„Microsoft-Mitarbeiter rufen nicht an“

Betrüger kaperten Rechner von mehreren Bürgern aus Stadt und Landkreis Kassel – Opfer installierten Fernzugriff-Software

Das Thema

Einbrüche, Enkeltrick, Phishing, Scamming und Internetbetrug, die Tricks der Kriminellen werden immer raffinierter, und die Opferzahlen steigen. In Kooperation mit der Polizei klären wir auf und geben Tipps zur Prävention.

Vorsicht bei Anrufen von angeblichen Microsoft-Mitarbeitern: Eine Frau aus Wolfhagen wäre beinahe das Opfer dieser Betrugsmasche geworden. Foto: Archiv

Von Bea Ricken

WOLFHAGER LAND. Die Wolfhagerin bereitet gerade das Mittagessen vor, als das Telefon klingelt. Ein „Mitarbeiter“ von Microsoft meldet sich und klingt besorgt: „Wir haben festgestellt, dass es mit ihrem Computer ein Problem gibt“, erzählt er der Frau aus Wolfhagen. Gern sei er ihr bei der Lösung des Problems behilflich. Die Wolfhagerin bedankt sich und schlägt vor, auf ihren Mann zu warten, der in Kürze zum Essen kommt. Der Mann am Telefon mahnt zur Eile, da sich ein Virus rasend schnell verbreite. Die Frau wird nervös und fährt den Computer hoch. Die 0800-Servicenummer auf dem Display wiegt sie in Sicherheit.

Unter Anleitung des Anrufers beginnt die Wolfhagerin ahnungslos eine Fernzugriffs-Software zu installieren. In diesem Moment ruft ihr Mann an. Sie erzählt ihm, dass sie gerade am Computer Hilfe von einem netten Microsoft-Mitarbeiter erhält. Ihr Mann hat schon von der Betrugsmasche gehört: „Zieh sofort den Stecker vom Computer raus“, brüllt er ins Telefon. Panisch reißt sie den Stecker aus der Dose und beendet das Telefonat.

Jörg Bringmann, stellvertretender Leiter des Internetkommissariats Kassel, nimmt den Fall später auf. „Die Frau hatte nochmal Glück, es war haarscharf“, sagt er. „Uns liegen mehrere Anzeigen von Opfern vor, die in den vergangenen Monaten von angeblichen Microsoft-Mitarbeitern per Telefon dazu gebracht wurden, Zugriff auf ihren PC zu gewähren. Den Opfern entstanden dabei finanzielle Schäden von mehreren hundert Euro“, so Bringmann. Im Präsidium sind in jüngster Zeit auch unzählige Strafanzeigen von Bürgern aus der Stadt und dem Landkreis Kassel eingegangen, die Anrufe von angeblichen Englisch sprechenden Service-Technikern der Firma Microsoft bekommen haben.

„Wenn die Täter ihre Opfer dazu gebracht haben, eine Fernzugriffs-Software, beispielsweise Teamviewer oder Ammyy auf ihrem PC zu installieren, könnten sie den gekaperten Computer von jedem Ort auf der Welt fernsteuern“, warnt Bringmann. „Microsoft ruft nicht an“, betont er.

Fenster auf dem Bildschirm

Die Mircosoft-Betrugsmasche geht auch ohne Anruf. Dann erscheint auf dem PC bei Internetnutzung plötzlich eine Einblendung mit einem angeblichen Computerproblem. Die Einblendung ist dabei so konzipiert, dass sie sich nicht einfach löschen lässt und der Bildschirm scheinbar gesperrt ist. Es wird eine Servicenummer mit eingeblendet, die man anrufen soll.

Wer darauf hereinfällt, hat wieder die hilfsbereiten „Mitarbeiter“ von Microsoft am Telefon.

HINTERGRUND

Anrufe meist auf Englisch

Die angeblichen Mitarbeiter von Microsoft, Apple oder anderen Unternehmen sprechen in der Regel englisch. Sie geben vor, dass der Computer des Angerufenen durch Schadsoftware belastet und sofortiges Handeln nötig ist, um eine Sperrung zu verhindern.

