



## NET.2: Funknetze

# NET.2.1: WLAN-Betrieb

## 1 Beschreibung

### 1.1 Einleitung

Über Wireless LANs (WLANs) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Hersteller-Konsortium „Wi-Fi Alliance“ ein, das basierend auf dem Standard IEEE 802.11 mit „Wi-Fi“ einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

Innerhalb von Institutionen können WLANs eingesetzt werden, um flexibel mit mobilen Geräten zu arbeiten und diesen den Zugang zum Netz der Institution zu ermöglichen. Hierfür werden innerhalb der Institution Netzzugänge über so genannten Access Points aufgebaut. Aufgrund der meist einfachen und schnellen Installation werden WLANs auch dazu eingesetzt, um temporär Netze einzurichten, beispielsweise auf Messen oder kleineren Veranstaltungen. Darüber hinaus können an öffentlichen Plätzen, wie Flughäfen oder Bahnhöfen, Netzzugänge über so genannte Hotspots angeboten werden. Dadurch werden den mobilen Benutzern Verbindungen in das Internet oder ihr Institutionsnetz ermöglicht. Die Kommunikation findet dann generell zwischen einem zentralen Zugangspunkt, dem Access Point, und der WLAN-Komponente des Endgeräts statt.

### 1.2 Zielsetzung

In diesem Baustein wird systematisch aufgezeigt, wie WLANs sicher in einer Institution aufgebaut und betrieben werden können.

### 1.3 Abgrenzung und Modellierung

Der Baustein NET.2.1 *WLAN-Betrieb* ist auf alle Kommunikationsnetze anzuwenden, die gemäß der Standard-Reihe IEEE 802.11 und deren Erweiterungen aufgebaut und betrieben werden.

Der Baustein enthält grundsätzliche Anforderungen, die beachtet und erfüllt werden müssen, wenn WLANs in Institutionen aufgebaut und betrieben werden. Anforderungen für eine sichere Nutzung von WLANs sind jedoch nicht Gegenstand dieses Bausteins. Die sichere Nutzung von WLANs wird im Baustein NET.2.2 *WLAN-Nutzung* behandelt.

WLANs können entsprechend den Bedürfnissen eines Betreibers und der Hardware-Ausstattung, die zur Verfügung steht, in zwei verschiedenen Modi betrieben werden. Im Ad-hoc-Modus kommunizieren zwei oder mehr WLAN-Clients direkt miteinander. WLANs im Ad-hoc-Modus können sich selbstständig, also ohne feste Infrastruktur, aufbauen und konfigurieren. Somit können sie eine

vollvermaschte parallele Netz-Infrastruktur etablieren. Dadurch ist der Ad-hoc-Modus in einer zu schützenden Umgebung ungeeignet und wird deshalb im Folgenden nicht weiter betrachtet. In den meisten Fällen werden WLANs im Infrastruktur-Modus betrieben, d. h. die Kommunikation der WLAN-Clients und die Verbindung in kabelgebundene LAN-Segmente erfolgt über Access Points.

Werden für die Authentisierung am WLAN entsprechende Dienste (z. B. RADIUS) eingesetzt, so müssen die entsprechenden IT-Systeme, auf denen die Dienste betrieben werden, gesondert abgesichert werden. Hierfür können die Bausteine der Schicht SYS.1, wie zum Beispiel SYS.1.1 *Allgemeiner Server*, herangezogen werden.

Wird ein WLAN betrieben, sollte dieses grundsätzlich mit berücksichtigt werden, wenn die Bausteine NET.1.1 *Netzarchitektur und -design*, NET.1.2 *Netzmanagement* und DER.2.1 *Behandlung von Sicherheitsvorfällen* umgesetzt werden.

## 2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein NET.2.1 *WLAN-Betrieb* von besonderer Bedeutung.

### 2.1 Ausfall oder Störung eines Funknetzes

In Funknetzen werden Informationen mittels elektromagnetischer Funkwellen übertragen. Strahlen andere elektromagnetische Quellen im selben Frequenzspektrum Energie ab, können diese die drahtlose Kommunikation stören und im Extremfall den Betrieb des WLANs verhindern. Dies kann durch andere Funksysteme und Geräte, wie beispielsweise Bluetooth, Mikrowellenherde oder andere WLAN-Netze hervorgerufen werden. Darüber hinaus sind auch Denial-of-Service-Angriffe möglich. Werden beispielsweise bestimmte Steuer- und Managementsignale wiederholt gesendet, kann dies dazu führen, dass das Funknetz nicht mehr verfügbar ist.

