profihost

E-Commerce. Cloud. Hosting.

Datensicherheit und Datenschutz im Internet

Version 1.5. vom 27.5.2015

Whitepaper von Fabian Kösters, Online-Redakteur bei der Profihost AG
Technisches Lektorat: Andreas Büggeln, 2nd Level Support

Inhaltsverzeichnis

Profihost AG
Expo Plaza 1 · 30539 Hannover
Telefon +49 511 5151 8181
Telefax +49 511 5151 8282
info@profihost.com
www.profihost.com

Commerzbank AG
BLZ 27040080 · Konto 6511646
Swift/BIC COBADEFFXXX
IBAN DE20270400800651164600
USt.-Ident.-Nr. DE813460827
Steuer-Nr. 2325 271 05518

Vorstand Cristoph Bluhm
Sebastian Bluhm
Stefan Priebe
Vorsitzender des Aufsichtsrats
Prof. Dr. iur. Winfried Huck
Amtsgericht Hannover · HRB 202350

Angriffe auf Server und Datenübertragung im Internet

Die Methoden, mit denen die Täter versuchen, in fremde Systeme einzudringen, sind sehr unterschiedlich. Hier seien drei verschiedene Vorgehensweisen genannt, mit denen sich Angreifer Schwachstellen der betroffenen Webseiten oder Server zunutze machen:

Sicherheitslücken

In der ersten Variante werden bestehende Sicherheitslücken innerhalb bestimmter Webanwendungen ausgenutzt, um sich unbefugten Zugang zu verschaffen. Das sind zum Beispiel Sicherheitslücken in verwendeter Software wie WordPress, Typo3, phpBB, etc. Insbesondere die Skriptsprache PHP (u.a. WordPress, Joomla!) ist anfällig für Angriffe dieser Art. Aber auch andere Elemente und Programme, die im Internet eingesetzt werden, ermöglichen unter Umständen unbefugten Zugriff. Besonders brisant wird es dann, wenn Software betroffen ist, die eigentlich für eine erhöhte Datensicherheit sorgen sollte, wie es etwa im April 2014 mit dem Verschlüsselungstool OpenSSL geschehen ist.

Entwickler von Webanwendungen versuchen, gefundene oder neue Sicherheitslücken, die sich etwa durch ein großes Update mit vielen neuen Möglichkeiten in der Webanwendung ergeben haben, durch entsprechende Updates zu beheben. So wird zum Beispiel durch das Blogsystem WordPress in regelmäßigen Abständen ein automatisches Systemupdate realisiert.

Zugangsdaten werden ausgespäht

In Zusammenhang mit bestehenden und den Angreifern bekannten Sicherheitslücken werden häufig Zugangsdaten zu Webseiten oder Serversystemen ausgespäht, um die Rechner und Programm dann gezielt für illegale Zwecke nutzen zu können. In diesem Zusammenhang kommt es aber auch häufig vor, dass die Täter sich die Unwissenheit der Nutzer zunutze machen und Zugangsdaten mithilfe von Viren oder Trojanern ausspähen, die diese dann weitergeben oder das betroffene System unbemerkt kapern und nutzen, etwa um Spam zu versenden oder den Virus weiter zu verbreiten.

Zu einfache Passworte

Nach wie vor sind auch zu einfache Passworte eine Möglichkeit, sich unbefugt Zugriff auf fremde Accounts und Systeme zu verschaffen. Insbesondere bei Anwendungen, die von vielen Nutzern mit unterschiedlichem Problembewusstsein genutzt werden, ist dies häufig ein Problem. Passworte wie „test123", Vornamen, Haustiernamen und so weiter sind ein ungenügender Schutz vor Angriffen. Mithilfe von langen Passwortlisten werden die einzelnen, einfachen Passworte so lange ausprobiert, bis eins davon passt.

Je weniger „natürlich" und je länger ein Passwort ist, desto schwieriger wird es, dieses zu knacken. Sogenannte „Brute Force Attacken" verzichten jedoch sogar auf „bekannte" Passworte und generieren zufällig erstellte Zeichenketten, um so in ein System einzudringen – wobei selbstverständlich auch „echte" Worte generiert werden.

Hier kann jedoch die Länge der verwendeten Kennwörter wiederum Abhilfe verschaffen: Je länger die Zeichenkette ist, die für ein Passwort genutzt werden kann, desto höher wird die Zahl der möglichen Passworte. Viele Anwendungen lassen nach einer bestimmten Anzahl von Versuchen zumindest für eine Weile keine weiteren Versuche zu. So wird für einen derartigen Angriff nicht nur je nach Passwortlänge mehr Rechenleistung, sondern auch mehr Zeit benötigt. Daher werden „Brute Force Attacken" häufig mit Hilfe von sogenannte Botnetzen durchgeführt. Hierbei versucht eine Vielzahl von häufig gekaperten Rechnern einen Zugang zu bekommen. So erkennt das angegriffene System nicht unbedingt, dass es sich um einen Angriff handelt bzw. es wird schwieriger, zwischen den Fehlversuchen der einzelnen Angreifer und den Zugriffen tatsächlicher Nutzer zu unterscheiden. So ist der Aufbau eines derartigen Botnetzes auch möglicher Zweck eines Angriffs, z.B. mittels Trojaner.

Sinn und Zweck der Angriffe

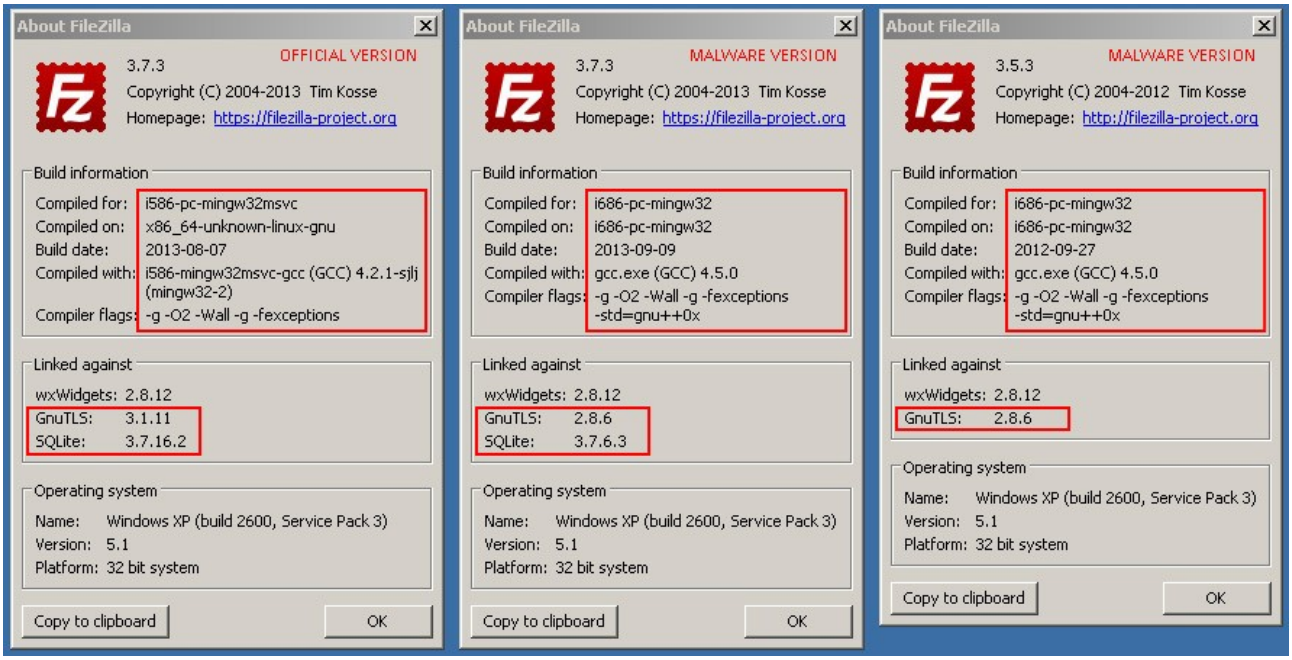
Wozu aber machen sich Angreifer eigentlich die Mühe, in Accounts einzudringen und Webseiten und Server auszuspionieren? Hier gibt es ein paar „Hauptanwendungsgebiete“:

