IT-Basiswissen

- Datenmanipulation mit LibreOffice
- IT-Sicherheit
- Tastenkürzel
- VPN-Client und Einrichtung der Verbindung

Datenmanipulation mit LibreOffice

Zwei Listen auf Zellinhalt vergleichen

Problem: Herausfinden, ob ein Zellinhalt in einer anderen Spalten vorkommt.

Lösung: ZÄHLENWENN-Funktion

Beispiel:

```
=WENN(ZÄHLENWENN(B$2:B204;A2);"enthalten";"nicht enthalten")
```

Zwei Listen auf Teilstring vergleichen

```
=ISTZAHL(VERGLEICH("*" & $C2 & "*";$B:$B;0))
```

→ Gibt Wahr/Falsch aus, je nachdem, ob der Teilstring gefunden wird.

```
=(VERGLEICH("*" & $C2 & "*";$B:$B;0))
```

→ Wird der Teilstring gefunden, wird die Zeile ausgegeben, in der der Teilstring enthalten ist.

Doppelte Einträge entfernen

Problem: Doppelte Einträge aus einer Liste entfernen

Lösung: Filter setzten

- Daten > Filter > Standardfilter
- Bedingung Feldname "keiner", Bedingung "enthält".
- "Mehr Optionen" → "Keine Duplikate"

siehe: Quelle

Zusammensetzten von mehreren Zellen

Problem: Der Inhalt von zwei Zellen soll in eine Zelle geschrieben werden

Lösung: &-Operator

```
=B1&B2
```

Umbruch in Kombination mit Zusammensetzten von mehreren Zellen kombinieren

Lösung: Trick mit Notepad++

1. In dem zusammengesetzten Text sollte ein Zeichen enthalten sein, welches durch den Umbruch ersetzt werden soll (zum Beispiel: #)
2. Der Text sollte dann in Notepad++ kopiert werden, dabei muss der Text in Anführungszeichen gesetzt werden
3. Danach kann das gesetzte Zeichen mit Suchen und Ersetzen durch "\n" ersetzte werden (Reguläre Ausdrücke müssen aktiviert sein)
4. Danach kann der Text wieder in die CSV oder ODS-Datei eingefügt werden

Prüfen, ob eine Zelle leer ist

Problem: Zusammensetzten von Kunden oder Artikelnamen aus mehreren Zeilen

Lösung: ISTLEER-Funktion

```
=WENN(ISTLEER(C2);D2;WENN(ISTLEER(D2);C2;C2&", "&D2))
```

Prüfen, ob der Inhalt einer Zelle in einer anderen Zelle enthalten ist

Lösung: SUCHEN-Funktion

```
=WENN(SUCHEN(C2;B2);B2;B2&"[["&C2&"]]")
```

Informationen aufteilen, aus eins mach zwei!

Problem: Mehrere Informationen sind in einer Zelle enthalten, Informationen werden für den Import aber in mehreren Spalten benötigt

Beispiel: Vorwahl von Telefonnummern (06233/12345) oder PLZ und Stadt (67227 Frankenthal)

Lösung: LINKS-RECHTS-Funktion in Kombination mit SUCHEN bzw. LÄNGE

```
=LINKS(A2;SUCHEN("/";A2)-1)
=RECHTS(A2;LÄNGE(A2)-SUCHEN("/";A2))
```

Blockweise durchnummerieren

Problem: Mehrere Informationen müssen abhängig von einer Variablen durchnummeriert werden.

Beispiel: mehrere Kundenpreise für einen Artikel

Lösung: WENN-DANN-Funktion:

```
=WENN(B3=B2;D2+1;1)
```

Doppelte Einträge farblich markieren

Spalte auswählen und bedingte Formatierung aufrufen, "Zellwert ist" und "mehrmals vorhanden" auswählen.
Vorlage verwenden: "Error"

oder:

Die zu markierende Spalte auswählen und die bedingte Formatierung aufrufen. Als Bedingung 1 "Formel ist" auswählen und folgende Formel hinterlegen:

```
=ZÄHLENWENN($A$1:$A$5000;A1)>1
```

"A" durch die entsprechende Spalte ersetzen.

Prüfen, ob Textteil auch in andere Zelle enthalten ist

Problem: Artikelnummer muss auch innerhalb einer anderen Zelle enthalten sein.

