Datenschutz und Sicherheit

Grundlagen

mit Windows 7-10 und Internet Explorer 10-11

DSSW10IE11-G

Markus Krimm

1. Ausgabe, Juni 2015

ISBN: 978-3-86249-425-5

HERDT

2

Computerkriminalität

2.1 Cybercrime und Cyberspying

Digitale Kriminalität

Cybercrime bzw. **Cyberspying** oder Computer-/Internetkriminalität bezeichnet u. a. den Diebstahl von Nachrichten, Informationen und Daten sowie die betrügerische Verwendung von Daten. Zu dieser illegalen und strafbaren Handlung zählt u. a. das Ausspähen im privaten Bereich (Verlust der Privatsphäre), das Abfangen von Wirtschaftsdaten als Teil der Wirtschaftskriminalität, die staatliche Überwachung und Spionage sowie die Nutzung und Verbreitung von illegaler Software und sogenannten Hacker-Tools.

Unter den Begriff „Cybercrime“ fallen:

- der Computerbetrug (der vorsätzliche Betrug mittels eines Computers),
- der Betrug mittels gestohlener Kreditkartendaten und PINs (Skimming),
- die Herstellung und Verbreitung von Schadsoftware (Malware),
- die Datenmanipulation und -sabotage,
- die Nutzung illegal erworbener Software oder ihre Verbreitung (Softwarepiraterie),
- das Ausspähen politischer Gegner und staatliche Überwachungs-/Spionageprogramme.

Einladung zum Diebstahl

Es muss aber nicht ausschließlich eine grob fahrlässige oder vorsätzliche Handlung eines Mitarbeiters vorliegen. Auch die Unwissenheit einzelner Benutzer kann dazu führen, dass Daten entwendet werden oder unbeabsichtigt verloren gehen. So besteht die Gefahr, dass Mitarbeiter unwissend schädliche Programme installieren. Durch die Verwendung von Trojanern (Programmen, die das Ausspionieren eines Computersystems ermöglichen), können Hacker auf empfindliche Daten zugreifen. Auch der Einbruch in ein Funkübertragungsnetz (Bluetooth oder WLAN) oder die Sabotage des eigentlichen Netzwerks sind Optionen, um Daten auszuspionieren.

Zertifikate sind eine Art „Verpackung“ für öffentliche Schlüssel und werden von Zertifizierungsstellen ausgestellt und unterzeichnet. Durch Zertifikate wird bestätigt, dass ein öffentlicher Schlüssel einem bestimmten Besitzer eindeutig zugeordnet ist. Die Zertifikate können verschiedene Attribute enthalten und für unterschiedliche Zwecke ausgestellt werden.

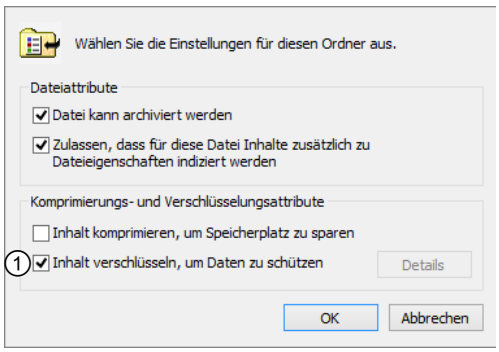
Die weitaus bekannteste Anwendung zur Public-Key-Verschlüsselung ist seit Langem das Verschlüsselungspaket PGP (Pretty Good Privacy). Sie können dieses Programm in verschiedenen Formen käuflich erwerben oder als Open-Source-Produkt kostenlos herunterladen und nutzen.

3.5 Den PC schützen

Dateien und Ordner verschlüsseln

Windows 7 - Windows 10 verfügen über ein Dateisystem, das es Ihnen ermöglicht, Dateien zu verschlüsseln. Damit lässt sich ein unbefugter Zugriff auf die Daten verhindern.

Versucht ein unbefugter Benutzer, auf die verschlüsselten Daten zuzugreifen, wird eine Fehlermeldung angezeigt. Die verschlüsselten Dateien können nur von Ihnen wieder entschlüsselt werden. Sie können mit verschlüsselten Daten genauso arbeiten wie mit unverschlüsselten Daten. Die Daten werden automatisch und von Ihnen unbemerkt im Hintergrund entschlüsselt.



- Klicken Sie (z. B. im Explorer) mit der rechten Maustaste auf die gewünschte Datei oder den gewünschten Ordner und wählen Sie *Eigenschaften*.
- Betätigen Sie im Register *Allgemein* die Schaltfläche *Erweitert*.
- Aktivieren Sie ① und bestätigen Sie zweimal mit *OK*.
- Klicken Sie auf den Eintrag *Nur Datei verschlüsseln* bzw. *Änderungen nur für diesen Ordner übernehmen*.

  oder Klicken Sie auf den Eintrag Datei und übergeordneten Ordner verschlüsseln bzw. Änderungen für diesen Ordner, untergeordnete Ordner und Dateien übernehmen.
- Bestätigen Sie abschließend mit *OK*.

