JUSTUS-LIEBIG-UNIVERSITÄT-GIESSEN
ALLG. BWL UND WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Schwickert, Axel; Schramm, Laura; Schick, Lukas;
Dörr, Lea

Basiswissen IT-Sicherheit – Reader zur WBT-Serie

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 06 / 2022
ISSN 1613-6667

Arbeitspapiere WI Nr. 06 / 2022

Autoren: Schwickert, Axel; Schramm, Laura; Schick, Lukas; Dörr, Lea

Titel: Basiswissen IT-Sicherheit – Reader zur WBT-Serie

Zitation: Schwickert, Axel; Schramm, Laura; Schick, Lukas; Dörr, Lea: Basiswissen IT-Sicherheit – Reader zur WBT-Serie, in: Arbeitspapiere WI, Nr. 06/2022, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2022, 72 Seiten, ISSN 1613-6667.

Kurzfassung: Die vorliegende WBT-Serie erläutert die Grundlagen der IT-Sicherheit im privaten Umfeld.

Zunächst wird die Notwendigkeit für IT-Sicherheits-Maßnahmen im privaten Umfeld aufgezeigt. Anschließend werden die relevanten Begriffe der IT-Sicherheit besprochen.

In den nachfolgenden WBT werden die Anwendungsbereiche der IT-Sicherheits-Maßnahmen betrachtet und anhand von Beispielen beleuchtet.

Schlüsselwörter: IT-Sicherheit, privates Netzwerk, Smart Home, Einkaufen im Internet,

A Zur Einordnung der WBT-Serie

Die WBT-Serie richtet sich an Interessenten des Themenbereiches „Basiswissen IT-Sicherheit“.

Für Ihr Selbststudium per WBT müssen Sie einen Internet-Zugang haben – entweder auf Ihren eigenen PCs, auf den PCs im JLU-Hochschulrechenzentrum, in den JLU-Bibliotheken oder dem PC-Pool des Fachbereichs.

B Die Web-Based Trainings

Der Stoff zu diesem Thema ist in Lerneinheiten zerlegt worden und wird durch eine Serie von Web-Based-Trainings (WBT) vermittelt. Mit Hilfe der WBT kann der Stoff im Eigenstudium erarbeitet werden. Die WBT bauen inhaltlich aufeinander auf und sollten in der angegebenen Reihenfolge absolviert werden.

WBT-Nr.	WBT-Bezeichnung	Bearbeitungs-dauer
1	Grundlagen der IT-Sicherheit	90 Min.
2	IT-Sicherheit im Eigenheim – Privates Netzwerk	90 Min.
3	IT-Sicherheit im Eigenheim – Smart Home	90 Min.
4	IT-Sicherheit im Eigenheim – Ein-kaufen im Internet	90 Min.

Tab. 1: Übersicht WBT-Serie

Die Inhalte der einzelnen WBT werden nachfolgend in diesem Dokument gezeigt. Alle WBT stehen Ihnen rund um die Uhr online zur Verfügung. Sie können jedes WBT beliebig oft durcharbeiten. In jedem WBT sind enthalten:

- Vermittlung des Lernstoffes,
- interaktive Übungen zum Lernstoff,
- abschließende Tests zum Lernstoff

Inhaltsverzeichnis

Seite

A Zur Einordnung der WBT-Serie I
B Die Web-Based Trainings II
Inhaltsverzeichnis III
Abbildungsverzeichnis VI

1 Grundlagen der IT-Sicherheit 1
1.1 Gefahr! 1
1.1.1 Die Situation 1
1.1.2 Die Notwendigkeit von IT-Sicherheits-Maßnahmen 1
1.1.3 Risiken und Konsequenzen vernachlässigter IT-Sicherheit 1
1.1.4 Typische Szenarien 2
1.1.5 Risiken vernachlässigter IT-Sicherheit 2
1.1.6 Konsequenzen vernachlässigter IT-Sicherheit 3
1.1.7 Umgang mit Risiken und Konsequenzen 4
1.2 Begriffe und Definitionen 4
1.2.1 Begriffe der IT-Sicherheit 4
1.2.2 Was bedeutet Computersicherheit? 4
1.2.3 Was bedeutet Datensicherheit? 5
1.2.4 Was ist eine Datensicherung? 5
1.2.5 Was bedeutet Datenschutz? 5
1.3 Was gilt es zu schützen? 6
1.3.1 Aber wo anfangen? 6
1.3.2 Das private Netzwerk 6
1.3.3 Das „Smart Home“ 7
1.3.4 Einkaufen und Bezahlen im Internet 7
1.3.5 Die Nutzung von Cloud-Diensten 7
1.3.6 Wichtige Daten 8
1.3.7 Soziale Netzwerke 8
1.3.8 Wie müssen die verschiedenen Anwendungsbereiche geschützt werden? 8
1.4 Typische Aufgabenstellungen 9

2 IT-Sicherheit im Eigenheim – Privates Netzwerk 10
2.1 IT-Sicherheit am Beispiel der Familie Müller 10
2.1.1 Was Sie bisher wissen 10
2.1.2 Familie Müller 10
2.1.3 Maßnahmen zur Steigerung der persönlichen IT-Sicherheit 11
2.1.4 Die verschiedenen Anwendungsbereiche 11
2.2 Das private Netzwerk 12
2.2.1 Das private Netzwerk 12
2.2.2 Privates Netzwerk – Inventur aller Geräte im Eigenheim 14
2.2.3 Inventur aller Geräte im Eigenheim der Familie Müller 14
2.2.4 Allgemeine Maßnahmen zur Sicherung des privaten Netzwerks 14
2.3 Maßnahmen zur Sicherung des Routers im privaten Netzwerk 15
2.3.1 Router: Umsetzung konkreter Maßnahmen 15
2.3.2 Aufrufen der Administrationsoberfläche der Fritzbox 15
2.3.3 Die Administrationsoberfläche der Fritzbox 17
2.3.4 Sicherheitseinstellungen der Fritzbox – Teil 1 18
2.3.5 Sicherheitseinstellungen der Fritzbox – Teil 2 18
2.3.6 Fritzbox-Benutzer-Einstellungen 19
2.3.7 WLAN-Sicherheit durch Passwort und Verschlüsselung 20
2.3.8 Geräte im privaten Netzwerk 20
2.3.9 Name des WLAN-Funknetzes 21
2.3.10 Umgesetzte Maßnahmen an der Fritzbox von Familie Müller 21
2.3.11 Umsetzung konkreter Maßnahmen zur Sicherung der privaten Endgeräte 22
2.4 macOS: Maßnahmen zur Sicherung der persönlichen Computer 22
2.4.1 macOS: Umsetzung konkreter Maßnahmen 22
2.4.2 Erste Maßnahmen an Lisas MacBook 23
2.4.3 Weitere Systemeinstellungen 24
2.4.4 Maßnahmen zum Viren- und Datenschutz an Lisas MacBook 24
2.4.5 Festplatten-Verschlüsselung aktivieren 25
2.4.6 Integrierten Viren- und Ransomware-Schutz sowie Firewall aktivieren 25

2.4.7 Datenschutz bei der Anwendungsnutzung 26
2.4.8 Umgesetzte Maßnahmen am MacBook von Lisa Müller 26
2.5 Windows: Maßnahmen zur Sicherung der persönlichen Computer 27
2.5.1 Windows: Umsetzung konkreter Maßnahmen 27
2.5.2 Erste Maßnahmen an Anettes Microsoft Windows PC 27
2.5.3 Backups aktivieren 28
2.5.4 Das Betriebssystem auf Updates prüfen 29
2.5.5 Passwortschutz für Benutzerkonten aktivieren 29
2.5.6 Maßnahmen zum Viren- und Datenschutz an Anettes Windows-PC 30
2.5.7 Umsetzung der Maßnahmen zum Viren- und Datenschutz 30
2.5.8 Maßnahmen zur Festplattenverschlüsselung an Windows-basierten Computern 31
2.5.9 Umgesetzte Maßnahmen am Microsoft Surface von Anette Müller 32
2.5.10 Genug für heute! 32
3 IT-Sicherheit im Eigenheim – Smart Home 33
3.1 IT-Sicherheit am Beispiel der Familie Müller 33
3.1.1 Was Sie bisher wissen 33
3.1.2 Familie Müller 33
3.1.3 Maßnahmen zur Steigerung der persönlichen IT-Sicherheit 34
3.1.4 Die verschiedenen Anwendungsbereiche 34
3.2 Das Smart Home der Familie Müller 35
3.2.1 Der Anwendungsbereich: Das Smart Home 35
3.2.2 Geräte in einem Smart Home 35
3.2.3 Theorie: Das Smart Home 39
3.2.4 Das Smart Home als Einfallstor für Angreifer 40
3.3 Überwachungskameras im Smart Home 41
3.3.1 Allgemeine Maßnahmen im Smart Home 41
3.3.2 Überwachungskamera: Umsetzung konkreter Maßnahmen 41
3.3.3 Einstellungen an der Überwachungskamera 42
3.3.4 Firmware-Upgrade an der Überwachungskamera 43

