Sind meine Daten in meiner Cloud sicher?

?

!

Ja, sie sind sicher!

?

!

Computeria@Horgen

26.04.2023

Ja, sie sind sicher!

Was ist zu tun, um diese Sicherheit zu erreichen?

- Zutritt zur Cloud absichern, Passwort auf Handy.
- End to End Verschlüsselung für den Transport übers Internet.
- VPN: Virtual Privat Network.

Zutritt zur Cloud absichern:

Meine persönlichen Daten für mich alleine sichtbar und nutzbar machen,

für alle anderen sperren!

Daten auf meiner Cloud sind offen, sichtbar für mich selber

Bildnachweis:
https://www.selbst.de/fensterlaeden-bauen-25854.html

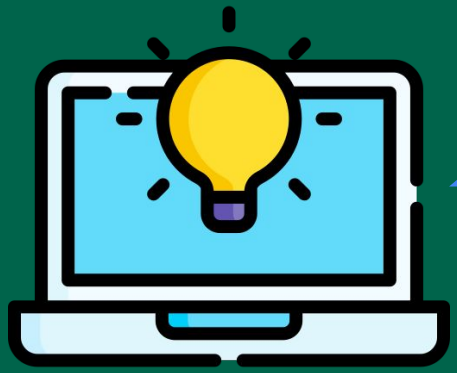
Daten auf meiner Cloud sind geschlossen für alle anderen

Bildnachweis:
https://www.selbst.de/fensterlaeden-bauen-25854.html

Computeria@Horgen

26.04.2023

Transport zur Cloud über das Internet:



?

unverschlüsselt
Sicherheit
fragwürdig

Ende zu Ende verschlüsselt
Sicherheit gewährleistet

Zutritt über Passwort (Zahlenschloss):

- Das Vorhängeschloss sichert die Tür zur Cloud.
- Der Zahlencode entspricht dem Passwort.
- Wer den Zahlencode weiterreicht, kann jeden Fremden eintreten lassen.
- Dasselbe gilt für ein Passwort!

Welche Schutzkonzepte kennen wir?
Verschlüsseln (Encryption):

Ein einzelnes Dokument wird vom Ersteller verschlüsselt und kann von niemandem eingesehen werden, auch wenn der Zutritt zur Cloud erfolgt ist. Zum Öffnen des Dokumentes (Text oder Foto oder ...) muss der Schlüssel erneut eingegeben werden.

Ein Passwort (Schlüssel) kann so aussehen: **abCD_123%&** **bgh8810$**

Möglichkeiten von Verschlüsselungen, z.B. Textseiten:

Klartext (Original)	`verschluesselt`	lesbar
Rückwärts (Pfadi Codierung)	`tlesseulhcsrev`	sicher? → nein!
Vertauschte Buchstaben Cäsar-Verschlüsselung	`wfstdimvfttfmu (v-w, e-f, r-s, ...)`	nur wenig sicher a→b, b→c, c→d,...
Enigma (siehe Enigma Wikipedia)	Verschlüsselungsmaschine WW2	sicher ? wurde geknackt !
Dokument verschlüsseln mit einem Schlüssel	ccrypt → (nächste Seite)	sicher
Zwei Schlüssel: Öffentlicher und privater Schlüssel	"openssl" auf Linux Mint: Secure Socket Layer OpenSSL Cryptography and SSL/TLS Toolkit	höchste Sicherheit

Beispiel von verschlüsseltem Foto (mit einem Schlüssel):

Im Terminal: ***ccrypt - -help***

Original: *IMG-20230326-WA0004.jpg*

ccencrypt IMG-20230326-WA0004.jpg:

ccdecrypt IMG-20230326-WA0004.jpg.cpt

Beispiel von verschlüsseltem Text (mit einem Schlüssel):

Im Terminal: ***ccrypt - -help***

Original: *test_schluessel.txt*

```
...Niemand kann den verschl..ss
elten Text lesen!
```

