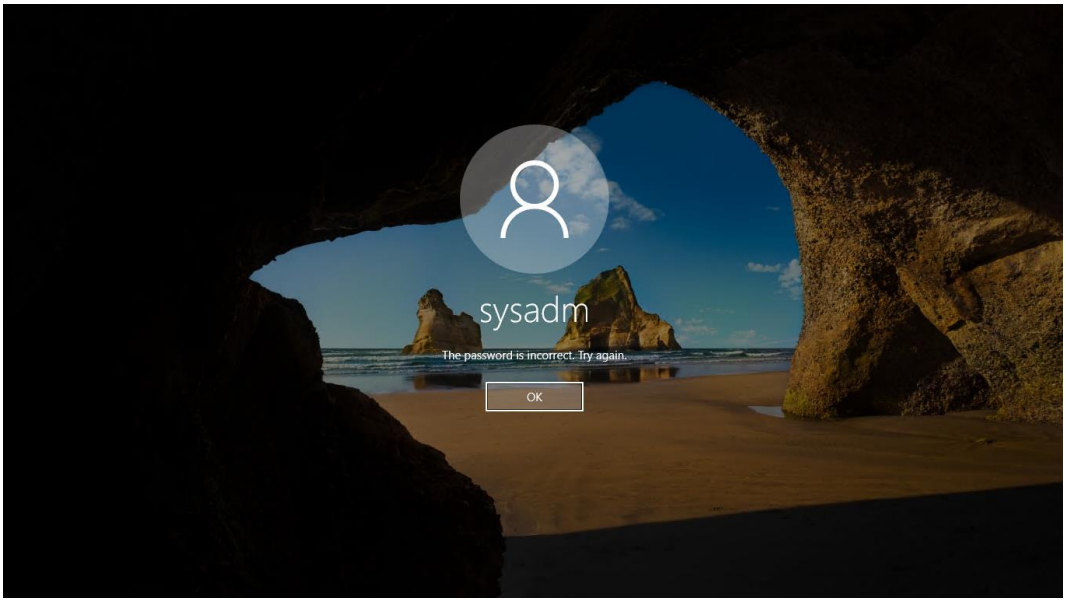
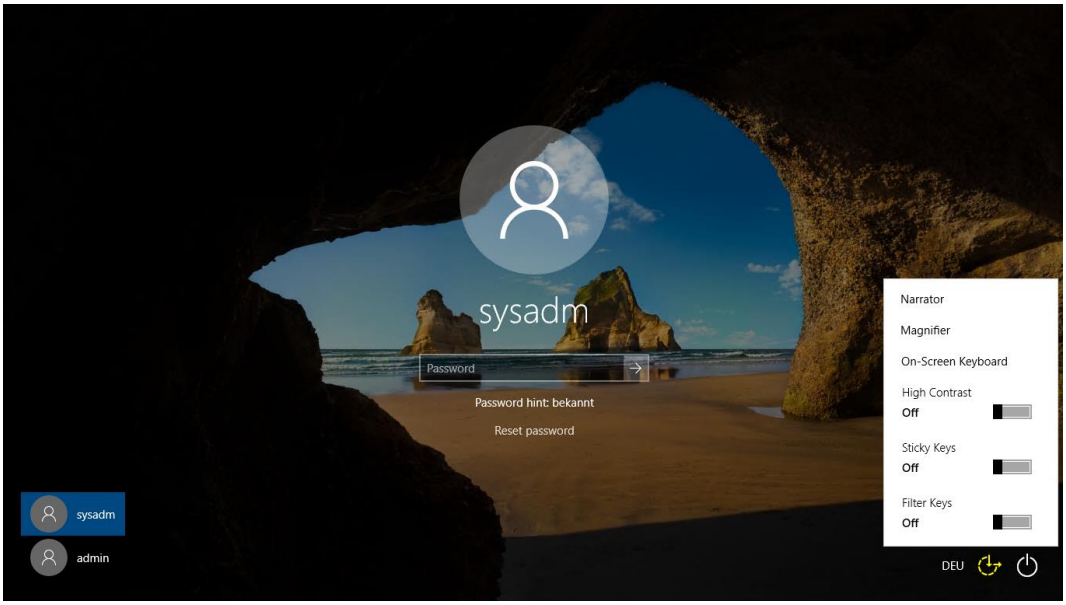
Inhalt