3.3.5 Sicheres Passwort für die Überwachungskamera 43
3.3.6 Fernzugriff an der Überwachungskamera deaktivieren 44
3.3.7 Datenschutz der Überwachungskamera 44
3.3.8 Umgesetzte Maßnahmen an den Überwachungskameras 46
3.4 Lampen und Rollos im Smart Home 46
3.4.1 Das Smart Home von Familie Müller 46
3.4.2 Smarte Lampen und smarte Rollos 46
3.4.3 Smarte Lampen und smarte Rollos: Umsetzung konkreter Maßnahmen 47
3.4.4 Sicheres und individuelles Passwort wählen 47
3.4.5 Prüfen und Einspielen von Firmware-Updates 48
3.4.6 Geräte-/Datenschutzeinstellungen überprüfen 48
3.4.7 Timer-Einstellungen anpassen 49
3.4.8 Umgesetzte Maßnahmen an den Lampen und Rollos 49
3.5 Steckdosen im Smart Home 469
3.5.1 Smarte Steckdosen: Umsetzung konkreter Maßnahmen 50
3.5.2 Zugriff auf die smarten Steckdosen via Fritzbox 50
3.5.3 Einstellungen zur Bedienung der Gruppen und Geräte 51
3.5.4 Einstellungen zur Bedienung einer smarten Steckdose 51
3.5.5 Automatische Schaltung einer smarten Steckdose 52
3.5.6 Umgesetzte Maßnahmen an den Steckdosen 52
3.6 Abendessen 53

4 IT-Sicherheit im Eigenheim – Einkaufen im Internet 54
4.1 IT-Sicherheit am Beispiel der Familie Müller 54
4.1.1 Was Sie bisher wissen 54
4.1.2 Familie Müller 54
4.1.3 Maßnahmen zur Steigerung der persönlichen IT-Sicherheit 55
4.1.4 Die verschiedenen Anwendungsbereiche 55
4.2 Einkaufen und Bezahlen im Internet 56
4.2.1 Einkaufen und Bezahlen im Internet 56
4.2.2 Allgemeine Maßnahmen zum sicheren Einkaufen und Bezahlen im Internet 56

4.2.3 Einkaufen im Internet: Umsetzung konkreter Maßnahmen 57
4.2.4 Überprüfung der Vertrauenswürdigkeit eines Web Shops – Impressum 57
4.2.5 Überprüfung der Vertrauenswürdigkeit eines Web Shops – Gütesiegel 57
4.2.6 Überprüfung der Vertrauenswürdigkeit eines Web Shops – https-Verschlüsselung 57
4.3 Die sichere Nutzung von Web Shops 58
4.3.1 Konkrete Maßnahmen zur Nutzung von Web Shops 58
4.3.2 2-Faktor-Authentifizierung im Web Shop 58
4.3.3 Sicheres Passwort im Web Shop 58
4.3.4 Sichere E-Mail-Adresse zur Verwendung im Web Shop 59
4.3.5 Betrachtete Maßnahmen zum sicheren Einkaufen im Internet 60
4.4 Abendessen 460

Abbildungsverzeichnis

Seite

Abb. 1: Typische Szenarien: Der Hacker im Smart Home 2
Abb. 2: Typische Szenarien: Vorsicht Erpresser 2
Abb. 3: Typische Szenarien: Der Hacker im Staubsauger 2
Abb. 4: Inventur aller Geräte im Eigenheim der Familie Müller 14
Abb. 5: Aufrufen der Administrationsoberfläche der Fritzbox 16
Abb. 6: Die Administrationsoberfläche der Fritzbox 17
Abb. 7: Sicherheitseinstellungen der Fritzbox – Teil 1 18
Abb. 8: Sicherheitseinstellungen der Fritzbox – Teil 2a 18
Abb. 9: Sicherheitseinstellungen der Fritzbox – Teil 2b 19
Abb. 10: Fritzbox-Benutzer-Einstellungen 19
Abb. 11: WLAN-Sicherheit durch Passwort und Verschlüsselung 20
Abb. 12: Geräte im privaten Netzwerk 20
Abb. 13: Name des WLAN-Funknetzes 21
Abb. 14: Maßnahmen: Backups aktivieren und durchführen 23
Abb. 15: Maßnahmen: Betriebssystem auf Updates prüfen 23
Abb. 16: Maßnahmen: Passwortschutz aktivieren 24
Abb. 17: Weitere Systemeinstellungen 24
Abb. 18: Festplatten-Verschlüsselung aktivieren 25
Abb. 19: Integrierten Viren- und Ransomware-Schutz sowie Firewall aktivieren 25
Abb. 20: Datenschutz bei der Anwendungsnutzung 26
Abb. 21: Windows-Einstellungen 28
Abb. 22: Backups aktivieren 28
Abb. 23: Das Betriebssystem auf Updates prüfen 29
Abb. 24: Passwortschutz für Benutzerkonten aktivieren 29
Abb. 25: Umsetzung der Maßnahmen zum Datenschutz 30
Abb. 26: Umsetzung der Maßnahmen zum Virenschutz 31
Abb. 27: Maßnahmen zur Festplattenverschlüsselung an Windows-basierten Computern 31
Abb. 28: Geräte in einem Smart Home 35
Abb. 29: Einstellungen an der Überwachungskamera 42
Abb. 30: Firmware-Upgrade an der Überwachungskamera 43
Abb. 31: Sicheres Passwort für die Überwachungskamera 43

Abb. 32: Fernzugriff an der Überwachungskamera deaktivieren 44
Abb. 33: Datenschutz-Einstellungen der Überwachungskamera 45
Abb. 34: Telemetrie-Einstellungen der Überwachungskamera 45
Abb. 35: Sicheres und individuelles Passwort wählen 47
Abb. 36: Prüfen und Einspielen von Firmware-Updates..... 48
Abb. 37: Geräte-/Datenschutzeinstellungen überprüfen 48
Abb. 38: Timer-Einstellungen anpassen..... 49
Abb. 39: Smart Home in der Fritzbox 50
Abb. 40: Einstellungen zur Bedienung der Gruppen und Geräte 51
Abb. 41: Einstellungen zur Bedienung einer smarten Steckdose 51
Abb. 42: Automatische Schaltung einer smarten Steckdose 52
Abb. 43: Sicheres und einzigartiges Passwort verwenden 59
Abb. 44: 2-Faktor-Authentifizierung aktivieren (im Shop und in der hinterlegten E-Mail-Adresse)..... 59
Abb. 45: 2-Faktor-Authentifizierung zum Schutz des E-Mail-Kontos..... 60

1 Grundlagen der IT-Sicherheit

1.1 Gefahr!

1.1.1 Die Situation

Minütlich registrieren sich weltweit zahlreiche neue Nutzer bei den verschiedensten Online-Diensten und eine Vielzahl neuer Geräte werden an das Internet angeschlossen.

Online-Shops, soziale Netzwerke, der neue intelligente Kühlschrank, die ferngesteuerte Waschmaschine oder der Smart Speaker Alexa.

Dabei erfreuen wir uns immer an den neuen Funktionen und Vorteilen von Plattformen und Geräten.

Die Nutzung dieser vielen Dienste und Geräte verursacht jedoch auch eine Menge neuer Daten, die entweder über das Internet übertragen oder über das Internet erreichbar sein sollen und fernab von Zuhause gespeichert werden.

Dieser nicht sichtbare Aspekt findet jedoch kaum Beachtung und wird somit solange vernachlässigt, bis etwas passiert ...

1.1.2 Die Notwendigkeit von IT-Sicherheits-Maßnahmen

Sie fragen sich, was soll schon passieren? Wen interessieren meine Daten und Geräte?

Um zu verstehen, warum jeder Nutzer von Geräten und Diensten ein potentielles Opfer eines IT-Sicherheitsvorfalls sein kann, reicht ein Blick auf die möglichen Risiken und Konsequenzen.

Diese Perspektive wird verdeutlichen, warum es notwendig ist, sich um die IT-Sicherheit im eigenen digitalen Umfeld zu kümmern und die Risiken eines IT-Sicherheitsvorfalls zu minimieren.

1.1.3 Risiken und Konsequenzen vernachlässigter IT-Sicherheit

Das alles klingt noch sehr abstrakt und kaum ein Nutzer fühlt sich direkt betroffen und motiviert, etwas an seinem Verhalten zu verändern.

Wir gehen davon aus, dass alle Systeme sicher und gut geschützt sind.

Erst bei einem IT-Sicherheitsvorfall wird einem bewusst, dass die Konsequenzen beispielweise eines Datenverlusts oder Datenmissbrauchs unkalkulierbar sind bzw. von kaum einem Nutzer vorher abgeschätzt werden können. Zudem steht der Aufwand der nachträglichen Behebung solcher Konsequenzen (wenn dies überhaupt noch möglich ist) in keinem Verhältnis zu einem präventiven Verhalten. Schauen wir uns nachfolgend ein paar Beispiele von möglichen Gefahrenszenarien an.

