|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "WLAN-Betrieb"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300037 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc81123251)

[Dokumentenhistorie 3](#_Toc81123252)

[Inhaltsverzeichnis 4](#_Toc81123253)

[Allgemeine Festlegungen 5](#_Toc81123254)

[Ziel / Zweck 5](#_Toc81123255)

[Geltungsbereich 5](#_Toc81123256)

[Zuständigkeiten 5](#_Toc81123257)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81123258)

[Aufbau des Dokuments 6](#_Toc81123259)

[Sicherheitsrichtlinie „WLAN-Betrieb" 7](#_Toc81123260)

[Basismaßnahmen 7](#_Toc81123261)

[Festlegung einer Strategie für den Einsatz von WLANs (NET.2.1.A1) 7](#_Toc81123262)

[Auswahl eines geeigneten WLAN-Standards (NET.2.1.A2) 7](#_Toc81123263)

[Auswahl geeigneter Kryptoverfahren für WLAN (NET.2.1.A3) 7](#_Toc81123264)

[Geeignete Aufstellung von Access Points (NET.2.1.A4) 7](#_Toc81123265)

[Sichere Basis-Konfiguration der Access Points (NET.2.1.A5) 7](#_Toc81123266)

[Sichere Konfiguration der WLAN-Clients (NET.2.1.A6) 8](#_Toc81123267)

[Aufbau eines Distribution Systems (NET.2.1.A7) 8](#_Toc81123268)

[Verhaltensregeln bei WLAN-Sicherheitsvorfällen (NET.2.1.A8) 8](#_Toc81123269)

[Standardmaßnahmen 9](#_Toc81123270)

[Sichere Anbindung von WLANs an ein LAN (NET.2.1.A9) 9](#_Toc81123271)

[Geeignete Auswahl von WLAN-Komponenten (NET.2.1.A11) 9](#_Toc81123272)

[Einsatz einer geeigneten WLAN-Management-Lösung (NET.2.1.A12) 9](#_Toc81123273)

[Regelmäßige Sicherheitschecks in WLANs (NET.2.1.A13) 9](#_Toc81123274)

[Regelmäßige Audits der WLAN-Komponenten (NET.2.1.A14) 9](#_Toc81123275)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc81123276)

[Verwendung eines VPN zur Absicherung von WLANs (NET.2.1.A15 - CI) 10](#_Toc81123277)

[Zusätzliche Absicherung bei der Anbindung von WLANs an ein LAN (NET.2.1.A16 - CIA) 10](#_Toc81123278)

[Absicherung der Kommunikation zwischen Access Points (NET.2.1.A17 - C) 10](#_Toc81123279)

[Einsatz von Wireless Intrusion Detection / Wireless Intrusion Prevention Systemen (NET.2.1.A18 - CIA) 10](#_Toc81123280)

# Allgemeine Festlegungen

## Ziel / Zweck

Über Wireless LANs (WiFi) 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.

Aufgrund der meist einfachen und schnellen Installation werden WLANs auch dazu eingesetzt, um temporär Netze einzurichten. 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 zum Netz der <Institution> ermöglicht. Die Kommunikation findet dann generell zwischen einem zentralen Zugangspunkt, dem Access Point, und der WiFi-Komponente des Endgeräts statt.

In dieser Sicherheitsrichtlinie wird systematisch aufgezeigt, wie WiFi-Netze sicher aufgebaut und betrieben werden können. Für die Erstellung der Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines NET.2.1 "WLAN-Betrieb" zurückgegriffen. Vorgaben für die Nutzung der bereitgestellten WiFi-Netze, werden hingegen in der Sicherheitsrichtlinie WLAN-Nutzung aufgezeigt.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „WLAN-Betrieb“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „WLAN-Betrieb"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

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

Es wurde eine Strategie für den Einsatz von WLAN entwickelt. Darin wird festgelegt, in welchen Organisationseinheiten, für welche Anwendungen und zu welchem Zweck WLAN eingesetzt und welche Informationen hierüber übertragen werden dürfen. Zusätzlich wurden die Verantwortlichen definiert. So ist geregelt, 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. Außerdem wurden die räumlichen Bereiche zum Aufbau von WLANs konzipiert.