### 2.2 Fehlende oder unzureichende Planung des WLAN-Einsatzes

Fehler in der Planung stellen sich oft als besonders schwerwiegend heraus, weil dadurch leicht flächendeckende Sicherheitslücken geschaffen werden können. Wird der Einsatz von WLANs nicht oder nur unzureichend geplant, kann sich eine Vielzahl von Problemen ergeben, beispielsweise:

- Vertrauliche Daten könnten mitgelesen werden, etwa wenn WLAN-Standards eingesetzt werden, die nicht mehr dem Stand der Technik entsprechen (z. B. WEP zur Verschlüsselung).
- Die Übertragungskapazität könnte unzureichend sein. Dadurch können bandbreitenintensive Anwendungen nicht mit der erforderlichen Dienstgüte genutzt werden.
- Die Abdeckung des WLANs könnte nicht ausreichend sein, sodass an bestimmten Orten kein Netz verfügbar ist.

### 2.3 Fehlende oder unzureichende Regelungen zum WLAN-Einsatz

Bei einer WLAN-Infrastruktur, die nicht zentral administriert wird, sind die Access Points in der Standard-Einstellung meist ohne oder nur mit unzureichenden Sicherheitsmechanismen vorkonfiguriert. Schließt ein Mitarbeiter beispielsweise aufgrund fehlender Regelungen einen ungenehmigten bzw. ungesicherten Access Point an ein internes Netz der Institution an, kann dies zu schwerwiegenden Problemen führen. Denn er untergräbt damit praktisch sämtliche innerhalb des LANs ergriffenen Sicherheitsmaßnahmen, wie z. B. die Firewall zum Schutz gegen unberechtigte externe Zugriffe.

### 2.4 Ungeeignete Auswahl von Authentisierungsverfahren

Wenn Authentisierungsverfahren und -mechanismen fehlen oder unzureichend sind, können Sicherheitslücken entstehen. Beispielsweise wird im Standard IEEE 802.1X (Port Based Network Access

Control) das Extensible Authentication Protocol (EAP) definiert. In einigen der beschriebenen EAP-Methoden sind aber Schwachstellen enthalten. So ist EAP-MD5 etwa anfällig gegenüber Man-in-the-Middle- und Wörterbuchangriffen. Wird EAP-MD5 eingesetzt, können Passwörter erraten werden. Außerdem kann die Kommunikation abgehört werden.

## **2.5 Fehlerhafte Konfiguration der WLAN-Infrastruktur**

Access Points und andere WLAN-Komponenten (z. B. WLAN Controller) bieten eine Vielzahl von Konfigurationseinstellungen, die insbesondere auch Sicherheitsfunktionen betreffen. Werden diese falsch konfiguriert, ist entweder keine Kommunikation über einen Access Point möglich oder die Kommunikation erfolgt ungeschützt bzw. mit einem zu geringen Schutzniveau.

## **2.6 Unzureichende oder fehlende WLAN-Sicherheitsmechanismen**

Im Auslieferungszustand sind WLAN-Komponenten häufig so konfiguriert, dass keine oder nur wenige Sicherheitsmechanismen aktiviert sind. Einige der Mechanismen sind darüber hinaus unzureichend und bieten somit keinen ausreichenden Schutz. Auch heute werden noch diverse WLAN-Komponenten eingesetzt, die lediglich unzureichende Sicherheitsmechanismen wie z. B. WEP unterstützen. Teilweise können diese Geräte nicht einmal auf stärkere Sicherheitsmechanismen aufgerüstet werden. Werden solche Geräte eingesetzt, kann ein Angreifer leicht die gesamte Kommunikation abhören und damit vertrauliche Informationen einsehen.

## **2.7 Abhören der WLAN-Kommunikation**

Da es sich bei Funk um ein Medium handelt, das sich mehrere Benutzer teilen können („Shared Medium“), können die über WLANs übertragenen Daten problemlos mitgehört und aufgezeichnet werden. Wenn die Daten nicht oder nur unzureichend verschlüsselt werden, können die übertragenen Nutzdaten leicht eingesehen werden. Zudem überschreiten Funknetze bzw. die ausgesendeten Funkwellen häufig die Grenzen der selbst genutzten Räumlichkeiten. So werden Daten auch noch in Bereiche ausgestrahlt, die nicht von den Benutzern oder einer Institution kontrolliert und gesichert werden können.

