Quelle: Siedle (alle Bilder)

**IP-basierte Türkommunikation**

# Smarte Türöffner – ein sensibles Thema

Bei der Türkommunikation lassen sich deutliche Trends feststellen: So wird die IP-basierte Türkommunikation immer wichtiger. Der mobile Türruf per App auf dem Smartphone ist heute oft schon eine Selbstverständlichkeit. Doch müssen Elektroinstallateure dafür immer wieder in das Kundennetzwerk eingreifen? Und wie ist es um die Sicherheitsaspekte bestellt?

Diese Fragen gilt es zu klären. Im folgenden Interview sprechen *Clemens Czibulinski*, Leiter der Softwareentwicklung bei S. Siedle & Söhne, und *Thomas Weiß*, Geschäftsführer von Teamfon, einem Dienstleister für IP-Telefonie und cloudbasierter Kommunikation, über IP-basierte Türkommunikation mit App, über neue Entwicklungen im mobilen Türruf und über die Datensicherheit im sensiblen Bereich zwischen außen und innen.

**»de«: Als Spezialist für Türkommunikation arbeitet Siedle in der App-Entwicklung mit Teamfon zusammen. Warum braucht Siedle für die App-Entwicklung externe Unterstützung?**

**C. Czibulinski:** Teamfon ist kein beliebiger App-Entwickler, sondern führender Spezialist für IP-Telefonie. Thomas Weiß und sein Team bringen ein umfassendes Systemverständnis im Bereich Voice over IP (VoIP) mit, also in der IP-basierten Telefonie. Sie ist heute in der Türkommunikation von immenser Bedeutung und steckt auch hinter unserer App. Die Entwickler bei Teamfon sind mit den Software-Ökosystemen von Apple und Android perfekt vertraut und stehen in stetigem Austausch mit den Anbietern.
**T. Weiß:** Um »am Ball zu bleiben«, schicken wir unsere Entwickler auch schon mal auf eine Apple-Entwicklerkonferenz in Kalifornien. So sind wir im Thema stets ganz vorne dabei. Und wir betrachten die App-Entwicklung ganzheitlich, haben also alle Anwendungsmöglichkeiten im Blick: neben dem Smartphone auch die Smartwatch oder das smarte Auto.

**»de«: IP-basierte Türkommunikation braucht also ständige Pflege und Weiterentwicklung?**

**C. Czibulinski:** Ja, in diesem Punkt unterscheidet sich die IP-Technologie prinzipiell von einem proprietären System, etwa einem Bus. Bei Siedle machen wir in der IP-Türkommunikation gerade einen großen Schritt. In der Vergangenheit gab es unterschiedliche Apps für verschiedene Systeme. Unsere neue App steht unter dem Motto »eine App für alle Systeme«. Wir bieten sie für unsere Bus-Schnittstelle »Smart Gateway« und seit kurzem auch für unser IP-System »Access« an.

Und neuerdings präsentieren wir mit den IQ-Haustelefonen eine Möglichkeit, die Türruf-App auch in Umgebungen mit 1+n und 6+n zu nutzen, im Neubau ebenso wie im Bestand.

**»de«: Was haben die Nutzer von einer App für alle Systeme?**

**C. Czibulinski:** Es gibt ein einheitliches Bedienkonzept – für iOS und Android. Wir bieten damit maximale Klarheit und Übersichtlichkeit. Außerdem sorgen wir dafür, dass die App inhaltlich schlank bleibt. Durch die Fokussierung auf das Wesentliche können wir besser auf die Bedürfnisse der Nutzer eingehen.

Vor ein paar Jahren gab es generell den Trend, sehr viele Funktionen in eine App zu packen. Das ist kompliziert in der Entwicklung und macht eine App schwieriger in der Benutzung. Deswegen konzentrieren wir uns bei unserer neuen App auf einen Anwendungsbereich, optimiert für die Nutzer. Denn wenn es klingelt, will ich das Smartphone aus der Tasche ziehen und direkt mit dem Besucher vor der Tür sprechen. Ich will mich nicht erst durch ein Bedienmenü klicken müssen.

**T. Weiß:** Die schlanke Software-Architektur mit einer App für alle Systeme spart auch Zeit in der Entwicklung und beim Testen. Davon profitieren natürlich auch die Nutzer. Sie erhalten Updates und Patches so schnell wie nie zuvor.