  Die betreffende Datei bzw. der betreffende Ordner und sein gesamter Inhalt (Unterordner und Dateien) werden nun verschlüsselt und können nur noch von Ihnen geöffnet werden. Der Vorgang kann bei größeren Ordnern eine gewisse Zeit in Anspruch nehmen.

Diese Methode der Verschlüsselung von Dateien und Ordnern schützt Ihre Daten nicht vor dem Zugriff staatlicher Institutionen. Möchten Sie Ihre Daten und Laufwerke vor dem Zugriff staatlicher Überwachungs- oder Spionageprogramme und Hackern/Crackern wirklich schützen, nutzen Sie zur Verschlüsselung Ihrer Daten und Laufwerke das Verschlüsselungspaket **PGP** (Pretty Good Privacy).

Wenn Sie im Fenster *Erweiterte Attribute* das Kontrollfeld ① deaktivieren und anschließend zweimal mit *OK* bestätigen, machen Sie die Verschlüsselung wieder rückgängig.

Wenn Sie viele Zugangsdaten nutzen, können Sie diese mit einem professionellen Tool (sogenannten Passwort-Managern) verwalten. Ein Passwort-Manager ist ein Programm, dass alle Ihre Benutzernamen und Kennwörter/Geheimzahlen verschlüsselt in einer Datenbank speichert und diese nach Eingabe eines Passwortes abrufbar macht. Entsprechende Programme, wie z.B. *KeePas* gibt es für unterschiedliche Betriebssysteme und Plattformen. Der Nachteil des Passwort-Managers ist aber, dass der Anwender von seiner Passwort-Datenbank abhängig ist – und im Schadensfall (der Computer ist defekt) abhängig von regelmäßig erstellten Sicherheitskopien ist.

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung dient als Identitätsnachweis und kombiniert dabei unterschiedliche und voneinander unabhängige Komponenten. Dies kann am Beispiel einer Zwei-Faktor-Authentifizierung einerseits die alltägliche Komponente bestehend aus Benutzername und Passwort sein, andererseits eine weitere Komponente bestehend beispielsweise aus der Zusendung eines Einmalpasswortes via SMS.

Passwörter richtig erstellen

Vor allem mit der richtigen Auswahl des Passwortes können Sie dazu beitragen, dass das einfache Erraten der Zeichenfolge fast unmöglich wird. Je einfacher ein Passwort ist, desto leichter kann es auch herausgefunden werden.

- Erfinden Sie möglichst lange Passwörter (mindestens 12 Zeichen).
- Die Passwörter sollten aus einer Kombination von groß- und kleingeschriebenen Buchstaben, Zahlen und Sonderzeichen bestehen. (Verwenden Sie keine zeichensatzspezifischen Sonderzeichen, sondern Zeichen wie : ; , - _ (), weil manche Server andere Zeichensätze nutzen.)
- Das Passwort sollte kein bestehendes und verständliches Wort sein. Nehmen Sie beispielsweise einen Satz, den Sie sich merken können, und verwenden Sie nur die Anfangsbuchstaben der Wörter.
- Vermeiden Sie Passwörter, die mit Ihren Hobbys, der Familie etc. in Verbindung stehen.
- Ändern Sie je nach Wichtigkeit in regelmäßigen Abständen die Passwörter.
- Verwenden Sie nicht dasselbe Passwort für unterschiedliche Dienste.
- Speichern Sie keine Passwörter für den Zugang zum Internet, E-Mail- oder Firmennetz auf dem Computer.
- Wechseln Sie sofort das Passwort, wenn Ihr Passwort Dritten bekannt geworden ist.

Beispiel für ein sicheres Passwort

Eingabe	Merksatz
HM!Gwhu11UeDe?	Hallo Markus! Gehen wir heute um 11 Uhr einen Döner essen?

Im Internet können Sie auf der Website des Datenschutzbeauftragten des Kantons Zürich (*www.passwortcheck.ch*) und auf der Website des Anti-Viren-Software-Herstellers Kaspersky (*www.blog.kaspersky.de/password-check*) die Sicherheit von Passwörtern überprüfen.