- Backdoors
- E-Mail Spam Versand
- Phishing-Seiten etablieren
- Botnetze betreiben
- Spionage und Sabotage
- Missbrauch von Kundendaten
- Just 4 Fun

Häufig ist es so, dass sich die unterschiedlichen Arten von Attacken bedingen oder ergänzen. Um z.B. einen Ausspäh-Angriff zu starten wird ein Botnetz genutzt, welches vorher durch den Einsatz von Schadsoftware (Trojaner) etabliert wurde.

Backdoors

Mit einer sogenannten Backdoor (Hintertür) nutzen Angreifer eine von den Entwicklern übersehene oder nach Abschluss einer internen Testphase nicht geschlossene Sicherheitslücke aus. So können sie etwa in interne Bereiche eindringen, wo möglicherweise dann weitere Zugänge geöffnet werden können. Backdoors werden auch durch installierte Trojaner realisiert, bei welchen die Nutzer unwissentlich Schadsoftware installiert haben. Diese Trojaner werden beispielsweise über Botnetze via Spam versendet oder auf gekaperten Seiten zum Download angeboten. So wurde z.B. die FTP-Software FileZilla manipuliert und auf eigens dafür eingerichteten Seiten verbreitet. Selbst für versierte Nutzer war es nicht möglich, auf Anhieb einen Unterschied zwischen der schädlichen und der sauberen Version zu erkennen:



Erkennbar war die infizierte Version nur an einer anderen Zahl im Fenster „About" (Menü „Hilfe" → „Über"). Hier hatten die Hacker eine andere Programmversion zum erstellen der fertigen Software benutzt, nämlich GnuTLS 2.8.6 statt 3.1.11 – tw. fehlte diese Angabe bei infizierten Programmen auch ganz. (Bild: Avast Antivirus)

Da im FileZilla häufig Passworte zu Servern gespeichert werden, waren die schadhaften Versionen wohlmöglich eine ergiebige Quelle für das Aushorchkommando. Die Datendiebe konnten sich so direkt und ohne Umwege über Backdoors auf die Server einloggen.

Schon beim herunterladen von Software sollte deshalb auf vertrauenswürdige Seiten zurückgegriffen werden. Auch aus diesem Grund ist vom Einsatz von auf zweifelhaften Wegen besorgten gecrackten Programmen zu warnen: Diese stammen häufig von denselben Leuten, die auch Webseiten kapern. Wer die Kosten für teure Software scheut, findet oftmals eine kostenlose Variante aus dem Open Source-Bereich, die im Leistungsumfang meist Ähnliches bietet wie das kostenpflichtige Programm. Oft bietet der Hersteller auch Prüfsummen an, um die Integrität des heruntergeladenen Programms prüfen zu können. Weicht diePrüfsumme (engl. „Checksum") des Herstellers von der heruntergeladenen Software ab, ist etwas nicht in Ordnung!

E-Mail Spam Versand

Eines schönen Tages fand ich in meinem Postfach eine Mail, in welcher zum Preis von ca. 100.000 US$ eine russische Schrottpresse angeboten wurde. Vielen Lesern werden ähnliche Merkwürdigkeiten widerfahren sein, denn neben beliebten Medikamenten und gefälschten Handtaschen wird so ziemlich alles mit Spam-E-Mails beworben. Dafür nutzen die Absender natürlich nicht die eigene, zurückverfolgbare Adresse, sondern bedienen sich ausgedachter oder irgendwo im Netz gefundener Absenderadressen. Die E-Mails selber werden häufig über gekaperte Mailserver oder auch nur Postfächer verschickt. Mitte April wurde zum Beispiel bekannt, dass in Deutschland ungefähr 3 Millionen Passworte von E-Mail Accounts aufgetaucht waren. Von diesen Accounts aus lassen sich einerseits E-Mails verschicken, die einen vertrauenswürdigen Absender aufweisen, andererseits werden die evtl. gespeicherten E-Mail Adressbücher genutzt, um sie in Listen zu speichern und zum Beispiel an zwielichtige Schrottpressenhändler zu verkaufen. Neben dem tatsächlichen Verkauf von mehr oder weniger koscheren Waren tauchen auch immer wieder E-Mails auf, die einen unverhofften Geldsegen versprechen. Die Geschichte, die hier erzählt wird, folgt häufig einem Schema wie dem Folgenden: In einem für die Empfänger exotischen Land ist jemand, oftmals ein vorgeblicher Staatsdiener oder Bankangestellter, durch einen glücklichen Zufall zu Geld gekommen. Um dieses Geld jedoch erlangen zu können, fehlt noch ein letztes kleines Puzzleteil: Es muss beispielsweise eine Bürgschaft oder Ähnliches übernommen werden. Der Sender verspricht dem Empfänger nun einen gehörigen Anteil an dem Vermögen. Dazu muss eine Gebühr überwiesen werden, die eine beträchtliche Summe darstellt, im Vergleich zum erhofften Gewinn aber nur eine kleine Investition bedeutet. Zweck der E-Mail ist selbstverständlich nur, die überwiesenen „Gebühren" zu erhalten, außer einer mehr oder weniger guten Geschichte haben die Absender nichts weiter anzubieten.

Natürlich ist die Frage berechtigt, wer auf eine derartige Räuberpistole herein fällt. Diese E-Mails werden jedoch nicht selten an 100tausende von Empfängern überall auf der Welt verschickt, so dass nur eine geringe Anzahl an Menschen die sich dadurch täuschen lassen, genügt, damit sich dieses Geschäft lohnt. Immer noch werden tägliche neue E-Mail Accounts aufgemacht, die Menschen gehören, die noch nie E-Mail geschrieben haben. Wer jetzt besonders leichtgläubig ist, den mag eine derartige Offerte vielleicht locken. Und der Aufwand zahlt sich, wie bereits erwähnt, bereits durch einige wenige Erfolge schon aus.