Wer sich auf das Spiel einlässt, wird von den Anrufern aufgefordert, eine Fernwartungssoftware wie Teamviewer oder Ammyy aufzuspielen. Diese Tools sind legal und kostenfrei. So wird auch keine Antivirensoftware aktiv. Im Anschluss bittet der Betrüger um die Teamviewer-Teilnehmernummer. Damit kann er sich auf dem Computer des Opfers einwählen und seine Arbeit verrichten. (ewa)

WLAN sofort beenden

Polizei gibt Tipps, wie man sich vor Telefon-Betrügern schützt

Wenn die Täter Zugriff auf den Rechner des Opfers haben, agieren sie so schnell, dass man die Schritte als ungeübter PC-Nutzer kaum nachvollziehen kann. Sehr gern wird die Antivirensoftware deaktiviert und neue Schadsoftware nachgeladen, zum Beispiel Spionagetools, die Passwörter ausspähen und Trojaner, die Daten verändern.

Ist der angebliche Reparaturvorgang abgeschlossen, möchten die Täter auch ihre Bezahlung dafür haben. So gibt es Fälle, wo Kreditkartendaten abgefragt wurden und später viel höhere Preise berechnet wurden. Zusätzlich werden Onlinebanking und andere Konten manipuliert. Die Polizei gibt Tipps, wie man sich schützen kann:

1. Microsoft und andere Supportanbieter rufen ihre Kunden nicht auf diese Art und Weise an. Sollten Sie einen solchen Anruf bekommen, beenden Sie das Gespräch. Falls diese Anrufe nerven, können Sie diese gegebenenfalls im Router/Telefon auf eine Sperrliste setzen, damit diese nicht mehr durchgestellt werden.

2. Sollten Sie auf eine entsprechende Webseite gelangen, bewahren Sie Ruhe. Beenden Sie die Webseite oder den Browser. Ein Neustart sollte in der Regel auch helfen. Eventuell muss der Browser entsprechend zurückgesetzt werden. Starten Sie zur Sicherheit Ihre eigene Antivirensuche mit einer ausführlichen Suche.

3. Notieren Sie die Rufnummer, die bei Ihnen auf dem Display erscheint. Auch wenn diese Rufnummer in der Regel durch die Täter gefälscht ist.

4. Sollten die Täter mittels Fernzugriff bereits auf Ihrem Rechner sein. Notieren Sie die Teilnehmernummer des Remote-Computers, mit dem der Zugriff auf Ihren Rechner erfolgt. Weitere Ermittlungen übernimmt die Polizei.

5. Prüfen Sie ausführlich Ihren Computer mit einer aktuellen Antivirensoftware. Zusätzliche Prüftools bekommen Sie auch auf **www.botfrei.de**

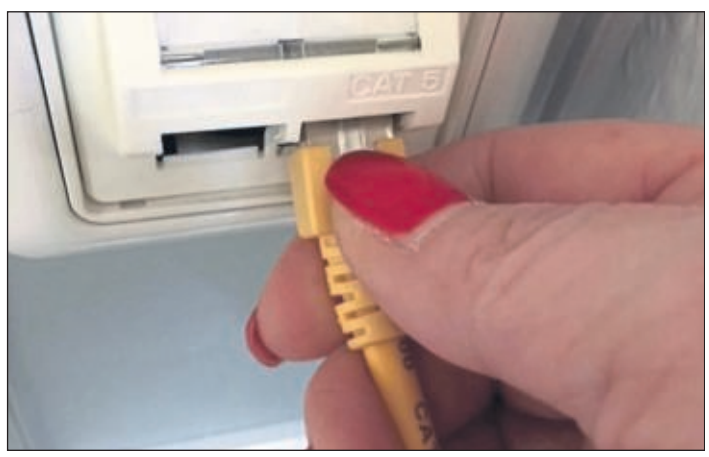
6. Beenden Sie die Internetverbindung (LAN-Kabel ziehen/WLAN beenden).

7. Bei Einblendungen hilft zumeist schon die Tastenkombination <Strg> F4 oder ein Reset des Computers. Eine regelmäßige Software-Aktualisierung des Internetbrowsers und der genutzten Java Scripts erschweren die Manipulation des Rechners.

