Symantec | Website Security Solutions

Die sechs größten Gefahren für Ihre Website **und wie Sie sich schützen können**

Whitepaper

April 2013

Symantec | Website Security Solutions

Ihre Website ist nicht nur ein wichtiges Verkaufs- und Marketinginstrument, sondern auch Ihr digitales Schaufenster, mit Ihrer Marke in der Auslage. Sie haben sich die Erstellung und Suchmaschinenoptimierung Ihrer Website vermutlich einiges kosten lassen. Sie ist im wahrsten Sinne des Wortes geschäftskritisch: Die Zerstörung oder Manipulation Ihrer digitalen Schaufensterscheibe hätte katastrophale Auswirkungen auf den guten Ruf Ihres Unternehmens und zukünftige Besucherzahlen. Deshalb ist die Website-Sicherheit von so großer Bedeutung.

Darüber hinaus sind viele Verbraucher noch immer misstrauisch, wenn es um Online-Einkäufe geht. Vertrauen und Sicherheit sollten daher genauso wie Design, Hosting, Suchmaschinenoptimierung und Marketing Kernbestandteile Ihrer Website-Strategie sein. Dennoch werden diese Aspekte von vielen Unternehmen vernachlässigt – mit möglicherweise verheerenden Folgen.

Dieses Whitepaper beschreibt sechs Gefahren, denen Ihr Online-Geschäft ausgesetzt ist, und erläutert, wie Sie sich und Ihre Website schützen können.

1. Malware-Infektion von Websites

Website-Server sind Malware gegenüber genauso anfällig wie Desktop-PCs. Online-Kriminelle missbrauchen zunehmend seriöse Websites, um deren Besucher mit Malware zu infizieren: Im Jahr 2012 stellte Symantec eine Verdreifachung derartiger Angriffe fest.[1]

Besonders bedenklich ist, dass die Eigentümer der infizierten Websites oft erst auf den erfolgten Angriff aufmerksam werden, wenn ihre Website von Suchmaschinen auf die schwarze Liste gesetzt wird oder Kunden sich darüber beschweren, dass ein Unternehmen ihre Computer mit Malware infiziert hat. Der potenzielle Schaden für betroffene Unternehmen hinsichtlich der Besucherzahlen und des Kundenvertrauens ist gewaltig.

Kriminelle können einsatzbereite Malware wie das weit verbreitete Toolkit Sakura kaufen und auf der Website ihrer Opfer installieren. Die Malware durchkämmt die Computer aller Besucher der infizierten Website auf bekannte Schwachstellen und wählt die effizienteste Angriffsmethode aus, um auch die Computer der Besucher zu infizieren.

[1] Symantec Internet Security Threat Report, Ausgabe 18

[2] „Symantec Attack Signatures: Sakura Exploit Toolkit“, http://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=25761

Online-Anzeige für ein Malware-Toolkit

Doch wie gelingt es den Kriminellen, auf einer fremden Website Malware zu installieren? Auch dafür gibt es Toolkits und Anleitungen, die die Erkennung und Infizierung anfälliger Systeme erleichtern. Das Toolkit LizaMoon ermöglichte beispielsweise die Infektion von Millionen von Websites durch SQL-Injection.[3]

Andere Taktiken nutzen Schwachstellen in Content-Management-Systemen, Software für Website-Hosting oder in den Betriebssystemen von Servern aus.

Empfehlungen:

- Installieren Sie alle verfügbaren Patches und Sicherheits-Updates umgehend, so dass die Software Ihrer Website-Server immer auf dem neuesten Stand ist.
- Regulieren Sie den Zugriff auf wichtige Systeme und nutzen Sie sichere Kennwörter oder Zweifaktoren-Authentifizierung.
- Nutzen Sie die im Leistungsumfang der Symantec-Zertifikate Secure Site Pro, Secure Site mit EV und Secure Site Pro mit EV SSL enthaltene Schwachstellenanalyse und tägliche Malware-Prüfung Ihrer Website.

