2 – Überwachen mit Virenschutz und Firewall

Welche «Zugangstüren» sind auf Ihrem Gerät offen und welche Viren gelangen darauf? Praktisch keine, wenn Sie eine Firewall aktiviert und ein Virenschutzprogramm installiert haben.

Wichtigste Merkpunkte:

- Nutzen Sie ein Virenschutzprogramm und aktivieren Sie dessen automatische Update-Funktion.
- Prüfen Sie Ihr Gerät regelmässig auf Schädlingsbefall, indem Sie eine vollständige Systemprüfung durchführen.
- Aktivieren Sie in Windows oder macOS die eingebaute Firewall, bevor Sie Ihr Gerät mit dem Internet oder einem anderen Netzwerk verbinden.

2 – Überwachen mit Virenschutz und Firewall

5 Schritte für Ihre digitale Sicherheit

Mit Cockpit alles unter Kontrolle!
Mit **Virenschutz** und **Firewall** den Datenverkehr überwacht!

eBanking aber sicher! www.ebas.ch

So gehen Sie vor

Verwenden Sie ein Virenschutzprogramm und eine Firewall, welche mit automatischen Updates immer auf dem neusten Stand gehalten werden, damit Sie auch gegen die neusten Gefahren geschützt sind.

Windows

Windows 10 bzw. Windows 11 werden mit einer standardmässig aktivierten Firewall und dem Virenschutzprogramm «Windows Defender» ausgeliefert. Damit sind Sie bestens geschützt.

Für zusätzliche Schutzfunktionen, wie beispielsweise einen Jugendschutzfilter etc. können Sie auch folgende zum Teil kostenlose Produkte einsetzen (nicht abschliessende Liste):

- AVG Free Anti-Virus (https://free.avg.com)
- Avira Free Antivirus (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- F-Secure (https://www.f-secure.com)

- G Data (https://www.gdata.de)
- Malwarebytes (https://www.malwarebytes.com)
- McAfee (https://www.mcafee.com)
- Norton (https://ch.norton.com)
- Panda (https://www.pandasecurity.com)
- Sophos (https://www.sophos.com)
- Trend Micro (https://www.trendmicro.com)

macOS

Aktivieren Sie unter macOS unbedingt die eingebaute, aber standardmässig ausgeschaltete Firewall. Klicken Sie dazu im Menü «Apple» auf «Systemeinstellungen ...». Unter «Netzwerk» im Register «Firewall» können Sie die Firewall aktivieren. Diese bleibt auch nach einem Neustart aktiviert.

macOS verfügt auch über einen integrierten Schutzmechanismus, welcher Malwareinfektionen verhindern soll. Die standardmässig aktivierte Software «Gatekeeper» schützt zudem davor, aus Versehen schädliche Software zu installieren.

Zusätzlichen Schutz bieten spezialisierte Virenschutzprogramme. Empfehlenswert sind folgende zum Teil kostenlosen Programme, welche auch Windows-Malware erkennen (nicht abschliessende Liste):

- AVG (https://free.avg.com)
- Avira (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- F-Secure (https://www.f-secure.com)
- Norton (https://ch.norton.com)
- Trend Micro (https://www.trendmicro.com)

Smartphone und Tablet

Auf einem Smartphone oder einem Tablet kann eine Firewall nicht ohne Weiteres installiert werden. Während bei einem Android-Gerät Root-Rechte erforderlich sind, muss auf einem iPhone ein «Jailbreak» durchgeführt werden. Sowohl ein Root- als auch Jailbreak-Vorgang kann das Gerät beschädigen und deaktiviert verschiedene Sicherheitsmechanismen der Betriebssysteme. Zudem gehen dadurch unter Umständen sämtliche Garantieansprüche verloren. Wir raten deshalb von solchen Vorgängen ab.

Unter **Android** sollte aber unbedingt ein Virenschutzprogramm verwendet werden. Für den Einsatz empfehlen wir folgende zum Teil kostenlosen Virenschutzprogramme:

- AhnLab (https://www.ahnlab.com)
- AVG (https://free.avg.com)
- Avira (https://www.avira.com)

- Bitdefender (https://www.bitdefender.de)
- G Data (https://www.gdata.de)
- McAfee (https://www.mcafee.com)
- Norton (https://ch.norton.com)
- Sophos (https://www.sophos.com)
- Trend Micro (https://www.trendmicro.com)

Für **iOS-Geräte** wie iPhone oder iPad sind zurzeit keine Virenschutzprogramme erforderlich. Der Grund dafür liegt im geschlossenen Betriebssystem, das die Installation von fragwürdigen Apps oder anderer Schadsoftware verhindern sollte und die Berechtigungen der installierten Apps stark einschränkt.

Schützen Sie Ihre Daten und alle Ihre Geräte mit den «5 Schritten für Ihre digitale Sicherheit»:

Schritt 1 – Sichern (https://www.ebas.ch/1-sichern-der-daten/)
Schritt 2 – Überwachen
Schritt 3 – Vorbeugen (https://www.ebas.ch/3-vorbeugen-mit-software-updates/)
Schritt 4 – Schützen (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/)
Schritt 5 – Aufpassen (https://www.ebas.ch/5-aufpassen-und-wachsam-sein/)

Weiterführende Informationen für Interessierte

Malwareinfektion – wie weiter?

Falls Sie den Verdacht auf eine Malware-Infektion eines Ihrer Geräte haben oder sogar Ihr Virenschutzprogramm Ihnen eine entsprechende Meldung anzeigt, finden Sie hier (https://www.ebas.ch/malwareinfektion/) weitere Informationen, was Sie tun können.

Firewall?

Wenn Benutzerinnen und Benutzer mit Ihrem Computer, Tablet oder Smartphone im Internet surfen, öffnen sich auf den Geräten für die Kommunikation unsichtbare «Zugangstüren» (Ports). Diese bieten eine Angriffsfläche für Attacken aus dem Internet. Eine installierte Firewall schliesst diese Türen soweit als nötig und überwacht den Datenverkehr zwischen den Geräten und dem Internet. Die Firewall alarmiert, wenn sie verdächtigen Netzwerkverkehr entdeckt.