
vodafone
business

IP Anlagen-Anschluss

Security Assessment

In Kooperation mit REPLY S.P.A.

vodafone business

Inhalt

1. Bedrohungslage und Bedrohungen
2. Gegenmaßnahmen
3. SIP-Registrierung
4. Verschlüsselung
5. Vodafone Voice Gateway im Modus E-SBC

Einleitung

Vodafone bietet seit 2006 mit dem IP Anlagen-Anschluss ein SIP-Trunking-Produkt an. In den letzten Jahren ist zunehmen das Thema Sicherheit in den Fokus gerückt. Immer mehr Kunden fragen nach Schutzmaßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit. Häufig basieren die Fragen auf Empfehlung des *Bundesamts für Sicherheit in der Informationstechnik* (BSI) oder *SIP-Connect.*

In Kooperation mit der REPLY S.P.A. (www.reply.com), einem Spezialisten für IT-Sicherheit und Telekommunikation, hat Vodafone die Bedrohungslage und die Wirksamkeit von Gegenmaßnahmen für den IP Anlagen-Anschluss systematisch untersucht und bewertet.

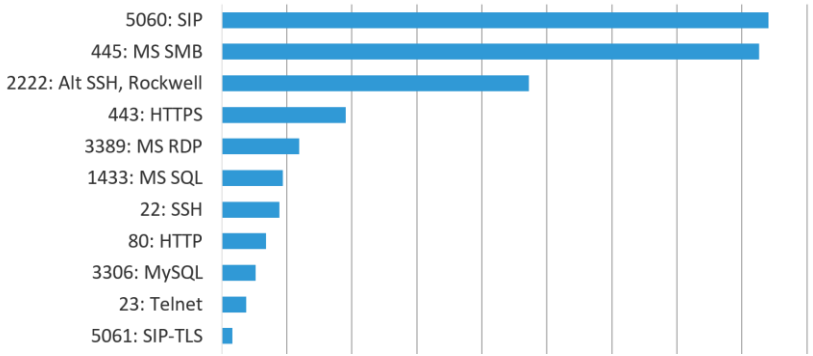
Seit 2024 unterstützt der IP Anlagen-Anschluss neben dem Static-Mode auch den Registration-Mode. Die bislang betrachteten Bedrohungen und Gegenmaßnahmen gelten auch für den Registration-Mode. Es sind allerdings auch Angriffe auf die SIP-Registrierung selbst möglich, welche in der vorliegenden Version dieses Dokuments ebenfalls betrachtet werden.

Zur Unterstützung der Sicherheit auf Kundenseite bietet Vodafone das *Voice Gateway im Modus E-SBC* an. Der Hardware-SBC wird von Vodafone bereitgestellt, installiert und betrieben.

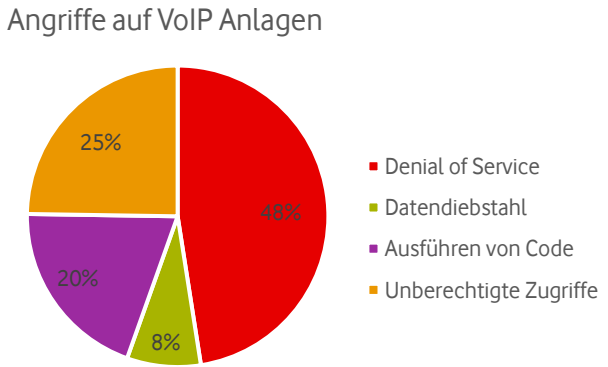
1 Bedrohungslage und Bedrohungen

Bedrohungslage

Aktuelle Statistiken zeigen, dass VoIP-Anlagen eines der am stärksten frequentierten Ziele von Angriffen im Internet sind. Eine Studie des Herstellers F5 aus dem Jahre 2019 sieht dabei das SIP Protokoll an erster Stelle der attackierten Netzwerkdienste. In einer anderen Studie wurde festgestellt, dass annähernd die Hälfte aller Attacken mit dem Ziel durchgeführt wurden, die Verfügbarkeit der Telefonanlagen zu beeinträchtigen.



https://www.f5.com/labs/articles/threat-intelligence/regional-threat-perspectives--europe



Quelle: Voice over IP Security: A Comprehensive Survey of Vulnerabilities and Academic Research

Allgemeine Bedrohungen

- **Caller-ID Spoofing**: Eingehende Anrufe mit einer gefälschten Identität (Rufnummer)
- **PBX-Hacking**: Angriffe auf Funktionen der Telefonanlage (z. B. Mailbox)
- **Call Flooding**: Überlastung der Telefonanlage durch viele eingehende Anrufe
- **Application-Layer DoS**: Angriffe auf die Telefonanlage durch spezielle SIP-Pakete
- **Distributed Flooding auf Netzwerkebene**: Angriffe durch eine Flut von UDP- oder TCP-Paketen
- **Ausnutzung von Software-Schwachstellen**: Gezielte Ausnutzung bekannter Fehler in VoIP-Netzelementen
- **UDP Spoofing**: SIP-UDP-Pakete mit gefälschter IP-Absenderadresse
- **SIP Header Information Leak**: Sammeln von Information über die VoIP-Infrastruktur auf Basis von SIP-Headern
- **Mithören von Gesprächen**: Aufzeichnen oder Duplizieren von Medienströmen
- **Man-in-the-Middle Angriffe**: Manipulation und Entschlüsselung von Gesprächen

Bedrohungen für SIP-Registrierung

- **Ungeschützte Registrierungsdaten:** Zugriff auf die Registrierungsdaten durch Dritte
- **Hash-Cracking:** Durch Ausprobieren einen gültigen Hash-Wert ermitteln, der normalerweise vom Endgerät unter anderem auf Basis des Benutzernamens und Passworts berechnet und bei der Registrierung übermittelt wird.
- **Replay-Angriffe:** Mitlesen einer Registrierung und Versuch einer eigenen Registrierung von einem anderen Endpunkt mit den gleichen Daten.
- **Man-in-the-Middle Angriffe**: Z. B. in Verbindung im einem Downgrade-Angriff, die Registrierung auf ein niedriges Sicherheitsniveau zu drücken.

