Sicherer Umgang mit Remote Support

Remote Support ist eine Technologie, um fremde Hilfe auf das eigene Gerät zu holen, ohne dass ein Techniker vor Ort sein muss. Auch Finanzinstitute und Softwarehersteller nutzen im Rahmen des Supports/Helpdesks diese Möglichkeit. Der sichere Umgang mit Remote Support erfordert aber einige Massnahmen.

Wichtigste Merkpunkte:

- Stellen Sie Verbindungen nur mit vertrauenswürdigen Personen her. Seien Sie insbesondere zurückhaltend, falls Sie nicht der Initiant der Verbindung sind (z. B. wenn Sie unerwartet telefonisch kontaktiert werden).
- Verwenden Sie eine verschlüsselte Verbindung.
- Verwenden Sie ein Sitzungs-Passwort oder eine Meeting-ID.
- Gewähren Sie keinen Vollzugriff auf Ihr System. Die Person, die Ihnen hilft, sollte nur passiv zusehen können.
- Beachten Sie, dass alles, was auf dem Bildschirm erscheint, vom Gegenüber gesehen auch aufgezeichnet werden kann.
- Geben Sie während der Sitzung so wenige Passwörter wie möglich ein.
- Surfen Sie nicht auf Internetseiten, die nichts mit der Sitzung zu tun haben – auch wenn Sie dazu angewiesen werden.
- Stellen Sie sicher, dass nach Inanspruchnahme der Hilfeleistung die Remote Support Verbindung beendet wird, um weitere Zugriffe auf Ihr Gerät zu unterbinden.

Viele Firmen nutzen Remote Support Software, damit das Support-Personal einen schnellen Blick auf das Gerät eines Benutzers erlangen kann, ohne dass gleich jemand vor Ort erscheinen muss.

Leider missbrauchen auch Kriminelle diese Technologie, um unter dem Vorwand, Support-Mitarbeiter einer Firma zu sein, sich Zugriff das Gerät von Internetanwendern zu erschleichen und beispielsweise Passwörter abzugreifen, eine Malware zu installieren oder eine Überweisung via E-Banking auszulösen. Achten Sie also darauf, wem Sie vertrauen!

Beachten Sie auch unser Merkblatt «So schützen Sie sich vor betrügerischen Supportanrufen.»

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

Remote Support Software ermöglicht den Fernzugriff auf ein entferntes System über ein lokales Netzwerk (LAN) oder das Internet. Dabei wird die Oberfläche des entfernten Gerätes am lokalen System angezeigt und erlaubt z. T. zugleich auch dessen Fernsteuerung.

Weiterführende Informationen für Interessierte

Einladung

Stellen Sie Verbindungen nur mit vertrauenswürdigen Personen her. Seien Sie insbesondere zurückhaltend, falls Sie nicht der Initiant der Verbindung sind (z. B. wenn Sie unerwartet telefonisch kontaktiert werden). Es ist mittlerweile eine gängige Masche von Angreifern, sich telefonisch z. B. als Mitarbeiter von Microsoft, Apple, einer IT-Support-Firma oder eines Finanzinstitutes auszugeben, um Zugriff auf Ihr Gerät zu erlangen. Die Sitzung sollte erst nach einer expliziten Einladung durch Sie aufgebaut werden können. Bevor Sie eine Verbindung durch die Software zulassen, sollten Sie dieser ausdrücklich zustimmen können.

Verschlüsselung

Bei der Wahl des Produktes sollte auf eine ausreichende Verschlüsselung geachtet werden, damit die Daten nicht im Klartext übertragen werden. Die Schlüssellänge sollte mindestens 128 Bit betragen.

Authentifizierung

Die Person, die eine Verbindung zu Ihrem Gerät aufbaut, muss sich über eine Meeting-ID und/oder ein Passwort authentisieren. Je nach verwendeter Software wird dies unterschiedlich umgesetzt. Um sicher zu stellen, dass diese sensiblen Informationen nur die richtige Person erhält, wird das Passwort oder die Meeting-ID am besten vorgängig per Telefon mitgeteilt.

Zugriffsrechte

Gewähren Sie keinen Vollzugriff auf Ihr System. Die Person, die Ihnen hilft, sollte grundsätzlich nur passiv zusehen können und Anweisungen geben. Damit ist sichergestellt, dass immer noch Sie die alleinige Kontrolle über Ihr System haben und keine unbeabsichtigten Änderungen erfolgen.

Aufnahme

Bitte beachten Sie, dass die Support-Sitzung aufgezeichnet werden kann. Alles was in dieser Zeit auf Ihrem Bildschirm erscheint, kann von der Gegenstelle gesehen und aufgezeichnet werden.

Sitzung

Geben Sie während der Sitzung so wenige Passwörter wie möglich (im Idealfall keine) ein und surfen Sie nicht auf Internetseiten, die nichts mit der Sitzung zu tun haben. Wenn Sie z. B. Support eines Finanzinstitutes erhalten, dann bleiben Sie auch nur auf der Website des betreffenden Finanzinstitutes.

Beenden

Stellen Sie sicher, dass nach Inanspruchnahme der Hilfeleistung die Remote Support Verbindung beendet wird, um weitere Zugriffe auf Ihr Gerät zu unterbinden. Solange die Verbindung aufgebaut ist, sollte auf dem Bildschirm dauerhaft eine Fernwartungs-Information eingeblendet sein, die nicht versteckt werden kann. Halten Sie sich an die Anweisungen in der Dokumentation zur Software.