WLAN-Checkliste	Konvention
	wlan-checklist 1.0.0
	Empfehlung

Kurzbeschreibung	Diese Checkliste erweitert das Dokument „Beachtens- und Wissenswertes zu WLANs in der Verwaltung" [WLAN03] um Weiterentwicklungen und Marktveränderungen im Umfeld WLAN. Vielmehr wird hier eine Kategorisierung von WLANs vorgeschlagen und es wird eine Unterstützung bei der Installation von Funknetzen in der Verwaltung in Form einer Checkliste geboten. Während [WLAN03] darauf abzielt, IT-Managern und Interessierten einen Überblick über die Funktionsweise und infrastrukturellen Rahmenbedingungen von WLANs zu verschaffen, soll sich diese Checkliste mit den vorgeschlagenen Konfigurationsempfehlungen für kategorisierte WLANs neben den WLAN-Entscheidungsträgern auch an WLAN-Verantwortliche in der Verwaltung richten. Die Empfehlungen zielen im Speziellen darauf ab, die bestmögliche Sicherheit in der jeweiligen Situation zu liefern und gleichzeitig ein Bewusstsein über verbleibende Restrisiken zu schaffen.

Autor(en)	Bernd Martin	Projektteam / Arbeitsgruppe
		Sicherheit

Stelle	Vorgelegt am	Angenommen am
IKT-Board	29.06.2004	29.06.2004
Länder	29.06.2004	18.08.2004
Gemeindebund	29.06.2004	18.08.2004
Städtebund	29.06.2004	18.08.2004

WLAN-Checkliste

Inhaltsverzeichnis

(1) Allgemeines

Im Zuge dieser Checkliste werden Behörden dabei unterstützt zum einen ihre WLAN-Netzwerke zu kategorisieren und zum anderen die damit verbundenen Sicherheitsrisiken anhand vorgeschlagener Abwehrmaßnahmen zu minimieren und die verbleibenden Restrisiken besser einschätzen zu können. Die hier angeführten Punkte stellen Empfehlungen dar und repräsentieren organisatorische und technische Minimalanforderungen zur Erhöhung der Sicherheit von WLANs. Während eine Unterschreitung der Sicherheitsanforderungen nicht erfolgen soll, steht den Verantwortlichen eine Implementierung von höheren Sicherheitsanforderungen frei. Dieser Checkliste liegen im Speziellen die folgenden Dokumente und Standards zugrunde:

- "802.11a: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Highspeed Physical Layer in the 5 GHz Band" [802.11]
- "802.11b: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band" [802.11]
- "802.11g: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher Rate Extensions in the 2,4 GHz Band" [802.11]
- "802.11i: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Method (MAC) Security Enhancements" (noch nicht ratifiziert)
- "Wi-Fi Protected Access", das eine Untermenge von 802.11i darstellt [WPA]
- "802.1X IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control" [802.1X] und
- das Grundlagenpapier „Beachtens- und Wissenswertes zu WLANs in der Verwaltung" [WLAN03]

Das Ziel ist es sicherheitsrelevante Aspekte auf organisatorischer und technischer Ebene abzudecken. Dazu wird ein WLAN-Projekt in drei Phasen unterteilt:

- Phase I: Zieldefinition, Analyse und Designphase
- Phase II: Implementierungs- und Testphase
- Phase III: Wartungsphase

(2) Phase I: Zieldefinition, Analyse- und Design

In diesem Abschnitt sind jene Punkte angeführt, die am Beginn jedes WLAN-Projekts berücksichtigt werden müssen. Für die Analyse- und Designphase wird empfohlen die Anweisungen des Teil 2 des [SiHB], Kapitel 4 zu befolgen.

Zu Beginn muss die Absicht einer neuen WLAN-Installation mit einer zugehörigen Zieldefinition festgelegt werden. Darin sollen die Notwendigkeit, eine Begründung für die WLAN-Installation aber auch eine Abgrenzung des Projekts enthalten sein.

Bevor es in weiterer Folge zu einer WLAN-Installation kommt, muss eine Sicherheitsanalyse gemacht werden. Dabei soll und muss der Sicherheitsverantwortliche der Organisation eingebunden werden. Das Ergebnis dieser Analyse soll sein, Risiken herauszufinden und eine Bewertung derselben durchzuführen. Darauf aufbauend kann entschieden werden, ob das Projekt auch wirklich umgesetzt wird. Sind die (Rest-) Risiken zu groß bzw. können die Sicherheitsanforderungen nicht erfüllt werden, muss von einer Umsetzung abgeraten werden.

(2.1) Zieldefinition

Vor der Sicherheitsanalyse bedarf es der Definition einer Zielsetzung für das WLAN. Mit der folgenden Grobeinteilung wurden jene vier Varianten angeführt, zwischen denen in der Verwaltung unterschieden werden muss:

a) **Infrastruktur-Netzwerk zum Zugang zum Internet ausschließlich für Besucher:** Häufig wird es vorkommen, dass in Besprechungsräumen und Aufenthaltsbereichen ein ‚offenes' WLAN implementiert werden soll. Externe (und selbstverständlich auch interne) Benutzer sollen die Möglichkeit haben, das Internet nutzen zu können, ohne gleichzeitig Zugriff auf die interne Infrastruktur zu haben und ohne große Konfigurationshindernisse bewältigen zu müssen. Ein solcher Zugang kann auch von einem externen Anbieter zur Verfügung gestellt werden. Die Vorteile wären u. a., dass Installation, Konfiguration, der Betrieb, die Wartung, usw. nicht selbst gemacht werden müssen und die Verantwortung an Experten übertragen werden kann, ein Nachteil hingegen die anfallenden Kosten und das Faktum, dass der Provider meist physisch im Gebäude Installationen vornehmen muss.

b) **Infrastruktur-Netzwerk zum Zugang zum Inter- und Intranet ausschließlich für interne Mitarbeiter:** Ein solches WLAN dient der Mobilitätsförderung der eigenen Mitarbeiter. Zugriff wird dabei unter Erfüllung diverser Sicherheitsanforderungen sowohl ins Internet als auch auf interne Ressourcen (z.B. Fileserver, Drucker, etc.) gewährt. Ein solcher Zugang muss in die interne Infrastruktur integriert werden und ist somit nur von bzw. unter Einbeziehung des Betreibers des bestehenden Netzwerkes realisierbar. Die Anforderungen dafür sind Integrität, Authentifizierung und Vertraulichkeit.

