eBUSINESSLOTSE

INFOBÜRO FÜR UNTERNEHMEN

SCHWABEN

LEITFADEN

Webseiten sicher betreiben

Hintergrundwissen für Unternehmen die eigene Webseiten betreiben

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Webseiten sicher betreiben

Deutlich mehr als die Hälfte aller KMUs und mehr als drei Viertel aller Einzelhändler in Deutschland besitzen eine eigene Internetpräsenz. Diese hilft das jeweilige Unternehmen online zu präsentieren, Kunden anzusprechen und Waren direkt zu verkaufen. Im vergangenen Jahr wurden in Deutschland durch E-Commerce mehr als 40 Milliarden Euro umgesetzt. Das ist mehr als eine Verdoppelung gegenüber 2010.

Allerdings birgt der eigene Internetauftritt auch beachtenswerte Risiken. So haben sich beispielsweise die jährlich erfassten Cyberangriffe seit 2010 mehr als vervierfacht. Ein Grund für uns, das Thema sicheres Hosting von Webseiten näher zu betrachten! Doch eins vorab: 100% Sicherheit ist ein Ziel, das in der Realität kaum erreicht werden kann. Der Fokus liegt deswegen darauf, die eigene Internetpräsenz weitestgehend abzusichern, es den Angreifern schwer zu machen und im Falle eines tatsächlich erfolgreichen Angriffs den Betrieb wieder aufnehmen zu können.

Welche einzelnen Bestandteile müssen geschützt werden?

Moderne Internetseiten bestehen aus einer Reihe an Komponenten, die für den Betrieb notwendig aber auch gleichzeitig für Angreifer interessant sind. Bei den meisten Webseiten sind diese Komponenten die folgenden:

- Web-Server
- Web-Applikation
- Datenbankserver
- Transportweg

Im weiteren Verlauf dieses Leitfadens werden wir Probleme erläutern, Fallstricke aufzeigen und mögliche Schutzmaßnahmen vorstellen.

Web-Server

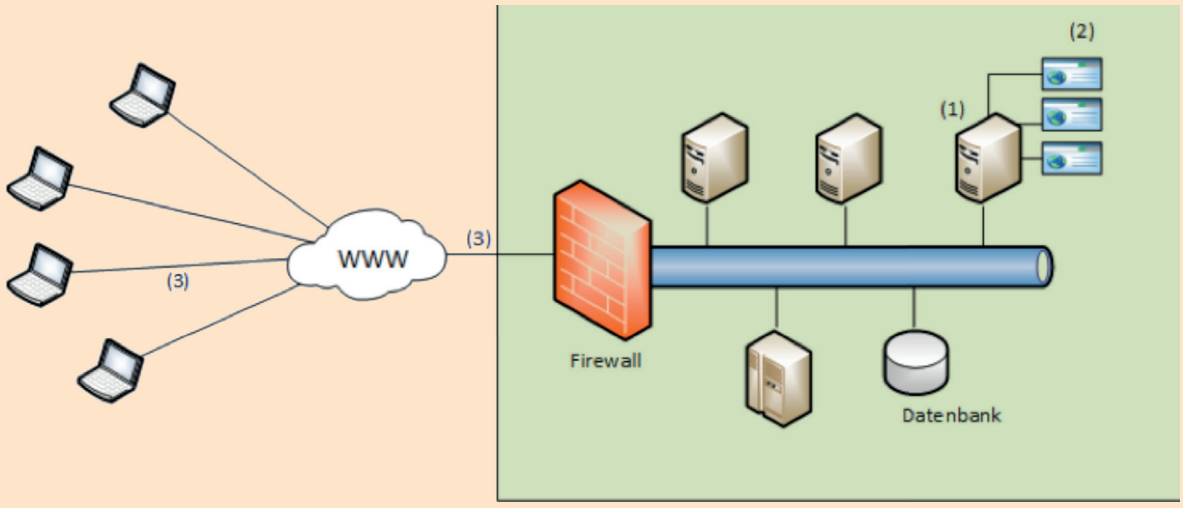
Als Web-Server wird der Computer bezeichnet, auf dem die Webseite selbst hinterlegt wird. Dieser Web-Server ist es, der nach dem Eintippen der Internet-Adresse von dem Browser des Benutzers angefragt wird. Für den Betrieb gibt es mehrere gängige und weit verbreitete Modelle:

