Dr. Andreas Gabriel & Steffen Klein

»Mehr Sicherheit für den eigenen Online-Shop

Die Anzahl der Online-Shopbetreiber wächst unbestritten ständig an. Der Aufwand den man betreiben muss, bis ein solcher Shop dann wirklich funktionsfähig im Netz ist, wird in der Regel heftig unterschätzt. Noch heftiger wird dann oft der nachfolgende und notwendige Aufwand unterschätzt, der im Online Marketing betrieben werden muss, damit der Shop überhaupt Besucher bekommt. Wer hat da schon Zeit, Nerven und Geld, sich auch noch um eine ganz besondere Gruppe Besucher zu kümmern, die auch ohne Marketingmaßnahmen von ganz alleine daher kommen: Die Bösen. Andreas Gabriel und Steffen Klein geben Tipps, wie man den Hackern das Leben deutlich schwerer machen kann.

DER AUTOR

Dr. Andreas Gabriel arbeitet als Forschungsassistent am Lehrstuhl für BWL und Wirtschaftsinfor-matik an der Universität Würzburg und beschäftigt sich u. a. mit sicheren Geschäftsprozessen von kleinen und mittleren Unternehmen.

DER AUTOR

Steffen Klein arbeitet als Netzwerk- und Systemadministrator bei der SYSTHEMIS AG und prüft im Rahmen von Penetrationstests u. a. die Sicherheit von E-Commerce-Anwendungen

Der Trend zur Intensivierung des eigenen Online-Handels wird von Unternehmen jeder Größe getragen; sowohl große Konzerne als auch kleine und mittelständische Unternehmen (KMU) nutzen Online-Shops, Power-Shopping etc., um den eigenen Umsatz durch den Absatz ihrer Leistungen über das Internet zu steigern (Quelle: Umfrage des NEG, www.ec-net.de). Die Umsetzung einer auf die individuellen Gegebenheiten des jeweiligen Unternehmens angepassten E-Commerce-Strategie befähigt die genannten Akteure, innerhalb dieses Vertriebskanals so erfolgreich zu agieren.

In Abhängigkeit vom Umsatzanteil des E-Commerce-Bereichs am Gesamtumsatz des Unternehmens müssen die Maßnahmen im Umfeld der Informationssicherheit entsprechend angepasst bzw. ausgebaut werden. Unternehmen wie z. B. Amazon setzen an dieser Stelle einen sehr hohen Maßstab, da augenscheinlich sehr viel Geld in Strukturen, Personal und Infrastruktur investiert wurde und noch immer wird. Dass die Umsatzzahlen auch für KMU steigen, belegt u. a. auch eine Studie des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG, www.kmu-sicherheit.de):

Die einzelnen Facetten einer angemessenen Sicherheitsstrategie hängen maßgeblich von der Branche des Unternehmens sowie vom Anteil des E-Commerce am Gesamtumsatz ab.

In Abhängigkeit von den individuellen Erwartungen müssen die Entscheidungsträger aus den folgenden Kategorien sinnvolle und ökonomisch vertretbare Schutzmaßnahmen ableiten:

Angriffe auf die Infrastruktur

Die maßgeblichen Angriffsziele dieser Kategorie sind das Geschäftsgebäude des Unternehmens und der Serverraum, in dem die E-Commerce-Anwendungen betrieben werden. Darüber hinaus können technische Komponenten wie z. B. eine Klimaanlage ins Visier der Angreifer geraten.

Die Wahrscheinlichkeit einer direkten Attacke auf die genannte Infrastruktur erscheint höchstens durch einen terroristischen Anschlag gegeben. In Europa kann das Risiko eines derartigen Angriffs im Moment wohl noch(?) vernachlässigt werden.

Allerdings besteht die Möglichkeit, dass durch Bedrohungen aus dem Umfeld der höheren Gewalt (Sturm, Feuer, Erdbeben o. ä.) ein Schaden an den hier betrachteten Komponenten entsteht. Auf Basis einer Risikoanalyse bzw. eines Sicherheits-Audits kann die damit verbundene Eintrittswahrscheinlichkeit bewertet und realistisch eingestuft werden.