In meinem Spam-Ordner befinden sich zur Zeit E-Mails mit diversen Trojaner, einige Aktienfonds-Empfehlungen mit Geld-Zurück-Garantie sowie Hinweise auf bewährte Methoden zur Steigerung der körperlichen Leistungsfähigkeit. Eine GmbH mit .de-Adresse, die ich selbst in die Spam-Absender einsortiert habe, weist auf eine ihrer Veranstaltungen hin. Ich hatte mich jedoch nie zuvor für diesen Newsletter angemeldet. Leider wissen manche Firmen immer noch nicht, dass auch das einfache Versenden von Werbe-Mails ohne Einwilligung des Empfängers als Spam gewertet wird, obschon kriminelle Energie hier vermutlich in den wenigsten Fällen die Ursache sein dürfte.

Phishing-Seiten etablieren

Eine E-Mail im Spam-Ordner weist mich darauf in, dass mit meiner Kreditkarte etwas nicht stimmt …

Betreff: Reaktivieren Verifizierte by Visa/Mastercard Service
Dateianhang: Reaktivieren-Visa-Mastercard.html

```
Sehr geehrter Kunde,

Unauthorized Kartenzahlung Versuch mit Ihrer Kreditkarte-Konto verknüpft wurde
vor kurzem erhalten haben. Um Ihnen vor weiteren nicht autorisierten Zahlung
Versuche zu schützen, haben wir nur begrenzten Zugang zu Ihrem Kartenkonto.
Bitte nehmen Sie sich eine Minute Zeit, um die Details unten bewerte und
welche Schritte Sie benötigen, um zu nehmen entfernen Sie die Grenzen.

Fall-ID-Nummer: V/M-1756-946-116

Was als nächstes zu tun
-----------------------------------

Achtung: Sie sind Verpflichtet, downloaden Form zu dieser E-Mail ange und
öffnen Sie sie in einem Web-Browser. Einmal geöffnet, werden Sie mit Schritten
zu Ihrem Kartenkonto wieder her gestellt werden.
Wir bitten um Ihr Verständnis, da wir die Arbeitssicherheit auf Ihr Konto.

-----------------------------------
Weitere Details
-----------------------------------

Es gibt keine weiteren Details fur diese Transaktion zu diesem Zeitpunkt.


Mit freundlichen Grüßen,
MasterCard® SecureCode / Verified by Visa
```

Die beigefügte Datei wird beim öffnen vermutlich auf eine Seite leiten, auf der ich zur Eingabe meiner PIN und TAN o.ä. aufgefordert werde, mit welcher die Absender dann von meiner *„Visamastercard"* Geld transferieren. Auch wenn diese plumpe Fälschung auf den ersten Blick erkennbar ist, so existieren doch Sendungen dieser Art, die sich sehr genau an den Formulierungen und der Gestaltung der nachgeahmten Institutionen orientieren. Auch die genutzten Webseiten sind in diesen Fällen häufig sehr exakte Fälschungen, die sich oft nur in kleinen Details von den Originalen unterscheiden. Hierbei handelt es sich um sogenannte „Phishing"-Seiten, mit denen wertvolle Kundendaten „gefischt" werden sollen. Sind diese erst einmal im Netz der Fischer gelandet, so bemerken die Betrogenen ihren Irrtum sehr schnell beim Blick aufs Konto oder die Kreditkartenabrechnungen. Um solche Webseiten über einige Zeit betreiben zu können, werden Seiten oder ganze Server gekapert, auf welchen dann die Phishing-Seite installiert wird.

Grundsätzlich gilt hier, und alle seriösen Banken, Versicherungen und Kreditkartenanbieter betonen dies immer wieder: Kunden werden niemals nach TAN oder PIN gefragt, wenn Sie sich nicht selber einloggen um z.B. Überweisungen zu tätigen. Nicht in E-Mails, nicht am Telefon und auch nicht per Post. Wenn tatsächlich einmal eine gesperrte Karte wieder freigegeben werden muss, was ja durchaus vorkommt, so geschieht dies auch im digitalen Zeitalter ohne die Eingabe einer PIN, sondern in aller Regel durch Identifikation mit Ausweispapieren in einer Filiale oder mit einem geheimen Passwort für den Kundenservice am Telefon (so beispielsweise bei der Packstation).

Botnetze betreiben

Auf einem gehackten Server lassen sich dauerhaft aktive Programme, sog. Bots, installieren, welche das Netz z.B. nach leicht zu knackenden Webseiten abgrasen. Eine vernetzte Gruppe derartig manipulierter Internet-Rechner ist ein Botnetz (engl. Botnet). Auch Spam-Mails werden über solche Botnetze verschickt, DoS- und DDoS-Attacken gesteuert oder durch automatisierte Bannerklicks massenhaft bezahlter Traffic generiert. Durch die Ansteuerung der Banner über verschiedene Rechner mit unterschiedlichen IP-Adressen fällt die Automatisierung und der Betrug nicht sofort auf, obschon es Überwachungsmöglichkeiten gibt, die in derartigen Klick-Wellen typische Muster zu erkennen vermögen. Bots fallen auch auf infizierten Rechnern (sog. *Zombies*) nicht unbedingt auf. Sie können hier auf datenkritische Programme wie etwa Browser etc. zugreifen, um so private Daten zu kopieren und zu betrügerischen Zwecken zu nutzen. Eine sichere SSL-Verbindung wird z.B. ausgehebelt, wenn die Sicherheitslücke auf dem eigenen Rechner besteht. Die meisten Bots lassen sich von außen steuern und veranlassen, eingesammelte Daten zu versenden.

Im „Prolexic Q2 2014 Global DDoS Attack Report"[1] wird für das zweite Quartal 2014 ein Anstieg der DDoS-Attacken um 22% festgestellt – im Vergleich zum 2. Quartal 2013. Die durchschnittliche Bandbreite, die attackierende Botnetze nutzen, ist um 72% angestiegen, die Dauer der Attacken ging hingegen um die Hälfte zurück (54%). Im Vergleich zum ersten Quartal 2014 zeigt sich in allen Bereichen jedoch ein leichter bis sehr starker Rückgang, so das hier konstatiert werden kann, dass die Zahl der Attacken auf hohem Niveau schwankt.

1 http://www.akamai.com/html/about/press/releases/2014/press-072214.html [5.8.2014]

Spionage und Sabotage

Wie im Abschnitt zu den Botnetzen bereits erwähnt, können gehackte Seiten oder Server zu Zwecken der Spionage und Sabotage genutzt werden. Diese Möglichkeit nutzen kriminelle Vereinigungen ebenso wie Geheimdienste. Neben der allseits geschmähten NSA schnüffelt z.B. der französische Geheimdienst nach Wirtschaftsgeheimnissen[2] , vermutlich aber auch viele weitere nationale Nachrichtendienste, die der eigenen Wirtschaft den Wissensvorsprung der Konkurrenz aus dem (auch befreundeten) Ausland näher zu bringen versuchen. Aber auch von Unternehmen selber wird Spionage betrieben[3], zumeist jedoch mit eher klassischen Methoden wie dem Einschleusen von Detektiven, aushorchen von Mitarbeitern und der geschickten Kombination frei zugänglicher Informationen, etwa aus Geschäftsberichten oder Case-Studies, die zur PR-Zwecken eingesetzt werden.

