Sicherheitsleitfaden für Astimax 3 IP Telefonanlagen

1 Allgemeines

Durch die Integration von Telefonanlagen in IP Netze bieten sich neue Angriffsziele für Hacker. Die Angriffe auf unzureichend gesicherte VoIP Lösungen nehmen permanent zu. Dabei ist das Ziel zumeist, die gehackte Telefonanlage zu missbrauchen, um Telefonate auf fremde Kosten führen zu können. Häufig werden bei Hackerangriffen kostspielige Rufnummern im Ausland angerufen, die die Telefonrechnung schnell in die Höhe treiben. Häufig werden dafür schlecht gesicherte SIP-Accounts verwendet, die nur durch ein einfach zu erratendes Passwort geschützt sind. Bei einer monatlichen Rechnungsstellung wird ein derartiges Problem zudem noch viel zu spät bemerkt.

Ein IT-Grundschutz der VoIP TK-Anlage ist somit genauso unerlässlich wie für die übrige IT Infrastruktur auch. Die nachfolgenden Punkte sollen Ihnen eine Hilfestellung geben, eine Grundsicherung bei der Installation einer Astimax IP Telefonanlage herzustellen.

Astimax IP Telefonanlagen verwenden zur Kommunikation sowohl mit dem Astimax Admin als auch mit dem Astimax User Interface im Standard SSL geschützte Verbindungen.

2 Passworte

Astimax IP Telefonanlagen bieten zahlreiche Möglichkeiten, Zugänge durch Passworte zu schützen. Diese sollten in jedem Fall genutzt werden. Generell gilt für Passworte

1) Verwenden Sie Passworte ausreichender Länge (mind. 8 Zeichen)
2) Verwenden Sie keine Worte, die in einem Lexikon stehen könnten
3) Verwenden Sie zufällige Kombinationen von Buchstaben, Zahlen und Sonderzeichen
4) Verwenden Sie sowohl Klein- als auch Großbuchstaben
5) Halten Sie Passworte geheim

2.1 Administratoren

Administratoren haben die Möglichkeit, sämtliche Funktionen der Telefonanlage zu steuern. Richten Sie jedem Administrator einen persönlichen Zugang mit einem eigenen sicheren Passwort ein.

2.2 Externe Systeme

Astimax IP Telefonanlagen können durch Fremdsysteme gesteuert oder überwacht werden. Zu diesen zählen im Speziellen

- BMS

- Nagios
- SNMP

die durch eigene Passworte gesichert werden können und müssen. Der Zugriff von BMS und Nagios wird zusätzlich durch das Hinterlegen einer IP Adresse der entsprechenden Systeme auf diese eingeschränkt.

2.3 Nebenstellen

Nebenstellen haben bis zu 3 verschiedene Passworte.

- Astimax User: Das Passwort für den Webzugriff der Benutzer
- TAPI: Für Geräte, die die TAPI-Schnittstelle verwenden
- SIP/IAX2: Das Passwort für die SIP- bzw. IAX2 Endgeräte

Insbesondere sollte das SIP/IAX2-Passwort kryptisch sein, da es sich hier um die Authentifizierung der Endgeräte handelt. Ist ein Endgerät angemeldet, kann es prinzipiell zunächst Telefonate generieren, wenn nicht weitere Schutzmaßnahmen greifen.

2.4 Sprachmailboxen

Sprachmailboxen sollten durch eine ausreichend lange PIN geschützt werden. Mit ihr ist es möglich, die Sprachmailboxen abzufragen und zu konfigurieren.

2.5 Ansagen

Die Ansagen bieten die Möglichkeit, Weiterleitungen auf Basis der Eingabe einer PIN durchzuführen.

2.6 VoIP Provider

Der Zugang zu VoIP Providern sollte durch ein Passwort geschützt werden.

2.7 Callthrough

Die Funktion Callthrough kann sowohl durch eine PIN geschützt als auch auf einzelne Rufnummern eingeschränkt werden.

3 Limitierung von gleichzeitigen Gesprächen

Das normale Telefonieaufkommen ist in der Regel bekannt, so dass es möglich ist, Limitierungen auf die maximal gleichzeitig möglichen Gespräche zu konfigurieren. Dies sollte entsprechend bei den SIP VoIP Provider eingestellt werden. Zusätzlich bieten die Astimax IP Systeme den Schutz, dass pro Nebenstelle im Standard nicht mehr als 3 gleichzeitige Gespräche geführt werden können. Dieser Wert lässt sich in einem Wertebereich zwischen 1 und 10 als Gesprächslimit pro Nebenstelle einstellen.

4 Rechte

Astimax IP Systeme bieten unterschiedliche Rechtesysteme sowohl auf Administrator- als auch auf Nebenstellenebene.

4.1 Administratoren

Administratoren können einzelne Zugriffsrechte auf Konfigurationsmasken zugeteilt werden. Jedem Administrator sollten damit nur so viele Rechte gegeben werden, wie er für seine tägliche Arbeit unbedingt benötigt.

4.2 Nebenstellen

Nebenstellen können Rechte zugeteilt werden, in welchen Entfernungszonen telefoniert werden darf. Es stehen 4 Klassen zur Auswahl.

- Intern
- Lokal
- National
- International

Teilen Sie jeder Nebenstelle nur die notwendige Entfernungszone zu.

4.3 AWS

Anrufweiterschaltungen lassen sich auf Entfernungszonen einschränken. Erlauben Sie nur die unbedingt notwendigen Entfernungszonen. AWS mit Entfernungszonen lassen sich an folgenden Stellen konfigurieren:

- Nebenstellen
- Teams

5 IP Sicherheit

Mit Hilfe der Maske Sicherheit können Sie die Zugriffs- bzw. Anmeldemöglichkeiten von SIP-, IAX- und AMI-Accounts auf bestimmte IP Netze oder IP Adressen einschränken. Eine Anmeldung einer SIP- bzw. IAX-Nebenstelle ist dann nur noch aus den erlaubten IP-Adressbereichen möglich. Auch die AMI-Accounts für TAPI werden auf die gleichen IP-Adressbereiche eingeschränkt.

6 Callrouting

Das Callrouting bietet Ihnen mehrere Möglichkeiten, abgehende Gespräche zu limitieren. Sie können Routings sowohl auf Wochentage und Tageszeiten einschränken als auch die IP-Adressen der Nebenstellen berücksichtigen.

- Erlauben Sie Routings nur für definierte IP-Netze, die von Ihren Nebenstellen verwendet werden. Meldet sich eine Nebenstelle aus einem anderen Netz an, so ist nur ein internes Gespräch möglich.
- Blockieren Sie unerwünschte Rufnummern, in dem Sie z.B. die Wahl von Rufnummern des Typs 0900 komplett unterbinden oder nur für einzelne Nebenstellen freischalten.
- Erlauben Sie nur Gespräche in die Länder, mit denen Sie wirklich kommunizieren müssen.
- Konfigurieren Sie Ihr Routing so, dass nur zu Ihren Geschäftszeiten telefoniert werden kann und erlauben Sie nur einzelnen Nebenstellen ggf. eine Ausnahme

7 Mappings

Prüfen und Löschen Sie alle Mappings auf interne Rufnummern, die von extern nicht erreichbar sein müssen oder sollen, um ggf. das Ausnutzen und Setzen geschickter Anrufweiterschaltungen zu erschweren.

8 Firewall

Schützen Sie in jedem Fall Ihre Telefonanlage vor dem öffentlichen IP-Netz durch eine Firewall. Erlauben Sie nur absolut notwendige Verbindungen beispielsweise zu Ihren VoIP Providern oder zu bekannten Nebenstellen und Partnern. Schränken Sie die Verbindungen auf die notwendigen Protokolle ein.

9 Alarmierungen

Überwachen Sie Ihre Telefonanlage und richten Sie sich bei ungewöhnlichen Verhalten Alarmierungen ein. Überwachungen sind beispielsweise durch SNMP möglich.

- CPU
- RAM
- Anzahl gleichzeitiger Calls

Fragen Sie Ihren VoIP Provider nach Alarmfunktionen bei Überschreitungen definierter Gebührenlimits oder ungewöhnlich hohen Gesprächsaufkommen ins Ausland.

10 Softwareupdates

Halten Sie die Software Ihrer Telefonanlage aktuell. So stellen Sie sicher, dass Sicherheitsprobleme auch durch notwendige Updates automatisch geschlossen werden.