c) **Infrastruktur-Netzwerk zum Zugang zum Internet für Besucher und Inter- und Intranet für interne Mitarbeiter:** Diese Art des WLANs stellt eine Kombination von a) und b) dar. Es muss dabei sichergestellt sein, dass Externe bzw. Besucher unter keinen Umständen unautorisiert und unberechtigt auf Intranetservices und zu vertraulichen Informationen gelangen bzw. diese verändern können. Demzufolge muss es eine klare Trennung zwischen diesen Benutzergruppen geben.

d) **Ad-hoc Netzwerk zwischen zwei oder mehreren Benutzern:** Diese Art kann für einen schnellen Datenaustausch über die Luftschnittstelle nach dem Standard 802.11b/g implementiert werden. Die Installation eines solchen Netzwerks kann nur dann unterbunden werden, wenn die Mitarbeiter keine Installationsrechte für unerlaubte HW-Komponenten bzw. keine Konfigurationsrechte für erlaubtes WLAN-Zubehör haben. Es ist unbedingt darauf zu achten, dass ein bestehendes abgesichertes Netzwerk nicht durch etwaige WLAN-Komponenten (z.B. in der Funktion einer Bridge) unsicher gemacht wird.

(2.2) Sicherheitsanalyse und Infrastruktur

Es muss eine Klassifizierung jener Daten erfolgen, die über das WLAN übertragen werden sollen. Gibt es bereits eine bestehende Einteilung von Informationen in Sicherheitsklassen, so sind diese auch beim WLAN heranzuziehen. Die Sicherheitsanforderungen hängen klarerweise sehr stark mit der zuvor definierten Zielsetzung zusammen.

Die Einteilung für eine allgemein anwendbare Lösung sieht folgendermaßen aus:

a) **Niedrige Sicherheitsanforderungen:** Es wird davon ausgegangen, dass keine sensiblen Informationen übertragen werden bzw. wenn, dann nur mit den gleichen Sicherheitsvorkehrungen, wie sie auch über das Internet genutzt werden. Der Zugriff auf Ressourcen ist somit äquivalent zu einem Zugang zum Internet von einem

öffentlichen Internetprovider. Der Zugang zum WLAN ist grundsätzlich ohne Authentifizierung möglich.

b) **Mittlere Sicherheitsanforderungen:** Dabei ist der Airlink abgesichert, d.h. für die Funkstrecke vom Client bis hin zum AP (Access Point) sind Authentizität, Integrität und bei Bedarf Vertraulichkeit sichergestellt. Zu beachten ist, dass der Zugang zum WLAN nur authentifizierten Benutzern erlaubt ist.

c) **Hohe Sicherheitsanforderungen:** Dabei soll der gesamte Datentransfer geschützt werden. Es besteht die Möglichkeit auf sensible Ressourcen zuzugreifen, wobei eine adäquate Zugriffsbeschränkung, Authentifizierung und Transportsicherheit, vielmehr eine zwischen Server und Client Ende-zu-Ende Sicherheit vorliegt.

In der Sicherheitsanalyse macht es sich bezahlt, dass auch bestehende Infrastrukturgegebenheiten und vorhandene -komponenten mit analysiert und festgehalten werden. Diese können für die eine spätere Entscheidungsfindung und Umsetzung von Bedeutung sein. Dazu zählen u.a. folgende Beobachtungen:

- Welche baulichen Einschränkungen gibt es bei der Positionierung der APs? Besteht die Möglichkeit die APs ‚unsichtbar' und schwer zugänglich zu montieren?
- Analyse bestehender HW-Komponenten: Gibt es HW-Komponenten, die den Einsatz von Virtuellen LANs (VLANs) zulassen? Sind noch Hubs in Verwendung? Gibt es bereits power-inline fähige Switches? etc.
- Analyse bestehender SW-/HW-Komponenten: Gibt es Firewall- und/oder Intrusion Detection Systeme (IDS) für Server (und Client)? Existiert bereits ein virtuelles privates Netzwerk (VPN) bzw. besteht die Möglichkeit der Verwendung eines solchen?
- Gibt es bereits eine implementierte PKI bzw. eine andere Form von etablierten Authentifizierungsmechanismen (z.B. ID-Token, RADIUS-Server, Kerberos, etc.)?

Diese Liste erhebt mit Sicherheit keinen Anspruch auf Vollständigkeit, soll aber den Verantwortlichen eine Einstiegshilfe bieten und aufzeigen, welche Informationen bei der späteren Umsetzung von Bedeutung sind.

Dauer

Es wird davon abgeraten, die Dauer einer Installation als Kriterium für etwaige Sicherheitsanforderungen zu akzeptieren. Eine kürzere Installationsdauer eines WLAN darf sich nicht auf die Sicherheitsanforderungen auswirken.

Es gibt in Bezug auf die Dauer lediglich die Unterscheidung zwischen Test- und Produktionsumgebung. Die Testumgebung wird im Vergleich zur Produktionsumgebung deutlich kürzer, d. h. eine sehr kurze zeitlich vorbestimmte Zeit, in Betrieb sein. So können in einer Testinstallation (und Testumgebung!) mehrere unterschiedliche Mechanismen in einem eigens zum Testen vorgesehenen Netzwerk auf Funktionalität und Sicherheitsanforderungen getestet werden. Für die Implementierung einer Produktionsumgebung ist dies aber irrelevant.

(2.3) Designentscheidungen

Darunter fallen Entscheidungen und Tätigkeiten, die bei der Planung eines WLAN-Netzwerks gefällt bzw. gemacht werden müssen.