Bei Sabotageakten sind insbesondere die Methoden DoS und DDoS hervorzuheben, mit denen Server oder Internetseiten blockiert werden können. Vereinfacht gesprochen, sendet dabei eine Vielzahl von einzelnen Rechnern, die z.B. in einem Botnetz zusammengefasst sind, sehr viele Anfragen an den Server. Der Bedarf an Rechenleistung oder Bandbreite reicht nicht aus, um das Anfragevolumen zu bewältigen und der Server ist ab einem bestimmten Zeitpunkt nicht mehr in der Lage, überhaupt eine Seite auszuliefern. Durch die Verteilung der Anfragen auf viele unterschiedliche Rechner mit unterschiedlichen IP-Adresse ist es nur schwer möglich, das Botnetz als Ganzes zu blockieren. Aber auch ein solcher Blockade-Mechanismus könnte überlastet werden. *„Das Content Delivery Network Akamai stellte eine Steigerung der Angriffe vom vierten Quartal 2013 zum ersten Quartal 2014 um 39% fest, zum Vorjahresquartal sind es 47%."*[4] DoS steht hier für „Denial of Service", DDoS für „Distributed Denial of Service", also ein über ein Netzwerk verteilter Angriff auf eine Webseite oder einen Server. Eine besondere Form ist die DRDos-Attacke, was für Distributed Reflected Denial of Service steht. Hierbei wird ein regulärer Internetdienst, etwa ein DNS-Server, attackiert. Dazu wird jedoch als gefälschte Anfrage-Adresse die IP des eigentlichen Zielrechners angegeben. Die Antworten des Dienstes an das scheinbar anfragende Opfer der DRDoS-Attacke führen dann an dieser Stelle zum Absturz einer Awendung oder eines ganzen Servers. Zahlreiche Server wurden zwischenzeitlich bereits mit Updates versorgt um diese Art von Angriff nicht mehr zu ermöglichen. So werden DRDoS Attacken seltener. Derartige Angriffe werden genutzt, um die Webseiten missliebiger Konkurrenten auszuschalten, oder um unerwünschte Informationen oder Meinungen zu unterbinden. So wurde bspw. die Nachrichtenseite von Al-Jazeera im Jahre 2003 durch einen Angriff lahmgelegt, bei welchem der Nameserver attackiert wurde, der für die Domain des Nachrichtensenders zuständig ist[5].

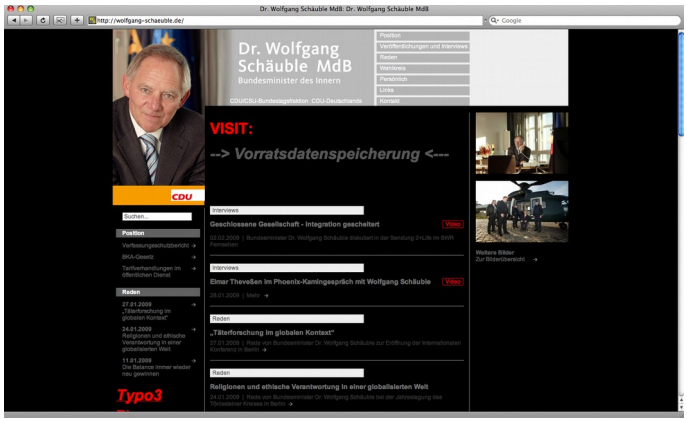
2 http://www.zeit.de/2014/08/frankreich-industriespionage-wirtschaftsspion [24.7.2014]
3 http://www.pcwelt.de/news/Schnueffeln-weit-verbreitet-290357.html [24.7.2014]
4 http://de.wikipedia.org/wiki/Denial_of_Service#DDoS_und_Botnetze [24.7.2014]
5 http://www.computerweekly.com/news/2240050118/Al-Jazeera-sites-still-down-after-DDOS-attack [24.7.2014]

Missbrauch von Kundendaten

Welchen Zwecken der Missbrauch von Kundendaten dient, ist offensichtlich: Mit gestohlenen Kontozugangsdaten lässt sich z.B. Geld überweisen oder es werden Einkäufe per Kreditkarte getätigt. Gestohlene E-Mail Zugänge werden genutzt, um Spam zu versenden und dadurch möglicherweise bei Freunden, Geschäftspartnern etc. mit der vertrauenserweckenden, weil bekannten E-Mail Adresse, ebenfalls Schaden anrichten zu können. Hier werden weitere Schadprogramme verschickt, die dann von den Betroffenen unwissentlich ausgeführt werden und den Rechner ebenfalls infizieren. So verbreiten sich E-Mail Viren, die dann zur Etablierung z.B. eines neuen Botnetzes führen. Aber auch mit gekaperten Accounts für Twitter oder Facebook lässt sich mit einem ähnlichen Mechanismus, viel Schaden anrichten. Der Empfänger klickt sorglos auf den gesendeten Link oder das Video, nur um dann auf eine Seite geleitet zu werden, die den eigenen Rechner attackiert und den Account zu knacken versucht.

Just 4 Fun

Insbesondere sog. Skriptkiddies nutzen frei erhältliche, wenn auch illegale Programme, um sich aus Spaß oder Neugierde Zugang zu fremden Rechnern zu verschaffen. Das Ende der 90er Jahre des letzten Jh. kursierende Back Orifice[6], mit welchem sich ein komplettes Windows95-Betriebssystem fernsteuern ließ, ist ein Paradebeispiel eines solchen weit verbreiteten Programms. Die auch als Fernwartungs-Werkzeug zu nutzende Anwendung konnte verdeckt ausgeführt werden, so dass sich die Betroffenen oftmals nicht darüber im Klaren waren, dass Ihr PC gekapert wurde. Das Programm ließ sich über infizierte Dateien verbreiten. Mit ihm konnte auf den betroffenen Rechnern alles getan werden, was der Nutzer am Arbeitsplatz ebenfalls tun konnte – inklusive dem Öffnen und Schließen der CD-ROM Schublade, eine vergleichsweise harmlose, wenn auch eindrucksvolle Funktion.



Gehackte Seite von Dr. Wolfgang Schäuble, 2009

Trojaner und andere Schadsoftware lassen sich mittlerweile auch im Internet mittels Trojaner-Baukasten zusammenklicken, die für ca. 30 $ zu erwerben sind. Da Virensoftware derartige „Malware von der Stange" schnell erkennen kann, installieren viele dieser Programme einen sog. *„Dropper"*[7], der die jeweils neueste Version des Schädlings nachlädt. Auch deshalb ist es wichtig, die Virensoftware am besten mit täglichen Updates auf dem neuesten Stand zu halten.

Andere Programme ermöglichen beispielsweise den Zugriff auf eingebaute Webcams und Mikrophone. Neben dem Eindringen in Arbeitsplatz-Rechner oder private PC werden auch Internetseiten „Just 4 Fun" gehackt. Häufig wird hier eine Persiflage auf die gehackte Seite eingespielt. Dies geschieht auch bei schlecht gesicherten Politikerseiten. So wurde 2009 z.B. ausgerechnet die Seite des damaligen Bundesinnenministers Dr. Wolfgang Schäuble gehackt[8], um auf die Debatte um die Vorratsdatenspeicherung aufmerksam zu machen. Derartige Angriffe finden aber auch ohne einen offensichtlichen Hintergrund statt – und sind oftmals vermeidbar. Wie man Server und Webseiten sowie die darauf installierten Webanwendungen möglichst effektiv gegen unbefugtes Eindringen und Manipulationen schützt, wird im folgenden Abschnitt beschrieben.