Angriffe auf die Netzanbindung

Die Verfügbarkeit der Netzanbindung ist, trotz aller technischen und/oder organisatori-

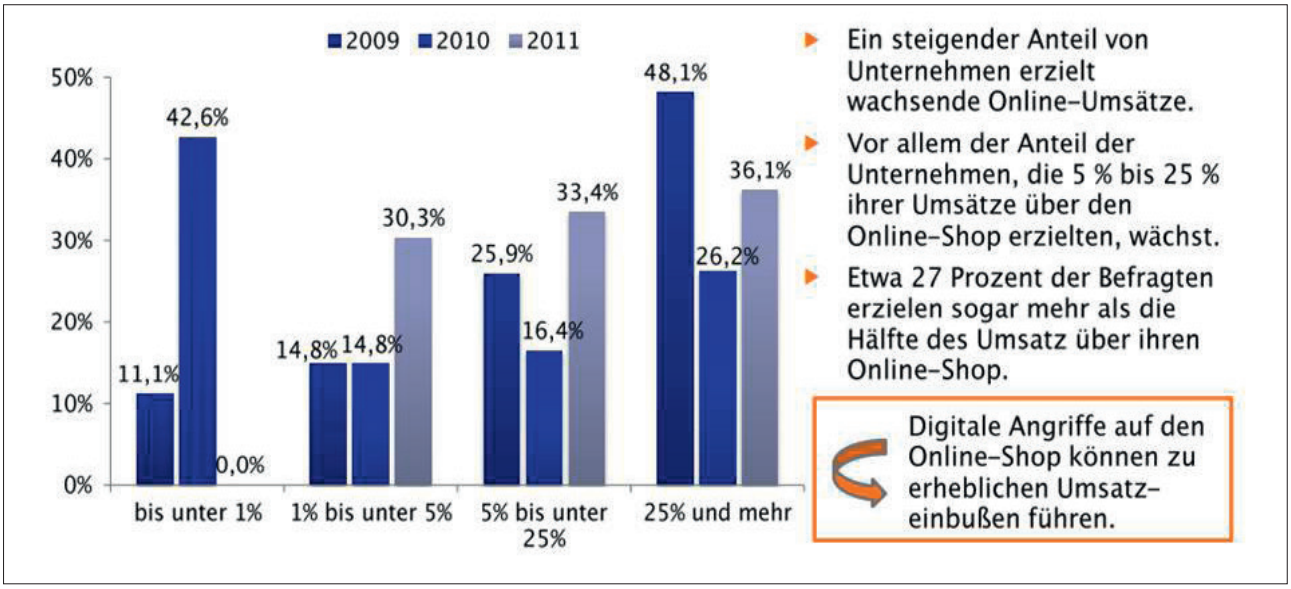

Abb. 1: Anzeige des Qualitätsfaktors mittels Sprechblase

schen Maßnahmen, einer der maßgeblichen Faktoren für den Erfolg eines Online-Shops. Daher wird dringend angeraten, den folgenden Fragestellungen nachzugehen

1. Welche Verfügbarkeit der Netzanbindung wird durch den Dienstleister für die Netzanbindung garantiert? Existiert zu dieser Vorgabe ein rechtssicher abgeschlossenes Service Level Agreement (SLA)?
2. Ist das Gelände bzw. das Gebäude redundant an das Backbone angeschlossen? (Die zwei Leitungen müssen durch getrennte Trassen eingeleitet werden, im Idealfall münden diese in verschiedenen Serverräumen.)
3. Wie erfolgt das Monitoring der Netzverfügbarkeit? Welche Eskalationsstufen sind mit diesem System gekoppelt?
4. Welche grundsätzliche Verfügbarkeit wird vom Top-Management vorausgesetzt?

Neben diesen grundsätzlichen Fragen der Netzanbindung muss es entsprechende Regelungen bezüglich der Reaktion auf Angriffe auf das Netzwerk bzw. die Netzanbindung geben. Es wurde in diesem Magazin am 07.08.2011 darüber berichtet, dass es bereits zu Erpressungsversuchen gegenüber den Betreibern von Online-Shops kam. Um eine gezielte Attacke auf die Performance des Netzwerks abwehren zu können, müssen ausgewählte Schutzmaßnahmen ergriffen werden:

Die Performance des Netzwerks und damit des Webservers kann durch ein Servercluster mit Load Balancing gesteuert und dadurch gezielt verbessert werden – gerade um Leistungsspitzen abzufangen (siehe Abbildung 2).

Um die Auslegung des Balancing-Systems realistisch planen zu können, müssen sich die Verantwortlichen darüber im Klaren sein, welchen Anforderungen sie gegenüberstehen. An dieser Stelle kann auf Erfahrungswerte der Vergangenheit zurückgegriffen werden, um auch auf saisonalen Kundenandrang vorbereitet zu sein.

