ERLEBEN, WAS VERBINDET.

MERKBLATT SICHERHEIT

In diesem Merkblatt geben wir Ihnen Antworten auf die wichtigsten Fragen zum Thema Internetsicherheit. Außerdem finden Sie hier viele hilfreiche Tipps, Links und Empfehlungen für ein sicheres Surfvergnügen.

AUSWIRKUNGEN VON SCHADSOFTWARE

Ein infizierter Rechner befindet sich nicht mehr vollständig unter der Kontrolle seines Eigentümers und mutiert zum sogenannten „Bot", wodurch der Computer zu einem gefügigen Instrument von Kriminellen wird. Bots verschleiern die kriminellen Zugriffe, liefern erbeutete Daten und holen neue Aufgabenlisten ab. Sie können großen Schaden verursachen:

- Teilnahme an Angriffen auf Internetserver (dDoS Attacken)
- Diebstahl privater Daten (Phishing)
- Weiterverbreitung von Schadsoftware
- Versendung von Spam (z. B. von rechtswidriger Werbung und zum Ausspionieren von Passwörtern)
- Nachinstallation von zusätzlicher Schadsoftware

SCHADSOFTWARE ENTDECKEN UND ENTFERNEN

Besonders erwähnenswert ist das „Tool zum Entfernen bösartiger Software", Seite https://www.microsoft.com/de-de/download/malicious-software-removal-tool-details.aspx und der „Microsoft Safety Scanner", welche Sie unter: https://www.microsoft.com/de-de/wdsi/products/scanner finden.

https://de.malwarebytes.org/ - kostenloses Tool zum prüfen des Rechners
http://www.botfrei.de/telekom - Anti Botnetz Beratungscenter
http://www.pentest-tools.com – Test Tool, ob offene Ports vorliegen (in englischer Sprache)

TIPP: Möchten Sie dauerhaft Unterstützung und Beratung bei PC-Fragen? Dann nutzen Sie am besten unsere Computerhilfe. Informationen erhalten Sie unter: http://telekom.de/computerhilfe

WIE KÖNNEN SIE SICH IN ZUKUNFT VOR GEFAHREN AUS DEM INTERNET SCHÜTZEN?

Einen grundlegenden Schutz bietet der Einsatz einer aktuellen und renommierten Schutzsoftware auf allen vorhandenen Rechnern und sonstigen Hardware, wie z.B. Tablett oder Smartphone. Falls Sie eine solche noch nicht im Einsatz haben, empfehlen wir Ihnen unser Sicherheitspaket Komplett, http://telekom.de/sicherheit
Viele weitere Informationen zum Schutz finden Sie auch auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik, https://bsi-fuer-buerger.de

HINWEISE ZUR VERMEIDUNG VON ERNEUTEN INFEKTIONEN

Keine Schutzsoftware kann vor allen Gefahren schützen, sie stellt nur einen Baustein von mehreren dar. Deshalb ist es notwendig, zusätzlich einige Sicherheitshinweise zu berücksichtigen:

- Betriebssystem und verwendete Software immer aktuell halten, denn veraltete Software mit Sicherheitslücken ist die häufigste Ursache für die Infektion mit Schadsoftware. Dies gilt ggf. auch für die auf Ihrem Router installierte Software (die sogenannte „Firmware") und ggf. installierte Plugins bzw. Add-Ons von Internetprogrammen (z. B. Adobe Flash, Java).
- Nutzen Sie ein WLAN, so verwenden Sie bitte als Verschlüsselungsverfahren mindestens WPA2 (besser WPA2-PSK) und sichern Sie den Zugang zur Konfiguration des Routers mit einem eigenen persönlichen Kennwort ab (Standardpasswort abändern).
- Stellen Sie den automatischen Start von Anwendungen auf mobilen Datenträgern (z. B. für USB-Sticks, MP3-Player, Digitalkameras) ab, falls Ihr Rechner durch Gäste genutzt wird.
- Öffnen Sie keine unverlangt zugesendeten Links und Dateien. Ist Ihnen der vermeintliche Absender bekannt, fragen Sie besser nach, ob er Ihnen diese wirklich zugesendet hat.
- Führen Sie keine Programme aus unsicheren Quellen aus. Laden Sie gewünschte Software möglichst direkt vom Hersteller oder einem als seriös bekannten Download-Portal herunter.
- **Geben Sie Ihre Zugangsdaten und persönlichen Passwörter niemals weiter!** Wenn Sie eine missbräuchliche Nutzung bemerken oder vermuten, ändern Sie unbedingt im Kundencenter https://kundencenter.telekom.de Ihre Passwörter unter „Persönliche Daten" ->„Passwörter und PINs". Wenn Sie mehr als eine E-Mail-Adresse eingerichtet haben, achten Sie bitte darauf, dass Sie bei allen E-Mail Adressen das Passwort ändern. Dazu müssen Sie sich mit dieser E-Mail-Adresse ins Kundencenter einloggen. Bei Fragen und Problemen wenden Sie sich bitte an unseren Kundenservice: http://telekom.de/kontakt
- Sofern Sie eine Server-Software verwenden, um Ihren Rechner auch aus dem Internet heraus erreichbar zu machen, genügt die regelmäßige Software-Aktualisierung nicht: Lesen Sie bitte auch die jeweiligen Dokumentationen und berücksichtigen Sie aktuelle Sicherheitshinweise.

TIPP: Tauschen Sie sich auch bequem mit anderen Kunden online in den Telekom Community über Sicherheits- und Konfigurationsfragen aus: http://telekom.de/community

WIE FINDE ICH EIN SICHERES PASSWORT?

Ein sicheres Passwort besteht aus einer Kombination mit mindestens 8 zufälligen alphanumerischen Zeichen und Sonderzeichen, z.B. **Ziffern 0-9, Buchstaben a-z; A-Z, erlaubte Sonderzeichen ! # % & ( ) * + , - . / : ; < = > ? ^ _ $**. Mit einer Eselbrücke können Sie aber auch ein schwieriges Passwort merken. Wählen Sie eine beliebige Phrase oder Redewendung und generieren Sie daraus Ihr Passwort.
Beispiel: „**G**ut **D**ing **w**ill **W**eile **h**aben". Ihr Passwort wäre demnach **GDwWh.** Dieses Passwort können Sie noch um Zahlen und Sonderzeichen erweitern, z. B. GDwWh23!

HABEN SIE NOCH FRAGEN?

Im Falle von weiteren Fragen, im Kontext Sicherheit, wenden Sie sich an abuse@telekom.de oder besuchen Sie uns auf: https://www.telekom.de/hilfe/festnetz-internet-tv/sicherheit/missbrauch-von-diensten

Stand: November 2017
Herausgeber: Telekom Sicherheitsteam