IT-SERVICEZENTRUM
Wir kümmern uns

WIE MACHE ICH MEINEN COMPUTER SICHER?

Damit Sie in Notfallsituationen vorbereitet sind, sollten Sie sich nachfolgende Situationen vorstellen und Ihre Reaktionsmöglichkeiten einschätzen.

- Der Rechner startet nicht mehr.
- Sie können keine Verbindung mehr mit dem Internet herstellen.
- Sie können nicht mehr auf Ihre Cloud-Dienste und -Daten zugreifen.
- Sie können sich nicht mehr in Ihrem Benutzerkonto an Ihrem PC anmelden.
- Ihre Daten sind plötzlich verschlüsselt oder fehlen.

Wenn Sie das Gefühl haben, dass Sie in diesen Situationen unsicher reagieren würden oder keine angemessenen Antworten finden, dann ist der folgende Leitfaden ein guter Anhaltspunkt für Sie.

DIE 12 WICHTIGSTEN TIPPS AUF EINEN BLICK:

1. Firewall aktivieren
2. Malwareschutzprogramm nutzen
3. Entfernen von ungenutzter Software
4. Täglich arbeiten ohne Admin-Account
5. Verwenden Sie einen sicheren Webbrowser
6. Führen Sie regelmäßig Updates von Windows und zusätzlicher Software durch
7. Nutzen Sie sichere Passwörter
8. Aktivieren Sie die Festplattenverschlüsselung

Aktivieren Sie Sicherheitsfunktionen

9. Passwortgeschützter Bildschirmschoner
10. Automatische Wiedergabe deaktivieren
11. Erzeugen eines Datenträgers zur Systemwiederherstellung und regelmäßige Datensicherung
12. Überprüfen der Datenschutzeinstellungen

Noch Fragen?

Haben Sie trotzdem noch Fragen zur IT-Sicherheit,
dann können Sie sich gern per Mail (ITS-Security@uni-bayreuth.de) an uns wenden.

1 Firewall aktivieren

Die integrierte Firewall ist auf Windows 10 standardmäßig aktiviert. Achten Sie darauf, dass Sie diese nicht versehentlich deaktivieren. Sie benötigen keine zusätzliche Firewall.

Zum Prüfen, ob diese aktiviert ist:
Einstellungen > Update & Sicherheit > Windows-Sicherheit > Firewall und Netzwerkschutz

2 Malwareschutzprogramm nutzen

Windows 10 bietet bereits mit dem Windows Defender ein aktiviertes Malwareschutzprogramm.

Falls Sie einen erweiterten Bedarf sehen, entscheiden Sie sich für ein Malwareschutzprogramm, das Ihren Anforderungen entspricht und informieren Sie sich unter www.av-comparatives.org oder www.test.de, ob die Programme eine gute Erkennungsleistung aufweisen.

3 Entfernen von ungenutzter Software

Mit dem Funktionsumfang eines Systems steigt auch dessen Angriffsfläche. Sie sollten Ihr System daher nur um Anwendungen bzw. Programme und Apps erweitern, die Sie tatsächlich benötigen.

Bereits installierte und nicht genutzte Software sollten Sie entfernen, um das Risiko weiterer Schwachstellen zu verringern.

5 Täglich arbeiten ohne Admin-Account

Bei der Windows 10 Installation wählen Sie zwischen einem lokalen oder Microsoft Konto. Das Standardkonto ist ein Admin-Konto mit umfassenden Berechtigungen zur Konfiguration. Wenn Sie ein Microsoft-Konto verwenden, sollten Sie dieses nicht mit Adminrechten ausstatten, um auszuschließen, dass ggf. kritische Informationen mit Cloud-Diensten synchronisiert werden.

Um ein neues Konto zu erstellen, befolgen Sie diese Schritte:
Start > Einstellungen > Konten > Familie und/oder andere(r) Benutzer > Diesem PC eine andere Person hinzufügen. Wählen Sie dann „ich kenne die Anmeldeinformation für diese Person nicht“ und auf der nächsten Seite „Benutzer ohne Microsoft-Konto hinzufügen“. Nun geben Sie einen Benutzernamen, ein Kennwort und 3 Sicherheitsfragen ein.
Wenn Sie dann auf **Weiter** klicken wird Ihr Konto erstellt.

6 Verwenden Sie einen sicheren Webbrowser

Um sich selbst im Internet zu schützen, ist es wichtig, einen angemessenen Browser zu nutzen. Windows 10 bringt den Browser **Microsoft Edge** mit sich, der mit Hilfe eines Smart-Screen-Filters Schutz vor Schadprogrammen und gefährlichen Websites bietet. Alternativ können Sie **Mozilla Firefox** nutzen.