Eine dynamische Ausgestaltung der internen Netzanbindung gestaltet sich dagegen relativ schwierig, da die Variationsmöglichkeiten recht überschaubar sind. Unabhängig davon, über welche Bandbreite die interne Netzanbindung verfügt und welche Performance ein ggf. vorgelagertes Load Balancing leisten

IM RAHMEN EINES AUDITS SOLLTE DEN FOLGENDEN FRAGESTELLUNGEN NACHGEGANGEN WERDEN (AUSWAHL):

1. Befindet sich das Geschäftsgebäude in einem besonders kritischen Bereich, z. B. nahe an einem Fluss?
2. Sind entsprechende Schutzmaßnahmen gegen Feuer (Rauchmelder etc.) und Wasser (Wassersensoren) instal-liert?
3. Befinden sich im direkten Umfeld des Serverraums wasserführende Leitungen?
4. Wurden in der Vergangenheit Notfallsimulationen wie z. B. eine Feuerschutzübung durchgeführt?
5. Wurde auf Basis einer Risikoanalyse bewertet, welche potenziellen Auswirkungen von den hier betrachteten Bedrohungen ausgehen? Wenn ja, welche Schutzmaßnahmen wurden in die Wege geleitet?
6. Erscheint der Aufbau eines redundanten Standortes sinnvoll, um auch auf eine Katastrophe angemessen reagieren zu können?

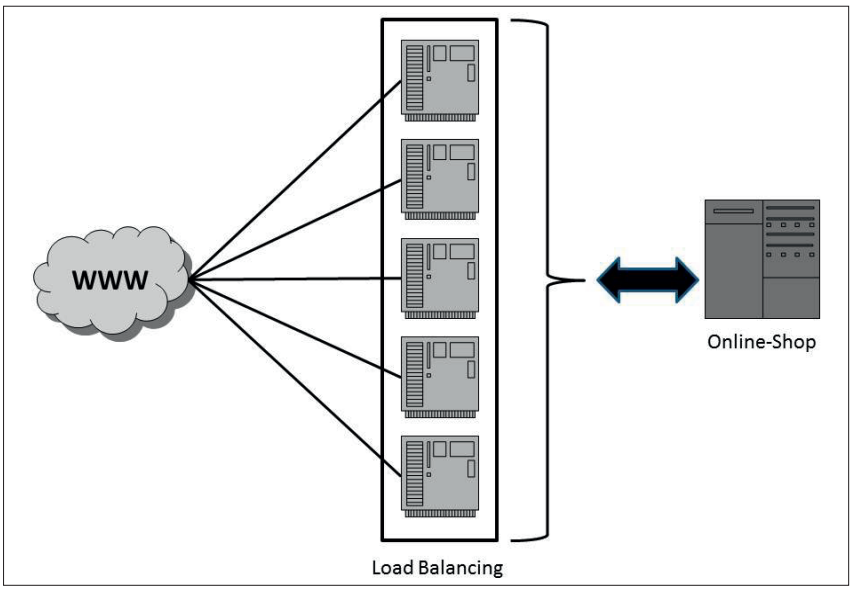

Abb. 2: Umsetzung Load-Balancing – um Leitungsspitzen auf Netzwerkebene abfedern zu können

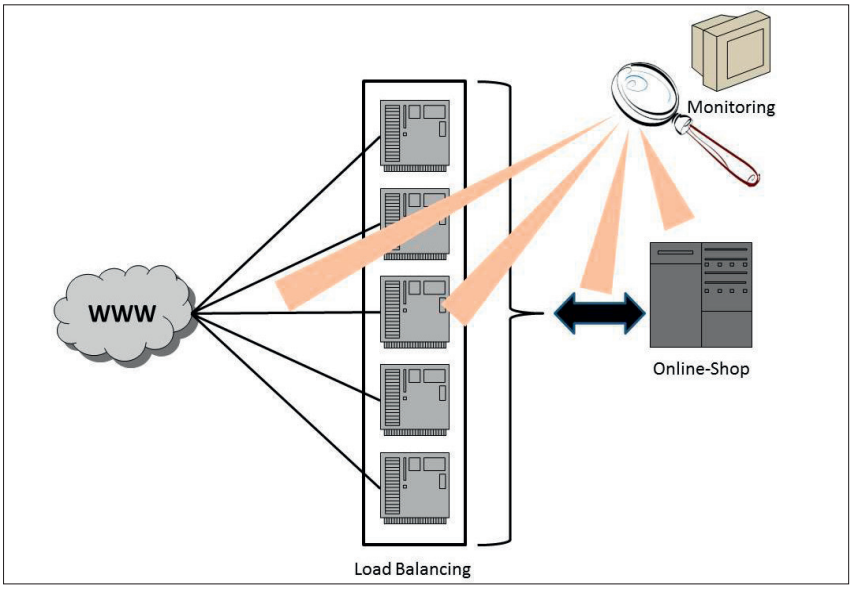

Abb. 3: Monitoring-Ansatz, um auf Schwankungen im Netzwerk reagieren zu können

kann, bleibt die Netzanbindung ein limitierender Faktor für den Online-Shop. Um auf Problemsituationen, die durch eine Online-Attacke hervorgerufen werden, zeitnah reagieren zu können, sind geeignete Monitoringmaßnahmen zu implementieren, z. B. eine dauerhafte Bandbreitenmessung durch ein Nagios-System (siehe Abbildung 3).

