Betrügerischen Benachrichtigungen, die scheinbar vom technischen Support (Microsoft-Support) kommen

In letzter Zeit treten wieder vermehrt Betrügereien bzw. versuchte Betrügereien durch sog. Support-Scam auf. Dabei versuchen Betrüger, Sie durch die Schilderung vermeintlicher Probleme zu überzeugen, für unnötige technische Supportdienste zu bezahlen, die Geräte-, Plattform- oder Softwareprobleme beheben sollen.

Vorgehensweise der Betrüger bei Support-Scam

Die Betrüger rufen Sie direkt an und geben vor, Mitarbeiter einer Softwarefirma zu sein. Sie können sogar die angezeigte Rufnummer so fälschen, dass die gültige Supportnummer eines vertrauenswürdigen Unternehmens angezeigt wird. Dann werden Sie in der Regel aufgefordert, Anwendungen zu installieren, die einen Remotezugriff auf Ihr Gerät ermöglichen. Per Remotezugriff sind die erfahrenen Betrüger in der Lage, die normale Systemausgabe so zu manipulieren, dass sie problematisch erscheint.
Wenn Sie sich auf die Betrüger einlassen, werden Ihnen möglicherweise Lösungen für Ihre „Probleme" angeboten, und Sie werden zur Zahlung einer einmaligen Gebühr oder zum Abschluss eines Abonnements für einen vermeintlichen Supportservice aufgefordert.

Betrugsversuche über das Telefon

Bei dieser Art von Betrug rufen die Betrüger Sie an und behaupten, dass sie zum technischen Supportteam von Microsoft oder anderen Anbietern gehören. Sie bieten dann an, Ihre Computerprobleme zu beheben.
Betrüger nutzen oft öffentliche Telefonverzeichnisse, um den zur Nummer gehörenden Namen und andere personenbezogene Informationen zu erfahren. Sie können sogar erraten, welches Betriebssystem Sie verwenden.
Sobald sie Ihr Vertrauen gewonnen haben, fragen sie möglicherweise nach Ihrem Benutzernamen und Passwort oder fordern Sie auf, eine Website aufzurufen und von dort Software herunterzuladen, mit der sie dann auf Ihren Computer zugreifen können, um ihn zu „reparieren". Wenn Sie die Software installieren und Anmeldeinformationen angeben, sind Ihr Computer und Ihre persönlichen Daten angreifbar.
Da Strafverfolgungsbehörden Telefonnummern ausfindig machen können, verwenden die Täter oft Münztelefone, Einwegmobiltelefone oder gestohlene Mobiltelefonnummern. Seien Sie also bei unerwarteten Anrufen skeptisch. Geben Sie keine persönlichen Informationen an.
Wenn Sie einen unerwarteten Anruf von jemandem erhalten, der behauptet, zum Microsoft-Support zu gehören, legen Sie auf. Microsoft tätigt diese Art von Anrufen nicht.

Es ist auch wichtig, Folgendes zu bedenken:

- Microsoft sendet keine unerwünschten E-Mails und führt keine unerwünschten Anrufe durch, um persönliche oder finanzielle Informationen anzufordern oder um Support für Fehler auf Ihrem Computer anzubieten.
- Jede Kommunikation mit Microsoft muss von Ihnen initiiert werden.
- Wenn eine Benachrichtigung mit einer Telefonnummer angezeigt wird, sollten Sie diese Nummer nicht anrufen. Fehler- und Warnmeldungen von Microsoft enthalten niemals Telefonnummern.
- Laden Sie Software nur von den Websites offizieller Microsoft-Partner oder aus dem Microsoft Store herunter. Seien Sie vorsichtig beim Herunterladen von Software über Drittanbieter-Websites, da einige von ihnen möglicherweise ohne das Wissen des Anbieters geändert wurden und nun falsche Supportsoftware und andere Malware bereitstellen.

- Verwenden Sie Microsoft Edge zum Surfen im Internet. Dieser Browser blockiert bekannte Sites, die betrügerische Supportsoftware anbieten, mithilfe von Windows Defender SmartScreen (das auch von Internet Explorer verwendet wird). Zudem hinaus kann Microsoft Edge Popupdialogschleifen stoppen, die von diesen Sites verwendet werden.
- Aktivieren Sie den Echtzeitvirenschutz „Windows-Sicherheit" in Windows 10. Er erkennt und entfernt bekannte Support-Scam-Malware.

BEZIRKSPOLIZEIKOMMANDO KREMS

Herbert GOLDNAGL, AbtInsp

Sicherheitskoordinator