**»de«: Die Vorteile für die App-Nutzer sind eine Sache. Aber was hat der Elektroinstallateur von der neuen App?**

**C. Czibulinski:** Im Hintergrund der App arbeitet eine neue Firmware. Sie macht die Inbetriebnahme viel einfacher und sicherer. Der Elektroinstallateur muss nicht mehr in das Kundennetzwerk eingreifen, er legt nur noch den App-Nutzer an. Dieser scannt dann mit seinem Smartphone und der App einen QR-Code zur Inbetriebnahme. Alle komplexen Anmeldeabläufe spielen sich im Hintergrund ab. Weder der Elektroinstallateur noch der App-Nutzer bekommen davon etwas mit.

**T. Weiß:** Der Elektroinstallateur braucht kein Passwort mehr zu vergeben. Das Passwort steckt im QR-Code. Durch das Einscannen wird dieses automatisch generierte Passwort über den neuen Siedle Server übermittelt. Aus meiner Sicht ist das die ideale Kombination aus Sicherheit und Komfort.

**C. Czibulinski:** Oft ist es schwierig, Sicherheit und Komfort anzuheben. Wenn ich etwas sicherer mache, geht es häufig auf Kosten des Komforts – oder umgekehrt. Bei der Firmware für die neue App ist es uns gelungen, sowohl Sicherheit als auch Komfort zu optimieren.

***Bild 1:*** *Clemens Czibulinski: »Bei Siedle machen wir in der IP-Türkommunikation mit einer App für alle Systeme gerade einen großen Schritt«*

***Bild 2:*** *Thomas Weiß: »Durch die schlanke Software-Architektur erhalten Nutzer Updates und Patches so schnell wie nie zuvor«*

**T. Weiß:** Der Komfort steigt auch, weil der Kunde die App auf seinem Smartphone zu einem beliebigen Zeitpunkt einrichten kann. Der QR-Code reicht dazu aus. Der Elektroinstallateur braucht sich nicht mehr darum zu kümmern.

**C. Czibulinski:** Außerdem muss sich der Elektroinstallateur keine Gedanken machen, wenn sein Kunde den Internetanbieter und den Router wechselt oder wenn Apple eine neue iOS-Version veröffentlicht. Unser Server als zentrale Komponente sorgt dafür, dass solche Anpassungen automatisch im Hintergrund laufen.

**T. Weiß:** Wir entwickeln die App permanent weiter und passen sie an neue Versionen von iOS und Android an. So ist sie immer auf dem neuesten Stand. Sobald zum Beispiel eine neue Betaversion von iOS kommt, fangen wir schon an zu testen. Zum Start sind wir dann gleich kompatibel.

**»de«: Sie haben das Thema Sicherheit angesprochen. Das ist an der Schwelle, im Bereich zwischen außen und innen, ein besonders sensibles Thema. Wie gewährleisten Sie Datensicherheit bei einer App, mit der man auch die Tür öffnen kann?**

**T. Weiß:** Ein wesentlicher Faktor bei Datensicherheit ist die Verschlüsselung. Im Fall der neuen Siedle App gibt es einen kryptografisch gesicherten Austausch mit dem Siedle Server. So ist sichergestellt, dass die App – und auch eine zwischengeschaltete Schnittstelle wie das Smart Gateway – sich ausschließlich mit dem Server verbindet. Es kann sich niemand dazwischenschalten. Wir bieten den höchsten Verschlüsselungsstandard, sogenanntes Certificate Pinning, auch bekannt als Transport Layer Security. Kryptografisch ist das »State of the Art«.

**»de«: Handelt es sich dabei um End-to-End-Verschlüsselung, wie sie aus der E-Mail-Kommunikation bekannt ist?**

**T. Weiß:** Die sicherheitsrelevanten Daten sind Ende-zu-Ende verschlüsselt, zum Beispiel der Türöffner und die Bilder von der Videokamera. Flüchtige Daten in der Audiokommunikation sind im Übertragungsweg verschlüsselt.

Das wichtigste ist der Türöffner, sozusagen das »Heiligste« in der Türkommunikation. Der Türöffner ist mit der neuen Siedle App immer garantiert Ende-zu-Ende verschlüsselt.

