2020.
APRIL
PriVacts - SecFacts

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

.blue: Zoom: Zugangsdaten für hunderttausende Accounts im Darknet angeboten

Login-Daten für den Videokonferenzdienst Zoom sind Hackern in die Hände geraten. Die S-COP GmbH empfiehlt Ihnen eine vorsorgliche Passwort-Änderung. Die Daten wurden von Mitarbeitern der IT-Sicherheitsfirma Cyble im Darknet entdeckt und wurden teilweise sogar kostenlos online gestellt. Da in der Vergangenheit bereits mehrere Sicherheitsmängel bei Zoom bekannt wurden, ist ein großes Datenleck sehr wahrscheinlich. Google blockiert die Zoom-Software auf den Computern seiner Mitarbeiter, nachdem diverse Sicherheitslücken und Datenschutz-Probleme bekannt wurden. Der Videokonferenzdienst selbst hat jedoch noch kein Datenleck bekannt gegeben.

externe Quelle

.red: Massive Betrugsfälle bei Corona-Soforthilfe

Ermittler konnten einigen der Tätern das Handwerk legen. Der Umfang des Schadens ist noch nicht absehbar. Eine Kopie des gesamten Webauftrittes des NRW-Wirtschaftsministeriums stand öffentlich im Netz, darunter auch das Formular zur Beantragung der Corona-Soforthilfe. Die Täter konnten damit Daten von bis zu 4.000 Antragsstellern abgreifen. Diese wollten mit den gestohlenen Daten selbst die Corona-Soforthilfe erhalten und das Geld auf sog. Bankdrops überweisen lassen. Das sind Bankkonten, auf die die wirklichen Inhaber keinen Zugriff mehr haben. Laut NRW-Innenminister Herbert Reul wird derzeit mit Finanz- und Wirtschaftsministerium versucht ein System zu entwickeln, mit dem Fehler schneller erkannt werden.

externe Quelle

.red: COVID-19: Cyberangriffe auf Regierungen und medizinische Organisationen

Bedrohungsaktivitäten von Cyberangreifern steigen während der COVID-19-Pandemie, insbesondere Phishing-Angriffe werden vermehrt beobachtet. Eine Gesundheitsorganisation der kanadischen Regierung und eine medizinische Forschungsuniversität wurde durch Ransomware angegriffen. Die E-Mails enthielten alle einen bösartigen Phishing-Locker im Rich Text Format. Wird dieser mit einer anfälligen Anwendung geöffnet, versuchten die Angreifer, eine Ransomware-Nutzlast über eine bekannte Sicherheitslücke in einer Microsoft-Komponente, auszuliefern.

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
Website I Datenschutz I Impressum