Bedrohungen – Risikobewertung

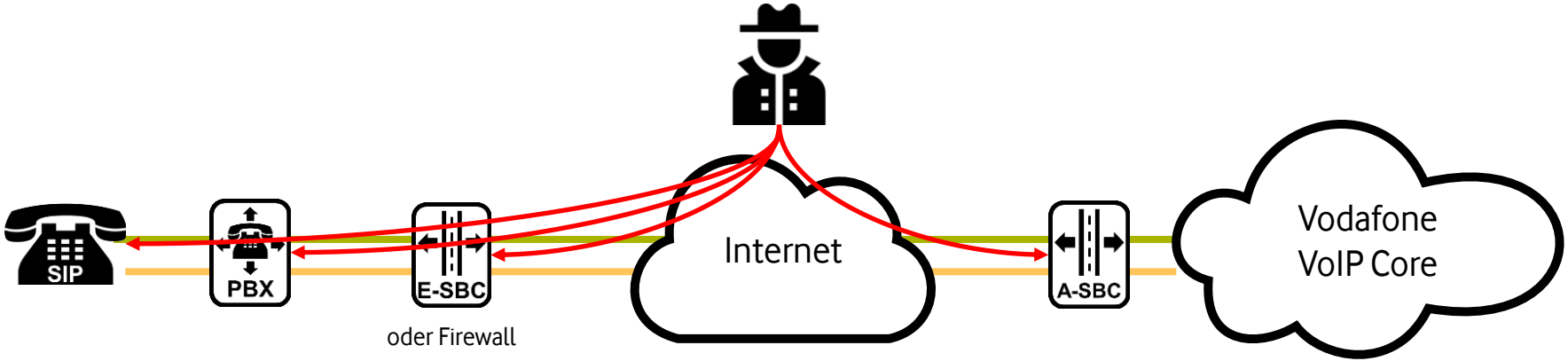
Die Tabelle beschreibt die Gesamtrisikobewertung der unterschiedlichen Bedrohungen auf Basis der Komplexität des Angriffs, der erforderlichen Privilegien des Angreifers, des Umfangs der Betroffenen und der Auswirkungen für die Betroffenen. Hierbei handelt es sich um eine generische Bewertung. Risiken können für Unternehmen sehr unterschiedlich eingestuft werden. Für manche Unternehmen steht die Verfügbarkeit an oberster Stelle, für andere die Vertraulichkeit.

Bedrohung	Gesamtrisikobewertung
Caller- ID Spoofing	Mittel
PBX-Hacking	Niedrig bis Mittel
Call Flooding	Hoch
Application-Layer DoS	Niedrig bis Mittel
Distributed Flooding auf Netzwerkebene	Hoch
Ausnutzung von Software-Schwachstellen	Mittel
UDP Spoofing	Mittel bis Hoch
SIP-Header Information Leak	Niedrig
Mithören von Gesprächen	Mittel
Man-in-the-Middle Angriffe	Mittel
SIP-Registrierung	
Ungeschützte Registrierungsdaten	Hoch
Hash-Cracking	Mittel
Replay-Angriffe	Gering
Man-in-the-Middle Angriffe	Mittel

Bedrohung – Angriffe aus dem Internet

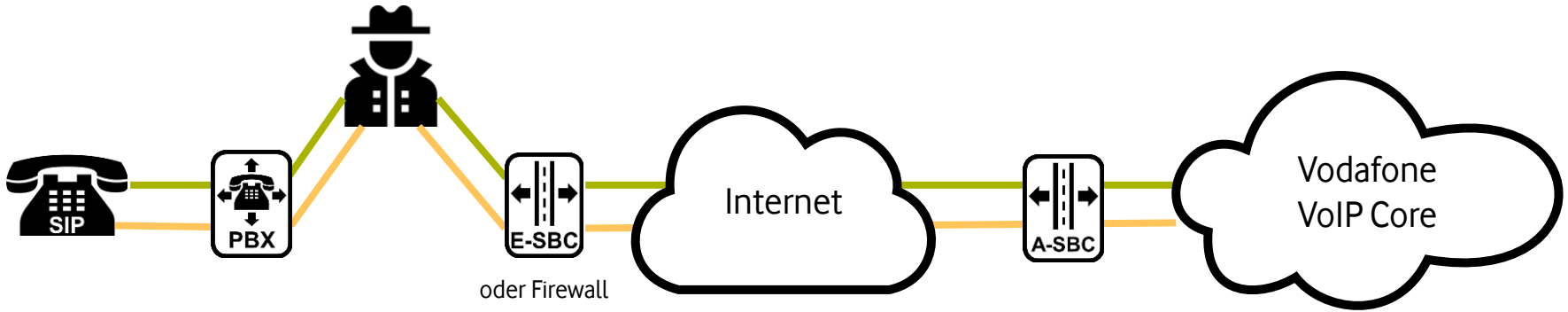
Die meisten Angriffe erfolgen aus dem Internet. Hierbei handelt es sich in erster Linie um Denial-of-Service und digitale Angriffe mit dem Ziel über Erpressung oder Gebührenbetrug finanzielle Gewinne zu erzielen. Die Komplexität der Angriffe ist gering. Für gezielt Angriffe benötigt der Angreifer aber Informationen über genutzte IP-Adressen.

Angriffe auf die Vertraulichkeit (z. B. Abhören von Gesprächen oder Man-in-the-Middle) sind aus dem Internet eher unwahrscheinlich, da der technische Aufwand hoch bis unmöglich ist.



Bedrohung – Innenangriffe

Angriffe auf die Vertraulichkeit erfolgen meistens innerhalb der Infrastruktur eines Unternehmens, z. B. durch *verstimme Mitarbeiter (disgruntled employee)*. Neben direkten Angriffen auf Netzelemente, sind Man-in-the-Middle-Angriffe möglich. Diese können darauf ausgerichtet sein, Inhalte zu verändern oder Verschlüsselungen zu brechen. Eine Verschlüsselung kann auch durch einen Downgrade-Angriff gebrochen werden, in dem sich der Angreifer beim Aufbau der verschlüsselten Verbindung, in die Aushandlung der Verschlüsselungsparameter einmischt und dafür sorgt, dass unsichere oder gar keine Verschlüsselung erfolgt.