Lösung:

```
=SUCHENB(A1;B1)
```

Zellen mit Zeilenumbruch zusammensetzen

Problem: Inhalte aus 2 Spalten gehören mit einem Zeilenumbruch verbunden. z.B. Mehrzeilige Artikelbeschreibung

Lösung:

```
=A1&Zeichen(10)&B1
```

Zeichen(10) = Zeilenumbruch

Hochkomma vor Zahlen/Daten entfernen

Problem: Beim Öffnen von CSV-Dateien oder Kopieren von Daten aus anderen Dokumenten werden Zahlen oder Daten manchmal in der Art '8173, mit vorangestelltem Hochkomma eingefügt. So können keine Rechenoperationen oder Formeln genutzt werden und die

Sortierung ist nicht numerisch, sondern Alphanumerisch ("8" > "10")

Lösung: Über Suchen und Ersetzen mit folgender Formel kann das Hochkomma entfernt werden:

```
Feld Suchen: ^.*$
Feld Ersetzen: &
```

```
Checkbox "Regex" aktivieren
```

Leerzeilen am Anfang eines Textes entfernen

Lösung: Über Suchen und Ersetzen mit folgender Formel können Leerzeilen am Anfang von Texten entfernt werden

```
Feld Suchen: ^\s+
Feld Ersetzen: leer
Checkbox: "Regex" aktivieren
```

Für Leerzeilen am Ende zum Suchen: \s+$ nutzen

IT-Sicherheit

IT-Sicherheit spielt in der heutigen vernetzten Welt eine entscheidende Rolle. Für normale PC-Benutzer ist es wichtig, ihre persönlichen Daten und Informationen vor Cyberangriffen und anderen Bedrohungen zu schützen. Dieser Artikel soll einen Überblick über grundlegende IT-Sicherheitskonzepte und bewährte Praktiken geben, die PC-Benutzer befolgen können, um ihre Online-Sicherheit zu verbessern.

Was ist IT-Sicherheit?

IT-Sicherheit bezieht sich auf den Schutz von Computersystemen und Netzwerken vor unerlaubtem Zugriff, Missbrauch, Datenverlust oder Schäden. Sie umfasst verschiedene Maßnahmen und Technologien, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen zu gewährleisten.

Warum ist IT-Sicherheit wichtig?

IT-Sicherheit ist wichtig, da sich die meisten Menschen in irgendeiner Weise mit Computern und dem Internet verbinden. Ohne ausreichenden Schutz können persönliche Informationen wie Passwörter, Bankdaten, E-Mails und private Fotos in die falschen Hände geraten. Cyberkriminelle können diese Informationen für betrügerische Aktivitäten nutzen, wie zum Beispiel Identitätsdiebstahl, finanzielle Betrügereien oder den Zugriff auf sensible Daten.

Tipps zur Verbesserung der IT-Sicherheit

1. Verwenden Sie starke Passwörter

Verwenden Sie für Ihre Online-Konten starke Passwörter, die aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Vermeiden Sie einfache und leicht zu erratende Passwörter wie "123456" oder "Passwort". Verwenden Sie für jeden Dienst ein einzigartiges Passwort und aktualisieren Sie sie regelmäßig. Unterstützend wird die Verwendung eines Passwortmanagers wie z.B Keepass, Bitwarden, 1Password oder Lastpass empfohlen.

2. Aktualisieren Sie Ihre Software regelmäßig

Halten Sie Ihr Betriebssystem, Ihren Webbrowser, Ihre Antivirensoftware und andere Programme auf Ihrem Computer immer auf dem neuesten Stand. Software-Updates enthalten oft wichtige Sicherheitspatches und Fehlerbehebungen, die Ihre Systeme vor bekannten Schwachstellen schützen.

3. Vorsicht bei E-Mail-Anhängen und Links

Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen oder dem Klicken auf Links in E-Mails, insbesondere von unbekannten Absendern. Diese können schädliche Software enthalten oder zu gefälschten Websites führen, die darauf abzielen, Ihre Daten zu stehlen. Überprüfen Sie immer die Echtheit der Quelle, bevor Sie Anhänge öffnen oder Links folgen.

4. Verwenden Sie eine Firewall und Antivirensoftware

Installieren Sie eine zuverlässige Firewall und eine aktuelle Antivirensoftware auf Ihrem Computer. Eine Firewall schützt Ihren Computer vor unerlaubten Zugriffen aus dem Internet, während eine Antivirensoftware schädliche Programme erkennen und entfernen kann. Halten Sie diese Programme stets auf dem neuesten Stand und führen Sie regelmäßig Scans durch.

