NET.2: Funknetze

NET.2.2: WLAN-Nutzung

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.

WLANs bieten einen Gewinn an Komfort und Mobilität. Jedoch birgt die Nutzung auch zusätzliches Gefährdungspotenzial für die Sicherheit der Informationen, da drahtlos kommuniziert wird. Daher ist es wichtig, dass neben dem IT-Betrieb auch die Benutzer für die möglichen Gefahren sensibilisiert werden, die entstehen können, wenn WLANs unsachgemäß verwendet werden. So müssen die Benutzer über die erforderlichen Kenntnisse verfügen, um Sicherheitsmaßnahmen richtig verstehen und anwenden zu können. Insbesondere müssen sie wissen, was von ihnen in Hinblick auf Informationssicherheit erwartet wird und wie sie in bestimmten Situationen reagieren sollten, wenn sie WLANs nutzen.

1.2 Zielsetzung

In diesem Baustein soll aufgezeigt werden, wie WLANs sicher genutzt werden können.

1.3 Abgrenzung und Modellierung

Der Baustein NET.2.2 *WLAN-Nutzung* ist auf alle IT-Systeme (WLAN-Clients) anzuwenden, die WLANs nutzen.

Der Baustein enthält grundsätzliche Anforderungen, die bei der Nutzung von WLANs zu beachten und zu erfüllen sind, um den spezifischen Gefährdungen entgegenwirken zu können. Anforderungen, mit deren Hilfe WLANs sicher betrieben werden können, sind dagegen nicht Gegenstand dieses Bausteins, sondern sind im Baustein NET.2.1 *WLAN-Betrieb* beschrieben. Darüber hinaus geht der Baustein nicht auf allgemeine Aspekte von Clients ein. Solche Aspekte werden im Baustein SYS2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt. Der Baustein NET.2.2 *WLAN-Nutzung* sollte grundsätzlich mit berücksichtigt werden, wenn die Bausteine ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und DER.2.1 *Behandlung von Sicherheitsvorfällen* umgesetzt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein NET.2.2 *WLAN-Nutzung* von besonderer Bedeutung.

2.1 Unzureichende Kenntnis über Regelungen

Kennen die Benutzer die Regelungen für den korrekten Umgang mit WLANs nicht oder nicht gut genug, können sie sich auch nicht daran halten. Werden Clients zum Beispiel gedankenlos mit fremden drahtlosen Netzen verbunden, können darüber unverschlüsselt übertragenen Informationen abgehört werden. Außerdem können durch den Betreiber des drahtlosen Netzes Informationen über den Benutzer, wie zum Beispiel besuchte Webseiten, gesammelt werden.

2.2 Nichtbeachtung von Sicherheitsmaßnahmen

Durch Nachlässigkeit und fehlende Kontrollen kommt es immer wieder vor, dass Personen die ihnen empfohlenen oder angeordneten Sicherheitsmaßnahmen nicht oder nur teilweise umsetzen. Wird beispielsweise ein WLAN-Client im Ad-hoc-Modus genutzt, obwohl dies in der Benutzerrichtlinie ausdrücklich verboten ist, kann ein anderer Client direkt mit dem WLAN-Client kommunizieren. So kann er z. B. unberechtigt auf vertrauliche Dokumente zugreifen, die eventuell auf dem Client freigegeben sind.

2.3 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. Werden die Daten nicht oder nur unzureichend verschlüsselt, können die übertragenen Nutzdaten leicht mitgelesen werden. Zudem überschreiten Funknetze bzw. die ausgesendeten Funkwellen nicht selten die Grenzen der genutzten Räumlichkeiten. So werden Daten auch noch in Bereiche ausgestrahlt, die nicht von den Benutzern oder der Institution kontrolliert und gesichert werden können.

2.4 Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation

Bei WLANs auf Basis von IEEE 802.11 wird die MAC-Adresse einer WLAN-Karte bei jeder Datenübertragung mit versendet. Da sie unverschlüsselt übertragen wird, können Bewegungsprofile über mobile Nutzer erstellt werden, z. B. wenn diese sich in öffentliche Hotspots einbuchen.

2.5 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 WLAN-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 Zielnetz 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.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.2.2 *WLAN-Nutzung* aufgeführt. Grundsätzlich ist der Benutzer 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	Benutzer
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein NET.2.2 *WLAN-Nutzung* vorrangig erfüllt werden:

NET.2.2.A1 Erstellung einer Benutzerrichtlinie für WLAN [IT-Betrieb] (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MÜSSEN die wesentlichen Kernaspekte für eine sichere WLAN-Nutzung in einer WLAN-Benutzerrichtlinie konkretisiert werden. In einer solchen Benutzerrichtlinie MÜSSEN die Besonderheiten bei der WLAN-Nutzung beschrieben sein, z. B. ob, wie und mit welchen Geräten Hotspots genutzt werden dürfen.

Die Richtlinie MUSS Angaben dazu enthalten, welche Daten im WLAN genutzt und übertragen werden dürfen und welche nicht.