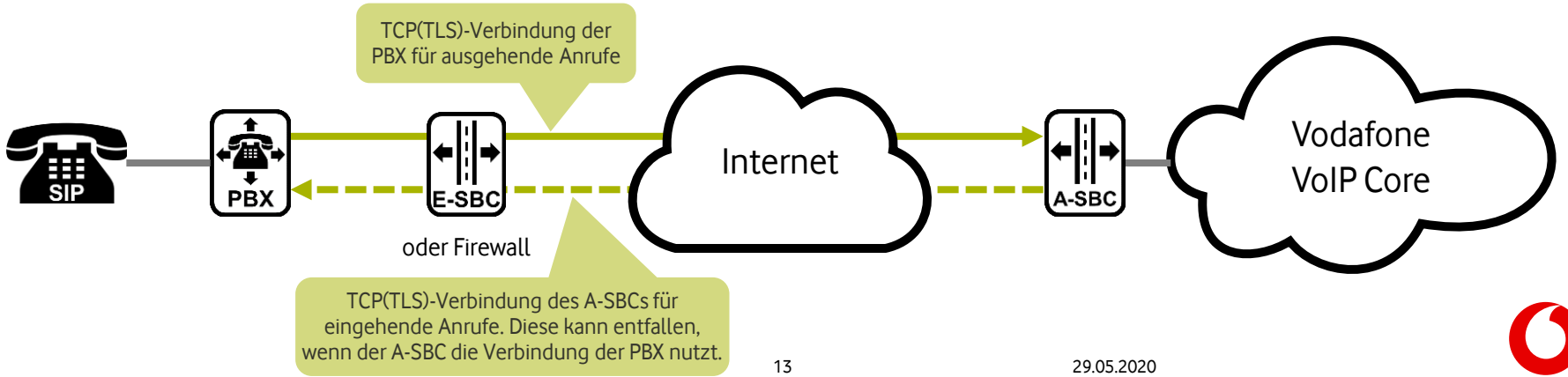


2

Gegenmaßnahmen

Gegenmaßnahmen gegen Angriffe aus dem Internet

- **Access-Listen:** Access-Listen auf Routern, Firewalls, E-SBC und Telefonanlagen, die ausschließlich Verkehre vom Vodafone A-SBC durchlassen, unterbinden die meisten Angriffe aus dem Internet. Sie schützen aber nicht vor UDP-Spoofing-Angriffe, weshalb auf UDP als Transportprotokoll für SIP verzichtet werden sollte. Ebenso wenig können sie TCP-Syn-Flooding abwehren, da auch hierbei die Absender-IP-Adresse gefälscht sein kann.
  Bei TCP baut normalerweise die Telefonanlage eine TCP-Verbindung zum Vodafone A-SBC für abgehende Gespräche und der A-SBC zur Telefonanlage für eingehende Gespräche auf. Der A-SBC kann optional aber auch die TCP-Verbindung der Telefonanlage für eingehende Anrufe nutzen, was als TCP-Connection-Reuse bezeichnet wird. So kann der Zugriff und damit die Bedrohung aus dem Internet auf die Unternehmensinfrastruktur weiter eingeschränkt werden. Das Gleiche gilt für TLS-Verbindung, die ebenfalls TCP als Transportprotokoll nutzen.



Gegenmaßnahmen gegen Angriffe aus dem Internet

- **Firewall-Konfiguration:** Firewalls und NAT-Router unterstützen UDP-Hole-Punching, dass automatisch symmetrische Verkehre eingehend zulässt. So muss keine explizite Freischaltung oder ein Port-Forwarding konfiguriert werden.
- **Enterprise-SBC:** Ein E-SBC ist ausschließlich für VoIP konzipiert und daher einer Firewall bezüglich VoIP-Sicherheit überlegen. Er agiert als *Back-to-Back User Agent (B2BUA).* D. h., er terminiert eine SIP-Verbindung auf der eingehenden Seite und baut eine neue Verbindung auf der ausgehenden Seite auf. Fehlerhafte Pakete oder Inhalte werden verworfen. Der SBC gibt keine IP-Adressen im SIP-Protokoll von ihnen nach Außen (Topology-Hiding). Zudem verfügen SBCs teilweise über Funktionen zur Erkennung und Abwehr von DoS-Angriffen. UDP-Spoofing-Angriffe kann auch ein SBC nicht abwehren. Daher wieder der Hinweis, dass auf UDP als Transportprotokoll verzichtet werden sollte.
  Es besteht auch die Möglichkeit E-SBCs in einer Cloud zu nutzen. Dieses ist aber nur sinnvoll, wenn auch die PBX sich in der Cloud befindet. Andernfalls wäre die Kommunikation zwischen dem SBC und einer lokalen TK-Anlage wieder einem erhöhten Risiko ausgesetzt.
  Vodafone bietet das *Voice Gateway im Modus E-SBC* an, das kundenseitig durch Vodafone installiert und betrieben wird. So kann sichergestellt werden, dass nur eine Kommunikation mit dem Vodafone VoIP-Netz mittels TCP/TLS möglich ist. Und der Kunde braucht kein eigenes E-SBC Know-how.
- **MPLS-VPN (CompanyNet):** Die effektivste Maßnahme gegen Angriffe aus dem Internet ist ein MPLS-VPN, das die VoIP-Infrastruktur eines Unternehmens mit dem Vodafone A-SBC verbindet. Da die meisten VPNs auch einen Übergang zum Internet haben, muss die VoIP-Infrastruktur auch gegen Angriffe über diesen Übergang geschützt werden.

Gegenmaßnahmen gegen Innenangriffe

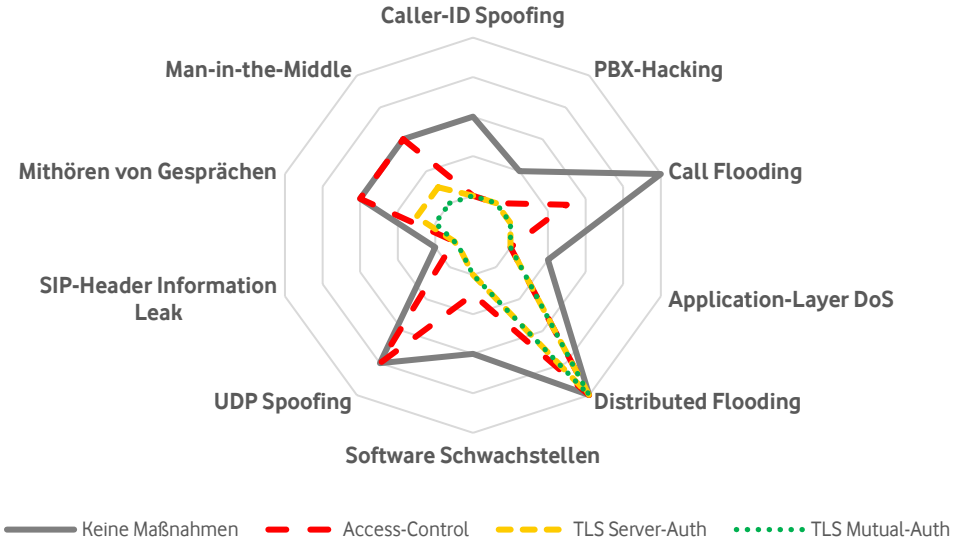
- **Kontrollierter Zugriff auf Netzelemente:** Nur autorisierte Personen dürfen einen administrativen Zugriff auf Netzelemente haben. Idealerweise sollte der Zugriff personalisiert sein und protokolliert werden.
- **Netzwerk-Monitoring:** Man-in-the-Middle Angriffe erfordern ein Umlenken von Datenströmen, um diese auf einem vom Angreifer kontrollierten System zu manipulieren. Verfügt eine Organisation über ein gut ausgebautes Netzwerk-Monitoring, lassen sich solche Angriffe teilweise schon auf Netzwerk-Ebene durch verändertes Routing oder höhere Latenzzeiten erkennen.
- **Verschlüsselung:** Verschlüsselung kann das unerlaubte Mitlesen oder Mithören von Netzwerkverkehr verhindern, bzw. erheblich erschweren. Dabei sollten starke Verschlüsselungsverfahren zum Einsatz kommen, ausreichend starke Schlüsselstärken verwendet und Vorkehrungen gegen Man-in-the-Middle Angriffe getroffen werden. Es ist zu beachten, dass sowohl die Signalisierung als auch der Nutzkanal gesichert werden müssen.
  Für die Signalisierung hat sich *SIP over TLS* als De-facto-Standard etabliert, was nicht mit *SIPS* verwechselt werden sollte. SIPS wurde für eine Ende-zu-Ende-Verschlüsselung konzipiert, die sich derzeit unter Berücksichtigung der gesetzlichen Anforderungen über ein öffentliches Telekommunikationsnetz nicht realisieren lässt.

