Bei Anruf Abzocke

Falsche Microsoft-Support-Anrufe

Betrüger geben sich als Microsoft-Techniker aus und ergaunern mit haarsträubenden Drohungen Lösegelder von Windows-Anwendern. Die Polizei feiert erste Erfolge gegen die meist im Ausland sitzenden Banden. Letztlich hilft gegen die Masche aber nur eine möglichst flächendeckende Aufklärung der Nutzer.

Von Hajo Schulz

Sein Rechner sei von einem Virus befallen und Teil eines Botnetzes. Wenn er dagegen nicht sofort etwas unternehme, werde Microsoft ihm seine Windows-Lizenz sperren: c't-Leser Rainer L. (Name geändert) fiel aus allen Wolken über das, was ihm der angebliche Microsoft-Support-Mitarbeiter da am Telefon eröffnete.

Um seiner Drohung Nachdruck zu verleihen, forderte der Anrufer L. auf, mal dieses, mal jenes Windows-Programm zu starten und ihm vorzulesen, was es ausgibt. Natürlich deutete er jede Antwort als weiteren Beweis für seine Behauptungen. Für zusätzlichen Stress sorgte dabei, dass der Anrufer englisch mit indischem Akzent sprach – L. bezeichnet seine eigenen Englisch-Kenntnisse als eher schwach.

Den drohenden Verlust seiner Windows-Lizenz und etlicher für ihn wertvoller privater Dateien vor Augen ließ L. sich schließlich dazu überreden, auf seinem Rechner eine Fernzugriffs-Software zu laden und dem vorgeblichen Microsoft-Techniker Zugang zu dem PC zu gewähren. Der setzte zunächst seine haarsträubende Show fort, mit der er L. davon überzeugen wollte, dass mit dem Rechner etliches im Argen liege. Unter anderem führte er die Webseite pcscan.us vor, die angeblich einen kompletten Rechner-Scan im Browser durchführt. Ein Blick in den Quelltext offenbart aber sehr schnell, dass die Seite nach dem Durchlauf der Fortschrittsbalken nur eine zufällig ausgewürfelte Zahl von vermeintlichen Sicherheitslücken, Registry-Fehlern und Ähnlichem ausgibt.

Mithilfe des Windows-eigenen Systemkonfigurationsprogramms (msconfig) demonstrierte der Anrufer schließlich, dass dieser Rechner nur noch eingeschränkt laufe und Microsoft schon etliche Dienste stillgelegt habe. Das lasse sich eindeutig an der hohen Zahl von „Beendet"-Einträgen auf der Seite „Dienste" des Programms erkennen. Dass das ein völlig normales Bild auf praktisch jedem Windows-PC ist, verschwieg der Anrufer geflissentlich.

Zu guter Letzt machte der Anrufer L. weis, dass seine Windows-Lizenz ohnehin nicht mehr gültig sei. Dazu führte er L. den Zertifikat-Manager von Windows vor, öffnete dort die Eigenschaften irgendeines abgelaufenen Microsoft-Zertifikats und behauptete, das sei das Windows-Zertifikat. L. müsse es erneuern, um sein Windows weiter benutzen zu können. Wenn er jetzt 29 Dollar bezahle, erwerbe er damit ein „Lifetime Certificate“ und sein Windows führe auch wieder alle Dienste aus.

Späte Einsicht

Irgendwann im Verlauf des Gesprächs ist L. klar geworden, dass er wohl eine Dummheit begangen hat und gerade geleimt wird. Der Anrufer hatte aber glaubhaft versichert, dass der PC mittlerweile gesperrt sei und L. ihn nicht werde benutzen können, solange er nicht das Windows-Zertifikat bezahlt habe. Einfach auflegen und den Fernzugang kappen kam also nicht mehr in Frage. Auf eine Sofort-Überweisung per Online-Banking aus der Fernsitzung heraus wollte er sich aber nicht einlassen – wer weiß, was sein beobachtender Gesprächspartner mit den Bankdaten anstellen würde, die er dabei in die Finger bekäme?