(2.3.1) Erstellen eines Lageplans

Ein Lageplan beschreibt bestmöglich die baulichen Gegebenheiten, um in weiterer Folge Netzabdeckung, Kanäle usw. planen und dokumentieren zu können. So beinhaltet dies die physikalische Erfassung mit ergänzenden und detaillierten Beschreibungen über diverse

Eigenschaften des Gebäudes. Weiters ermöglicht eine Miterfassung des unmittelbaren *Grenzgebiets* (in Bezug auf die zukünftig geplante WLAN-Verfügbarkeit), die Dokumentation der (eigenen und evtl. Fremdanbietern) Funkwellenausbreitung außerhalb der vorgesehenen Zone und damit verbundene mögliche Risiken bzw. Interferenzen mit fremden WLAN-Installationen.

(2.3.2) Konfiguration der verwendeten Kanäle

Diese Einstellung an den APs zählt deswegen zu diesem Maßnahmenkatalog, weil damit u. a. ungewollte DoS Attacken abgewendet werden können. Kommen mehr APs zum Einsatz bzw. werden solche von externen Unternehmen betrieben und senden zwei oder mehr auf der gleichen Frequenz bzw. überschneiden sich die Funkwolken, dann treten Interferenzen auf und die APs stören sich gegenseitig[1]. Aus diesem Grund müssen die Kanäle bestmöglich verteilt werden (drei parallele Kanäle sind im 802.11b Frequenzband möglich, acht bei 802.11a).

Die geplanten zu verwendenden Kanäle sollen bei der Planung im Lageplan eingetragen werden. Im Lageplan ist demzufolge auch die Existenz von angrenzenden WLAN-Installationen zu berücksichtigen (vgl. auch (2.3.1)).

(2.3.3) Erstellen einer WLAN-Policy

Gibt es bereits eine Policy für Remote-Access Benutzer könnte diese mit den WLAN-Anforderungen ergänzt werden. Existiert keine solche Policy, soll eine eigene erstellt und veröffentlicht werden.

Zu den Inhalten für die Policy zählen zumindest folgende Punkte:

- Definition des WLAN-Benutzerkreises und den Bedingungen, welche erfüllt sein müssen, damit diese Personen das WLAN nutzen dürfen
- Definition des WLAN-Umfanges (Internet und/oder Intranet) inkl. einer Klassifizierung der möglichen übertragenen Daten
- Vorgaben für die Installation von APs
    - Wer ist berechtigt WLAN relevante Komponenten installieren?
    - Physikalische Sicherheitsvorgaben
    - Konfigurationsvorgaben für APs (z.B. Verweis auf die Passwortpolicy, etc.)
- Definition und Richtlinien für das Schlüsselmanagement (u.a. auch Unterscheidung ob manuell oder automatisch)
- Definition und Richtlinien für geeignete Authentisierungsmechanismen
- Definition und Richtlinien für WLAN-Endgeräte
    - Konfigurationsvorgaben für WLAN-Clients
    - Vorgaben zur Absicherung gegen Diebstahl
- Definition und Richtlinien zum Reporting und Logging
- Vorgaben zur regelmäßigen Sicherheitsüberprüfungen

[1] Dies kann u.a. auch durch APs, die eine automatische Frequenzwahl ermöglichen, vermieden können.

(2.4) Auswahl des Equipments und Positionierung der APs

Aufgrund des Lageplans und der Ist-Analyse der bestehenden Infrastruktur wird es möglich, eine Abschätzung über die notwendige Anzahl von APs und weiteren notwendigen WLAN-Komponenten zu machen. Im Lageplan sind die möglichen Standorte von APs zu vermerken.

(3) Phase II: Maßnahmenkatalog für Implementierung

Ist die erste Phase abgeschlossen, muss ein Konsens zwischen dem WLAN-Auftraggeber, dem Sicherheitsverantwortlichen und dem zukünftigen Betreiber über die Implementierung gefunden werden. Dabei werden alle Maßnahmen festgelegt, die für die adäquate Umsetzung notwendig sind und im Einklang mit der WLAN-Policy stehen.

Es sei an dieser Stelle noch angemerkt, dass einige bekannte Angriffe – bedingt durch die Technologie als solches – einfacher werden. So kann z.B. ein DNS-Spoofing mit anschließender man-in-the-middle Attacke durchgeführt werden, da der DNS Server typischerweise im kabelgebundenen Bereich liegt und somit die Antwort eines Angreifers aus dem Wireless-Bereich so gut wie immer schneller ist.

Im Folgenden finden sich mehrere auswählbare Maßnahmen wieder, die zum Teil für sich alleine keinen großen Schutz darstellen, werden sie jedoch kombiniert und somit mehrere Sicherheitsschichten implementiert, desto höher der Schutz des Netzwerks. Der Maßnahmenkatalog gliedert sich in einmalige Maßnahmen und wiederkehrende Tätigkeiten.

(3.1) Einmalige Maßnahmen

Diese werden, wie der Name verspricht, im Allgemeinen nur einmal ausgeführt. Ändern sich jedoch Rahmenbedingungen, müssen auch diese Maßnahmen noch einmal überdacht, evaluiert und bei Bedarf neu umgesetzt werden.

(3.1.1) Positionierung von Access Points

Ein Access Point muss in Abhängigkeit von der für ihn vorgesehen Funkzelle bestmöglich positioniert werden, um die Funkwellenausbreitung optimal auszulegen. Obwohl eine mögliche Strahlung außerhalb des Versorgungsbereichs grundsätzlich nicht ausgeschlossen werden darf, soll diese Tätigkeit mit großer Sorgfalt gemacht werden, um die Randstrahlung so gering wie möglich zu halten. Zur Erreichung dieses Ziels sind genaue Messungen der Reichweite der Funkwolke notwendig. Dazu wird z.B. ein AP am vorgesehen Platz aufgestellt und mit Hilfe eines Notebooks als WLAN Client die Funkwellenausbreitung und -stärke am Lageplan vermerkt. Vorsicht sei in Anbetracht unterschiedlicher Antennen geboten (siehe auch (3.1.2)).

