DATENSCHUTZ-NEWS – APRIL 2017

HURRA! Der Innovationspreis-IT gehört wieder uns!

Wir freuen uns sehr, dass uns die Initiative Mittelstand zum zweiten Mal in Folge mit dem Innovationspreis-IT 2017 – Prädikat BEST OF 2017 – für unser eLearning „Schulungen-Datenschutz" ausgezeichnet hat.

www.innovationspreis-it.de

Cloudmark kündigt für E-Mail-Sicherheit DANE/TLS an

Das Internet-Schwergewicht Cloudmark hat angekündigt, dass die kommende Version 5.2 der *Cloudmark Security Platform for Email* die auf DNSSEC gründende Sicherheitstechnik DANE/TLS nutzen wird.

Die Entscheidung wird ausdrücklich mit dem Verweis auf niederländische und deutsche Sicherheitsstandards begründet. In den Niederlanden ist der Einsatz der DANE-Technik für Behörden bereits verpflichtend. In Deutschland legt die BSI-Richtlinie TR-03108 „sicherer E-Mail-Transport" mit Chiffren, Methoden und auch der DANE/TLSA-Technik Kriterien für eine BSI-Zertifizierung fest.

Quelle: www.heise.de

Tausende Clouds anfällig in Deutschland

Über 20.000 in Deutschland betriebene Clouds, die veraltete Versionen der Software ownCloud und Nextcloud einsetzen, weisen zum Teil kritische Sicherheitslücken auf. Durch den unsicheren Betrieb können Angreifer auf die in der Cloud gespeicherten Daten zugreifen, sie manipulieren oder gar veröffentlichen.

Betroffen sind u. a. die Cloud-Anwendungen großer und mittelständischer Unternehmen, öffentlicher und kommunaler Einrichtungen, von Energieversorgern, Krankenhäusern, Ärzten, Rechtsanwälten und privater Nutzer.

Provider sind aufgerufen, ihre Kunden, die die Clouds in Eigenverantwortung betreiben, entsprechend zu informieren.

Quelle: www.bsi.bund.de

Windows 10 Creators Update

Microsoft hat nunmehr detailliert angegeben, welche Daten das Creators Update für Windows 10 über die Microsoft-Nutzer sammelt.

Konkret geht es dabei um Informationen zu dem Gerät, dessen Verbindungen und Konfigurierung sowie der Nutzung von Produkten und Services. Auch Daten zum Surf- und Suchverhalten aus dem Browser sowie Spracherkennungs- und Ortungsdaten werden gesammelt. Windows teilt den Servern außerdem mit, welche Musik der Nutzer hört oder welche Filme er schaut.

Laut Microsoft dient dieses Datensammeln dazu, Windows auf dem neuesten Stand und sicher zu halten.

Diese große Datenmenge wird laut Microsoft aber nur erfasst, wenn der Nutzer die Einstellungen unter „Feedback und Diagnose" auf „vollständig" belässt.

Quelle: t3n.de

US-Provider dürfen private Nutzerdaten verkaufen

Das US-Repräsentantenhaus hat eine Resolution des US-Kongresses bestätigt, welche die Regelung zum Schutz von Nutzerdaten wieder rückgängig macht.

Großen IT-Service-Providern ist es damit wieder erlaubt, das Surfverhalten ihrer Kunden ohne deren Zustimmung zu tracken und auch ungefragt weiterzugeben.

Quelle: www.golem.de

Hälfte aller Android-Geräte erhalten Sicherheitspakete nicht

Im Kampf gegen Playstore-Malware macht Google Fortschritte. Jedoch hat Google nunmehr zugeben müssen, dass mehr als eine halbe Milliarde Android-Geräte die regelmäßigen Sicherheitsupdates der Firma nicht erhält. Viele dieser Geräte haben daher eklatante Sicherheitslücken.

Was diese Sicherheitslücken bedeuten, zeigen bspw. zuletzt die Vault-7-Leaks. Demnach bedient sich auch die CIA solcher Lücken, um ihre Ziele auszuspionieren. Je später Lücken gestopft werden, umso einfacher haben es Angreifer wie die US-Nachrichtendienste.

