

# Passwörter im Browser speichern? Bequem! Sollten Sie aber nicht tun!

**cebra GmbH - new technologies**  
Sankt Martin Str. 9, 84539 Ampfing  
Telefon: +49 8636 69 76 67  
E-Mail: [info@cebra.it](mailto:info@cebra.it)  
Webseite: <https://www.cebra.it>



## Allgemeines

Autor:	Christian Sigl
Version:	1.0
Versionsdatum:	2022-12-22

## Vorwort

Wer kennt es nicht? Passwort für eine Website (z.B. Facebook, Dropbox etc.) im Browser eingeben - man wird gefragt, ob man das Passwort im Browser speichern möchte - super! Dann muss ich es beim nächsten Login nicht erneut eintippen.

Sehr bequem, aber gefährlich!

**Anmeldeinformationen stehen im Fokus von Angreifern und werden sogar im Darknet gehandelt!**

**Das Erschreckende: Anmeldeinformationen, welche am PC z.B. in einer Remotesitzung oder im Webbrowser hinterlegt wurden, lassen sich innerhalb weniger Minuten und**

## ohne große Vorkenntnisse auslesen!

Wenn Hacker Netzwerke und Active Directory angreifen, verwenden sie gerne die immergleichen Tools und Vorgehensweisen. In den meisten Fällen „hacken“ Angreifer auch nichts, sondern sie erhalten über verschiedene Wege, zum Beispiel durch Social Engineering, die Anmeldedaten eines Benutzers. Mit denen melden sich die Hacker dann ganz normal an.

Cyberattacken basieren meistens auf dem Diebstahl von Identitäten und Anmeldeinformationen. Hinzu kommt, dass in nahezu allen Organisationen Endgeräte existieren, auf denen Anmeldeinformationen nicht ausreichend geschützt sind, zum Beispiel zwischengespeicherte Anmeldeinformationen für die Remoteeinwahl oder Login-Daten in Webbrowsern. Die recht prominente WannaCry-Ransomware ist zum Beispiel bekannt dafür, RDP-Sitzungen zu kapern.

## Hacker hacken nichts, sie melden sich einfach an

Hacker hacken also meistens nicht, sie melden sich einfach mit ergaunerten Anmeldedaten an. Erst anschließend beginnt die eigentliche Aktivität des Angreifers. Wenn er sich erfolgreich im Netzwerk positioniert hat, versucht er, an weitere Anmeldedaten zu kommen, die er mit Tools wie LaZagne, BloodHound und Mimikatz in lokalen Netzwerken abgreift. Dabei hat er immer Konten mit einer höheren Berechtigungsstufe im Fokus, bis schlussendlich auch Anmeldedaten oder Kerberostickets von Administratoren oder anderen privilegierten Konten in Active Directory vorliegen.

Die bekannte Hackerin Alissa Knight sagt dazu: „Sobald ich in einem Netzwerk eine Lücke gefunden habe, mache ich mich zunächst auf die Suche nach Domänenadministrator-Rechten, indem ich Anmeldeinformationen aus dem Speicher der Systeme auslese. Ich suche so lange, bis ich solche Rechte in einem Netzwerk finde. Und das tue ich immer!“.

Handelt es sich bei dem gekaperten Konto um ein privilegiertes Benutzerkonto, sind die Schutzfunktionen in den meisten Unternehmen bereits ausgehebelt, bevor irgendjemand etwas von dem Angriff bemerkt.

---

Revision #1

Created 22 December 2022 10:21:19 by Christian Sigl

Updated 22 December 2022 10:36:41 by Christian Sigl