Sicherheitshinweis Anlagenhacking

Stand 10/2017

Liebe Kundinnen und Kunden,

leider hat in den letzten Jahren das nicht gesetzeskonforme Verhalten unterschiedlicher Personen und / oder Gruppen zugenommen. Die Ursache hierfür ist sicherlich – neben anderen Ursachen – auch in dem permanenten Bestreben, die eigene finanzielle Situation zu verbessern, zu sehen. Leider bedient sich dabei nicht jede Person und / oder Gruppe legaler Mittel.

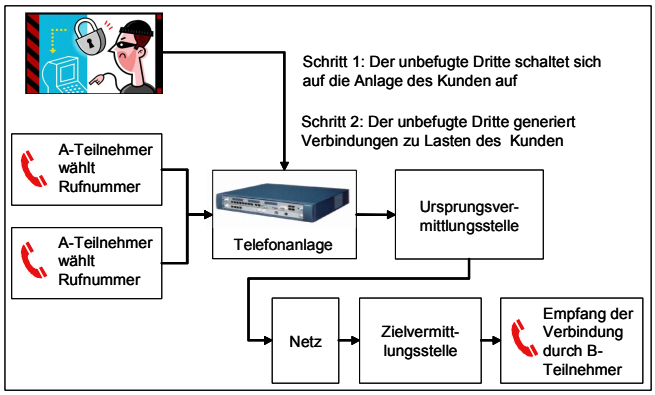
Um Sie als unsere Kunden über mögliche Gefahrenquellen zu informieren, haben wir den nachfolgenden Hinweis zum Thema Anlagenhacking entwickelt. Wir als 1&1 Versatel GmbH hoffen, Ihnen damit eine kleine Hilfestellung geben zu können, wie Sie sich besser vor Eingriffen in Ihre Telefonanlagen schützen können.

Jörg Elsäßer
Chief Sales Officer

Winfried Schnitzler
Head of Internal Audit, Compliance & Security

Eine kurze Einführung zum Anlagenhacking

Hacking bezeichnet die Generierung und Weiterleitung missbräuchlichen Verkehrs durch Manipulation fremder Telefonanlagen. Dabei werden in der Regel Gespräche ins Ausland generiert.



Ursache für die Generierung missbräuchlichen Verkehrs ist oftmals der mangelhafte Schutz von Telefon- oder VoIP Anlagen.

Vorgehensweise

Bei den Angriffen auf die Telekommunikationsanlagen gibt es zurzeit zwei Vorgehensweisen:

1. Der Angriff erfolgt über das Telekommunikationsnetz:

Die Telefonanlagen besitzen ein Leistungsmerkmal, welches den Nutzern bei aktivierter Sprachbox (Voicebox) die Konfiguration der Telefonanlage aus der Ferne gestattet. Dies erfolgt durch Anwahl der Telefonnummer des Nutzers. Erfolgt dann die Ansage der Voicebox, besteht die Möglichkeit, unter Eingabe einer Tastenkombination (herstellerabhängig) und einer PIN (meistens vierstellig, alles Ziffern), Veränderungen an der Telefonanlage vorzunehmen. Hier bestehen dann unter anderem folgende Möglichkeiten:

- Einrichtung neuer Nebenstellen für die Anlage;
- Automatische Anrufweiterschaltung auf Nebenstellen der Anlage (z.B. auf eine ausländische Rufnummer oder eine Servicerufnummer);
- Weitervermittlung auf Nebenstellen der Anlage.

Wenn die Täter diese Veränderungen vorgenommen haben, werden alle Anrufe, die auf den manipulierten Nebenstellen eingehen, auf die eingerichtete Rufnummer der Anrufweiterschaltung geleitet.

Nachfolgend möchten wir Ihnen einige Möglichkeiten erläutern, die Ihnen zur Verfügung stehen um Ihre Telefonanlage zu schützen:

- Generelles Deaktivieren der oben genannten Funktionalitäten. Dadurch können Veränderungen (wie z.B. Anrufweiterleitung) nur noch von Anschlüssen erfolgen, die direkt mit der Anlage verbunden sind.
- Änderung der Anzahl der möglichen Fehlversuche bei falscher PIN-Eingabe (ist jedoch nicht bei allen Anlagen möglich). Bei den Anlagen, die diese Funktion beinhalten, sollte die Anzahl der Fehlversuche auf maximal drei begrenzt werden.
- Bei jeder eingerichteten Voicebox muss das werksseitig eingerichtete Passwort geändert werden. Wenn die Anlage die Funktion besitzt, sollte das Passwort auf wenigstens acht Zeichen heraufgesetzt werden. Bei dem neuen Passwort sind möglichst keine Zahlenreihen (12345678) oder gleiche Zahlen (99999999) zu verwenden.
- Softwareaktualisierungen der Anlage müssen regelmäßig durchgeführt werden, damit die Anlage auf den neuesten Stand ist. Es besteht die Gefahr, dass bei Softwareupdates Ihrer Anlage eingerichtete Passwörter zurückgesetzt werden. Bitte prüfen Sie daher nach erfolgtem Update alle Passwörter und passen diese ggf. auf ein sicheres Niveau an.

2. Der Angriff erfolgt über das Internet:

Haben Telekommunikationsanlagen eine Internetanbindung, so kann der Angriff auch über ungeschützte SIP-Ports erfolgen. In den meisten Fällen sind dies die Ports 5060/5061. Hier gibt es die Schutzmöglichkeit der Portsicherung über eine Firewall oder die Deaktivierung dieser Ports.

Telefonanlagen besitzen in der Regel einen Fernwartungszugang, der aus dem Internet erreichbar ist. Dieser Fernwartungszugang sollte ebenfalls mit einem komplexen Passwort und einer Sperre nach mehreren Fehlversuchen versehen werden, idealerweise liegt der Fernwartungszugang hinter einer Firewall, die den Zugriff limitiert.

Gesprächsprotokolle im Router sollten regelmäßig kontrolliert und ausgewertet werden.

Disclaimer

Leider können diese Hinweise keinen Anspruch auf Vollständigkeit erheben. Personen und / oder Gruppen, die über Eingriffe in fremde Telefonanlagen missbräuchlichen Verkehr generieren, sind in der Auswahl ihrer Methoden sehr variantenreich.

Bitte kontaktieren Sie im Bedarfsfall auch Ihren Anlagenbetreuer, wenn Sie Unterstützung bei der Umsetzung von Sicherheitsmaßnahmen zum Schutze Ihrer Telefonanlagen benötigen.

1&1 Versatel GmbH, Niederkasseler Lohweg 181-183, 40547 Düsseldorf
Geschäftsführer: Dr. Jürgen Hernichel (Vorsitzender), Dirk Brameier, Jörg Elsäßer, Guido Mannshausen
Sitz der Gesellschaft: Berlin, Registergericht: Charlottenburg HRB 146659 B