2. Malvertising

Eine weitere Gefahr für seriöse, durch Werbung finanzierte Websites sind als Werbung getarnte Schadprogramme, die sogenannten „Malvertisements“. Im vergangenen Jahr wurden auf diese Weise an die zehn Milliarden Anzeigenaufrufe kompromittiert.[4]

Diese Angriffe sind nur schwer erkennbar, da die Eigentümer einer Website oft weder selbst entscheiden, welche Werbung auf ihrer Website angezeigt wird, noch kontrollieren, woher die einzelnen Anzeigen stammen. Kriminelle können also nicht nur die Anzeigen seriöser Anbieter mit ihrer Malware infizieren, sondern auch ganz legitim bei einem kommerziellen Werbenetzwerk Anzeigeflächen kaufen. Darüber hinaus finden herkömmliche Verfahren zur Durchsuchung von Websites mitunter nur die Malvertisements, die während der Durchsuchung sichtbar sind.

Das bloße Aufrufen einer Webseite mit einem Malvertisement reicht zur Infektion des Computers eines Besuchers aus, auch wenn dieser nicht auf die infizierte Anzeige klickt. Wenn der Computer des Besuchers nicht ausreichend durch Anti-Malware-Software geschützt ist, steht der Infizierung nichts im Wege. Bemerkt der Benutzer die Infektion, kommt er vermutlich (und nicht ganz unberechtigt) zu dem Schluss, dass die Website, von der sein Computer infiziert wurde, gefährlich ist. Seine Meinung über das Unternehmen, dem diese Website gehört, wird darunter selbstverständlich leiden.

Empfehlungen:

- Nutzen Sie seriöse Werbenetzwerke.
- Soweit dies möglich ist, sollten Sie in Anzeigen nur statische Bilder und Text gestatten und die Ausführung von Programmcode unterbinden.
- Erwägen Sie den Einsatz des cloudbasierten Sicherheitstools Symantec AdVantage, das Malvertisements durch Echtzeitüberwachung erkennt, blockiert und zu ihrer Quelle zurückverfolgt.

[3] CNNMoney, „LizaMoon attack infects millions of websites“, http://money.cnn.com/2011/04/01/technology/lizamoon/index.htm

[4] Online Trust Alliance, letzter Zugriff am 12. März 2013, https://otalliance.org/resources/malvertising.html

3. Blockierung durch Suchmaschinen

Suchmaschinen wie Google und Bing durchsuchen Websites nach Malware und setzen infizierte Websites auf eine schwarze Liste. Das bedeutet, dass diese Websites nicht mehr in Suchergebnissen erscheinen, wodurch die Besucherzahlen drastisch sinken. In manchen Browser können Suchmaschinen auch dann mit einer Warnmeldung auf die Malware-Infektion hinweisen, wenn ein Besucher die URL der Website direkt eingibt.

Ein Unternehmen, dessen Website von Suchmaschinen auf die schwarze Liste gesetzt wird, büßt nicht nur Besucher, sondern womöglich auch seinen guten Ruf ein. Aufwendige und teure Bemühungen zur Suchmaschinenoptimierung können dadurch völlig zunichtegemacht werden. Selbst nach der Behebung des Problems werden Websites nicht immer sofort von allen Suchmaschinen von der schwarzen Liste gelöscht und wieder in die Suchergebnisse aufgenommen.

Suchmaschinen setzen auch Websites auf die schwarze Liste, deren Betreiber tatsächlich oder anscheinend die vom Suchmaschinenbetreiber aufgestellten Richtlinien missachtet und versucht, die Website in den Suchergebnissen nach vorn zu lancieren. Google veröffentlicht hilfreiche Richtlinien (in englischer Sprache) zu guten und schlechten Praktiken, darunter auch detaillierte Beschreibungen von Methoden, die zur Blockierung von Websites führen.[5]

Google sperrt Berichten zufolge jeden Tag 6000 Websites.[6] Selbst die Websites renommierter Unternehmen wie TechCrunch und New York Times wurden schon auf die schwarze Liste gesetzt, weil sie versehentlich infizierte Anzeigen enthielten.[7]

- Schützen Sie Ihre Website also wie oben beschrieben vor Malware und Malvertisements.
- Vermeiden Sie dubiose Methoden zur Suchmaschinenoptimierung.
- Melden Sie sich für die Webmaster-Tools von Google und Bing an, um E-Mail-Benachrichtigungen zu erhalten, falls Ihre Website auf die schwarze Liste gesetzt wird.