5. Sichern Sie Ihre Daten regelmäßig

Erstellen Sie regelmäßige Backups Ihrer wichtigen Dateien und Daten. Speichern Sie diese Backups an einem sicheren Ort außerhalb Ihres Computers, beispielsweise auf einer externen Festplatte oder in der Cloud. Dadurch können Sie Ihre Daten wiederherstellen, falls Ihr Computer beschädigt wird oder Daten verloren gehen.

6. Seien Sie vorsichtig in sozialen Netzwerken

Seien Sie in sozialen Netzwerken vorsichtig mit den Informationen, die Sie teilen. Stellen Sie sicher, dass Ihre Privatsphäre-Einstellungen angemessen konfiguriert sind und dass Sie nur vertrauenswürdige Kontakte hinzufügen. Teilen Sie keine sensiblen Informationen wie Ihre Telefonnummer, Adresse oder finanzielle Details öffentlich.

Meldepflicht im Falle eines erfolgreichen Cyberangriffs

Eine wichtige Komponente der IT-Sicherheit für Unternehmen ist die Meldepflicht im Falle eines erfolgreichen Cyberangriffs. In vielen Ländern gibt es Gesetze und Vorschriften, die Unternehmen dazu verpflichten, bestimmte Arten von Datenschutzverletzungen oder Sicherheitsvorfällen innerhalb einer bestimmten Frist zu melden. Eine gängige Frist beträgt 72 Stunden.

> Genauere Informationen und Unterstützung im Falle eines Cyberangriffs finden Sie hier: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

Was ist die Meldepflicht?

Die Meldepflicht ist eine rechtliche Anforderung, die Unternehmen dazu verpflichtet, Sicherheitsvorfälle oder Datenschutzverletzungen an die zuständigen Behörden oder

Aufsichtsorgane zu melden. Diese Vorschriften sollen dazu beitragen, den Schutz personenbezogener Daten und die Transparenz bei Sicherheitsvorfällen zu gewährleisten.

Warum besteht eine Meldepflicht?

Die Meldepflicht dient mehreren Zwecken. Erstens ermöglicht sie den Behörden, angemessene Untersuchungen durchzuführen und mögliche Verstöße gegen Datenschutzgesetze zu verfolgen. Zweitens ermöglicht sie es den Betroffenen, informiert zu werden und gegebenenfalls geeignete Maßnahmen zum Schutz ihrer Daten zu ergreifen. Schließlich trägt die Meldepflicht auch zur Schaffung eines Bewusstseins für die Bedeutung von IT-Sicherheit bei Unternehmen bei und fördert bewährte Praktiken im Umgang mit Sicherheitsvorfällen.

Was muss gemeldet werden?

Die genauen Details dessen, was gemeldet werden muss, variieren je nach Land und Rechtsprechung. In der Regel müssen Unternehmen jedoch Sicherheitsvorfälle oder Datenschutzverletzungen melden, die zu einem Verlust, Diebstahl oder Zugriff auf personenbezogene Daten führen können. Dazu gehören beispielsweise Datenpannen, bei denen Kundendaten, Benutzernamen und Passwörter, Kreditkarteninformationen oder andere vertrauliche Informationen kompromittiert wurden.

72-Stunden-Frist

Die 72-Stunden-Frist ist eine weit verbreitete Vorgabe für die Meldung von Sicherheitsvorfällen oder Datenschutzverletzungen. Innerhalb dieser Frist müssen Unternehmen den Vorfall den zuständigen Behörden oder Aufsichtsorganen melden. Es ist wichtig, dass Unternehmen diese Frist ernst nehmen und sicherstellen, dass sie über die erforderlichen Prozesse und Ressourcen verfügen, um innerhalb dieser Frist angemessen zu reagieren.

Strafen bei Nichteinhaltung

Die Nichteinhaltung der Meldepflicht kann zu rechtlichen Konsequenzen führen. Unternehmen können mit Geldstrafen belegt werden, und in einigen Fällen können auch strafrechtliche Sanktionen gegen Einzelpersonen verhängt werden. Die genauen Strafen variieren je nach Land und den spezifischen Umständen des Vorfalls.

