Ihre POLIZEI
Votre POLICE
La vostra POLIZIA

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

SKPPSC

Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

FACT SHEET *Betrügerische Supportanrufe (MICROSOFT-Betrug)*

Wie der Betrug abläuft

Am Telefon geben sich die Kriminellen oft als Mitarbeiter von Microsoft oder eines IT-Support-Centers aus. Als Vorwand für ihren Anruf bringen sie beispielsweise vor, der Computer der betreffenden Person sei von einem Virus befallen, das System laufe zu langsam oder es gebe irgendein anderes technisches Problem. Dabei besteht ihre wahre Absicht darin, ihr Gegenüber davon zu überzeugen, ihnen einen Remote-Zugriff auf ihren Computer zu gewähren. Oder sie wollen sie dazu bringen, ein Programm herunterzuladen oder eine gefälschte Webseite aufzurufen, die genau gleich aussieht wie eine offizielle Webseite, aber nur dazu dient, die Benutzerdaten des Opfers zu stehlen.

Mit diesen Methoden gelingt es den Betrügern, direkt auf die Geräte ihrer Opfer zuzugreifen, ihre Passwörter abzufangen oder die auf dem Computer gespeicherten Daten herunterzuladen, womit sie in das digitale Leben der betroffenen Person eingreifen können. Die angeblichen Support-Dienste sind zudem oft kostenpflichtig. Deshalb verlangen die Kriminellen von ihren Opfern manchmal auch die Angabe einer Kreditkartennummer, die sie dann ebenfalls für ihre Zwecke missbrauchen.

Der Videoclip des zweiten Teils der nationalen Präventionskampagne 2020, der am 8. September lanciert wird, erzählt die missliche Geschichte von Simon, der auf den betrügerischen Anruf von Martin eingegangen ist und ihm die Kontrolle über seinen Computer überlassen hat.

Die Anruferinnen und Anrufer sprechen zwar oft nicht gut Englisch. Aber weil die Rufnummern manipuliert werden können, wird auf dem Telefon des Opfers dann tatsächlich die Nummer der Firma angezeigt, von der aus der Anruf angeblich getätigt wird.

Es kommt auch immer häufiger vor, dass sich die falschen Support-Mitarbeiter von ihren Opfern selbst anrufen lassen. Das funktioniert so: Beim Surfen im Internet erscheint ein Pop-up-Fenster auf dem Bildschirm, das den Nutzer auf ein fiktives technisches Problem aufmerksam macht. In diesem Fenster ist zudem eine Schweizer Telefonnummer angegeben, die man zur Lösung des Problems anrufen soll. Wenn man das tut, schlagen die Betrüger zu und lassen ihre Opfer für vermeintliche Antivirenprogramme zahlen.

Warum lassen sich so viele Menschen hereinlegen?

Tatsächlich verlieren viele Menschen den Kopf, wenn man ihnen sagt, dass die Daten auf ihrem Computer bedroht sind. Da die Betrüger sehr professionell argumentieren und auch sofort eine Lösung für das Problem anbieten (nämlich ihren Online-Support), erstaunt es nicht, dass viele diese

Hilfe dankbar annehmen. Zudem ist es für die Betrüger ein Leichtes, sich eine bestehende Telefonnummer anzueignen und für ihre Zwecke zu missbrauchen, beispielsweise diejenige einer Helpline. Damit wollen sie das Misstrauen ihrer potenziellen Opfer zerstreuen: Diese sehen dann eine Schweizer Telefonnummer und denken, dass die Anruferin oder der Anrufer tatsächlich für ein hiesiges IT-Unternehmen arbeitet und es gut mit ihnen meint.

Einige Zahlen

Die «klassische» Kriminalität im Bereich der Vermögensdelikte wie etwa Einbruchdiebstähle ist in der Schweiz zwar deutlich zurückgegangen (- 50,6 % vom Rekordjahr 2012 bis 2019). Es ist aber zu erwarten, dass die neuen Technologien die Ausbreitung und Entwicklung von neuen Vorgehensweisen ermöglichen, die typisch sind für die «digitale» Kriminalität. Aktuell gibt es keine offizielle nationale Statistik für Tech-Support-Betrug (Microsoft-Scam). Von den 286'207 Vermögensdelikten, die 2019 in der Schweiz begangen wurden, handelte es sich bei 17'606 oder rund 6,2 % um Betrugsfälle. Sie haben damit im Vergleich zum Vorjahr um 7,9 % zugenommen und ein Teil dieses Anstiegs dürfte auf die Entwicklungen im Bereich der digitalen Modi Operandi zurückzuführen sein.

Empfehlungen

Denken Sie immer daran:

Egal, ob es sich um Microsoft oder ein anderes IT-Unternehmen (oder einen Support-Dienst) handelt: Es ist extrem selten, dass solche Firmen jemanden unaufgefordert anrufen, um ihre Dienste anzubieten. Bei technischen Problemen sollten die Betroffenen immer selbst Kontakt mit einer Firma aufnehmen, die ihnen bekannt ist oder ihren Standort in der Nähe hat.

Damit Sie kein Opfer werden:

- Legen Sie bei unaufgeforderten Anrufen von angeblichen Mitarbeiterinnen oder Mitarbeitern von Microsoft oder anderen IT-Support-Centern sofort auf.
- Verlassen Sie sich nicht auf die Nummer, die bei einem Anruf auf Ihrem Telefon angezeigt wird.
- Geben Sie nie persönliche Angaben (Passwörter oder Kreditkartennummer) an andere Personen weiter.
- Gewähren Sie niemandem einen Remote-Zugriff auf Ihren Computer.
- Laden Sie nie kostenlose Software von Webseiten herunter, die nicht vertrauenswürdig sind.
- Rufen Sie falls nötig immer die offiziellen Telefonnummern von Microsoft oder der Support-Dienste an, die auf der offiziellen Webseite dieses Konzerns aufgeführt sind.
- Nutzen Sie zur Kontaktaufnahme mit Ihrer Bank ausschliesslich die offiziellen Telefonnummern, die Sie beispielsweise auf Ihren Bankauszügen finden.

Wenn es zu spät ist und Sie jemandem bereits Zugang zu Ihrem Computer gewährt haben:

- Trennen Sie sofort die Internetverbindung und schalten Sie Ihren Computer aus.
- Schalten Sie Ihren Computer erst wieder ein, wenn das Netzwerk (z. B. WiFi) ausgeschaltet ist, und überprüfen Sie Ihre Festplatte sofort mit einem Antivirenprogramm.
- Ändern Sie all Ihre Passwörter.

- Zögern Sie nicht, professionelle Hilfe in Anspruch zu nehmen, wenn Sie unsicher sind.
- Wenn Sie vertrauliche Daten weitergegeben haben (z. B. Bankangaben oder Informationen zu Ihrer Kreditkarte), dann nehmen Sie unverzüglich Kontakt mit Ihrem Kreditkartenanbieter und/oder Ihrer Bank auf, um alle laufenden Transaktionen zu stoppen und Ihr Konto zu sperren.
- Melden Sie sich dann bei Ihrer örtlichen Polizeidienststelle.

Zitat eines Opfers

«Ich wusste nicht besonders viel über Informatik und er schien sich so gut auszukennen. Na ja, und dann habe ich ihm vertraut und gesagt, ich sei einverstanden. Er meinte dann, er müsse kurz auf meinen Computer zugreifen, um das Problem zu lösen. Weil ich wusste, dass das gefährlich sein kann, habe ich einen Moment gezögert. Aber schliesslich habe ich ihn machen lassen.»