7 Führen sie regelmäßig Updates von Windows & zusätzlicher Software durch

Sollten Sie die Einstellung zur Systemaktualisierung in Windows 10 nicht geändert haben, lädt das System im Hintergrund die Sicherheitsaktualisierungen und -Upgrades automatisiert. Stellen Sie nach einem solchen Update sicher, dass sich Ihre Einstellungen im Betriebssystem nicht geändert haben.

Achten Sie neben den Microsoft-Programmen ebenfalls darauf, dass Programme von Drittanbietern regelmäßig (z. B. monatlich) aktualisiert werden.

7 Nutzen Sie sichere Passwörter

Verwenden Sie sichere, unterschiedliche Passwörter für verschiedene Online-Dienste. Merken Sie sich das Passwort leichter, indem Sie die Anfangsbuchstaben eines Satzes verwenden. Schreiben Sie die Passwörter auf, aber bewahren Sie sie sicher außerhalb Ihres Computers auf, z. B. in einem Safe oder an einem geschützten Ort.

Weitere Passwort-Tipps finden Sie hier:
www.it-sicherheit.uni-bayreuth.de > Downloads

8 Verschlüsselung der Festplatte

Zum Schutz Ihrer Daten vor unbefugtem Zugriff durch Dritte, etwa durch Diebstahl oder Verlust, sollten Sie die Festplatte des Computers verschlüsseln. Dies funktioniert sowohl für Notebooks, als auch für Desktop-Rechner. Unter Windows 10 Home steht Ihnen dafür z. B. die Windows Geräteverschlüsselung zur Verfügung.

Ab Windows 10 Professional können Sie hierzu den BitLocker nutzen. Wählen Sie im mit Windows 10 Professional vorinstallierten BitLocker die zu verschlüsselnde Festplatte aus. Legen Sie dafür ein Passwort oder eine andere Authentifizierungsmethode fest. Verwahren Sie den bei der Verschlüsselung des Rechners erstellten Wiederherstellungsschlüssel sicher und getrennt vom Gerät. Ein Verlust des Wiederherstellungsschlüssels sperrt Sie dauerhaft aus dem System aus!

9 Passwortgeschützter Bildschirmschoner

Durch das Konfigurieren eines passwortgeschützten Bildschirmschoners können Sie vermeiden, dass Ihr Desktop längere Zeit geöffnet bleibt, wenn Sie nicht mit dem Rechner arbeiten (z. B. bei Abwesenheit).

Diesen Schutz können Sie in den Einstellungen, Bereich „Personalisierung“ in der Kategorie „Sperrbildschirm“ unter „Einstellungen Bildschirmschoner“ konfigurieren. Wählen Sie hierzu einen Bildschirmschoner Ihrer Wahl und setzen Sie den gewünschten Wert für die Wartezeit (z. B. 10 Minuten). Zur Aktivierung des Passwortschutzes müssen Sie noch einen Haken bei „Anmeldeseite bei Reaktivierung“ setzen.

10 Deaktivieren der automatischen Wiedergabe

Die automatische Wiedergabe bzw. der Autostart von Programmen auf Wechseldatenträgern gefährdet die Sicherheit Ihres Systems durch Schadprogramme und sollte deaktiviert werden.

Sie können diese Funktion in den Einstellungen in der Kategorie „Geräte“ unter „Automatische Wiedergabe“ deaktivieren.

11 Erzeugen eines Datenträgers zur Systemwiederherstellung und regelmäßige Datensicherung

Die meisten neuen Systeme werden heute ohne Installationsmedien ausgeliefert. Daher sollten Sie nach der ersten Inbetriebnahme einen Systemreparaturdatenträger erstellen, indem Sie einen USB-Speicherstick mit ca. 8-16 GB Speicherkapazität verwenden. Dieser Datenträger ermöglicht es Ihnen, im Falle eines Defekts oder Absturzes Ihre Windows 10-Installation wiederherzustellen. Vergessen Sie auch nicht, regelmäßig eine Sicherung Ihrer Daten auf einem externen Medium durchzuführen, um im Ernstfall Ihre Daten wiederherstellen zu können.

Um einen Systemreparaturdatenträger zu erstellen, suchen Sie nach „Wiederherstellungslaufwerk erstellen“ und sichern Sie dabei die Systemdateien, damit der Datenträger später zur Neuinstallation verwendet werden kann.

12 Überprüfen von Datenschutzeinstellungen

Die Assistenz- und Unterstützungsfunktionen von Windows 10 erfordern einen umfangreichen Zugriff auf Ihre Daten.

Die eingerichteten Zugriffsberechtigungen können Sie unter „Einstellungen > Datenschutz“ überprüfen und nach Ihren Wünschen anpassen.