Es MUSS beschrieben sein, wie mit clientseitigen Sicherheitslösungen umzugehen ist. Die Benutzerrichtlinie MUSS ein klares Verbot enthalten, ungenehmigte Access Points an das Netz der Institution anzuschließen. Außerdem MUSS in der Richtlinie darauf hingewiesen werden, dass die WLAN-Schnittstelle deaktiviert werden muss, wenn sie über einen längeren Zeitraum nicht genutzt wird.

Es MUSS regelmäßig überprüft werden, ob die in der Richtlinie geforderten Inhalte richtig umgesetzt werden. Ist dies nicht der Fall, MUSS geeignet reagiert werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

NET.2.2.A2 Sensibilisierung und Schulung der WLAN-Benutzer [Vorgesetzte, IT-Betrieb] (B)

Die Benutzer von WLAN-Komponenten, vornehmlich von WLAN-Clients, MÜSSEN sensibilisiert und zu den in der Benutzerrichtlinie aufgeführten Maßnahmen geschult werden. Hierfür MÜSSEN geeignete Schulungsinhalte identifiziert und festgelegt werden. Den Benutzern MUSS genau erläutert werden, was die WLAN-spezifischen Sicherheitseinstellungen bedeuten und warum sie wichtig sind. Außerdem MÜSSEN die Benutzer auf die Gefahren hingewiesen werden, die drohen, wenn diese Sicherheitseinstellungen umgangen oder deaktiviert werden.

Die Schulungsinhalte MÜSSEN immer entsprechend den jeweiligen Einsatzszenarien angepasst werden. Neben der reinen Schulung zu WLAN-Sicherheitsmechanismen MÜSSEN den Benutzern jedoch auch die WLAN-Sicherheitsrichtlinie ihrer Institution und die darin enthaltenen Maßnahmen vorgestellt werden. Ebenso MÜSSEN die Benutzer für die möglichen Gefahren sensibilisiert werden, die von fremden WLANs ausgehen.

NET.2.2.A3 Absicherung der WLAN-Nutzung an Hotspots [IT-Betrieb] (B)

Dürfen Hotspots genutzt werden, MUSS Folgendes umgesetzt werden:

- Jeder Benutzer eines Hotspots MUSS seine Sicherheitsanforderungen kennen und danach entscheiden, ob und unter welchen Bedingungen ihm die Nutzung des Hotspots erlaubt ist.

- Werden Hotspots genutzt, dann SOLLTE sichergestellt werden, dass die Verbindung zwischen Hotspot-Access Point und IT-System des Benutzers nach dem Stand der Technik kryptografisch abgesichert wird.
- WLANs, die nur sporadisch genutzt werden, SOLLTEN von den Benutzern aus der Historie gelöscht werden.
- Die automatische Anmeldung an WLANs SOLLTE deaktiviert werden.
- Wenn möglich, SOLLTEN separate Benutzerkonten mit einer sicheren Grundkonfiguration und restriktiven Berechtigungen verwendet werden.
- Es SOLLTE sichergestellt sein, dass sich kein Benutzer mit administrativen Berechtigungen von seinem Client aus an externen WLANs anmelden kann.
- Sensible Daten DÜRFEN NUR übertragen werden, wenn allen notwendigen Sicherheitsmaßnahmen auf den Clients, vor allem eine geeignete Verschlüsselung, aktiviert sind.
- Wird die WLAN-Schnittstelle über einen längeren Zeitraum nicht genutzt, MUSS diese deaktiviert werden.
- Über öffentlich zugängliche WLANs DÜRFEN die Benutzer NUR über ein Virtual Private Network (VPN) auf interne Ressourcen der Institution zugreifen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein NET.2.2 *WLAN-Nutzung*. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.2.2.A4 Verhaltensregeln bei WLAN-Sicherheitsvorfällen (S)

Bei WLAN-Sicherheitsvorfällen SOLLTEN die Benutzer Folgendes umsetzen:

- Die Benutzer SOLLTEN ihre Arbeitsergebnisse sichern.
- Sie SOLLTEN den WLAN-Zugriff beenden und die WLAN-Schnittstelle ihres Clients deaktivieren.
- Fehlermeldungen und Abweichungen SOLLTEN durch die Benutzer genau dokumentiert werden. Ebenso SOLLTEN die Benutzer dokumentieren, was sie gemacht haben, bevor bzw. während der Sicherheitsvorfall eingetreten ist.
- Die Benutzer SOLLTEN über eine geeignete Eskalationsstufe (z. B. User Help Desk) den IT-Betrieb benachrichtigen.Wird die WLAN-Schnittstelle über einen längeren Zeitraum nicht genutzt, MUSS diese deaktiviert werden.
- Über öffentlich zugängliche WLANs DÜRFEN die Benutzer NUR über ein Virtual Private Network (VPN) auf interne Ressourcen der Institution zugreifen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Für den Baustein NET.2.2 *WLAN-Nutzung* sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

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: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle 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.2.2 *WLAN-Nutzung* von Bedeutung.

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.43 Einspielen von Nachrichten