## **2.8 Vortäuschung eines gültigen Access Points (Rogue Access Point)**

Ein Angreifer kann sich als Teil der WLAN-Infrastruktur ausgeben, indem er einen eigenen Access Point mit einem geeignet gewählten Namen (SSID) in der Nähe eines WLAN-Clients installiert. Dieser vorgetäuschte Access Point wird als „Rogue Access Point“ bezeichnet. Bietet dieser dem WLAN-Client eine stärkere Sendeleistung als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls diese sich nicht gegenseitig authentisieren. Zusätzlich könnte auch der echte Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzer melden sich an einem Netz an, das nur vorgibt, das Ziernetz zu sein. Dadurch ist es einem Angreifer möglich, die Kommunikation abzuhören. Auch durch Poisoning- oder Spoofing-Methoden kann ein Angreifer eine falsche Identität vortäuschen bzw. den Netzverkehr zu seinen IT-Systemen umlenken. So kann er die Kommunikation belauschen und kontrollieren. Besonders in öffentlichen Funknetzen (sogenannten Hotspots) ist ein Rogue Access Point ein beliebtes Angriffsmittel.

## **2.9 Ungeschützter LAN-Zugang am Access Point**

Sind Access Points sichtbar und ohne physischen Schutz montiert, kann sich ein Angreifer zwischen die Access Points und die Switch-Infrastruktur schalten, um den gesamten Netzverkehr abzuhören. Selbst wenn die drahtlose Kommunikation mit WPA2 verschlüsselt wird, stellt dies eine Gefährdung dar, weil diese Methoden nur die Luftschnittstelle absichern, die Ethernet-Anbindung aber nicht weiter berücksichtigen.

## **2.10 Hardware-Schäden**

Hardware-Schäden können dazu führen, dass der Funkverkehr gestört wird. Im schlimmsten Fall kann

das WLAN sogar komplett ausfallen. Dies betrifft insbesondere WLAN-Geräte, die außerhalb von geschützten Räumen angebracht werden, z. B. um offene Plätze abzudecken. Sie sind zusätzlichen Gefährdungen ausgesetzt, wie beispielsweise vorsätzlichen Beschädigungen durch Angreifer oder umweltbedingten Schäden durch Witterung oder Blitzeinschlag.

### 2.11 Diebstahl eines Access Points

Werden WLAN Access Points ungesichert in öffentlichen Bereichen installiert, können sie gestohlen werden. Dadurch lässt sich beispielsweise ein Shared-Secret Key für die Authentisierung am RADIUS-Server oder der verwendete Schlüssel (beispielsweise für WPA2-Personal) auslesen. Mit diesen Informationen kann dann unberechtigt auf das WLAN zugegriffen werden.

## 3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.2.1 *WLAN-Betrieb* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planer, Haustechnik

### 3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein NET.2.1 *WLAN-Betrieb* vorrangig erfüllt werden:

#### NET.2.1.A1 Festlegung einer Strategie für den Einsatz von WLANs (B)

Bevor in einer Institution WLANs eingesetzt werden, MUSS festgelegt sein, welche generelle Strategie die Institution im Hinblick auf die Kommunikation über WLANs plant. Insbesondere MUSS geklärt und festgelegt werden, in welchen Organisationseinheiten, für welche Anwendungen und zu welchem Zweck WLANs eingesetzt und welche Informationen darüber übertragen werden dürfen. Ebenso MUSS der Abdeckungsbereich des WLAN festgelegt werden.

Außerdem MUSS schon in der Planungsphase festgelegt sein, wer für die Administration der unterschiedlichen WLAN-Komponenten zuständig ist, welche Schnittstellen es zwischen den am Betrieb beteiligten Verantwortlichen gibt und wann welche Informationen zwischen den Zuständigen ausgetauscht werden müssen.

#### NET.2.1.A2 Auswahl eines geeigneten WLAN-Standards [Planer] (B)

Im Rahmen der WLAN-Planung MUSS zuerst ermittelt werden, welche der von der Institution betriebenen Geräte (z. B. Mikrowellengeräte, Bluetooth-Geräte) in das ISM-Band bei 2,4 GHz sowie in das 5 GHz-Band abstrahlen.

Außerdem MÜSSEN die vorhandenen Sicherheitsmechanismen der einzelnen WLAN-Standards gegeneinander abgewogen werden. Generell MUSS sichergestellt sein, dass nur als allgemein sicher anerkannte Verfahren zur Authentisierung und Verschlüsselung eingesetzt werden. Die Entscheidungsgründe MÜSSEN dokumentiert werden.