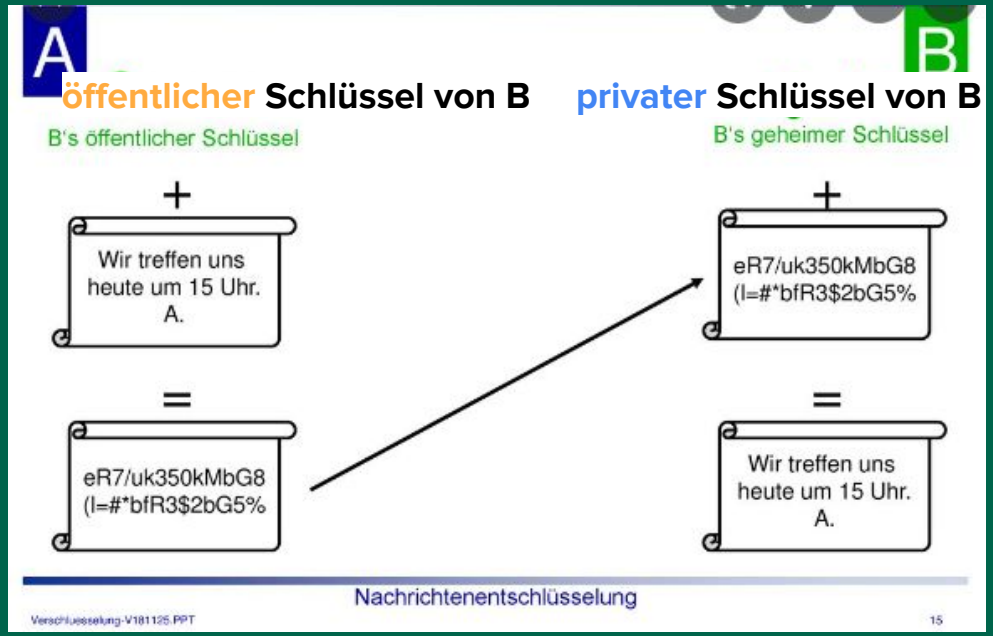
ccencrypt test_schluessel.txt.cpt

```
Q.;[....U...k........WG...f.~..
3..h..(Rr.s....B|D..6.._.uk.N..
Rk.4q......H...L{.
```

ccdecrypt test_schluessel.txt

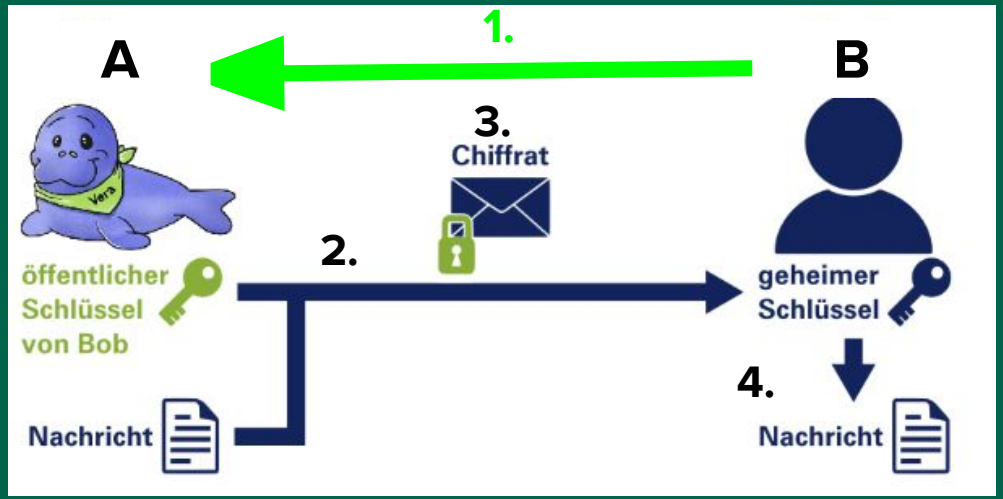
```
...Niemand kann den verschl..ss
elten Text lesen!
```

Mit einem Schlüsselpaar:
Verschlüsseln mit öffentlichem Schüssel,
Öffnen mit privatem Schlüssel

