# Aktuelles aus dem Netz

**Von Christian Zwick, Kriminalhauptkommissar, Polizeipräsidium Rheinpfalz**

## Polizei 2020: Datenzugriff „jederzeit und überall“

Bundesinnenminister Thomas de Maizière verspricht, dass mit dem neuen System künftig jeder Polizist „jederzeit und überall Zugriff auf die notwendigen Informationen haben soll, die er oder sie für die Aufgabe benötigt“.
Umgesetzt werden solle dies durch ein „einheitliches IT-Haus der Polizeien“. „Polizei 2020“ heißt das Programm, das der Bund für die Entwicklung eines neuen polizeilichen IT-Systems für Bund und Länder aufgelegt hat. > Mehr, Meldung vom 14.12.2017.

## Bye, bye BIOS: Intel schickt den Klassiker in Rente

Chip-Hersteller Intel plant, seine Mainboards bald nur noch mit dem UEFI-Standard auszuliefern. Das altgediente BIOS soll verschwinden. > Mehr, Meldung vom 21.11.2017.

## Zankapfel Fahrzeugdaten: TÜV-Dachverband gegen Speicherung auf Hersteller-Servern

Moderne Autos mit ihrer Vielzahl von Sensoren und Steuergeräten sind nach verbreiteter Einschätzung durchaus anfällig für Hackerangriffe. Nach dem von der Autoindustrie bevorzugten Konzept sollen die Daten vom Fahrzeug auf sichere Server der Hersteller überspielt werden. Andere Unternehmen sollen dann nur auf dem Umweg über diese Server Zugriff auf die Daten erhalten. Davon hält der TÜV-Verband nichts: „Die Datenverarbeitung muss aus unserer Sicht im Fahrzeug stattfinden und darf nicht in Backend-Server ausgelagert werden“. > Mehr, Meldung vom 31.10.2017.

## Wie Hacker Ihr Passwort knacken

Passwort-Cracker haben Zugriff auf mehr gestohlene Passwörter und raffiniertere Hacking-Tools als je zuvor. Aufzuhalten sind sie nicht - tätig werden sollten Sie trotzdem. > Mehr, Meldung vom 20.11.2017.

## Pläne zum digitalen Gegenschlag: Wenn der Staat zum Hacker wird

Was tut ein Rechtsstaat, wenn ihm sensible Daten gestohlen wurden? […] Dem Parlamentarischen Kontrollgremium des Bundestags erläuterte Maaßen vor einiger Zeit seine Vorstellung einer digitalen „Nacheile“. […] Es müsse möglich sein, gestohlene „Daten löschen zu können, bevor sie weiterverbreitet werden“, sagte Maaßen. Deutsche Sicherheitsbehörden sollten Angriffsserver ausländischer Hacker auch selbst mit Schadsoftware infizieren dürfen, um mehr Informationen über die Angreifer zu sammeln. > Mehr, Meldung vom 10.12.2017.

## Android: Google bekommt Standortdaten auch ohne GPS-Aktivierung

Dafür verantwortlich ist der Firebase-Cloud-Messaging-Dienst. […] Dazu wird seit Anfang des Jahres der ungefähre Standort der Nutzer übermittelt, der durch Triangulation der Position zwischen verschiedenen Mobilfunkmasten ermittelt werden kann. Google will die umstrittene Praxis einstellen. > Mehr, Meldung vom 21.11.2017.

## Tool enttarnt Datensammler auf dem Handy

Spione enttarnt: Ein neues Tool enthüllt, welche Apps auf unserem Handy Daten an Dritte weitergeben und so heimlich unser Verhalten tracken. Dadurch können Nutzer erstmals in übersichtlichen Diagrammen und Grafiken selbst erkennen, mit welchen Drittservern das Smartphone kommuniziert. Noch ist diese Hilfssoftware ein Prototyp, aber die Forscher hoffen, sie schon bald als App zur Verfügung stellen zu können. > Mehr, Meldung vom 23.11.2017.

## Überwachungstechnik: Die Tücken der Gesichtserkennung

Die automatische Gesichtserkennung in Fotos und Videos macht große Fortschritte. Deutsche Behörden setzen seit Jahren auf die Technik. Doch es gibt Gründe, ihr zu misstrauen. > Mehr, Meldung vom 27.11.2017.