6 http://de.wikipedia.org/wiki/Back_Orifice – Anm.: Wir wissen, dass es sehr viele neuere Beispiele für Rootkits gibt. Dieses ist der Nostalgie des Autors geschuldet ;-)
7 http://www.focus.de/digital/computer/chip-exklusiv/tid-7867/it-sicherheit_aid_137679.html [9.4.2015]
8 Quelle Screenshot: http://saschalobo.com/2009/02/11/wolfgang-schaubles-website-gehackt/ [17.11.2014]

Gegenmaßnahmen

Die hier aufgeführten Gegenmaßnahmen beziehen sich vorwiegend auf Attacken und Manipulationsversuche an Internetseiten, Servern und Webanwendungen. Sie sind in ähnlicher Form natürlich auch auf private Rechner oder Rechner am Arbeitsplatz umsetzbar. Virenscans, Backups wichtiger Daten, sichere Passworte und vorsichtiger Umgang mit E-Mails sind auch hier geeignete Vorsichtsmaßnahmen. Insbesondere kriminelle Eindringlinge bevorzugen einfache Ziele, die nicht die letzte Anwendungsversion installiert haben und leicht zu merkende Passworte zum Schutz vor Attacken nutzen. Dies gilt sowohl für Webserver als auch für PCs etc.

Geeignete Methoden zur Erhöhung der Sicherheit sind z.B.:

- Updates regelmäßig und zeitnah einspielen
- Accounttrennung – verschiedene Benutzernamen und Passworte verwenden
- IP-Beschränkungen für FTP, SSH, E-Mail und MySQL
- Verzeichnisse per .htaccess vor unbefugten Zugriffen schützen
- Versionierungssystem nutzen
- SSH Key anstatt Passworten nutzen
- SSL Zertifikate und Verschlüsselung einsetzen
- Virenscan auf dem Webaccount
- Backupkonzepte

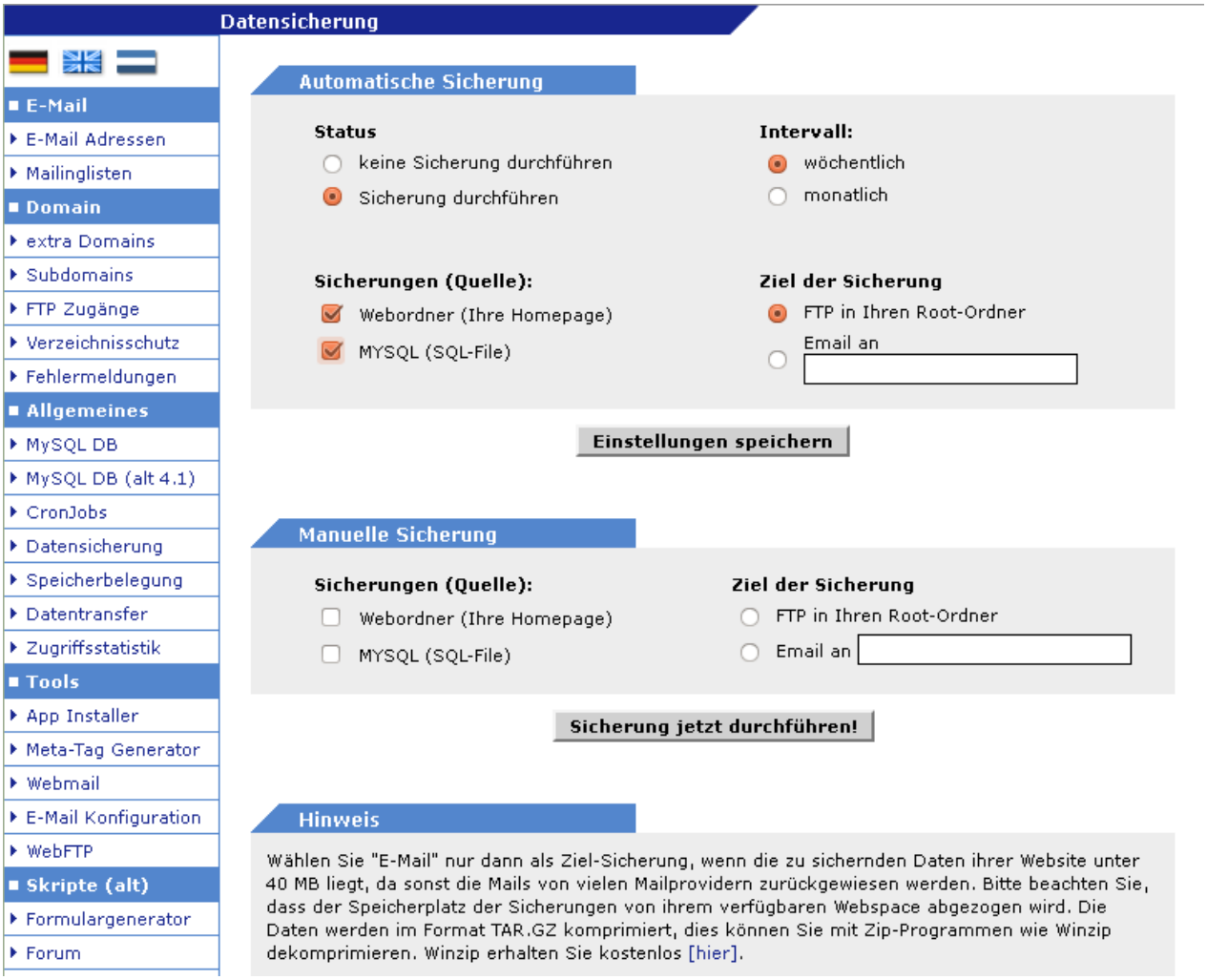
Backups sind kein eigentliches Sicherheitskriterium, aber geeignet, um nach einem Datenverlust oder einem Angriff eine funktionierende Version wieder herzustellen. Ein Backup hilft aber nie, einen Angriff zu verhindern!

Eine Kombination aus mehreren dieser Maßnahmen erhöht die Sicherheit exponentiell. In den folgenden Abschnitten werden die Methoden zur Verbesserung der Server- und Accountsicherheit im Detail erläutert.

Backups durchführen

Backups dienen der Datensicherung von Kundendaten, Webanwendungen und natürlich auch Inhalten von Webseiten. Ein großer Shop mit einem umfangreichen Sortiment, welches über Jahre aufgebaut wurde, entspricht dem Gegenwert vieler Arbeitsstunden. Mit einem Backup werden nicht nur die wertvollen Kundendaten in regelmäßigen Abständen gesichert, sondern auch die Inhalte des Shops und die ebenfalls mit viel Arbeitsaufwand verbundene Konfiguration und Anpassung inkl. aller Zusatzmodule.