Geräte, die von anerkannt sicheren Verfahren auf unsichere zurückgreifen müssen, DÜRFEN NICHT

mehr eingesetzt werden.

#### **NET.2.1.A3      Auswahl geeigneter Kryptoverfahren für WLAN [Planer] (B)**

Die Kommunikation über die Luftschnittstelle MUSS komplett kryptografisch abgesichert werden. Kryptografische Verfahren, die unsicherer als WPA2 sind, DÜRFEN NICHT mehr eingesetzt werden.

Wird WPA2 mit Pre-Shared Keys (WPA2-PSK) verwendet, dann MUSS ein komplexer Schlüssel mit einer Mindestlänge von 20 Zeichen verwendet werden.

#### **NET.2.1.A4      Geeignete Aufstellung von Access Points [Haustechnik] (B)**

Access Points MÜSSEN zugriffs- und diebstahlsicher montiert werden. Wenn sie aufgestellt werden, MÜSSEN die erforderlichen Bereiche ausreichend abgedeckt werden. Darüber hinaus MUSS darauf geachtet werden, dass sich die Funkwellen in Bereichen, die nicht durch das WLAN versorgt werden sollen, möglichst nicht ausbreiten. Außeninstallationen MÜSSEN vor Witterungseinflüssen und elektrischen Entladungen geeignet geschützt werden.

#### **NET.2.1.A5      Sichere Basis-Konfiguration der Access Points (B)**

Access Points DÜRFEN NICHT in der Konfiguration des Auslieferungszustandes verwendet werden. Voreingestellte SSIDs (Service Set Identifiers), Zugangskennwörter oder kryptografische Schlüssel MÜSSEN vor dem produktiven Einsatz geändert werden. Außerdem MÜSSEN unsichere Administrationszugänge abgeschaltet werden. Access Points DÜRFEN NUR über eine geeignet verschlüsselte Verbindung administriert werden.

#### **NET.2.1.A6      Sichere Konfiguration der WLAN-Infrastruktur (B)**

Es MUSS sichergestellt sein, dass mittels der WLAN-Kommunikation keine Sicherheitszonen gekoppelt werden und hierdurch etablierte Schutzmaßnahmen umgangen werden.

#### **NET.2.1.A7      Aufbau eines Distribution Systems [Planer] (B)**

Bevor ein kabelgebundenes Distribution System aufgebaut wird, MUSS prinzipiell entschieden werden, ob physisch oder logisch durch VLANs auf den Access Switches des kabelbasierten LANs getrennt wird.

#### **NET.2.1.A8      Verhaltensregeln bei WLAN-Sicherheitsvorfällen (B)**

Bei einem Sicherheitsvorfall MUSS der IT-Betrieb passende Gegenmaßnahmen einleiten:

- Am Übergabepunkt der WLAN-Kommunikation ins interne LAN SOLLTE bei einem Angriff auf das WLAN die Kommunikation selektiv pro SSID, Access Point oder sogar für die komplette WLAN-Infrastruktur gesperrt werden.
- Wurden Access Points gestohlen, MÜSSEN festgelegte Sicherheitsmaßnahmen umgesetzt werden, damit der Access Point oder hierauf abgespeicherte Informationen nicht missbraucht werden können.
- Wurden WLAN-Clients entwendet und wird eine zertifikatsbasierte Authentisierung verwendet, MÜSSEN die Client-Zertifikate gesperrt werden.

Es MUSS ausgeschlossen werden, dass entwendete Geräte unberechtigt verwendet werden, um auf das Netz der Institution zuzugreifen.

### **3.2    Standard-Anforderungen**

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein NET.2.1 WLAN-Betrieb. Sie SOLLTEN grundsätzlich erfüllt werden.

#### **NET.2.1.A9      Sichere Anbindung von WLANs an ein LAN [Planer] (S)**

Werden WLANs an ein LAN angebunden, SOLLTE der Übergang zwischen WLANs und LAN abgesichert werden, beispielsweise durch einen Paketfilter. Der Access Point SOLLTE unter Berücksichtigung der Anforderung NET.2.1.A7 *Aufbau eines Distribution Systems* eingebunden sein.

