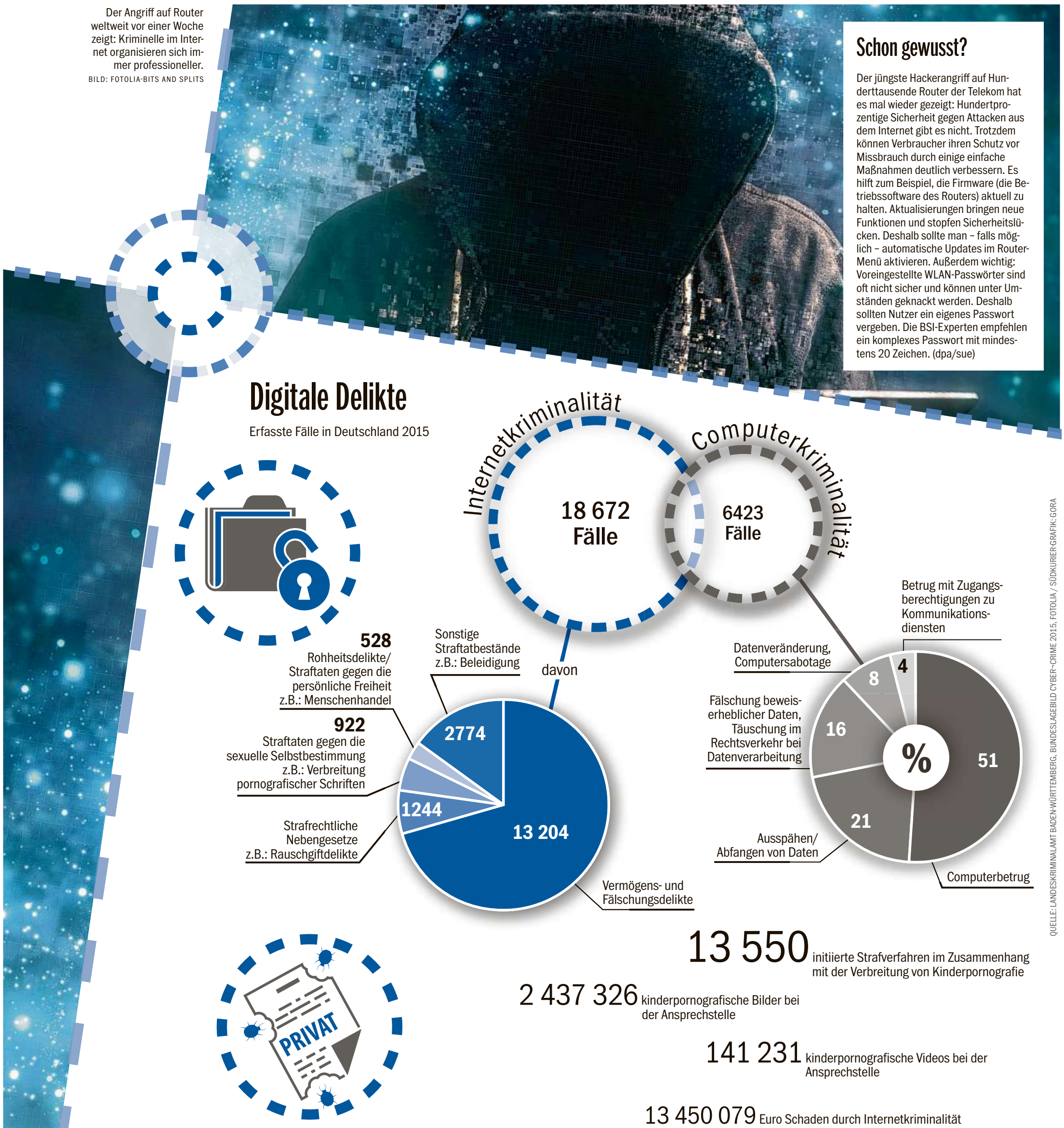

Der Angriff auf Router weltweit vor einer Woche zeigt: Kriminelle im Internet organisieren sich immer professioneller.
BILD: FOTOLIA-BITS AND SPLITS

Schon gewusst?

Der jüngste Hackerangriff auf Hunderttausende Router der Telekom hat es mal wieder gezeigt: Hundertprozentige Sicherheit gegen Attacken aus dem Internet gibt es nicht. Trotzdem können Verbraucher ihren Schutz vor Missbrauch durch einige einfache Maßnahmen deutlich verbessern. Es hilft zum Beispiel, die Firmware (die Betriebssoftware des Routers) aktuell zu halten. Aktualisierungen bringen neue Funktionen und stopfen Sicherheitslücken. Deshalb sollte man – falls möglich – automatische Updates im Router-Menü aktivieren. Außerdem wichtig: Voreingestellte WLAN-Passwörter sind oft nicht sicher und können unter Umständen geknackt werden. Deshalb sollten Nutzer ein eigenes Passwort vergeben. Die BSI-Experten empfehlen ein komplexes Passwort mit mindestens 20 Zeichen. (dpa/sue)

Digitale Delikte

Erfasste Fälle in Deutschland 2015

13 550 initiierte Strafverfahren im Zusammenhang mit der Verbreitung von Kinderpornografie

2 437 326 kinderpornografische Bilder bei der Ansprechstelle

141 231 kinderpornografische Videos bei der Ansprechstelle

13 450 079 Euro Schaden durch Internetkriminalität

QUELLE: LANDESKRIMINALAMT BADEN-WÜRTTEMBERG, BUNDESLAGEBILD CYBER-CRIME 2015, FOTOLIA / SÜDKURIER-GRAFIK: GORA

Was Sie über den jüngsten Hackerangriff auf Router weltweit wissen sollten

Der Angriff auf Router der Telekom war ein Schock. Aber was wollen die Hacker eigentlich erreichen und wie gefährdet sind Geräte anderer Anbieter? Wichtige Fragen und Antworten zum Thema.

