SPECTRUM news
Unabhängiger KANZLEI Systempartner

Gibt es wirklich Microsoft-Mitarbeiter denen das Wohl Ihres PCs am Herzen liegt?

Wieder greift eine dreiste Phishing-Masche um sich . . .

SPECTRUM warnt:

Seien Sie skeptisch, wenn ein vermeintlicher Microsoft-Mitarbeiter Sie anruft. Hierbei handelt es sich nämlich wahrscheinlich um eine geschickt aufgezogene Phishing-Masche *).

Wie funktioniert die Masche?

Hier handelt es sich um einen alten Trick, der immer wieder einmal mit neuen Maschen angewandt wird und leider fallen verblüffender weise trotz der Plumpheit des Tricks immer wieder viele Anwender darauf herein. Man bekommt z.B. einen Anruf – ja richtig per Telefon, häufig auf Englisch – bei dem einem dann erklärt wird, dass z.B. Microsoft festgestellt hätte, dass der PC von einer Schadsoftware befallen sei und man nun schleunigst gemeinsam diese Schadsoftware beseitigen müsste, um weiteren Schaden zu vermeiden und der Anrufer würde einem nun dabei helfen. Man wird dann gebeten zum PC zu gehen und den telefonischen Anweisungen zu folgen.

Täglich passiert das über 1.000 Mal täglich in Deutschand!

> *SPECTRUM-Mitarbeiter und SPECTRUM-Kunden berichten in den letzten Wochen, dass man sogar mehrfach täglich solche Anrufe erhalten hat.*

Der Anrufer fordert einen mit diesem angeblichen Support-Anrufes mit einer gewissen Bestimmtheit dann auf, ein „harmloses“ Fernwartungsprogramm herunterzuladen, damit der Anrufer einem auch richtig bei der Beseitigung der Schadsoftware helfen kann.

Hiermit haben die Betrüger dann aber vollen Zugang auf den PC des Opfers! Nach dem Zugriff auf den PC, wird einem dann vorgegaukelt, wie das vom Betrüger vorgeschwindelte Problem behoben wird. Dieses augenscheinlich positive Verhalten ist jedoch tückisch: In dieser Phase hat der Betrüger vollen Zugriff auf das System, kann die Maus bewegen, den Bildschirm sehen und Befehle eintippen und er kann vor allem im Hintergrund einen Trojaner installieren und Daten absaugen.

Und was passiert dann?

Nachdem der PC „gewartet“ wurde, soll man für die Befreiung des PCs von dem fiktiven Schadcode auch erst einmal bezahlen. Meistens ist es aber zu diesem Zeitpunkt bereits zu spät für Misstrauen, denn dann sind schon Daten unbemerkt gestohlen worden: Adresslisten aus Outlook, das Onlinebanking wurde ausspioniert oder alle Zugangsdaten und Passwörter wurden ausgelesen usw.. Weigert man sich gegen die Bezahlung für diesen „Service“, meist Konten von dubiosen Banken in Zypern, im nahen und fernen Osten oder auf Karibikinseln, kann es durchaus passieren, dass der eigene Computer gesperrt wird, man nicht mehr an seine Programme und Daten kommt und der PC nicht mehr funktioniert.

Fallen Sie nicht auf diese Masche rein. Microsoft & Co kümmern sich nicht weltweit um das Wohl einzelner PCs. Legen Sie einfach auf! Microsoft selbst warnt auf seiner Internet-Seite vor solchen Anrufen und rät das Gespräch sofort zu beenden. Lassen Sie vor allem die Installation einer Fernwartungssoftware nicht zu.

Ihr freier, unabhängiger KANZLEI-Systempartner, der mehr für Sie macht

Ihr SPECTRUM COMPUTER-SYSTEMHAUS-Team

*) Phishing-Masche = Phishing ist Kunstwort abgeleitet von „Fishing“ = „Angeln“ und man versteht hierunter Versuche an persönliche Daten eines Internet-Benutzers zu gelangen, um z.B. mit diesen Daten Bankkonten zu plündern, mit falscher Identifikation in Internet-Shops Ware zu bestellen oder Anwender zu erpressen.