Sobald die Möglichkeiten der Schutz- bzw. Überwachungstechnologien ausgereizt sind, müssen sich die Verantwortungsträger mit der Implementierung organisatorischer Schutzmaßnahmen auseinandersetzen.

So kann das Vorhandensein eines Alarm-, Notfall- und Katastrophenplans sicherstellen, dass bei einem – i.d.R. unerwarteten – Angriff von außen geeignete Deeskalationsverfahren existieren.

Angriffe auf die Software (auf den verschiedenen Ebenen des ISO/OSI-7-Schichten-Modells)

Ein Angriff auf die unterschiedlichen (Software-)Programme, die zum Betrieb eines Online-Shops notwendig sind, kann auf den folgenden Ebenen erfolgen:

1. Das Betriebssystem des Servers (i.d.R. Microsoft oder Linux)
2. Die eigentliche Applikation des Webservers (Apache oder Microsoft IIS)
3. Die Anwendungssoftware (Shop-Software – als Individuallösung oder Standardprodukt)
4. Sonstige Applikationen, die ausschließlich für eine spezielle Anwendung genutzt werden

Eine vollumfängliche Liste aller möglichen Angriffsarten würde den Rahmen dieses Beitrags bei Weitem sprengen. Im Grunde ist es allerdings nicht von entscheidender Bedeutung, auf welchem Software-Level der Angriff erfolgt, i.d.R. kommen immer die gleichen Angriffsarten zum Einsatz. (Dabei wird immer davon ausgegangen, dass grundlegende Schutzmaßnahmen auf Netzwerk- (Firewall etc.), Applikations- (Backup, Versionierung etc.) sowie Prozessebene (z. B. ein Workflow für das Benutzermanagement) implementiert sind.)

Im ersten Szenario wird davon ausgegangen, dass der (Web-)Server direkt aus dem WWW zu erreichen ist und lediglich die bereits genannten Basis-Sicherheitsmaßnahmen installiert wurden.

Denial of Service (DOS)/distributed DOS (DDOS)

Der Server wird mit einer Vielzahl von Anfragen konfrontiert, die er ab einer bestimmten Belastungsgrenze nicht mehr bearbeiten kann. Daher stellt dieser seinen Dienst ein und der Online-Auftritt steht daher nicht mehr zur Verfügung (= DOS).

Um die Komplexität dieses Angriffs zu erhöhen, wird der Server von mehreren Quellen parallel attackiert, sodass etwaige Schutzmaßnahmen wie z. B. die Sperrung bestimmter Webadressen nicht mehr praktikabel umgesetzt werden können. Gerade die Nutzung sog. Bot-Netze macht diesen „verteilten Angriff“ so gefährlich (= DDOS).

Cross-Site-Scripting

Nimmt die Webapplication unge-

prüft Benutzereingaben entgegennimmt, besteht die Möglichkeit, direkten Schadcode auf der Webseite zu platzieren (Gästebücher, Feedback-Seiten, Rezensions-Seiten sind beliebte Angriffsziele). Wenn dort ungeprüft html/JavaScript übergeben werden kann, wird dies beim Besuch des nächsten Kunden direkt im Browser ausgeführt und kann je nach Sicherheitseinstellungen bis zum Identitätsdiebstahl führen.

SQL-Injektion

Die Zugriffe auf die Datenbank werden gezielt attackiert, um entweder die Applikation zu sabotieren oder vorhandene Inhalte auszulesen. Ähnlich wie beim Cross-Site-Scripting wird hier versucht, ungeprüften Schadcode in Formulare einzubinden (z. B. Login), um Datenbankinhalte auszulesen/zu ändern.

Exploits

Für jedes Programm müssen sog. Updates eingespielt werden, um Schwachstellen zu schließen und dadurch Angriffe unmöglich zu machen. In der Praxis werden immer wieder Fälle bekannt, bei denen ein Update-Prozess unterbleibt. Die dadurch bestehenden Sicherheitslücken werden durch sog. Exploits gezielt angegriffen.