1 Der Angriff, der die Geräte der Telekom lahmlegte, schreckte viele Menschen auf. Welches Ziel verfolgten die Angreifer? Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) war das Ziel, die Geräte mit Schadsoftware zu infizieren und in das Botnetz „Mirai“ einzubinden. Diese Bots sollten dann unauffällig im Hintergrund agieren. Je mehr Bots zu einem Netz gehören, desto größer ist auch die Masse der gleichzeitig aktiven Computer, über welche etwa Spam-Mails versendet oder auch sensible Daten ausspioniert werden können.

2 Ist es den Hackern gelungen, die Router in das Botnetz einzubinden? Nein, dieser Versuch schlug fehl, da die Telekom-Router immun gegen den eigentlichen Angriff waren. Die Sicherheitslücke, die die Hacker nutzen wollten, besteht in Geräten mit dem Betriebssystem „Linux“. Telekom-Router haben ein System des Herstellers „Arcadyan“.

3 Hatten die Hacker auch andere Router im Visier? Eindeutig ja, „der Angriff auf die Telekom-Router war Teil einer noch laufenden Angriffswelle auf Routersysteme aller Hersteller“ – mit dem Ziel, diese in das Botnetz zu integrieren, erklärt Jürgen Neuschwander, IT-Professor an der HTWG in Konstanz. Das heißt jedoch auch: Der Ausfall der Speedport Router der Telekom war nicht das eigentliche Ziel der Hacker.

4 Weshalb sind die Router dennoch ausgefallen? Jens Müller, Experte aus Konstanz und Chef des IT-Sicherheitsunternehmens MDBW, erklärt, dass an dem Zusammenbruch nicht die Schadsoftware schuld war, sondern die Tatsache, dass die Router mit Anfragen bombardiert wurden: „Wenn viele gleichzeitige Anfragen auf dem Port eingehen, geht das Gerät in die Knie und stürzt ab“, sagt er.

5 Sind die Geräte der Telekom mittlerweile wieder sicher? Die Telekom weist auf ihrer Homepage weiterhin darauf hin, dass ein Software-Update den Fehler beheben könne. Zur automatischen Aktivierung des Updates sollten Nutzer den Router 30 Sekunden vom Stromnetz (Netzstecker ziehen) nehmen und dann neu starten. Wer immer noch Probleme hat, kann die technische Hotline kontaktieren: 0800 330 1000. Infos und Links unter: **www.telekom.de.**

6 Müssen sich auch Besitzer anderer Router Sorgen machen? Laut Jens Müller sind „Router aller Hersteller potenziell gefährdet“, insofern diese über das Internet auf Port 7547 das TR-069 Protokoll (Fernwartung und Fernkonfiguration) bereitstellen. Denn so kann der Router aus dem Internet erreicht werden. Ein Angriff über den Port 7547 würde von der Fritzbox grundsätzlich abgewiesen, erklärt eine Pressesprecherin. Nur ein Provider könne dem Gerät einen Verbindungswunsch mitteilen. Andere Funktionen seien über diesen Port nicht erreichbar, versicherte sie.

7 Was müssten Hersteller tun, um Nutzer zu schützen? Die Hersteller müssten Sicherheitseinstellungen beim Design ihrer Geräte maßgeblich mitberücksichtigen, sagt etwa Thorsten Urbanski von G Data. Bei vielen Geräten würden vielfach Standard-Passwörter gesetzt, die von den Nutzern dann nicht geändert werden. Angreifer hätten damit ein leichtes Spiel. Das müsse sich unbedingt ändern.

8 Wer steckte eigentlich hinter dem Angriff auf Router weltweit? Wer hinter der Attacke auf Router weltweit steckt, ist unklar. Manche Politiker und IT-Experten sprechen jedoch davon, dass die Regierung Russlands etwas mit dem Angriff zu tun haben könnte. Bundeskanzlerin Angela Merkel (CDU) hat zum Beispiel einen möglichen Zusammenhang zwischen Cyber-Angriffen und der russischen Strategie „hybrider Auseinandersetzungen“ hergestellt. Zuvor hatte der Präsident des Bundesnachrichtendiensts (BND), Bruno Kahl, vor Daten-Angriffen und Desinformationskampagnen gewarnt, die aus Russland gesteuert würden. Es gebe „Erkenntnisse, dass Cyber-Angriffe stattfinden, die keinen anderen Sinn haben, als politische Verunsicherung hervorzurufen“. (sue/dpa)

SK Nicht nur Cyber-Kriminelle stellen im Online-Alltag eine Gefahr dar, sondern auch die Unwissenheit der Nutzer selbst. Mehr über die Tücken des digitalen Alltags lesen Sie unter: **www.sk.de/exklusiv**