ERLEBEN, WAS VERBINDET.

KUNDENINFORMATION ZUM SICHEREN EINSATZ VON STATIONÄREN ENDGERÄTEN BEI DER OCTOPUS NETPHONE UND OCTOPUS NETPHONE CLOUD

1. Allgemeines

1.1. Die Deutsche Telekom GmbH (im Folgenden Telekom genannt) bietet verschiedene Endgeräte zum stationären Einsatz bei der Octopus NetPhone an. Dies sind insbesondere System- und DECT-Telefone wie hier im Internet angeboten, die im Kunden-LAN eingesetzt werden.

1.2. Bereits vor der Zulassung dieser Endgeräte sorgt die Telekom zusammen mit ihren Lieferanten für größtmögliche Sicherheit dieser Geräte.
Bei einem stationären Einsatz im Kundennetz verbleiben Freiräume bzw. Risiken, die durch den Kunden selbst oder dem von ihm beauftragten Service eingeschränkt werden sollten. Nur so kann ein Höchstmaß an Sicherheit bei der Nutzung dieser Endgeräte erreicht werden.

1.3. In dieser Kundeninformation werden entsprechende Hinweise zu dem sicheren Betrieb und der sicheren Nutzung dieser Endgeräte gegeben. Bitte beachten Sie, dass einige dieser Hinweise auf Grund der spezifischen Eigenschaften des Endgerätes, des seitens der Telekom vorgegebenen Geräteprofils oder des Einsatzes (zentral gemanagt) nicht für alle Endgeräte zutreffen.

2. Empfehlungen zur Erhöhung der Sicherheit während der Installation der Endgeräte

2.1. Die folgenden Empfehlungen zur Installation der Endgeräte sollten durch den kundenseitigen Administrator oder z.B. durch den technischen Kundenservice der Telekom beachtet werden:

- Das standardmäßig vorgegebene Passwort für den administrativen Zugang ist für alle ausgelieferten Geräte identisch, es sollte daher bei der ersten Nutzung geändert werden.
  Hinweis: dieses neue Passwort ist an einem sicheren Ort zu verwahren, da ohne Kenntnis dieses Passwortes kein Zurücksetzen in den Auslieferungszustand möglich ist.
- Nicht benötigte Dienste des Endgerätes (z.B. Bluetooth) sollten deaktiviert werden.
- Das Gerät sollte so konfiguriert werden, dass verfügbare Updates automatisch eingespielt werden.
- Das Gerät sollte so konfiguriert werden, dass die jeweils – umgebungs- und einsatzabhängig – bestmögliche Verschlüsselung genutzt wird bzw. werden kann (preferred), d.h. dass anstelle von SIP SIPS (SIP über SSL/TLS) zum Session-Aufbau und bei der Sprachübertragung SRTP statt RTP genutzt wird.
- Die Geräte sind zum Betrieb in einem privaten Netzwerk gedacht, das durch eine Firewall vom öffentlichen Internet getrennt wird. Eine direkte Erreichbarkeit eines Gerätes aus dem Internet heraus sollte vermieden werden.
- Die Möglichkeit zur Ausführung von über USB-Datenspeicher eingebrachter Software sollte spätestens nach Abschluss der Installation ausgeschaltet sein.

3. Empfehlungen zur Erhöhung der Sicherheit während der Nutzung der Endgeräte

3.1. Die folgenden Empfehlungen sollten hinsichtlich der Nutzung der Endgeräte durch den kundenseitigen Administrator und/oder Nutzer beachtet werden:

- Wird der Arbeitsplatz in einem nicht zugangsgeschützten Umfeld verlassen, sollte der Nutzer wie bei einem PC den Zugriff auf ein von ihm alleinig genutztes Endgerät sperren und damit auch dessen Bildschirm verriegeln.
- Das Passwort bzw. die PIN für die Sperrung sollte regelmäßig geändert werden.
- Der administrative Zugang erfolgt üblicherweise als Web Service unter Nutzung eines Internet-Browsers, dem als Ziel die lokale IP-Adresse des Endgerätes vorgegeben wird. Bei Beendigung einer Session sollte sich der Administrator bzw. der Nutzer unbedingt abmelden, bevor das entsprechende Browser-Fenster geschlossen wird.
- Das Passwort für den administrativen Zugang sollte ebenfalls regelmäßig geändert werden.
- Passworte sollten so gewählt werden, dass das Erraten auch auf Basis von Wissen über den Administrator bzw. Nutzer praktisch unmöglich ist.
- Wird über verfügbare Updates (z.B. Octopus NetPhone / Octopus NetPhone Cloud) informiert, sollten diese zeitnah eingespielt werden, sofern dies nicht bereits automatisch erfolgt.
- Die PIN für die SIP-Telefonie müssen bei Geräten, die von mehreren Personen genutzt werden, geheim gehalten werden. Jeder Nutzer muss sich mit seinem persönlichen Passwort anmelden und darf nicht das Passwort eines/einer Kollegen/Kollegin verwenden.

4. Empfehlungen zur Erhöhung der Sicherheit nach der Nutzung der Endgeräte

4.1. Die folgenden Empfehlungen zur Sicherheit nach Nutzung der Endgeräte sollten durch den kundenseitigen Administrator beachtet werden.

Dies ist z.B. in den folgenden Fällen notwendig:
- Störungsfall, bei dem das Endgerät von der Telekom oder dem Lieferanten zurückgenommen wird
- Beendigung der Nutzung des Endgerätes durch einen Nutzer

- Bitte beachten Sie, dass im Endgerät nutzerindividuelle Daten (z.B. Anruferlisten, Wahlwiederholungslisten) gespeichert werden. Das Endgerät sollte daher nach Nutzung in den Auslieferungszustand zurückgesetzt werden (Factory Reset).

5. Weiter Quellen und Produkte zum Thema Sicherheit

5.1. Telekom Ratgeber „Sicher leben in der digitalen Welt“ (www.sicherdigital.de)

5.2. Im Internet bietet die Telekom unter https://geschaeftskunden.telekom.de spezielle Produkte und Services für die Sicherheit der kundenseitigen Netze und Geräte an:

- Sicherheitsprodukte der Deutschen Telekom
- Sicherheitsprodukte der Deutschen Telekom speziell für Endgeräte
- Protect Service bei standortübergreifender Vernetzung
- Sicherheitsprodukte für Netzwerke und Zugänge