WINDOWS GEHACKT NOTFALLPLAN

Phase 1 – Sofort handeln

Wenn dein Windows-PC gehackt wurde, ist schnelles und strukturiertes Handeln entscheidend. Dieses Dokument zeigt dir ein universelles Vorgehen, das für nahezu alle Rechner funktioniert.

1. **Netzwerkverbindung trennen**:

Trenne deinen PC sofort vom Internet. Nutzt du WLAN, dann schalte dieses aus. Bei LAN kannst du das Kabel ziehen.

Malware und Trojaner kommunizieren in der Regel über das Internet mit dem Hacker. Hat dein Computer keinen Internetzugriff, kann der Hacker nicht auf ihn zugreifen.

2. **Wirf einen Blick in den Task-Manager**

Mit einem Rechtsklick auf die Taskleiste kannst du den Task-Manager öffnen.

Schaue dir dort die "Apps" an. Fällt dir eine Anwendung mit komischen Namen auf? Dann beende diesen Prozess.

3. **Scanne den Rechner mit dem Windows-Defender**:

Suche nach Windows-Sicherheit und öffne den Virenschutz. Hier kannst du deinen PC nach Malware scannen.

Wichtig: **Nutze nicht die Schnellüberprüfung**

Wähle stattdessen vollständiger Scan und anschließend Offlineüberprüfung

4. **Bist du nach dem Scan immer noch skeptisch?**

Dann hilft es nur, wenn du Windows neu installierst.

Über **Einstellungen → System → Wiederherstellungsoptionen** kannst du das Gerät zurücksetzen. Alternativ kannst du Windows mit einem Installationsmedium neu installieren.

Wichtig: **Wähle eine Option, die alle Daten von der Festplatte entfernt!**

Du brauchst Hilfe dabei? Dann melde dich gerne unter: **kontakt@itsicher.online**

5. **Ändere die Passwörter deiner wichtigen Konten**

Sollte der Defender etwas gefunden haben, dann kann es sein, dass der Angreifer auch schon Zugriff auf einen deiner Accounts hat.

Ändere zur Sicherheit das Passwort und füge die 2-Faktor-Authentifizierung hinzu.

Anleitung: https://youtu.be/Hlyg3TZ4TpA

Phase 2 – Infektion verhindern

1. **Sei achtsam, was du online herunterlädst**:

Viren, Malware und Trojaner stammen meist von Downloads aus unseriösen Quellen. Hacker wollen dich mit Angeboten locken, die in der Regel zu gut sind, um wahr zu sein.

Wenn du so etwas siehst, ist es meistens eine Falle.

2. **Gefahren in Gruppenchats:**

Gruppenchats und öffentliche Foren haben oft keine Prüfung, wer dort beitritt. Häufig teilen Angreifer ihren Schadcode in diesen Foren.

Wenn du dein Gegenüber nicht kennst, dann sei lieber etwas misstrauisch.

3. **Werbungen**

Unseriöse Webseiten halten häufig Werbung mit Verlinkungen zu Schadcode-Webseiten. Interagiere so wenig wie möglich mit diesen Seiten und klicke niemals auf die Werbebanner!

Auch wenn die Werbung dir anbietet, deinen Rechner abzusichern oder zu beschleunigen.

4. **Anhänge in Spam-Mails**

Spam-E-Mails enthalten häufig Anhänge, hinter denen sich Schadcode versteckt. Wenn du der E-Mail oder dem Absender nicht vertraust oder sie nicht kennst, dann öffne den Anhang auf keinen Fall.

Phase 3 – Den Rechner absichern

1. **Windows-Updates**

Um den Rechner auf lange Sicht sicher zu halten, ist es wichtig, die Windows Updates zu aktivieren und regelmäßig durchzuführen.

Jede Aktualisierung schließt eine Sicherheitslücke, die ein Virus früher ausnutzen konnte.

Du findest die Updates unter: **Einstellungen → Windows Update**

2. **Updates von Microsoft-Produkten**

Auch Office-Programme wie Word oder Excel brauchen Updates.

In den Windows-Update-Einstellungen findest du unter **“Erweiterte Optionen”**, den Punkt **“Updates für andere Microsoft-Produkte erhalten”**. Aktiviere diesen, um Office, Teams, etc. aktuell zu halten.

3. **Andere Apps und Programme**

Apps aus dem Microsoft Store können in der Regel über diesen aktualisiert werden. In den Einstellungen kannst du dort auch automatische Updates aktivieren.

Alle weiteren Programme, wie Chrome, Firefox, Banking-Apps usw. musst du meist manuell prüfen.

Hier kannst du in die Einstellungen oder “Über” Menüs der App springen. Dort finden sich mehrheitlich die Update-Optionen.

Phase 4 – Sichere deine Daten

1. **Backups**

Erstelle ab sofort regelmäßige Sicherungen deiner wichtigen Daten. Kopiere Dokumente, Bilder und Videos z.B. auf eine externe Festplatte oder in die Cloud deines Vertrauens.

(Mehr dazu in folgenden Videos)

Kommt es in Zukunft wieder zu einer Infektion oder einem Schaden an deinem Gerät, kannst du Windows problemlos neu installieren, ohne dass deine Daten verloren gehen.

Nächste Schritte

Kombiniere diese Schritte mit den Tipps, um deinen Account wiederzuholen. Dadurch kannst du dir sicher sein, dass Angreifer von deinem Gerät und aus deinen Konten entfernt sind.

ITsicher.online

Colin Brown

kontakt@itsicher.online

https://itsicher.online