Weiters ist unbedingt darauf zu achten, dass die APs bestmöglich gegen physische Zugänglichkeit von unberechtigten Personen geschützt sind. Speziell sei auf den ‚*Reset*' Button hingewiesen, der bei einigen Produkten am AP zur Verfügung steht, um das Gerät wieder in den Defaultzustand zurück zu versetzen. Unbefugte könnten so den AP in den Urzustand zurücksetzen und so u. U. unberechtigten Zugriff auf das Netzwerk erhalten.

(3.1.2) Auswahl der richtigen Antennen und Sendeleistung

Neben der korrekten Positionierung der APs ist auch auf die korrekte Auswahl der Antennen und der eingestellten Sendeleistung zu achten. Mehr über Antennen kann in [WLAN03] nachgelesen werden.

(3.1.3) Passwortmanagement von APs

a) Jene Defaultpasswörter, die bei APs den Zugriff zur Konfiguration bieten, müssen bei Installationsbeginn und später in regelmäßigen Abständen geändert werden. Grundsätzlich sind dabei *starke* Passwörter zu verwenden, jedenfalls sind die Anforderungen einer bestehenden Passwortpolicy zu befolgen. Die Konfiguration über ein Webinterface soll zumindest über TLS/SSL (Transport Layer Security/Secure Socket Layer) mit Authentifizierung bzw. SSH (Secure Shell) gemacht werden. Es ist anzuraten, dass der Zugang zum AP von einem anderen Netz als jenem, in dem sich die mobilen Nutzer befinden, erfolgen soll. Die wohl sicherste Lösung wäre die Deaktivierung des Web- bzw. Telnet Zugangs. Die Konfiguration wäre dann nur über eine direkte serielle Schnittstelle oder über sicherheitstechnisch anerkannte Protokolle (z.B. SSH) möglich. Es sei festgehalten, dass schon das Vorhandensein eines Dienstes (z.B. Telnet) zu Sicherheitsproblemen führen kann (wie z.B. zu DoS-Attacken).

   Zu bevorzugen ist ein AP, der es auf OSI Schicht 2 erlaubt, eine Unterscheidung zwischen Benutzer- und AP-Managementdaten zu treffen (unterschiedliches VLAN mit einer zweiten Netzwerkkarte).

b) Bieten die erworbenen Produkte einen stärkeren Authentifizierungsmechanismus bzw. eine 2-Phasen-Authentifizierung an (z.B. mittels Token), so ist im jeweiligen Fall dafür zu entscheiden.

(3.1.4) IP-Management von APs

Die Default IP-Adressen an den APs sollen geändert werden und in einem Adressbereich liegen, der vom Netzwerkverantwortlichen vergeben wird.

(3.1.5) Segmentierung des WLAN-Netzwerks, Einsatz von Firewalls

Zum gegenwärtigen Zeitpunkt ist aus Sicherheitsgründen anzuraten, dass ein WLAN vom herkömmlichen LAN netzwerktechnisch z.B. über ein VLAN getrennt wird. Eine Kommunikation zwischen LAN und WLAN darf nur über eine gesicherte Verbindung, nach erfolgreicher Authentifizierung über eine eigens dazwischen geschaltete Firewall erfolgen.

(3.1.6) Einsatz von SNMP

Es ist darauf zu achten, dass lediglich SNMPv3 unter Verwendung von starken kryptographischen Mechanismen einen geeigneten Sicherheitsgrad garantieren kann. Von SNMPv1 und SNMPv2 wird abgeraten.

(3.1.7) Intrusion Detection System (IDS)

Solche Systeme werden eingesetzt, um unberechtigte Benutzer zu lokalisieren, die dabei sind, Zugriff zum Netzwerk zu erhalten bzw. das Netzwerk bereits kompromittiert haben. Man unterscheidet dabei zwischen host-, netzwerkbasierten und hybriden IDS-Systemen. Während erstere auf spezielle Systeme abzielen (z.B. Datenbanken, Dateisystem, etc.) und dabei ungewöhnliche Zugriffsverhaltensmuster auf Ressourcen feststellen, bietet ein netzwerkbasiertes IDS-System eine in Echtzeit stattfindende Netzwerkanalyse, um Angriffsmuster erkennen zu können. Verdächtige Verhaltensmuster lösen dann Aktionen aus (Anhalten des Systems, Versenden einer E-Mail, etc.). Ein hybrides IDS verbindet die Vorteile der beiden anderen Varianten.

Es ist zu beachten, dass

- ein netzwerkbasiertes IDS bei verschlüsselten Verbindungen, bei Client-Client-Verbindungen im selben Subnetz (sofern das IDS hinter dem AP installiert wurde) und klarerweise bei ad-hoc Verbindungen seiner Funktion nicht nachkommen kann.

Große Gefahr besteht vor allem bei ad-hoc Verbindungen, die als Bridge unberechtigten Benutzern Zugriff auf das interne Netz geben können.

- ein IDS im Allgemeinen erst dann Angriffe entdeckt, wenn eine Kommunikation ins kabelgebundene Netz erfolgt. Dabei ist das Funknetz bereits kompromittiert!
- ein IDS Sensor auf Paketebene im Allgemeinen keine Angriffe erkennt, die auf der physikalischen bzw. Verbindungsschicht (nach ISO/OSI Referenzmodell) des WLAN erfolgen (Flooding, Jamming, etc.).

Daher sollen bestehende IDS auf oben genannte Punkte geprüft, und ebenso wie bei Neuinstallationen bei Bedarf erweitert oder neu implementiert werden

(3.1.8) Einsatz von DHCP

Kommt DHCP zum Einsatz ist es einem Angreifer leicht möglich unautorisierten Zugang zum Netzwerk zu erhalten. Um das Risiko zu minimieren, kann auf DHCP verzichtet und stattdessen statische IP-Adressen verwendet werden. Dies ist aber aufgrund des Administrationsaufwands nur bei überschaubaren WLAN-Netzwerken mit einem nahezu statischen Benutzerkreis umsetzbar.

(3.1.9) MAC Access Control Listen

MAC Listen beinhalten jene MAC-Adressen, die berechtigt sind, das WLAN Netzwerk zu nutzen. Da aber MAC-Adressen im Klartext übertragen werden und eine MAC-Adresse bei einem Client leicht gefälscht werden kann, ist genau genommen kein Sicherheitsgewinn gegeben. Außerdem bedeutet es in einem größeren Netzwerk – wie auch in (3.1.8) angeführt – einen nicht unerheblich großen Administrationsaufwand. Einen Schutz bieten MAC Listen nur vor weniger versierten Hackern.