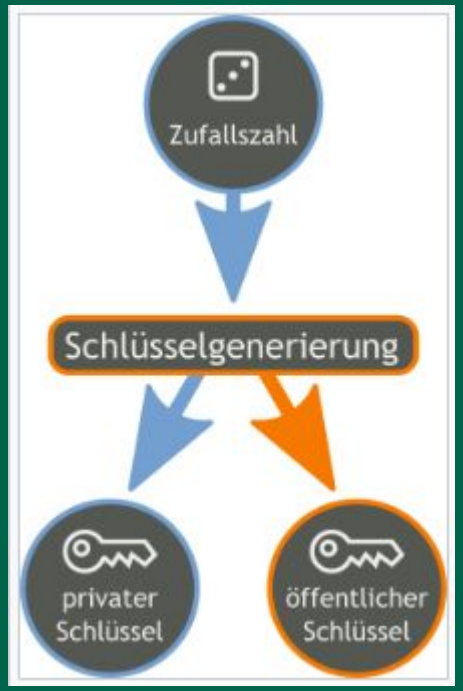


- A verschlüsselt die Botschaft mit dem öffentlichen Schlüssel.
- B entschlüsselt den unlesbaren Text mit dem privaten Schlüssel.
- Der Text ist jetzt lesbar.
- Die beiden Schlüssel können nach kurzer Zeit unwirksam gemacht werden.

1. B sendet seinen öffentlichen Schlüssel an A, behält den geheimen Schlüssel bei sich. Niemand darf den geheimen Schlüssel sehen.
2. A verschlüsselt die Nachricht mit dem öffentlichen Schüssel.
3. Niemand kann die Nachricht lesen.
4. B entschlüsselt die Nachricht mit dem geheimen, privaten Schlüssel.



Schüsselpaar generieren:



A generiert zwei zusammenpassende Schlüssel (mit openssl):

- den privaten Schlüssel, diesen muss A geheim halten.
- den öffentlichen Schlüssel, dieser darf ungeschützt versendet werden.

Siehe dazu:
Wikipedia: Schlüssel, Kryptologie

Öffentlicher Schüssel:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC7LztS43hgLutafPiQJ0Fk3ype9EeaWX4dKA/
+CUzYkhMTflrCFJGBcqs3g4NP3/
X6IwqmX4ohAHkgymoYWPxIW9ApQgZi1mXanWbtxfv3oVnHORitXswtIO+WWIOss3CcS6x8OMGhllvs+q
rE58ZutWH3UCC3DY3opwtvu3k3u8rAJ1rutMnC4ur+Lb0pySw52rwSfJPr2selrIkK8Ol9AKL+W7fHPd
vewPnO5TmRs4fzIxdd5K0iIn0pO4kT609rcAK9MOx0w+ScNtAbX84NKR3FsRzgFGyPxXNypObNKNGKmd
T2BJuWJH/NJLafn8t/
7+CeKfECqDPcrVLbX+AgiQiPYBe0Fc02jtWAxVQeRwCZFWdernMtKJ8GfOFpYEVKEvJLUbe4L6psTwvs
8XfrgGDsX1Wm1mnPHLha5GPxqRbam3AxPxqG7jp/xX5IBKevyjJq+Uzu/
+eVDGNHfz3tsd8Gx+COY8xLpTHCkkcT/
8bsjaxhjD+EEXZ19ltD4reetEh7XvnGAcrPTHxz5aAY796qINERSwKCRSn4wFL5yPqOLXTYr49MVSIDX
E6DTaMyF+vl6cN64zdsQwFDZBNzc+dvEVZI1xPb2rQ0rq1RbsXx1tMSgZ9SQ1QI7ed2249G/
eC7z4S9sGz0X3zpUj6qtTE5h20ZXDnfO/va6DiYXw== martin@martin-HP-Pavilion-All-in-
One-24-r0xx
```

Privater Schüssel:

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABAOZ02zJQ
Z/eqgBU9Amr1CLAAAAEAAAAAEAAAIXAAAAB3NzaC1yc2EAAAADAQABAAACAQC7LztS43hg
LutafPiQJ0Fk3ype9EeaWX4dKA/+CUzYkhMTflrCFJGBcqs3g4NP3/X6IwqmX4ohAHkgym
oYWPxIW9ApQgZi1mXanWbtxfv3oVnHORitXswtIO+WWIOss3CcS6x8OMGhllvs+qrE58Zu
tWH3UCC3DY3opwtvu3k3u8rAJ1rutMnC4ur+Lb0pySw52rwSfJPr2selrIkK8Ol9AKL+W7
fHPdvewPnO5TmRs4fzIxdd5K0iIn0pO4kT609rcAK9MOx0w+ScNtAbX84NKR3FsRzgFGyP
xXNypObNKNGKmdT2BJuWJH/NJLafn8t/7+CeKfECqDPcrVLbX+AgiQiPYBe0Fc02jtWAxV
QeRwCZFWdernMtKJ8GfOFpYEVKEvJLUbe4L6psTwvs8XfrgGDsX1Wm1mnPHLha5GPxqRba
```

