WPA2 SICHERHEITSLÜCKE ENTDECKT: DAS SOLLTEST DU TUN, UM DEINE DATEN ZU SCHÜTZEN

Veröffentlicht am 17. Oktober 2017 von jkonrad

Um ein **WLAN Netzwerk** abzusichern und vor Dritten zu schützen, galt das Verschlüsselungsverfahren **WPA2** bisher als sicher. Doch Sicherheitsforscher der Universität Leuven haben im Oktober 2017 **Sicherheitslücken** entdeckt, die gravierende Folgen haben können. Was Du tun kannst, um Dich dauerhaft vor **Hackerangriffen** zu schützen, erfährst Du hier.

Anlässlich der ermittelten Schwachstelle im WPA2 Sicherheitsprotokoll im Oktober 2017 haben wir diesen Blogartikel als **Erste Hilfe Maßnahme** für Dich recherchiert. Durch verschiedene Updates von Android, iOS und Google wurde die WPA2 Sicherheitsschwachstelle behoben. Und jetzt kommt zum Glück bald der neue **WLAN-Standard WPA 3**! Natürlich macht die rasante Reaktion der Anbieter und der **Wi-Fi Alliance** nicht den Schock wett, den viele bei der Meldung der Sicherheits Lücke erlitten haben. Durch **KRACK** konnten **Hacker** die WLAN-Verschlüsselung aushebeln und so den Datenverkehr in einem WLAN-Netz verfolgen und sogar manipulieren. Firmen und Privatpersonen mussten um ihre **sensiblen Daten** bangen. Vor allem Unwissen über die spezifischen Begriffe wie WLAN, WPA2, WIFI, WEP usw., wie auch ihre technischen Zusammenhänge und Bedeutungen, schüren Ängste und treffen uns häufig unvorbereitet. Damit Du zukünftig vor **Hackeraktivitäten** und **Sicherheitsstörungen** im Internet bzw. im Datenverkehr geschützt bist, haben wir ein kleines **Sicherheitslexikon** für Dich entwickelt. In diesem sind alle wichtigen Begrifflichkeiten zusammengefasst und erklärt. So verschaffst Du Dir einen **schnellen Überblick** und bist ab sofort gut gewappnet.

Schon gewusst? Ein **neuer Sicherheitsstandard** wird im Laufe des Jahres **2018** von der **Wi-Fi-Alliance** vorbereitet: WPA 3! Das hat die Organisation Wi-Fi Alliance bekanntgegeben. Ob als Antwort auf die Krack Sicherheitslücke Ende 2017 oder als zwangsläufige Weiterentwicklung von WPA2, die optimierte Verschlüsselungstechnik soll **4 neue Sicherheitsfunktionen** enthalten, welche über die **WLAN-Router**, **Clients** und **Access Points** integriert werden. Mehr dazu erfährst Du hier.

„Krack" (Key Reinstallation Attack) ist der Begriff, unter dem sich Angreifer in jede Verbindung hacken können, die mit dem Sicherheitsstandard WPA2 (Wi-Fi Protected Access) verschlüsselt sind. Nahezu alle Netzwerke sind mit WPA2 abgesichert. Darunter fallen alle Geräte, die sich über einen **Router** per WLAN mit dem Internet verbinden – Smartphones, Computer, Drucker oder andere Geräte in Deinem WLAN Netzwerk wurden somit unsicher.

DAS VERSCHLÜSSELUNGSVERFAHREN WPA2

WPA2 soll nicht nur dafür sorgen, dass nur ausgewählte Nutzer den Zugriff auf das **WLAN Netzwerk** bekommen, sondern auch unbefugte Dritte davon abhalten, Daten abzufangen oder zu manipulieren.

Ältere Standards wie **WPA** und **WEP** (Wired Equivalent Privacy) wurden schon vor Jahren als unsicher eingestuft. WEP sollte nicht nur den Zugang zum Netz regeln, sondern auch die Vertraulichkeit und Integrität von Daten sicherstellen. Doch aufgrund verschiedener Schwachstellen sollte damals auf WPA zurückgegriffen werden – eher empfahl sich allerdings hier die sichere Variante WPA2, die jetzt nun auch nicht mehr sicher scheint.

