Das Magazin für Kommunalwirtschaft
www.rathausconsult.de

15. Jahrgang
20. Juni · Ausgabe 2/2016

# rathausconsult

## IT-SICHERHEIT FÜR KOMMUNALE INFRASTRUKTUREN UND PRÄVENTION VON CYBER-CRIME:

# Es kann jeden treffen

## ROUNDTABLE im Landeskriminalamt NRW

ISSN 1619-3105

rathausconsult

**ISSN1619-3105** 15. Jahrgang

**Herausgeber:**
Kommunal-Verlag GmbH
Klingelhöferstraße 8, 10785 Berlin
Telefon 0 30/2 20 70-4 71
Telefax 0 30/2 20 70-4 79
Geschäftsführer: Tim-Rainer Bornholt

**Verlag und Druck:**
Union Betriebs-GmbH
Egermannstraße 2, 53359 Rheinbach
Telefon 0 22 26/8 02-0
Telefax 0 22 26/8 02-1 11
E-Mail: verlag@ubgnet.de
HRB 10605 AG Bonn
Geschäftsführer: Rudolf Ley

**Chefredaktion:**
Andreas Oberholz (verantwortlich)
Holbeinstraße 26, 42579 Heiligenhaus
Telefon 0 20 56/5 73 77
Telefon 0 22 26/8 02-2 13 (Verlag)
Telefax 0 20 56/6 07 72
E-Mail: pressebuero_oberholz@t-online.de

**Anzeigen:**
Union Betriebs-GmbH
Egermannstraße 2, 53359 Rheinbach
Telefon: 02226 802-213
Telefax: 02226 802-111
E-Mail: elke.linstaedt@ubgnet.de

Wolfgang Braun, Braun Medien GmbH
Riedelstraße 14, 42349 Wuppertal
Telefon 02 02/3 17 86 93
Telefax 02 02/3 17 86 95
E-Mail: braun@braun-medien-gmbh.de

**rathausconsult** erscheint viermal jährlich.

Es gilt die Anzeigenpreisliste 1/2016
ab 1. Januar 2016.

**Titelfoto:** Fotolia / Marco2811

Dieser Ausgabe sind Werbebeilagen der Bundesanzeiger Verlag GmbH sowie der Verlag C.H. Beck oHG beigefügt. Wir bitten unsere Leser um Beachtung.

IVW-geprüft





# Es kann jeden treffen

Im Februar 2016 meldete das in Neuss angesiedelte Lukas-Krankenhaus „Land unter". Denn: Ein Computervirus hatte die renommierte 540-Betten-Klinik in die 1990-er Jahre zurückkatapultiert. Eine Schadsoftware sorgte dafür, dass alle IT-Systeme heruntergefahren werden mussten. Stattdessen wurde gedruckt und gefaxt, Befunde mit Boten übermittelt, etwa 15 Prozent der Operationen mussten abgesagt werden. Der Virus war von Hackern offenbar im Anhang einer E-Mail versteckt worden.

Das Problem: Neuss ist (potenziell) überall. So sind mehrere Krankenhäuser in Nordrhein-Westfalen in letzter Zeit von Computer-Viren angegriffen worden, nach Zeitungsberichten u.a. in Mönchengladbach, Essen, Köln, Kleve und Kalkar. Im August 2015 sollte eine Klinik im Ruhrgebiet mit einer Virenattacke gar zur Zahlung von Geld gezwungen werden. Was für die Computersysteme in Krankenhäusern gilt, ist natürlich auch für Verwaltung und kommunale Unternehmen eine Bedrohung. „Es kann jeden jederzeit treffen", warnte eindringlich ein Fachmann des Landeskriminalamtes NRW anlässlich des rathausconsult-Roundtables zum Thema IT-Sicherheit am 19. Mai in Düsseldorf (siehe S. 30 ff).

Wie kann man sich schützen, welche organisatorischen und technischen Maßnahmen müssen ergriffen werden? Deutschland steht vor einem tiefgreifenden digitalen Wandel, der alle Lebens- und Arbeitsbereiche erfasst. Während die Wirtschaft sich bereits sehr konkret mit der digitalen Transformation beschäftigt, stellt sich die Frage, ob die öffentliche Verwaltung und möglicherweise auch die kommunalen Unternehmen dem Stand der Technik und damit der Problematik noch deutlich hinterherhinken? Und wenn dem so ist: Liegt es an fehlenden Haushaltsmitteln, föderalen Strukturen oder ganz anderen Umsetzungshürden? Wie steht es beispielsweise um die Ausbildung des Personals? Nur mit den Mitarbeitern werden Veränderungsprozesse gelingen, formuliert die Bundesregierung in ihrem Programm „Digitale Verwaltung 2020". Aber wird diesen auch das nötige Rüstzeug an die Hand gegeben.