Immerhin gibt sich Google Mühe, die Lücken so früh wie möglich zu entdecken. Im vergangenen Jahr hat das Unternehmen fast eine Million US-Dollar an unabhängige Sicherheitsforscher als Belohnungen für entdeckte Android-Lücken ausgezahlt.

Quelle: www.heise.de

Bußgeld wegen Geoscoring

Der Schufa-Konkurrent Bürgel (Hamburg) soll gemäß Erlass des Datenschutzbeauftragten Johannes Caspar eine Strafe wegen des Einsatzes von Geoscoring zahlen. Grund hierfür ist, dass Bürgel aufgrund einer Bonitätsanfrage einer Online-Firma hin dieser allein einen Scorewert über die Wohnanschrift des Kunden ermittelte.

Seit einer Reform von 2009 untersagt das Bundesdatenschutzgesetz, „ausschließlich" Wohnortdaten für die entsprechende Wahrscheinlichkeitsberechnung zu nutzen. Auskunfteien dürfen demnach nicht die potenzielle Zahlungsfähigkeit eines Betroffenen allein aus seiner Wohngegend ableiten, ohne weitere personenbezogene Informationen und Parameter einzubeziehen.

Die Zahlungsaufforderung ist auf 15.000,00 € festgesetzt. Die Firma Bürgel will das Urteil jedoch nicht akzeptieren.

Quelle: www.heise.de

Hacker erpressen Apple

Die Hacker-Gruppe „Turkish Crime Family" behauptet, sich Zugang zu 300 Millionen iCloud-Accounts verschaffen zu können und fordert nunmehr von Apple 75.000 Dollar in der virtuellen Währung Bitcoin oder Ethereum bzw. 100.000 Dollar in Form von iTunes-Geschenkkarten.

Aufgrund widersprüchlicher Angaben über die Anzahl der Accounts seitens der Hacker-Gruppe ist es jedoch fraglich, ob diese Drohung überhaupt real ist.

Nach einer internen Überprüfung durch Apple, habe es keinen Anhaltspunkt für einen Einbruch in das Firmensystem gegeben.

Quelle: datenschutz nord GmbH

Telnet-Lücke in Cisco-Switches

Cisco, ein US-amerikanisches Unternehmen aus der Telekommunikationsbranche, warnt vor einer kritischen Sicherheitslücke in über 300 Switch-Modellen. Diese Sicherheitslücke wurde durch eine Analyse der von Wikileaks mit Vault 7 enthüllten CIA-Dokumente entdeckt.

Die zuvor auch dem Hersteller nicht bekannte Schachstelle wirkt sich schon bei der standardmäßigen Konfiguration betroffener Geräte aus und kann über IPv4 oder IPv6 ausgenutzt werden. Dem US-Geheimdienst soll durch diese Zero-Day-Lücke der Zugang zu hunderttausend Geräten möglich gewesen sein. Cisco hat die gefährdeten Modelle bereits aufgelistet (Link) und die Veröffentlichung eines kostenlosen Software-Updates angekündigt, um die Schwachstelle zu schließen.

Zu diesem Zeitpunkt rät der Hersteller, bei den betroffenen Geräten Telnet zugunsten von SSH zu deaktivieren.

Quelle: www.zdnet.de

Möglicher Missbrauch von Gendaten

Saarbrücker Forscher des Kompetenzzentrums für IT-Sicherheit (CISPA) haben bewiesen, dass die Daten weniger unterschiedlicher micro-RNA ausreichen, um einen Personenbezug herzustellen. Die IT-Forscher haben daraufhin begonnen, micro-RNA-Datenbanken auf Datenmissbrauch zu untersuchen und konnten mit zwei Angriffsmethoden die Studienteilnehmer herausfinden. Aufgrund dessen hat CISPA entsprechende Gegenmaßnahmen zur Abwehr von Angriffen entwickelt.

Denn bspw. kann eine Krankenkasse mit den veröffentlichten Studienergebnissen herausfinden, ob ein Mitglied teilgenommen hat und unter welchen Krankheiten dieses leidet, sofern sie das micro-RNA-Profil des Mitglieds kennt.

Quelle: datenschutz nord GmbH