RUHR-UNIVERSITÄT BOCHUM

50 Jahre

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

SONDERAUSGABE

50 JAHRE FAKULTÄT FÜR ELEKTROTECHNIK UND INFORMATIONSTECHNIK

IT-SICHERHEIT

Smartphones, Browser, Ladesäulen schützen

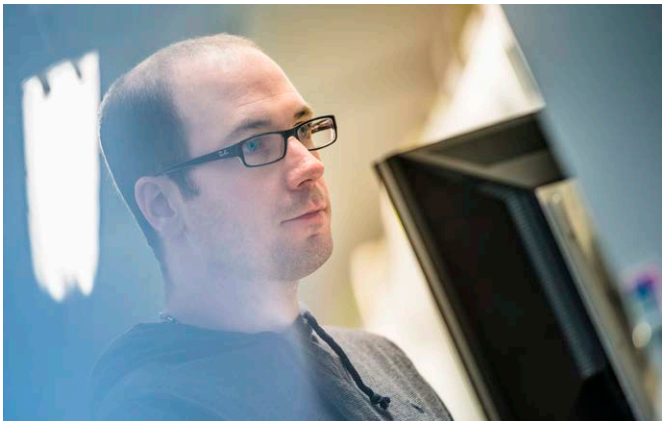
PLASMAFORSCHUNG

Kunststoffe dichter machen und Keime töten

#25 Jahrgang
Sonderheft | 2015
4,00 Euro

SMARTPHONE-APPS: GESUNDES MISSTRAUEN GEFRAGT

Ein Virenscanner für das Smartphone? Unnötig, hört man oft. Die Gefahr sei längst nicht so groß wie bei Desktop-Computern. Aber gerade Android-Nutzer sollten Vorsicht walten lassen. Ein Kommentar von Thorsten Holz



Prof. Dr. Thorsten Holz (Foto: dg)

Im Jahr 2007 führte Apple das iPhone ein und revolutionierte damit den Markt für Mobilfunkgeräte. Ein Jahr später startete der Siegeszug von Android. Seitdem hat sich die Technik deutlich weiterentwickelt. Mit ihrer Rechenpower und ihrem Speicherplatz sind moderne Smartphones quasi Computer für die Hosentasche. Sie speichern persönliche Daten wie Kontakte, Bilder oder SMS und werden auch zur Absicherung von anderen Diensten genutzt, zum Beispiel für mobile TANs beim Online-Banking. Dadurch haben sich die Geräte zu einem interessanten Angriffsziel für Cyberkriminelle entwickelt, und wir beobachten einen deutlichen Anstieg solcher Angriffe in den letzten Monaten.

Interessanterweise haben sich in der Smartphone-Welt zwei „Ökosysteme“ entwickelt, die aus Sicherheitssicht ziemlich unterschiedlich sind: Einerseits gibt es mit Apples Betriebssystem iOS ein eher geschlossenes System, bei dem der Hersteller eine (fast) vollständige Kontrolle über die Hard- und Software hat. Neue Apps kann man quasi nur über den App Store von Apple installieren, und auch ansonsten hat Apple eine starke Kontrolle über die Geräte. Andererseits ist Googles Android ein eher offenes System. Man kann neben „Google Play“ auch Marktplätze von Drittanbietern nutzen, um Apps zu installieren. Auch der Zugang für Entwickler ist einfacher. Das hat Folgen. Während Angriffe auf iOS-Geräte in der Praxis kaum zu beobachten sind, existieren viele Arten von Schadsoftware für Android. Dort entwickeln sich solche Angriffe gerade zu einem ähnlichen Problem wie für Desktop-Computer. Der Grund ist einfach: Während Google für seinen eigenen „Play Store“ viele Sicherheitsüberprüfungen einbaut und Apps detailliert untersucht, bevor sie zum Download angeboten werden, fehlen solche Überprüfungen bei vielen Drittanbietern. Angreifer nutzen dabei häufig die Gier der User aus: Sie stellen eine eigentlich kostenpflichtige App kostenlos zur Verfügung, aber haben die App zuvor um eine Schadkomponente erweitert. Wenn Nutzer solche Anwendungen installieren, infizieren sie unabsichtlich ihr eigenes Smartphone mit Schadsoftware – nur um ein paar Euro zu sparen.

