

DATENSCHUTZ-NEWS – DEZEMBER 2016

BSI: Zahl der Angriffe steigt

Wie bereits in den Vorjahren ist die Zahl der Angriffe auf IT-Systeme auch in 2016 wieder deutlich angestiegen. Dabei ist seit einigen Jahren eine Professionalisierung der Angreifer zu verzeichnen. Diese Angreifer operieren zumeist im Ausland.

Auch die Zahl der für die Angriffe eingesetzten Schadsoftwarevarianten steigt von Jahr zu Jahr. Waren 2012 noch rund 100.000.000 bekannte Schadprogramme im Einsatz, hat sich ihre Zahl bis zum Jahr 2016 fast versechsfacht.

Nicht gestiegen hingegen ist die Zahl der Angreifer, die sich mittels Identitätsdiebstahl Zugang zu den Identifikations- und Authentifizierungsdaten ihres Opfers verschafft haben. Begründet wird dies mit dem höheren Entdeckungsrisiko, dem sich Täter bei einem Identitätsdiebstahl ausgesetzt sehen.

Jedoch wird durch die Zahlen im Jahresbericht des BSI deutlich aufgezeigt, dass die Aufrechterhaltung der IT-Sicherheit ein wichtiges Thema für die Nutzer von IT-Systemen sein sollte – sowohl in Unternehmen als auch im privaten Bereich.

Quelle: intersoft consulting services AG

Yahoo wiederholt Daten gestohlen

Erst im September 2016 musste Yahoo zugeben, dass im Jahr 2014 ca. 500 Mio. Nutzerdaten

durch „staatlich unterstützte Angreifer“ gestohlen wurden. Mitte Dezember dieses Jahres wurde bekannt, dass bereits 2013 mind. 1 Milliarde Nutzerdaten entwendet wurden. Dabei handelt es sich um die Zugänge und Profile der Yahoo-Kunden.

Dabei ist es den Angreifern wohl gelungen, sich dauerhaft in den Quellcode von Yahoo einzunisten und so die Logins mitzulesen.

Quelle: newsrep.net

Datenleck bei Mitfahrgelegenheit.de

Das Mitfahrportal Mitfahrgelegenheit.de gibt es nicht mehr. Dennoch kam es zu einem großen Datendiebstahl.

Zusammen mit dem Portal Mitfahrzentrale.de wurden Mitfahrgelegenheit.de insgesamt circa 600.000 Nutzerdaten gestohlen. Obwohl das Portal seit März abgeschaltet ist, hatte ein Unbekannter bereits Ende Oktober unerlaubt die Datenbanken kopiert.

Dabei enthielten die Archiv-Datenbanken bspw. IBAN- bzw. Kontonummern, E-Mail-Adressen als auch Mobilfunknummer – teilweise mit Namen und Adressen.

Quelle: t3n.de

Polizei warnt vor gefährlicher Massen-E-Mail

Seit Anfang Dezember kursiert eine E-Mail, welche angeblich

vom „Polizeipräsidium Köln, Polizeiinspektion Cyberabteilung“ versandt wird. In dieser werden die Empfänger personalisiert angeschrieben und ihnen mitgeteilt, dass gegen sie ein Ermittlungsverfahren wegen Betruges bei der Polizei Köln geführt wird.

Die E-Mail enthält die angebliche Ermittlungsakte, welche als Word-Dokument angehängt ist. Sobald die Datei geöffnet wird, installiert sich automatisch ein Trojaner, der den Computer verschlüsselt und Online-Banking-Daten ausspäht. Die Polizei empfiehlt daher dringend, die E-Mail sofort zu löschen und den Anhang vorher nicht zu öffnen.

Quelle: newsrep.net

Wohnungsbaugesellschaften missachten Datenschutz

Mindestens neun Wohnungsbaugesellschaften in Deutschland übertragen sensible Daten unverschlüsselt im Internet. Hierbei handelt es sich um Eingaben in Interessenten- und Suchformulare wie bspw. Angaben über Einkommen, Arbeitsverhältnis und Sozialleistungen.

Inzwischen wurden die Sicherheitslücken durch die jeweiligen Wohnungsbaugesellschaften geschlossen. Die Datenschutzbeauftragten der entsprechenden Bundesländer wurden über die Fälle informiert.