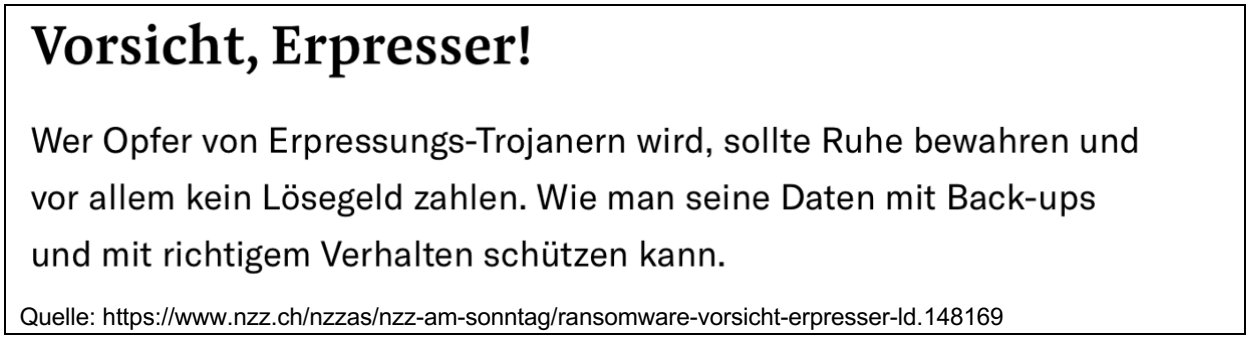
1.1.4 Typische Szenarien

Der Hacker im Smart Home: Amazons Ring-Kameras werden immer öfter gehackt

Neben Polizeibehörden, die immer öfter auf Videos von Ring-Kameras zugreifen, veranstalten jetzt auch noch Hacker ihre Shows in den Schlafzimmern der Käufer.

Quelle: heise.de/-4617254

Abb. 1: Typische Szenarien: Der Hacker im Smart Home



Vorsicht, Erpresser!

Wer Opfer von Erpressungs-Trojanern wird, sollte Ruhe bewahren und vor allem kein Lösegeld zahlen. Wie man seine Daten mit Back-ups und mit richtigem Verhalten schützen kann.

Quelle: https://www.nzz.ch/nzzas/nzz-am-sonntag/ransomware-vorsicht-erpresser-ld.148169

Abb. 2: Typische Szenarien: Vorsicht Erpresser

Smart Home: Wenn der Hacker über den Staubsauger Daten klaut

Intelligente Geräte dimmen das Licht oder saugen den Boden – über das Internet gesteuert. Ein "Smart Home" bietet Komfort, aber auch leichten Zugriff für Cyberkriminelle. Vor kurzem erst hat ein Hacker rund eine halbe Million Anmeldedaten, auch von smarten Internet-of-Things-Tools, ausgespäht.

Quelle: https://www.haufe.de/immobilien/wirtschaft-politik/smart-home-einfallstor-fuer-hacker-und-cyberkriminelle_84342_508446.html

Abb. 3: Typische Szenarien: Der Hacker im Staubsauger

1.1.5 Risiken vernachlässigter IT-Sicherheit

Risiken bestehen bei jeder Nutzung von Diensten und Geräten. Diese Risiken werden jedoch erst im Nachhinein sichtbar. Dann, wenn es meist schon zu spät ist. Nachfolgend sehen Sie einen kleinen Ausschnitt möglicher IT-Risiken.

1. Datenmissbrauch
   - Identitätsmissbrauch
   - Missbrauch von Zahlungsdaten
   - Missbrauch von Benutzerdaten
   - Manipulation von Geräten im Smart Home
   - ...

2. Datenverlust
   - Durch Versagen von Speichermedien
   - Durch fehlerhafte Bedienung
   - Durch Malware, Ransomware, Viren etc.
   - ...
3. Datenabfluss
   - Manipulierte Office-Dateien
   - Phishing
   - Trojaner
   - Brute-Force-Attacken
   - Man-in-the-Middle-Attacken
   - Schwache Authentifizierungsmethoden
   - …
4. …
   - …

1.1.6 Konsequenzen vernachlässigter IT-Sicherheit

Die Konsequenzen eines IT-Sicherheitsvorfalls sind ebenso vielfältig wie die Risiken und können ein breites Spektrum annehmen.

1. Rechtlich
   - Inkasso
   - Abmahnungen
   - Anzeigen
   - ...
2. Kostenbezogen
   - Sachschäden
   - Wiederbeschaffung von Daten und Geräten
   - Opportunitätskoten
   - ...
3. Persönlich
   - Image-Schäden
   - Rufmord
   - Identitätsmissbrauch
   - Verletzung der Privatsphäre
   - Verlust von Daten mit immateriellem Wert
   - …
4. …

- …

1.1.7 Umgang mit Risiken und Konsequenzen

Um die zuvor genannten Risiken und Konsequenzen zu minimieren, müssen sich Nutzer in ihrem Verhalten reflektieren und anpassen. Zwar gibt es noch weitere Faktoren, die die Risiken minimieren bzw. sogar eliminieren können. Den effektivsten und größten Wirkungsbereich stellt jedoch das Nutzerverhalten dar.

Bevor man sich als Nutzer um seine persönliche IT-Sicherheit kümmern kann, ist es unentbehrlich, sich mit wesentlichen Begriffen aus dem Bereich der IT-Sicherheit zu befassen: Computersicherheit, Datensicherheit, Datensicherung, Datenschutz.

Im nachfolgenden Kapitel werden wir uns daher mit wesentlichen Begriffen auseinandersetzen, um darauf aufbauend spezifische Anwendungsbereiche genauer adressieren zu können.

1.2 Begriffe und Definitionen

1.2.1 Begriffe der IT-Sicherheit

Dass mit der Nutzung vieler Geräte und Dienste gewisse Risiken und Gefahren einhergehen, sollte jedem bewusst sein.

Bevor wir uns die verschiedenen Anwendungsbereiche anschauen, in denen diese Risiken und Konsequenzen auftreten können und die es somit primär zu schützen gilt, ist es essentiell, sich zunächst mit verschiedenen Begriffen der IT-Sicherheit zu befassen.

Was bedeuten also Computersicherheit, Datensicherheit, Datensicherung und Datenschutz?

Da viele dieser Begriffe als Oberbegriffe oder Synonyme verwendet werden, kann man schnell den Überblick verlieren. Auch weiß man nie genau, an welcher Stelle man anfangen soll, seine eigene IT-Sicherheit zu stärken.

Schauen wir uns daher zunächst ein paar Begriffe und Definitionen an.

1.2.2 Was bedeutet Computersicherheit?

Unter der „Computersicherheit“ versteht man die Sicherheit eines persönlichen Computers oder Computer-Systems. Wenn dieser vor Ausfall, Manipulation und unerlaubtem Zugriff geschützt ist, ist dieser „sicher“.

Aber was genau bedeuten die Begriffe „Ausfall“, „Manipulation“ und „unerlaubter Zugriff“?

Ausfall: Der persönliche Computer steht jederzeit funktionsbereit zur Verfügung und hat keine Ausfallzeiten. Das heißt, dieser funktioniert immer dann, wenn er gebraucht wird und

erfüllt die gewünschten Aufgaben ordnungsgemäß. Aufgaben können bspw. der Abruf von E-Mails, Web Sites oder das Bearbeiten von Dokumenten sein.

Manipulation: Der persönliche Computer funktioniert wie erwartet und führt keine fehlerhaften oder ungewollten Aufgaben oder Prozesse selbständig oder auf Befehl unerlaubter Dritter aus.

Unerlaubter Zugriff: Nur berechtige Nutzer sind befugt, den persönlichen Computer zu steuern.

1.2.3 Was bedeutet Datensicherheit?

„Datensicherheit“ befasst sich nicht mit dem persönlichen Computer selbst, sondern mit den darauf gespeicherten Daten. Die Datensicherheit ist eine wesentliche Voraussetzung für den Datenschutz.

Datensicherheit hat das Ziel, sämtliche auf dem persönlichen Computer gespeicherte Daten vor Verlust, Manipulation und anderen ungewollten Szenarien zu schützen.

Verlust: Die auf dem persönlichen Computer gespeicherten Daten können nicht verloren gehen, selbst wenn der Rechner einen Defekt hat.

Manipulation: Die auf dem persönlichen Computer gespeicherten Daten können nicht ungewollt verändert werden.

1.2.4 Was ist eine Datensicherung?

Unter einer „Datensicherung“ versteht man eine Schutzmaßnahme, die Daten vor einem Verlust oder einer ungewollten Veränderung schützt.

Bekannte Maßnahmen sind bspw. das Spiegeln von Daten auf einen externen Datenträger (DVD, externe Festplatte, NAS etc.) oder auf einen per Internet zugreifbaren Speicherplatz (Cloud-Speicher).

Sollten Daten ungewollt verändert oder verloren gehen, kann eine zuvor erstellte Datensicherung helfen, die Daten wiederherzustellen. So schließt man entweder den externen Datenträger an oder verbindet sich mit seinem Cloud-Speicher und kopiert die verloren gegangenen Daten zurück auf seinen persönlichen Computer.

1.2.5 Was bedeutet Datenschutz?

Der Begriff „Datenschutz“ bezieht sich zwar auf alle Daten, die auf einem persönlichen Computer gespeichert sind, Daten mit Personenbezug stehen aber ganz besonders im Fokus.

Personenbezogene Daten sind Daten, die im direkten Zusammenhang zu einer Person stehen. Beispiele hierfür sind der Name, das Alter, die Anschrift oder die Zahlungsdaten einer Person. Personenbezogene Daten lassen sich also eindeutig einer natürlichen Person zuordnen und können diese bspw. identifizieren.

Wenn die personenbezogenen Daten vor Missbrauch durch Dritte geschützt sind, also Dritte die Daten weder lesen noch verändern können, ist der Datenschutz sichergestellt. Auf diese Weise wird die Privatsphäre einer Person gewahrt.

1.3 Was gilt es zu schützen?

1.3.1 Aber wo anfangen?

Da wir nun wissen, was die verschiedenen Begriffe bedeuten und welche Risiken und Konsequenzen aus einem vernachlässigtem Umgang mit der IT entstehen können, sollten wir handeln! Doch wo beginnt man und wo lohnt es sich überhaupt, die persönliche IT zu schützen?