Das Verfahren WPA2 funktioniert in **vier Stufen**. Unter anderem einigen sich Sender und Empfänger mit einem „Handshake" auf den zu nutzenden Schlüssel für die Session. Auf Stufe 3 kann dieser Schlüssel durch einen Designfehler mehrmals verwendet werden - was es Hackern möglich macht, die Verschlüsselung zu knacken.

BESONDERE GEFÄHRDUNG BEI ANDROID UND LINUX

Grundsätzlich sind alle Geräte betroffen, die in einem Netzwerk mit WPA2 verschlüsselt sind - besonders allerdings Geräte mit den Betriebssystemen **Linux** und **Android** mit dem System 6.0, was 40% aller Android-Nutzer ausmacht. Bei Windows- und Apple Betriebssystemen können die Schwachstellen nur eingeschränkt ausgenutzt werden. Auch sind Angriffe auf Macs oder iPhones möglich – bisher sind aber hier die Ausmaße noch nicht klar. Die **Fritz Box** von Hersteller AVW ist nach eigenen Angaben des Router-Herstellers nicht von KRACK betroffen.

FOLGEN

Theoretisch können alle Daten von Hackern abgefangen werden. Hier ist jedoch zu beachten, dass besonders **sensible Daten** – zum Beispiel beim Online-Banking – separat verschlüsselt werden und somit schwer abzufangen sind. Anders als bei dem berüchtigten „Heartbleed"-Fehler - der die Sicherheit der Hälfte aller Server weltweit angriff - muss der Hacker sich bei einem möglichen Angriff **in der Nähe des WLANS** – also vor Deiner Haustür – aufhalten, um Deine Daten auslesen oder komplett abgreifen zu können. Außerdem muss er sich in einer Man-in-the-Middle-Attacke befinden, sich also zwischen Router (Zugangspunkt) und Klient befinden. Voraussetzung ist hierfür, dass der Klient sich freiwillig ummeldet. Damit das passiert, muss der Hacker näher am Klienten sein, als der Router.

Trotzdem rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) dazu, vorerst auf Online-Banking und Online-Shopping in einem WPA2 gesicherten WLAN Netzwerk zu verzichten – solange, bis **Updates** installiert werden können und sich die Sicherheitslücke so schließt. Surfst Du mit Kabel, ist die Verbindung weiterhin sicher.

Bei **Unternehmen** ist die Lage allerdings anders zu betrachten. Sich in ein Firmennetz zu hacken ist für Angreifer weitaus lukrativer: Hier kann beispielsweise Industriespionage betrieben oder ganze Netzwerke lahmgelegt werden, um Konkurrenten vorübergehend zu dämpfen.

Generell sind momentan allerdings noch keine Angriffe bekannt, die sich aus der Sicherheitslücke von „Krack" ergeben haben – weder bei Privatpersonen, noch in Unternehmen.

MASSNAHMEN

Die Wi-Fi-Alliance hat bereits erste Maßnahmen ergriffen, um die Sicherheitslücke zu beheben. Hierbei handelt es sich um ein Konsortium, in dem über 300 Unternehmen tätig sind und das die Geräte auf der Basis des Standards IEEE-802.11 zertifiziert. Laut diesem gibt es aktuell noch keine Anzeichen, dass diese Sicherheitslücke böswillig ausgenutzt wurde.

Das Konsortium hat dennoch veranlasst, dass alle angeschlossenen Zertifizierungsstellen die Produkte auf die WPA2 Schwachstelle hin prüfen. Die Mitgliedsfirmen erhalten hierfür ein Erkennungstool. Bevor das Tool öffentlich wird, sollen die Anbieter allerdings die Möglichkeit haben, entsprechende Updates an ihre Nutzer zu verteilen. Diese Updates sollen keine Veränderungen erfordern, die die Kompatibilität zwischen WLAN Geräten beeinträchtigen.