Quelle: www.faz.net

Bayern bekommt eigenes Landesamt für IT-Sicherheit

Laut Finanzminister Markus Söder soll in Nürnberg ein Landesamt für IT-Sicherheit gegründet werden. Dessen Hauptziele sind die Abwehr von Internetkriminalität und Cyberterrorismus, der Schutz von Behördennetzen und die Beratung von Bürgern und Kommunen. Mit dem neu geschaffenen Landesamt soll eine neue Ebene der IT-Sicherheit erreicht werden.

Um dies umzusetzen, sollen bis 2025 rund 200 IT-Sicherheitsspezialisten in Nürnberg arbeiten. In der Anfangsphase würden jedes Jahr 20-30 neue Experten angestellt.

Quelle: www.br.de

Datenleck in der Telekom-Cloud

Durch eine Datenpanne konnte ein Nutzer des Hosted-Exchange-Angebots der Telekom tausende Kontakte aus den Adressbüchern anderer Kunden einsehen.

Heikel daran ist, dass sich solche Angaben bestens als Ausgangsbasis für gezielte Social Engineering-Angriffe missbrauchen lassen. Im Datensatz finden sich bspw. Vertreter von großen Organisationen wie einem Car-Sharing-Anbieter oder einem Tankstellenbetreiber sowie tausende kleinere Organisationen.

Die Telekom schrieb umgehend alle betroffenen Kunden an, um den Vorfall zu erklären. Zudem wurde die Aufsichtsbehörde über

den Datenschutzvorfall informiert.

Quelle: www.heise.de

Führerscheine offen einsehbar

Anwohner der Mülheimer Altstadt haben die Möglichkeit, einen Bewohnerparkausweis online zu beantragen. Hierbei müssen eine Reihe sensibler Dokumente (wie bspw. Führerschein, Fahrzeugschein) hochgeladen werden. Diese Daten sollten verschlüsselt an die Stadt übermittelt werden.

Jedoch veröffentlichte die Stadt die Daten unverschleiert und ohne Login-Verpflichtung im Internet. Somit hatte jeder die Möglichkeit zu sehen, wer einen Parkausweis beantragt hat und welche Dokumente vorgelegt wurden.

Laut der Stadt Mülheim handelte es sich hierbei um ein „Einstellungsproblem im Online-Antrag“, welcher nunmehr behoben ist.

Quelle: www.ruhrbarone.de

BND will angeblich WhatsApp knacken

Wegen der wachsenden Verbreitung sogenannte Krypto-Messenger fällt es dem BND immer schwerer, Kommunikationsinhalte einzusehen. Deshalb soll nun in den nächsten Jahren rund 150 Millionen Euro dafür ausgegeben werden, um Krypto-Messenger wie WhatsApp zu knacken.

Der Geheimdienst will in dem Projekt "ANISKI" ("Aufklärung nicht-

standardisierter Kommunikation im Internet") die Fähigkeiten entwickeln, wieder auf Inhalte von Messengern zugreifen können. Denn nach den Snowden-Enthüllungen führten immer mehr Messenger eine Ende-zu-Ende-Verschlüsselung ein, bei der weder die Anbieter noch Sicherheitsbehörden oder Geheimdienste direkt an Inhalte gelangen können.

Bewilligt sind die Gelder in Höhe von 150 Millionen Euro jedoch bislang noch nicht.

Quelle: www.heise.de

Spam-Welle bei Skype

Mitte November hatten Skype-Nutzer mit einer Spam-Welle zu kämpfen, die in Nutzerforen bereits zu zahlreichen Beschwerden geführt hat. Aufgrund dieser Welle erhielten die Nutzer unseriöse Werbenachrichten von ihren Kontakten. Diese Nachrichten beinhalteten Verlinkungen zu Angeboten von sonderbaren Produkten.

Das Problem geht hierbei von übernommenen Nutzer-Accounts aus, über die dann Spam-Nachrichten verschickt wurden.

Bei den „abgegriffenen“ Nutzerdaten handelt es sich um Nutzerdaten, die von anderen Diensten „erbeutet“ und anschließend von den Betrügern bei Skype massenhaft ausprobiert wurden. Unter den Opfern sind bspw. LinkedIn, Yahoo oder Dropbox.

Quelle: [intersoft consulting services AG](http://intersoftconsultingservices.com)