(3.1.10) SSID-Name und SSID-Broadcasting

a) Die Default-SSID muss geändert werden. Der vergebene Name des Netzwerkes soll nicht auf das Unternehmen bzw. die Abteilung oder ähnliches schließen lassen, damit der Angreifer nicht gleich die Quelle des Funksignals feststellen kann.

b) Weiters soll (sofern aus Kompatibilitätsgründen[2] möglich) das SSID-Broadcasting am AP deaktiviert werden. Dies ist zwar keine Sicherheitsvorkehrung im eigentlichen Sinn, da eine SSID leicht ausgelesen werden kann bzw. der AP zur Bekanntgabe gezwungen werden kann, birgt aber eine weitere Hürde für Gelegenheitshacker. Diese Maßnahme wird empfohlen, zumal kein großer Administrationsaufwand damit verbunden ist.

(3.1.11) Beacon Intervall maximieren

Um das Auffinden bestehender APs zu erschweren, kann das Intervall zum Versenden der Beacon Frames maximiert werden. Die Steigerung des Sicherheitsgrades ist damit eher vernachlässigbar.

(3.1.12) Personal Firewall am Client

In Funknetzen sind mobile Endgeräte (z.B. Notebooks) höheren Gefahren ausgesetzt als es ihre ‚fest verdrahteten' Pendants im stationärem Betrieb sind. Personal Firewalls auf mobilen

[2] Die Erfahrung hat gezeigt, dass WLAN Komponenten unterschiedlicher Hersteller nicht immer problemlos ohne SSID-Broadcasting kommunizieren können.

Clients können Risiken verkleinern und dürfen bei WLAN Benutzern nicht fehlen. Kommen VPNs zum Einsatz, wird meist auch schon eine Firewall mitgeliefert.

Werden die Personal Firewalls nicht zentral gewartet (die Benutzer können die Konfiguration selbst vornehmen), so ist auf eine dementsprechende Schulung und Sensibilisierung zu achten. Empfohlen wird in diesem Zusammenhang eine zentral gewartete Firewall, die den Sicherheitsrichtlinien der Behörde folgt und deren Konfiguration nicht vom Benutzer verändert werden kann.

Unter diesen Punkt fällt auch die Überprüfung von freigegebenen Verzeichnissen und Laufwerken. Dies stellt ein potentielles großes Sicherheitsrisiko dar.

(3.1.13) Verschlüsselung mit WEP bzw. WEP+

Die bekannten Schwächen von WEP haben gezeigt, dass der Einsatz keinen wirklichen Schutz bietet. Weniger als 20 000 Pakete, die mit dem gleichen Schlüssel verschlüsselt wurden, können bereits ausreichen, einen erfolgreichen Angriff durchzuführen.

Daher wird dringend empfohlen auf verbesserte Sicherheitsmechanismen wie WPA (Wi-Fi Protected Access) mit 802.1X und TKIP bzw. zukünftig 802.11i zurückzugreifen.

- Sofern WEP dennoch zum Einsatz kommen soll, müssen jedenfalls die Default-Schlüssel geändert werden. Außerdem muss die höchstmögliche Schlüssellänge verwendet werden. In diesem Zusammenhang ist es notwendig, auch geeignete Policyeinträge zum Schlüsselmanagement bereitzustellen, damit die eingesetzten Schlüssel häufig und regelmäßig getauscht werden.
- Authentifizierung: Da die Shared-Authentication ein weiteres Sicherheitsrisiko darstellt (Nachrichten können *unbemerkt* gefälscht werden) und die Authentifizierung nur einseitig stattfindet, wird empfohlen, mit einer Open-Authentication zu arbeiten.

(3.1.14) WPA – Wi-Fi Protected Access

Diese Spezifikation basiert auf 802.11i und verspricht neben dem Entgegenwirken der WEP-Schwächen auch herstellerübergreifend kompatibel zu sein. Es setzt auf bestehenden Endgeräten auf und kann bei älteren APs meist durch ein Firmwareupdate nachinstalliert werden. Ebenso wird auch für Clienthardware von den Herstellern meist ein kostenloses SW-Update angeboten. Der von WEP bekannte RC4 Algorithmus bleibt zwar erhalten, kommt nun aber im Zuge vier neuer Algorithmen zum Einsatz (vergrößerter Initialisierungsvektor, Message Integrity Code „Michael", Schlüsselgenerierung und -verteilung, TKIP (Temporal Key Integrity Protocol)).

WPA kann sowohl mit einem beidseitig bekannten Schlüssel (WPA-Personal) als auch mit einem Authentifizierungsserver (WPA-Enterprise) betrieben werden. Während erstere Möglichkeit eher für den Heimbereich (SOHO-Bereiche) vorgesehen ist, ist letztere für Produktionsumgebungen im Business-Bereich die adäquate. WPA dient auch nur der Absicherung des Airlinks.

Die Authentifizierung und das Schlüsselmanagement (Länge von 128 Bit und dynamisches Schlüsselmanagement) werden bei WPA mit Hilfe von 802.1X realisiert.

(3.1.15) Benutzerauthentifizierung über 802.1X

802.1X ist Bestandteil von WPA und 802.11i.

Bevor Benutzer das WLAN nutzen können, sollten diese bereits bei mittleren Sicherheitsanforderungen authentifiziert werden. MAC-Listen stellen diesbezüglich keine (geeignete) Authentifizierung dar.

Die Anmeldung kann via Passwort bzw. bei höheren Sicherheitsanforderungen mittels Softwarezertifikaten oder mit einem anderen Authentifizierungstoken wie z.B. einer Smartcard, Passwortgenerator, etc. erfolgen. Es wird empfohlen Passwörter grundsätzlich zu vermeiden. Sollen aber dennoch Passwörter zum Einsatz kommen, muss über eine Passwortpolicy (diese kann in einer Policy enthalten und sollte unabhängig der Sicherheitsanforderungen sein) die Verwendung von starken Passwörtern vorgeschrieben sein[3].

