profihost

E-Commerce. Cloud. Hosting.

Profihost AG – Pressemitteilung vom 8.4.2015

Zunehmende Attacken auf Internetseiten, Server und Webanwendungen: Maßnahmen zur Verbesserung von Datenschutz und Datensicherheit

Hannover – Die Attacken auf Server, Datenübertragungen und Webanwendungen nehmen zu: Die Zahl der Hackerangriffe auf Unternehmen ist laut PwC-Studie „Global State of Information Security 2015" im letzten Jahr weltweit im Vergleich zum Vorjahr um 48 Prozent auf 42,8 Millionen angestiegen. Pro Tag entspricht das 117.300 Angriffen. Die Angreifer machen sich dabei Schwachstellen der betroffenen Webseiten oder Server zunutze: „Häufig werden Zugangsdaten zu Webseiten oder Serversystemen ausgespäht, um die Rechner und Programme dann gezielt für illegale Zwecke zu nutzen. Und nach wie vor sind zu einfache Passworte eine Möglichkeit, sich unbefugt Zutritt zu fremden Accounts und Systemen zu verschaffen", macht Fabian Kösters, Online-Redakteur bei der Profihost AG (www.profihost.de), aufmerksam.

Der Webhoster hat eine Übersicht zusammengestellt, was Nutzer von Internet-Infrastruktur proaktiv zu ihrem eigenen Schutz und zur Verbesserung der Datensicherheit unternehmen können. Diese Gegenmaßnahmen beziehen sich vorwiegend auf Attacken und Manipulationsversuche an Internetseiten, Servern und Webanwendungen. Sie sind in ähnlicher Form auch auf private Rechner oder Rechner am Arbeitsplatz umsetzbar.

Die nachfolgend aufgeführten Maßnahmen werden in einem nun veröffentlichten Whitepaper noch tiefer gehend erläutert. Das Whitepaper steht auf der Webseite von Profihost zum Download bereit unter:

https://www.profihost.com/know-how#whitepaper-datenschutz

Backups

Zwar kein eigentliches Sicherheitskriterium, sind Backups aber geeignet, um nach einem Datenverlust oder einem Angriff eine funktionierende Version eines Systems wieder herzustellen. „Je nachdem, wie häufig ein Online-Shop oder eine Webseite aktualisiert wird, sollten Backups in entsprechenden Abständen getaktet werden. Bewährt hat sich der Abstand von 5 Tagen zwischen den einzelnen Backups. Die Sicherungen können hierbei entweder auf einem serverinternen Backup-Laufwerk durchgeführt werden, oder sie werden auf einem gesonderten Backup-Server gespeichert, der auch in einem anderen Rechenzentrum stehen kann. Letztere Methode ist zwar die sicherste, aber auch am aufwändigsten in der Ausführung", informiert Fabian Kösters.

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

Regelmäßige Updates

Zwar wird es eine hundertprozentig sichere Software in offenen Systemen nicht geben, aber durch zeitnahes Einspielen von Aktualisierungen wird eine größtmögliche Absicherung gegen unbefugtes Eindringen auf Ebene der Webanwendungen angestrebt. Nutzer, die 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 Sicherheitsmaßnahmen beachten. „Bei jedem Update sollte 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 einer Internetpräsenz, wie Warenwirtschaftsmodule oder gekoppelter CRM-Software, zu Unregelmäßigkeiten kommen", rät Kösters.

Accounts separieren

Zwar ist es einfach, für jede Webanwendung und jedes Social Media Profil etc. dieselbe Mailadresse, Nutzernamen und dasselbe Passwort zu nutzen. Dann aber benötigen potentielle Angreifer nur einen geknackten Account, um auf alle genutzten Dienste und Programme zugreifen zu können. Besser deshalb: Accounts separieren und für jede Anwendung eigene Zugangsdaten, mindestens aber ein eigenes, sicheres Passwort, erstellen.

IP-Kreis beschränken

Zugänge, beispielsweise zum Backend einer Webanwendung, können auf eine IP beschränkt werden. Dadurch haben nur Personen Zugriff auf diese Dienste, die von einem Rechner innerhalb eines Büros das Internet nutzen. Damit sich Webanwendungen weiterhin mobil nutzen lassen, können solchen IP-Schranken nur auf einzelne Verzeichnisse angewendet werden. Somit besteht die Sperre dann nur für bestimmte Anwendungen und Mitarbeiter haben auch von unterwegs zum Beispiel Zugriff auf den Kalender oder zum Mailserver. Der Zugang für das Shop-Backend aber hingegen ist auf das Büronetzwerk beschränkt.