Und wie steht es grundsätzlich um die Ausbildung 4.0 der Generation, die in wenigen Jahren bei der Öffentlichen Hand und in der Wirtschaft den Karren ziehen soll? Ist die Digitalisierung in unseren Berufs- und weiterführenden Schulen als auch in der Grundausbildung des Verwaltungsnachwuchses in Deutschland angekommen? Ich habe da so meine Zweifel. Spätere Fortbildungskurse werden diese Misere nicht aufheben, fallen sie doch oft Budget- oder Ausbildungszeitbeschränkungen zum Opfer und setzen zudem ein freiwilliges Grundinteresse voraus. Viele Fragen, noch wenig Antworten. Wir werden uns deshalb an dieser Stelle noch häufig zu diesem Thema „treffen", wetten?

Ihr

CYBERATTACKEN AUF MOBILE GERÄTE

# Gegenwehr für **Behörden** und **Kommunen**

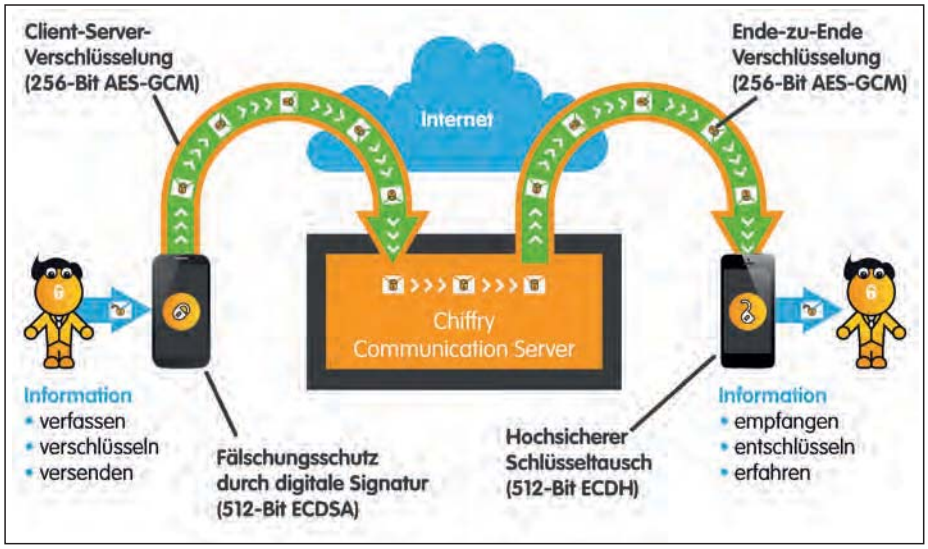
Die zunehmende Vernetzung von Geräten mit dem Internet liefert immer neue Angriffspunkte für Cyberkriminelle. Besonders mobile Applikationen sind ein wachsendes Einfallstor. Was tun?

Der digitale Wandel hält auf allen sozialen Ebenen Einzug und birgt zu den neuen Errungenschaften auch zahlreiche Gefahren. Wie angreifbar gesellschaftswichtige Institutionen sind, zeigten kürzlich erst die Cyberangriffe auf Krankenhäuser in Nordrhein-Westphalen. Durch eingeschleuste Computerviren wurde das IT-Sicherheitssystem der Kliniken durchbrochen. Folglich mussten anstehende Operationen tagelang verschoben werden. Zum Glück ohne tödlichen Ausgang für Pflegebedürftige.

Wie das Beispiel zeigt, ist die vernetzte Gesellschaft sowie die darin befindlichen Organisationen wie Städte und Kommunen vor solchen Attacken nicht ausreichend geschützt. Die zunehmende Vernetzung von Geräten mit dem Internet liefert stetig neue Angriffspunkte für Cyberkriminelle. Besonders mobile Applikationen sind ein wachsendes Einfallstor. Im Vergleich zum Vorjahr verzeichneten Android-Schadprogramme einen Zuwachs um 153 Prozent und iOS-Schadsoftware sogar ein Anstieg um 230 Prozent.

