Angreifer bieten kann, sofern Sicherheitsvorschriften nicht beachtet werden. Eine aktuelle Befragung des Netzwerk Elektronischer Geschäftsverkehr zeigt, dass die Betreuung der Website in jedem achten befragten Unternehmen von Personen ohne sicherheitsspezifische Kenntnisse durchgeführt wird. Ein Drittel der befragten Unternehmen hat bereits einen Angriff auf die eigenen Webseiten oder das eigene Netzwerk erlitten, wobei die Ursache bei nahezu jedem fünften Fall im eigenen Unternehmen lag – beispielsweise durch einen unbedachten Umgang mit Passwörtern [1]. Vergeben Sie daher die Benutzerrechte für die Website mit Bedacht und aktualisieren Sie diese stets, nachdem ein personeller Wechsel stattgefunden hat. **Eine besondere Gefahr besteht durch die nachlässige Vergabe von Administratorrechten. Nur Mitarbeiter, die Systemverantwortung haben, sollten diese umfassenden Rechte erhalten.**

Schulen Sie alle Mitarbeiter in IT- und Informationssicherheit, um ein hohes Sicherheitsniveau zu erreichen. Durch Schulungen kann eine gute Akzeptanz eingeführter Sicherheitsrichtlinien erzielt werden. Unternehmensweite Richtlinien sollten beispielsweise für Passwörter festgelegt werden. Hilfreiche Informationen dazu erhalten Sie in den IT-Sicherheitstipps „*Passwort sicher erstellen*“ und „*Beschäftigte für IT-Sicherheit sensibilisieren*“ [2] Grundsätzlich sollte bei jedem Dienst ein anderes Passwort verwendet werden. Ermutigen Sie Ihre Beschäftigten, einen Passwortmanager zu nutzen, um eine Vielzahl starker Passwörter sicher zu verwalten.

Für die inhaltliche Gestaltung von Webseiten ist die Beachtung von rechtlichen Vorschriften maßgeblich. **Für jeden Betreiber einer Internetseite ist es von großer Bedeutung, sich mit den gesetzlichen Bestimmungen auseinanderzusetzen.** Weiterführende Informationen, beispielsweise zur Impressumspflicht und dem Umgang mit personenbezogenen Daten liefert Ihnen die

NEG-Informationsbroschüre *„IT-Sicherheit: Themenfokus Website“* [1].

Sichern Sie die technische Betreuung Ihrer Website ab

Stellen Sie sicher, dass Datensicherungen (engl.: Backups) der kompletten Website regelmäßig und bestenfalls automatisiert ausgeführt werden und dass diese Datensicherungen brauchbar sind. Wie eine aktuelle Befragung des Netzwerk Elektronischer Geschäftsverkehr ergeben hat, hat weniger als die Hälfte der befragten Unternehmen die vollständige Wiederherstellung von Daten schon einmal geprüft [1]. Ein großer Anteil von Unternehmen läuft damit Gefahr , bei einem Systemausfall wichtige Daten endgültig zu verlieren. **Darüber hinaus sollten die Datensicherungen in verschlüsselter Form vorgehalten werden, damit kein Missbrauch durch Dritte möglich ist.** Idealerweise sollte zur Verschlüsselung das Public-Key-Verfahren Verwendung finden, ohne den privaten Schlüssel auf dem Webserver vorzuhalten, sodass auf dem System zwar automatisiert verschlüsselt, aber nicht entschlüsselt werden kann.

Halten Sie vertraglich fest, dass Sicherheitsupdates für Web-Dienste und Module zeitnah eingespielt werden. Hierunter fallen sowohl Systemupdates wie zum Beispiel der Webserver als auch Sicherheitsupdates für das CMS und Erweiterungsmodule. Tragen Sie Sorge dafür, dass die Logfiles des Servers regelmäßig überprüft werden, damit Unregelmäßigkeiten, die auf Angriffsversuche hinweisen könnten, frühzeitig erkannt werden.