eigener Webserver: Bei einem eigenen Webserver verfügt der Besitzer über sehr weitreichende Rechte auf dem System. Dabei spielt es kaum eine Rolle ob der Server physikalisch vor Ort in den eigenen Geschäftsräumen oder in einem Rechenzentrum steht bzw. ob es sich um einen physikalischen oder virtuellen Server handelt. In der Regel ist der jeweilige Besitzer hier vollständig für die Absicherung und den Betrieb des Servers verantwortlich.

- Diese Variante ist nur für sehr erfahrene Anwender bzw. Firmen mit eigener IT-Abteilung zu empfehlen.

Angemieteter Web-Space: Hier wird kein ganzer Server angemietet sondern innerhalb eines Servers nur ein Bereich, in dem die eigene Webseite hinterlegt werden kann. Der Betreiber des jeweiligen Rechenzentrums kümmert sich dann um die Betreuung des Servers wie beispielsweise das Aktualisieren von Betriebssystem und Komponenten, Berechtigungs-Management, evtl. Back-ups, Updates von Drittanwenderbibliotheken, Konfiguration der Firewall, Virenscanner etc.

Rechenzentrum



(1) Webserver zum Hosten von Internetseiten / Wep-Applikationen

(2) Mehrere Web-Applikationen auf demselben physischen Server gehostet

(3) Transportweg zwischen Rechenzentrum und Besucher

- Diese Variante ist für kleinere Firmen sowie unerfahrene Benutzer eindeutig zu empfehlen.

Bei den Modellen, bei denen ein externer Hoster als Dienstleister mit in das Hosting und somit in die Abwicklung damit verbundener Prozesse eingebunden wird, ist es wichtig verschiedene Punkte zu beachten:

Zuverlässigkeit des Hosters: Abhängig von dem konkreten verwendeten Modell des Hostings übernimmt der Hoster verschiedene Pflichten und Aufgaben des Administrators. Damit erhält

Was muss bei der Zusammenarbeit mit einem Hosting-Dienstleister berücksichtigt werden?

er zum Teil sehr weitreichende Möglichkeiten, die Arbeit der jeweiligen Web-Applikation zu beeinflussen. Bei der Auswahl des Hosters sollte deswegen großer Wert darauf gelegt werden, einen Partner zu wählen, der die notwendige Professionalität, Erfahrung und ggf. Zertifizierungen mitbringt. Bei den „großen Hostern“ ist das in der Regel immer der Fall.

Ort der Datenspeicherung: Abhängig von dem Ort der Daten-Verarbeitung und -speicherung kann es notwendig sein, weitere Regelungen wie beispielsweise Auftragsdatenverarbeitungsverträge zu berücksichtigen. Bei der Anmietung von Serverkapazitäten außerhalb Deutschlands sollte dies explizit geprüft werden. Hierbei spielt es keine Rolle, ob die fraglichen Daten in Form von Dateien oder als Inhalt einer Datenbank vorliegen.

Applikation

Web- und Datenbankserver alleine sind nicht ausreichend um dem Besucher eine Webseite zu präsentieren. Hierfür werden zusätzlich entweder statische Inhalte oder – die gebräuchlichere Methode – Content Management Systeme oder Web-Applikationen verwendet. Typische Beispiele hierfür sind Wordpress oder Joomla als CMS-Systeme und xt:Commerce als Web-Shop. Beide fallen in die allgemeinere Gruppe der Web-Applikationen.