Je nachdem, wie häufig z.B. ein Online-Shop aktualisiert wird, sollten die Backups getaktet werden. Bewährt hat sich hier der Abstand von 5 Tagen. Die Sicherungen können entweder auf einem serverinternen Backuplaufwerk durchgeführt werden, oder sie werden auf einem gesonderten Backup-Server gespeichert, der auch in einem anderen Rechenzentrum stehen kann. Letztere Methode ist am allersichersten einzuschätzen, ist aber auch am aufwändigsten. Der gesamte zu sichernde Inhalt muss über eine sichere Internet-Verbindung übertragen werden. Diese Methode ist daher nur dann zu empfehlen, wenn die abzusichernden Inhalte auch vor einem Komplettausfall des Rechenzentrums, etwa durch Feuer oder einen sonstigen Schaden, gesichert werden sollen. Da Rechenzentren einen sehr hohen Sicherheitsstandard aufweisen, ist dieser Fall jedoch sehr unwahrscheinlich.



Regelmäßige Updates

Viele Software-Entwickler sind bestrebt, ihre Webanwendungen möglichst sicher zu gestalten. Auch nach Veröffentlichung bekannt gewordene Sicherheitslücken werden in der Regel schnell behoben, und den Anwendern wird ein Update zur Installation zur Verfügung gestellt, welches die Sicherheitslücke schließt. Eine 100% sichere Software wird es in offenen Systemen nicht geben, aber durch das zeitnahe Einspielen der entsprechenden Aktualisierung wird eine größtmögliche Absicherung gegen unbefugtes Eindringen auf Ebene der Webanwendungen angestrebt. Nutzer, die hier proaktiv agieren und ihre Systeme möglichst auf dem neuesten Stand halten, sollten gegen diese Form der Bedrohung recht gut geschützt sein – sofern sie auch alle anderen Maßnahmen wie sichere Passworte usw. beachten und z.B. auf Blogs wie WordPress keine Erweiterungen o.Ä. aus unsicheren Quellen installieren.

Oft verfügen Programme wie z.B. Webshopsoftware oder Blogsoftware über integrierte Update-Module, mit denen auch der jeweils neueste Sicherheitsstandard gesichert eingespielt wird. Bei jedem Update sollte jedoch vorher nach Möglichkeit auch ein Backup des aktuellen Standes erstellt werden. Webanwendungen sind komplex und bei Aktualisierungen kann es, insbesondere im Zusammenspiel mit anderen Elementen der Internetpräsenz (Warenwirtschaftsmodule, gekoppelte CRM-Software etc.), zu Unregelmäßigkeiten kommen. Zusätzlich zu einem Backup kann hierfür ein Versionierungssystem genutzt werden, mit welchem die Webanwendung jederzeit auf einen vorherigen Stand wiederhergestellt werden kann. Zu nennen sind hier insbesondere die bekannten Werkzeuge Git und SVN, auf welche in einem der nächsten Abschnitte eingegangen wird.

Es ist ratsam, freie Software wie z.B. WordPress, Typo3 oder phpBB immer zu aktualisieren, sobald Updates erscheinen. Sollte die Webanwendung über kein automatisiertes Update-Werkzeug verfügen, mit welchem Administratoren z.B. beim Login auf Neuerungen hingewiesen werden, so können die Anwender z.B. über den Newsletter der Entwickler von sicherheitsrelevanten Updates erfahren.

Accounts separieren

Dieser Hinweis ist ein wenig unbequem. Denn natürlich ist es einfacher, für jede Webanwendung und jedes Social Media Profil usw. dieselbe Mailadresse, Nutzernamen und dasselbe, womöglich auch noch unsichere, Passwort zu nutzen. Dann aber benötigen potentielle Angreifer nur einen geknackten Account, um auf alle genutzten Dienste und Programme zugreifen zu können. Dies kann verheerende Folgen haben. Daher die Empfehlung, nach Möglichkeit für jede Tür einen eigenen Schlüssel zu nutzen. In Blog-Software wie z.B. WordPress und Serendipity, aber auch in CMS wie Typo3 und Joomla!, wird oft der Nutzername „Admin" als Standard eingesetzt. Auch individuelle Nutzernamen sind Teil einer ganzheitlichen Sicherheitsstrategie: Auch wenn sie nicht unbedingt geheim sind, muss ein eventuell angreifender Bot sie zunächst recherchieren. Dies wird erschwert, wenn ein Nutzer mit Namen „Admin" gar nicht vorhanden ist, denn dann sind für eine Manipulation des Systems schon zwei Unbekannte Parameter notwendig. Wie sinnvolle und sichere Passworte generiert werden und welche Technologie alternativ zu Passworten genutzt werden kann, wird im weiteren Verlauf noch beschrieben.

Die Accounttrennung kann bspw. auch auf den Dienst FTP übertragen werden. Wenn hier für jedes „Untersystem" einer Webseite (Blog, Forum, Hauptseite etc.) ein eigener Account genutzt wird, so kann – zumindest via FTP, um in diesem Beispiel zu bleiben – auch nur dieser Teil der Seite verändert und manipuliert werden. Auch sinnvoll ist es, die Rechteverwaltung, etwa in Redaktionssystemen, zu nutzen. Hiermit können die Rechte vergeben werden, welcher Nutzertyp was im System machen darf. Dies geht tw. so weit, dass Redakteure zwar Artikel schreiben dürfen, diese aber dann von einer anderen Person/Account veröffentlicht werden. Hier kann dann nur von außen sichtbar etwas verändert werden, sofern ein Account mit dem Recht zur Veröffentlichung kompromittiert worden ist.

Auch diese Form der Einschränkung von Nutzerrechten bedeutet zunächst mehr Arbeit und ein Konzept zum Content-Management. Dieser Mehraufwand ist jedoch durch das Plus an Sicherheit, dass er mit sich bringt, mehr als gerechtfertigt. Ein weiterer Vorteil ist, dass viele noch unerfahrene Publisher oder Content-Manager und Shop-Betreuer, es möglicherweise als Erleichterung empfinden, wenn sie wissen, dass sie zwar verunglückte Texte schreiben, nicht aber das komplette Seitendesign durch unbedachtes Handeln verändern können. Um hier eine kundenfreundliche Lösung zu ermöglichen, bietet die Profihost AG bspw. bei Managed Servern die Einbindung eines externen Accounts via Proxy an.

Zugriffe auf eigene IP-Adresse beschränken

Sofern Sie von Ihrem Internet-Zugangs-Provider eine feste IP-Adresse zugewiesen bekommen haben, können die Zugriffe, bspw. zum Backend Ihrer Webanwendung, auf diese IP-Adresse und so auf einen vertrauenswürdigen Nutzerkreis eingeschränkt werden. Eine solche Zugriffsbeschränkung kann gezielt für einzelne Anwendungen und Verzeichnisse eingerichtet werden, um zum Beispiel den Zugriff auf den Kalender oder zum Mailserver von überall erlauben. So können mobil Termine eingesehen und geändert und Mails gelesen werden. Der Zugang für das Shop-Backend ist hingegen weiterhin z.B. auf das Büronetzwerk beschränkt.