Dazwischen liegen ca. 40 Zeilen !!!

```
54joOwCHxyl8f64gzNvVItbHoZfEjyT8QlCcxQY60wCYiqrCJbNaXmCffDusY6Tk2rin/t
f8sMcwtDXATiVKtGx4Wkrqy4+n1QDrwuru1ISgGwjlCIoGPdv2szHScW4/1uxgMtFYWW6s
/MvKqWLrn0j3k7W+9WTYuQSut2YJZ3mWe1blAJs4076mPkOLy1wT+4O88w10UOAaOp/D4c
Q8Rps0BVpK52j5/MQQzIyhCc/nnqhqLOqsSMg/aLzG0vSFJf9DjWAHemq/sWFV7bn6cw==
-----END OPENSSH PRIVATE KEY-----
```

Beide generiert mit “openssl” auf Linux Mint:

OpenSSL
Cryptography and SSL/TLS Toolkit

Neuentwicklung von Apple und Google:
Passkey statt Passwort:

- Lokal erzeugtes Schlüsselpaar (privat und öffentlich).
- Die Anmeldung und Autorisierung erfolgt ohne unser Zutun über 2-Faktor-Identifizierung, alles im Hintergrund!
- Nach erfolgreichem Einloggen wird das Schlüsselpaar gelöscht.

Passkey wird heute schon verwendet und eines Tages die Passwörter ersetzen!
Darauf freuen wir uns alle!

Chrome unterstützt jetzt Passkeys

Der Browser Chrome von Google unterstützt jetzt die Authentifizierung auf Websites mithilfe sogenannter Passkeys. Passkeys seien sicherer als Passwörter, weil sie nicht durch Phishingangriffe erbeutet werden könnten, sagt Google. Ein Passkey wird beim Besuch einer Website jeweils vom benutzten Endgerät erzeugt und verschlüsselt übertragen. Dazu muss sich der Internetnutzer lediglich an seinem eigenen Gerät anmelden - so wie er es zum Beispiel beim Entsperren des Smartphones tut. Neben Google unterstützen auch Apple, Microsoft und andere Internetkonzerne die Technik. *(hir.)*

Schweiz lagert staatliche Daten auf Server von US-Firma aus

Erstmals hat ein Bundesamt Daten auf eine ausländische Cloud hochgeladen. Weitere Bundesämter sollen folgen.

Mirko Plüss

Es sind für einmal digitale Wolken, mit denen sich Meteo Schweiz derzeit beschäftigt. Das Bundesamt für Meteorologie und Klimatologie nutzt seit kurzem eine sogenannte Cloud, wo es seine Unmengen an gewonnenen Daten ablegen kann. Wie Meteo Schweiz auf Anfrage bestätigt, hat es «meteorologische und klimatologische Daten» auf die Server des amerikanischen Cloud-Computing-Anbieters Amazon Web Services AWS geladen. AWS wurde einst als Tochterunternehmen des Internetgiganten Amazon gegründet. Es gehe bei der Auslagerung der Daten darum, «die Ausfallsicherheit der kritischen Systeme weiter zu erhöhen», führt eine Sprecherin des Bundesamts aus. Zudem sei der Schritt nötig geworden wegen «stark steigender Datenvolumen».