Alle Details zu den aktuellen Sicherheitslücken sollen allerdings erst am 01. November vorgestellt werden - bei einem Vortrag auf der ACM Conference on Computer and Communications Security. Bis dahin haben wir hier wichtige Hinweise für Dich, wie Du Deine Daten schützt und Dich gegen Hackerangriffe wehren kannst.

AUF EINEN BLICK: SO SCHÜTZT DU DEINE DATEN

Aufgrund der Sicherheitslücke Dein WLAN Passwort zu ändern, hilft nicht. Die Fehler müssen durch ein Software-Update aller Geräte beseitigt werden.

Was Du sonst noch beachten musst, um sicher im Internet zu surfen, haben wir Dir hier zusammengefasst.

VERSCHLÜSSELUNG DURCH VPN

Ein privates Netzwerk verschlüsselt Deine Daten und schützt sie vor unbefugten Dritten - das solltest Du vor allem in öffentlichen WLAN Netzwerken beachten. Dadurch kannst Du von jedem Ort auf der Welt sicher auf Webseiten zugreifen, denn es handelt sich dabei um ein in sich geschlossenes Netzwerk, indem die Teilnehmer tausende Kilometer voneinander getrennt sein können. Diese verbinden sich über ein VPN Protokoll zu einem Loginserver und erhalten so eine neue IP Adresse. So ist nun die gesamte Verbindung verschlüsselt und niemand kann innerhalb dieser Daten Informationen mitlesen oder verändern.

ROUTER UND GERÄTE AKTUALISIEREN

Einzelne Hersteller bieten bereits jetzt ein Update an – diese solltest Du installieren, um die Sicherheitslücke zu schließen. Das gilt für Router genauso wie für Deine Smartphones, PCs oder Laptops – mit veralteter Firmware macht man es Hackern einfach. Router aktualisieren sich meistens automatisch, Du solltest die Einstellungen aber lieber nochmal checken. Einige Router nutzen den 4 Stufen „Handshake“ nicht um ihr Netzwerk abzusichern und sind daher nicht von „Krack“ betroffen. Wenn Du Dir nicht sicher bist, erkundige Dich bei dem Hersteller.

SSID-KENNUNG ÄNDERN

Häufig wird die Benutzererkennung bei Installation eines Routers vom Anbieter voreingestellt, die sogenannte SSID (Service Set Identifier) – und setzt dabei Deinen Namen als Kennung ein. Bei der ersten Inbetriebnahme solltest Du diese Einstellungen ändern. Hacker können sonst feststellen, wo genau sich ein Netz in ihrer Nähe befindet. Auf keinen Fall darfst Du hier für den Benutzernamen und das Passwort den gleichen Begriff verwenden.

AUF VERSCHLÜSSELTEN WEBSEITEN SURFEN

Ist die WPA2 Verschlüsselung gehackt, kannst Du auf eine weitere Verschlüsselung setzen: HTTPS (Hypertext Transfer Protocol Secure). Hier handelt es sich um ein Kommunikationsprotokoll im Internet, um Daten sicher zu übertragen. Browser kennzeichnen seriöse Webseiten damit als „sicher" - mit HTTPS Everywhere zwingst Du Dein System, nur noch sichere Seiten zu betreten. Ist die Website Deines Unternehmens noch nicht auf HTTPS ausgerichtet, sprich uns an - wir helfen Dir dabei, von Google als seriöse und sichere Website eingestuft zu werden.

Kontakt aufnehmen

FIREWALL AKTIVIEREN

Konfiguriere die Firewall Deines Routers so, dass eine Freigabe von Dateien und Druckern deaktiviert ist und aktiviere dabei den „geschützten Modus". So verweigerst Du Hackern den Zugriff auf Deine persönlichen Daten. Um den Schutz zu überprüfen, kannst Du Software wie Shields Up! Verwenden.

