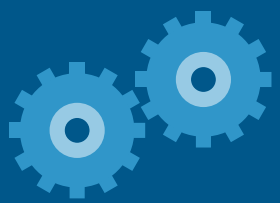
GRUNDEINSTELLUNGEN – FÜR EINEN SICHEREN ARBEITSPLATZ

LERNEINHEIT 1



Berufsschüler BOTTOM-UP! für IT-Sicherheit

DIE THEMEN:

1. IT-SICHERHEITSRISIKEN: VIREN, TROJANER UND CO.
2. ABWEHR VON SCHADSOFTWARE
3. VORKEHRUNGEN FÜR DIE SICHERHEIT BEI BROWSER UND SOFTWARE
4. 123456? DAS SICHERE PASSWORT IM ARBEITSALLTAG
5. ZUSAMMENFASSUNG

1. IT-SICHERHEITSRISIKEN: VIREN, TROJANER UND CO.

SCHADPROGRAMM/SCHADSOFTWARE/MALWARE

schleust sich in andere Programme und Daten ein, und führt diverse Schadfunktionen aus.

COMPUTERVIREN

sind selbstverbreitende Programme, die sich selbst in andere Programme oder Dateien einschleusen und sich dadurch reproduzieren.

WÜRMER

suchen aktiv nach Sicherheitslücken und richten meist unbemerkt Schaden an.

TROJANISCHE PFERDE

sind vermeintlich nutzvolle Software – im Hintergrund laufen nicht sichtbare schädliche Funktionen.

1. IT-SICHERHEITSRISIKEN: VIREN, TROJANER UND CO.

VERBREITUNGSWEGE VON VIREN

WECHSEL-DATENTRÄGER

NETZWERKE

E-MAIL (-ANHÄNGE)

DOWNLOADS

INFIZIERTE WEBSEITEN

INSTANT MESSENGER

1. IT-SICHERHEITSRISIKEN: VIREN, TROJANER UND CO.

HINWEISE AUF EINEN MÖGLICHEN VIRENBEFALL

> Der Computer wird immer langsamer,

> Funktionen, die vorher funktioniert haben, laufen nicht, Dateien verschwinden,

> Abstürze häufigen sich,

> der Computer reagiert komisch und zeigt merkwürdige Meldungen.

2. ABWEHR VON SCHADSOFTWARE

ANTIVIRENPROGRAMM: VIRENSCANNER

Kann Schadsoftware aufspüren, blockieren und ggfs. beseitigen **nachdem** die Malware ins System gelangt ist.

IDEAL	Scanner entfernt Virus aus befallener Datei („Reinigung“ oder „Reparatur“).
ALTERNATIVEN	Löschen der befallenen Datei > Dateiinhalte gehen verloren Quarantäne > befallene Datei wird isoliert

2. ABWEHR VON SCHADSOFTWARE

FIREWALL

Verhindert das Eindringen von Schadsoftware bevor diese es von außerhalb in das System und auf den Rechner schaffen kann.

Die Firewall kann

> nur präventiv schützen

> nicht aktiv in die Virenvernichtung eingreifen

> nur ein Teilaspekt eines Sicherheitssystems sein

2. ABWEHR VON SCHADSOFTWARE

ZUSÄTZLICHE VIRENSCHUTZ-TIPPS

- ✓ Keine E-Mails mit unbekannten Anhängen öffnen!
- ✓ Nicht mit Admin-Rechten im Internet surfen!
- ✓ Regelmäßige Aktualisierung des Virenschutzprogrammes!
- ✓ Sichere Passwörter nutzen!
- ✓ Vorsichtig sein mit fremder Software und Dateien von Kunden oder Geschäftspartnern!

3. VORKEHRUNGEN FÜR DIE SICHERHEIT BEI BROWSER UND SOFTWARE

Wichtig: Softwareaktualisierung

> Hersteller veröffentlichen Updates, sobald sie eine potenzielle Schwachstelle im Programmcode ihrer Software entdecken.