Szenario

Von einem wichtigen PC ist das Kennwort für alle vorhandenen Benutzer nicht mehr bekannt. Es gibt auch keine alternativen Konten, mit denen wir uns anmelden können. Und dennoch müssen wir wieder auf die Daten zugreifen:



Dieses kleine HowTo zeigt eine Option auf, die selbst mit dem heute aktuellen Windows 10 V1709 und Windows Server 2016 noch funktioniert: den UtilMan-Hack. Dabei wird das System mit einem anderen Betriebssystem gestartet und eine Datei wird ausgetauscht. Diese Datei ist eigentlich auf der Anmeldeseite für die Konfiguration des Ease Of Access gedacht:



Das interessante dabei: der Prozess wird unter maximalen Rechten gestartet. Da lässt sich einiges an Unfug mit anstellen…

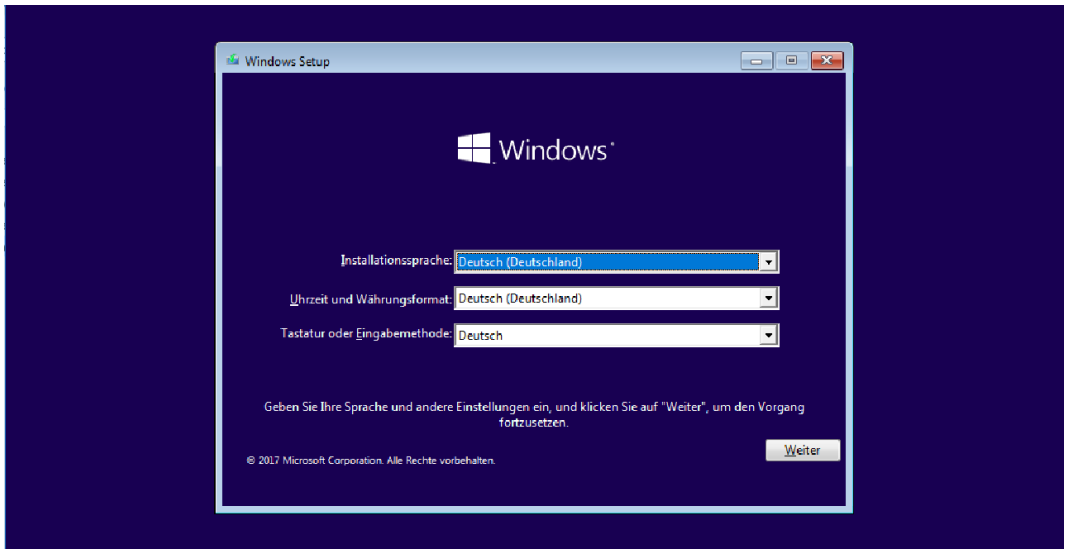
Zurücksetzen des Passwortes

Vorbereitung

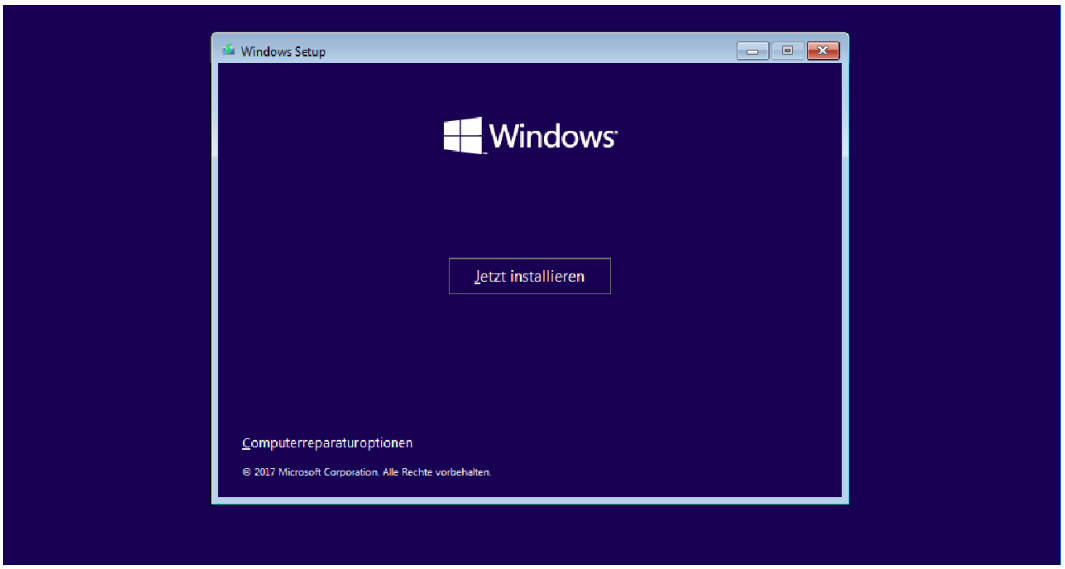
Das System wird alternativ gestartet. In meinem Beispiel verwende ich eine Installations-DVD von Microsoft Windows 10. Denkbar wäre auch