DAS RICHTIGE KENNWORT

Es klingt einfach: Du verwendest den Namen oder das Geburtsdatum Deines Partners/Deiner Partnerin als Kennwort– so vergisst Du es wenigstens nicht. Schlechte Idee! So machst Du es Hackern einfach, das Kennwort zu erraten. Wähle einen Begriff, der ein wenig komplizierter ist und verwende Buchstaben in Kombination mit Zahlen. Solltest Du irgendwann nicht mehr durchsteigen, gibt es hilfreiche Apps, die Deine Passwörter sicher speichern.

GASTZUGÄNGE EINRICHTEN

Benötigen Deine Gäste einen Zugriff auf Dein WLAN Netzwerk, dann hast Du die Möglichkeit, ihnen einen Gastzugang (also einen privaten Hotspot) einzurichten. Diesen kannst Du in den Einstellungen Deines Routers vornehmen. Hier kannst Du Zeitraum und Passwort für die Nutzung vorgeben und es nach Belieben ändern. Außerdem kannst Du den Zugang auf bestimmte Anwendungen einschränken, indem Du zum Beispiel bestimmte Webseiten verbietest.

WLAN ABSCHALTEN

Bist Du tagsüber nicht zuhause und benötigen daher keinen Zugriff auf Deinen Router, kannst Du ihn ebenso ausschalten. Das spart nicht nur Strom, auch können Hacker in der Zeit nicht angreifen.

Um ganz sicher zu gehen, kannst Du Deinen Router deaktivieren und nur noch über LAN (Local Area Network, zum Beispiel Ethernet) – also per Kabel – surfen. Experten halten diese Maßnahme allerdings für überzogen. Alternativ kannst Du diese Methode aber nutzen, wenn Du Online-Banking betreibst – also sehr sensible Daten rausschickst.

EIN WEITERER TIPP FÜR UNTERNEHMEN

Viele kleine Firmen verwenden den persönlichen Modus von WPA2: WPA2 Personal. Hier wird eine Passphrase – ein Passwort, bei dem es sich nicht einfach nur um ein einzelnes Wort handeln sollte – genutzt, die allen Mitarbeitern gemeinsam zur Verfügung steht. Das bedeutet, dass alle – Personen sowie Geräte – den gleichen Code nutzen. Für ein Heimnetzwerk mag das ausreichen, in Unternehmen ist diese Methode allerdings anfällig für unbefugte Zugriffe. Zum Beispiel haben Mitarbeiter nicht nur die Möglichkeit den Code an Externe weiterzugeben, auch können sie diesen nach einem Ausscheiden aus dem Unternehmen weiterhin nutzen. Das gleiche passiert, wenn ein Gerät verloren geht – auch der Finder kann sich weiterhin im Netzwerk anmelden. Die Folge: Nach jedem Ausscheiden eines Mitarbeiters oder eines Geräteverlustes müsste das Passwort geändert und bei jedem noch berechtigen Mitarbeiter neu eingestellt werden. Somit werden nicht nur Nerven, sondern auch Zeit verschwendet.

Die Lösung: Die Nutzung von **WPA2-Enterprise**. Hier ist ein weiteres Setup nötig, das bietet allerdings Vorteile: Statt einer gemeinsamen Passphrase erhält jeder User ein universelles Passwort. So müssen Unternehmen nicht jedes Mal die Passphrase ändern, sondern können Anmeldeinformationen einfach löschen oder aktualisieren. Zusätzlich müssen sich die Endnutzer kein Passwort mehr merken oder es konfigurieren, sondern der Administrator stellt die Anmeldeinformationen schon von Anfang an bereit.

DAS VERSCHLÜSSELUNGSVERFAHREN WPA3

WLANs sollen endlich wirklich sicher gemacht werden. Die Organisation Wi-Fi-Alliance hat im Januar 2018 auf der **Technikmesse CES in Las Vegas** ein neues Standard Protokoll für die Verschlüsselung von drahtlosen Datennetzwerken inklusive neuer Sicherheitsfunkionen vorgestellt: WPA3. Das Verschlüsselungsverfahren WPA3 ist der Nachfolger von WPA2. Noch 2018 sollen Geräte auf den Markt kommen, die das neue Protokoll unterstützen.