4. Sicherheitswarnungen und abgelaufene Zertifikate

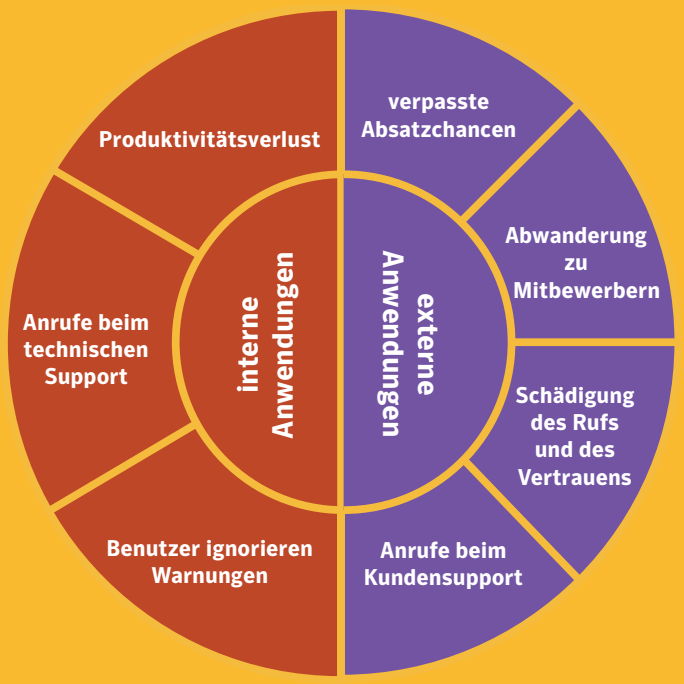
Stellen Sie sich vor, Sie seien ein Kunde, der sich gerade zu einem Online-Kauf entschlossen hat. Doch wenn Sie auf die Schaltfläche „Zur Kasse gehen“ klicken, erscheint eine Sicherheitswarnung, weil ein SSL-Zertifikat abgelaufen ist. An dieser Stelle werden Sie den Kauf vermutlich abbrechen. Ob Sie später zu diesem Anbieter zurückkehren ist fraglich. Das gleiche gilt auch für Ihre Kunden: Wenn Sie Online-Anwendungen und -Services mit SSL-Zertifikaten schützen und diese dann nicht rechtzeitig erneuern, schwindet das Kundenvertrauen in Ihr Serviceangebot schnell.

TheVerge.com

[5] Google Webmaster Guidelines: http://support.google.com/webmasters/bin/answer.py?hl=en&answer=35769

[6] http://mobile.businessweek.com/articles/2012-05-07/protect-your-companys-website-from-malware

[7] „Google Flags Ad Network Isocket for Alleged Malware; chrome blocks TechCrunch, Cult of Mac, others (Updated)“, The Next Web, letzter Zugriff am 12. März 2013, 12 March 2013, http://thenextweb.com/google/2013/01/15/google-flags-ad-network-isocket-for-alleged-malware-chrome-blocks-techcrunch-cult-of-mac-others/



Die Folgen von unerwartet abgelaufenen SSL-Zertifikaten und Warnmeldungen im Browser

Die Verwaltung von SSL-Zertifikaten ist eine ernstzunehmende Herausforderung für alle Unternehmen, die mehr als nur einige wenige Zertifikate und Server besitzen. Wer ist für den Kauf und die Erneuerung der Zertifikate verantwortlich? Wie wird über die Zertifikate Buch geführt? Wie kann der unautorisierte Kauf von Zertifikaten verhindert werden? Wie wird sichergestellt, dass alle Zertifikate rechtzeitig erneuert werden?