Tastenkürzel

Windows

Tastenkombination	Funktion
F2	Gewählte Datei umbenennen
Alt + Tab	Zwischen offenen Anwendungen umschalten
Alt + F4	Aktuelle Anwendung schließen
Alt + ← oder →	Vor- oder zurückspringen im Browser-Verlauf
Win + Zahl	Öffnen der entsprechenden Anwendung aus der Schnellstartleiste
Win + Shift + Zahl	Neue Instanz der entsprechenden Anwendung aus der Schnellstartleiste öffnen
Strg + Win + D	Neuen virtuellen Desktop starten
Strg + Win + F4	Aktuellen virtuellen Desktop schließen (Nur bei mehreren offenen)
Strg + Win + ←/→	Zwischen aktiven virtuellen Desktops wechseln
Strg + A	Gesamten Text im aktiven Feld markieren
Strg + C	Markierten Text in die Zwischenablage kopieren
Strg + X	Markierten Text ausschneiden und in die Zwischenablage kopieren
Strg + V	Text aus der Zwischenablage einfügen
Strg + Shift + T	Letzten geschlossenen Tab wieder öffnen
Win + A	Windows Benachrichtigungen öffnen
Win + L	PC sperren

Win + D	Alle aktiven Fenster minimieren

In Eingabefeldern

Tastenkombination	**Funktion**
Strg + Backspace	Zeichenkette bis zum letzten Sonder- oder Leerzeichen löschen (Löschung nach links ab Cursorposition)
Strg + Entf	Zeichenkette bis zum nächsten Sonder- oder Leerzeichen löschen (Löschung nach rechts ab Cursorposition)
Strg + ← oder →	Cursor bis zum nächsten Sonder- oder Leerzeichen nach links oder rechts bewegen
Strg + A	Gesamten Text im aktiven Feld markieren
Strg + C	Markierten Text in die Zwischenablage kopieren
Strg + X	Markierten Text ausschneiden und in die Zwischenablage kopieren
Strg + V	Inhalt der Zwischenablage in das aktive Feld kopieren
Strg + Shift + ← oder →	Text bis zum letzten oder nächsten Sonder-/Leerzeichen markieren (Ab Cursorposition)
Shift + ← oder →	Text nach links oder rechts zeichenweise markieren
Strg + Z	Letzte Aktion (Einfügen oder Löschen) im Textfeld rückgängig machen

Browser

Tastenkombination	**Funktion**
Pos 1	An den Anfang der Seite springen
Ende	Ans Ende der Seite springen
Space	Nach unten scrollen (Nicht wenn Cursor in Textfeld)
Alt + ← oder →	Vor oder Zurück

Strg + F	Suche auf Seite
Strg + Bild hoch oder Bild runter	Tab nach rechts oder links wechseln
Strg + Tab	Tab nach rechts wechseln
Strg + Shift + Tab	Tab nach links wechseln
Strg + W	Aktiven Tab schließen
Strg + Shift + T	geschlossenen Tab wiederherstellen
Tab	Zum nächsten Eingabefeld springen
Shift + Tab	Zum vorherigen Eingabefeld springen
Strg + R oder F5	Neuladen der Browserseite
Strg + Shift + R	Seite ohne Cache neu laden
Strg + J	Auflistung der heruntergeladenen Dokumente
Strg + Shift + Entf	Öffnet ein Pop-up, um den Cache zu entfernen

Im ERP

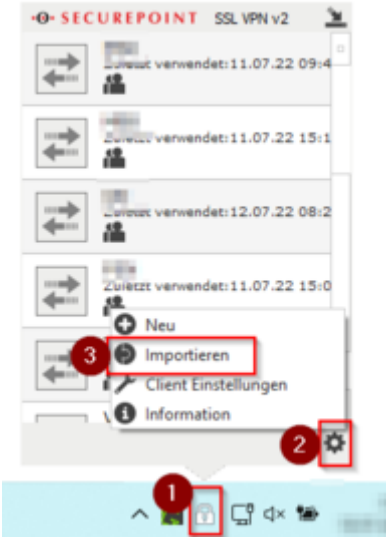
Tastenkombination	Funktion
Alt + S	Dokument / Datensatz speichern
Alt + P	Druckdialog aufrufen
Alt + V	Druckdialog für Vorschau aufrufen

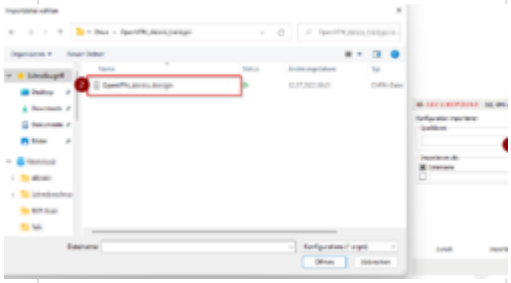
VPN-Client und Einrichtung der Verbindung

Dieser Artikel behandelt die Einrichtung und Nutzung der VPN-Clients SecurepointSSL-VPN-Client unter Windows und des Gnome NetworkManagers unter Linux (Ubuntu/Debian).

