profihost

E-Commerce. Cloud. Hosting.

Profihost AG – Pressemitteilung vom 5.12.2014

Online-Shops zur Weihnachtszeit beliebte Ziele von Hacker-Angriffen

Penetrationstests simulieren Attacken und decken Schwachstellen der IT-Infrastruktur auf

Hannover – Etwa 33 Millionen Bundesbürger werden nach Angaben des BITKOM dieses Jahr ihre Weihnachtsgeschenke online kaufen. Millionen Daten also, die für Hacker gerade zur Weihnachtszeit ein lukratives Geschäft sind: Passwörter, Kreditkartendaten und Geburtsdaten etwa sind besonders beliebt, mahnen die Experten des Webhosters Profihost. Philipp Reger, Vorstandsassistent (Vertrieb) bei der Profihost AG, weiß, was mit diesen gestohlenen Daten passiert: „Entweder sie werden verkauft oder die Datendiebe gehen selbst auf Kosten der Bestohlenen einkaufen. Für Online-Shops wäre es in jedem Falle nicht nur ein immenser wirtschaftlicher Schaden. Es wäre vor allem auch ein hoher Vertrauensverlust."

Um Schaden zu vermeiden, können und müssen Shop-Betreiber einige Maßnahmen zur Absicherung ihres Unternehmens, ihrer Daten und der Daten ihrer Kunden, selber durchführen. Dazu zählen neben einer Grundsicherung – etwa dem Einsatz einer Firewall, der konsequenten Verschlüsselung der Kommunikation mit SSL-Zertifikaten oder Passwortregeln für Käufer – beispielsweise auch der Einsatz von Session Cookies und die Nutzung sicherer Bezahlverfahren. Shopbetreiber, die als Zahlungsart Bankeinzug oder Kreditkarte anbieten, sollten sich der Sensibilität dieser Daten bewußt sein und z.B. einen zertifizierten Payment Service Provider zu Abwicklung der Transaktionen wählen. „Website-Betreiber sollten grundsätzlich die Nutzer-Daten so speichern, dass sie für unbefugte Dritte möglichst unbrauchbar sind. Sprich: Bestenfalls verschlüsselt und unknackbar. Hierzu stehen diverse kryptografische Hash- und Salt-Funktionen zur Verfügung, die über Zusatzmodule auch mit vielen beliebten Content Management Systemen genutzt werden können", rät Reger. Die Sicherheitsmaßnahmen sind übrigens für Besuchern und Kunden „sichtbar" und geben Vertrauen: Ein Schloss-Symbol in der Browser-Leiste oder die grüne Adressleiste zeugen davon, dass persönliche Informationen verschlüsselt an den Anbieter übertragen werden.

Oft ist es auch hilfreich, aus einer neutralen Position heraus und mit dem nötigen Fachwissen die Server-Sicherheit von Außen zu prüfen. Profihost stellt mit so genannten Penetrationstests dabei die IT-Sicherheit mit simulierten Angriffen auf die Systeme und IT-Infrastruktur auf die Probe. Das Ziel: Mögliche Schwachstellen erkennen und frühzeitig handeln. Beim Penetrationstest wird eine Hosting-Umgebung, das darunterliegende System, der SSH- und FTP-Zugang sowie die Login-Bereiche aus Sicht eines unangemeldeten Besuchers auf ihre Sicherheit hin überprüft. „Die simulierte Attacke geschieht immer von verschiedenen Angriffspunkten aus: Einerseits wird versucht, das System aus der Sicht eines x-beliebigen Besuchers heraus zu manipulieren. Andererseits wird überprüft, ob unbefugte Zugriffe durch Mitarbeiter des Unternehmens möglich sind. Denn häufig sind es leider auch Mitarbeiter, die in einem Unternehmen versehentlich oder zum eigenen Vorteil unberechtigt auf Daten zugreifen und diese womöglich missbräuchlich nutzen", erklärt Philipp Reger.

Weitere Informationen unter: www.profihost.com

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