Durch Einführung von 802.1X und EAP (Extensible Authentication Protocol) wird eine starke Benutzerauthentifizierung möglich. Gleichzeitig bleibt die Kompatibilität zum späteren Standard 802.11i gewahrt. Voraussetzung: beide Kommunikationspartner müssen 802.1X verstehen. EAP stellt das Transportprotokoll für Authentisierungsinformationen zwischen Authentifizierungsserver (z.B. RADIUS) und dem mobilen Client dar. Die eigentliche Authentifizierung wird durch den EAP-Typ durchgeführt. Folgende Typen stehen zur Auswahl: EAP-MD5 (Message Digest), EAP-TLS (Transport Layer Security), EAP-TTLS (Tunnelled TLS {Funk Software, Certicom}), LEAP (Lightweight EAP {Cisco}), und PEAP (Protected EAP {Cisco, Microsoft, RSA Security}), wobei sich EAP-TLS als de-facto Standard durchgesetzt hat und auch hier empfohlen wird. Da einige Lösungen proprietäre Entwicklungen darstellen, ist in den geschwungenen Klammern {} jeweils der Hersteller angeführt.

(3.1.16) 802.11i

Sobald der Standard verabschiedet ist, sollte dieser in WLAN-Implementierungen berücksichtigt werden. WEP, WEP+ und WPA sollten mit dieser Technologie ersetzt werden.

Bei 802.11i (auch mit WPA2 bezeichnet) wird der in WPA und WEP verwendete RC4-Algorithmus durch den AES ersetzt und es wird anstelle von *Michael* in WPA das CCMP (Counter Mode Encryption mit CBC-MAC Protocol) verwendet um Daten-, Headerintegrität und Vertraulichkeit sicherzustellen.

Anmerkung: Für den AES ist es wohl notwendig aufgrund der komplexeren Berechnungen und damit verbundenen höheren Ressourcenanforderungen die Hardware zu tauschen. Aus diesem Grund ist auch die Rückwärtskompatibilität nicht gewährleistet.

(3.1.17) VPN-Lösung

Einen höheren Sicherheitsgrad bietet die Implementierung eines IPSec-VPN. Dabei verbindet sich ein Client mit einem VPN-Gateway über den AP, der wiederum hinter der Firmenfirewall platziert wird. Der Nachteil dieser Lösung ist, dass es auf den Clients notwendig wird, eine VPN-Client-Software zu installieren. Jedoch bieten die gängigsten Plattformen IPSec Clients bereits standardmäßig an (z.B. der Microsoft L2TP/IPSec VPN Client ist standardmäßig ab Windows 2000 im Betriebssystem inkludiert und kann auch auf Windows 98 bzw. WinNT nachinstalliert werden; auf Linux gibt es die freie Free S/WAN Implementierung zum Download).

VPN-Lösungen können den Vorteil haben, dass sie bereits in der Organisation zum Einsatz kommen. Somit sind die NutzerInnen mit der Technologie bereits vertraut und auch die Netzwerkverantwortlichen haben Erfahrungen damit.

[3] Das hier angesprochene Passwort ist nicht der WEP-Schlüssel. Ein starkes Passwort kann aufgrund der Schwäche von WEP grundsätzlich die Sicherheit nicht erhöhen.

(3.1.18) Alternativer Lösungsansatz

Wie in [WLAN03] beschrieben, kann auch ein sog. Wireless Firewall Gateway [[NASA}] umgesetzt werden. Der Client benötigt für die Authentifizierung lediglich einen Webbrowser und DHCP Software – beides wird von den meisten Betriebssystemen zur Verfügung gestellt. Der eingesetzte DHCP Server erlaubt das dynamische Löschen von Einträgen aus den Firewall-Access-Listen, wenn die IP-Adressen vom DHCP Server freigegeben werden und beantwortet nur Anfragen aus dem Funklan-Bereich. Eine Firewall ist initial so konfiguriert, dass ohne eine positive Authentifizierung nur absolut notwendige Protokolle erlaubt sind. Mittels eines IP-Filters, der nur Verbindungen zu diesem Authentifizierungsservice passieren lässt, ist damit ohne vorherige Authentisierung keine weitere Kommunikation möglich. Erst nach einer positiven Authentifizierung wird ein entsprechender Eintrag in den Firewallregeln gemacht und es wird eine weitere Kommunikation möglich.

(3.1.19) Schulung und Sensibilisierung

Die Benutzer eines WLANs müssen eine Einschulung erhalten. Ziel ist, dass diese dann wissen, was sie tun dürfen, worauf sie achten müssen und wann sie sich etwaigen Gefahren aussetzen. Zum Schulungsinhalt kann je nach implementierten Maßnahmen auch die Bedienung der Personal Firewall oder die Verwendung des VPN-Clients zählen. Eine solche Maßnahme erleichtert nicht nur dem Helpdesk die Arbeit, sondern resultiert meist auch in einer höheren Akzeptanz. Vielmehr kann dadurch auch erreicht werden, dass Sicherheit im Unternehmen gelebt wird.

(3.1.20) Überprüfung der WLAN-Policy

Nach erfolgreicher Implementierung muss mit den gewonnenen Erkenntnissen eine Überprüfung der erstellten bzw. angepassten Policy erfolgen. Bei Bedarf muss nachgebessert werden.

(3.1.21) Dokumentation

Nachdem das WLAN implementiert und getestet wurde, muss eine Dokumentation über das Netzwerk erstellt werden. Diese soll zumindest die Punkte

- Ziel und Zweck
- Positionierung (grafisch eingezeichnet im Lageplan) der APs
- Konfiguration der APs (IP-Adresse, Kanal, Filter, aktuelle Firmware/Software etc.)
- Benennung und Kontaktadresse der Verantwortlichen
- Netzabdeckung (grafisch eingezeichnet im Lageplan)

beinhalten.