Als Web-Applikation werden ganz allgemein Programme bezeichnet, die auf dem Server laufen und über Webseiten mit den Besuchern interagieren können. Diese sind häufig in PHP oder Java geschrieben und benötigen in den meisten Fällen für den Regelbetrieb Zugriff auf eine Datenbank. Je größer und desto weiter verbreitet die jeweilige Web-Applikation ist, desto höher ist die Wahrscheinlichkeit, dass die Funktionalität der Software durch sogenannte „Add-Ons“ oder „Plugins“ ergänzt werden kann. Durch diese können Entwickler, die nichts mit der Entwicklung der eigentlichen Web-Applikation zu tun haben, kleine Programme schreiben, die die Web-Applikation um neue Funk-

tionen ergänzen. Plugins werden deswegen häufig dazu genutzt Funktionen bereit zu stellen, die nur für einen Teil der Nutzer der Software relevant sind. Diese können sich dann auf Wunsch individuell die entsprechenden Funktionen nachinstallieren.

Sowohl die Web-Applikationen selbst als auch die hinzugefügten Plug-ins und Add-Ons können bislang unentdeckte Softwareschwachstellen enthalten. Um die Wahrscheinlichkeit und das Risiko, dass diese ausgenutzt werden gering zu halten, ist es „best practice“, die Applikation selbst und auch die damit verbundenen Komponenten in regelmäßig und laufend zu aktualisieren. Durch die Aktualisierungen werden zwischenzeitlich durch den jeweiligen Hersteller erfolgte Korrekturen am Programmcode in die eigene Webanwendung integriert und diese dadurch geschützt.

Die Erfahrung zeigt, dass das Einspielen der Aktualisierungen besonders bei Plugins wichtig ist, da diese im Durchschnitt eine niedrigere Softwarequalität als die eigentliche Kernkomponente besitzen und somit in der Regel anfälliger für Fehler und Angriffe sind. Dies ist darauf zurückzuführen, dass die eigentlichen Kernkomponenten häufig von festen und erfahrenen Programmierer-Teams entwickelt werden, während Plug-ins oft nur von einzelnen Programmierern, teilweise ohne Erfahrung in sicherheitsrelevanter Programmierung, erstellt werden.

Neben dem häufigen Aktualisieren der Web-Applikation und der verbundenen Applikationen existieren noch weitere Möglichkeiten um sich gegen gängige Angriffe zu schützen. Viele Betreiber schalten beispielsweise sogenannte Web Application Firewalls (WAFs) zwischen die Web-Applikationen und das Internet. Zweck dieser WAFs ist es, den ankommenden Internetverkehr nach bekannten Angriffsmustern zu durchsuchen, bei Erkennen zu blockieren und dadurch die Web-Anwendung zu schützen. Das Zuschalten der WAF kann abhängig vom jeweiligen Hoster Kosten verursachen. Ihr Einsatz befreit jedoch nicht von der Empfehlung die installierte Web-Applikation auch weiterhin zu aktualisieren.

Für erfahrenere Anwender kann es zudem praktikabel sein den Server, insbesondere das Dateisystem oder Logdateien auf ungewöhnliche Änderungen hin zu überwachen. Hierfür stehen fertige und teilweise kostenlose Tools wie beispielsweise SAMHAIN zur Verfügung. Durch den Einsatz solcher Tools lassen sich mögliche Angriffe auf den Server besser erkennen oder bei erfolgreichen Angriffen die Auswirkungen genauer einschätzen.

In vielen Fällen bieten auch externe Dienstleister die regelmäßige Kontrolle des Servers an. Im Falle der Web-Applikation Wordpress kann dies beispielsweise durch das Add-On Wordfence realisiert werden. So benötigt der eigentliche Betreiber nur noch minimales technisches Know How und erhält dennoch ein relativ hohes Schutzniveau.