Gegenmaßnahmen – Gegenüberstellung Internet-Access

Das Spinnennetzdiagramm beschreibt die Wirksamkeit der unterschiedlichen Gegenmaßnahmen bezogen auf die Bedrohungen für einen IP Anlagen-Anschluss über Internet-Access. Die äußere Linie entspricht einem hohen, die innere einem geringen Risiko.

Die dargestellten Maßnahmen bauen aufeinander auf. Durch Access-Controls werden bereits einige Risiken reduziert. Die zusätzliche TLS-Verschlüsselung bringt zusätzlich einen erheblichen Sicherheitsgewinn.

TLS Mutual-Authentication verringert das Risiko gegenüber Server-Authentication nur minimal, da hier in beiden Fällen von einer sehr hohen Komplexität auszugehen ist und der SIP-Trunk nur von einer Domain (einem Kunden) genutzt wird.

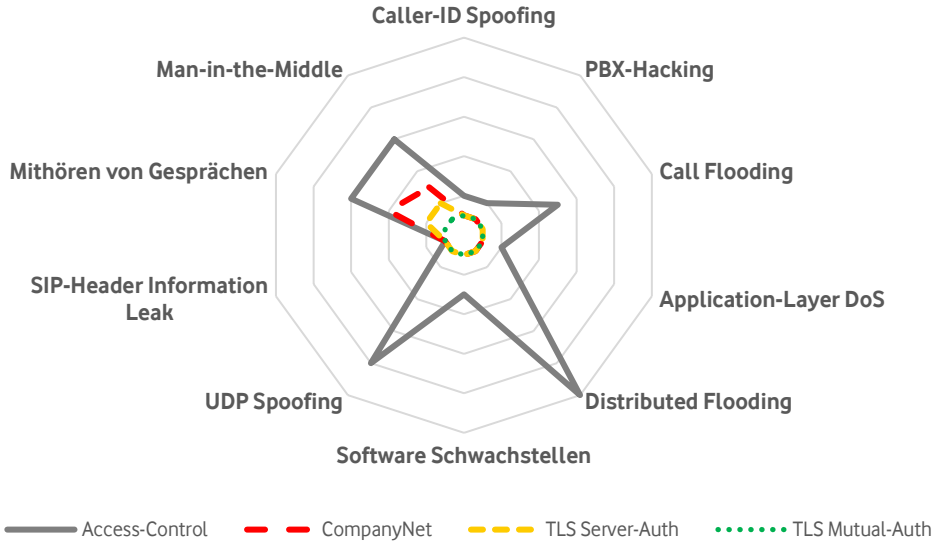


Gegenmaßnahmen – Gegenüberstellung CompanyNet

Durch das CompanyNet reduziert sich das Risiko gegenüber einer Implementierung mit Inter-Access und Access-Controls schon erheblich. Erhöht bleiben die Bedrohungen *Mithören von Gesprächen* und *Man-in-the-Middle,* da hier in erster Linie von einem Innenangriff ausgegangen werden muss.

Gegen diese beiden Bedrohungen ist die Verschlüsselung eine wirksame Gegenmaßnahme.

TLS Mutual-Authentication verringert das Risiko gegenüber Server-Authentication wiederum nur minimal, aus erwähnten Gründen.



SIP-Registrierung – Bedrohungen

Beim Registration-Mode muss sich eine TK-Anlage erst mit einem Benutzernamen und Passwort am Vodafone-Netz registrieren, bevor Telefongespräche möglich sind. Der Registration-Mode hat einige Vorteile. Er funktioniert mit dynamischen IP-Adressen und mehrere TK-Anlagen können die gleiche öffentliche IP-Adresse nutzen, was z. B. bei Cloud-TK-Anlagen häufig der Fall ist.

Die Registrierung selbst stellt aber auch ein Risiko dar, wenn die Registrierungsdaten in die falschen Hände geraten oder ausgespäht werden. Die folgenden Bedrohungen wurden betrachtet:

- **Ungeschützte Registrierungsdaten:** Wenn ein Angreifer zufällig oder über Dritte in den Besitzt der Registrierungsdaten kommt, ist ein Angriff mit einfachen Mitteln möglich.
- **Hash-Cracking:** Ein Angreifer liest die SIP-Registrierung der TK-Anlage mit und versucht aus den übertragenen Hash-Werten das Passwort zu ermitteln.
- **Replay-Angriff:** Ein Angreifer liest die SIP-Registrierung der TK-Anlage mit und versucht sich mit einer Kopie der Registrierungsnachricht am Vodafone-Netz zu registrieren und damit die Registrierung der TK-Anlage zu überschreiben.
- **Man-in-the-Middle-Angriff:** Ein Angreifer bringt sich zwischen TK-Anlage und Vodafone-SBC und manipuliert die Registrierungsnachrichten, um z. B. die Registrierung auf ein niedrigeres Sicherheitsniveau zu drücken.

Das Risiko von Angriffen auf die SIP-Registrierungs-Signalisierung kann im Vergleich zu ungeschützten Registrierungsdaten als gering betrachtet werden.

