2020.
JULI

PriVacts - SecFacts

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

Als PDF öffnen

.blue: Millionen-Bußgeld für AOK Baden-Württemberg

Der LfDI Baden-Württemberg hat gegen die AOK Baden-Württemberg eine Geldbuße von 1,24 Mio. € verhängt. Grund dafür war ein Verstoß gegen die Pflichten sicherer Datenverarbeitung gem. Art. 32 DSGVO: Bei Gewinnspielen von 2015 bis 2019 erhob das Unternehmen personenbezogene Daten der Teilnehmer, neben Kontaktdaten auch deren Krankenkassenzugehörigkeit. Um die Daten der Gewinnspielteilnehmer auch zu Werbezwecken zu nutzen, mussten die Teilnehmer dafür einwilligen. Die Maßnahmen genügten jedoch nicht und folglich wurden personenbezogene Daten von mehr als 500 Gewinnspielteilnehmern ohne ausreichender Einwilligung zu Werbezwecken verwendet.

externe Quelle

.blue: Tiktok ist ein Datensammel-Alptraum

Tiktok ist die am schnellsten wachsende Social-Media-Plattform der Welt und wurde per "reverse engineering" überprüft. Die Schlußfolgerung ist niederschmetternd: „Tiktok sei ein Datensammel-Alptraum“. Im Januar-Newsletter hatten wir von gravierenden Sicherheitslücken der App berichtet, u.a. fehlende Verschlüsselung. Im März entdeckten Security-Experten, wie u.a. die Tiktok-App mitliest, was Nutzer in die Zwischenablage kopieren. Darunter sind z.B. Passwörter, Kontodaten, Nachrichten etc. Weiterhin werden Informationen über die genutzte Hardware, verbundene Netzwerke sowie sonstige verwendeten Apps gesammelt und der Standort der User wird getrackt. Es ist offensichtlich, wie solche mobilen Anwendungen Daten sammeln und für Werbezwecke unerlaubt genutzt werden. „Tiktok ist eine als soziales Netzwerk getarnte Malware.“

externe Quelle

.red: Ransomware: Gefälschte E-Mail im Namen der Bundesregierung

Die Ransomware-Angriffe setzen sich fort, wir berichteten bereits im April-Newsletter davon. Experten von Proofpoint, ein Unternehmen für Unternehmenssicherheit, haben eine neue Ransomware-Kampagne in Deutschland identifiziert. Diese nutzt als Köder eine gefälschte E-Mail im Namen der Bundesregierung, in der angeblich Dokumente zur Schließung des Unternehmens aufgrund Corona als Download-Link enthalten sind. Die E-Mail wurde vermehrt an deutsche Unternehmen aus dem verarbeitenden Gewerbe sowie die Lebensmittel- und Getränkeindustrie versandt. Der Link in der E-Mail sollte die PCs der potentiellen Opfer bei der Attacke verschlüsseln. Für eine Bezahlung von 200€ würden die Erpresser den PC wieder freischalten.

externe Quelle

Newsletter-Archiv

S-COP GmbH I Rathausplatz 5 I 83684 Tegernsee
+49 8022 7058 185 I datenschutz@s-cop.bayern
Sitz der Gesellschaft: Tegernsee I Registergericht: München HRB 240890
Geschäftsführer: Andreas Habedank