Quellenangaben:
1 | http://de.statista.com/statistik/daten/studie/70983/umfrage/eigene-websites-von-handelsunternehmen-nach-wirtschaftszweig/

http://de.statista.com/statistik/daten/studie/151766/umfrage/anteil-der-unternehmen-mit-eigener-website-in-deutschland/

2 | http://de.statista.com/statistik/daten/studie/71568/umfrage/online-umsatz-mit-waren-seit-2000/

3 | http://de.statista.com/statistik/daten/studie/348766/umfrage/jaehrliche-anzahl-von-internetangriffen-weltweit/

4 | http://la-samhna.de/samhain/

5 | http://www.wordfence.com/

6 | http://www.wieistmeineip.de/

Transportweg:

Die Verbindung zwischen dem Computer des Besuchers der Webseite und dem Server selbst wird als Transportweg bezeichnet. Das für die Standardkommunikation eingesetzte Protokoll im Internet heißt HTTP (Hyper Text Transfer Protokoll). Dieses ist Standardmäßig unverschlüsselt was dazu führt, dass die Daten ungeschützt vor Mitlesen oder Änderungen durch das Internet transportiert werden. Somit ist die Verwendung für den Austausch sensibler Informationen wie Benutzername und Kennwörtern, Bankdaten etc. nicht zu gebrauchen. Wenn dies dennoch möglich sein soll muss die Verbindung verschlüsselt werden. Hierfür hat sich im Internet das sogenannte PKI-System (Public Key Infrastructure) etabliert. Hierfür muss der Betreiber der Webseite ein Zertifikat erwerben und dies per Konfiguration des Servers den Besuchern zur Verfügung stellen. Die erfolgreiche Verwendung erkennt man daran, dass die Seite künftig über den „https://“-Präfix anstelle über „http://“ zu erreichen ist. Für die, der Verschlüsselung zugrunde liegenden Zertifikate, gibt es drei unterschiedliche Typen:

DomainSSL-Zertifikate sind die einfachste Form der Zertifikate. Hier wird innerhalb des Zertifikats lediglich angegeben, für welche Internetseite oder –seiten es gültig sein soll. Dies ist für reine Verschlüsselung ausreichend, verrät dem Benutzer jedoch noch nichts über die tatsächliche Identität der Gegenstelle. Die nächst strenge Prüfung erfolgt bei **OrganizationSSL-Zertifikaten**. Bei ihnen wird geprüft, ob die Organisation, die das Zertifikat beantragt, tatsächlich berechtigt ist die angegebene Internetadresse zu führen. Die strengste Prüfung erfolgt bei **Extended Validation (EV) SSL-Zertifikaten**. Hierbei werden sowohl die Organisation selbst als auch deren Recht auf Verwendung einer Internetadresse geprüft und soweit möglich mit amtlichen Einträgen abgeglichen. Nicht alle Zertifizierungsstellen sind berechtigt diese Überprüfung durchzuführen.

Verschlüsselungszertifikate können kostenpflichtig über kommerzielle Anbieter wie „Thawe“ oder “Verisign“ bezogen werden. Alternativ gibt es auch kostenfreie Stellen die Zertifikate ausstellen. Zu diesen zählen „StartSSL“ und „LetsEncrypt“ . Einige Hoster bieten zudem die Möglichkeit an, SSL-Zertifikate direkt über sie zu beziehen.

Verschlüsselung als Wettbewerbsvorteil: Die Möglichkeit verschlüsselt auf die Internetseite zugreifen zu kön-

nen kommt nicht nur der Privatsphäre der Benutzer zugute. Im August 2014 hat der Suchmaschinenriese Google im Rahmen seiner „HTTPS-Everywhere“-Kampagne bekannt gegeben, zukünftig HTTPS als ein Kriterium für die Bewertung von Internetseiten heran zu ziehen. Somit besteht die Möglichkeit, dass die eigene Webseite bei gleichbleibenden Inhalt durch die Verwendung von HTTPS besser positioniert in den Suchlisten von Google erscheint. Somit wird die Verwendung von Verschlüsselung im Internet zu einem Wettbewerbskriterium.