### Auswahl eines geeigneten WLAN-Standards (NET.2.1.A2)

Innerhalb der WLAN-Planung wurde überprüft, welche der von der <Institution>betriebenen Systeme in das ISM-Band bei 2,4 GHz sowie in das 5 GHz-Band abstrahlen. Die vorhandenen Sicherheitsmechanismen der einzelnen WLAN-Standards wurden miteinander verglichen und ausführlich bewertet. Somit wird sichergestellt, dass nur als allgemein sicher anerkannte Verfahren zur Authentisierung und Verschlüsselung eingesetzt werden. Die Entscheidungsgründe wurden dokumentiert. Geräte, die von anerkannt sicheren Verfahren auf unsichere zurückgreifen müssen, werden nicht berücksichtigt.

### Auswahl geeigneter Kryptoverfahren für WLAN (NET.2.1.A3)

Die Kommunikation mittels WLAN wird komplett kryptographisch abgesichert. Es werden keine kryptographischen Verfahren, die unsicherer als WPA2 sind verwendet. Sollte WPA2 mit statischen Pre-Shared Keys (WPA2-PSK) verwendet werden, ist ein komplexer Schlüssel mit einer Mindestlänge von 20 Zeichen zu verwenden. Der WPA Pre-Shared Key ist regelmäßig zu wechseln.

### Geeignete Aufstellung von Access Points (NET.2.1.A4)

Alle Access Points wurden zugriffssicher montiert. Die Ausbreitung der Funkwellen innerhalb der Bereiche, die nicht durch das WLAN versorgt werden sollen, sind auf ein Minimum zu reduzieren. Außeninstallationen sind vor Witterungseinflüssen und elektrischen Entladungen ausreichend zu schützen.

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

Access Points werden sicher installiert und konfiguriert. Voreingestellte SSIDs (Service Set Identifiers), Zugangskennwörter oder kryptographische Schlüssel sind geändert worden. Access Points werden verschlüsselt administriert. Alle unsicheren Administrationszugänge sind abzuschalten.

### Sichere Konfiguration der WLAN-Clients (NET.2.1.A6)

Alle mit dem WLAN gekoppelten Clients werden sicher konfiguriert. Zusätzlich werden die über einen längeren Zeitraum nicht genutzte WLAN-Schnittstellen deaktiviert. Es wird sichergestellt, dass mittels der WLAN-Kommunikation keine Sicherheitszonen gekoppelt werden.

### Aufbau eines Distribution Systems (NET.2.1.A7)

Wird ein Distribution System aufgebaut, ist prinzipiell zu entschieden, ob physisch oder logisch durch VLANs auf den Access Switches des kabelbasierten LANs getrennt wird. Hierbei sind auch die Anforderungen aus der Sicherheitsrichtlinie Netzarchitektur und -design sowie Netzmanagement zu beachten.

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

Bei der Behandlung von Sicherheitsvorfällen sind Verantwortlichkeiten und Ansprechpartner festzulegen. Alle Mitarbeiter sind über ihre Aufgaben und Kompetenzen zu unterrichten. Es ist zu regeln, wer die mögliche Entscheidung für eine Untersuchung trifft, nach welchen Kriterien diese vorgenommen wird und wann sie erfolgen soll. Um einen Sicherheitsvorfall erfolgreich zu beheben, sollte der folgende Prozessablauf eingehalten werden.

* Eingrenzung des Problems,
* Finden der Ursache,
* Auswahl erforderlicher Maßnahmen zur Behebung,
* Einholen einer Freigabe zur Umsetzung,
* Beseitigen der Ursache und
* Herstellung eines sicheren Zustandes.