**»de«: Diese Verschlüsselung kann also niemand hacken?**

**C. Czibulinski:** Sicherheit ist immer eine Frage des Aufwands. Und Sicherheit ist nicht statisch, schon gar nicht in der digitalen Welt. Es gibt kein Prüfsiegel, das die Sicherheit einer Software garantieren kann. Denn die kann sich ganz schnell ändern. Unsere Strategie bei Siedle ist deshalb: Sicherheit durch permanente Software-Updates.

**T. Weiß:** Bei einem privaten Bauvorhaben habe ich persönliche Erfahrungen mit der Elektrobranche machen können. Nicht jeder Zulieferer für die Elektrobranche hat verstanden, dass Software-Updates und Sicherheit elementar sind. Manche Anbieter können gar keine genaue Auskunft darüber geben, wie es

um die Sicherheit von Apps oder um die Serverkomponenten steht. Das Verständnis hierfür hat sich noch nicht überall durchgesetzt.

**C. Czibulinski:** Unsere Software wird kontinuierlich auf Sicherheitslücken überprüft. Für uns ist wichtig, dass wir in der Lage sind, schnell auf Sicherheitslücken zu reagieren. Wir müssen nicht ein halbes Jahr Analyse und Entwicklungsaufwand hineinstecken. Wenn eine Sicherheitslücke auftritt, können wir kurzfristig ein Patch veröffentlichen, also eine Software zur Fehlerbehebung. Dadurch gewährleisten wir Sicherheit.

**T. Weiß:** Je nachdem, wo eine Sicherheitslücke auftritt, ist auch meine Firma involviert. Dann ist es wichtig, eine offene, transparente Kommunikation zu haben, und die pflegen wir. So können wir potenzielle Sicherheitslücken gemeinsam am schnellsten schließen.

**»de«: Sie haben über die Verschlüsselung der Daten gesprochen. Was aber ist mit dem Server selbst?**

**T. Weiß:** Der Siedle Server wird von uns betrieben, in München. Der Standort Deutschland ist ganz wichtig für die Datensicherheit. Würde der Server etwa in den USA stehen, könnten dortige Behörden Siedle zur Herausgabe von Daten zwingen, weil die Rechtslage eine andere ist. Diese Gefahr besteht nicht, weil der Siedle Server und die gesamte IP-Kommunikation ausschließlich deutschem und europäischem Recht unterliegen.

Außerdem bildet der Server physikalisch einen eigenen, abgeschotteten Bereich mit eigener Firewall und eigenen IP-Ranges. Er ist abgekapselt vom anderem Betrieb in unserem Haus. Es ist keine Public Cloud; es handelt sich um einen dedizierten Siedle-Service. Auf ähnliche Art und Weise haben wir auch schon Banken gehostet. Wir können in diesem Bereich auf mehr als 25 Jahre Erfahrung zurückblicken.

**»de«: Teamfon ist nach der ISO-Norm 27001 für Informationssicherheit zertifiziert. Was hat es damit auf sich?**

**T. Weiß:** Wir sind seit mehr als fünf Jahren zertifiziert. Eine neutrale Prüfinstanz stellt in regelmäßigen Audits unsere Konformität fest. Das ISO-Zertifikat hat eine technische und eine organisatorische Seite. Die Auditoren prüfen, was technisch gelöst wird: zum Beispiel Daten, die so verschlüsselt sind, dass auch Mitarbeiter meiner Firma oder von Siedle nicht daran gelangen können.

Und wenn es um Daten geht, mit denen unsere Mitarbeiter arbeiten müssen, ist die Frage: Wie ist es organisatorisch geregelt, wer

***Bild 3:*** *Eine Türruf-App lässt sich mit dem IQ-Haustelefon von Siedle auch im Bestand nachrüsten*

sind die berechtigten Personen? Ist sichergestellt, dass nur sie an die Daten kommen und dafür gut geschult sind? Wir achten immer darauf, mit Daten sparsam zu sein und sie so zu verschlüsseln, dass weder Teamfon noch Siedle darauf zugreifen können. So werden Bildinhalte direkt verschlüsselt und auf der App entschlüsselt. Niemand außer dem Nutzer kann darauf zugreifen.