(3.2) Wiederkehrende Tätigkeiten

Nicht nur bevor bzw. kurz nach der Inbetriebnahme eines Produktiv-WLAN-Systems müssen Sicherheitsüberprüfungen durchgeführt werden, sondern zu regelmäßigen und/oder zufällig wiederkehrenden Zeitpunkten. Bei diesen Überprüfungen sollen u.a. folgende Punkte beachtet werden:

(3.2.1) Überprüfung der Einhaltung der WLAN-Policy

In regelmäßigen Abständen soll eine Überprüfung der vorgegebenen Policy erfolgen. Entstehen neue Anforderungen bzw. werden neue Technologien verfügbar, die eine

Verbesserung der Sicherheit und/oder Infrastruktur zur Folge haben, muss die Policy bei Bedarf angepasst werden.

(3.2.2) Überprüfung der installierten APs und Netzwerkscans

Entsprechende Soft- und Hardware kann diese Überprüfungen zum Großteil automatisiert durchführen. Diese Maßnahme verhindert den Verlust von Vertraulichkeit und/oder Integrität von Unternehmensdaten, Verlust von Bandbreite als auch eventuelle Überlappungen von verwendeten Sendekanälen (Interferenzen und Störungen des Funk-LANs).

Zugriffsberechtigung bei APs und weiteren Netzwerkkomponenten

Es muss sichergestellt sein, dass nur berechtigte Personen Konfigurationsänderungen vornehmen können. Daher sollten APs mit entsprechenden Netzwerktools kontinuierlich überwacht werden. Kommen weitere Netzwerkkomponenten zum Einsatz (VPN-Gateways, Firewalls, IDS, etc.), so sind auch diese regelmäßig zu überprüfen und zu warten.

Unrechtmäßig betriebene WLANs

Gleichzeitig wird bei diesen Überprüfungen dringend empfohlen auch Netzwerkscans durchzuführen, sodass jene APs, die unberechtigter Weise, meist von ‚technologie-motivierten' Mitarbeitern installiert wurden, aufgespürt werden können.

Fremdbetriebene WLANs

Weiters sollen fremdbetriebene APs gefunden werden, die außerhalb der Unternehmensgrenzen installiert wurden und deren Funkwolke jedoch über diese Grenzen hinweg reicht.

Auswertung der Logdateien

Die vorhandenen Logdateien von APs müssen regelmäßig auf ungewöhnliche Vorkommnisse überprüft werden. Dazu zählt im Falle von MAC-Adress-Filtering z.B. die Überprüfung auf unerlaubte MAC-Adressen etc.

Kommen weitere Netzwerkkomponenten zum Einsatz (VPN-Gateways, Firewalls, IDS, etc.), so sind auch deren Logdateien auszuwerten.

(3.2.3) Physische Überprüfung der installierten APs

Weiters muss darauf geachtet werden, dass APs auf Zugänglichkeit, Beschädigungen, etc. kontrolliert werden, um jene Risiken auszuschließen, die über eine missbräuchliche Verwendung der Verbindung zum Ethernet des Unternehmens entstehen können (Man-in-the-middle Attacken, etc.).

(3.2.4) Überprüfungen bei den Clients

Neben den Netzwerkkomponenten für das WLAN müssen auch die clientseitigen Einstellungen regelmäßig kontrolliert und gewartet werden. Dazu zählen die WLAN- als auch etwaige Firewall- Konfigurationen, sowie betriebssystemabhängige Einstellungen (freigegebene Ordner, etc.).

(3.2.5) Patches und Upgrades

a) Sowohl die SW der APs als auch jene der Clients muss ständig auf den neuesten Stand gebracht werden.

b) Hersteller ermöglichen das Abonnieren von Mailinglisten, in denen sie auf Bugfixes und Patches für ihre Produkte hinweisen. Administratoren von WLANs sollten von diesem Service Gebrauch machen.

Oft werden durch Patches bekannte Bugs korrigiert. Eine Onlinedatenbank mit bestehenden Schwächen von Produkten wird vom NIST zur Verfügung gestellt[4].

(4) WLAN-Kategorisierung

Je nach Zielsetzung (siehe Abschnitt (2) auf Seite 3) ergeben sich auch Vorgaben in Bezug auf die anderen WLAN-Kriterien und die zu installierenden Maßnahmen aus dem Maßnahmenkatalog. Es werden hier nur jene Maßnahmen angeführt, die sich für die einzelnen Kategorien unterscheiden.

[4] Link: http://icat.nist.gov/icat.cfm

(4.1) WLAN für niedrige Sicherheitsanforderungen

[Zugang zum Internet für Besucher]

Maßnahme	Empfohlen	Optional	Anmerkungen
(2.3.1) Erstellen eines Lageplans	x		
(2.3.2) Konfiguration der verwendeten Kanäle	x		
(2.3.3) Erstellen einer WLAN-Policy	x		
(3.1.1) Positionierung von Access Points	x		
(3.1.2) Auswahl der richtigen Antennen und Sendeleistung	x		
(3.1.3) Passwortmanagement von APs	x		
(3.1.4) IP-Management von APs	x		
(3.1.5) Segmentierung des WLAN-Netzwerks, Einsatz von Firewalls	x		Für diese Kategorie bedarf es grundsätzlich keiner Kommunikation zwischen LAN und WLAN
(3.1.6) Einsatz von SNMP zur Wartung		x	Sofern SNMPv3
(3.1.7) Intrusion Detection System (IDS)			
(3.1.8) Einsatz von DHCP	x		
(3.1.9) MAC Access Control Listen			
(3.1.10) SSID-Name und SSID-Broadcasting	x		
(3.1.11) Beacon Intervall maximieren			
(3.1.12) Personal Firewall am Client	x		Gilt für betriebseigene Clients
(3.1.13) Verschlüsselung mit WEP bzw. WEP+			
(3.1.14) WPA – Wi-Fi Protected Access		x	Je nach Anforderung
(3.1.15) Benutzerauthentifizierung über 802.1X		x	Je nach Anforderung
(3.1.16) 802.11i		x	Je nach Anforderung
(3.1.17) VPN-Lösung			