Allgemeine Empfehlungen

Regelmäßige Back-Up´s: Für den sicheren Betrieb eines Servers sind auch Maßnahmen für die Ausfallbehandlung zu treffen. Das umfasst insbesondere das Erstellen und Vorhalten von aktuellen Backups aller beteiligter Komponenten (z.B. Datenbanken, Dateien & Ordner). Häufig bieten Webhoster diese Funktionen bereits als Bestandteil von Hosting-Paketen an.

Üben für den Ernstfall: Die Praxis zeigt, dass viele Betreiber nach einem Serverausfall Probleme damit haben, aus den vorhandenen Back-Up´s wieder ein funktionierendes System zu erstellen. Das kann auf mangelnde Erfahrung, defekte Backups oder falsche Back-Up-Einstellungen zurückzuführen sein. Deswegen empfiehlt es sich, je nach Art der gehosteten Applikation, in angemessenen Zeitabständen diese Rekonstruktion zu testen und zu prüfen ob sich mit angemessenem Aufwand aus den gesicherten Daten wieder eine funktionsfähige Applikation erstellen lässt.

Server härten: Um potentiellen Angreifern eine möglichst geringe Angriffsfläche zu bieten hat es sich als „Best Practice“ etabliert Server zu härten. Darunter versteht man das Abschalten bzw. Deinstallieren nicht verwendeter Software, das Sperren bzw. Entfernen von nicht benötigten Benutzern (z.B. „Gast“) und auch das regelmäßige Aktualisieren der verwendeten Software.

Hilfe annehmen: Gerade bei kleineren Webpräsenzen oder nicht erfahrenen Administratoren sollte in Erwägung gezogen werden, nicht alle Sicherheitsvorkehrungen selbst zu treffen sondern dabei auf erfahrenere Dienstleister zurückzugreifen. Häufig sind die Kosten für diese geringer als die Folgekosten eines Systemausfalls und dem damit verbundenen Image-Verlust.

7 | https://www.thawte.de/

8 | http://www.verisign.com/

9 | http://www.startssl.com/

10 | https://letsencrypt.org/

11 | http://googlewebmastercentral.blogspot.de/2014/08/https-as-ranking-signal.html?m

Auf was muss man bei der Auswahl eines Webhosters achten, wenn man sicher gehen will?

- Gibt es eine Möglichkeit für automatische Back-Up´s des Dateisystems und der Datenbanken?
- In welchen Abständen werden die Back-Up´s durchgeführt. (täglich, wöchentlich,…)
- Wie lange werden Back-Up´s auf dem Server gespeichert?
- Wie aufwändig ist die Wiederherstellung der Daten aus einem Back-Up´s?
- Welche Kosten werden durch die Inanspruchnahme der Back-Up-Funktion verursacht?
- Bietet der Betreiber die Möglichkeit den Datenverkehr zu verschlüsseln?
- Bietet der Betreiber die Möglichkeit die Installierten Web-Applikationen automatisch zu aktualisieren?
- Wie hoch ist die zugesicherte Verfügbarkeit der Hosting-Dienstleistung?
  (Service Level Agreement = SLA)
- Bietet der Betreiber die Möglichkeit an, eine Web Application Firewall oder einen Virenscanner zuzuschalten?
- Bietet der Betreiber die Möglichkeit den Mail-Verkehr auf ausgehenden Spam zu untersuchen und ggf. zu reagieren?
- Kosten, Erreichbarkeitszeiträume des Supports und technischer Ansprechpartner
- Standort der Rechenzentren (in Deutschland, im EWR, weltweit)

eBUSINESSLOTSE
INFOBÜRO FÜR UNTERNEHMEN
SCHWABEN

Der eBusiness-Lotse Schwaben ist Teil der Förderinitiative „eKompetenz-Netzwerk für Unternehmen“, die im Rahmen des Förderschwerpunkts „Mittelstand-Digital – IKT-Anwendungen in der Wirtschaft“ vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird. Der Förderschwerpunkt unterstützt gezielt kleine und mittlere Unternehmen (KMU) sowie das Handwerk bei der Entwicklung und Nutzung moderner Informations- und Kommunikationstechnologien (IKT). Mittelstand-Digital setzt sich zusammen aus den Förderinitiativen „eKompetenz-Netzwerk für Unternehmen“ mit 38 eBusiness-Lotsen, „eStandards: Geschäftsprozesse standardisieren, Erfolg sichern“ mit 16 Förderprojekten und „Einfach intuitiv – Usability für den Mittelstand“ mit zurzeit 13 Förderprojekten.

