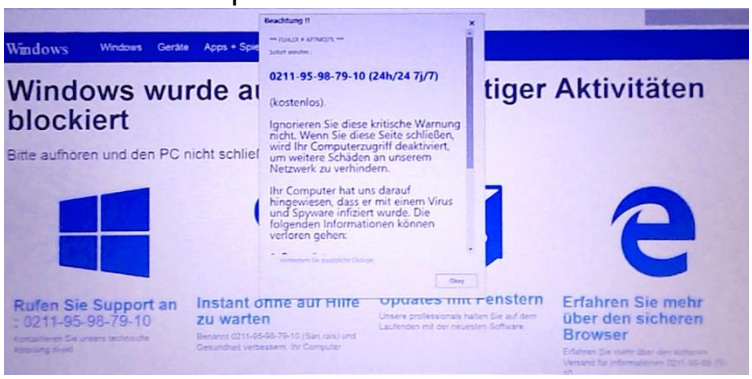
Diese zwei Betrugsversuche gibt es immer noch!

Wir möchten erneut eindringlich vor zwei Betrugsversuchen warnen, die immer noch in Deutschland die Runde machen. Über beide Fälle haben wir in der Vergangenheit bereits mehrfach berichtet. Dennoch erreichen uns fast jede Woche neue Anfragen von Menschen, die Opfer dieser Kriminellen wurden. Daher haben wir uns entschieden, die beiden Fälle erneut zu schildern und zu erläutern, was zu tun ist, falls Sie selbst in diese Situation geraten. Bitte seien Sie nicht übermütig und denken Sie nicht: “Darauf werde ich schon nicht reinfallen, das kenne ich ja schon.” Die Betrüger sind sehr clever, eloquent und wirken äußerst seriös – oft scheinen Sie sogar besorgt zu sein, behaupten, sie wollen helfen. Der gesamte Auftritt und der Eindruck, der beim Opfer erweckt wird, lassen in keinster Weise an einen Betrug denken!
Die beiden Methoden können beschrieben werden als “**Der angebliche Microsoft-Anruf**” und “**Die angebliche Hacker-E-Mail**“. Wir schreiben hier extra “angeblich”, da beide Szenarien von den Betrügern frei erfunden sind: weder stammt der Anruf von einem echten Microsoft-Mitarbeiter, noch kommt die Mail von einem echten Hacker.

1. Der angebliche Microsoft-Anruf

Die Betrüger geben sich als Microsoft-Mitarbeiter aus und rufen auf dem Telefon zuhause an. Die Anrufer erzählen Ihnen (oft in schlechtem Englisch), auf Ihrem Computer gäbe es ein Sicherheitsproblem und es müsse sofort gehandelt werden. Dafür bieten die Anrufer sofortige Hilfe an, und zwar per Fernwartung direkt auf dem Computer. Haben die Kriminellen erst einmal Zugriff auf den Computer erlangt, können sie dort alle möglichen Dinge anstellen. Das Dreisteste ist: Danach verlangen sie für ihre angebliche Hilfeleistung sogar noch eine Zahlung.
Es gibt eine Variante dieser Betrugsmasche: Oft verzichten die Betrüger auf den Anruf und blenden stattdessen eine Meldung auf Webseiten ein, die der Nutzer besucht. Das heißt, man ist im Internet unterwegs und plötzlich öffnet sich ein neues Fenster, das alles andere überlagert (siehe Foto). Die Meldung sieht aus, als ob der Windows-Computer selbst den Warnhinweis ausgeben würde.



Dabei handelt es sich aber um eine klassische Werbeanzeige, die nicht von einer seriösen Firma gebucht wurde, sondern von den Betrügern. Die Werbung ist so geschickt gestaltet, dass niemand merkt, dass es Werbung ist. Jeder Nutzer wird im ersten Augenblick denken, es sei eine Warnmeldung vom Windows-Computer. Die “kritische Warnung” behauptet, dass der Computer blockiert sei und weitere Schäden drohen, weil der Computer mit einem Virus infiziert sei. Oft wird auch behauptet, es müsse ein Sicherheitsupdate installiert werden, man solle schnell handeln. Doch Gottseidank, die Rettung sei nahe, es gäbe eine schnelle Möglichkeit per Fernwartung, um den Computer sicher zu machen. Aber: Die “schlimmen angedrohten Konsequenzen” sind in Wahrheit völlig aus der Luft gegriffen und wer auf die Fernwartung eingeht, ist in die Falle getappt. Gehen Sie auf diese Fernwartung ein, so erlangen die Kriminellen vollen Zugriff auf Ihren Computer, können dort Änderungen vornehmen, Daten und Passwörter ausspionieren und Schadprogramme installieren.

