# Mich hat eine Firma angerufen und gesagt, dass mein Computer mit Schadsoftware verseucht sei

**Vorsicht:** In letzter Zeit häufen sich erneut Anrufe von Betrügern, die sich als Mitarbeiter von Microsoft ausgeben, um an sensible Daten zu gelangen.

## Wie gehen die Betrüger vor?

Die Angerufenen werden typischerweise angeleitet, auf ihrem Computer die Ereignisanzeige (Englisch Event-Viewer) aufzurufen, mit welchem jegliche Ereignisse und Aktivitäten des Computers aufgezeigt werden können. Auch ein einwandfrei funktionierendes System produziert gelegentlich Fehlermeldungen. Je nach Alter und Konfiguration des Computers kann die Liste der Fehlermeldungen im Event-Viewer sehr lange sein, ohne dass das System ein grundsätzliches Problem hat. Das Aufrufen-Lassen dieses Programms wird von den Support-Anrufern typischerweise benutzt, um den Opfern eine glaubwürdige Kulisse zu präsentieren respektive Angst zu machen. Ziel der Betrüger ist, die angerufene Person dadurch zu überzeugen, ein Fernzugriffs-Programm (Remote Access Tool) herunterzuladen und ihnen dann Fern-Zugriff auf den Computer zu erlauben. Die Betrüger erlangen auf diese Weise vollen Zugriff auf das System und damit dieselben Möglichkeiten, den Computer zu manipulieren, wie wenn sie selbst direkt davorsitzen. Schliesslich wird meistens versucht, dem Opfer eine Softwarelizenz oder eine Dienstleistung (Systemreinigung oder Schutz vor Hackerangriffen) zu verkaufen, wozu dann nach Kreditkarteninformationen gefragt oder eine Barüberweisung verlangt wird.

## Was genau passiert mit meinen Daten?

Es ist von Fall zu Fall verschieden, was diese Personen jeweils genau auf einem Computer anstellen (Kopieren/Manipulieren/Löschen von Daten, Installation von Programmen, Einrichten einer Hintertür um später wieder auf das System zugreifen zu können, etc. oder aber einfach Zeit verbringen um dann die Bezahlung der Dienstleistung zu fordern).

## Was kann ich als Betroffener tun?

Da keine allgemeingültige Aussage zur Vorgehensweise der Täterschaft (respektive den Täterschaften) gemacht werden kann, empfehlen wir jeweils, den Computer von einer Fachperson untersuchen zu lassen oder die Festplatte des Computers komplett zu löschen und das Betriebssystem neu zu installieren. Hierbei muss allerdings beachtet werden, die persönlichen Daten jeweils vorab zu sichern, damit diese nicht verloren gehen.

Zudem sollten nach der Säuberung/Neuinstallation des Computers (oder von einem anderen Computer aus) bei allen Internet-Diensten, welche damit genutzt wurden, die Passwörter geändert werden.

Sollten Sie Ihre Kreditkartendaten angegeben haben, empfehlen wir Ihnen, mit Ihrem Kreditkarteninstitut Kontakt aufzunehmen, damit dieses die Kreditkarte sperren kann.

**OCOM AG** Englisch-Gruss-Strasse 6, Postfach 556, 3902 Brig-Glis
**OCOM STORE** Kantonsstrasse 21, 3902 Brig-Glis, **shop.ocom.ch**
T 027 922 10 10, F 027 922 10 11, ocom@ocom.ch, www.ocom.ch