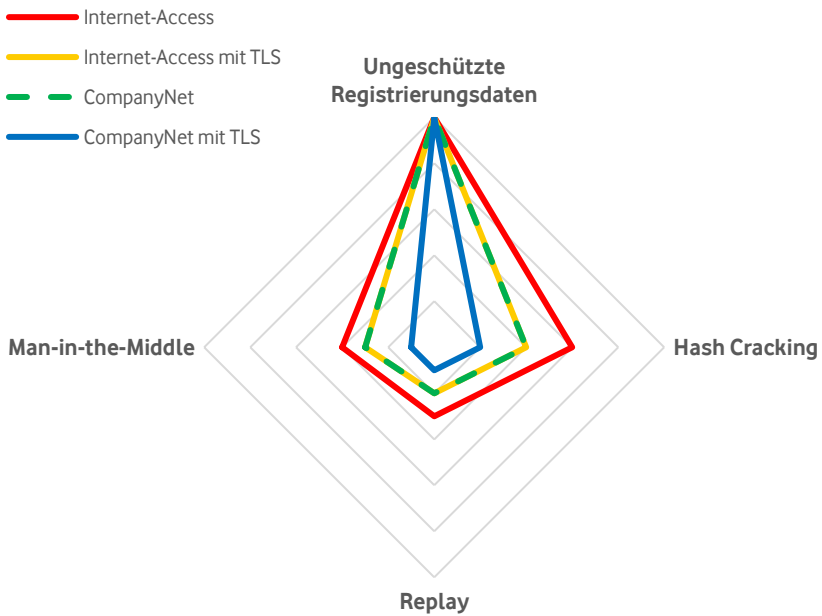
SIP-Registrierung – Gegenmaßnahmen

Die **Registrierungsdaten** müssen sicher aufbewahrt werden. Das Passwort kann nach der Konfiguration auf der TK-Anlage auch gelöscht werden, da es über den Voice Manager selbst zurückgesetzt werden kann. Die Berechtigung ein neues Passwort im Voice Manager zu generieren, darf nur ausgewählten Administratoren vergeben werden. Das Missbrauchsrisiko kann durch ein regelmäßiges Ändern des Passworts reduziert werden. Durch TLS oder CompanyNet kann dieses Risiko nicht reduziert werden.
Beim Einsatz des Vodafone Voice Gateways im Modus E-SBC, werden die Registrierungsdaten mit der Konfiguration automatisch auf den E-SBC übertragen. Das Risiko wird so minimiert.

Für **Hash Cracking** braucht der Angreifer einen Zugriff auf SIP-Registrierungen der TK-Anlage. Dieser Zugriff wird sowohl durch TLS als auch CompanyNet erschwert. Eine Kombination von TLS und CompanyNet bietet somit den größten Schutz.

Gegen **Replay-Angriffe** ist das Vodafone-Netz geschützt, so dass durch TLS und CompanyNet nur die Wahrscheinlichkeit von Angriffsversuchen reduziert werden kann.

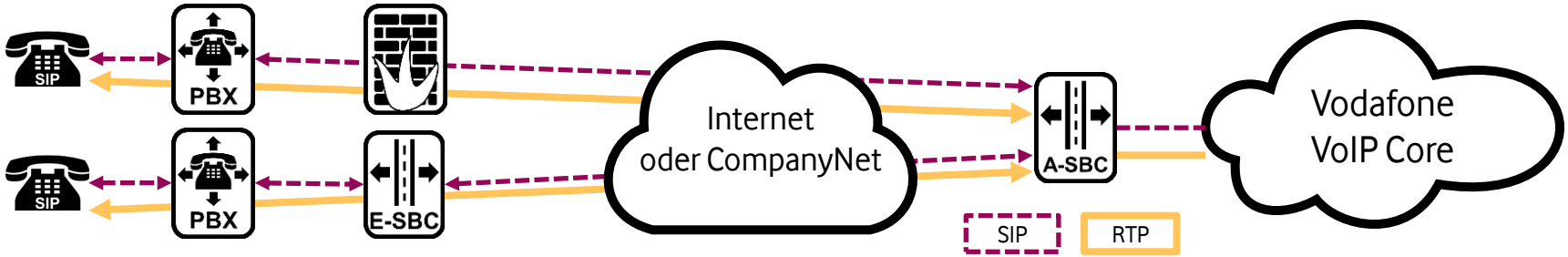
Man-in-the-Middle-Angriffe sind sehr komplex und es ist unwahrscheinlich, dass sie nur auf die SIP-Registrierung ausgerichtet sind. In jedem Fall bringt die Verwendung TLS und CompanyNet einen Sicherheitsgewinn.