Sorgen Sie für eine sichere Datenübertragung und -speicherung mittels geeigneter Verschlüsselungstechniken, wenn sensible Daten auf der Website eingegeben werden. Jedes achte in der Studie zur Netz- und Informationssicherheit 2011 befragte Unternehmen betreibt einen Online-Shop ohne den Einsatz einer Verschlüsselung und läuft damit Gefahr, dass Kundendaten von Dritten missbräuchlich verwendet werden [1]. Für die sichere Übertragung von Daten eignet sich das Verfahren *Secure Sockets Layer,* kurz SSL. Stellen Sie bei der Datenspeicherung sicher, dass die Benutzerpasswörter ausschließlich nach aktuellen Standards als sogenannte Hashsummen in der Datenbank hinterlegt werden und niemals solche im Klartext.

Sichern Sie Ihre Webseiten durch regelmäßige Kontrollen ab

Bereits bevor es zur Realisierung der Webseiten durch einen Dienstleister kommt, sollte sichergestellt sein, dass die Sicherheitsansprüche des Auftraggebers voll erfüllt sind. Aktuelle Erfahrungen des Instituts für Internet-Sicherheit zeigen, dass die Entwicklung und der Betrieb von Webseiten bei Dienstleistern mit wenig Kenntnis im Bereich IT-Sicherheit eine Gefahr von Sicherheitsproblemen birgt. Bei der Beauftragung einer Internetseite sind häufig Design und Kostenfaktoren maßgeblich. Der Stellenwert IT-Sicherheit ist oftmals sowohl Auftragnehmer als auch Auftraggeber nicht bewusst. Sicherheit ist häufig nicht auf den ersten Blick sichtbar, doch macht sich langfristig bezahlt.

Sofern auf Ihren Webseiten sensible Kundendaten, wie Kreditkartennummern von Kunden gespeichert sind, sollten Sie die Sicherheit Ihres Systems (mittels sogenannter Web Penetration Tests) regelmäßig von einem unabhängigen Dienstleister in puncto IT-Sicherheit kontrollieren lassen. Besonders Eingabemöglichkeiten wie Formulare sollten auf sicherheitskritische Funktionalitäten geprüft werden. Sind Formularfelder nicht sicher programmiert, kann durch Angriffsmethoden, wie sogenannte *SQL-Injections* oder *Cross-Site-Scripting*, das Einschleusen von schädlichem Code möglich sein. Anbieter für Sicherheitstests bei Webseiten (engl. *Web Penetration Tester*), wie z.B. IT-Sicherheitsexperten am Institut für Internet-Sicherheit, decken vorhandene Sicherheitslücken auf und geben Ihnen Empfehlungen für die Behebung dieser. **Nach der Beseitigung der sicherheitskritischen Funktionen sollte auf Ihren Webseiten in Form eines Zertifikats dargestellt werden, dass die Webseiten von einem unabhängigen Anbieter geprüft und für sicher empfunden wurde.** Erneuern Sie die Sicherheitstests regelmäßig. Als Faustregel gilt, dass jede neue Anwendung mit Benutzerinteraktion auf Ihren Webseiten vor der Freischaltung auf Sicherheitslücken getestet werden sollte.

Tipps für Betreiber eines eigenen Webservers

Der Betrieb eines eigenen Webservers ist für ein Unternehmen dann sinnvoll, wenn es das Hauptgeschäft erfordert, sehr viele verschiedene Online-Dienste oder Online-Schnittstellen anzubieten. **Die technische Betreuung eines Webservers erfordert entsprechendes Detailwissen und Zeit für die professionelle Verwaltung der Systeme.**