Schauen wir uns daher nachfolgend einige Anwendungsbereiche an, die primäre Angriffsziele darstellen und durch richtiges Handeln seitens der Nutzer zumindest überwiegend geschützt werden können.

Anwendungsbereiche:

- Das private Netzwerk
- Smart Home
- Einkaufen im Internet
- Cloud-Dienste
- Wichtige Daten
- Soziale Netzwerke

1.3.2 Das private Netzwerk

Das private Netzwerk in den eigenen vier Wänden beheimatet heutzutage viele verschiedene Geräte und ist per Router an das Internet angebunden. Erst wenn man anfängt zu zählen, wie viele Geräte man mit seinem Router verbunden hat, wird einem bewusst, dass sich nicht nur der Computer und das Smartphone im Netzwerk befinden.

Viele weitere Geräte befinden sich heutzutage in unseren privaten Netzwerken: Router, Computer, Smartphones, Tablets, Smart TVs, Überwachungskameras, Thermostate, Lampen, Staubsauger, Kühlschränke, Waschmaschinen ....)

Das private Netzwerk besteht jedoch nicht nur aus Geräten! Auch die Verbindungen zwischen den einzelnen Geräten (WLAN, LAN, Bluetooth, etc.) müssen geschützt werden. Was bringt es also, wenn alle Geräte im privaten Netzwerk geschützt sind, aber das Passwort für den WLAN-Zugang „123“ ist?

1.3.3 Das „Smart Home“

Einen besonderen Stellenwert im eigenen privaten Netzwerk nimmt das sog. „Smart Home“ ein. Unter Smart Home versteht man alle Geräte im eigenen Haushalt, welche an den Router und somit an das Internet oder Netzwerk angeschlossen werden, untereinander selbständig kommunizieren, Daten austauschen und Aktionen ausführen.

Diese Geräte sind besonders anfällig für IT-Sicherheitsvorfälle, da bei diesen Geräten der Verkaufsaspekt auf der Funktionsvielfalt liegt und nicht auf deren IT-Sicherheit.

So können Spielzeuge, Haushaltsgeräte, Werkzeuge, Rollläden, Heizungen und viele weitere Gegenstände smart sein und an das Internet bspw. zur Fernsteuerung angeschlossen werden.

Leider kommt es immer häufiger vor, dass auch nicht autorisierte Personen Zugriff auf diese Geräte im eigenen Heim erhalten.

1.3.4 Einkaufen und Bezahlen im Internet

Einkaufen und Bezahlen im Internet ist komfortabel. Mit wenigen Klicks und hinterlegten Zahlungsdaten werden die gewünschten Produkte in Windeseile nach Hause geliefert.

Doch für diese komfortable Einkaufsmöglichkeit hinterlegen wir Anschriften, Zahlungsdaten und persönliche Wunschlisten. Meist werden diese Angaben im Online-Shop gespeichert, um nicht beim nächsten Kauf alle Daten erneut eingeben zu müssen.

Aber was passiert, wenn nicht autorisierte Dritte an diese Daten gelangen? Diese werden dann die erbeuteten Zahlungsdaten verwenden, um Käufe damit zu tätigen oder verkaufen gar die Informationen zu diesen erbeuteten Zahlungsdaten im Web.

1.3.5 Die Nutzung von Cloud-Diensten

Fast jeder nutzt in irgendeiner Art und Weise verschiedene Cloud-Dienste, wie z. B. soziale Netzwerke, Online-Speicher, Online Shops oder Streaming-Dienste.

Diese Dienste speichern Daten ihrer Nutzer. Teils ist diese Daten-Speicherung notwendig, teils erfolgt sie nur aus Werbe- und Verdienstgründen. Eins hat diese Speicherung jedoch gemein: Sollte ein nicht autorisierter Dritter Zugang zu diesen Daten erhalten, stellt dies sowohl für den Dienst selbst als auch für dessen Nutzer ein erhebliches Problem dar.

So können Anmeldedaten, persönliche Dateien, private Nachrichten, medienbezogene Vorlieben oder andere wichtige Daten der Nutzer offengelegt werden.

Wird ein Nutzer-Passwort offenbart, welches gleichzeitig auch für andere Dienste verwendet wird, hat der Angreifer auf einen Schlag Zugang zu den Nutzer-Konten mehrerer Dienste erlangt.

1.3.6 Wichtige Daten

Wir alle speichern jede Menge Daten auf unserem persönlichen Computer. Auch wenn wir denken, dass dieser nicht verloren gehen könnte, liegen doch auf jedem Computer Daten, die man bei Verlust schmerzlich vermissen würde. Sind es Urlaubsbilder und -videos, ärztliche Dokumente, Bewerbungen, Passwörter, Sicherungskopien anderer Geräte oder andere wichtige private oder dienstliche Dokumente.

Erst wenn diese verloren gegangen sind, fehlen sie uns. Aus diesem Grund ist es zwingend notwendig, Sicherheitskopien der eigenen wichtigen Daten anzulegen. Dies kann mithilfe von externen Datenträgern oder Cloud-Speichern erfolgen.

Die Erstellung solcher Sicherheitskopien (engl. Backups) ist meist in wenigen Minuten eingerichtet. Die Wiederbeschaffung von verlorenen Daten ist um ein Vielfaches aufwendiger und kostspieliger.

1.3.7 Soziale Netzwerke

In sozialen Netzwerken legen Nutzer ein Profil an, um die eigene Person im Internet gegenüber anderen Menschen zu repräsentieren. Man verbindet sich mit Freunden, tauscht Fotos und Nachrichten aus oder lädt sich gegenseitig zu Veranstaltungen ein.

Doch was passiert, wenn ein Angreifer Zugriff zum persönlichen Profil erhält?

Der Angreifer kann dann sämtliche Inhalte einsehen und die eigene Identität im Internet übernehmen. Die persönlichsten Geheimnisse können offengelegt, teuer an weitere Kriminelle im Internet verkauft, oder zur Erpressung des Profil-Inhabers verwendet werden.

1.3.8 Wie müssen die verschiedenen Anwendungsbereiche geschützt werden?

Im Laufe dieses WBT haben wir erfahren, was die unterschiedlichen Risiken und Konsequenzen einer vernachlässigten IT-Sicherheit sein können und haben im Rahmen dieser verschiedene Begriffe betrachtet.

Anschließend erfolgte eine Beleuchtung der unterschiedlichen zu schützenden Anwendungsbereiche.

Nun wissen wir also, wo wir ansetzen sollten, um die persönliche IT-Sicherheit zu stärken. Wir wissen nur noch nicht, wie wir das anstellen.

Die verschiedenen Maßnahmen zur Steigerung der persönlichen IT-Sicherheit werden wir uns in den nachfolgenden zwei WBT anhand der Familie Müller anschauen.

1.4 Typische Aufgabenstellungen

Zur Bearbeitung dieser Aufgabenstellungen beachten Sie bitte: Verlangt ist eine fachlich zutreffende, inhaltlich nachvollziehbare und kausal zusammenhängende Erörterung aus vollständigen Sätzen in lesbarer Handschrift. Für jede Aufgabe: Maximal zwei Seiten Text!

Aufgabe 1: Erläutern Sie die Notwendigkeit von IT-Sicherheitsmaßnahmen, verwenden Sie prägnante Beispiele / typische Szenarien, um diese Notwendigkeit aufzuzeigen.

Aufgabe 2: Erläutern Sie typische Risiken und Konsequenzen vernachlässigter IT-Sicherheit.

Aufgabe 3: Erläutern Sie die Begriffe Computersicherheit, Datensicherung, Datensicherheit und Datenschutz.

Aufgabe 4: Nennen Sie drei schützenswerte Bereiche und begründen Sie, warum es sich hier lohnt, die persönliche IT zu schützen.

2 IT-Sicherheit im Eigenheim – Privates Netzwerk

2.1 IT-Sicherheit am Beispiel der Familie Müller

2.1.1 Was Sie bisher wissen ...

Im vorangegangenen WBT haben Sie bereits die Grundlagen zum Thema IT-Sicherheit kennengelernt.

In Kapitel 1 des ersten WBT haben Sie erfahren, wie intensiv wir Menschen digitale Geräte und damit auch das Internet im Alltag nutzen,

- warum es notwendig ist, sich mit IT-Sicherheitsmaßnahmen zu befassen und
- welche Risiken und Konsequenzen aus einer vernachlässigten IT-Sicherheit entstehen und wie mit diesen umgegangen werden kann.

In Kapitel 2 des ersten WBT haben Sie erfahren, was unter den Begriffen „Computersicherheit“, „Datensicherheit“, „Datensicherung“ und „Datenschutz“ verstanden wird.

In Kapitel 3 des ersten WBT haben Sie des Weiteren gelernt, welche Bereiche es zu schützen gilt. Dabei wurden insbesondere die Bereiche „Privates Netzwerk“, „Smart Home“, „Einkaufen und Bezahlen im Internet“, „Cloud-Dienste“, „Wichtige Daten“ und „Soziale Netzwerke“ betrachtet.