**»de«: Das Türöffnen per App ist die Gegenwart. Welche Entwicklungen sehen Sie für die Zukunft? Wie wird IP die Türkommunikation in den nächsten Jahren verändern?**

**C. Czibulinski:** Ein großes Zukunftsthema ist der Keyless Entry, also der schlüssellose Zugang, bei dem wir neue Möglichkeiten erproben. Uns ist wichtig: Bei allen Lösungen, die Siedle für den Eingang entwickelt, hat Sicherheit oberste Priorität. In jüngster Zeit sind intelligente persönliche Assistenten ein großes Thema, am bekanntesten ist wohl Alexa von Amazon. Wir werden immer wieder nach Verknüpfungen oder Einbindungen in die Türkommunikation gefragt. Auch hier gilt: Sicherheit zuerst. Wir prüfen sehr genau, was dahintersteckt, schließlich geht es um den Zugang zum eigenen Haus.

**T. Weiß:** Bei diesen Software-Assistenten gibt es verschiedene Systemarchitekturen. Die muss man sich immer genau anschauen. Sowohl Alexa von Amazon als auch Siri von Apple sind intelligente persönliche Assistenten, die ich mir mit Lautsprecher in mein Smart Home stellen kann und mit denen ich dann kommuniziere. Die entscheidende Frage ist: Wo findet die Applikation statt? Unternehmen wie Google oder Amazon verdienen mit Daten viel Geld. Ihnen ist wichtig zu wissen: Was machen die Nutzer? Darauf basiert ihr Geschäftsmodell. Das wirkt sich natürlich auch in der Verschlüsselung der Daten und damit letztlich in der Sicherheit aus. Bevor man also eine Software in die IP-Türkommunikation einbindet, muss man immer den Datenfluss im Auge haben: Welche Daten gelangen wohin? Und wer hat Zugriff darauf?

Was aus Nutzersicht komfortabel wirken mag, widerspricht möglicherweise der Sicherheit. Dazu ein Gedankenspiel: Wenn in Ihrem Smart Home ein Fenster gekippt ist und irgendjemand würde hineinrufen: »Smart Device, öffne die Haustür« und die Tür geht dann wirklich auf … das wäre unter dem Sicherheitsaspekt natürlich verheerend!

**C. Czibulinski:** Aus meiner Sicht ist der schlüssellose Zugang oder Keyless Entry trotzdem ein wichtiges und zukunftsträchtiges Thema. Ich denke, heute kann niemand sagen, wie das Thema App in fünf oder zehn Jahren aussehen wird – ob es dann überhaupt noch Apps geben wird. Aber das Smartphone als Device, als Schlüssel in der Hosentasche, das wird uns weiter begleiten.

**T. Weiß:** Allerdings ist der Begriff Keyless Entry genaugenommen nicht richtig. Es gibt ja noch einen Schlüssel, einen Key: Das ist das Smartphone. Es ist eben kein physikalischer Schlüssel mehr. Man kann diese Entwicklung auch in der Autobranche beobachten. Es gibt mittlerweile Autos, die ich mit dem Smartphone öffnen kann. Ähnliches gilt übrigens auch für die Geldtasche. Apple Pay und Google Pay sind inzwischen schon recht etabliert. Damit kann ich mit meinem Smartphone oder meiner Smartwatch an der Supermarktkasse zahlen und brauche kein Portemonnaie mehr bei mir zu haben.

Viele Menschen haben die Sorge, dass damit einiges unsicherer wird. In Wirklichkeit ist es aber sicherer. Verliere ich meinen Hausschlüssel, kann jeder den Schlüssel verwenden. Aber wenn ich mein Smartphone verliere, ist dieses meist PIN-geschützt. Und den digitalen Hausschlüssel darauf kann ich aus der Ferne, remote, löschen. Dann hat ein Dieb keinen Zugriff auf meinen Hausschlüssel. Bei welchem mechanischen Schlüssel kann ich sagen: Den lösche ich einfach? – Gefühlt wirkt das Smartphone unsicherer als ein mechanischer Schlüssel. Tatsächlich ist es aber weitaus sicherer.

***Autor:***
*Clemens Jesenitschnig*
*Unternehmenskommunikation,*
*S. Siedle & Söhne, Furtwangen*