Darüber hinaus werden den Mitarbeiter und Mitarbeiterinnen von Behörden in der Regel keine datenschutzkonformen Anwendungen bereitgestellt, sodass die Gefahr besteht, dass ggfs. die benannten Anwender aus der beruflichen Motivation heraus, ihre privaten Endgeräte sowie privaten Messenger Dienst für berufliche Zwecke verwenden, mit dem Ziel einen einsatzbedingten zeitnahen Datenaustausch innerbetrieblich durchzuführen. Dies stellt einen dienstrechtlichen Verstoß dar und wird bei Kenntnisnahme mit disziplinarrechtlichen Maßnahmen ggfs. mit strafrechtlichen Konsequenzen geahndet. Zudem könnte ein erheblicher Imageschaden in der Öffentlichkeit die Folge sein.

Um dies zu vermeiden, ist es sehr erforderlich, dass auf Entscheider Ebene, innerhalb der Behörden, neben dem Verbot von unsicherem Messenger, geeignete Alternativen verwendet werden, die datenschutzkonforme Lösungen für ihre Mitarbeiter und Mitarbeiterinnen garantieren. Gut geeignet für diese Zwecke sind Anwendungen mit dem Qualitätszeichen „IT-Security made in Germany“ wie beispielsweise der Secure Messenger Chiffry.




## Voraussetzung für eine einheitliche Kommunikationsplattform

Diese Anwendung liefert die technische Voraussetzung für eine einheitliche Kommunikationsplattform zur einfachen und reibungslosen behördlichen Korrespondenz, intern wie extern. Chiffry ermöglicht die abhörsichere Telefonie, den verschlüsselten Versand von Bilder, Videos, Text- und Sprachnachrichten sowie alle anderen Dokumenttypen.

Der Einsatz ist ohne aufwendige administrative Tätigkeiten und Verschlüsselungsdefinitionen möglich. Für jede Nachricht generiert Chiffry einen neuen Verschlüsselungsschlüssel und versendet diesen an den Empfänger mittels moderner 512-Bit Elliptischen-Kurven-Kryptografie. Anschließend wird die Mitteilung mit einer Ende-zu-Ende-Verschlüsselung mit 256-Bit AES im GCM-Modus codiert, an den Empfänger zugestellt und dort mit dem bereits anvertrauten Schlüssel decodiert.

Die Chiffry-Funktionen bieten Behörden und Kommunen vorteilhafte Anwendungsmöglichkeiten. Zu dem einfach schnellen Informationsaustausch können Ämter bzw. deren einzelnen Abteilungen auch in Gruppen organisiert werden, die die interne Kommunikation zudem vereinfachen und fördern. Gerade bei externen Terminen werden Beamte über abteilungswichtige Informationen auf dem Laufenden gehalten. Dies kann ebenfalls mit Hilfe der

Broadcast-Funktion erfolgen. Damit können Führungskräfte den eingesetzten Beamten, unabhängig vom Arbeitsort, eine Art Rundmail bzw. Newsletter mit internen oder externen Neuerungen zusenden. Weiterhin können Treffpunkte oder Kontaktpersonen sicher übermittelt werden.

In der Basis- und Premiumversionen verläuft die Kommunikation über die sich in Deutschland befindenden Server. Diese sind in einem nach ISO 27001 zertifizierten Rechenzentrum untergebracht und löschen die Nachrichten sofort nach der Zustellung bzw. spätestens nach 21 Tagen.

Mit der Businessversion erhalten Behörden und Kommunen eine auf ihre Bedürfnisse angepasste Lösung sowie einen eigenen Kommunikationsserver in ihrem lokalen Rechencenter. Somit verschafft sie sich die umfassende Kontrolle über die erhobenen sensiblen und personenbezogenen Daten. Es wird somit sichergestellt, dass keine Informationen bei externen Serveranbietern gespeichert oder missbräuchlich verwendet werden.

Neben der Businessversion können auch die Basis- oder Premiumversion auf einem Smartphone installiert werden. Damit kombiniert die Anwendung das private- mit dem geschäftlichen Umfeld. Einen besonderen Schutz bieten Smartphones mit abgehärtetem Betriebssystem wie Knox oder BizzTrust. Diese Systeme ermöglichen die Einteilung des Endgerätes in einen sicheren und öffentlichen Bereich.

