## PRESSEMITTEILUNG

Cyber-Kriminalität

# Experte warnt: Web-Applikationen laden Hacker geradezu ein

- Datendiebstahl durch russische Hacker keine Überraschung
- Kundenportale und Webseiten sind Schwachstellen
- Unternehmen oftmals zu sorglos

**Bielefeld, 07.08.2014 – Am Mittwoch ist der mutmaßlich größte Datendiebstahl aller Zeiten bekannt geworden: Unbekannte Hacker sollen sich nach Angaben der US-amerikanischen IT-Firma Hold Security Zugang zu 1,2 Milliarden Passwörtern und Nutzernamen verschafft haben. Dies geschah über rund 420.000 Webseiten, darunter auch die Präsenzen großer Unternehmen. Für Christian Book, Senior Consultant beim IT-Beratungsunternehmen Ceyoniq Consulting, kommt der Vorfall wenig überraschend.**

Frage: Hat Sie die Nachricht von dem mutmaßlichen Datendiebstahl überrascht?

Book: Der Diebstahl an sich nicht, der kolportierte Umfang hingegen schon. Generell gilt aber: Die Zahl der Hacker-Angriffe auf Web-Applikationen und das Ausmaß der damit verbundenen Schäden für Unternehmen und deren Kunden steigen.

Frage: Wo genau setzen die Hacker an?

Book: Web-Applikationen wie Internetpräsenzen, Web-Shops oder Kundenportale sind für Hacker interessant. Diese Anwendungen enthalten häufig Programmierfehler, die ein Angreifer ausnutzen kann. Weit verbreitet sind beispielsweise sogenannte SQL-Injections, bei denen der Angreifer große Datenmengen beispielsweise mit Kundendaten oder Passwörtern aus Datenbanken stiehlt oder gezielt einzelne Datensätze manipuliert. Darüber hinaus bieten die Netzwerke der Unternehmen verschiedene Schwachstellen, von schlecht administrierten Firewall-Systemen bis hin zu Betriebssystemen, die nicht regelmäßig durch Updates aktualisiert werden.

Frage: Warum schützen sich die Unternehmen nicht ausreichend?

Book: Einerseits ist vielen Unternehmen das Risikopotential nicht bewusst, da IT-Risikoanalysen insbesondere bei kleinen und mittelständischen Unternehmen nur selten durchgeführt werden. Andere Unternehmen denken, sie seien für Angreifer gar nicht interessant oder argumentieren, dass bisher noch nie etwas passiert sei. Nicht zuletzt scheitert das Thema Informationssicherheit in einigen Fällen an den Ressourcen. Es mangelt an ausgebildeten Fachkräften und den notwendigen Budgets.

Frage: Wie entwickelt sich das Bewusstsein für solche Gefahren?

Book: Generell rückt das Thema Informationssicherheit in den letzten Jahren immer mehr in den Fokus. Schwerwiegende Hacker-Attacken auf große Konzerne wie Sony und die mediale Berichterstattung über Datenschutzverstöße schaffen ein Risikobewusstsein. Mit dem Bekanntwerden der NSA-Spionageprogramme wurde die Aufmerksamkeit noch einmal merklich erhöht. Wir re-

gistrieren seit einiger Zeit steigende Anfragen von kleinen und mittelgroßen Unternehmen.

Frage: Was können Unternehmen jetzt tun?

Book: Die letztlich Betroffenen sind in erster Linie Privatpersonen. Für sie ist es jetzt abermals ratsam, wichtige Passwörter zu ändern. Tatsächlich aber sind es die Betreiber von Web-Anwendungen, die ihre Hausaufgaben machen müssen. Viele Beratungsunternehmen bieten entsprechende Sicherheitsprüfungen an, zum Beispiel sogenannte Penetrationstests, bei denen Hacker-Angriffe simuliert werden. So lässt sich oft relativ schnell feststellen, ob und wo Handlungsbedarf besteht.

***Über Christian Book:***

*Christian Book ist Senior Consultant beim IT-Beratungsunternehmen Ceyoniq Consulting GmbH. Der studierte Wirtschaftsinformatiker arbeitet als "ethischer" Hacker und ist als sogenannter Penetrationtester vom International Council of Electronic Commerce Consultants (EC Council) lizensiert.*

*Christian Book zur aktuellen IT-Sicherheitsdebatte bei "RTL aktuell":*
*http://www.rtl.de/cms/news/rtl-aktuell/russische-hacker-bande-stiehlt-millionen-datensaetze-3e699-51ca-15-2000048.html*

*Christian Book zu IT-Sicherheitsmaßnahmen für Unternehmen bei "Handelsblatt Online":*
*http://www.handelsblatt.com/unternehmen/it-medien/it-sicherheit-denken-wie-ein-krimineller/10290822.html*

**Weitere Informationen unter:** www.ceyoniq-consulting.com

## Über die Ceyoniq Consulting GmbH:

Die Ceyoniq Consulting GmbH ist ein deutschlandweit tätiges IT-Beratungsunternehmen mit Sitz in Bielefeld und weiteren Standorten in Leipzig und Oldenburg. Seit der Gründung 2007 ermöglicht eine stringente Themen- und Branchenausrichtung dem Beratungshaus, komplexe Herausforderungen in Kundenprojekten zu konzipieren, zu realisieren und zu betreuen. Das Unternehmen fokussiert sich neben dem Leistungsspektrum Informationssicherheit (IT- und Web-Security sowie Datenschutz) ebenfalls auf Kunden aus der Energieversorgungswirtschaft (Prozess-/ Systemharmonisierung, Erneuerbare-Energien-Markt und regulatorische Themen/ BNetzA) und der Versicherungsbranche (Leben/ Schaden, Riester sowie Code of Conduct). Die Ceyoniq Consulting GmbH gehört zu der Ceyoniq Unternehmensgruppe, welche zusätzlich aus der Ceyoniq Innovations GmbH, der Ceyoniq Technology GmbH sowie der Ceyoniq Media GmbH besteht.

## Kontakt für Journalisten & Redaktionen:


Malte Limbrock
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Schumannstraße 71
53113 Bonn
Tel.: +49 (0)228 / 30412-630
Fax: +49 (0)228 / 30412-639
limbrock@agentur-sputnik.de
www.sputnik-agentur.de

Nils Dietrich
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Hafenweg 9
48155 Münster
Tel.: +49 (0)2 51 / 62 55 61-25
Fax: +49 (0)2 51 / 62 55 61-19
dietrich@sputnik-agenutr.de
www.sputnik-agentur.de