Betrügerische Supportanrufe

Kriminelle nutzen nicht nur das Internet, um an vertrauliche Informationen zu gelangen. Immer öfter wird dafür auch das Telefon eingesetzt. «Vishing» nennt sich diese Kriminalitätsform.

Schützen Sie sich, indem Sie...

- unaufgeforderte Anrufe angeblicher Mitarbeitenden von Microsoft, IT-Support-Firmen oder Finanzinstituten sofort beenden.
- sich nicht auf die Richtigkeit der auf Ihrem Telefondisplay angezeigten Nummer verlassen.
- persönliche Daten wie Passwörter oder Kreditkartenangaben nie einer anderen Person bekannt geben.
- bei Support-Fragen immer die offiziellen Telefonnummern von Microsoft oder IT-Support-Firmen wählen.
- Ihr Finanzinstitut nur über die offiziellen Telefonnummern kontaktieren, die Sie z.B. auf Ihren Kontoauszügen finden.

Kriminelle nutzen nicht nur das Internet, um an vertrauliche Informationen zu gelangen. Immer öfter wird dafür auch das Telefon eingesetzt. «Vishing» nennt sich diese Kriminalitätsform.Der Begriff «Vishing» steht für «Voice-Phishing». Ähnlich wie beim klassischen Phishing werden Personen durch vorgetäuschte Tatsachen dazu gebracht, vertrauliche Informationen preiszugeben oder vermeintliche Sicherheitsprogramme zu installieren – in Tat und Wahrheit handelt es sich dabei aber um Schadsoftware.

Oft geben sich die Anrufenden dabei als Mitarbeitende von Microsoft, einer IT-Support-Firma oder eines Finanzinstituts aus. Die Anrufer behaupten beispielsweise, eine Virusinfektion sei erkannt worden oder ein anderes technisches Problem läge vor. Die Absicht der Betrügerinnen und Betrüger ist es, das Gegenüber zu überzeugen, entweder Programme aus dem Internet herunterzuladen oder eine gefälschte, jedoch täuschend echt aussehende Webseite zu besuchen.

Über beide Wege können sich die Betrügerinnen und Betrüger so einen direkten Zugriff auf das jeweilige Gerät verschaffen und beispielsweise unbemerkt Passwörter ausspionieren oder alle auf dem Computer gespeicherten Daten einsehen, kopieren und bearbeiten. Teilweise verlangen die Betrügerinnen und Betrüger für den vermeintlichen «Support-Dienst» sogar Gebühren, wozu die Kreditkartennummer angegeben werden muss, die natürlich missbräuchlich verwendet wird.

Die Anrufenden sprechen oft gebrochenes Englisch. Da Rufnummern technisch manipuliert werden können, erscheint auf dem Telefondisplay der Opfer unter Umständen die echte Telefonnummer des Unternehmens.

Immer häufiger lassen sich die angeblichen Mitarbeitenden mittlerweile auch anrufen. Dazu werden den Opfern beim Surfen im Internet Werbefenster (Pop-ups) angezeigt, in welchen auf angebliche Probleme hingewiesen wird. Im gleichen Fenster wird auch eine Schweizer Telefonnummer angegeben, welche für die Lösung des Problems angerufen werden sollte.

Ist es bereits zu spät und Sie haben bereits den Zugang zu Ihrem Gerät ermöglicht, dann trennen Sie Ihr Gerät sofort vom Internet oder schalten Sie es aus. Schalten Sie Ihr Gerät nur mit deaktiviertem Netzwerk (z.B. ausgeschaltetem WLAN) wieder ein und prüfen Sie danach umgehend die gesamte Festplatte mit einem Virenschutzpro-

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik

gramm. Ändern Sie ausserdem alle Ihre Passwörter. Ziehen Sie bei Bedarf oder Unsicherheit eine Fachperson bei.

Haben Sie bereits sensible Daten herausgegeben (z.B. Kreditkarteninformationen oder Bankdaten), melden Sie dies bitte umgehend Ihrer Kreditkartenfirma und/oder Ihrem Finanzinstitut sowie der örtlichen Polizei.

*Microsoft, andere IT-Support-Firmen oder Finanzinstitute tätigen **keine** unaufgeforderten Anrufe an private Nutzer, um technischen Support anzubieten! Die Initiative bei einem solchen Anliegen muss immer von den Kundinnen und Kunden selbst ausgehen.*

Merkblatt:

(https://www.ebas.ch/wp-content/uploads/2019/09/supportSKP_de.pdf)

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik