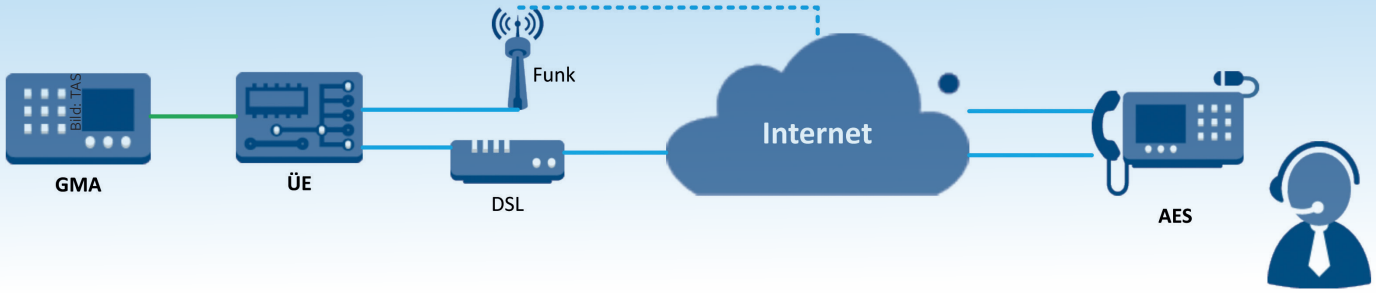

Schema einer normkonformen Alarmübertragung.

Cyber-Security in der Übertragungstechnik

All-IP bringt neue Gefahren

Florian Engels

Eine Alarmübertragungseinrichtung (ÜE) übernimmt die Weiterleitung bei Alarm- und Störmeldungen von Einbruch- und Brandmeldeanlagen (GMA) hin zu Alarm-Empfangs-Stellen (AES). Früher wurden dazu leitungsvermittelnde Netze wie ISDN, analog oder GSM verwendet. Bedingt durch die Migration ins sogenannte All-IP – also alles wird IP – werden heute paketvermittelnde Netze wie IP oder Funk (2G/3G/4G) genutzt.

Die Gründe für den Wandel der Netze sind zahlreich. So werden beispielweise ISDN und analog sukzessive abgeschafft, um den Breitbandinternetausbau vorantreiben zu können. Auch die Funknetze werden ausgedünnt. Hier kommt derzeit das GSM-Netz in den Fokus der Provider. So wird derzeit Zug um Zug CSD (Circuit Switched Data) abgeschafft, ein in der Alarmübertragungstechnik viel genutzter Datendienst. Auch hier steht der Breitbandausbau in Form von LTE (4G) und künftig 5G im Vordergrund.

Angriffsziel Alarmüberübertragungsgeräte

Dieser Wandel bleibt nicht ohne Folgen. So wird beispielweise beim Kunden die bisherige notstromversorgte ISDN-Leitung durch einen All-IP-Anschluss ersetzt. Den Internetzugang stellt dabei ein DSL-Router her, der lediglich mit einem einfachen Steckernetzteil betrieben wird. Die bisherige Notstromversorgung entfällt daher.

Darüber hinaus bringt die neue All-IP-Welt auch Gefahren mit sich, die man bisher bei Alarmübertragungsgeräten nicht kannte. So sehen sich Alarmübertragungsgeräte durch die Wandlung der Netze nun auch Cyber-Attacken ausgesetzt.

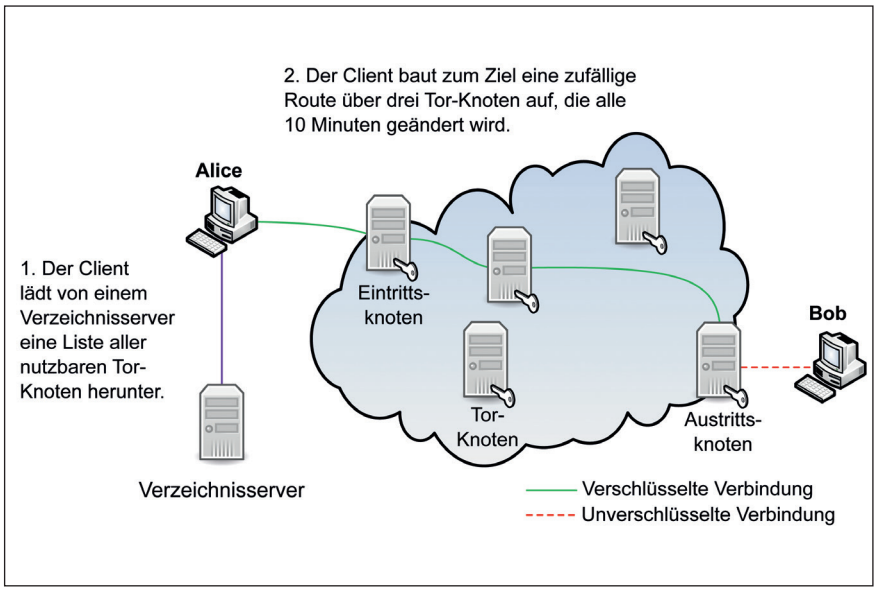

Bild: Wikipedia.org

Das Prinzip Onion-Routing von Tor.

Schwachstelle Remote-Zugang

Eine zentrale Schwachstelle stellt dabei der Remote-Zugang dar. Die einschlägige Norm im Bereich der Alarmübertragungstechnik – die EN 50136 – beschäftigt sich dabei Stand heute vorwiegend mit der Umsetzung einer sicheren Alarmaufschaltung bei einer ständig besetzten Leitstelle (AES). Eine Regelung oder Verpflichtung zur Realisierung eines sicheren Remote-Zuganges gibt es dagegen derzeit nicht.

Bisher erfolgte ein Remote-Zugriff direkt auf die Endgeräte via ISDN, analog oder via GSM. Dabei wurde die bei ISDN oder GSM mitgeschickte Rufnummer auf den Endgeräten ausgewertet und der Zugriff gestattet oder abgewiesen. Der Schluss liegt nahe, dass auch in der neuen All-IP-Welt ein direkter Remote-Zugriff sinnvoll wäre. Aus Sicht von Sicherheitsexperten birgt dies jedoch massive Gefahren.

So müssen für einen direkten Fernzugriff in der Firewall des Routers Ports freigeben werden, über welche die Kommunikation zur Übertragungseinrichtung weitergeleitet wird. Dieses Verfahren wird auch Portweiterleitung beziehungsweise „Portforwarding“ genannt. Allerdings steigt mit jedem geöffneten Port das Risiko, angreifbar zu werden.

Wie Hacker vorgehen

Hacker könnten genau das ausnutzen und sich einen Zugang zum System verschaffen. Insbesondere dann, wenn unsichere Kennwörter verwendet werden, ist das Risiko hoch, Opfer einer Cyber-Attacke zu werden.

Eine Rückverfolgbarkeit ist dabei nur schwer gegeben, da Cyber-Kriminelle ihre wahre Identität zu verschleiern wissen. So wird von Cyber-Kriminellen häufig das beliebte Anonymisierungsnetzwerk „Tor“ missbraucht. Tor funktioniert nach dem Prinzip des sogenannten Onion-Routings. Das bedeutet, dass die Verbindung innerhalb des Tor-Netzwerkes verschlüsselt über drei Server geleitet wird, um eine Rückverfolgbarkeit massiv zu erschweren. Zusätzlich wird die Route alle zehn Minuten geändert.

Mit Hilfe dieser Anonymisierung sowie kostenloser legaler Tools für Linux-Betriebssysteme ist es Hackern möglich, anonym die Kontrolle über Endgeräte zu übernehmen, sofern diese schlecht gesichert sind. Unsichere Kennwörter wie beispielweise „123456“ können mit Hilfe von Passwortlisten innerhalb von Sekunden gefunden werden und stellen daher keinen Schutz dar.

Doch nicht nur Kennwörter stellen eine Gefahr dar, sondern auch Software, die auf Endgeräten läuft. So kann ein Angreifer auch beispielsweise die Kontrolle über ein System übernehmen, wenn der dort verwendete Browser zu alt ist und Sicherheitslücken aufweist. Sogenannte Exploits öffnen einem Angreifer dann Tür und Tor, indem sie einen sogenannten Speicherüberlauf (englisch: Bufferoverflow) produzieren, der ausführbaren Schadcode – auch „Payload“ genannt – in das Endgerät einschleust. Dieser Schadcode wird nicht einfach „weggeworfen“, sondern fällt wie bei einer Sektpyramide in andere Speicherbereiche und wird ausgeführt.