Um die Bedrohungen, die von diesen Angriffen ausgehen, zu reduzieren, sollten die folgenden Schutzmaßnahmen umgesetzt werden:

(Server-)Load Balancing

Die Konfiguration der IT-Infrastruktur wird derart modifiziert, dass der Zugriff aus dem WWW nicht mehr direkt auf den Webserver erfolgt, sondern ein Load-Balancing-System dazwischengeschaltet wird (vgl. Abbildung 5).

Dabei steht der Grundgedanke im Vordergrund, dass die eingehenden Anfragen von mehreren Systemen parallel empfangen und verarbeitet werden können. Dadurch steigt die Performance der E-Commerce-Anwendung und Schwankungen bei der Bearbeitung von (Kunden-)Anfragen können abgefangen werden.

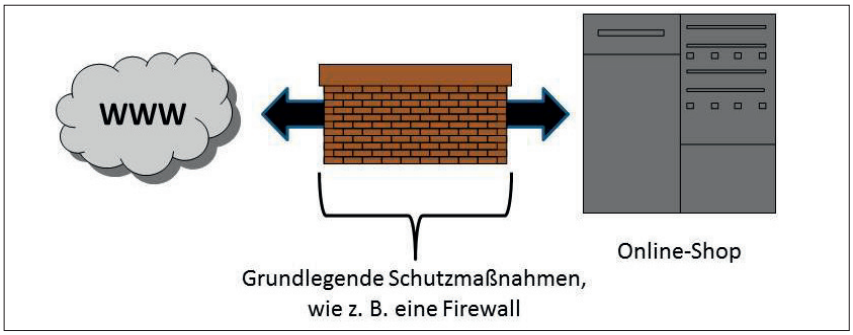

Abb. 4: Basis-Absicherung des Online-Shops

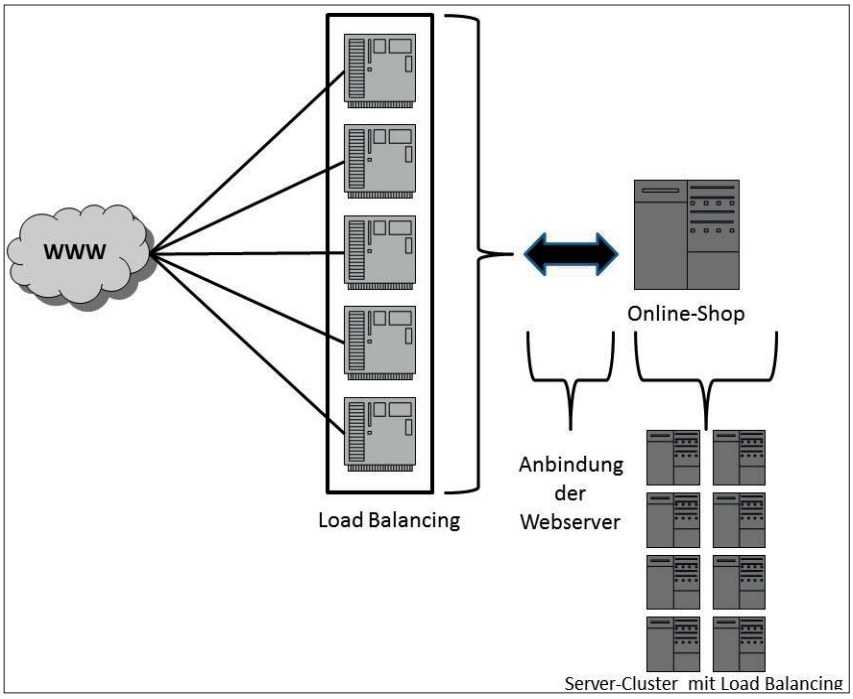

Abb. 5: Absicherung Nr. 2: Server-Cluster mit Load Balancing

Security Feeds/Updates

Wer für Shop-Software oder eine Serverarchitektur Verantwortung übernimmt, muss sich vieler möglicher Risiken bewusst sein. Ein „run and forget" hätte in diesem Fall ernste Konsequenzen (z. B. der Mailserver wird zum Versand von Spam-Nachrichten missbraucht, Webspace wird zum Verteilen von Raubkopien verwendet oder die Datenbankinhalte gehen verloren). Das Wichtigste in diesem Fall ist, immer „up to date" zu sein. Das Beheben von Softwarefehlern ist für den Shop und für das Betriebssystem durch das Einspielen von Updates meistens mit nur wenigen Klicks- oder Befehlen erledigt und deckt damit dann einen großen Teil von Sicherheitslücken ab. Informationen über aktuelle Bedrohungen findet man über Security Feeds der Softwarehersteller oder über allgemeine Kanäle wie z. B. Heise oder Golem.