Abhilfe ist also einfach: Installieren Sie Software nur aus vertrauenswürdigen Quellen, also zum Beispiel über den Google Play Store. Bei Gratis-Apps sollten Sie immer im Hinterkopf behalten, dass die Entwicklung solcher Apps nicht kostenlos ist und dass die Hersteller entsprechend irgendwie Geld verdienen müssen. Häufig tun sie das, indem sie Werbung anzeigen. Häufig aber auch, indem sie Daten über das Smartphone sowie den Nutzer sammeln. Ein gesundes Misstrauen ist also ratsam. Denken Sie vor dem Installieren von Apps immer an Ihre Privatsphäre, auch wenn es dabei häufig einen Konflikt zwischen Bequemlichkeit/Nutzbarkeit und der IT-Sicherheit gibt. Beides gleichzeitig zu erreichen ist leider schwierig.

Prof. Dr. Thorsten Holz, Systemsicherheit

REDAKTIONSSCHLUSS

99,9 %

DES UNIVERSUMS BESTEHEN AUS PLASMA.

Die Erde ist hingegen beinahe plasmafrei – bis auf Blitze, Feuer und Polarlichter. Da Plasmen aber den energiereichsten Zustand der Materie darstellen, sorgt der Mensch dafür, dass sie ein klein wenig häufiger auf der Erde werden. In Forschung und Industrie werden Plasmen technisch hergestellt und für eine Vielzahl von Anwendungen genutzt. Wofür? Ein paar Beispiele finden sich in diesem Heft auf den Seiten 12 bis 27.

Bild: NASA, ESA, and M. Livio and the Hubble 20th Anniversary Team (STScI)

IMPRESSUM

HERAUSGEBER: Fakultät für Elektrotechnik und Informationstechnik der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation (Abteilung Wissenschaftskommunikation) der Ruhr-Universität Bochum

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Abteilung Wissenschaftskommunikation, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25528, Fax: 0234/32-14136, rubin@rub.de, rubin.rub.de

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Raffaela Römer (rr)

Die Redaktion hat sich um die Einholung der nötigen Bildrechte mit allen Mitteln bemüht; wo das nicht möglich war, bitten wir eventuelle Rechteinhaber, sich mit der Redaktion in Verbindung zu setzen.

FOTOGRAFIE: Damian Gorczany (dg), Hofsteder Str. 45a, 44791 Bochum, Tel.: 0176/29706008, www.damiangorczany.de; Roberto Schirdewahn (rs), RUB Agentur

COVERFOTO: Damian Gorczany

WEBAUFTRITT: Andreas Rohden, Abteilung Markenbildung, RUB

GRAFIK, LAYOUT UND SATZ: VISUELL MARKETING GMBH, Springorumallee 2, 44795 Bochum, Tel.: 0234/459803, www.visuell-marketing.com

DRUCK: VMK Druckerei GmbH, Faberstrasse 17, 67590 Monsheim, Tel.: 06243/909-110, www.vmk-druckerei.de

AUFLAGE: 4.000

ANZEIGENVERWALTUNG UND -HERSTELLUNG: VMK GmbH & Co. KG, Faberstraße 17, 67590 Monsheim, Tel.: 06243/909-0, www.vmk-verlag.de

BEZUG: Die Sonderausgabe 2015 des Wissenschaftsmagazins RUBIN ist erhältlich in der Fakultät für Elektrotechnik und Informationstechnik der Ruhr-Universität, Gebäude ID, Etage 1, Raum 643. Das Wissenschaftsmagazin RUBIN erscheint zweimal im Jahr. ISSN 0942-6639