Weitere Informationen finden Sie unter www.mittelstand-digital.de.

eBUSINESSLOTSE
INFOBÜRO FÜR UNTERNEHMEN
SCHWABEN

IT-Fachwissen:
Für die Region. Aus der Region.

Der eBusiness-Lotse Schwaben ist durch seine Nähe zu forschenden Einrichtungen in der Lage, auf tagesaktuelle Entwicklungen aus dem Themengebiet der IT-Sicherheit einzugehen und in diesem Bereich tiefgehend und fundiert zu informieren.

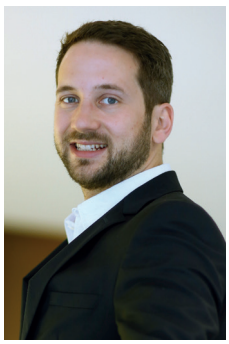
Zu den Mitarbeitern des eBusiness-Lotsen Schwaben gehören unter anderem Mitglieder der HSASec, der Forschungsgruppe IT-Security und Forensik der Hochschule Augsburg. Die Forschungsschwerpunkte der HSASec liegen in den Bereichen des Penetration-Testing, des Secure Software Development Lifecycles sowie der IT-Forensik und der Industrieautomatisierungssicherheit.

Hierbei arbeitet die Forschungsgruppe mit national als auch international tätigen Unternehmen zusammen. Erkenntnisse aus diesen Themengebieten können somit zeit- und praxisnah durch den Lotsen bereitgestellt werden. Dadurch profitieren die Unternehmen im Einzugsgebiet des schwäbischen Lotsen von den Erkenntnissen aus Forschungstätigkeiten, auf die sie unter anderen Umständen keinen Zugriff erhalten hätten.

Der eBusiness-Lotse Schwaben bietet u.a. Informationen zu den sicherheitsrelevanten Themen IT-Sicherheit und Datenschutz an. Ferner werden Informationen zu den Themen Cloud, Social Media, mobile Dienste und mobiles Arbeiten angeboten.


Sebastian Kraemer


Andrea Henkel


Peter Rosina

Partner dieses Leitfadens:

Impressum

Verantwortlicher Redakteur/Herausgeber:
Präsident Prof. Dr.-Ing. Dr. h.c. Hans-Eberhard Schurk
Hochschule für angewandte Wissenschaften Augsburg
An der Hochschule 1
86161 Augsburg
Tel: +49 (0) 821 / 55 86-0
Fax: +49 (0) 821 / 55 86-3222
eMail: info@hs-augsburg.de

Autor:
Sebastian Wolfgang Kraemer, Wissenschaftlicher Mitarbeiter an der Hochschule Augsburg

Zuständige Aufsichtsbehörde:
Bayerisches Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst
80327 München

Rechtsform:
Körperschaft des öffentlichen Rechts

Geschäftsführung:
Präsident Prof. Dr.-Ing. Dr. h.c. Hans-Eberhard Schurk

Ihr Kontakt zu uns:
Fon: +49 (0) 821 / 450 433 - 106
E-Mail: Team@eBusinessLotse-Schwaben.de
www.eBusinessLotse-Schwaben.de

eBusiness-Lotse Schwaben:
c/o IT-Gründerzentrum GmbH
Werner-von-Siemens-Str. 6
D-86159 Augsburg

Redaktion:
Florian Mattler

Gestaltung und Produktion:
Technik & Grafik
Kerstin Meister
Fon: +49 (0) 8238 / 958338
E-Mail: kerstin.meister@technikundgrafik.de

Bildnachweise:
jamdesign, Nmedia (3) – Fotolia.com