

Phishing-Abwehr

7. Juli 2020

Deutsche Unternehmen sind beliebtes Ziel für Phishing-Angriffe

München. Deutsche Unternehmen sind besonders häufig im Visier krimineller Phishing-Angriffe. Dieses Risiko hat sich in der Corona-Pandemie nochmals verstärkt. Das zeigt der aktuelle Phishing-Report von Cofense. TÜV SÜD, ein führender neutraler Experte für Cyber-Sicherheit, Risk Awareness und Datenschutz, arbeitet als Partnerunternehmen mit Cofense bei der Phishing-Abwehr zusammen. Eine TÜV SÜD-Infografik zeigt, woran Phishing-E-Mails schnell erkennbar sind.

Seit Beginn der Corona-Pandemie und der damit verbundenen Zunahme von Fernzugriffen sowie deutlich höherem Online-Datenverkehr, ist besonders die Anzahl der Phishing-Versuche stark gewachsen. Diese Angriffsmethode erfreut sich allgemein großer Beliebtheit unter Hackern, umso mehr, weil das Arbeiten im Homeoffice oft schlechter gegen virtuelle Angriffe abgesichert ist als innerhalb eines Unternehmensnetzwerkes.



Aktuelle Zahlen aus dem Phishing-Report von Cofense für das erste Quartal 2020, zeigen, dass die Command-and-Control-Server krimineller Aktionen mit 4,78 Prozent am zweithäufigsten in Deutschland stehen. „Die tatsächliche Position einer Hacker-Gruppe kann sich zwar durchaus an einem anderen Ort befinden“, erklärt Stefan Vollmer, CTO bei TÜV SÜD Sec-IT. „Die hohe Zahl der Command-and-Control-Server lässt jedoch ebenfalls auf ein großes Interesse an deutschen Firmen schließen. Denn: Ein deutscher Server, von dem die Malware-Attacken ausgehen, sitzt in einem vertrauenswürdigen Land, weswegen manche Spam-Regeln möglicherweise nicht greifen und die Postfächer der deutschen Unternehmen es gewohnt sind, von dieser Quelle E-Mails zu erhalten.“

Außerdem, so Vollmer weiter, bieten deutsche Unternehmen schon allein deshalb grundsätzlich eine gute Angriffsfläche für Phishing Attacken, weil hierzulande einige Weltmarktführer zu Hause sind und dadurch viel Industrie und Know-how gebündelt vorhanden sind. „Kriminelle und erpresserische Angriffe werden dadurch umso lohnenswerter“, erklärt Vollmer. „Außerdem können die Informationen eines kleinen oder mittelständischen und schlechter geschützten Weltmarktführers – sogenannter Hidden Champions – interessanter sein, als die eines gut abgeschirmten Großkonzerns.“

TÜV SÜD ist Partner im Cofense® Managed Security Service Provider (MSSP)-Program. Gemeinsam bieten die beiden Unternehmen modernste Anti-Phishing-Services für Organisationen an. Da die meisten Angriffe von Cyberkriminellen mit einem versuchten Phishing-Angriff beginnen, sollten Unternehmen über die richtigen Werkzeuge verfügen, um diese Versuche rechtzeitig zu erkennen.

Mehr Informationen unter www.tuvsud.com/phishingabwehr.

Der aktuelle Cofense Phishing Report ist hier verfügbar: <https://go.cofense.com/q1-2020-phishing-review/>

Pressekontakt:

Sabine Krömer TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 29 35 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail sabine.kroemer@tuev-sued.de Internet www.tuvsud.com/de
--	---

Im Jahr 1866 als Dampfkesselrevisionsverein gegründet, ist TÜV SÜD heute ein weltweit tätiges Unternehmen. Mehr als 25.000 Mitarbeiter sorgen an über 1.000 Standorten in rund 50 Ländern für die Optimierung von Technik, Systemen und Know-how. Sie leisten einen wesentlichen Beitrag dazu, technische Innovationen wie Industrie 4.0, autonomes Fahren oder Erneuerbare Energien sicher und zuverlässig zu machen. www.tuvsud.com/de