Sichere Konzepte

Umgehen kann man dieses Problem, indem bei Übertragungsgeräten wie der „TAS-Link“, „SIRO-Port“ oder „MC-Link-Serie“ ein monolithischer Block von Software eingesetzt wird, der keine Möglichkeit zum Nachladen von Software bietet.

Darüber hinaus stellen sichere Kennwörter sowie sichere Fernzugangskonzepte einen Garant für Sicherheit dar. Sichere Fernzugangskonzepte sehen neben Vollverschlüsselung auch eine vorgelagerte Authentifizierungsplattform vor. So ist ein direkter Fernzugriff auf Übertragungsgeräte nicht mehr möglich, ohne sich zunächst bei einem zentralen Server zu authentifizieren. TAS stellt hier für TAS-Übertragungseinrichtungen der Serien „TAS-Link III, SIRO-Port“ oder „MC-Link“ den TAS-Connection-Server (TCS)“ zur Verfügung.

Die Funktionsweise des TCS sieht vor, dass die Alarmübertragungseinrichtungen sich selbständig mit dem TCS verbinden, welcher beispielsweise bei einer Errichterfirma oder auch einem Wachdienst untergebracht werden kann. Ist ein Remote-Zugriff gewünscht, so muss sich der Service-PC/Notebook zunächst am TCS authentifizieren und erhält erst dann Zugriff auf alle erlaubten und aufgeschalteten Übertragungsgeräte.

Da sich die Übertragungsgeräte selbständig mit dem TCS verbinden, müssen vor Ort keine Firewall-Regeln eingerichtet werden. Auch muss keine IP-Adresse des DSL-Routers bekannt sein, da eine Vermittlung durch den TCS mittels Identnummer erfolgt. Neben dem IP-Festnetz funktioniert die TCS-Fernwartung auch über den Mobilfunkweg.

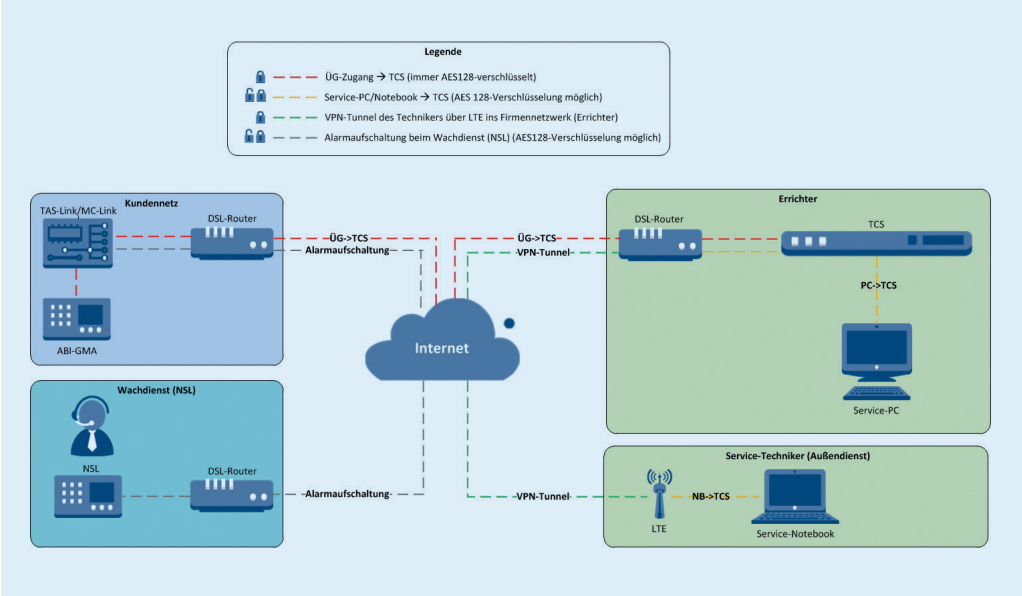

Bild: TAS

Arbeitsweise des TAS-Connection-Servers.

Florian Engels, Produktmanager Security, Telefonbau Arthur Schwabe GmbH & Co. KG, www.tas.de