

# Hackerangriff auf mein WLAN

---

## 1. Vorinformation

Ich bin von einem raffinierten Computerhacker überfallen worden und ich möchte Ihnen gerne den Ablauf schildern. Ich habe die Kreditkarten und alle meine Konti sofort gesperrt und die Firma Viseca, bei welcher ich die Kreditkarten habe, hat mich angehalten nichts gegen die Hacker zu unternehmen. Ich denke die Firma Viseca wird versuchen die Gauner ausfindig zu machen. Wenn Sie Ihrerseits bereits gewisse Informationen über diese Gauner haben, oder gegen Sie vorgehen wollen, bitte ich Sie deshalb höflich, mit Viseca Kontakt aufzunehmen. Aber ich denke, dass ich nicht das erste Opfer dieser Betrüger war und auch nicht das letzte und Sie deshalb vielleicht schon in dieser Sache mit der Firma Viseca oder anderen Kreditkartenfirmen zusammenarbeiten. Ich hoffe deshalb, dass diese Gauner so schnell wie möglich gefasst werden können, damit der Schaden nicht noch grösser wird.

## 2. Ablauf

Am Freitag den 21. August wurde ich um 13:40 von einem Herrn Alex Marshall angerufen. Er behauptet bei Microsoft USA zu arbeiten und für die Überwachung der Internetsicherheit zuständig zu sein. Ein Server von Microsoft hätte gemeldet, dass auf meinem Computer Online Hacking Files seien und diese die Sicherheit gefährden. Er sprach nur Englisch und er könne mich nicht mit jemandem verbinden der Deutsch spreche, da niemand dort Deutsch spreche. Auf die Frage was denn diese Online Hacking Files seien antwortete er mir nur, dass diese das gesamte Internet infizieren könnten und viel gefährlicher als Viren seien. Danach wollte ich wissen wie ich diese erkennen und unschädlich machen könne. Darauf antwortete er mir, dass es mir unmöglich sei diese zu erkennen und ich könne sie auch nicht vernichten, da diese in ganz normalen Betriebssystem Files versteckt seien. Aufgrund der Informationen die er auf seinem Server vorgefunden habe, wisse er welche Betriebssystem Files infiziert seien. Und nur er hätte aufgrund der Meldungen die Information welche Files auf meinem PC ersetzt werden müssten und nur er hätte die Rechte um einzelne Betriebssystem Files herauszugeben. Er dürfe diese nicht per E-Mail versenden und ich könne nicht wissen wo diese auf dem PC zu finden wären. Würde eigentlich soweit glaubwürdig klingen, aber im Nach hinein muss ich mir vorwerfen, dass ich ihn länger über diese Online Hacking Files ausfragen hätte sollen. Aber im Nachhinein ist man immer schlauer. Ich kann mir auch nicht vorstellen, wie mir da irgendjemand Betriebssystem Files einfach so austauschen hätte können, da sowohl die Firewall wie auch der Virens scanner immer aktiv sind. Ausserdem verwende ich Kaspersky Internet Security, welches laut Tests von renommierten Computerzeitschriften der beste und umfangreichste Schutz bietet. Er bat mich dann mit dem Command Interpreter diverse Commands auszuführen, womit wir auf diverse Seiten von Microsoft gelangten, Seiten die ich zuvor via Google auch schon besucht hatte, also eigentlich nichts Neues. Aber mit dem herumspielen mit diesen Commands wollte er mich wohl überzeugen, dass er tatsächlich ein Microsoft Mitarbeiter war. Und deshalb war ich nach wie vor der festen Überzeugung, dass er wirklich ein Mitarbeiter von Microsoft USA sei, denn er schien alle Commands aus dem ff zu kennen wie ein Profi. Leider weiss ich erst jetzt, dass genau das seine Masche war. Weiter erklärte er mir wie ich das Logfile öffnen könne und er sagte, dass ich selber auch darin die Fehler- und Alarm Meldungen finden könne. Ich fand natürlich keine, da ja auch keine da waren, denn wie bereits gesagt ist mein PC hervorragend geschützt und arbeitet auch immer zuverlässig und sauber. Er wies mich an, nach diesen Fehler zu suchen, aber da ich mich damit nicht auskannte wusste ich nicht wie ich vorgehen sollte. Da ich nach wie vor davon überzeugt war, dass er wirklich ein Mitarbeiter von Microsoft USA sei, gewährte ich ihm auch Zugang auf meinen PC. Er wies mich an, eine Software von der Homepage von Microsoft zu installieren, was ich denn leider auch ausführte. Das war dumm wie ein kleines Kind, aber wie bereits gesagt glaubte ich inzwischen selbst an diese ominösen Online Hacking Files und vor allem, dass er wirklich ein Mitarbeiter von Microsoft USA sei. Eine äusserst raffinierte Masche zwar, aber im Nachhinein durchschaubar, aber eben im Nachhinein weiss man immer alles besser.

