

Bezahlungssysteme im Netz

Bezahlsysteme im Netz

- **Paypal**

Sitz in USA, ca. 192 Mio. Nutzer, mehr als 100 verschiedene Währungen, keine Konto-Nr., Identität wird durch email Adresse definiert, hohe Verbreitung, kostenlos für Privatanwender

- **Giropay**

Entwickelt von deutscher Kreditwirtschaft, wird von Sparkassen, Postbank VoBa und Raiffeisenkassen unterstützt, basiert auf online Banking

- **Wirecard**

Zahlungsdienstleister mit Sitz im Raum München, DAX Mitglied, ermöglicht auch kontaktloses Bezahlen per NFC mittels mobile APP (ähnliche Apple Pay oder Google Pay). Prüft Kreditwürdigkeit der Kunden und garantiert Bezahlung auch bei Zahlungsausfall. Schwerpunkt ist Reisegewerbe

- **Paydirekt**

Online-Bezahlsystem deutscher Banken. Girokonto erforderlich

- **Klarna**

Online Bezahlssystem . Benutzer wird auf das Online Banking System seiner Bank weitergeleitet.

- **Banküberweisung**

Erfolgt durch Überweisungsformular, Onlinebanking . Wird von vielen Banken in unterschiedlicher Art angeboten.

- **Sofortüberweisung**

Händler Erhält sofort die Zahlungsbestätigung und gibt die Ware dann frei.

- **Kreditkarte**

Beispiele sind Master Card und Visa die direkt mit den Banken zusammenarbeiten während American Express oder Diners über die Kreditkartenfirma die Bezahlung regeln und der Kunden erhält dann Rechnung zum Begleichen.

- **Bitcoin**

Kryptowährung. Basiert auf Blockchain Technologie. Jeder Nutzer ist Teilnehmer

Wenn Sie also eines der vorher angezeigten Bezahlssysteme, oder eines welches der Dienstanbieter vorgibt, benutzen, dann gibt es nach dem:

Click  **Jetzt bezahlen**



2 Möglichkeiten

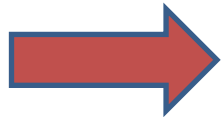
1. Sie haben alles richtig gemacht

Die Ware wird Ihnen zugestellt, oder Sie erhalten Zugriff auf einen Download oder auf eine spezielle Webseite etc.

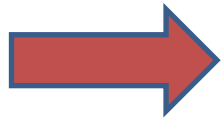
Der bezahlte Betrag wird von Ihrem Konto abgebucht.

Alles ist soweit OK

2. Folgende Probleme treten auf



Sie erhalten nichts !!!



Geld wird vom Konto abgebucht !!!



Geld zurückzubekommen ist meist aussichtslos !!!

**Damit diese soeben beschriebenen Probleme
nicht auftreten:**

**Möchte ich
über folgende Themen
Reden**

1. Digitale Identitäten

- was ist eine Digitale Identität

2. Digitale und Physische Identitäten

- wie werden diese verbunden

3. Sichere Authentifizierung

- Möglichkeiten für die sichere Anmeldung bei Web- Diensten

4. Identitätsdiebstähle

- Angriffe auf Accounts und Passwörter


5. Schutzmaßnahmen

1. Digitale Identitäten

Die virtuelle Welt im Internet wird immer größer. Unzählige Online Dienste sind verfügbar:

- **Social Media**
- **Shopping Portale (eBay, Amazone etc.)**
- **Streaming Dienste (Audio, Video)**
- **Stadtführer**
- **Vergleichsportale (Idealo, Geizhals etc.)**
- **Cloud Funktionen**

Für die Nutzung eines Dienstes müssen Sie sich

anmelden  **Registrieren**

Weil der Dienst Sie als Nutzer kennen muss:

- **Wer** kauft ein
- **Wer** bezahlt
- **Wer** lädt herunter (Musik, Video etc.)
- **Wer** postet etwas (SMS, soz. Medien, Chat etc.)