Für den Normalbürger längst Alltag geworden, ist die Auslagerung in eine ausländische Cloud für den Bund eine Premiere. Bisher wurden die Daten in eigenen Rechenzentren und selber betriebenen Clouds gespeichert. Letztes Jahr unterzeichnete die Bundeskanzlei dann Verträge über 110 Millionen Franken mit den vier US-Konzernen AWS, Microsoft, Oracle und IBM sowie dem chinesischen Anbieter Alibaba. Meteo Schweiz ist das erste Bundesamt, das diesen Schritt gemacht hat, heisst es bei der Bundeskanzlei. Zwei weitere Verwaltungseinheiten stünden kurz vor dem Abschluss und ein halbes Dutzend seien in Abklärung.

Die Daten werden in Sicherheitsstufen eingeteilt. Primär geht es um solche, die ohnehin öffentlich sind. In die Cloud dürfen aber auch Daten, die als «intern» klassifiziert sind, wobei die Server der ausländischen Firmen in diesem Fall zwingend in der Schweiz stehen müssen. Im Fall von Meteo Schweiz befinden sich die AWS-Server ebenfalls in der Schweiz - die Sicherheitsstufe ist nicht bekannt.

Bemerkenswert ist: Der Bund hat schon vor Monaten losgelegt, ohne entsprechende Urteile abzuwarten. Ein Bürger hatte verlangt, dass die Auslagerung vorsorglich gestoppt wird. Er scheiterte ein erstes Mal vor dem Bundesverwaltungsgericht und erst kürzlich auch vor Bundesgericht.

Pause

10 Minuten

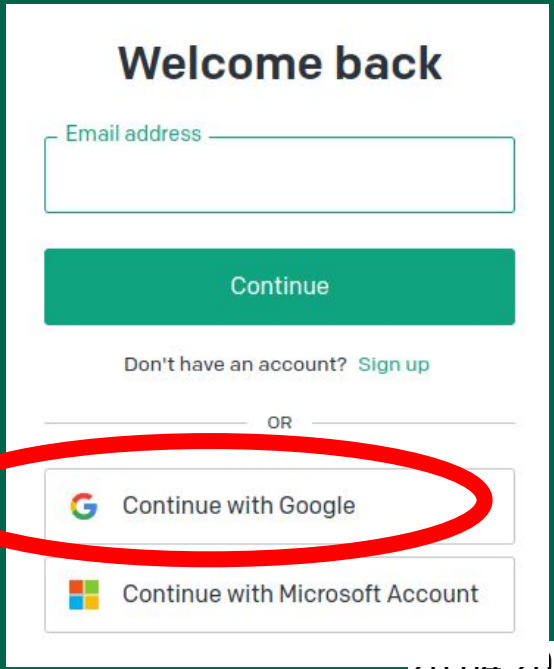
Getränke und Snacks im Foyer

Photo by Emre on Unsplash

Beispiel für passwortfreien Zugang zu Websites:

“Continue with Google” (Microsoft, Facebook, Apple)

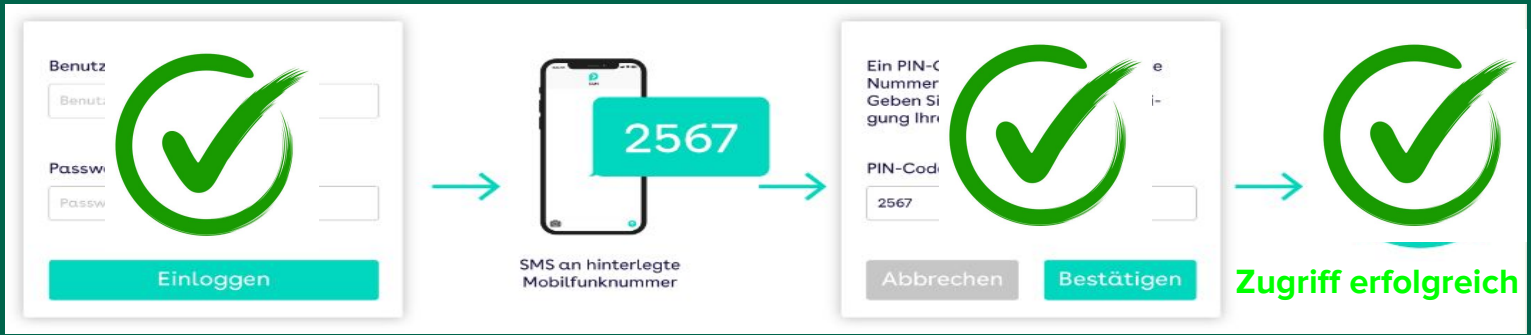
Gewisse Seiten bieten einen vereinfachten Zugang an, der aber nichts an Sicherheit einbüsst. Im Gegenteil, die Sicherheit wurde verstärkt! Der Schlüssel ist nur kurzzeitig gültig.
Beispiel:
https://chat.openai.com/auth/login
Login (vorab muss Sign Up gemacht werden)
Klick auf *Continue with Google*
Eigenes Konto auswählen
—-> Anmeldung ist erfolgt, ohne ein Passwort einzugeben! Ähnlich wie Passkey!