Ziele von WPA3:

- Steigerung der Sicherheit von WLANs
- verschlüsselte WLAN Verbindungen vereinfachen

In dem neuen Verschlüsselungsverfahren wurden **4 neue Funktionen** integriert:

1. robuster Schutz bei der Verwendung von einfachen Passwörtern (Passphrases wären somit nicht unbedingt notwendig)
2. Sicherheit und Vereinfachung der Konfiguration auch für Geräte die über keinen Bildschirm verfügen. Dies ist vor allem hinsichtlich der immer populärere werdenden Smart Home Assistenten sehr aktuell: Amazon Echo Dot und Google Mini haben beispielsweise keine Bildschirme.
3. Stärkung der Privatsphäre der Nutzer durch individualisierte Verschlüsselung von Daten in offenen Netzwerken
4. Ermöglichung der Betreibung von WiFi Netzwerken auch in Bereichen mit erhöhten Sicherheitsanforderungen wie Regierungseinrichtungen

Eine Frage stellt sich Dir jetzt bestimmt: **Brauche ich bald WPA3 oder bin ich auch mit WPA2 abgesichert?**

Der neue Sicherheitsstandard wird erstmal hauptsächlich auf **Neugeräten** zum Einsatz kommen. So wird es eine Weile dauern bis er sich durchgesetzt hat. Wenn Du also einen Router hast, der nach dem KRACK Vorfall ein Sicherheits-Update bekommen hat, musst Du nicht unbedingt einen neuen **Rooter** mit WPA3 kaufen.

Die **WiFi Alliance** hat zudem erklärt, dass WPA2 auch zukünftig in zertifizierten Geräten integriert ist. WPA2 wird auch weiterhin durch Uptdates verbessert und weiterenwickelt, um die Sicherheit zu gewährleisten. WPA3 ist also kein unmittelbarer Ersatz für WPA2, sondern eine Weiterentwicklung, die in **Neugeräten** eingesetzt wird.

Hast Du noch Fragen zur Datensicherheit in Deinem Unternehmen? Wir unterstützen Dich gern dabei, Deine Daten zu schützen.

Kontakt aufnehmen

KLEINES SICHERHEITSLEXIKON

BSI – das Bundesamt für Sicherheit in der Informationstechnik ist eine Bundesbehörde, die sich mit der IT-Sicherheit im Land beschäftigt. Sie ist insbesondere zuständig für den Schutz der Netze des Bundes sowie für die Abwehr von Cyberangriffen auf die Regierungsnetze. Unter anderem ist sie für die Warnung der Bürger bei Sicherheitslücken und die Zertifizierung von Produkten und Dienstleistungen der IT in Deutschland zuständig. Der BSI gibt den **IT-Grundschutz-Katalog** heraus. Diese dient Behörden und Unternehmen als Richtlinie für die Maßnahmen, die zur Erlangung eines zertifizierten IT-Grundschutzes notwendig sind. Mit der Zertifizierung können Unternehmen zeigen, dass sie zur Absicherung ihrer IT-Systeme geeignete Maßnahmen für den Schutz vor IT-Sicherheitsbedrohungen unternommen haben.

Firewall
– hier handelt es sich um ein Sicherheitssystem. Diese Sicherheitswand bzw. „Brandwand" schützt zum Beispiel einen Computer vor unzulässigen Netzwerkzugriffen. Um die IT- und Datensicherheit zu gewährleisten, werden Firewalls implementiert.

HTTPS (
Hypertext Transfer Protocol Secure) ist ein Protokoll bzw. eine Transportverschlüsselung, welches die Aufgabe hat unsere Kommunikation bzw. Daten abhörsicher zu übertragen. Es wurde von Netsape zusammen mit **SSL** entwickelt. Durch eine HTTP-Verbindung werden Daten zwischen verschiedenen Geräten wie Computern hin und her übertragen. Um diese zu sichern und nicht angreifbar und änderbar zu machen, werden die HTTP-Daten verschlüsselt und werden somit zu HTTPS. Dafür wird die Technik des Protokolls TLS verwendet.