- ein Start von einem USB-Stick
- das Ausbauen der Festplatte und der Einbau in einen anderen Computer

Das System startet:



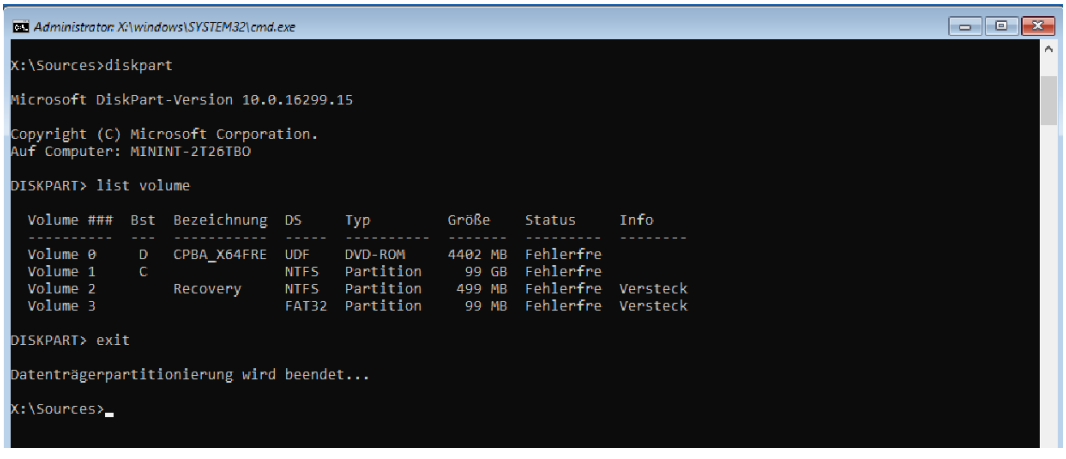
Auf der nächsten Seite verwende ich die Reparaturoption:



Weiter geht es mit der Problembehandlung:

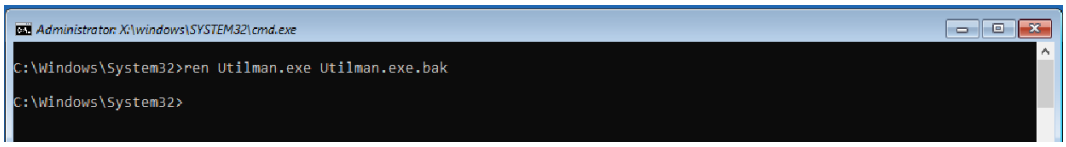
Und dann in die Eingabeaufforderung:

Nun muss die Partition mit dem betroffenen Windows Betriebssystem gefunden werden. Ein Blick mit diskpart.exe kann das schnell erledigen:

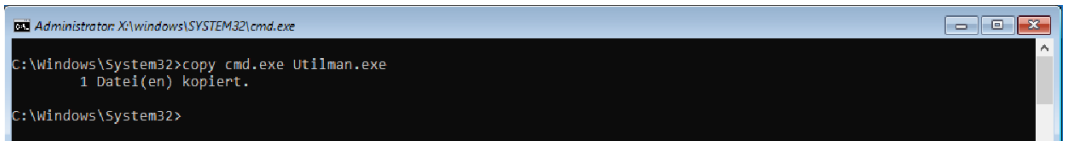


Mein Betriebssystem liegt in Volume 1 und hat den Laufwerksbuchstaben C:. Da geht's nun weiter. In C: suche ich das Verzeichnis Windows\System32 auf:

Hier benenne ich zuerst die richtige utilman.exe in utilman.exe.bak um:



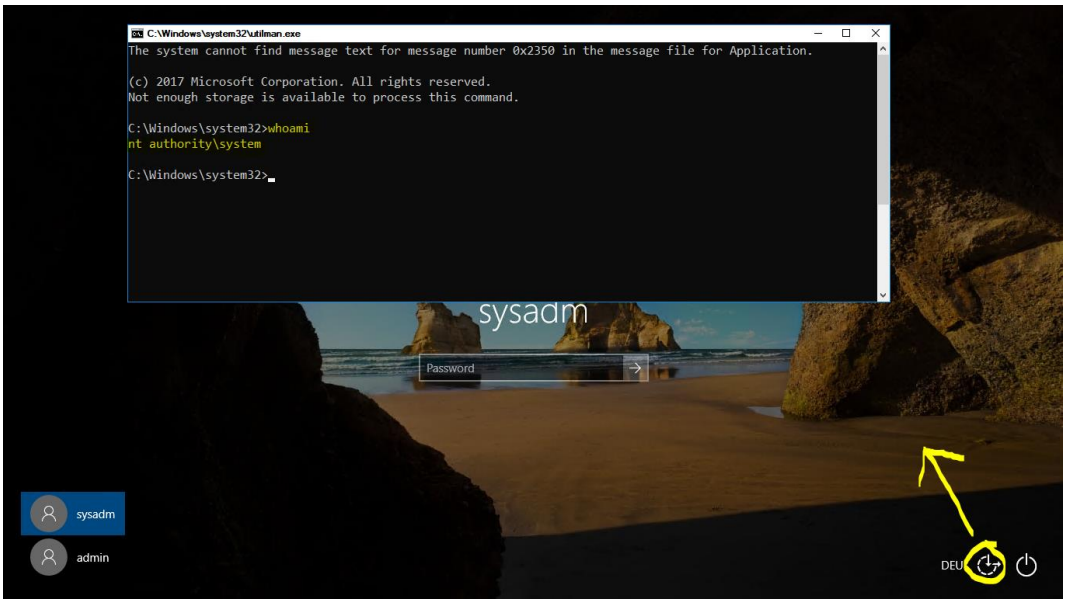
Dann kopiere ich das Tool meiner Wahl mit dem Namen utilman.exe in das Verzeichnis. Ich nehme die cmd:



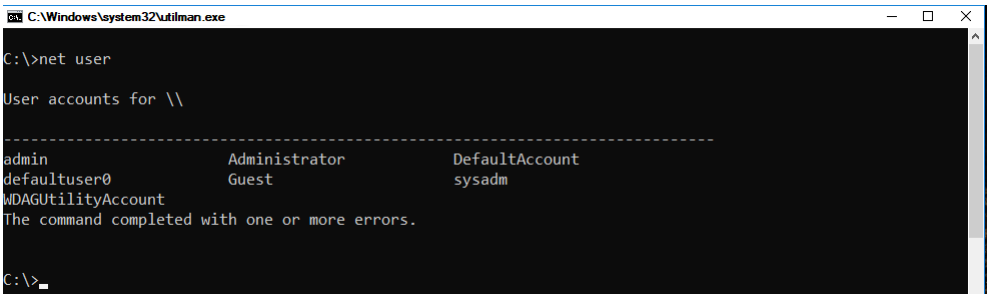
Das wars auch schon. Der Computer kann nun neu gestartet werden.