Verzeichnisse sperren

Ähnlich der Möglichkeit den IP-Kreis zu beschränken, lassen sich auch einzelne Verzeichnisse und bei Bedarf auch eine ganze Domain (das Hauptverzeichnis) mit einem Passwortschutz versehen. So kann der Zugriff auf einzelne Unterverzeichnisse eingeschränkt werden, um einen zusätzlichen Schutz vor Manipulationsversuchen zu etablieren. Denkbar ist beispielsweise ein zusätzlicher Passwort-Schutz für den Backend-Bereich eines Webshops.

Einsatz eines Versionierungssystems

Ein Versionierungssystem erleichtert die Abbildung einer Webanwendung in verschiedenen Entwicklungsstadien. Mit einem Versionierungssystem wie beispielsweise Git oder SVN werden, sehr vereinfacht ausgedrückt, Kopien von Dateien erstellt, welche einer Zeitleiste zugeordnet werden. So ist es möglich, jederzeit zu einer bestimmten Version zurückzuschalten. Wurde eine Webseite oder ein Webshop gehackt, so kann mit diesem System zum letzten sauberen Stand zurückgegangen werden. Ein Versionierungssystem kann auch alternativ zum Backup eingesetzt werden.

Externe Datenbank-Freigabe mit beschränktem Zugriff

Externe Zugänge zu einer MySQL-Datenbank können auf einen IP Adressbereich beschränkt werden. So kann zur Administration von MySQL-Datenbanken nur von dieser IP aus zugegriffen werden. Auch kann ein Nutzer angelegt werden, der nur eingeschränkten Zugriff auf bestimmte Funktionalitäten in der Administration hat. Potentielle Angreifer haben durch diese Beschränkung auch mit vorhandenen korrekten Zugangsdaten keine Möglichkeit, auf die Datenbank zuzugreifen.

SSH-Key statt Login mit Passwort

Beim Einloggen auf den Webspace oder Webserver wird oft ein FTP-Programm mit Zugangsdaten und Passwort genutzt, um Dateien zu übertragen. Alternativ dazu besteht durch Absicherung der Zugänge mit SSH-Keys zusätzlich die Möglichkeit, den Zugriff auf Daten noch besser zu kontrollieren. Der Zugang erfolgt dann über ein Schlüsselpaar, von welchem sich ein Schlüssel (“Public Key”) auf dem Server befindet. Dazu passend wird ein Nutzer-Schlüssel (“Private Key”) erstellt. Es ist empfehlenswert, diesen durch ein “Passphrase” genanntes Passwort zusätzlich zu schützen.

SSL-Zertifikate / Verschlüsselung

Mit einem SSH-Zugang sichern Seitenbetreiber ihre eigene Verbindung zum Webangebot und Webserver ab. Für die Besucher der Webseite können Seitenbetreiber unabhängig davon eine verschlüsselte Datenübertragung mittels SSL-Zertifikat einrichten. Dabei sind die zu übertragenden Inhalte nur auf dem sendenden Rechner und dem Empfänger-Rechner lesbar. „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 Kunden von Onlineshops bedeutet dieses Verfahren einen zusätzlichen Schutz ihrer Adress- und Kontodaten”, ergänzt Fabian Kösters.

Virenscan

Auch für Webhosting-Accounts und Webserver können Virenscans durchgeführt werden. Virenscans finden Backdoors, Spamscripte, Trojaner und anderen Schadcode, die durch eine Sicherheitslücke auf dem Webaccount installiert werden konnten. „Sollte eine Virus oder ähnliches gefunden werden, können Betroffene – auch in Zusammenarbeit mit ihrem Hosting-Provider – geeignete Maßnahmen ergreifen. Die betroffenen Bereiche können dann entweder bereinigt werden, oder es wird ein virenfreies Backup wiederhergestellt bzw. eine mit einem Versionierungssystem erstellte frühere Version der Webanwendung”, so Fabian Kösters.

Weitere Informationen unter: https://www.profihost.com/know-how