Wenn Du eine Website besuchst, die mit „https" beginnt, ist der Datenaustausch zwischen Deinem Computer und der Website über HTTPS verschlüsselt.

Du möchtest mehr über HTTPS und SSL Verschlüsselung erfahren und wissen, warum das für deine Websiten unverzichtbar ist? Dann schau mal hier.

„Krack" (Key Reinstallation Attack) ist der Begriff, unter dem sich Angreifer in jede Verbindung hacken können, die mit dem Sicherheitsstandard WPA2 (Wi-Fi Protected Access) verschlüsselt sind. Nahezu alle Netzwerke sind damit abgesichert. Darunter fallen alle Geräte, die sich über einen **Router** per WLAN mit dem Internet verbinden – Smartphones, Computer, Drucker oder andere Geräte in Deinem WLAN Netzwerk.

Klient
oder **Client** bezeichnet eine Anwendung bzw. ein Computerprogramm, das in einem Netzwerk den Dienst eines Servers (Zentralrechner) verwendet und mit diesem kommuniziert und Daten überträgt. So ein Client ist zum Beispiel ein Webbrowser, wie Chrome oder Mozilla.

Patch – ist eine Nachbesserung bzw. Korrektur für Software und Daten. Diese wird unter anderem ausgegeben, um bekanntgewordene Sicherheitslücken wie den Krack Angriff zu lösen. Durch Patches können Funktionen nachgerüstet werden. Bei Windows Microsoft heißen diese Patches zum Beispiel Service Pack. Änderungen die durch solche Patches bei Betriebssystemen durchgeführt werden, finden häufig ohne das Wissen des Nutzers statt.

Passphrase – hier handelt es sich um ein besonders sicheres Passwort, welches länger ist als typische Passwörter. Oft sind solche Passphrases bis zu 100 Zeichen lang. Das BSI empfiehlt übrigens im Internet die Verwendung von Passwörtern mit mindestens zwölf Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern. Für für WLAN-Zugänge empfiehlt die IT-Sicherheitsbehörde sogar Passwörter aus mindestens zwanzig Zeichen.

Phishing sind Cyberangriffe, die zum Ziel haben, persönliche Daten eines Internet Nutzers abzugreifen und deren Identität zu stehlen. Cyberkriminelle versuchen Daten bzw. Passwörter zu „angeln", um zum Beispiel Geldkonten zu plündern. So wird beispielsweise die Sparkassen Homepage simuliert und die Daten abgegriffen, wenn der Kontonutzer diese eingibt, um sich zum Online Banking anzumelden. Die Verschlüsselung einer Website kannst Du allerdings überprüfen. Du kannst Dir die Sicherheitsinformationen zur Website ansehen. Dazu gehst Du im Google Chrome Browser auf den Sicherheitsstatus neben der Webadresse. Das kleine grüne Handtaschen Symbol zeigt Dir, ob die Verbindung sicher ist.

Sicherheitsstatus auf einer Website checken

Router

– hier handelt es sich um ein Netzwerkgerät, welches Datenpakete bzw. Netzwerkpakete zwischen mehreren Netzen und Rechnern hin und herleitet. Wir kennen den Router als Internetrouter, den wir installieren, um WLAN in unseren vier Wänden zu haben.

SSL (Secure Sockets Layer) bzw. auch bekannt unter dem aktuellen Namen
TLS (Transport Layer Security) ist ein Verschlüsselungsprotokoll bzw. ein Netzwerkprotokoll zur sicheren Übertragung von Daten. Die TLS-Verschlüsselung wird mit HTTPS eingesetzt. Es wurde von Netsape zusammen mit HTTPS entwickelt.