4

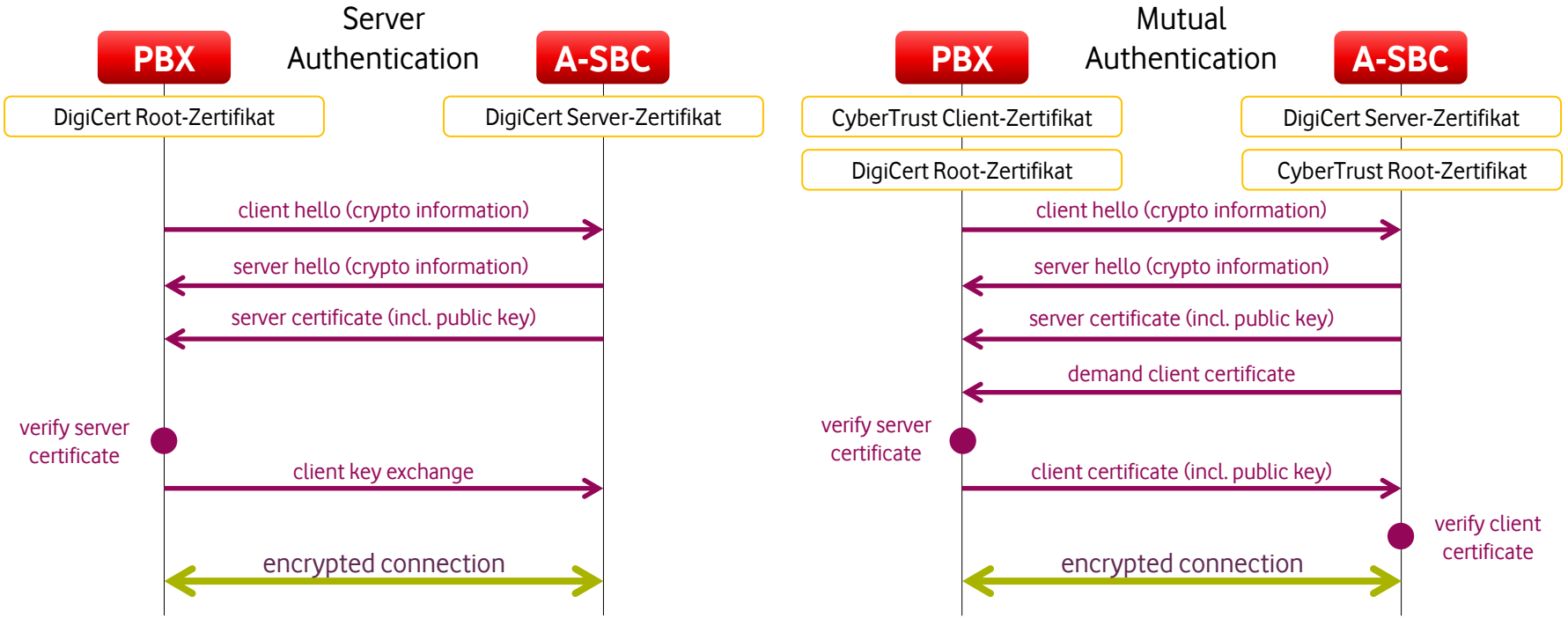
Verschlüsselung

Verschlüsselung – Konzept



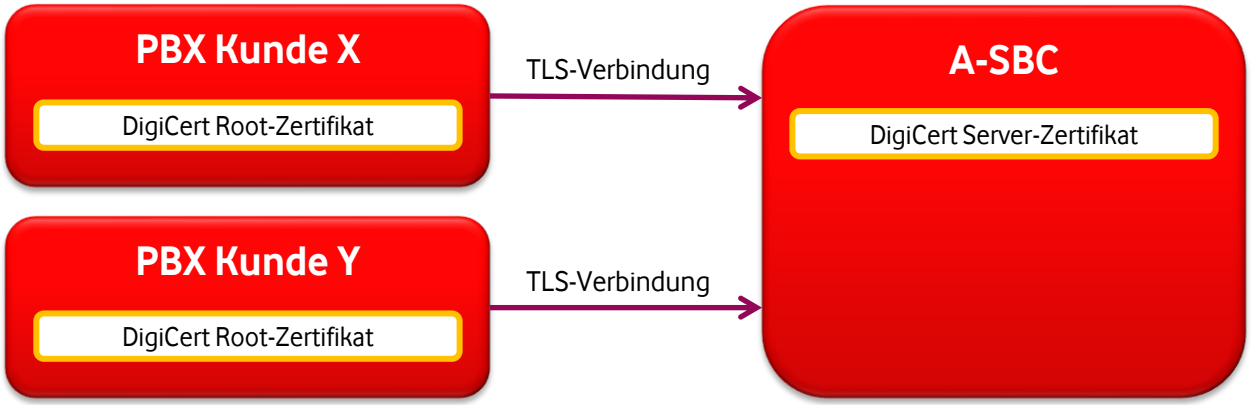
- SIP-TLS-Verschlüsselung erfolgt in Abschnitten zwischen Vodafone SBC, Kunden-SBC/PBX und Telefon
- RTP-Verschlüsselung erfolgt zwischen Vodafone SBC und Telefon. Der RTP-Schlüssel wird in SIP von PBX (und E-SBC) durchgereicht.
- Im Normalfall wird vom Kunden-SBC oder PBX eine TLS-Verbindung zum Vodafone SBC für abgehende Anrufe aufgebaut und umgekehrt vom Vodafone SBC zum Kunden-SBC oder PBX eine TLS-Verbindung für eingehende Anrufe.
- Die TLS-Verbindungen bleiben permanent bestehen, da beide Seiten regelmäßige SIP Options Pings schicken, um die Erreichbarkeit der Gegenseite zu überprüfen. Wird eine Verbindung unterbrochen, so sollte sie direkt wieder aufgebaut werden.
- Alternativ kann auf dem Vodafone SBC *Connection-Reuse* aktiviert werden, sodass er die TLS-Verbindung des Kunden für eingehende Anrufe nutzen kann. In dem Fall braucht der Kunden-SBC oder die Firewall keine Verbindung von außen zuzulassen.

Verschlüsselung – TLS Server- und Mutual-Authentication



Aufbau der TLS-Verbindung von der PBX zum Vodafone A-SBC. Im Normalfall baut der A-SBC ebenso eine TLS-Verbindung zur PBX auf, bei der die Client-/Server-Rollen vertauscht sind. Die PBX benötigt somit in jedem Fall ein Server-Zertifikat, das auch als Client-Zertifikat genutzt werden kann. Nur bei Server-Authentication in Verbindung mit *Connection-reuse* (Nur die PBX baut eine TLS-Verbindung auf, die vom A-SBC mit genutzt wird.) kann auf der PBX auf ein Zertifikat verzichtet werden.

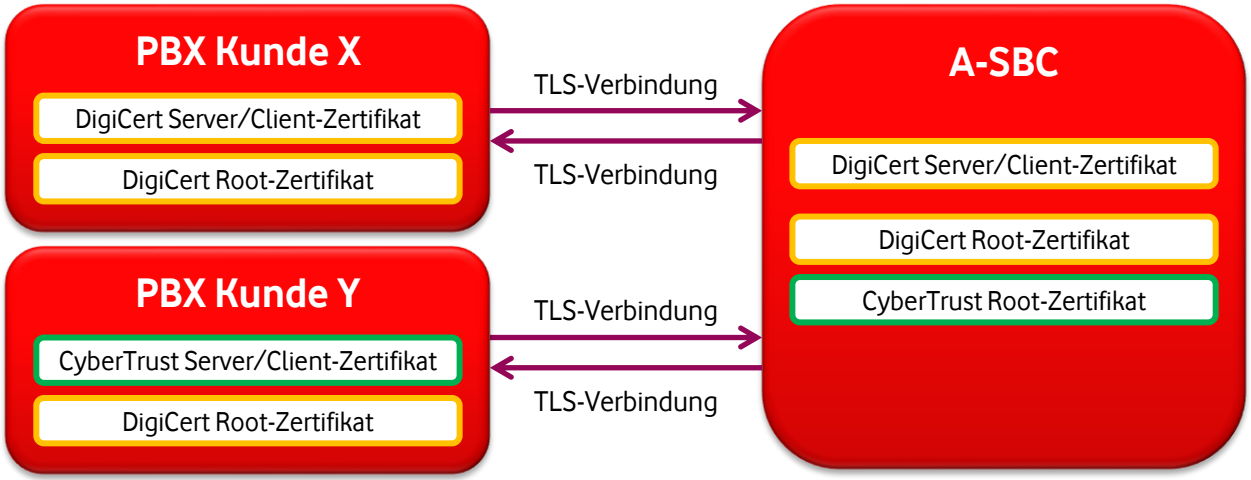
Verschlüsselung – TLS Server–Authentication mit Connection–Reuse



Vodafone lässt seine Server-Zertifikate von der Certificate Authority *DigiCert* ausstellen. Deshalb benötigen TLS-Kunden auf ihrer PBX das zugehörige Root-Zertifikat, dass kostenlos von der *DigiCert*. Homepage heruntergeladen werden kann (https://www.digicert.com/kb/digicert-root-certificates.htm). *DigiCert* bietet Zertifikate mit verschiedenen Sicherheitsstufen für unterschiedliche Anwendungen an, die jeweils andere Root-Zertifikate haben. Daher benötigt der Kunde eine Information, welches Root-Zertifikat er benötigt. Root-Zertifikate haben Laufzeiten von über 10 Jahren, Server-Zertifikate meistens zwei Jahre. Bei der Erneuerung von Server-Zertifikaten braucht das Root-Zertifikat nicht ausgetauscht werden. Die hier angesprochenen Sicherheitsstufen beziehen sich ausschließlich auf den Prozess der Zertifikatsausstellung, nicht auf die Verschlüsselung.