Es ist eine aktuelle Liste von internen und externen Sicherheitsexperten zu führen, die bei Sicherheitsvorfällen für Fragen hinzugezogen werden können. Bei einem WLAN zentrierten Sicherheitsvorfall sind durch die Betriebsverantwortlichen passende Gegenmaßnahmen einzuleiten.

* Im Falle eines Angriffs ist die Kommunikation selektiv pro SSID, Access Point oder die komplette Infrastruktur zu sperren.
* Wurden Access Points gestohlen, sind Sicherheitsmaßnahmen einzuleiten, um den Missbrauch zu verhindern.
* Sind WLAN-Clients entwendet worden und wird eine zertifikatsbasierte Authentisierung verwendet, sind die Client-Zertifikate zu sperren.
* Alle möglichen Konsequenzen von Sicherheitsvorfällen sind zu untersuchen. Der unberechtigte Zugriff entwendeter Geräte auf das Netz der <Institution> ist zu verhindern.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Sichere Anbindung von WLANs an ein LAN (NET.2.1.A9)

Der Übergang zwischen WLAN und LAN innerhalb der <Institution> ist abgesichert. Die Access Points werden unter Berücksichtigung des Kapitels „Aufbau eines Distribution Systems“ eingebunden.

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

Für eine geeignete Auswahl von WLAN-Komponenten wurde eine Anforderungsliste erstellt. Anhand dieser Liste sind die auf dem Markt erhältlichen Produkte zu bewerten. Werden die WLAN-Komponenten beschafft, ist neben der Sicherheit auch auf Datenschutz und Kompatibilität zu den anderen WLAN-Komponenten zu achten.

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

Es wird eine zentrale WLAN-Management-Lösung eingesetzt. Der Leistungsumfang der eingesetzten Managementlösung erfolgt im Einklang mit den Anforderungen der WLAN-Strategie.

### Regelmäßige Sicherheitschecks in WLANs (NET.2.1.A13)

Es werden regelmäßige Sicherheitschecks durchgeführt. Dabei wird unter anderem überprüft:

* ob potenzielle Sicherheitslücken existieren,
* ob unbefugt Access Points installiert werden können,
* ob die Performance den Erwartungen entspricht.

Die Ergebnisse dieser Sicherheitschecks werden dokumentiert und mit dem Soll-Zustand abgeglichen. Sollten Abweichungen vorkommen, wird diesen nachgegangen.

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

Es finden regelmäßige Audits der WLAN-Komponenten statt. Dabei wird überprüft, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und korrekt konfiguriert sind. Öffentlich aufgestellte Access Points werden ebenfalls regelmäßig stichprobenartig auf gewaltsame Öffnungs- und Manipulationsversuche überprüft. Die Auditergebnisse werden dokumentiert und mit dem Soll-Zustand abgeglichen. Sollten Abweichungen vorkommen, wird diesen nachgegangen.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Verwendung eines VPN zur Absicherung von WLANs (NET.2.1.A15 - CI)

Um die Kommunikation zusätzlich abzusichern, sollte bei erhöhtem Schutzbedarf ein VPN eingesetzt werden.

### Zusätzliche Absicherung bei der Anbindung von WLANs an ein LAN (NET.2.1.A16 - CIA)

Wird eine WLAN-Infrastruktur an ein LAN angebunden, ist der Übergang zwischen WLAN-Infrastruktur und LAN entsprechend des höheren Schutzbedarfs zusätzlich abzusichern.

### Absicherung der Kommunikation zwischen Access Points (NET.2.1.A17 - C)

Um die Vertraulichkeit bei der Datenübermittlung zu gewährleisten, wird die Kommunikation zwischen den Access Points über die Funkschnittstelle und das LAN verschlüsselt.

### Einsatz von Wireless Intrusion Detection / Wireless Intrusion Prevention Systemen (NET.2.1.A18 - CIA)

Um Sicherheitsvorfälle und Schwachstellen zeitnah zu entdecken und entsprechende Gegenmaßnahmen direkt einleiten zu können, sind Wireless Intrusion Detection Systeme bzw. Wireless Intrusion Prevention Systeme einzusetzen.