Danach verlangen die Betrüger für die angebliche Reparatur Ihres Computers, wie oben bereits erwähnt, sogar noch Geld.

Was ist zu tun?
Wenn Sie einen solchen Anruf erhalten sollten, **beenden Sie sofort das Gespräch und legen Sie auf**. Sind Sie auf den Betrugsversuch hereingefallen, dann sollten Sie die während des Betrugs installierte Software sofort entfernen, **alle (!) Kennwörter ändern und den PC mit einem Virenschutzprogramm untersuchen**. Wenn Sie nicht genau wissen, wie das geht, holen Sie sich Hilfe von Experten. Leisten Sie auf keinen Fall eine eventuell geforderte Zahlung! Außerdem können Sie Ihr örtliches Polizeirevier kontaktieren und den Vorfall zur Anzeige bringen. Denn dieser aktive schadhafte Betrugsversuch sollte, anders als bei Spam-Mails, zur Anzeige gebracht werden.

2. Die angebliche Hacker-E-Mail

Die E-Mail, die seit über 2 Jahren für besonders große Aufregung sorgt, ist unglaublich dreist. In der E-Mail behauptet der Absender ganz unverblümt, er hätte Ihren Computer gehackt. Doch damit nicht genug. Der angebliche Hacker behauptet weiter, er hätte zudem Ihre Kamera am Computer gehackt und Sie dabei gefilmt, wie Sie sich unseriöse Internetseiten angesehen hätten. Nun droht der Absender damit, diese Aufnahmen zu veröffentlichen und an alle Ihre Bekannten zu schicken, wenn Sie nicht einen bestimmten Betrag bezahlen. Die Mail endet also mit einer Erpressung.
Diese Mail kursiert in verschiedenen Versionen, zunächst nur auf Englisch, mittlerweile aber auch auf Deutsch. Die Mail hat vielen Menschen einen sehr großen Schrecken eingejagt, vermutlich weil die Vorgehensweise so neu ist. Noch nie zuvor hat in einer Spam-Mail ein Betrüger uns so direkt angeschrieben und behauptet, er hätte unseren Computer gehackt. Vermutlich aus diesem Grund wurde die Mail von vielen Menschen ernst genommen. Wir haben in den letzten Wochen immer wieder Zuschriften von Menschen erhalten, die uns fragten, was sie nun machen sollen.

Was ist zu tun?
Die Antwort ist ganz einfach: Nichts! Sie müssen nichts tun, außer die Mail sofort zu löschen. Alles an dieser Mail ist frei erfunden! Egal wie abenteuerlich die Vorwürfe und Behauptungen klingen, lassen Sie sich bitte nicht davon verunsichern! Ignorieren Sie die Mail, löschen Sie sie und denken Sie nicht mehr darüber nach. Es ist einfach nur ein dreister Betrugsversuch, nichts weiter. **Ihr Computer wurde nicht gehackt, Ihre Kamera wurde nicht gekapert und es wurde auch kein Video von Ihnen gemacht.**
Diese Mail wurde auch nicht an Sie persönlich versendet, sondern wird millionenfach verschickt. Es bringt daher auch nichts, die Polizei zu informieren (anders als im ersten Fall der Anrufe). Es handelt sich um eine herkömmliche Spam-Mail, die aus dem Ausland verschickt wird. Auch wir haben diese Mail schon dutzendfach erhalten. Die Polizei kann hier kaum etwas unternehmen, der Absender ist kaum zu ermitteln.

Quelle: https://levato.de/diese-zwei-betrugsversuche-gibt-es-immer-noch/