Bei SIP über TCP(TLS) baut der SBC normalerweise für terminierende Anrufe auch eine TCP-(TLS-)Verbindung zur PBX auf. Für den Fall wäre die PBX der TLS-Server und der SBC der Client. Entsprechen bräuchte die PBX ein Server-Zertifikat und der SBC das zugehörige Root-Zertifikat. Mit *Connection-Reuse* wird das vermieden. Der SBC nutzt die TCP-(TLS-)Verbindung der PBX für terminierende Anrufe.

Verschlüsselung – TLS Mutual–Authentication ohne Connection–Reuse



Bei Mutual-Authentication (gegenseitiger Authentifizierung) fordert der TLS-Server beim Verbindungsaufbau auch vom Client ein Zertifikat an, weshalb die PBX für seine TLS-Verbindung zum SBC ein Client-Zertifikat benötigt, das der Kunde bei einer Certificate Authority beantragen und bezahlen sowie vor Ablauf erneuern muss. Der TLS-Server braucht zur Validierung des Client-Zertifikat auch das zugehörige Root-Zertifikat.

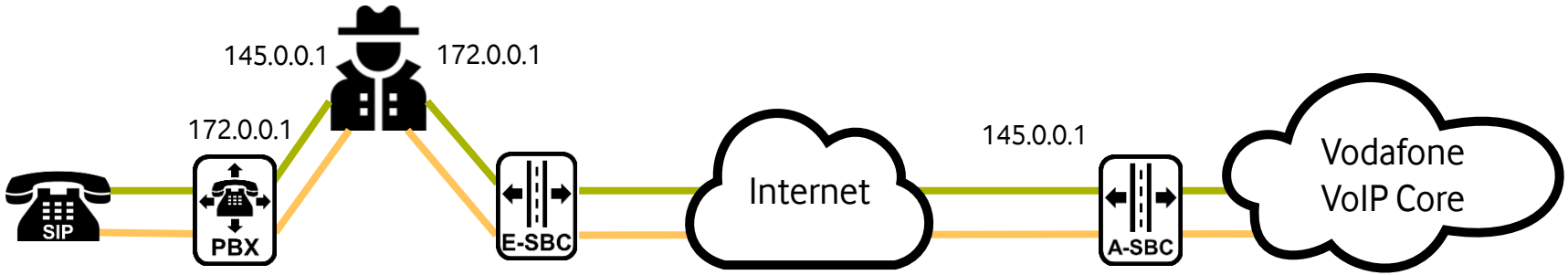
Da Mutual-Authentication im Allgemeinen nicht in Verbindung mit Connection-Reuse genutzt wird, baut der SBC ebenfalls eine TCP-(TLS-)-Verbindung zur PBX auf. Für diese Verbindung ist die PBX der TLS-Server und der SBC der Client. Entsprechend braucht die PBX ein Server-Zertifikat und der SBC ein Client-Zertifikat. Da der SBC und die PBX einmal Server und einmal Client sind, muss bei der Beantragung des Zertifikats bei der Certificate Authority muss ein kombiniertes Server/Client-Zertifikat beantragt werden.

Nutzt der Kunde ein Standard SSL Zertifikat von DigiCert, so ist das erforderliche Root-Zertifikat bereits auf dem SBC vorhanden. Nutzt der Kunde ein Zertifikat einer anderen CA, muss auf dem SBC das entsprechende Root-Zertifikat nachinstalliert werden. Die meisten Kunden werden Zertifikate der größten CAs benutzten, sodass nur selten weitere Root-Zertifikate installiert werden müssen.

Verschlüsselung – TLS Server- und Mutual-Authentication

SIPconnect empfiehlt die Nutzung von Mutual-Authentication. RFC 5923 fordert Mutual-Authentication in Verbindung mit Connection-Reuse. In dem RFC wird diese Forderung mit Multiuser-Systemen auf Client-Seite begründet, auf dem sich ein böswilliger Nutzer befinden kann, der die TLS-Verbindung eines anderen Nutzers missbraucht.

Solche Szenarien sind für den IP Anlagen-Anschluss nicht relevant. Kunden nutzen eigene, dedizierte Systeme, die jeweils nur eine TLS-Verbindung zu Vodafone aufbauen. Zusätzlich akzeptiert Vodafone nur TLS-Verbindungen von festen, definierten Kunden-IP-Adressen. Ein Angreifer müsste somit ein TCP-Spoofing durchführen, was für einem Angriff aus dem Internet ausgeschlossen werden kann. Es bleibt ein Man-in-the-Middle-Angriff eines Innentäters.



Der Angreifer muss es schaffen, dass die IP-Adressen des SIP-Trunks über ihn geroutet werden. Bei Server-Authentication muss er der PBX ein Zertifikat präsentieren, welches der Validierung der PBX standhält. Die PBX kann die Validierung der Zertifikate auf einen oder wenige Aussteller beschränken. Bei Mutual-Authentication muss der Angreifer zusätzlich Vodafone ein Zertifikat präsentieren. Da es sich bei dem Angreifer um einen Innentäter handelt, der es geschafft hat, das Routing im LAN zu manipulieren, liegt es auch im Bereich des Möglichen, dass er ein gültiges Zertifikat für seinen Server hat. Der Sicherheitsgewinn durch Mutual-Authentication ist entsprechend gering.

Verschlüsselung – TLS Empfehlungen

Protokollversionen

- Grundsätzlich werden TLS 1.2 und TLS 1.3 empfohlen.
- Grundsätzlich ist der Einsatz von TLS 1.0 und TLS 1.1 nicht empfohlen, unter anderem da schwache Hashing-Algorithmen zum Einsatz kommen können
- SSL 2.0 und SSL 3.0 sollte unter keinen Umständen eingesetzt werden. Mit RFC 7568 wurden diese Algorithmen abgekündigt.