Die Zentralisierung der Zertifikatsverwaltung ist nicht nur empfehlenswert, sondern unbedingt erforderlich, um das unbemerkte Ablaufen bzw. die überstürzte Erneuerung von Zertifikaten in letzter Minute zu vermeiden.

Empfehlungen:

- Erstellen Sie eine Bestandsliste aller Zertifikate in Ihrem Unternehmen, so dass Sie genau wissen, welche Zertifikate Sie besitzen, wer sie ausgestellt hat und wann sie ablaufen.
- Fassen Sie alle Zertifikate in einer einzigen Verwaltungsstruktur zusammen.
- Mit Symantec® Managed PKI for SSL erhalten Sie ein cloudbasiertes Toolkit zur Zertifikatsuche und -verwaltung. Darin ebenfalls enthalten ist die tägliche Durchsuchung Ihrer öffentlich zugänglichen Webseiten nach Malware.
- Nutzen Sie automatische Warnmeldungen bzw. Kalendereinträge zur rechtzeitigen Erinnerung an ablaufende Zertifikate. Symantec teilt Ihnen einen persönlichen Account Manager zu, der Sie bei all diesen Aufgaben unterstützt.

5. Nachahmung Ihrer Marke (Phishing)

Kriminelle missbrauchen bekannte Namen und Marken, um Verbraucher zur Preisgabe vertraulicher Daten bzw. zur Installation von Malware zu bewegen. Dazu fälschen sie häufig die Websites renommierter Unternehmen. Das bekannteste Beispiel dieser „Phishing“ genannten Angriffsform sind von Betrügern eingerichtete Websites, die angeblich Banken gehören und auf denen Verbraucher zur Eingabe ihrer Bank- bzw. Kreditkartendaten und Kennwörter aufgefordert werden.

In einer neueren Masche nutzen Phisher soziale Medien, um ihre Opfer auf gefälschte Websites zu locken. Dort wird versucht, sie mit Versprechen auf einen Gewinn wie einen Gutschein oder ein Handy zur Preisgabe vertraulicher Daten, etwa ihrer Anmeldedaten für soziale Netzwerke, zu bewegen.

Typischer Täuschungsversuch in einem sozialen Netzwerk

Gefälschte Website mit Scheinumfrage

Solche Praktiken machen es unerlässlich, dass seriöse Unternehmen die Fälschung ihrer Website und das Kapern ihrer Marke(n) unterbinden, indem sie die Authentizität ihrer echten Websites schützen und deutlich sichtbar hervorheben. Ein SSL-Zertifikat mit Extended Validation bewirkt, dass die Adressleiste des Browsers grün hinterlegt und der Firmenname in der Adressleiste angezeigt wird. Dadurch wird die Echtheit der Website bestätigt. Der Prozess für die Ausstellung eines SSL-Zertifikats mit Extended Validation und die Authentifizierung umfasst die eingehende Überprüfung, ob das Unternehmen der rechtmäßige Eigentümer der Website ist. Dadurch wird die Fälschung ungleich schwieriger.

Viele führende Unternehmen, wie beispielsweise Twitter und Facebook, setzen von der An- bis zur Abmeldung SSL ein, um die Sicherheit ihrer Websites unter Beweis zu stellen. Diese Maßnahme wird auch als Always-On SSL bezeichnet. Das bedeutet, dass alle Seiten verschlüsselt werden, nicht nur Kassenseiten und Seiten, auf denen Benutzer vertrauliche Daten eingeben sollen. Ein wichtiger Vorteil von Always-On SSL ist, dass Besucher auf jeder Seite daran erinnert werden, dass sie sich auf einer geschützten Website befinden, der sie vom ersten Klick an vertrauen können.