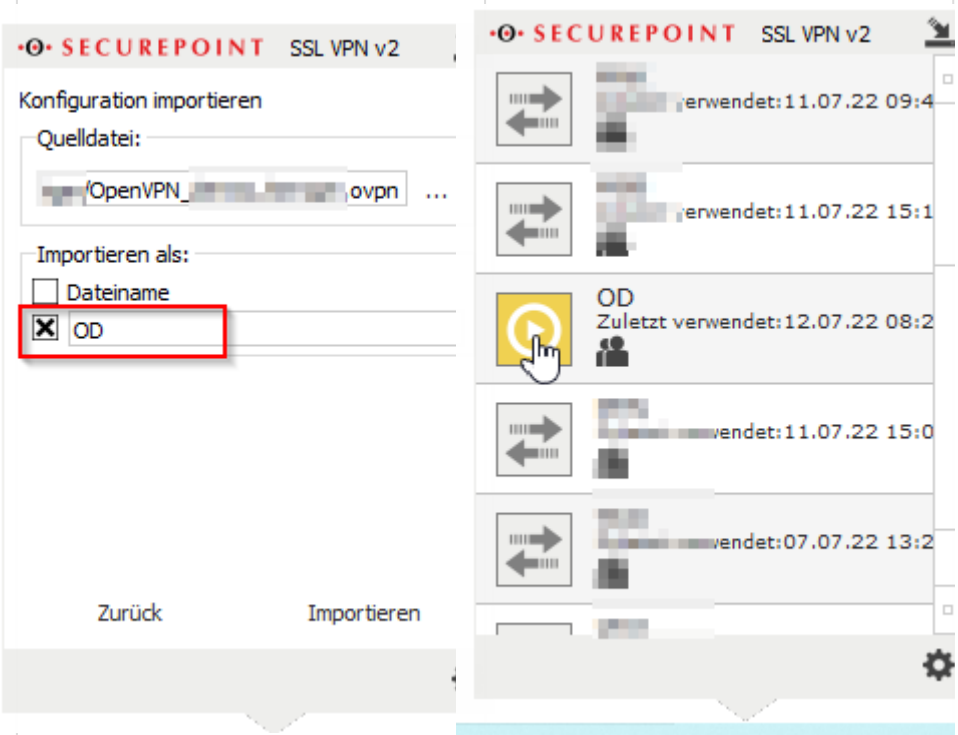
Windows

Wenn SecurepointSSL-VPN-Client installiert und gestartet wurde, kann das Menü durch Doppelklick auf das Schloss-Symbol geöffnet werden.
In der Übersicht auf das Zahnrad klicken und im Menü den Punkt "Importieren" auswählen. Im Anschluss die "..." Schaltfläche betätigen und die erhaltene OVPN-Datei für den Import auswählen.





Im nächsten Fenster de
Dateinamen festlegen und m
der Schaltfläche "Importiere
den Import beenden.
Im Anschluss wird die Verbindu
durch Klick auf den "Play-Butto
hergestellt.
In den darauffolgenden Dialoge
den eigenen Benutzernamen ur
Passwort angeben. Sollen d
Zugangsdaten gespeiche
werden, muss der Haken geset
werden.



Ubuntu/Debian - Gnome

Sicherstellen, dass alle benötigten Pakete installiert sind:

```
sudo apt update && sudo apt install network-manager-openvpn-gnome -y
```

Import der OVPN-Datei:

```
nmcli connection import type openvpn file [VPN.ovpn]
```

Fehlerbehebung/Workaround in neueren Ubuntu/Debian-Versionen

In der Datei `/etc/ssl/openssl.cnf` die folgenden Zeilen einkommentieren/einfügen:

```
[openssl_init]
providers = provider_sect

[provider_sect]
default = default_sect
legacy = legacy_sect

[default_sect]
activate = 1
```

```
[legacy_sect]
activate = 1
```