Dazu, dem Anrufer einen Scan seines Personalausweises zu schicken, ließ L. sich aber schließlich doch überreden. Warum er seinem sehr geduldigen und offenbar in Gesprächsführung geschulten Gegenüber diesen Wunsch erfüllte, kann er sich im Nachhinein nicht mehr erklären. Das gefühlt ewig dauernde Gespräch, bei dem man sich zum Überwinden der Sprachbarriere immer wieder gegenseitig Sätze in den Google Translator eintippte, hatte ihn wohl weichgekocht. Dem Ziel, seine angebliche Zahlungspflicht zu erfüllen, ist er damit jedenfalls nicht näher gekommen.

Man einigte sich schließlich darauf, dass die Rechnung über eine Bareinzahlung bei dem Finanzdienstleister Western Union beglichen werden solle. Als Empfänger sollte L. einen angeblichen Microsoft-Agenten in Taiwan eintragen. Dabei ergab sich allerdings das Problem, dass Western Union einen solchen Geldtransfer erst ab einem Betrag von 300 Euro anbietet. L. solle doch einfach 329 Euro überweisen; den überschüssigen Betrag werde Microsoft auf demselben Weg umgehend zurücküberweisen, versprach sein Gegenüber. Wenig überraschend blieb diese Überweisung bis heute aus.

Mit einer gefälschten Systemdiagnose soll das Opfer davon überzeugt werden, dass sein Rechner befallen ist. In Wahrheit prüft die Seite gar nichts und gibt nur Zufallszahlen aus.

Immerhin wurde L. nach der erfolgten Zahlung das Kennwort mitgeteilt, mit dem er sich wieder an seinen PC anmelden konnte. Zum Sperren des Zugangs hatten die Angreifer das Windows-eigene Programm syskey verwendet: Mit ihm lässt sich ein Kennwort vergeben, das den Teil der Registry verschlüsselt, in dem die Informationen über die Benutzerkonten gespeichert sind. Nach jedem Neustart muss man daraufhin dieses Kennwort eingeben, bevor man sich an Windows anmelden kann. Mit demselben Programm und dem richtigen Passwort lässt sich die Verschlüsselung anschließend auch wieder auf den Standard zurücksetzen, bei dem der Schlüssel im System gespeichert ist und vor der Anmeldung keine Kennwortabfrage stattfindet.

Auch wenn er all seine Programme und Dateien anscheinend unversehrt vorgefunden hat, bleibt für L. ein mulmiges Gefühl: Was mögen die Angreifer in den Stunden, während derer sie Zugriff auf seinen Rechner hatten, alles an Hintergrundprogrammen installiert haben? Welche Daten haben sie abgegriffen? Immerhin hat L. auf seinen Bankkonten in den ersten drei Wochen nach dem Angriff keine verdächtigen Aktivitäten bemerkt. Auch hat sich bislang niemand aus seinem Bekanntenkreis mit einem Eintrag in seinem Adressbuch über ähnliche Anrufe oder andere seltsame Vorfälle beschwert. Bislang …

Ermittlungserfolge

Es gibt aber gute Chancen, dass seine Befürchtungen unbegründet sind. Jedenfalls hat die Polizei keine Erkenntnisse darüber, dass die Täter bei einem solchen Support-Betrug nebenbei weitere Daten abfischen und im Anschluss für weitere Straftaten nutzen. Das erklärte Alexander Sirowi im Gespräch mit c’t: Er ist beim LKA Niedersachsen seit letztem Jahr damit beschäftigt, die hinter den gefälschten Support-Anrufen steckenden Täter dingfest zu machen. Er war auch an dem spektakulären Schlag beteiligt, der dem LKA gemeinsam mit der Staatsanwaltschaft Osnabrück und in Zusammenarbeit mit indischen Behörden im März dieses Jahres gegen eine Operationsbasis der Betrüger in Kalkutta gelang.