(3.1.19) Schulung und Sensibilisierung	x		Für eigene Mitarbeiter
(3.2.5) Patches und Upgrades	x		
(3.1.21) Dokumentation	x		
(3.2) Wiederkehrende Tätigkeiten	x		

(4.2) WLAN für mittlere Sicherheitsanforderungen

[Zugang zum Inter- und Intranet für interne Mitarbeiter und Internet für Besucher]

Maßnahme	Empfohlen	Optional	Anmerkungen
(2.3.1) Erstellen eines Lageplans	x		
(2.3.2) Konfiguration der verwendeten Kanäle	x		
(2.3.3) Erstellen einer WLAN-Policy	x		
(3.1.1) Positionierung von Access Points	x		
(3.1.2) Auswahl der richtigen Antennen und Sendeleistung	x		
(3.1.3) Passwortmanagement von APs	x		
(3.1.4) IP-Management von APs	x		
(3.1.5) Segmentierung des WLAN-Netzwerks, Einsatz von Firewalls	x		es bedarf nicht unbedingt einer Kommunikation zwischen LAN und WLAN
(3.1.6) Einsatz von SNMP zur Wartung		x	Sofern SNMPv3
(3.1.7) Intrusion Detection System (IDS)		x	
(3.1.8) Einsatz von DHCP	x		
(3.1.9) MAC Access Control Listen		x	Nur bei kleinen nahezu statischen Netzwerken
(3.1.10) SSID-Name und SSID-Broadcasting	x		
(3.1.11) Beacon Intervall maximieren			
(3.1.12) Personal Firewall am Client	x		Gilt für betriebseigene Clients

(3.1.13) Verschlüsselung mit WEP bzw. WEP+		**x**	Nur bei kleinen nahezu statischen Netzwerken
(3.1.14) WPA – Wi-Fi Protected Access	**x**		Je nach Anforderung
(3.1.15) Benutzerauthentifizierung über 802.1X	**x**		Je nach Anforderung
(3.1.16) 802.11i	**x**		Je nach Anforderung
(3.1.17) VPN-Lösung		**x**	
(3.1.19) Schulung und Sensibilisierung	**x**		Für eigene Mitarbeiter
(3.2.5) Patches und Upgrades	**x**		
(3.1.21) Dokumentation	**x**		
(3.2) Wiederkehrende Tätigkeiten	**x**		

(4.3) WLAN für hohe Sicherheitsanforderungen

[Zugang zum Inter- und Intranet für interne Mitarbeiter und Internet für Besucher]

Maßnahme	**Empfohlen**	**Optional**	**Anmerkungen**
(2.3.1) Erstellen eines Lageplans	**x**		
(2.3.2) Konfiguration der verwendeten Kanäle	**x**		
(2.3.3) Erstellen einer WLAN-Policy	**x**		
(3.1.1) Positionierung von Access Points	**x**		
(3.1.2) Auswahl der richtigen Antennen und Sendeleistung	**x**		
(3.1.3) Passwortmanagement von APs	**x**		
(3.1.4) IP-Management von APs	**x**		
(3.1.5) Segmentierung des WLAN-Netzwerks, Einsatz von Firewalls	**x**		Für diese Kategorie bedarf es grundsätzlich keiner Kommunikation zwischen LAN und WLAN
(3.1.6) Einsatz von SNMP zur Wartung		**x**	Sofern SNMPv3
(3.1.7) Intrusion Detection System (IDS)	**x**		

(3.1.8) Einsatz von DHCP	**x**		
(3.1.9) MAC Access Control Listen		**x**	Nur bei kleinen nahezu statischen Netzwerken
(3.1.10) SSID-Name und SSID-Broadcasting	**x**		
(3.1.11) Beacon Intervall maximieren			
(3.1.12) Personal Firewall am Client	**x**		Gilt für betriebseigene Clients
(3.1.13) Verschlüsselung mit WEP bzw. WEP+		**x**	Nur bei kleinen nahezu statischen Netzwerken
(3.1.14) WPA – Wi-Fi Protected Access		**x**	Je nach Anforderung
(3.1.15) Benutzerauthentifizierung über 802.1X		**x**	Je nach Anforderung
(3.1.16) 802.11i		**x**	Je nach Anforderung
(3.1.17) VPN-Lösung	**x**		
(3.1.19) Schulung und Sensibilisierung	**x**		Für eigene Mitarbeiter
(3.2.5) Patches und Upgrades	**x**		
(3.1.21) Dokumentation	**x**		
(3.2) Wiederkehrende Tätigkeiten	**x**		

(5) Referenzen

[802.11]

IEEE P802.11, The Working Group for Wireless LANs. Abgerufen aus dem World Wide Web am 20. Februar 2004 unter http://grouper.ieee.org/groups/802/11/

[802.1X]

IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control, Oktober 2001. Abgerufen aus dem World Wide Web am 20. Februar 2004 unter http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[NASA}

Advanced Supercomputing Divsion, Wireless Firewall Gateway White Paper, Abgerufen aus dem World Wide Web am 15. Mai 2004 unter http://hyatus.dune2.info/Wireless_802.11/nasa_wireless.html

[WLAN03]

B. Martin, Beachtens- und Wissenswertes zu WLANs in der Verwaltung, Version 1.3, 06. Mai 2003. Abgerufen aus dem World Wide Web am 15. Mai 2004 unter http://www.cio.gv.at/it-infrastructure/wlan/WLAN_u_need_2_know_v13.pdf

[WPA]

Wi-Fi Protected Access, Abgerufen aus dem World Wide Web am 15. Mai 2004 unter http://www.wi-fi.org/OpenSection/protected_access.asp

[SiHB]

Chief Information Office, IKT-Stabsstelle, Österreichisches IT-Sicherheitshandbuch Teil 1: IT-Sicherheitsmanagement Version 2.1 Mai 2003 und Teil 2: IT-Sicherheitsmaßnahmen Version 2. 1 Mai 2003. Abgerufen aus dem World Wide Web am 15. Mai 2004 unter http://www.cio.gv.at/securenetworks/sihb/

History

Version	Datum	Kommentar
1.0.0	03.06.2004	Initialversion erstellt.
Ersteller Bernd Martin		