2.1.2 Familie Müller

Familie Müller:

> Hallo, wir sind die Müllers.
>
> Wir sind Hans, Anette, Timo und Lisa.
>
> Wir wohnen in einem Einfamilienhaus und haben über die Zeit eine ganz schöne Menge an Geräten und Haushaltsgegenständen angesammelt und nutzen viele verschiedene Online-Dienste wie Web Shops, Cloud-Speicher und soziale Netzwerke.
>
> Auch hat sich bei uns inzwischen eine nicht zu unterschätzende Menge an wichtigen Dokumenten digital angesammelt. Dazu gehören beispielweise Ausweisdokumente, Urkunden oder auch Familienfotos.
>
> Leider haben wir jedoch ein wenig den Überblick verloren, wie es dabei um die IT-Sicherheit bestellt ist. Gerade erst haben wir von Bekannten erfahren, wie prekär es sein kann, wenn man Opfer eines IT-Sicherheitsvorfalls wird. Man hat auf einmal mit ungeahnten Problemen zu tun. Unsere Freunde erhielten beispielsweise Post von Inkasso-Büros, Anwälten und von Web Shops bzgl. nicht bezahlter Rechnungen, obwohl sie nichts bestellt hatten.

Wir sind uns in einem sicher – wir müssen uns um unsere private IT-Sicherheit kümmern, damit uns so etwas nicht auch passiert.

2.1.3 Maßnahmen zur Steigerung der persönlichen IT-Sicherheit

Familie Müller:

Aus dem vorangegangenen WBT wissen wir nun also, wo wir ansetzen sollten, um die persönliche IT-Sicherheit zu erhöhen. Wir wissen nur noch nicht, wie wir dabei vorgehen sollten.

Die Möglichkeiten und Maßnahmen zur Steigerung der persönlichen IT-Sicherheit können sehr umfangreich und vielfältig sein. Um den Überblick nicht zu verlieren, sollte deshalb geplant und strukturiert vorgegangen werden. So kann es beispielsweise hilfreich sein, einzelne Maßnahmen anhand von praktischen Anwendungen zu betrachten.

Aus diesem Grund zeigen wir anhand unserer Familie, wie wir im Privaten mit dem Thema IT-Sicherheit umgehen.

2.1.4 Die verschiedenen Anwendungsbereiche

In WBT 1 haben wir bereits sechs Anwendungsbereiche kennengelernt, die uns helfen können, unsere private IT-Sicherheit deutlich zu erhöhen.

Diese sechs Anwendungsbereiche schauen wir uns nachfolgend im Detail an und werden sie mit konkreten Maßnahmen sicherer gestalten.

Da dies eine nicht zu unterschätzende Aufgabe ist, werden wir uns in diesem WBT zuerst um unser privates Netzwerk kümmern. Die nachfolgenden WBT betrachten anschließend die weiteren fünf Anwendungsgebiete.

2.2 Das private Netzwerk

2.2.1 Das private Netzwerk

Wir betrachten jetzt unser privates Netzwerk. Dies besteht aus allen Geräten (Knoten) in unserem Haus, die an den Router angeschlossen sind oder untereinander kommunizieren. Hinzu kommen alle Verbindungen (Kanten), welche die jeweiligen Geräte mit dem Internet verbinden.

- Router
- Computer
- Smartphones
- Tablets
- Smart TVs
- Überwachungskameras
- Thermostate und Lampen
- Staubsauger
- Kühlschränke
- Waschmaschine
- LAN und WLAN
- Bluetooth
- Verbindungen im Smart Home

Geräte wie Thermostate, Lampen, Staubsauger, Kühlschränke und Waschmaschinen betrachten wir im zweiten Anwendungsgebiet „Smart Home“.

2.2.2 Privates Netzwerk – Inventur aller Geräte im Eigenheim

Wir haben den Überblick verloren und wissen inzwischen nicht mal mehr, welche Geräte überhaupt in unserem privaten Netzwerk vorhanden sind.

Bevor mit der Planung von IT-Sicherheitsmaßnahmen begonnen werden kann, müssen wir uns erst einmal einen strukturierten Überblick über unser Zuhause verschaffen.

Einen Smart TV und Tablets haben wir schon mal nicht, aber einen Router, Computer, Smartphones, Überwachungskameras, WLAN- und LAN-Verbindungen setzen wir definitiv in unserem Eigenheim ein.

Am Besten inventarisieren wir zunächst einmal alle Geräte und Verbindungen in unserem privaten Netzwerk.

2.2.3 Inventur aller Geräte im Eigenheim der Familie Müller

Soo, das war ein ganz schönes Stück Arbeit. Wir sind in jede Ecke und jeden Winkel in unserem Haus gekrochen und haben angefangen, unsere Geräte einmal aufzulisten.

Nun wissen wir genau, welche Geräte wir im Einsatz haben, wo diese stehen und wie diese vernetzt sind.

Gerät	Standorte	Art der Vernetzung
Laptops	Arbeitszimmer, Wohnzimmer	WLAN, LAN
Smartphones	Kein fester Standort	WLAN
Thermostate	Im gesamten Haus	WLAN
Überwachungskameras	Vor der Haustür und im Garten	WLAN, LAN
Router	Im Arbeitszimmer	WLAN, LAN
...	...	...
...	...	...

Abb. 4: Inventur aller Geräte im Eigenheim der Familie Müller

2.2.4 Allgemeine Maßnahmen zur Sicherung des privaten Netzwerks

Für die soeben betrachteten Elemente in unserem privaten Netzwerk lassen sich Maßnahmen definieren, die wir für alle Elemente umsetzen sollten. Schauen wir uns die Maßnahmen erst einmal allgemein an. In den folgenden Kapiteln werden wir diese Maßnahmen konkretisieren. Dabei beginnen wir mit der Sicherheit unseres Routers.

Folgende allgemeine Maßnahmen sollten wir bei den Geräten und Verbindungen in unserem privaten Netzwerk umsetzen:

- Software-Updates herunterladen und aktivieren
- Passwort-Schutz für Nutzer-Accounts aktivieren
- Standard-Passwörter durch individuelle und sichere Passwörter ersetzen
- Verbindungen im privaten Netzwerk (WLAN, LAN etc.) sichern
- Werkseinstellungen überprüfen (Datenschutz /Telemetrie)
- Nicht notwendige Funktionen deaktivieren
- Firewall-Einstellungen überprüfen (muss ein Gerät von überall erreichbar sein?)
- Fernzugänge absichern

2.3 Maßnahmen zur Sicherung des Routers im privaten Netzwerk

2.3.1 Router: Umsetzung konkreter Maßnahmen

Hans:

Schauen wir uns zuerst unseren Router und dessen Verbindungen (WLAN, LAN etc.) in unserem privaten Netzwerk an.

Timo, den Router hast Du eingerichtet. Welche Maßnahmen können wir hier konkret umsetzen?

Timo:

Genau Papa, ich habe unseren Router eingerichtet. Wir setzen wie zahlreiche andere Haushalte in Deutschland eine Fritzbox ein.

Im Administrationsbereich der Fritzbox lassen sich konkrete Maßnahmen zur individuellen Absicherung des eigenen Netzwerks konfigurieren.

Konkrete Maßnahmen zur Sicherung des Routers:

- Auf Updates prüfen und ggf. durchführen
- Administrationspasswort ändern
- WLAN-Passwort ändern
- WLAN-Verschlüsselung auf WPA 2 + WPA 3 ändern, falls nicht bereits vorgegeben
- Verbundene Geräte überprüfen und zuordnen
- Verändern des Netzwerknamens
- Fernzugriff abschalten oder sicher konfigurieren
- (Optional): Gäste-WLAN einrichten
- (Fortgeschritten): SSID abschalten und WLAN nur noch manuell finden
- (Fortgeschritten): MAC-Filter als Zugangskontrolle einsetzen
- (Fortgeschritten): Falls Fernzugriff notwendig, VPN-Zugriff aktivieren

2.3.2 Aufrufen der Administrationsoberfläche der Fritzbox

Timo:

Um die konkreten Maßnahmen bei unserer Fritzbox umzusetzen, müssen wir uns zuerst Zugriff auf die Administrationsoberfläche unserer Fritzbox verschaffen.

Dazu muss ich mich mit unserem privaten Netzwerk verbinden und die IP-Adresse des Routers aufrufen. Standardmäßig lautet die IP-Adresse des Routers „192.168.0.1“. Wir haben aus verschiedenen Gründen eine andere IP-Adresse für unseren Router vergeben.

Ich logge mich schnell mit dem Administrationspasswort in die Administrationsoberfläche ein.

