Niedersächsisches Ministerium
für Inneres und Sport

Wirtschaftsschutz - *Info*

Hannover im März 2018

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 weiterhin besorgniserregend an. Aktuell ist der sogenannte „google conditional hack“ wieder ein häufig gemeldeter Angriff auf Unternehmenswebseiten.

Ebenso scheint die Welle der „CEO-Fraud“ Angriffe nicht abzuebben. Zu dieser Angriffsart bekommt der Wirtschaftsschutz regelmäßig Hinweise von Unternehmensvertretern, zum Teil mit hohen Schadenssummen. Aktuelles Zielland für Überweisungen ist London und nicht mehr, wie in der Vergangenheit, Hongkong.

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

Für Fragen zu diesen Themen stehen wir jederzeit gerne zur Verfügung, wobei das Angebot des Wirtschaftsschutzes zu individuellen und vertraulichen Gesprächen unberührt bleibt.

Ihr Wirtschaftsschutz-Team

Niedersächsische Verfassungsschutzbehörde

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. Manipulierte Webseiten mittels „google conditional hack“

Unbekannte Täter dringen über Schwachstellen im Content Management System des Internetauftrittes eines Unternehmens in deren Webserver ein und manipulieren diesen entsprechend. Als Folge werden Verlinkungen bzw. Weiterleitungen auf Internetseiten mit pornographischem Inhalt sowie Potenzmittelwerbung im Webauftritt vorgefunden.

Das besondere bei dieser schon recht alten Angriffsart ist, dass es für einen normalen Surfer nicht feststellbar ist, dass diese Webseite manipuliert wurde. Beim Aufrufen der Webseite wird nämlich der Useragent des Surfers ausgewertet. Wird ein Googlebot erkannt, welcher die Seite indexieren will, werden die manipulierten Seiteninhalte ausgeliefert, ansonsten nur die normale Seite.

Wie können Sie prüfen, ob Sie betroffen sind:

Suchen Sie über die Googlesuche ihre Homepage mit dem „site“ Befehl und folgenden beispielhaften Parametern auf:

site: firmenhomepage.de viagra
site: firmenhomepage.de teen

In den Trefferlisten von Google dürfen keine Hinweise auf entsprechende Angebote auftauchen.

Sollten es bei Ihnen zu entsprechenden Treffern in den Googlesuchergebnissen kommen, lesen Sie unsere weiterführenden Informationen und Hinweise zum Thema CMS Hacking in unserer **Wirtschaftsschutz-Info 12/2014** auf unserer Homepage unter:

https://www.verfassungsschutz.niedersachsen.de/wirtschafts_geheimschutz/wirtschaftsschutz/Newsletter/newsletter-54241.html

Fall 2. CEO-Fraud

Mitarbeiter mit Zahlungsvollmacht werden von deren vermeintlichen Vorgesetzten per E-Mail angeschrieben und zur Überweisung von größeren Geldsummen ins Ausland angewiesen. Eine weitere Kommunikation mit dem Vorgesetzten wird per Anweisung auf reinen E-Mail-Verkehr beschränkt.

Hier werden die Mitarbeiter mit einem gefälschten Anzeigenamen im E-Mail-Programm über den wahren Absender getäuscht.

Wie hätten Sie erkennen können, dass hier etwas nicht stimmt:

Über Rechtsklick auf den Anzeigenamen des E-Mailabsenders kann man sich über die Eigenschaften die Original-E-Mail-Adresse anzeigen lassen. In der Regel werden hier Gmail.com- oder Yahoo.com-Konten verfälscht eingesetzt.

Was hätten Sie tun können, um der Täuschung zu entgehen:

Benutzen Sie nicht die „Antworten“ Schaltfläche Ihres E-Mail-Programmes um dem Absender zu antworten, sondern geben Sie die E-Mail-Adresse händisch in die Adresszeile ein. So verhindern Sie, dass Sie an eine gefälschte Absenderadresse zurückschreiben.

Weiterführende Informationen und Hinweise zum Thema CEO-Fraud finden Sie in unserer **Wirtschaftsschutz-Info 08/2015 sowie 12/2016** auf unserer Homepage unter:

https://www.verfassungsschutz.niedersachsen.de/wirtschafts_geheimschutz/wirtschaftsschutz/Newsletter/newsletter-54241.html

Ein Hinweis in eigener Sache:

Der Wirtschaftsschutz des Verfassungsschutzes Niedersachsen ist auf der Hannover Messe Industrie auf dem Stand des Niedersächsischen Ministeriums für Wissenschaft und Kunst vertreten. Sie finden uns in Halle 2 auf den Stand A08.

Wenn Sie uns besuchen wollen, können Sie sich unter dem folgenden Link eine kostenfreie Dauerkarte für die HMI freischalten:

https://www.hannovermesse.de/ticketregistrierung?gc37d

Es ist notwendige das Ticket unter www.hannovermesse.de/ticketregistrierung vor dem Besuch der Messe online zu registrieren

Das personalisierte Ticket gilt als Dauerticket für alle Veranstaltungstage. Es ist aber nicht als Fahrkarte im öffentlichen Nahverkehr Hannover gültig.

Alternativ zur Verwendung des Links können Sie auch den QR-Code nutzen. Sie können sich darüber mobil registrieren.

Nach erfolgreicher Registrierung wird Ihnen ihr personalisiertes e-Ticket per E-Mail zugeschickt. Das Ticket ermöglicht ausgedruckt, oder auf einem mobilen Endgerät angezeigt, den direkten Zugang zum Messegelände.