Reverse-Proxy

Durch die Einrichtung eines Reverse-Proxy (z. B. Squid, Nginx) wird der Zugriff auf den Webauftritt zusätzlich geschützt. Auf den Webserver wird nicht mehr unmittelbar aus dem Internet zugegriffen, sondern der Proxy nimmt die externen Anfragen entgegen und gibt sie an den Webserver weiter. Somit lassen sich auch Loginbereiche/Verwaltungsbereiche von extern effizient abschotten.

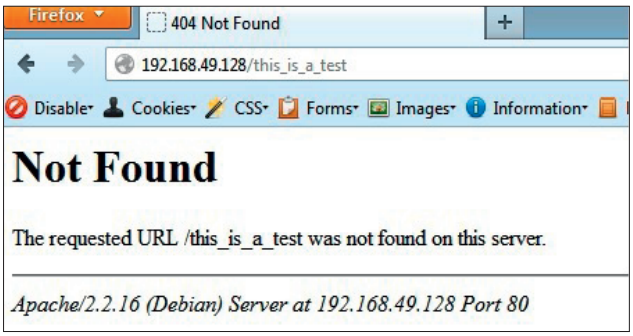

Abb. 6: Standardausgabe Apache-Web-Server

Abb. 7: Ausgabe nach Durchführung der beschriebenen Änderungen

Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems (IPS)

Das permanente Monitoring des Netzwerks bringt die Verantwortlichen in die Lage, die maßgebliche Komponente „Verfügbarkeit" zu messen und automatisiert Eskalationsschritte in die Wege zu leiten, um angemessene Schutzmaßnahmen anzustoßen (= IDS).

Darüber hinaus besteht die Möglichkeit, mit einem IPS Schutzmaßnahmen abzurufen, die proaktiv vor bzw. mit dem Auftreten einer Anomalie Anwendung finden.

In beiden Fällen des Monitorings müssen die geeigneten Einsatzstellen definiert werden. Diese Festlegung sollte auf Basis einer Risikoanalyse erfolgen, um die kritischsten Ansatzpunkte definieren zu können.

Durch die hier beschriebenen Schutzmaßnahmen werden maßgebliche Schwachstellen eines E-Commerce-Angebots geschlossen. Die Schwachstelle verlagert sich dadurch von der grundsätzlichen Erreichbarkeit und den eingesetzten Applikationen des Online-Auftritts hin zu der Administration aller Systeme.

Angriffe, die nur durch fehlerhafte Administration zustande kommen können

Auch an dieser Stelle ist die Liste potenzieller Probleme umfangreich. Durch nachstehende Beispiele werden zwei wesentliche Facetten der Informationssicherheit verdeutlicht:

1. Eine versehentliche Falschkonfiguration durch die Administratoren ermöglicht einem Angreifer direkten Zugriff auf sensible Informationen (z. B. Dateisystemberechtigungen, falsche User-/Gruppen-Zuweisung).
2. Durch kleinere „Eingriffe" in die Standardkonfiguration der Server-Systeme können zahlreiche Schwachstellen nachhaltig geschlossen werden.

Angriffsflächen minimieren

Wenn mit einer erfundenen URL-Adresse der Apache-Web-Server seine Standardfehlerseiten ausliefert, enthält diese in der Grundeinstellung leider auch die Versionsnummer und das Betriebssystem. Das erleichtert natürlich den Angriff, da so ohne Aufwand wichtige Informationen ausgelesen werden können (Beispiel siehe Abbildung 6).

Lösung

```
echo ServerTokens Prod >>
/etc/apache2/apache2.conf
echo ServerSignatur off >>
/etc/apache2/apache2.conf
```

Nach einem Neustart des Webservers hat sich die Ausgabe grundlegend verändert. Es werden keine Informationen über die verwendeten Applikationen mehr angezeigt (siehe Abbildung 7).

Umbenennen von Verwaltungssoftware am Beispiel von phpmyadmin

Um die Erreichbarkeit der genannten Verwaltungssoftware auf Basis einer standardisierten Vorgehensweise signifikant zu erschweren, sollte die folgende Konfiguration vorgenommen werden:

Durch folgenden Befehl wird der Alias umbenannt und ist dadurch für einen Angreifer schwerer zu finden:

```
/etc/apache2/conf.d/phpmyadmin.
conf
```

Der neue Name des Alias könnte z. B. „mydb" lauten. (VORSICHT: Die Änderungen werden erst nach einem Neustart des Systems wirksam.)