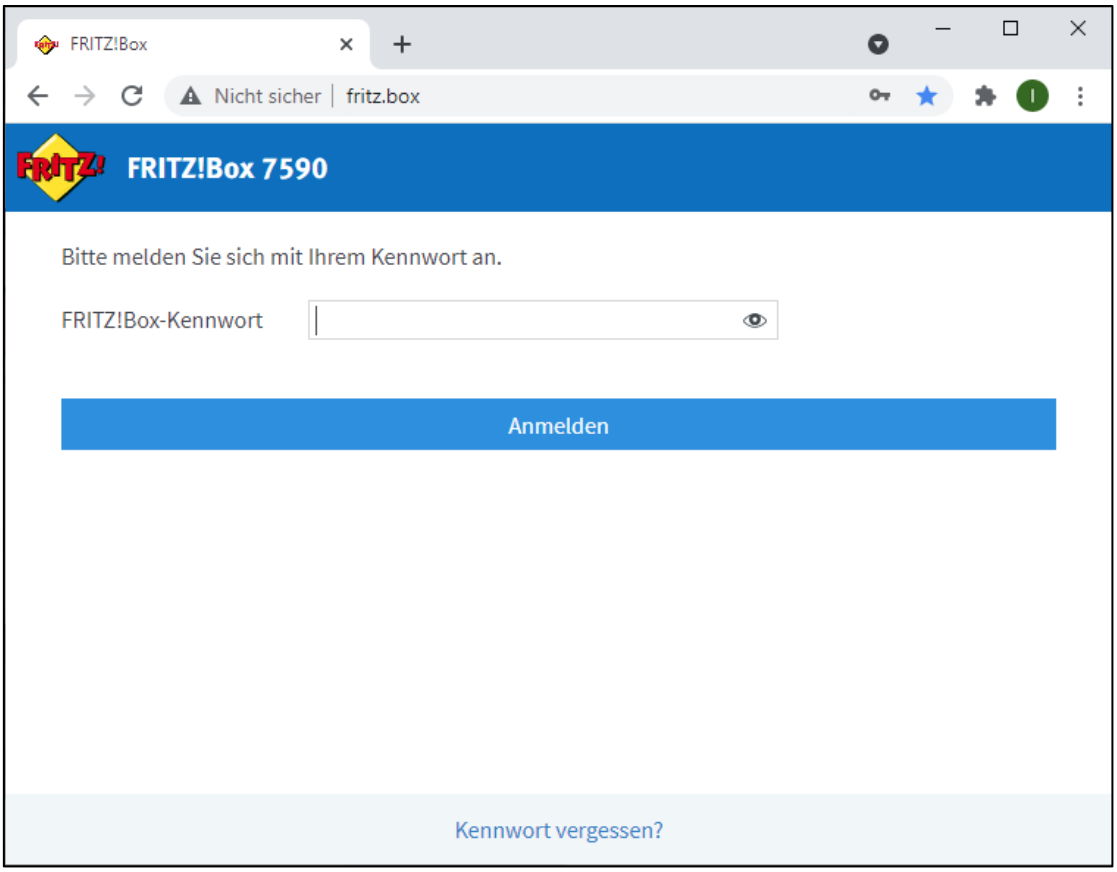


Abb. 5: Aufrufen der Administrationsoberfläche der Fritzbox

- Ihnen ist vielleicht aufgefallen, dass die Verbindung nicht gesichert (nicht per SSL-Zertifikat geschützt) ist.

  Dies ist an dieser Stelle kein Problem, da wir uns nur innerhalb unseres eigenen Netzes mit dem Router verbinden. Wir gehen davon aus, dass sich nur berechtigte Personen in unserem Netzwerk befinden.

- Alternativ zur IP des Routers können Sie auch dessen Hostname (Gerätenamen) eingeben, z. B. fritz.box oder fritz.repeater.
- Standardmäßig ist die FritzBox bereits mit einem mitgelieferten Passwort geschützt. Dieses müssen Sie initial hier eingeben.

2.3.3 Die Administrationsoberfläche der Fritzbox

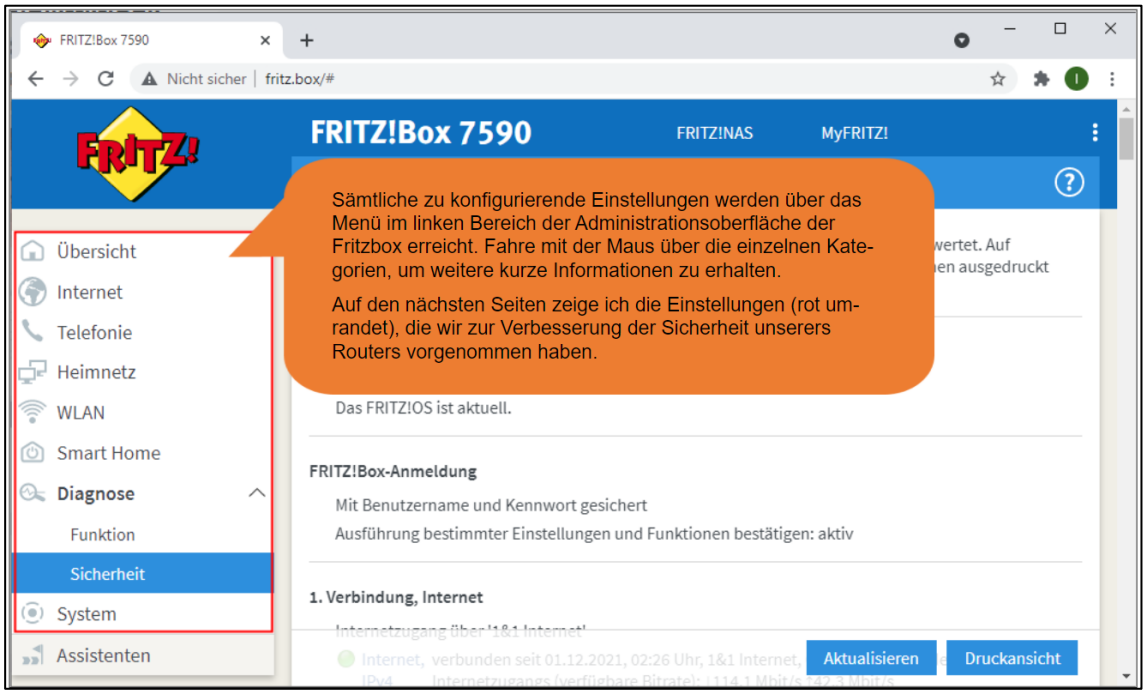


Abb. 6: Die Administrationsoberfläche der Fritzbox

- In der Kategorie „Übersicht“ erhalten Sie alle Statusinformationen Ihrer Fritz!Box auf einem Blick.
- In der Kategorie „Internet“ sehen Sie den Verbindungsstatus Ihrer FritzBox mit dem Internet.
- In der Kategorie „Telefon“ sehen Sie alle Informationen zu Ihren Telefonverbindungen.
- In der Kategorie „Heimnetz“ sehen Sie die Einstellungen zu Ihrem Heimnetz, die damit verbundenen Geräte, Verbindungen, Speicher etc.
- In der Kategorie „WLAN“ sehen Sie alle Einstellungen des WLAN bzgl. Funknetz, gewählten Kanälen, Sicherheitseinstellungen und Gastzugängen.
- In der Kategorie „Smart Home“ werden alle intelligenten Geräte im Heimnetz samt Einstellungen aufgelistet. Diese Kategorie werden wir uns im Anwendungsgebiet „Smart Home“ noch näher anschauen
- In der Kategorie „Diagnose“ können Sie Ihrer Fritz!Box auf Funktionstüchtigkeit überprüfen und Sicherheitseinstellungen vornehmen, die Ihre Fritzbox betreffen.
- In der Kategorie „System“ sehen Sie alle Ereignisse, also Logs zu Ihrer FritzBox, sowie die eingetragenen Nutzer.