Eine IP-Sperre ist also, insbesondere auch mit weiteren hier aufgeführten Sicherheitsmaßnahmen, ein erprobtes zusätzliches Mittel, um die Möglichkeiten eines Angriffs zu verkleinern und die Attacke selber möglichst schwierig zu machen. Hier muss im Hinblick auf die vorliegende Organisationsstruktur individuell entschieden werden, ob und wenn ja welche Anwendungen nur intern erreichbar sein sollen.

Beispiel:

Mit dem folgenden Beispiel einer .htaccess Datei lässt sich der Zugriff auf das Verzeichnis /backend einer Webanwendung auf eine bestimmte IP-Adresse beschränken:

```
Order Allow,Deny
Allow from <MEIN IP-ADRESSE>
Deny from All
```

Ob Sie eine feste IP für den Zugang zum Internet nutzen und wie diese lautet, können Sie beim Kundendienst Ihres Zugangsproviders (z.B. QSC, Dt. Telekom, htp, EWE-Tel) erfragen. Eine IP-Sperre kann auch in Zusammenhang mit einem VPN-Zugang genutzt werden, um den Zugriff z.B. von einem Tablet oder Smartphone mit dynamischer IP zu erlauben. Damit wählen sich die Nutzer zunächst über eine VPN-Verbindung von unterwegs oder Zuhause ins Firmennetz ein, von wo aus der Zugang zu den betreffenden Diensten gestattet ist. Mehr zum Thema VPN erfahren Sie in einem der folgenden Kapitel.

Ebenso kann der Zugriff auf Datenbanken auf einzelne IP-Adressen oder -Netze eingeschränkt werden. Hier ist es zudem möglich, Nutzer mit eingeschränkten Rechten zu generieren. Diesem Thema widmen wir uns ebenfalls in einem der folgenden Kapitel.

Verzeichnisse schützen

Ebenfalls über die .htaccess Datei können einzelne Verzeichnisse oder bei Bedarf auch eine ganze Domain (das Hauptverzeichnis) mit einem Passwortschutz versehen werden. Dabei sollten unterschiedliche Identitäten (Benutzer-/Passwort-Kombinationen) hinterlegt und verwendet werden.

Profihost hat ein Tool zum Erstellen verschlüsselter Passworte im ServerCon Administrationstool integriert. Hierzu wählen Sie im Menü „Domain" den Punkt Verzeichnisschutz aus. Eine entsprechende .htaccess Datei wird dann auf Ihrem Webaccount angelegt. Siehe hierzu Kap. 2.4 im Handbuch zur ServerCon Verwaltung[9].

Alternativ legen Sie im zu schützenden Unterverzeichnis eine entsprechende .htaccess Datei an oder fügen dieser Datei die entsprechenden Angaben hinzu. Hier ein Beispiel für den Inhalt einer solchen Datei.

```
AuthUserFile /home/xyz/www.example.com/test/.htpasswd
AuthGroupFile /dev/null
AuthName "Passwortgeschuetzter Bereich!"
AuthType Basic
Require valid-user
```

In diesem Beispiel soll das Unterverzeichnis /test der Domain www.example.com (also www.example.com/test) geschützt werden. Der obere Pfad ist hier der Pfad auf dem Webserver, auf welchem die Domain „example.com" gehostet wird. Alle Pfadangaben sind Beispielangaben, die einzelnen Spezifikationen sind je nach Benutzer und Hosting-Anbieter unterschiedlich. Wenn Sie nicht genau wissen, welche Pfadangabe hier korrekt ist, fragen Sie den Support Ihres Hosters.

In der .htaccess Datei steht der Pfad zu einer Datei (.htpasswd), in welcher die Benutzer und Passworte für das Verzeichnis (*Require valid-user*) eingetragen sind. Der Inhalt der Datei .htpasswd sieht bspw. folgendermaßen aus:

```
test:$apr1$ip801hBF$5DRLQuAvE2PmvbH.v1T5h/
```

Das Passwort für den Benutzer „test" ist hier verschlüsselt eingetragen. Auch wenn die Datei .htpasswd Unbefugten in die Hände geraten sollte, so müsste das verschlüsselte Passwort zunächst dekodiert werden – die Verschlüsselungszeichenkette lässt sich nicht als Passwort verwenden. Bei der Einrichtung

9 https://www.profihost.com/pdf/profihost-servercon-admin.pdf

dieser Dateien haben sich entsprechende Werkzeuge zum Verschlüsseln von Passworten als hilfreich erwiesen.

http://www.htaccesstools.com/htpasswd-generator/

Die Daten müssen dann in die entsprechende Datei kopiert werden, welche dann auf den Server übertragen wird. Wenn Sie eine Fernzugriff auf Ihren Webserver nutzen, können Sie die .htaccess Datei auch mit einem entsprechenden Texteditor direkt im Unterverzeichnis anlegen.

Einsatz eines Versionskontrollsystems

Ein Versionskontrollsystem erleichtert die Abbildung Ihrer Anwendung in verschiedenen Entwicklungsstadien. Mit einem Versionskontrollsystem wie z.B. Git oder SVN erstellen Sie, einfach ausgedrückt, Kopien ihrer Dateien, welche einer Zeitleiste zugeordnet werden. So ist es möglich, jederzeit zu einer bestimmten Version zurück zu schalten. Wenn z.B. eine Webseite oder ein Webshop gehackt worden ist, können Veränderungen schnell erkannt und die Applikation auf den letzten „sauberen" Stand zurück gerollt werden.

Auch erleichtert beispielsweise Git das Entwickeln unterschiedlicher Teilbereiche einer Webpräsenz. Einzelne Elemente lassen sich damit parallel entwickeln und zusammenführen. Dabei nutzt das Versionskontrollsystem eine inkrementelle Datenverwaltung, in welcher immer nur die Teilbereiche einer Dateien geändert werden, die bearbeitet worden sind. Es werden also im Prinzip Veränderungen zur vorherigen Version gespeichert und nicht ganze Dateien überschrieben. Mit Git lassen sich auch kollaborative Großprojekte realisieren, da die Möglichkeit besteht, einzelne Module und Entwicklungsstufen einer bestimmten Nutzergruppe oder öffentlich zur Verfügung zu stellen.

Externe Datenbank-Freigabe mit beschränktem Zugriff

Externe Zugänge zu einer MySQL-Datenbank können ebenfalls auf bestimmte IP-Adressen oder -Netze beschränkt werden. So kann zur Administration der Datenbanken nur von diesen IP-Adressen aus zugegriffen werden. Auch kann ein Nutzer angelegt werden, der nur eingeschränkten Zugriff (SELECT) hat. Potentielle Angreifer haben durch diese Beschränkungen nur noch wenige Möglichkeiten, auf die Datenbank zuzugreifen. Da die Kommunikation mit dem Datenbank-Dienst im Klartext abläuft, empfiehlt sich hier außerdem die Nutzung von VPN (Siehe S. 16 „IP-Kreis beschränken“). Der Zugriff auf die Datenbank wird mit dem Tool HeidiSQL[10] Client oder phpMyAdmin[11] realisiert. Letzteres ist bei vielen Webhostern, so auch bei der Profihost AG, in die Account-Verwaltung integriert[12].