Generell sollten Sie bedenken, dass Sie für die Sicherheit Ihrer Server verantwortlich sind. Mieter und Betreiber von Servern sind voll haftbar, wenn ein Server angegriffen, gehackt und womöglich für kriminelle Machenschaften missbraucht wird. **Um das Angriffspotential deutlich zu minimieren, sollten Sie für alle Systemkomponenten und Dienste, wie beispielsweise dem Datenbanksystem, regelmäßig Sicherheitsupdates einspielen. Außerdem empfiehlt es sich regelmäßig Datensicherungen durchzuführen und sich mit dem Thema Datenschutz auseinander zu setzen.** Eine Firewall für Webserver ist grundsätzlich empfehlenswert. In die Entscheidung für eine passende Lösung spielen viele Faktoren mit ein, weshalb Sie sich an einen professionellen Dienstleister wenden sollten. Beachten Sie den Grundsatz, dass auf dem Webserver keine anderen Dienste mit sensiblen Daten installiert sein sollten. Vergeben Sie Passwörter für die Verwaltung der Dienste nicht mehrfach und achten Sie stets auf sichere Passwörter.

Ein Webserver, der nicht nach aktuellen Standards geschützt ist, bietet an vielen Stellen Angriffsflächen. Treffen Sie daher bewusst Vorkehrungen, um das System zu härten und Einfallstore für Angreifer zu schließen. Ein Beispiel für ein offenes Tor ist die standardmäßige Anzeigen der Verzeichnislistung, die es Angreifern leicht ermöglicht, vermeintlich versteckte Dateien aufzufinden. **Unterbinden Sie daher die Verzeichnislistung und richten Sie einen Verzeichnisschutz ein.** Einen einfachen, aber wirkungsvollen Verzeichnisschutz können Sie beispielsweise erzielen, indem Sie Verzeichnisse mit einem Passwortschutz versehen. So erhalten Nutzer nur Zugriff auf

die Bereiche der Website, die für sie bestimmt sind. Außerdem ist es ratsam, an einen Webserver gerichtete Anfragen mittels einer geeigneten Software umzuschreiben. Eine solche Funktion ist bei jedem Webserver möglich, bei *Apache*-Webservern beispielsweise durch das Modul *„mod_rewrite“*.

Bei der Freigabe von Diensten auf Webservern gilt der Leitsatz „So viel wie nötig - so wenig wie möglich“. Schaffen Sie eine starke Absicherung von Schnittstellen zum System. Stellen Sie nur die Dienste nach außen bereit, die auch wirklich benötigt werden. Das sind beispielsweise die Protokolle *„HTTP“*,*„HTTPS“* und *„SSH“*. *„SSH“*, kurz für *„Secure Shell“*, bietet die Möglichkeit, über eine verschlüsselte Netzwerkverbindung mit dem Webserver zu kommunizieren und liefert damit eine sichere Alternative zu „FTP“, dem „File Transfer Protocol“. **Aus Sicherheitsgründen sollten Sie reinen „FTP“-Zugriff nicht ermöglichen, da bei dieser Art von Zugriff das Passwort unverschlüsselt übertragen wird.** Sichern Sie *„SSH“* mit einem sehr starken Passwort. Tauschen Sie personenbezogene Daten ausschließlich via SSL aus.

Als Betreiber eines Webservers sollten Sie sich besonders mit dem Rechtemanagement auseinander setzen. **Legen Sie eigene Benutzerrechte für Ihre Web-Anwendungen an und gehen Sie besonders bei der Vergabe mit sogenannten *Root*-Rechten äußerst sparsam um.** Dabei handelt es sich um die primären Zugriffsrechte, welche nur für systemnahe Verwaltungsaufgaben genutzt werden sollten. Eine unbedachte Benutzung kann bereits die vollständige Neuinstallation des gesamten Systems zur Folge haben.

Autoren

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen

[1] http://www.kmu-sicherheit.de

http://www.ec-net.de

[2] http://ratgeber.it-sicherheit.de

https://www.internet-sicherheit.de

http://www.bsi-fuer-buerger.de

http://www.bitkom.de

http://www.sicher-im-netz.de

Bildquelle: © Joerg Habermeier - Fotolia.com

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: http://www.kmu-sicherheit.de

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de