SSID
(Service Set Identifier) bezeichnet den Namen des Funknetzes bzw. des Heimnetzwerkes, das Du nutzt. Jeder, der seine Internetverbindung über WLAN laufen lässt, sollte wissen, was das ist. Der Name des Funknetzes wird in der Regel automatisch über den WLAN Router zugewiesen. Man kann die SSID ändern und so zum Beispiel der Verwechslung mit anderen Nutzer vorbeugen, die eine ähnliche SSID haben. Die SSID kann auch versteckt werden, um Neugierigen nicht direkt ins Auge zu fallen. Einen richtigen Schutz vor Hackern ins WLAN bietet das Verstecken des Heimnetzwerkes bzw. der SSID nicht.

WEP – der Sicherheitsstandard Wired Equivalent Privacy stellte sich schon nach kurzer Zeit als unsicher und anfällig für Hackerangriffe heraus.

WLAN
– das **Wireless Local Area Network** ist, wie der Name schon sagt, ein drathloses lokales Netzwerk bzw. ein lokales Funknetz. Mit diesem können wir drahtlos im Internet surfen, egal ob mit dem Handy, Tablet, Computer oder Smart Home Systemen. Damit das WLAN verschlüsselt und somit sicher ist und niemand die Daten anderer Internetnutzer mitlesen kann, wird dieses durch ein Sicherheitsprotokoll geschützt. WEP, WPA, WPA2 sind solche Sicherheitsprotokolle. Wenn Du mit sensiblen Daten zu tun hast und zum Beispiel Online Banking betreibst, kannst Du das WLAN beim Versenden dieser Daten auch kurzzeitig abschalten und stattdessen ein LAN-Kabel nutzen. HTTPS ist natürlich sicher.

WPA
– der Wi-Fi Protected Access ist eine Verschlüsselungstechnik für drahtloses Surfen im Internet (Wireless LAN). Hierbei handelt es sich um den Vorgänger von WPA2. WPA basiert auf dem mittlerweile als unsicher eingestuften WEP.

WPA2
ist die aktuellste Sicherheitstechnik und Nachfolger von WPA. Bei der Sicherheitstechnik wurde der vollständige 802.11i Standard umgesetzt sowie zusätzlich der Verschlüsselungsalgorithmus AES

(Advanced Encryption Standard). Momentan ist die Weiterentwicklung von WPA2 zu **WPA3** im vollen Gange, diese könnte schon im Laufe 2018 realisiert werden.

WIFI wird zwar meist als Synonym zu WLAN genutzt, dies ist jedoch falsch: Während WLAN das Funknetzwerk bezeichnet, ist WIFI die Zertifizierung durch die **Wi-Fi Alliance**. Es gibt Wi-Fi-zertifizierte Produkte, welche den **IEEE-802.11-Standards** entsprechen. Diese Produkte sind als **802.11-konform** ausgezeichnet.

WIFI Alliance – Zertifizierungsorganisation für WLAN Geräte. Die Alliance hat die Aufgabe, Produkte von verschiedenen Herstellern zu testen und zu zertifizieren. So soll die Kompatibilität zwischen verschiedenen Geräten sichergestellt werden. Die Produkte der über 300 Mitglieder der Organisation werden auf die eigenen aufgestellten Richtlinien hin getestet und erhalten das Wi-Fi-Zertifikat und das Wi-Fi-Logo. Zu den Mitgliedern gehören unter anderem Apple, Asus, Canon, T-Mobile USA, IBM, Nokia, Microsoft und Samsung.

Würmer – ein Computerprogramm, das sich böswillig über das Computernetzwerk verbreitet und sich schnell selbst vermehrt. Einen Computerwurm kann Deinen Computer befallen, wenn Du beispielsweise infizierte E-Mails öffnest. Durch den Einsatz von Virenscannern können Computerwürme in der Regel schnell entfernt werden.

Es gibt Begrifflichkeiten, die bei Dir weitere Fragezeichen hervorrufen und die Du von uns erklärt haben möchtest? Kein Problem, schreib uns in den Kommentaren – gerne nehmen wir weitere IT-Begriffe mit in unser Lexikon auf.