Spionage-Software statt Sicherheits-Update
Polizei warnt vor Anrufen von falschen Microsoft-Mitarbeitern

Donnerstag 16. Oktober 2014 - **Hameln/Holzminden (wbn). Cyberkriminalität im Weserbergland. In einer Mischung aus einer Art Telefonbetrug, Computersabotage und Datenklau versuchen findige Täter derzeit, an das Geld und die persönlichen Daten von Computernutzern in der Region zu gelangen. Insbesondere im Bereich der Polizeiinspektion Hameln-Pyrmont/Holzminden haben sich die Fälle in den vergangenen Tagen gehäuft.**

Alles beginnt mit einem Anruf aus dem asiatischen Raum – vermutlich aus Indien. Ein etwas anderer „Computer-Inder“ gibt sich sodann zumeist in englischer Sprache als Mitarbeiter des Microsoft-Supports aus und erklärt, dass vom PC der Angerufenen ein Sicherheitsrisiko ausgehe und nun dringend ein Sicherheitsupdate durchgeführt werden müsse. Es folgt die mündliche Anleitung zum Aufspielen des entsprechenden Update-Programms – das sich hinterher als Fernwartungssoftware herausstellt und den Kriminellen Tür und Tor zum Rechner öffnet.

Fortsetzung von Seite 1

Die Folge: Der vermeintliche Computer-Techniker hat vollen Zugang zum PC und wird versuchen, die Zugangsdaten zum Online-Banking oder verschiedene Passwörter auszuspionieren.

Deshalb warnt die Polizei jetzt vor zweifelhaften Anrufen, rät, sich die eventuell im Display aufleuchtende Nummer zu notieren, das Gespräch danach sofort zu beenden und die nächste

Polizeidienststelle zu informieren.

Nachfolgend der Polizeibericht aus Hameln:

„Derzeit häufen sich Fälle im Zuständigkeitsbereich der Polizeiinspektion, bei denen falsche Microsoft-Mitarbeiter versuchen, Computerbesitzer zu betrügen.

Nach immer derselben Masche rufen angebliche Mitarbeiter des Microsoft-Supports wahllos Haushalte an und suggerieren dabei den Angerufenen, dass von deren PC ein Sicherheitsrisiko ausgeht und auf ihrem Computer dringend ein Update der Sicherheitssoftware installiert werden müsse.

Meistens in englischer Sprache werden Anweisungen zur Installation einer sogenannten Fernwartungssoftware erteilt, über die der falsche Support-Mitarbeiter Zugang zum PC erhalten und als angeblich hilfsbereiter Techniker das Update vornehmen könnte.

In wenigen Fällen wird vorab für die Serviceleistung zu einer Zahlung aufgefordert und daher die Bekanntgabe von Kreditkartendaten verlangt.

Nach der Installation der Fernwartungssoftware hat der fremde Techniker vollen Zugang zum PC und wird versuchen, die Zugangsdaten zum Online-Banking oder die Passwörter von eMail-Konten oder von Internet-Accounts auszuspionieren.

Hinter dieser Vorgehensweise stecken Täter aus dem asiatischen Raum, vermutlich Indien, und agieren über Callcenter nicht nur in Deutschland sondern weltweit.

Deshalb warnen wir eindringlich vor solchen falschen Microsoft-Mitarbeitern und geben folgende Hinweise:

- erhalten Sie einen solchen Anruf notieren Sie sich nach Möglichkeit, sofern eine angezeigt wird, die im Display erscheinende Telefonnummer,

- nicht auf die Forderungen des Anrufers eingehen und sofort das Gespräch beenden,

- keine Installation von Software durchführen, zu der man am Telefon aufgefordert wird,

- keine Konto- oder Kreditkartendaten herausgeben,

- melden Sie den Vorfall bei Ihrer nächsten Polizeidienststelle.“