Empfehlungen:

- Nutzen Sie SSL-Zertifikate mit Extended Validation, um die Echtheit Ihrer Website zu belegen und Kunden zu bestätigen, dass sie sich nicht auf einer gefälschten Website befinden.
- Erwägen Sie den Einsatz von Always-On SSL mit Symantec Secure Site Pro SSL-Zertifikaten, um deutlich sichtbar zu signalisieren, dass der gesamte Datenverkehr zwischen Ihrer Website und dem Browser der Benutzer verschlüsselt wird und sicher ist.

6. Sicherheitsbedenken der Kunden

Angesichts der Menge und Vielfalt von Betrugsversuchen im Internet ist es nicht verwunderlich, dass viele Verbraucher Websites nur mit äußerster Vorsicht begegnen und nach Anzeichen für deren Sicherheit Ausschau halten. Hinzu kommt, dass ihnen mit etwa 634 Millionen Websites eine enorme Auswahl zur Verfügung steht.[8] Besucher beurteilen Websites daher sehr schnell: Sie verbringen im Schnitt weniger als eine Minute[9] auf einer Website; die ersten zehn Sekunden sind ausschlaggebend. Deshalb muss die Sicherheit einer Website auf den ersten Blick erkennbar sein.

Mit Vertrauensmarken wie dem Norton Secured-Siegel können Sie Ihren Besuchern zeigen, dass Sie die Sicherheit ernst nehmen. Eine Vertrauensmarke signalisiert auch, dass Ihre Website regelmäßig auf Malware und Schwachstellen untersucht wird. Diese vertrauenschaffende Maßnahme zahlt sich aus: In einer aktuellen Umfrage gaben 94 Prozent der Befragten an, dass sie einen Einkauf mit größerer Wahrscheinlichkeit fortsetzen, wenn sie eine Vertrauensmarke sehen.[10]

Mit dem Vertrauensaufbau können Sie schon beginnen, bevor Ihre Website aufgerufen wird. Nicht von Suchmaschinen blockiert zu werden, ist natürlich eine Grundvoraussetzung, aber mit Symantec Seal-in-Search™ können Sie Ihre Website in den Suchergebnissen hervorheben und potenziellen Besuchern zeigen, dass diese sicher ist. Symantec Seal-in-Search™ gehört ebenso wie das Norton Secured-Siegel zum Funktionsumfang aller Symantec SSL-Zertifikate.

Empfehlung:

- Signalisieren Sie Ihren Besuchern auf der Website selbst und, wenn möglich, in Suchergebnissen, dass Ihre Website sicher und vertrauenswürdig ist und regelmäßig überprüft wird.

[8] Netcraft December 2012 Web Server Survey: http://news.netcraft.com/archives/2012/12/04/december-2012-web-server-survey.html.

[9] Jakob Nielsen's Alertbox: How Long do users stay on web pages, September 12, 2011: http://www.nngroup.com/articles/how-long-do-users-stay-on-web-pages/.

[10] Online-Verbraucherumfrage von Symantec in den USA im Februar 2011.

Wählen Sie den richtigen Partner

Online-Kriminalität bedroht nicht nur den guten Ruf, sondern auch das Überleben Ihres Online-Geschäfts. Daher war die Auswahl eines bekannten, renommierten Sicherheitspartners noch nie so wichtig wie heute. Symantec sichert bereits über eine Million Webserver weltweit[11] mit einem ganzheitlichen Ansatz, der nicht nur SSL-Zertifikate, sondern auch die Verschlüsselung, Zertifikatsverwaltung, Überprüfung auf Malware und Schwachstellen, Vertrauensmarken und andere Maßnahmen umfasst. Das Unternehmen stellt hohe Anforderungen an seine hauseigene Sicherheit: Die Authentifizierungsverfahren werden vom Wirtschaftsprüfungsunternehmen KPMG überprüft und die Rechenzentren für die SSL-Infrastruktur sind nach militärischen Maßstäben gesichert. Wenn es um Sicherheit und Online-Vertrauen für Ihre Website geht, ist Symantec der richtige Partner.

[11] Einschließlich Partner- und Tochterunternehmen sowie Vertriebspartnern von Symantec.