Die Registrierung bei einem Dienst erfordert auch **zusätzliche Attribute** um Personen voneinander zu unterscheiden z.B :

- **Name**
- **Adresse**
- **Geburtstag**
- **Bankverbindung**
- **Telefon Nummer**
- **etc.**

Registrierung  **Digitale Identität**

Personen können viele verschiedene Identitäten haben z.B.:

- anderer Nutzername
- andere Email-Adresse
- andere Kreditkartennummer
- Andere Telefonnummer


Auch für unterschiedliche Zwecke z.B.:

- Anonym
- Privat
- Geschäftlich

2. Digitale und physische Identitäten

Bei der Registrierung , Anmeldung bei einem Web-Dienst will dieser natürlich wissen ob die angegebenen Daten wirklich zu einer echten Person gehören.

Deshalb Verbindung von:

Digitaler Identität  **Physischer Identität**

Hierzu gibt es verschiedene Möglichkeiten:

- **Post-Ident Verfahren -> Postfiliale**
- **Videoident**
- **Neuer Personalausweis**

Als Beispiele für:

- **Videoident**
- **Neuer Personalausweis**

Wie funktioniert **Viodeoident-Verfahren**:

Voraussetzungen:

- Internet fähiger Rechner mit Kamera und Mikrofon
- Gültiges Ausweisdokument (Personalausweis oder Reisepass)
- Browser oder WebID-App

Ablauf:

- Nutzer gibt seine Daten bei Onlinedienst ein
- Danach erfolgt Weiterleitung zu WebID-Seite
- Nutzer startet VideoChat mit Person bei WebID
- Nutzer hält Ausweis in Kamera und beantwortet Fragen
- Danach übermittelt WebID das Ergebnis an Onlinedienst
- Anschließend hat Nutzer Zugang zu Onlinedienst

Wie funktioniert das **Personalausweis-Verfahren**:

Voraussetzungen:

- Neuer Personalausweis mit aktivierter Online-Funktion
- Internet fähiger Rechner und Kartenlesegerät
- Ausweis -App

Ablauf:

- Nutzer clickt bei Onlinedienst auf Login-Button
- Ausweis-App öffnet sich auf Computer
- Nutzer legt Ausweis auf Kartenlesegerät
- Ausweis-App prüft ob Dienst Berechtigung hat
- Nutzer sieht welche Daten der Dienst haben möchte
- Nutzer bestätigt die Übertragung mit PIN
- Daten werden verschlüsselt zum Dienst übertragen
- Anschließend hat Nutzer Zugang zu Onlinedienst

WebID-Verfahren:

Vorteile:

- Identifikation jederzeit möglich
- Video-Chat dauert nur wenige Minuten
- Kann man von zuhause machen
- Kein Weg zur Post erforderlich

Nachteile:

- Vertrauen in das WebID Unternehmen erforderlich
- Video-Chat Mitarbeiter erfährt persönliche Daten

Personalausweis-Verfahren:

Vorteile:

- Hoher Schutz der digitalen Identität
- Kombination aus Personalausweis und PIN (2Faktor)
- Datenübertragung erst nach PIN Eingabe
- Übertragung ist Ende-zu-Ende verschlüsselt
- Jeder hat einen Personalausweis

Nachteile:

- Kartenlesegerät erforderlich
- Erst wenige Dienste unterstützen den Personalausweis

3. Sichere Authentisierung

Eine Person muss Nachweis erbringen dass sie eine bestimmte Digitale Identität nutzen kann.

Hierzu gibt es verschiedene Möglichkeiten:

- **Wissen** -> z.B. Passwort, PIN
- **Besitz** -> z.B. Smartcard, Personalausweis
- **Biometrie** -> Fingerabdruck, Iris, Gesicht

Beispiele für sichere Authentisierung

Anmeldung bei Onlinedienst mittels **2Faktor Authentisierung**:

Ablauf

- Nutzer startet Anmeldung bei Dienst
- Nutzer gibt login-Namen an (meist email-Adresse)
- Nutzer gibt sein Passwort ein -> **1. Faktor**
- Nutzer erhält vom Dienst eine Nachricht mit Code
- Nutzer gibt den erhaltenen Code bei Dienst ein -> **2. Faktor**
- Nutzer erhält Zugriff auf den Dienst

1. Faktor = Wissen

2. Faktor = Besitz (z.B. Smartphone, Telefon etc.)

Ohne Besitz erhält der Nutzer den Code nicht

Viele Internetdienste bieten eine 2Faktor Authentisierung an:

z.B. ebay, Paypal, Banken etc.