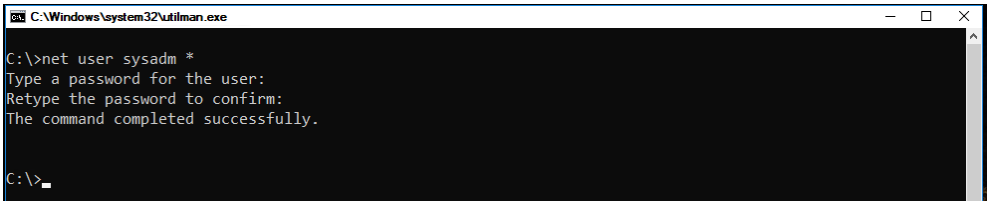
Passwortänderung

Auf der Anmeldeseite rufe ich nun den Schalter für die utilman.exe auf. Wenn dieser Schalter nun betätigt wird, erscheint eine cmd. Und diese ist sehr hoch berechtigt:



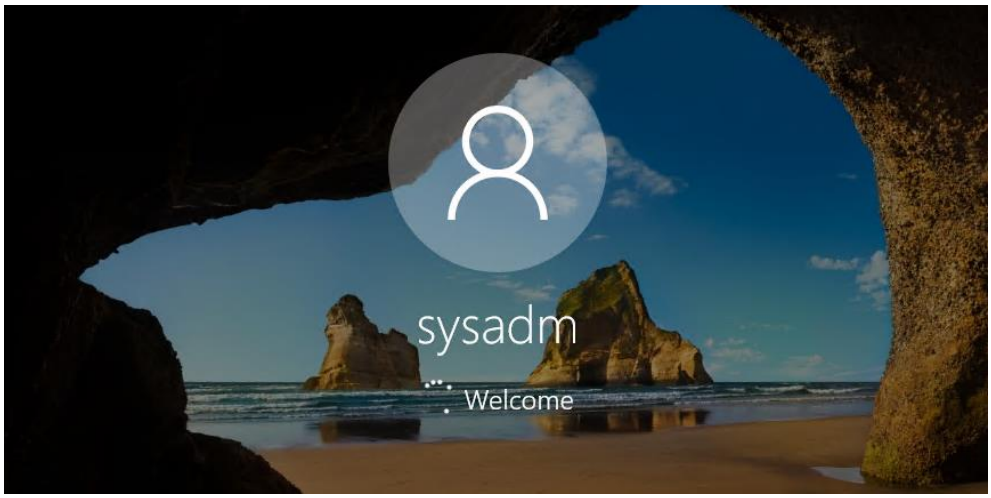
Über einfache cmd-Befehle kann nun das Kennwort der Benutzer zurückgesetzt werden:





Anmeldung mit dem geänderten Kennwort

Und nun kann ich mich mit dem neuen Kennwort anmelden:



Und ich bin drin:

Schutzmaßnahmen

Wie schützt man sich nun davor? Es gibt seit Langem die „10 unveränderbaren Gesetze der Computersicherheit“.

1	Wenn ein Angreifer dich überzeugt, sein Programm (Virus/Trojaner) auf deinem Computer auszuführen, ist es nicht mehr dein Computer
2	Wenn ein Angreifer dein Betriebssystem verändern kann, ist es nicht mehr dein Computer.
3	Wenn ein Angreifer uneingeschränkten physikalischen Zugang zu deinem Computer hat, ist es nicht mehr dein Computer
4	Schlechte Passwörter zerstören sichere Systeme
5	Ein Computer ist nur so sicher wie der Administrator, der ihn versorgt
6	Computer auf dem aktuellen Stand halten
7	Vorsichtig sein bei unbekannten Email-Anhängen
8	Daten regelmäßig sichern
9	Sensible Informationen nicht leichtfertig preisgeben
10	Aufmerksam, kritisch und informiert bleiben

Beachtet man das 3. und das 4. Gesetz, dann sollte der utilman-Hack nicht möglich sein. Das Betriebssystem müsste Microsoft verändern, um den utilman-Hack zu verhindern. Das ist bisher aber nicht passiert.

Deshalb gelten folgende Regeln:

- Lasst euren Computer nicht frei zugänglich herumstehen. Wenn jemand physikalisch darauf zugreifen kann und eine DVD oder einen USB-Stick zum Booten verwenden darf, dann hast du verloren! Ebenso könnte ein Angreifer auch einfach die Festplatte ausbauen und kompromittieren!
- Der Administrator des Systems (Ihr) muss dafür sorgen, dass die Daten eben NICHT von außen verändert werden können. Deshalb sollte man:
    - Den Zugriff auf die Startoptionen so gut es geht blockieren (z.B. mit einem UEFI-Passwort)
    - Den Betriebssystemdatenträger verschlüsseln (z.B. mit Bitlocker; es gibt aber auch Festplatten mit eingebauter Verschlüsselung)