Zertifikate

- Es sollten nur Zertifikate einer vertrauenswürdigen Certificate Authority (CA) genutzt werden
- Empfangene Zertifikate sollten validiert werden
- Nur genutzte Root-Zertifikate sollten auf einem System installiert sein.

Verschlüsselung – TLS Empfehlungen

Cipher-Suites

Gemäß RFC 7525 *Recommendations for Secure Use of Transport Layer Security,* werden die folgenden Cipher-Suites für TLS 1.2 empfohlen, die auch in der Liste empfohlener Cipher-Suites des BSI enthalten sind:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Vodafone unterstützt alle vier Cipher-Suites. Auf der PBX sollte die Auswahl der Chipher-Suites möglichst eingeschränkt werden. Alle aufgeführten Cipher-Suites nutzen *Perfect Forward Secrecy (PFS)*, sodass ein Angreifer, der in den Besitzt eines Langzeitschlüssels eines Servers kommt, nicht eine vorher mitgeschnittene TLS-Verbindung entschlüsseln kann.

Verschlüsselung – sRTP Empfehlungen

Cipher-Suites

Für die RTP-Verschlüsselung wird ausschließlich die Cipher-Suite AES_CM_128_HMAC_SHA1_80 unterstützt.

Dabei kommt ein 128-bit-Schlüssel und ein 80-bit (Prüfsumme) zum Einsatz. Die Prüfsumme stellt sicher, dass die Nachricht nicht verändert wurde.

Vodafone verzichtet auf eine Unterstützung der Cipher-Suite AES_CM_128_HMAC_SHA1_32, da 32-bit Prüfsummen mittlerweile als unsicher gelten und alle Endgeräte 80 bit unterstützen.


5
Vodafone Voice Gateway
im Modus E-SBC

Vodafone Voice Gateway im Modus E-SBC

Das Vodafone Voice Gateway wird vom *Bundesamt für Sicherheit in der Informationstechnik* zertifiziert und stellt unter anderem die folgenden Sicherheitsfunktionen bereit:

- Im Modus E-SBC arbeitet das Voice Gateway als Back-2-Back User Agent (B2BUA) und terminiert damit VoIP-Verbindungen auf der eingehenden Seite und setzt zur ausgehenden Seite eine neue Verbindung auf. Die Topologie/Endgeräte bzw. ihre IP-Adressen innerhalb der Kundeninfrastruktur werden nicht nach außen weitergegeben (Topology Hiding).
- IP-Pakete von unbekannten Quellen werden ignoriert.
- Andere Protokolle als SIP und RTP/RTCP kann der E-SBC nicht verarbeiten bzw. durchlassen.
- Die Syntax der SIP-Signalisierung wird überprüft. Anrufe mit fehlerhafter Syntax werden abgelehnt.
- Bei RTP-Paketen wird der Absender, Adressat und Inhalt auf Basis der SDP-Informationen überprüft, bevor sie weitergeleitet werden.
- DoS- und DDoS-Angriffe werden unterbunden.
- Die Verbindungen zwischen E-SBC und dem Vodafone-Netz sind mit TLS bzw. sRTP verschlüsselt.

Zusätzlich übernimmt der E-SBC die Failover-Funktion für den Fall, dass ein Vodafone A-SBC nicht erreichbar ist.

Gegenüberstellung: E-SBC – Internet-Access – CompanyNet

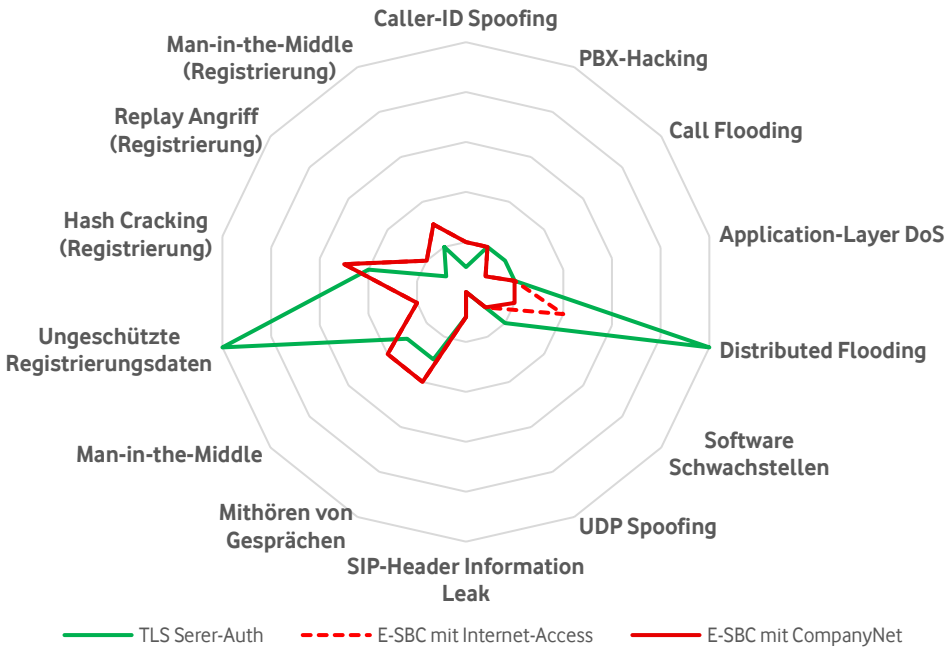
Das Spinnennetzdiagramm beschreibt die Wirksamkeit des E-SBCs im Vergleich zur direkten Registrierung einer TK-Anlage. In der Mitte des Diagramms ist das geringste, am Rand das größte Risiko.

Der E-SBC ist durch seine speziellen Sicherheitsfunktionen bezüglich einiger Bedrohungen vielen TK-Anlagen überlegen, z. B. Distributed Flooding.

Einen erheblichen Vorteil bietet der E-SBC beim Schutz der Registrierungsdaten, da diese automatische auf dem E-SBC konfiguriert werden und gar nicht an den Kunden übermittelt werden müssen.

Der E-SBC hat gegenüber einer Verschlüsselung bis zur TK-Anlage den Nachteil, dass die Verbindung zwischen E-SBC und TK-Anlage unverschlüsselt ist. Wenn dieser Abschnitt im Kunden-LAN innerhalb eines geschützten Raums liegt, kann der Unterschied vernachlässigt werden.

CompanyNet bietet gegenüber dem Internet-Access nur noch einen geringfügigen Sicherheitsgewinn bezüglich Distributed Flooding, da der E-SBC gar nicht aus dem Internet erreichbar ist.




Danke
vodafone
business