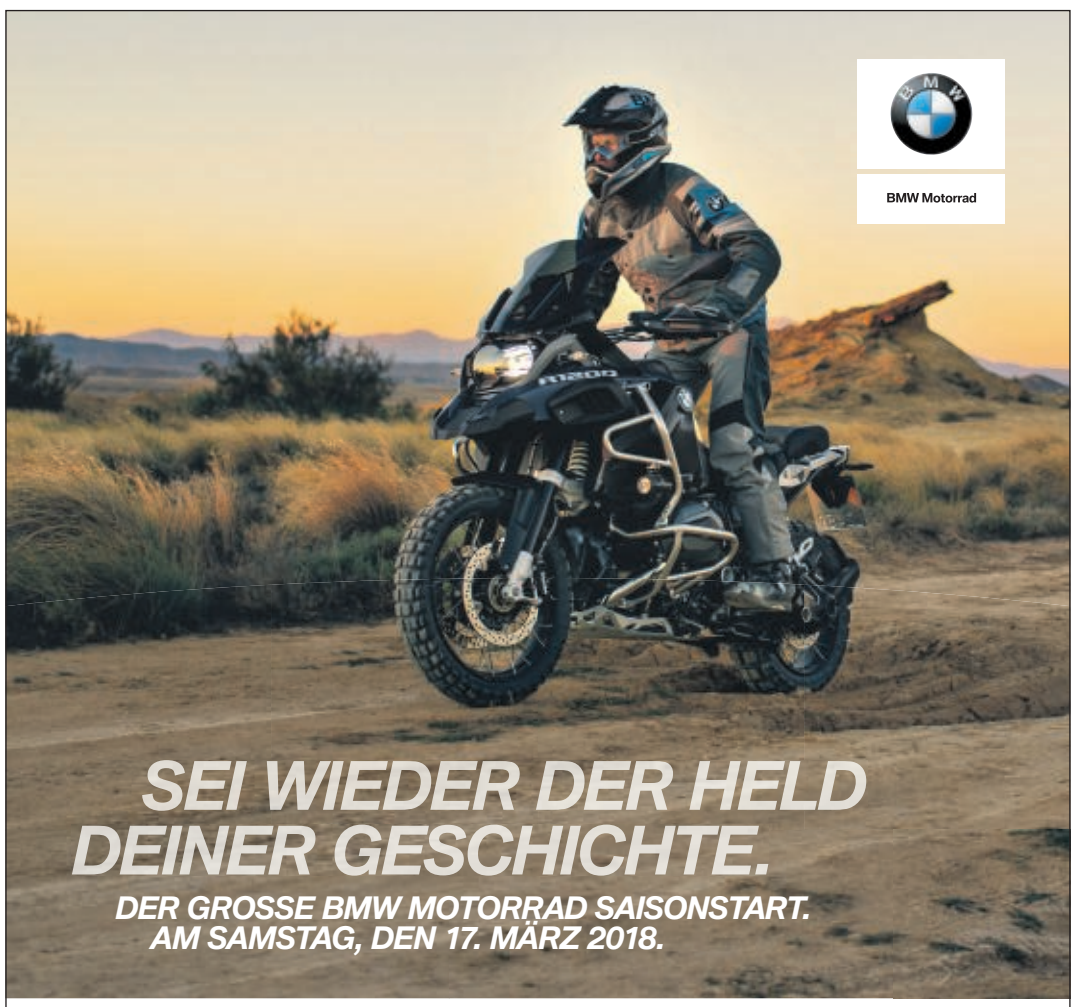
8. Informieren Sie die örtliche Polizei und erstatten Sie im Schadensfall Anzeige. Sollten Bankdaten (oder vergleichbare Daten) benutzt worden sein, informieren Sie unverzüglich die entsprechende Bank. Achten Sie zukünftig auf unberechtigte Abbuchungen. Gegebenenfalls sollte eine Kreditkarte sofort gesperrt werden.

9. Da der Täter, wenn er Zugang zum Computer hatte, alles Erdenkliche auf den Rechner aufgespielt haben könnte, sollte man sich mit einer Fachfirma in Verbindung setzen und den Rechner erforderlichenfalls reinigen lassen.

Mehr Tipps unter: http://zu.hna.de/betrugsanrufe



Verbindung trennen: Wenn die Betrüger schon Zugriff auf den Computer haben, hilft manchmal noch Kabel ziehen. Foto: Ricken



Endlich wieder Freiheit auf zwei Rädern spüren. Endlich wieder Deine eigene Geschichte schreiben – jede Kurve, jeder Hügel und jede Abfahrt bieten Stoff für neue Kapitel.

Und für jede gute Geschichte braucht man bekanntlich einen guten Einstieg: den großen BMW **Saisonstart am Samstag, den 17. März von 9:00 bis 16:00 Uhr in Deinem BMW Motorrad Zentrum Kassel.**

Feiere den offiziellen Start in die Saison 2018 bei spannenden Benzingesprächen mit Gleichgesinnten, leckeren Snacks und vielem mehr.

Also: Gib Gas, feiere mit uns und mach Deine Bike-Saison 2018 legendär!

Wir freuen uns auf Dich!

BMW AG Motorrad Zentrum Kassel
www.kassel.bmw-motorrad.de

Scharnhorststraße 14
34125 Kassel
Tel.: 0561-57000-998