



2020.

SEPTEMBER PriVacts - SecFacts

Interessante Neuigkeiten zu
Privacy/Datenschutz (.blue) und
Security/Informationssicherheit (.red) als
Newsletter. Zur viralen Verbreitung geeignet.



.blue: 16,7 Mio. € Bußgeld für italienisches Kommunikationsunternehmen

Der Kommunikationsanbieter Wind Tre hat mehrmals gegen die Datenschutzgrundverordnung verstoßen. Deswegen wurde ihm von der italienischen Datenschutzbehörde ein Bußgeld von 16,7 Mio. Euro auferlegt. Das Unternehmen hatte personenbezogene Daten seiner Kunden rechtswidrig zu Werbezwecken missbraucht. Die Kunden gaben keine Einwilligung zur Nutzung ihrer Daten zu Werbezwecken. So wurden Verbraucher in Form von Kurznachrichten, Telefonanrufen oder E-Mails mit Angeboten kontaktiert. Des Weiteren wurden verschiedene Angaben der Kunden in öffentlichen Telefonbüchern ohne vorherige Einwilligung publiziert. Auch die Handelspartner von Wind Tre wurden nicht ausreichend beaufsichtigt. Ein beauftragtes Drittunternehmen hatte tatsächlich personenbezogene Daten in rechtswidriger Weise gesammelt und ein Bußgeld von 200.000 Euro auferlegt bekommen. Wind Tre muss bei selbst beauftragten Firmen Kontrollen entsprechend selbst vornehmen.

[externe Quelle](#)

.red: Office-Dateien verbreiten auffallend oft Malware

Laut dem IT-Security-Spezialisten SonicWall werden MS-Office-Dateien auffallend oft von Kriminellen zum Verbreiten von Schadsoftware missbraucht. Fast ein Viertel aller Malware wird derzeit über MS-Office-Dateien, wie z.B. *.doc oder *.xls Dateien, verbreitet. In der ersten Jahreshälfte 2020 stieg die Anzahl der Angriffe über diese Dateikategorie auf mehr als das Doppelte an. Laut dem Report von SonicWall gab es bei Erpressungstrojanern wie Emotet einen Anstieg um 20 %. Ein Grund dafür sei, dass mehr Arbeitskräfte aufgrund von Corona im Home Office arbeiten und vermehrt auf die Online-



Anwendungen der Office-Suite zugreifen. Besonders gefährlich sind die Office-Dateien, die von Emotet verwendet werden. Diese kommen oft als Antwort auf eine eigene E-Mail von einem scheinbar vertrautem Absender. Eine neue Betrugsstrategie von Emotet zeigt eine Meldung beim Öffnen der Datei, dass das Dokument mit Windows 10 Mobile erzeugt wurde und der Empfänger deswegen auf den Button "Bearbeiten aktivieren" klicken müsse. Wer dieser Aufforderung folgt, startet Makros, die das System mit Emotet infizieren. Nur durch intelligente Virenschutzlösungen auf jedem Rechner und Tablet besteht die Möglichkeit, diese Infektionen vermeiden zu können – gerne beraten wir Sie bei Ihrem IT-Risk-Assessment bzw. Ihrer Risikoeinschätzung.

[externe Quelle](#)



.blue: Viele Beschwerden gegen Erfassung von Gästedaten in Bayerns Lokalen

Damit bei Corona-Fällen Kontaktpersonen ermittelt werden können, sind Gastronomen zur Erfassung von Gästedaten verpflichtet. Die bayerische Datenschutzbehörde hat mehr als 100 Beschwerden gegen die Erfassung der Gästedaten in der Gastronomie wegen der Corona-Krise erhalten. In manchen Restaurants seien Listen für mehrere Gäste verwendet worden. So könne der Gast, der seine Daten einträgt, die Angaben der Personen sehen, die zuvor gekommen seien, was datenschutzrechtlich sehr bedenklich und ohne korrekter Einwilligung auch unzulässig sei. Datenschützer empfehlen für jeden Tisch ein eigenes Blatt zu verwenden, um solche Probleme zu vermeiden. Bei mehrmaligen Verstößen, wäre auch ein Bußgeld möglich.

[externe Quelle](#)

Jetzt Newsletter abonnieren

JEDEN MONAT. PRIVACTS - SECFACTS

@S-COP GmbH 
@andreas.habedank 
@S-COP GmbH 

[Newsletter-Archiv](#)

S-COP GmbH | Rathausplatz 5 | 83684 Tegernsee

+49 8022 7058 185 | datenschutz@s-cop.bayern

Sitz der Gesellschaft: Tegernsee | Registergericht: München HRB 240890

Geschäftsführer: Andreas Habedank

Website | Datenschutz | Impressum

Wenn Sie diesen Newsletter nicht mehr erhalten möchten,
können Sie sich **hier abmelden**.