Wie kann die persönliche Cloud geschützt werden?

2-Faktor-Authentifikation:

Der Besitzer der Cloud hinterlegt eine Handy-Nummer.
Nach dem Einloggen schickt die Cloud einen einmaligen, kurzlebigen Code auf dieses Handy.
Der neue Code muss im PC eingegeben werden. Damit ist die berechtigte Person identifiziert. Jetzt ist der Zugriff auf die Cloud erlaubt.



2-Faktor-Authentifikation:

Nur ein Faktor: ➜ Kein Passwort?
➜ Zugriff sofort gesperrt!

Zwei Faktoren: ➜ Passwort OK! (1. Faktor)
➜ Kein Handy? Oder Code falsch! (2. Faktor)
➜ Zugriff gesperrt!

Mehrfacher persönlicher Zugriff - Volle Sichtbarkeit:

1. Einloggen vom eigenen PC, z.B. Linux
2. Einlogen vom Android-Tablet,
3. Einloggen von fremdem Windows-PC, z.B. Hotel,
4. Einloggen von Apple Mac,
5. usw.

... solange das Passwort und das vorgemerkte Handy verwendet werden, ist alles (gleichzeitig) möglich!

Alle Geräte schauen in die persönliche Cloud, nichts läuft auf der eigenen Maschine!
Änderungen werden sofort auf alle eingeloggten Geräten verteilt.

Kritische Stimmen

Oft kommt der Einwand von “zu viel Automatismen”:

Wer mit dem Handy Fotos aufnimmt, kann diese ohne sein Zutun, unmittelbar oder auch später, in der Cloud via den PC ansehen.

Auch hier: Volle und wertvolle Sichtbarkeit!

Wer die Automatismen versteht, schätzt sie!
Wer sie nicht versteht, ängstigt sich!

Wo endet die Transparenz?

Wo der Persönlichkeitsschutz im Vordergrund steht, ist Transparenz nicht sinnvoll und wird generell gesperrt. Sichtbarkeit dort wo nötig, nicht dort wo möglich!

Beispiel: Covid Zertifikat. Hier wird alles auf dem eigenen Handy gespeichert, nichts auf einer Cloud. Auch kein staatlicher Zugriff ist möglich! Lediglich die Echtheit wird auf einem zentralen Server geprüft, nicht aber der Inhalt. Das ebenfalls gültige Papier-Zertifikat beweist diesen Sachverhalt (dass es ohne Elektronik geht)!

Meine Daten sind geschützt, für Fremde unsichtbar, hingegen sind Programme offengelegt, für alle sichtbar

Es setzt sich allmählich die Erkenntnis durch, dass die sicherste Software jene ist, die allen Programmierern uneingeschränkt offen steht, eben transparent für alle ist.
Je mehr Augen hinsehen, desto mehr Lücken werden erkannt und können geschlossen werden!
"Open Source" ist ein Gewinn für die Allgemeinheit, eine grosszügige Geste des Erstellers des Programmes. Beispiel dazu sind Wikipedia, GNU-Linux, Covid-Zertifikat, (GNU heisst: GNU is Not Unix)

GNU-Lizenz wurde von Richard Stallman geschrieben.
Siehe dazu Youtube: GNU License, (Englisch)

Danke für Ihre Aufmerksamkeit!

Fragen? Wünsche?

Anregungen? Kritik? Diskussion?