Dabei wurden 250 Callcenter-Arbeitsplätze stillgelegt und sieben Personen verhaftet. Die der Polizei angezeigten Fälle seien seitdem deutlich gesunken, erzählt Sirowi. Allerdings habe man es mit einem Bereich zu tun, in dem es ein großes Dunkelfeld nicht angezeigter Taten gebe.

Unser Leser Rainer L. hat mit einem Schaden von gut 300 Euro fast noch Glück gehabt: Die meisten Opfer bezahlen das Lösegeld mit einer Kreditkarte online, während die Betrüger den Rechner unter Kontrolle haben. Kurz vor dem Abschluss der Transaktion ändern sie den angewiesenen Betrag unbemerkt; dabei kommen nicht selten deutlich höhere Summen zustande. Außerdem versuchen sie häufig, mit den erbeuteten Kreditkartendaten weitere Geschäfte zu tätigen.

Sirowi rät deshalb zu einer möglichst raschen Reaktion, sollte man Opfer eines

solchen Betrugs geworden sein: „Wenn man erst nach zwei Tagen reagiert, dann ist das Geld tatsächlich weg. Wenn man allerdings schnell reagiert und sich mit seiner Bank in Verbindung setzt, weil man irgendeinen Verdacht hat oder weil einem das Ganze irgendwie nicht koscher ist, dann hat man gute Chancen, das Geld wieder zurückzuholen.“ Die benutzte Kreditkarte gehört natürlich umgehend gesperrt, um weiteren Missbrauch zu verhindern.

Bei einer Barzahlung über Western Union oder ähnliche Dienstleister ist das Geld aber praktisch immer futsch, weil es sich der Empfänger meist sehr schnell und bar auszahlen lässt. Auch für die Polizei sind weitere Nachforschungen dann in der Regel fast nicht mehr möglich: Die Betrüger arbeiten mit Strohmännern und Pseudonymen, die sich in vielen Fällen kaum ermitteln lassen.

Trotzdem sollte man in jedem Fall Anzeige erstatten, wenn man Opfer eines solchen Betrugs geworden ist, rät Sirowi. Im Prinzip gilt das auch für erfolglose Anruf-Versuche, die man gleich als Betrug erkannt und schnell beendet hat – auch eine versuchte Straftat ist eine Straftat. Allerdings kann die Polizei in einem solchen Fall nicht wirklich ermitteln: Die im Telefon angezeigte Anruferkennung ist praktisch immer gefälscht.

Anders sieht es aus, wenn man sich darauf eingelassen hat, die geforderte Fernwartungssoftware zu installieren und dem Anrufer Zugang zum PC zu verschaffen: Aus den Log-Dateien auf dem eigenen Rechner oder beim Betreiber der Fernzugangslösung lassen sich für die Polizei sehr wohl Erkenntnisse gewinnen, die dabei helfen können, die Angreifer zu fassen. Bei erfolgter Zahlung ergeben sich aus dem Empfänger oder dem Ort, wo das Geld ausgezahlt wurde, weitere Indizien.

Von der Idee, einen betrügerischen Anrufer in ein langes Gespräch zu verwickeln, um ihm möglichst viel Zeit zu stehlen, hält Sirowi nichts: Die Betrüger seien sehr gut geschult. Je länger man sich auf ein Gespräch einlasse, desto höher sei die Gefahr, dass man doch noch auf deren Überredungskünste hereinfalle.

Microsofts Sicht

Auch Microsoft rät Anwendern, bei unerwarteten Anrufen von angeblichen Microsoft-Mitarbeitern sofort aufzulegen. „Microsoft tätigt keine proaktiven Anrufe an private Nutzer, um technischen Support anzubieten. Ein derartiges Anliegen muss immer vom Kunden selbst initiiert sein“, gibt Michael Kranawetter zu Protokoll, seines Zeichens Chief Security Officer bei Microsoft Deutschland. Diese Art von Betrug werde sich leider nie ganz vermeiden lassen. Microsoft empfehle seinen Kunden, nie einer unbekannten dritten Person Kontrolle über den eigenen Computer zu geben. Microsoft betreibt eine eigene „Digital Crimes Unit“, die diese Art von Betrugsfällen untersucht und eng mit den lokalen Behörden zusammenarbeitet, um gegen Betrüger vorzugehen.