10 http://www.heidisql.com/ [17.11.2014]
11 http://www.phpmyadmin.net/
12 https://www.profihost.com/pdf/profihost-servercon-admin.pdf, Kap. 3.1.1 phpMyAdmin [17.11.2014]

SSH-Key statt Login mit Passwort

Beim Einloggen auf den Webspace oder Webserver wird oft ein FTP-Programm mit Zugangsdaten und Passwort genutzt, um z.B. Dateien zu übertragen. Alternativ dazu besteht durch Absicherung der Zugänge mit SSH-Keys die Möglichkeit, den Zugriff auf Daten noch besser abzusichern. Der Zugang erfolgt dann unter Verwendung eines Schlüsselpaares (privater und öffentlicher Schlüssel), wobei der private Schlüssel stets geheimzuhalten ist und auf dem eigenen System verbleibt und der öffentliche Schlüssel auf dem Zielsystem hinterlegt wird. Bei der Erstellung des Schlüsselpaares ist es empfehlenswert, den privaten Schlüssel durch ein Passwort (sog. "Passphrase") zusätzlich zu schützen.

Eine detaillierte Anleitung zur Erstellung eines SSH-Key finden Sie in den Profihost-FAQ unter dieser Adresse:

https://www.profihost.com/forum/ftp/kann-ich-das-public-key-verfahren-fur-ssh-und-ftp-nutzen/

SSL-Zertifikate / Verschlüsselung

Mit einem SSH-Zugang sichern Sie Ihre eigene Verbindung zu Ihrem Webangebot und Webserver ab. Für die Besucher Ihrer Webseite können Sie unabhängig davon eine verschlüsselte Datenübertragung mittels eines SSL-Zertifikats einrichten. Dabei sind die zu übertragenden Inhalte nur auf dem sendenden Rechner und dem Empfänger-Rechner lesbar, also zum Beispiel auf dem PC eines Besuchers und Ihrem Webserver. Weder der Webhosting-Anbieter noch der Internet Service Provider oder Andere können die übertragenen Daten während der Übertragung entschlüsseln. So ist gewährleistet, dass sensible Daten nicht durch Unbefugte abgefangen und missbraucht werden können. Für die Kunden von z.B. Onlineshops bedeutet dieses Verfahren einen zusätzlichen Schutz ihrer Daten wie etwa Adressdaten, Kontodaten etc.

Bei SSL-Zertifikaten bestehen Unterschiede beim Grad der Verschlüsselung und somit bei der Qualität der Datensicherheit. Am besten ist es, wenn Server immer versuchen, die sicherste Verschlüsselung auszuhandeln. Dabei können einige ältere Methoden weiterhin unterstützt werden, um möglichst wenige Besucher auszusperren.

Bei konventionelle SSL-gesicherte Übertragungen wird der Schlüssel zu Beginn jeder Übertragung gesendet. Hierbei kann es zu einem unbemerkten Abhören der versendeten Informationen kommen, etwa wenn der Schlüssel geknackt wurde. Auch wurden bereits verschlüsselte Kommunikationen abgefangen und gespeichert, um sie zu einem späteren Zeitpunkt, wenn z.B. ein Verfahren zur unbefugten Entschlüsselung gefunden wurde, auszuwerten. Der öffentliche Schlüssel wird immer an den Browser des Besuchers gesendet. Der Browser verschlüsselt die Daten mit dem Schlüssel, der Server kann sie mit einem privaten Schlüssel wieder entschlüsseln. Zu Beginn der Sitzung wird über dieses asymmetrische Verschlüsselungsverfahren ein länger genutzter Schlüssel ausgehandelt. Alle Daten asymmetrisch zu verschlüsseln wäre sehr aufwendig, daher wendet man hier einfach asymmetrisch und symmetrische Verschlüsselung an.

Keine Verschlüsselungsmethode bietet 100%igen Schutz, da offene Systeme immer die Möglichkeit der Manipulation beinhalten. Eine sehr gute Methode zur SSL-Verschlüsselung ist jedoch die Kodierung mittels Forward Secrecy[13]: Bei dieser Methode kommt ein zufällig generierter und zwischen Sender und Empfänger ausgehandelter Schlüssel zum Einsatz. Dieser wird mit dem äußerst sicheren Elliptic-Curve-Diffie-Hellman (Schlüssel)austauschverfahren (ECDH) generiert. So wird für jede Übertragung eine neue Verschlüsselung genutzt. Dies hat den Effekt, dass anstatt eines einzigen Schlüssels, der für eine lange Zeit genutzt wird, sehr viele Schlüssel geknackt werden müssten. Diese Vielzahl an Schlüsseln wird zudem nur einmalig genutzt und nach der Übertragung sofort gelöscht[14]. Dieses Schlüsselaustauschprotokoll hat die Eigenschaft der Folgenlosigkeit. Dies *„bedeutet in der*

13 http://de.wikipedia.org/wiki/Perfect_Forward_Secrecy [5.8.2014]
14 https://www.profihost.com/blog/2014/03/11/webhosting/mehr-webserver-sicherheit-durch-forward-secrecy [5.8.2014]

Kryptographie die Eigenschaft von Schlüsselaustauschprotokollen, dass aus einem aufgedeckten geheimen Langzeitschlüssel nicht auf damit ausgehandelte Sitzungsschlüssel eines Kommunikationskanals geschlossen werden kann"[15]. Wie eingangs angedeutet, soll dafür gesorgt werden, dass auch wenn der längerfristig genutzte, zu Sitzungsbeginn ausgehandelten Schlüssel bekannt ist, kein Rückschluss auf die mit diesem Verfahren genutzten weiteren Sitzungsschlüssel gezogen werden kann. Es ist anzuraten, bei der Wahl Ihres Hosting-Anbieteters bzw. SSL-Zertifikats darauf zu achten, dass eine möglichst effektive Methode zur Sicherung der Datenübertragung verwendet wird.

15 http://de.wikipedia.org/wiki/Perfect_Forward_Secrecy#cite_note-HAC-1 [17.11.2014]

Virenscan

Analog zu einem Virenscan auf dem heimischen Rechner können auch für Webhosting-Accounts und Webserver Virenscans durchgeführt werden. Mit einem zeitgesteuerten Virenscan werden bestimmte Bereiche auf Schadcode gescannt und das Ergebnis wird via E-Mail an eine festgelegte Adresse versandt. Sollte eine Virus oder ähnliches gefunden werden, so können Betroffene – auch in Zusammenarbeit mit ihrem Hosting-Provider – geeignete Maßnahmen ergreifen. Virenscans finden Backdoors, Spamscripte, Trojaner und anderen Schadcode, die durch eine Sicherheitslücke auf dem Webaccount installiert werden konnten. Die betroffenen Bereiche können entweder bereinigt werden, oder es wird ein virenfreies Backup wiederhergestellt bzw. eine mit einem Versionskontrollsystem erstellte frühere Version der Webanwendung.

Antivirus-Programme sollten, wie allgemein üblich, stets auf dem neuesten Stand gehalten werden. Durch stete Updates wird sichergestellt, dass die jeweils aktuellen Erkennungsmuster für neue Bedrohungen auf dem System zur Verfügung stehen. Dadurch wird, zusammen mit einem Virenscan in regelmäßigen Abständen, sichergestellt, dass der Server oder der Webaccount stets optimal vor Viren und Schadsoftware geschützt ist.