2.3.4 Sicherheitseinstellungen der Fritzbox – Teil 1

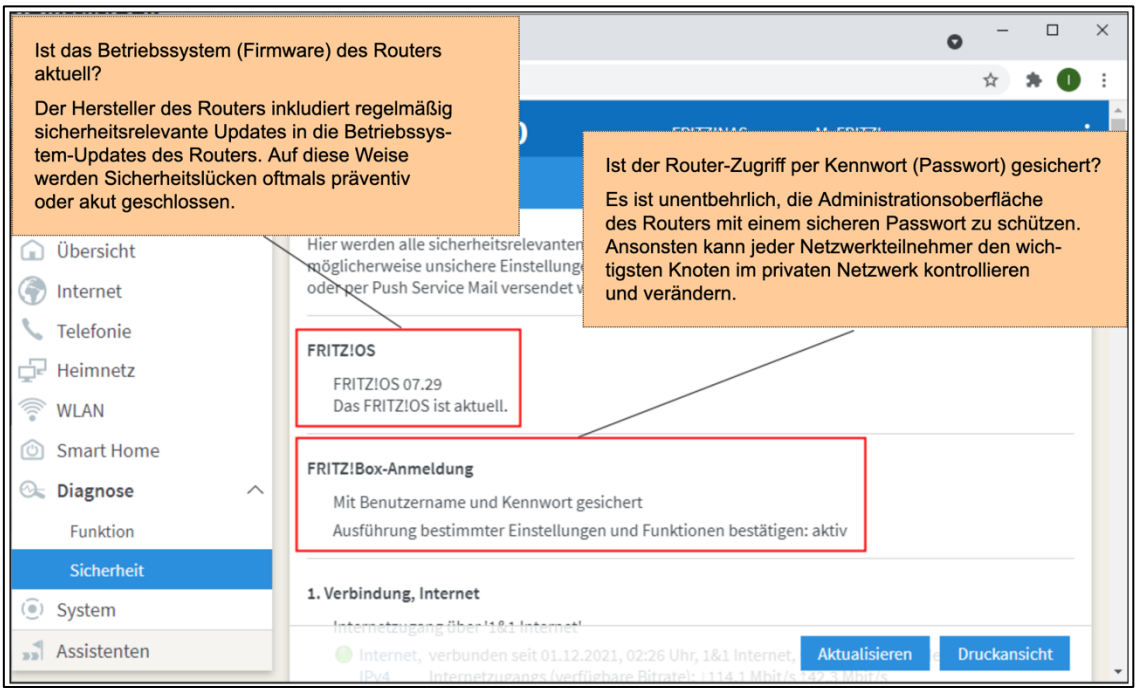


Abb. 7: Sicherheitseinstellungen der Fritzbox – Teil 1

2.3.5 Sicherheitseinstellungen der Fritzbox – Teil 2

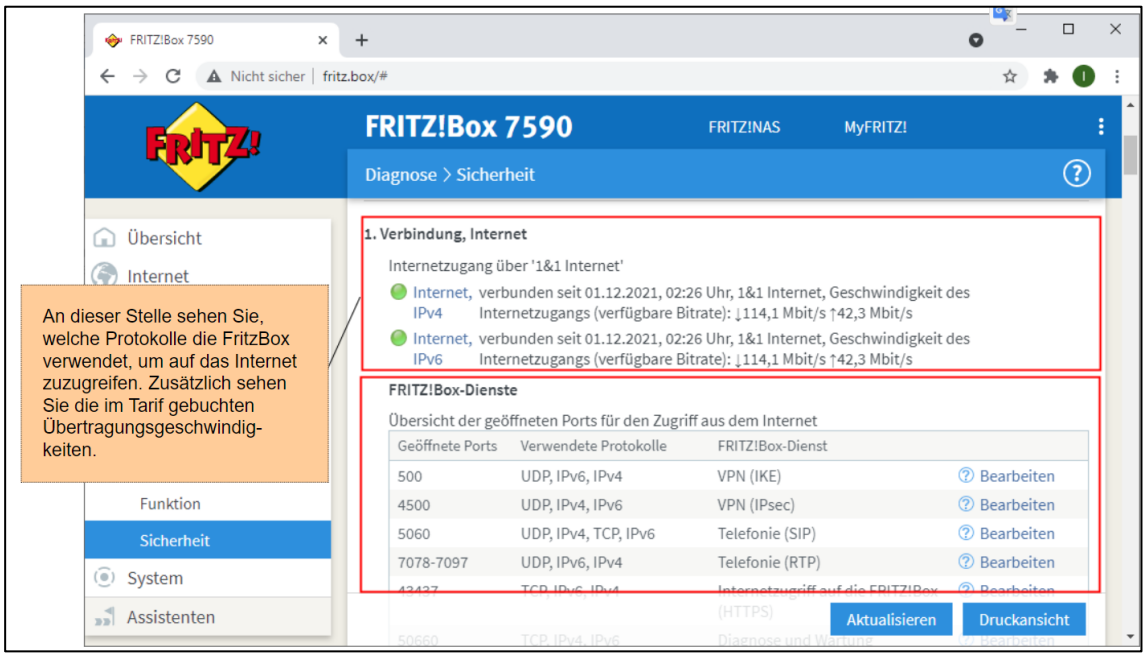


Abb. 8: Sicherheitseinstellungen der Fritzbox – Teil 2a

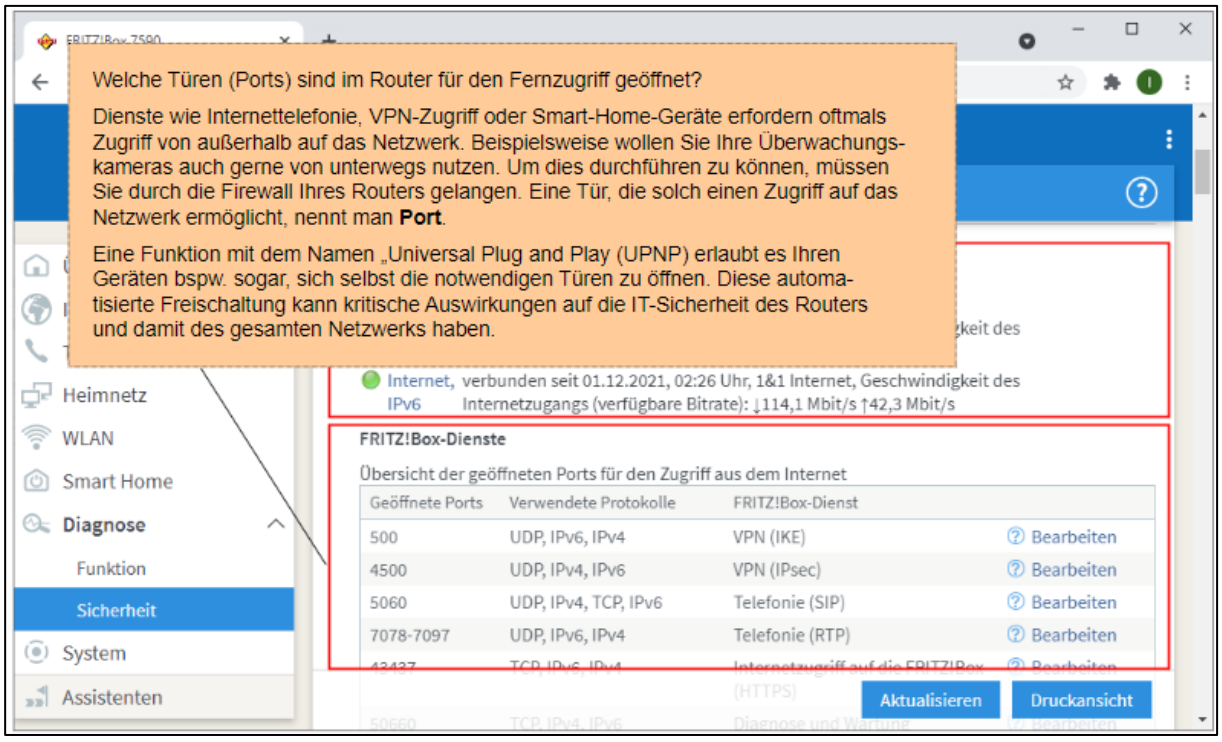


Abb. 9: Sicherheitseinstellungen der Fritzbox – Teil 2b

2.3.6 Fritzbox-Benutzer-Einstellungen

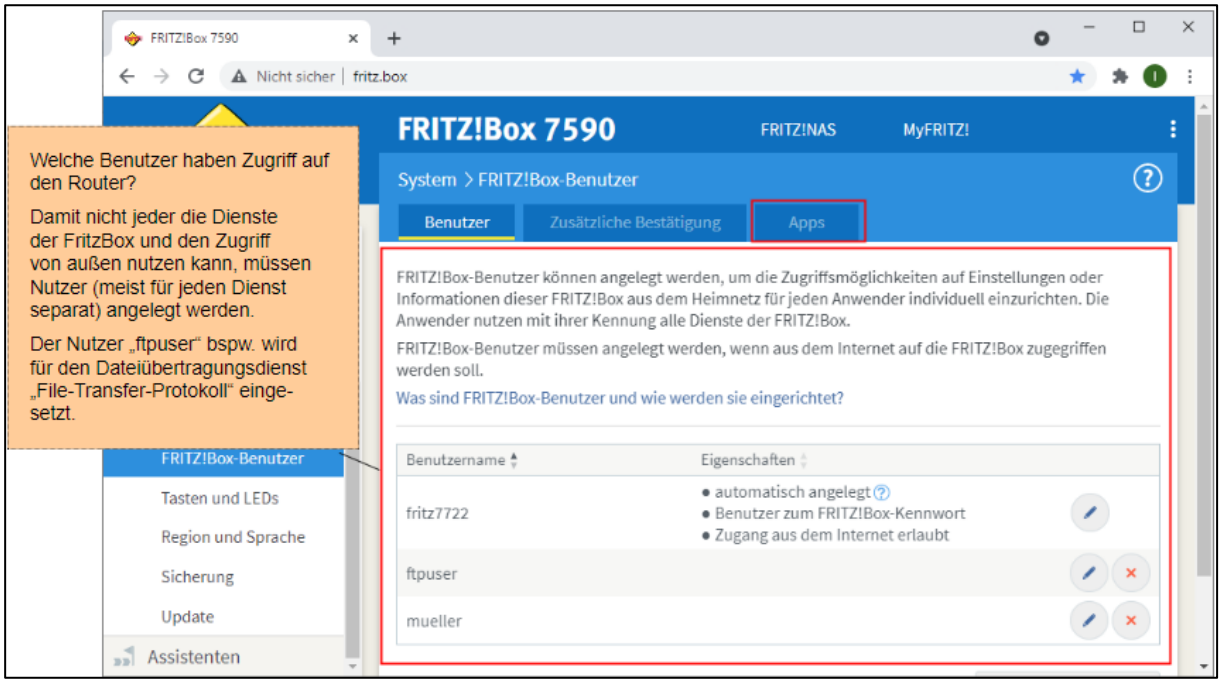


Abb. 10: Fritzbox-Benutzer-Einstellungen

2.3.7 WLAN-Sicherheit durch Passwort und Verschlüsselung

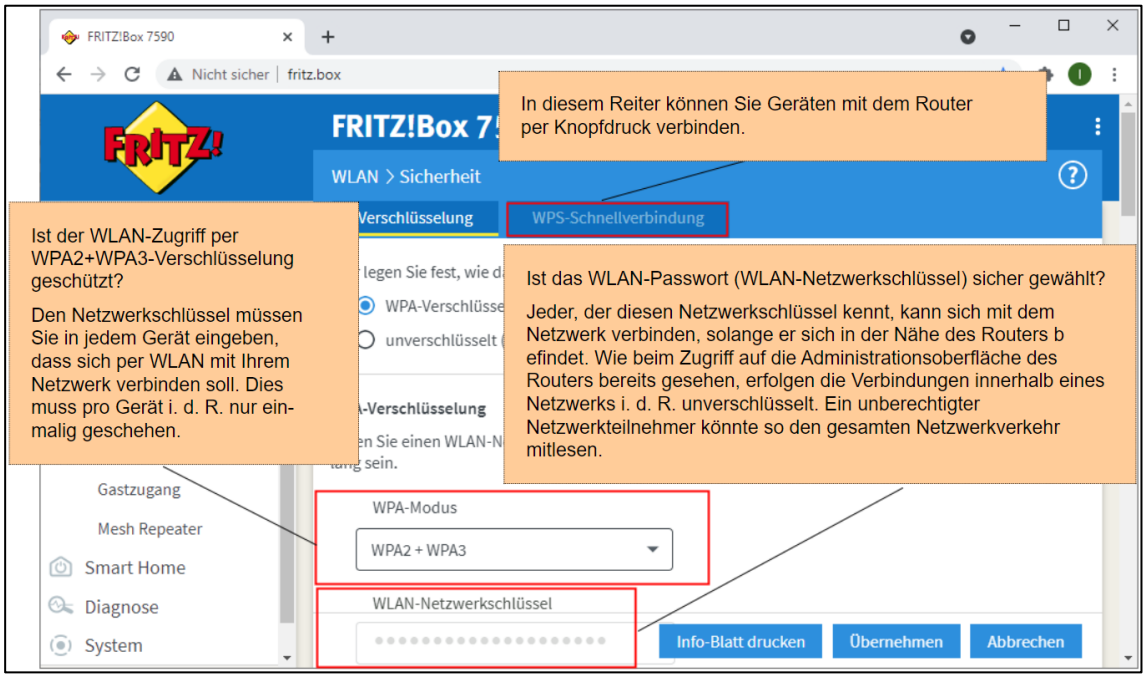


Abb. 11: WLAN-Sicherheit durch Passwort und Verschlüsselung

2.3.8 Geräte im privaten Netzwerk

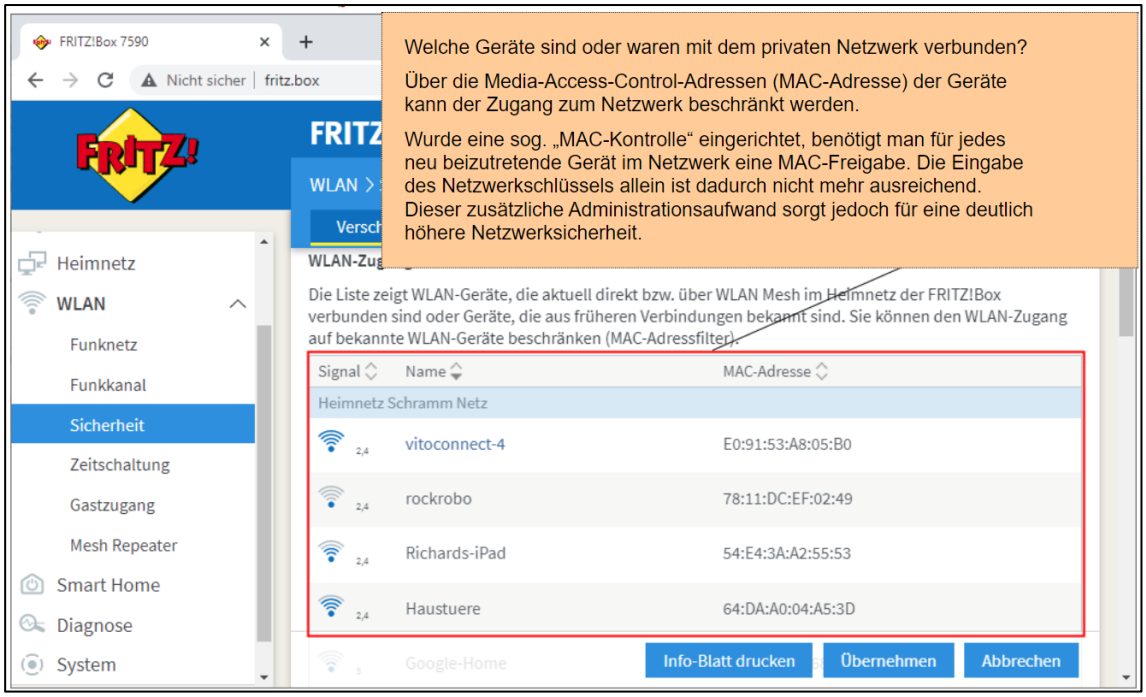


Abb. 12: Geräte im privaten Netzwerk

2.3.9 Name des WLAN-Funknetzes

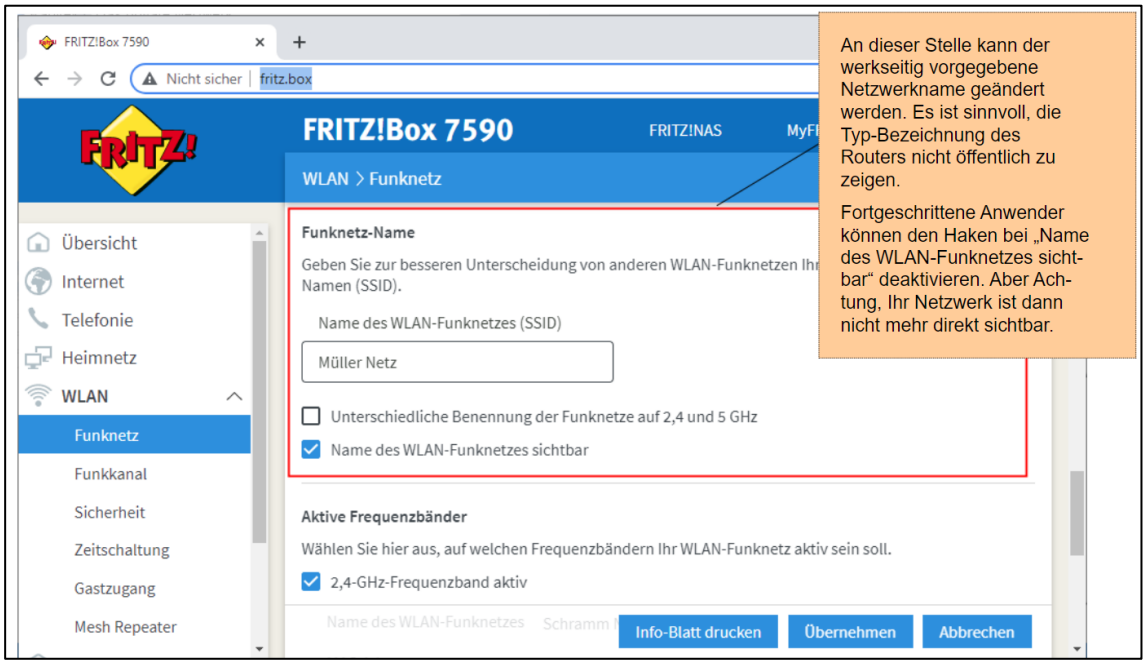


Abb. 13: Name des WLAN-Funknetzes

2.3.10 Umgesetzte Maßnahmen an der Fritzbox von Familie Müller

Timo:
Ich habe nun einige relevante Sicherheitsmaßnahmen am Beispiel unserer Fritzbox gezeigt. Es gibt darüber hinaus viele weitere Einstellungsmöglichkeiten, welche die Sicherheit unseres privaten Netzwerks erhöhen.

Konkrete Maßnahmen zur Sicherung des Routers:

- ✓ Auf Updates prüfen und ggf. durchführen
- ✓ Administrationspasswort ändern
- ✓ WLAN-Passwort ändern