Nun ging alles sehr schnell, ich kam da überhaupt nicht mehr mit was er da innerhalb kürzester Zeit alles anstellte. Auf jeden Fall war das besagte Logfile plötzlich voller Fehler und ich weiss wirklich nicht wie er das so schnell gemacht hat. Ausserdem behauptete er, dass meine Lizenz ungültig sei, das obwohl ich immer alle Updates bekommen habe. Der PC sei jetzt von Microsoft gesperrt worden und er würde mir diesen wieder freischalten, sobald ich eine Gebühr von 17€ bezahlt hätte. Auf diesem PC arbeite ich immer noch mit dem guten alten Windows XP, obwohl ich seit dem 8. April 2014 von Microsoft keine Updates mehr bekomme.

Aber diese Updates brauche ich auch nicht, denn ich habe mir mit Acronis True Image ein Image erstellt womit ich meinen PC jederzeit wieder in einen bestimmten Zustand zurückversetzen kann. Ausserdem kann ich die gesamte HD mit dem Acronis – Tool richtig löschen und nicht nur irgendein billiges Formatieren bei welchem dann doch nichts richtig gelöscht wird. Danach kann ich einen neuen MBR und das Image das ich in einem gesunden Zustand des PCs erstellt habe darauf spielen. Damit ist mein PC wieder völlig gesund. Dadurch würde auch seine Sperrung wirkungslos, aber ich hatte ganz einfach keine Lust mich mit Microsoft darüber zu streiten.

Er bestand darauf, dass ich ihm diese 17€ mit Kreditkarte bezahle. Leider habe ich das gemacht und so gelangte dieser Gauner an meine Daten der Kreditkarte. Die Bezahlung als solche sah genau gleich aus wie bei jeder anderen Zahlung auch, nur dass er mir dabei zusehen konnte habe ich nicht gewusst. Er behauptete dass meine Überweisung irgendwie nicht richtig gelaufen sei und dass er mich am darauf folgenden Tag noch einmal anrufen würde. Das ganze Prozedere dauerte mehr als 3 Stunden und ich hatte nun genug und machte das, was ich schon vor 3 Stunden hätte machen sollen. Ich unterbrach das Geplänkel und hängte auf.

Danach logte ich auf einem anderen PC ein um meine E-Mails zu lesen. Da war eine Mail von der Firma Viseca, bei welcher ich die Kreditkarten habe, dass ich sie umgehend zurückrufen solle. Man erklärte mir, dass da innerhalb der letzten paar Stunden um die 1000 CHF auf meine Kreditkarte belastet worden waren und ob das meine Überweisungen seien. Ich liess natürlich sofort die Karte Sperren und erklärte ihm den Vorfall und dass diese Zahlungen ein Betrug seien. Auch sperrte ich sicherheitshalber alle weiteren Konti auf der Bank, für den Fall, dass dieser Betrüger noch irgendwelche Daten auf meinem PC gefunden haben könnte.

Ich habe heute noch nach der Nummer von welcher er mich angerufen gegoogelt. Diese lautet 00688899. Hätte ich das sofort gemacht, wäre ich nicht auf diesen Betrüger hereingefallen. Aber nachdem ich den Anruf entgegengenommen habe, habe ich die Nummer nicht mehr gesehen und ja, im Nachhinein ist man immer schlauer. Aber vielleicht sollte man die Öffentlichkeit vor solchen Anrufen warnen, damit sich die Menschen von solchen Betrüger gar nicht erst auf ein Gespräch einlassen.