**NET.2.1.A10 Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs (S)**

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die wesentlichen Kernaspekte für einen sicheren Einsatz von WLANs konkretisiert werden. Die Richtlinie SOLLTE allen Verantwortlichen bekannt sein, die an Aufbau und Betrieb von WLANs beteiligt sind. Sie SOLLTE zudem Grundlage für ihre Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Werden die Inhalte der Richtlinie nicht umgesetzt, MUSS geeignet reagiert werden. Die Ergebnisse SOLLTEN geeignet dokumentiert werden.

**NET.2.1.A11 Geeignete Auswahl von WLAN-Komponenten (S)**

Anhand der Ergebnisse der Planungsphase SOLLTE eine Anforderungsliste erstellt werden, mithilfe derer die am Markt erhältlichen Produkte bewertet werden können. Werden WLAN-Komponenten beschafft, SOLLTE neben Sicherheit auch auf Datenschutz und Kompatibilität der WLAN-Komponenten untereinander geachtet werden.

**NET.2.1.A12 Einsatz einer geeigneten WLAN-Management-Lösung (S)**

Eine zentrale Managementlösung SOLLTE eingesetzt werden. Der Leistungsumfang der eingesetzten Lösung SOLLTE im Einklang mit den Anforderungen der WLAN-Strategie sein.

**NET.2.1.A13 Regelmäßige Sicherheitschecks in WLANs (S)**

WLANs SOLLTEN regelmäßig daraufhin überprüft werden, ob eventuell Sicherheitslücken existieren. Zusätzlich SOLLTE regelmäßig nach unbefugt installierten Access Points innerhalb der bereitgestellten WLANs gesucht werden. Weiterhin SOLLTEN die Performance und Abdeckung gemessen werden. Die Ergebnisse von Sicherheitschecks SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTEN untersucht werden.

**NET.2.1.A14 Regelmäßige Audits der WLAN-Komponenten (S)**

Bei allen Komponenten der WLAN-Infrastruktur SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt sind. Außerdem SOLLTE überprüft werden ob alle Komponenten korrekt konfiguriert sind. Öffentlich aufgestellte Access Points SOLLTEN regelmäßig stichprobenartig daraufhin geprüft werden, ob es gewaltsame Öffnungs- oder Manipulationsversuche gab. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTEN untersucht werden.

### **3.3 Anforderungen bei erhöhtem Schutzbedarf**

Im Folgenden sind für den Baustein NET.2.1 *WLAN-Betrieb* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

**NET.2.1.A15 Verwendung eines VPN zur Absicherung von WLANs (H)**

Es SOLLTE ein VPN eingesetzt werden, um die Kommunikation über die WLAN-Infrastruktur zusätzlich abzusichern.

**NET.2.1.A16 Zusätzliche Absicherung bei der Anbindung von WLANs an ein LAN (H)**

Wird eine WLAN-Infrastruktur an ein LAN angebunden, SOLLTE der Übergang zwischen WLANs und LAN entsprechend des höheren Schutzbedarfs zusätzlich abgesichert werden.

**NET.2.1.A17 Absicherung der Kommunikation zwischen Access Points (H)**

Die Kommunikation zwischen den Access Points über die Funkschnittstelle und das LAN SOLLTE verschlüsselt erfolgen.

**NET.2.1.A18 Einsatz von Wireless Intrusion Detection/Wireless Intrusion Prevention Systemen (H)**

Es SOLLTEN Wireless Intrusion Detection Systeme bzw. Wireless Intrusion Prevention Systeme eingesetzt werden.

## 4 Weiterführende Informationen

### 4.1 Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:

- BSI-Standard zur Internet-Sicherheit (ISi-Reihe): Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Das National Institute of Standards and Technology (NIST) hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:

- NIST Special Publication 800-153 „Guidelines for Securing Wireless Local Area Network (WLANs)“
- NIST Special Publication 800-97 „Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11“

## 5 Anlage: Kreuzreferenztablelle zu elementaren Gefährdungen

Die Kreuzreferenztablelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein NET.2.1 *WLAN-Betrieb* von Bedeutung.

G 0.9	Ausfall oder Störung von Kommunikationsnetzen
G 0.15	Abhören
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.23	Unbefugtes Eindringen in IT-Systeme
G 0.24	Zerstörung von Geräten oder Datenträgern
G 0.25	Ausfall von Geräten oder Systemen
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.40	Verhinderung von Diensten (Denial of Service)
G 0.43	Einspielen von Nachrichten
G 0.44	Unbefugtes Eindringen in Räumlichkeiten