Durch diese Konfiguration endet dann in den meisten Fällen eine Brute-Force-Attacke gegen den Datenbankserver bereits in der Einleitungsphase.

Allein die Tatsache, dass der Administrationsbereich der Datenbank nicht mehr auf einfachem Wege erreichbar ist, erhöht das Sicherheitsniveau erheblich.

Offene Ports herausfinden und schützen

Mit Nutzung der Applikation „nmap" lassen sich lokal auf einem Rechner oder remote über das WWW die geöffneten Ports des Hosts ermitteln.

Um einen Webserver angemessen zu schützen, müssen zuerst die Ports definiert werden, die öffentlich zugänglich sein müssen, um die jeweils installierten Applikationen zu betreiben. Die sind i.d.R. die Ports 80 (http) und/oder 443 (https). Über diese beiden Zugänge erfolgt gerade im E-Commerce die Abwicklung der einzelnen Kundengeschäfte. Darüber hinaus werden die Verantwortlichen verschiedene Verwaltungsports wie z. B. ssh öffnen müssen, um interne bzw. administrative Zugänge zu ermöglichen. Diese Ports müssen speziell geschützt werden und obliegen einem besonderen Monitoring. Die Absicherung kann z. B.

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-09-10 09:18 CEST
Interesting ports on localhost (127.0.0.1):
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
3306/tcp open  mysql
```

Abb. 8: Portscan des lokalen Servers

über eine Hardware-Firewall erfolgen. Da deren Einrichtung aber nicht immer möglich ist (z. B. wegen eines Rootservers beim Hosting-Dienstleister), sollte zumindest eine dem Betriebssystem zugehörige Firewall verwendet werden.

Schutz der Konfiguration

Tools wie z. B rkhunter oder chkrootkit prüfen auf Unixartigen Betriebssystemen periodisch auf das Vorhandensein von Schädlingen.

Angriffe auf vorhandene Schutzmaßnahmen

Bei allen bisher beschriebenen Angriffsszenarien wurde davon ausgegangen, dass bereits grundlegende Schutzmaßnahmen z. B. in Form von Firewalls, Routern/Gateways oder Anti-Malware implementiert wurden.

Der Betrieb derartiger Systeme ist mittlerweile obligat und bedarf keiner zusätzlichen Rechtfertigung. Es ist anzuraten, für alle Schutzmaßnahmen ein Monitoring- und Überwachungssystem einzurichten, um bei einem Ausfall unverzüglich reagieren zu können.

TIPP:

Im Falle von Outsourcing
Sollten derartige Systeme von einem Dienstleister betrieben werden, sollte unbedingt darauf geach-tet werden, dass sowohl der Betrieb als auch das Monitoring etc. in einem SLA punktgenau beschrieben sind.

Nur wenn alle Schutzmaßnahmen ineinandergreifen und fehlerfrei betrieben werden, ist ein grundlegendes Sicherheitsniveau aufrechtzuerhalten.

Angriffe auf die Angestellten

Der „menschliche Faktor“ stellt nach wie vor eine wesentliche Bedrohung für jedes IT-System dar. Durch gezielte Attacken auf einen Angestellten, z. B. durch Social Engineering, können grundlegende und teilweise vertrauliche Informationen schnell in falsche Hände gelangen und gezielt gegen das anzugreifende Unternehmen verwendet werden.

Nur durch iterative Sensibilisierungs- und Schulungsmaßnahmen kann diese Bedrohung eingedämmt und dadurch auf ein akzeptables Niveau reduziert werden.

Organisatorische Rahmenbedingungen

Trotz aller Schutzmaßnahmen kann ein 100-prozentiges Schutzniveau zu keiner Zeit erreicht werden. Um aber ein angemessenes Sicherheitsniveau zu erreichen und vor allem für die Zukunft aufrechtzuerhalten, sollten alle organisatorischen und technischen Schutzmaßnahmen in einem sog. Informationssicherheitsmanagementsystem (ISMS) zusammengefasst werden. Um den eigenen Erfolg zu messen, empfiehlt es sich, die Anforderungen hinsichtlich Verfügbarkeit, Performance und Reaktionszeit eindeutig zu definieren und in festen Abständen zu hinterfragen. Ein derartiges Kennzahlensystem ermöglicht eine gezielte Kontrolle der implementierten Schutzmaßnahmen und wird das unternehmensinterne ISMS auf lange Sicht weiter voranbringen und verbessern.

