Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im Dezember 2014

Sehr geehrte Damen und Herren,

zur Außendarstellung von Unternehmen oder zum Vertrieb der eigenen Produkte sind Webseiten eine beliebte Plattform. Leider steigt die Zahl der erfolgreichen Hackerangriffe auf Internetseiten besorgniserregend an. Gängige Folgen sind, dass die unbekannten Täter Kundendaten aus den Datenbanken entwenden, die Webmailerfunktion als Spamversender missbrauchen oder Schadsoftware auf der Webseite hinterlegen um mittels Drive-by-Download[1] die Rechner der Kunden mit Malware zu infizieren.

In diesem Zusammenhang möchten wir Ihnen wieder aktuelle Fälle aus unserer täglichen Arbeit näherbringen.

Die Lehre aus diesen und vielen ähnlichen Fällen ist, dass es nicht mit der Erstellung einer Webseite getan ist. Wartung und Pflege eines Internetangebotes ist von wesentlicher Bedeutung für Ihre Sicherheit und die Ihrer Kunden.

Für Rückfragen zu diesem Thema stehen wir jederzeit gerne zur Verfügung, wobei das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen unberührt bleibt.

Ihr Wirtschaftsschutz-Team

[1] Unter einem Drive-by-Download versteht man die Beeinflussung eines Rechners oder sogar die Infizierung des PC durch den bloßen Besuch einer verseuchten Webseite.

Niedersächsisches Ministerium für Inneres und Sport
Referat 55 - Wirtschaftsschutz

Postfach 4420
30044 Hannover
Tel.: 0511 / 6709-247 oder -248
Email: wirtschaftsschutz@verfassungsschutz.niedersachsen.de

Falldarstellung

Fall 1.

Unbekannte Täter dringen über Schwachstellen im Content Management System des Internetauftrittes eines Unternehmens in das Intranet der Firma ein und leiten die Daten des dortigen Active Directory (u.a. Benutzerverwaltung) aus. Mit den gestohlenen Benutzerdaten werden im Nachgang unautorisierte Anmeldungen im internen Netzwerk festgestellt. Ob es zum Datenabfluss aus dem Unternehmensnetzwerk gekommen ist, ist zurzeit Gegenstand der Ermittlungen.

Fall 2.

Nachdem sich Kundenbeschwerden über Schadsoftwarebefall nach Besuch der Firmenhomepage des Unternehmens häuften, wurde bei der Untersuchung des Quellcodes der Webseite festgestellt, dass hier über ein nachträglich eingebautes IFrame[2] Besucher der Seite auf eine attackierende Webseite umgeleitet wurden.

Wie können Sie sich schützen:

Um Ihre Webseite gegen Angriffe zu schützen, empfehlen sich folgende, nicht abschließende, Maßnahmen:

- Verwenden Sie immer die aktuellste Version Ihres Content-Management-Systems.
- Installieren Sie zeitnah alle Updates, insbesondere auch für installierte Erweiterungen (Module).
- Nutzen Sie sichere Passwörter mit mindesten 8 Zeichen Länge, welche aus Kombinationen von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen.

[2] Ein IFrame (Inline Frame) ist ein HTML-Dokument, das in einem zweiten HTML-Dokument auf einer Website eingebettet ist.

- Aktivieren Sie den Verzeichnisschutz mittels .htaccess-Datei für den Administrationsbereich Ihres CMS unter Verwendung eines gesonderten Passwortes.
- Benennen Sie den Administrator Accountnamen **nicht** admin, Administrator oder Superuser.
- Machen Sie ein regelmäßiges Backup Ihrer Webseite inklusive der Datenbank.
- Aktivieren Sie die Web-Applikations-Firewall ihres CMS und installieren Sie ggf. weitere Sicherheitsfeatures, sofern verfügbar.
- Nicht verwendete bzw. nicht aktivierte Erweiterungen sollten deinstalliert werden.
- Testen Sie ihre Webseite auf Verwundbarkeiten. Siehe Hinweis unter Links.

Bitte beachten Sie, dass es keinen 100% Schutz gegen Hackerangriffe gibt, aber sich das Risiko mit den vorgenannten Maßnahmen deutlich verringern lässt.

Ihre Webseite wurde gehackt, was nun?:

Sollten die vorgenannten Maßnahmen nicht geholfen haben und Sie wurden Opfer eines Hackerangriffs, gilt es Schadensbegrenzung zu betreiben.

- Stellen Sie Ihre Webseite umgehend offline.
- Ändern Sie alle verwendeten Passwörter.
- Identifizieren Sie die Sicherheitslücke im System und schließen diese. Hierzu benötigen Sie ggf. externe Unterstützung.
- Spielen Sie anschließend, sofern vorhanden, ein bestehendes Backup ein.
- Falls kein Backup vorhanden ist, sichern Sie ihre Datenbank, reinigen den Server und löschen auch die Datenbank, anschließend installieren Sie ihr CMS neu und importieren dann ihre Datenbankinhalte.
- Überprüfen Sie vor Onlinestellung Ihres Internetauftrittes die Verzeichnis- bzw. Dateirechte auf dem Server.

Sollten diese Hinweise für Sie nicht umsetzbar sein, ist die Inanspruchnahme eines Dienstleisters anzuraten.

Links zum Schutz Ihre Webseite:

Test auf Schwachstellen unter: http://sitecheck.sucuri.net/
Webseitenabsicherung durch die Initiative-S: https://www.initiative-s.de

Ein interessanter Link in anderer Sache:

Das Ergebnis der Umfrage 2014 der Allianz für Cybersicherheit finden sie unter:
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/Umfrage/umfrage2014.html%3bjsessionid=EB699046227EEB7BF6BEF49E6A0F026A.2_cid286