> z.B. für Betriebssysteme, E-Mail-Programme, Bild- und Textverarbeitungsprogramme u.v.m.

Zu beachten:

> direkt über die Programme oder per Download auf der Webseite des Anbieters herunterladen!
> Vorsicht bei Pop-ups auf Webseiten über vermeintliche Updates: Betrugsversuch! Viren!
> Bei unnötigen Berechtigungsanfragen misstrauisch werden!

3. VORKEHRUNGEN FÜR DIE SICHERHEIT BEI BROWSER UND SOFTWARE

Plug-ins als Erweiterungen für mehr Sicherheit beim Surfen

> zum **Unterdrücken von Skripten** wie Flash und JavaScript(verbreiten auf unzureichend gesicherten oder kriminellen Webseiten oftmals Schadsoftware)

> zum **Kontrollieren des Trackens** des Nutzerverhaltens

> zum **Aufbauen sicherer Verbindungen** (wenn möglich)

> zum **Unterdrücken von Werbebannern** („Ad-Blocker“)

3. VORKEHRUNGEN FÜR DIE SICHERHEIT BEI BROWSER UND SOFTWARE

Sicherheitsrisiko Cookies

> Textdateien mit Daten über besuchte Webseiten

> Datenschutzrisiko für Unternehmen

Maßnahmen

> Automatische Löschung nach jeder Online-Sitzung

> „Cookies von Drittanbietern“ nicht zulassen

> Mitteilung an Web- und Werbeanbietern („do not track“)

4. 123456? DAS SICHERE PASSWORT IM ARBEITSALLTAG

Die wichtigsten Regeln für ein sicheres Passwort

- ✓ Keine einfachen Passwörter (leicht zu erraten)
- ✓ Keine Namen
- ✓ Buchstaben- und Ziffernkombinationen erhöhen die Sicherheit
- ✓ Keine Umlaute verwenden
- ✓ Länger ist sicherer
- ✓ Passwörter nicht am Rechner notieren
- ✓ Passwörter nicht mehrfach benutzen
- ✓ Passwörter regelmäßig ändern

5. ZUSAMMENFASSUNG

Für die sichere Nutzung von Computern am Arbeitsplatz:

- ✓ sollte jede genutzte Software immer auf dem neusten Stand sein,
- ✓ gehören Antivirenprogramme und eine Firewall zum Sicherheitskonzept,
- ✓ sind die Sicherheitseinstellungen im Browser korrekt eingestellt,
- ✓ werden ggfs. Plug-ins installiert und die Cookie-Einstellungen angepasst,
- ✓ verwenden alle Mitarbeiter sichere und unterschiedliche Passwörter für alle Logins.

Bottom-Up: Berufsschüler für IT-Sicherheit hat zum Ziel, die Mitarbeiter*innen von morgen bereits während der dualen Ausbildung auf die Herausforderungen des digitalen Arbeitsalltags im Hinblick auf IT-Sicherheit und Schutz von Daten vorzubereiten. Damit leistet Bottom-Up einen wichtigen Beitrag zu mehr IT-Sicherheit in kleinen und mittelständischen Unternehmen. **www.dsin-berufsschulen.de**

Bottom-Up: Berufsschüler für IT-Sicherheit ist ein Angebot von
Deutschland sicher im Netz e.V.
Albrechtstraße 10 / 10117 Berlin
www.sicher-im-netz.de

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der Initiative:
IT-Sicherheit IN DER WIRTSCHAFT

Ein Projekt von:
DsiN Deutschland sicher im Netz

Initiative „IT-Sicherheit in der Wirtschaft“
Die Initiative „IT-Sicherheit in der Wirtschaft“ des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unter-nehmen beim sicheren Einsatz von IKT-Sys-temen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: www.it-sicherheit-in-der-wirtschaft.de abrufbar.