Banken bieten oft auch einen **TAN-Generator** an der wie folgt funktioniert:

- Nutzer startet Online Banking seiner Bank
- Nutzer gibt den login Namen und das Passwort ein
- Nutzer gibt Daten für Überweisung ein
- Nutzer führt seine Bankkarte in den TAN-Generator
- TAN-Generator erzeugt eine TAN
- Nutzer gibt die erzeugte TAN in Formular ein
- Nutzer bestätigt die Überweisung

4. Identitätsdiebstähle

Wenn eine Dritte Person in Besitz der digitalen Identität eines Nutzers gelangt, kann diese alle Dienste und Ressourcen nutzen für die der Nutzer Rechte hat.

- Online Shopping**
- Banküberweisung**
- Videos ansehen**
- Medien herunterladen**
- usw.**

Identitätsdiebstahl ist für Cyberkriminelle sehr attraktiv und erfolgt meist über:

- Diebstahl der Kundendatenbank

Erbeuten von Passwörtern

- Datendiebstahl mit Malware

Spyware, Keylogger

- Phishing

Nutzer wird auf gefälschte Web-Seite gelockt

- Social Engineering

Manipulationen von Personen zur Erlangung deren Daten
(z.B. soziale Netzwerke)

Über Malware und wie man sich davor schützt und über sichere Passwörter habe ich bereits in meinem letzten Vortrag (2018) berichtet, der auf der Webseite des Internetcafe55+ zugänglich ist

<https://internetcafe55plus-suedwerk.de/vortrag-schutz-vor-schadsoftware-malware/>

5. Schutzmaßnahmen

- Hat die besuchte Web-Seite ein Impressum
- Registrierung bei einem Web-Dienst **nur mit HTTPS://**

nicht mit  HTTP://

- **Angaben bei Registrierung**
zusätzliche Angaben, Fragen bei Rücksetzung des Passworts
keine persönlichen Daten eingeben: (z.B. Vorname Mutter-> 5tZ%aX)
- **Sichere Passwörter**
Benutzung von Passwörtern mit mindestens 12 Zeichen
Groß/Kleinbuchstaben + Zahlen + Sonderzeichen
Kein Passwort aus Wörterbüchern
Regelmäßige Änderung der Passwörter (alle 3 Monate) !!

- **Keine unbekannten e-mails oder Anhänge öffnen**
Lieber beim Versender nachfragen
Vorsicht wenn Sie email erhalten dass Ihr Passwort geändert wurde, aber nicht von Ihnen
- **Immer 2 Faktor Authentisierung benutzen**
- **Achtung in öffentlichen WLAN-Netzen**
Daten können von anderen mitgelesen werden
- **Für jeden Web-Dienst ein anderes Passwort**
- **Regelmäßige Updates ihres Betriebssystems**
- **Benutzung eines aktuellen Antiviren Programms**
- **Keine Software aus unbekanntem Quellen installieren**

Anhang

Nützliche Hilfsmittel

Wurden Sie ausspioniert ?

Zur Überprüfung bei folgenden URL :
Allerdings **keine Garantie** für's Ausspionieren !!!

Identity Leak Checker (Hasso Plattner Institut Potsdam)

<https://sec.hpi.de/ilc/search?lang=de>

Have I been pwned (Australischer Sicherheitsforscher Troy Hunt)

<https://haveibeenpwned.com/>

Aufdringliche Werbung und Nachverfolgen bei Android verhindern

Für Android Smartphones und Tablets:

<https://blokada.org/de/>