Präventionshinweise des Polizeipräsidiums Freiburg aufgrund aktueller Betrugsstraftaten (Teil 7):

Falsche Microsoft-Mitarbeiter am Telefon

Ihr Telefon klingelt. Ein Unbekannter meldet sich und stellt sich als Mitarbeiter von Microsoft vor. Er behauptet, Ihr Rechner, z.B. Computer oder Laptop, sei von Viren befallen. In diesem Fall legen Sie am besten gleich wieder den Hörer auf. Denn am anderen Ende der Leitung sind höchstwahrscheinlich Betrüger, die nichts mit Microsoft zu tun haben, sondern in einem Call-Center in Indien sitzen.
Die angeblichen - häufig nur Englisch oder gebrochen Deutsch sprechenden - Microsoft-Mitarbeiter behaupten, dass der Rechner des Angerufenen Fehler aufweise, von Viren befallen oder ein neues Sicherheitszertifikat benötige und bieten ihre Hilfe an. Dazu sollen ihre Opfer auf ihren Geräten eine Fernwartungssoftware installieren.
Mit diesem Programm haben die Betrüger Zugriff auf die Rechner ihrer Opfer und können sensible Daten, beispielsweise Passwörter für das Online-Banking ausspähen. Darüber hinaus verlangen sie für ihre vermeintliche Service-Leistung eine Gebühr. Manchmal fordern Sie für das Erneuern einer angeblich abgelaufenen Lizenz ebenfalls Geld oder sie überreden ihre Opfer dazu, einen kostenpflichtigen Wartungsvertrag einzugehen.

So schützen Sie sich

- Seriöse Unternehmen wie Microsoft nehmen **nicht unaufgefordert Kontakt** zu ihren Kunden auf. Sollte sich ein Servicemitarbeiter bei Ihnen melden, ohne dass Sie darum gebeten haben: **Legen Sie einfach den Hörer auf.**
- Geben Sie auf **keinen Fall private Daten** z.B. Bankkonto- oder Kreditkartendaten, oder Zugangsdaten zu Kundenkonten (z.B. PayPal) heraus.
- Gewähren Sie einem unbekannten Anrufer **niemals Zugriff auf Ihren Rechner** beispielsweise mit der Installation einer Fernwartungssoftware.

Wenn Sie Opfer wurden

- Trennen Sie Ihren Rechner vom Internet und fahren Sie ihn runter. Ändern Sie **über einen nicht infizierten Rechner** unverzüglich betroffene Passwörter.
- Lassen Sie Ihren Rechner überprüfen und das **Fernwartungsprogramm auf Ihrem Rechner löschen.**
- Nehmen Sie Kontakt zu den Zahlungsdiensten und Unternehmen auf, deren Zugangsdaten in den Besitz der Täter gelangt sind.
- Lassen Sie sich von Ihrem Geldinstitut beraten, ob Sie bereits getätigte Zahlungen zurückholen können.
- Erstatten Sie Anzeige bei der Polizei.
- Sie können den Betrugsversuch zusätzlich bei Microsoft melden: www.microsoft.com/de-DE/concern/scam

Haben Sie weitere Fragen oder möchten Sie sich beraten lassen, so melden Sie sich gerne über **freiburg.pp.praevention@polizei.bwl.de**.

Wir möchten, dass Sie sicher leben!
Ihr Polizeipräsidium Freiburg

POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM FREIBURG