4.5 Firewalls

Aufgaben einer Firewall

Der englische Begriff Firewall steht für eine Wand aus unbrennbarem Material, die in Gebäuden platziert wird, um die flächendeckende Ausbreitung von Bränden zu verhindern. Als Analogie in der Informationsverarbeitung soll eine Firewall, die sich klassischerweise an der Grenze zwischen dem eigenen Netzwerk und dem Internet befindet, die Ausbreitung von Gefahren aus dem Internet in das eigene Netz verhindern.

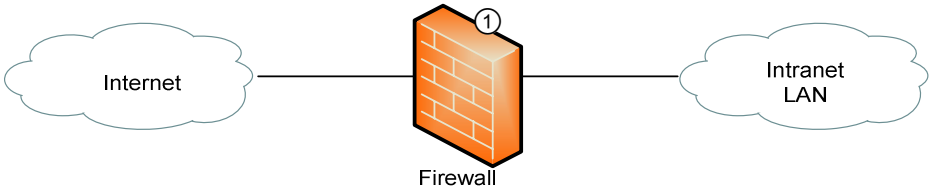
Eine Firewall ist ein System bzw. eine Gruppe von Systemen, deren Aufgabe darin besteht, die Kommunikation zu und von einem Netzwerk anhand von vorhandenen Regeln (Policys) zu kontrollieren. Beachten Sie, dass eine Firewall Regeln benutzt, um den Datenverkehr einzuschränken. Wurde eine Firewall eingerichtet, ohne dass sinnvolle Regeln erstellt wurden, ist sie relativ nutzlos.

Obwohl Firewalls gewisse Schutzmaßnahmen gegen Hacker zur Verfügung stellen können, ist ihre Existenz alleine kein Allheilmittel. In vielen Firmen wird immer noch geglaubt, mit der Anschaffung einer Firewall wären alle Sicherheitsprobleme gelöst. Dieses falsche Sicherheitsgefühl kann schlimmere Folgen haben als das Bewusstsein, keinen Schutz zu besitzen.

Firewall-Konzepte

Je nach Schutzbedarf und Topologie (Anordnung bzw. Struktur) eines Netzwerkes können eine oder mehrere Firewalls sinnvoll sein. Wichtig in allen Fällen ist jedoch, dass sämtliche Kommunikationswege in das geschützte Netzwerk hinein und aus dem geschützten Netzwerk heraus über die Firewall laufen. Das beste Firewall-Konzept wird untergraben, wenn sich hinter der Firewall im internen Netz z. B. ein Einwahlserver oder ein WLAN-Access-Point befindet, der Zugriffe von außen erlaubt. Der WLAN-Access-Point dient als Schnittstelle (elektronischer Zugangspunkt) für kabellose Geräte, z. B. für einen Computer, der auf das Internet zugreifen will.

Die einfachste Lösung besteht aus einer Firewall ①, die am Übergabepunkt vom firmeneigenen Intranet (ein nicht öffentliches Firmennetzwerk) zum Internet den Datenverkehr überwacht. Unter einem Intranet versteht



Obwohl diese Lösung relativ einfach zu realisieren ist, ist die damit erzielte Sicherheit vergleichsweise eher bescheiden. Sollte diese Firewall selbst einem Angriff zum Opfer fallen, so steht das Intranet dem Angreifer offen.

Darüber hinaus ist es problematisch, im Intranet einen Server zu betreiben, der vom Internet aus erreichbar sein soll. Wird eine Firewall so konfiguriert, dass Zugriffe von außen auf einen Server (z. B. auf einen WWW-Server) erlaubt sind, könnte dies wiederum auch ein Angriffspunkt für Hacker werden. Gelingt es einem Angreifer, Kontrolle über den WWW-Server zu erlangen, so kann dieser Zugriff auf andere Rechner im Netzwerk bekommen.

4.7 WLAN nutzen

WLANs (persönliche Hotspots) richtig nutzen

Bei der Auflistung von drahtlosen Netzwerken in der Umgebung werden stets alle sichtbaren WLANs in Reichweite angezeigt. Bei der Nutzung von drahtlosen Netzwerken müssen Sie stets die Bestimmungen Ihres Unternehmens beachten. Dies setzt vor allem voraus, dass Sie sich nur in durch Ihr Unternehmen verifizierte Netzwerke einloggen.

Haben Sie die Berechtigung und den entsprechenden Schlüssel für ein geschütztes Netzwerk, ist eine sichere Nutzung gewährleistet. Das Login in ein offenes WLAN kann dahin gehend Schaden verursachen, dass einerseits nicht sichergestellt ist, dass Dritte nicht auf Ihre lokal gespeicherten Daten zugreifen oder aber Sie Ihr Firmennetzwerk gefährden. Andererseits greifen Sie möglicherweise ohne Befugnis unwissentlich in ein bestehendes Netzwerk ein.

