

# Bei Anruf Abzocke

## INTERNETKRIMINALITÄT Falsche Microsoft-Mitarbeiter kapern Rechner

Internetkriminalität wird immer ausgeklügelter, die Opferzahlen steigen. Einer Studie zufolge war jeder zweite Internetnutzer 2018 von Kriminalität im Web betroffen. In Kooperation mit der Polizei geben wir Tipps.

VON NICOLE SCHIPPERS

Kassel – Das war ein Anruf zur rechten Zeit, zumindest schien es kürzlich einem 63-jährigen Kasseler so. Schon seit Längerem hatte er Computerprobleme, wollte seinen Rechner schon fast zum Fachgeschäft zur Reparatur bringen. Da klingelt sein Telefon, und ein angeblicher Service-Mitarbeiter des Software-Konzerns Microsoft ist dran. Man habe festgestellt, dass es mit dem Computer ein Problem gebe, sagt er, und bietet seine Hilfe an.

Der Kasseler nimmt sie dankbar an. Unter Anleitung des Anrufers installiert er eine Fernwartungssoftware. Tatsächlich richtet der Betrüger am anderen Ende der Leitung einen Trojaner ein, über den er auf den Rechner zugreifen und ihn nach Belieben ausspionieren kann, beispielsweise nach Passwörtern oder Zahlungsinformationen.

Anschließend möchte der angebliche Microsoft-Mitarbeiter für seine Hilfe natürlich entlohnt werden. Er fordert den Kasseler auf, ihm das Geld, um die 50 Euro, zu überweisen. Der kommt der Bitte nach, füllt die Überweisung samt Transaktionsnummern (Tan) online aus, scheidet



**Vorsicht bei Anrufen von angeblichen Microsoft-Mitarbeitern:** Ein Mann aus Kassel wurde kürzlich Opfer dieser Betrugsmasche.

FOTO: JULIAN STRATENSCHULTE/DPA

tert aber zu seinem Erstaunen drei Mal. Derweil hat der Anrufer die drei Tans abgegriffen und verwendet sie später, um sich jeweils 500 Euro vom Konto seines Opfers zu überweisen.

Als dem Kasseler die Beträge auf seinem Kontoauszug auffallen, erstattet er Anzeige. Zuvor hatte er noch auf Drängen des Anrufers eine iTunes-Geschenkekarte im Supermarkt gekauft und ihm den Code übermittelt, um damit die ausstehende Forderung zu bezahlen. iTunes-Kar-

ten sind ein beliebtes Mittel bei allen Arten von Internet-Betrügern, und -Erpressern: Die digitale Währung im iTunes Store lässt sich praktisch nicht nachverfolgen.

„Die Betrüger bringen ihre Opfer dazu, ihre Konto- und Kreditkartendaten zu offenbaren und ihren Personalausweis abzufotografieren“, schildert Jörg Bringmann vom Kasseler Kommissariat für Internetkriminalität das Vorgehen der Täter. Mit den Daten richteten sie oftmals ein Konto für die virtuelle

Währung Bitcoin ein, um anonyme Transaktionen tätigen zu können.

Eine leicht abgewandelte Variante der beschriebenen Betrugsmasche funktioniert auch ohne Anruf und könne jeden treffen, der im Internet surft, warnt Bringmann. Dabei erscheint eine Viruswarnung auf dem Bildschirm. Sie fordert dazu auf, eine gefälschte Kundendienstnummer des Windows-Herstellers Microsoft anzurufen. Andernfalls werde der Computer deaktiviert. Die Einblendung

lässt sich nicht schließen, der Bildschirm ist scheinbar gesperrt. Wer jetzt anruft, hat wieder einen vermeintlichen Microsoft-Mitarbeiter am Telefon, der den Anrufer überzeugen will, bis zu 400 Euro für ein Software-Wartungspaket gegen Viren zu zahlen und per Fernwartung Zugriff auf den Rechner zu geben.

Bringmanns Rat bei einem solchen Warnhinweis: Den Computer herunterfahren und neu starten. „Danach sollte der Warnhinweis verschwunden sein.“

### TIPP DES TAGES

#### Schnäppchen-Preise

 -Pullis

**50 %** günstiger

**Einzelteile**

bis zu

**70 %** reduziert

**Döring**

Fachgeschäft für  
bequeme Damenmode

Vellmar · Rathausplatz 3  
Tel. 05 61 / 82 14 87  
E-Mail: [info@modedoering.de](mailto:info@modedoering.de)  
[www.modedoering.de](http://www.modedoering.de)

### HINTERGRUND

#### Microsoft ruft nicht an

Die vermeintlichen Microsoft-Mitarbeiter sprechen laut Kriminalhauptkommissar Jörg Bringmann vom Kasseler Zentralkommissariat für Internetkriminalität meist Englisch oder gebrochenes Deutsch. Sie verwenden häufig eine vertrauenerweckende 0800-Service-Nummer. Microsoft erklärt, dass das Unternehmen keine unaufgeforderten Anrufe tätigt, wenn es um Supportanfragen geht. Die Kommunikation erfolge seitens Microsoft meist per E-Mail. Zudem erhebe das Unternehmen keine Zahlungsinformationen. Auch persönliche Daten sollten bei einem Anruf niemals herausgegeben werden. Betroffene können sich bei Microsoft unter [micro-soft.com/de-DE/concern/scam](http://micro-soft.com/de-DE/concern/scam) melden.

nis