»Microsoft tätigt keine proaktiven Anrufe an private Nutzer, um technischen Support anzubieten.«

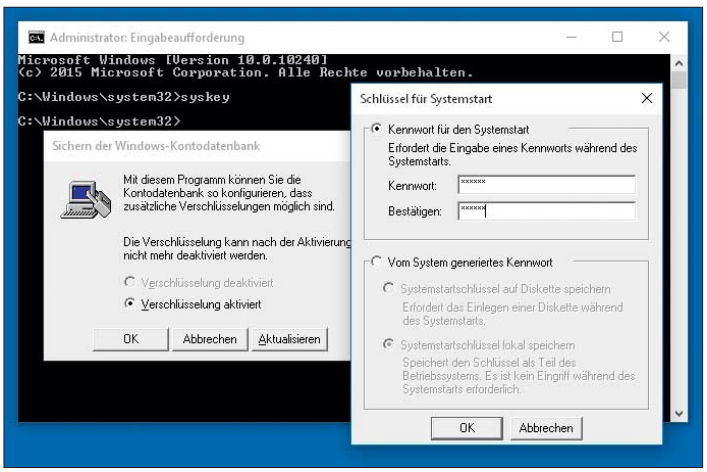
Michael Kranawetter, CSO, Microsoft Deutschland

Für die jüngst erschienene „Global Tech Support Scam Survey 2016“ hat Microsoft von Sommer 2015 bis Sommer 2016 Anwender in zwölf Ländern und Regionen weltweit befragen lassen, welche Erfahrungen sie mit Support-Schwindel gesammelt haben. Dabei ging es nicht nur um betrügerische Anrufe, sondern auch um Pop-up-Fenster und Weiterleitungen zu Webseiten sowie um Online-Werbung und unaufgeforderte Mails.

Mehr als zwei von drei Befragten hatten im Untersuchungszeitraum Kontakt mit der einen oder anderen Form von Panik heischenden Alarmen, in Deutschland etwa jeder zweite. Von denjenigen, die angaben, von Support-Scam belästigt worden zu sein, berichtete etwa die Hälfte von Pop-up-Fenstern und Alarmmeldungen auf Webseiten, 30 Prozent haben einen unaufgeforderten Anruf erhalten.

Die Betrüger sind der Befragung zufolge mit ihrer Masche sehr erfolgreich: Bei etwa jedem fünften Teilnehmer führte ein Angriff dazu, dass er sich darauf einließ, etwa Software herunterzuladen, eine bestimmte Webseite zu besuchen oder den Betrügern Zugriff auf seinen Rechner zu gewähren. In Deutschland ließen sich etwa 7 Prozent der Angegriffenen zu weiteren Aktionen bewegen. Etwa jeder zweite Gutgläubige hat in der Folge auch einen finanziellen Schaden erlitten. In Marketing-Kreisen würde eine Konversionsrate von 3 Prozent als Traumwert angesehen werden.

Bei der Aufklärung hat Microsoft also noch einen weiten Weg vor sich: Fast 20 Prozent der Befragten mit Scamming-Erfahrung halten unaufgeforderte Support-Anrufe für authentisch. Um es noch einmal deutlich zu sagen: Das sind sie nie! Schon gar nicht, wenn der Anrufer englisch spricht. Nach der Lektüre dieses Artikels werden Sie hoffentlich nicht mehr auf die Masche hereinfallen. Tragen Sie dieses Wissen bitte auch in Ihrem Verwandten- und Bekanntenkreis weiter! Spätestens bei der Frage eines Angehörigen, ob etwa der TeamViewer eine vertrauenswürdige Software sei, sollten Sie hellhörig werden … *(hos@ct.de)* c't



Wenn die Benutzerdatenbank von Windows mit dem Programm syskey verschlüsselt wurde, ist ohne das passende Kennwort keine Anmeldung mehr möglich.