Persönlicher Hotspot

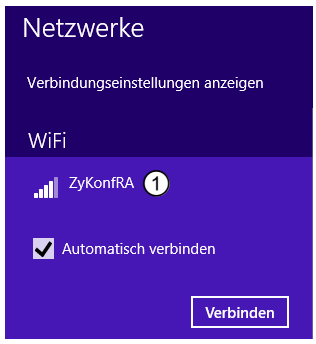
Ist kein WLAN in Reichweite, können Sie, mithilfe Ihres Smartphones oder Tablets einen persönlichen Hotspot einrichten und so mit dem Computer ins Internet gehen. Für den persönlichen Hotspot nutzen Sie dabei die mobile Datenverbindung Ihres Smartphones bzw. Tablets.

Sich mit einem WLAN unter Windows 7 - 10 verbinden

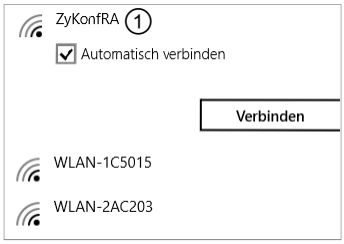
Möchten Sie sich unter Windows 7 mit einem ungeschützten bzw. geschützten WLAN verbinden, gehen Sie wie folgt vor:

- Klicken Sie nach dem Aktivieren des WLANs im Infobereich der Taskleiste unter Windows 7 auf bzw. unter Windows 8 - 8.1 auf und unter Windows 10 auf .
- Klicken Sie auf den Namen ① eines offenen bzw. geschützten WLANs und klicken Sie *Verbindung automatisch herstellen* bzw. auf *Automatisch verbinden*.
- Klicken Sie auf *Verbinden*.

WLAN unter Windows 7



WLAN unter Windows 8 - 8.1



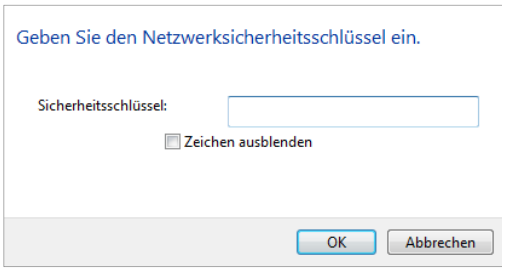
WLAN unter Windows 10

Handelt es sich um ein offenes WLAN, dessen IP automatisch vergeben wird, wird direkt eine Verbindung hergestellt.

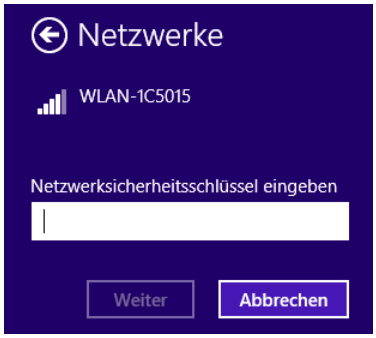
- Ist das WLAN geschützt, geben Sie unter Windows 7 im Feld *Sicherheitsschlüssel* das entsprechende Passwort ein.

  oder Tragen Sie unter Windows 8 - 10 im Feld *Netzwerksicherheitsschlüssel eingeben* das entsprechende Passwort ein.
- Klicken Sie unter Windows 7 auf *OK*.

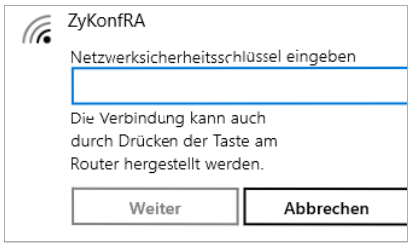
  oder Klicken Sie unter Windows 8 - 10 auf *Weiter*.



WLAN unter Windows 7



WLAN unter Windows 8 - 8.1



WLAN unter Windows 10

Unter Windows die WLAN-Verbindung trennen

- Klicken Sie im Infobereich der Taskleiste auf unter Windows 7 auf unter Windows 8 - 8.1 auf und unter Windows 10 auf .
- Klicken Sie auf den Namen des verbundenen WLANs und wählen Sie *Trennen*.

Persönlichen Hotspot unter Android aktivieren und deaktivieren

- Tippen Sie unter *Einstellungen* auf *Mehr*.
- Tippen Sie auf Tethering & mobiler Hotspot.
- Tippen Sie unter *Tethering & mobiler Hotspot* auf *Mobiler WLAN-Hotspot* bzw. auf *WLAN-Hotspot*, um den persönlichen Hotspot zu aktivieren.

Zum Deaktivieren des persönlichen Hotspots tippen Sie unter *Tethering & mobiler Hotspot* erneut auf *Mobiler WLAN-Hotspot* bzw. auf *WLAN-Hotspot*.