Die Unternehmen, die maßgeblich im Endkundengeschäft tätig sind, sollten darüber nachdenken, die sichere Abwicklung des eigenen Online-Shops

TIPP:

„Iptables“ bei Linux, „PF“ (Packetfilter) bei bsd sind mächtige Werkzeuge, um unerwünschte Zugriffe zu unterbinden. Man kann mit wenigen Zeilen Regelwerk die Ports 80/443 für alle Nutzer öffnen, den Zugriff über Port 22 (ssh) aber nur für bestimmte IPs erlauben oder sich einen VPN-Zugang erstellen, mit dem alle Verwaltungstools auch von extern bedient werden können (Fernwartung).

mit einem Gütesiegel belegen zu lassen. Durch die Kontrolle eines (externen) Dritten (= Prüfer) kann ein glaubhafter Nachweis darüber geführt werden, dass alle Geschäftstransaktionen auf einem angemessen sicheren Niveau betrieben werden. Die verschiedenen Möglichkeiten, ein Gütesiegel zu erwerben, können nachstehender Abbildung entnommen werden.

Für den Fall, dass ein derartiges Gütesiegel für den Online-Shop als nicht umfassend bzw. ausreichend genug eingestuft wird, besteht die Möglichkeit, das gesamte Unternehmen einer Sicherheitsbegutachtung zu unterziehen. Hierfür existieren in Deutschland zwei wesentliche Möglichkeiten, die in Betracht gezogen werden können:

1. Eine Zertifizierung nach der international anerkannten Sicherheitsnorm ISO/IEC 27001:2005
2. Eine Zertifizierung nach BSI-Grundschutz auf Basis der ISO 27001

Diese beiden – im Grunde konkurrierenden – Ansätze, das betriebseigene ISMS im Bereich der Informationssicherheit zu prüfen, ermöglichen es dem Unternehmen, nach bestandenem Zertifizierungsaudit gegenüber seinen Kunden einen Nachweis darüber zu führen, dass vollumfänglich alle internen und externen Prozesse einem angemes-

Abb. 9: Gütesiegel für den Online-Shop als vertrauensbildende Maßnahme in KMU noch nicht weit verbreitet [Quelle: *http://einfach.st/nuis*]

senen Schutzniveau genügen.

Auf Basis einer derartigen Bewertung wird es zukünftig sicherlich einfacher sein, einerseits Angriffen jeglicher Art zu begegnen und andererseits das Vertrauen der Kunden für sich zu gewinnen. Dies sind zwei sehr erstrebenswerte Ziele, die eine Basis für zukünftige Bemühungen schaffen sollten.

Sowohl die Erlangung eines Gütesiegels für die E-Commerce-Anwendung als auch eine Sicherheitszertifizierung sind zwei sehr komplexe Projekte, die einer eingehenden Planung und Vorbereitung bedürfen. Bis eine derartige Prüfung (= Audit) abgelegt werden kann, sollten schrittweise die internen Prozesse an den Forderungen dieser Normen und Standards ausgerichtet werden. Dies erleichtert einen späteren „Projektstart Zertifizierung" signifikant und es wird vermieden, Prozesse ein zweites Mal grundlegend überarbeiten zu müssen.

Alle hier beschriebenen Maßnahmen führen zu dem Schluss, dass nur auf einer sicheren technischen und organisatorischen Basis ein unternehmerischer Erfolg möglich ist. Dieses Bewusstsein muss sich in den Köpfen der Entscheidungsträger festsetzen, denn nur so kommt dem Thema Informationssicherheit die Rolle zu, die es innehaben muss, denn Sicherheit ist der Enabler, die grundlegende Basis, für die Umsetzung von E-Commerce-Anwendungen.

Sollten die Verantwortlichen in einem Unternehmen zu der Entscheidung kommen, dass der interne Aufwand für den Betrieb eines Online-Shops zu hoch sei, besteht die einfache Möglichkeit, einen IT-Dienstleister mit dieser Aufgabe zu betrauen. Auf Basis dieser klassischen „Make-or-buy"-Entscheidung erfolgt der Betrieb entweder intern im Unternehmen oder extern bei einem externen Unternehmen. Bei der letztgenannten Vorgehensweise muss der Geschäftspartner mit Bedacht gewählt werden, da eine Zusammenarbeit wesentlichen gesetzlichen Vorgaben entsprechen muss. Hier ist an erster Stelle die Auftragsdatenverarbeitung (ADV) zu nennen, die aus § 11 Bundesdatenschutzgesetz (BDSG) abzuleiten ist. Die damit verbundene Vorgehensweise basiert u. a. auf der Durchführung eines Sicherheitsaudits. ¶