### Zusätzliche Absicherung

Somit werden nur vom Administrator definierte Anwendungen wie die Chiffry Businessversion im sicheren Bereich zugelassen. Die Premium bzw. Basisversion des Secure Messengers sowie andere Anwendungen können in dem öffentlichen Bereich installiert werden. Durch die Integration des Emoji-Sperrbildschirms mit Capture Protection wird der Zugang zum Messenger zusätzlich abgesichert. Entwickelt wurde Chiffry von der DIGITTRADE GmbH aus Teutschenthal in Sachsen-Anhalt. Das Unternehmen ist als Hersteller von hochsicheren verschlüsselten Festplatten bekannt.

Diese sind für viele Behörden keine Neuheit und werden in den einzelnen Abteilungen und Organisationen gern als Backupspeicher für die datenschutzkonforme Sicherung bzw. Archivierung der Daten verwendet. Die vom ULD zertifizierte Festplatte HS256S verschlüsselt die Daten mit 256-Bit AES im CBC-Modus und bewahrt diese mit Hilfe der 2-Faktor-Authentifizierung bestehend aus Smartcard und PIN.

Dank externer Speicherung des Verschlüsselungsschlüssels auf der Smartcard eignet sich diese Festplatte sehr gut für eine sichere und kostengünstige postalische Zustellung von hochsensiblen Daten zwischen einzelnen Kommunalämtern und anderen Behörden.

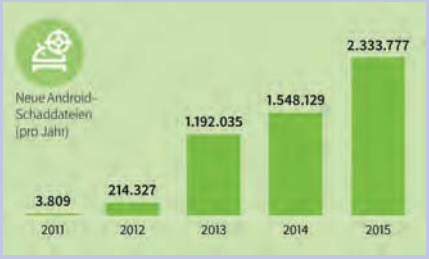

DER AUTOR

**Leonid Gimbut**
ist CEO der Digittrade GmbH in Teutschenthal.


ANDROID-SCHADDATEIEN

## Neues Rekordhoch

Allein in Deutschland nutzten 2015 fast 68 Prozent der Smartphone-Besitzer ein Gerät mit einem Android-Betriebssystem. Analog zu dieser Entwicklung stieg im vergangenen Jahr auch die Anzahl neuer Schädlinge auf ein Rekordhoch von über 2,3 Millionen. Im Vergleich zum Jahr 2014 (Gesamtzahl 1.584.129) steigt die Anzahl neuer Schad-Apps für Android um fast 50 Prozent. Für 2016 erwarten die G DATA Experten einen weiteren Anstieg von mobilen Schädlingen. Ein Grund: Immer mehr Anwender nutzen ihre mobilen Geräte als Alternative zum Desktop-PC für Online-Banking und –Shopping. Der G DATA Mobile Malware Report Q4/2015 ist online erhältlich.




758.133 neue Android-Schaddateien zählten die G DATA Sicherheitsexperten im vierten Quartal 2015. Im Vergleich zum dritten Quartal (574.706) beträgt der Anstieg damit fast 32 Prozent. Das Jahr 2015 erreicht damit wieder einen Negativrekord von insgesamt 2.333.777 neuen Schadprogrammen nur für das Android-Betriebssystem.

### G DATA Prognosen für 2016

- **Evolution der Android-Malware:** Cyberkriminelle sehen im Android-Betriebssystem die Möglichkeit auf hohe finanzielle Gewinne. In 2016 wird sich dieser Wandel vom PC zum Mobilgerät weiter fortsetzen. Die Experten rechnen daher erneut mit deutlich steigenden Schadcode-Zahlen.
- **Das Internet der Dinge im Cybercrime-Visier:** Gehackte Autos, Fitness-Armbänder oder Netzwerke: Das Internet der Dinge wird immer beliebter, sowohl in den eigenen vier Wänden als auch im Unternehmen. Kriminelle verstärken hier ihre Aktivitäten und suchen gezielt nach Sicherheitslücken, um diese auszunutzen. Zahlreiche Endgeräte werden über Android-Apps gesteuert. 2016 erwarten die Experten eine steigende Bedrohung.

### Info

Der G DATA Mobile Malware Report ist online erhältlich unter: https://secure.gd/dl-de-mmwr201504.

Die G DATA Software AG gilt als Erfinder des AntiVirus. Das 1985 in Bochum gegründete Unternehmen hat vor mehr als 29 Jahren das erste Programm gegen Computerviren entwickelt. Heute gehört G DATA zu den weltweit führenden Anbietern von IT-Security-Lösungen. Weitere Informationen: www.gdata.de