- ✓ WLAN-Verschlüsselung auf WPA 2 ändern, falls nicht bereits vorgegeben
- ✓ Verbundene Geräte überprüfen und zuordnen
- ✓ Verändern des Netzwerknamens
- ✓ Fernzugriff abschalten oder sicher konfigurieren
- (Optional): Gäste-WLAN einrichten
- (Fortgeschritten): SSID abschalten und WLAN nur noch manuell finden
- (Fortgeschritten): MAC-Filter als Zugangskontrolle einsetzen
- (Fortgeschritten): Falls Fernzugriff notwendig, VPN-Zugriff aktivieren

2.3.11 Umsetzung konkreter Maßnahmen zur Sicherung der privaten Endgeräte

Lisa:

Als nächstes schauen wir uns unsere Endgeräte an. Dazu gehören Personal Computer (PC) und Smartphones. Tablets und Smartwatches besitzen wir nicht. Weitere Endgeräte wie bspw. Kühlschränke betrachten wir in der Einheit zum Anwendungsbereich Smart Home.

Wir beginnen am besten mit unseren PCs. Ich nutze ein MacBook, Mama hingegen arbeitet mit einem Windows-basierten PC. Ich zeige Euch die Umsetzung konkreter Maßnahmen anhand des Betriebssystems macOS.

Die Umsetzung der Maßnahmen für Windows zeigt Euch Mama im Anschluss.

2.4 macOS: Maßnahmen zur Sicherung der persönlichen Computer

2.4.1 macOS: Umsetzung konkreter Maßnahmen

Lisa:

In den Systemeinstellungen meines MacBooks lassen sich konkrete Maßnahmen zur individuellen Sicherheit durchführen.

Anette:

Super, Lisa. Vergiss aber nicht, dass diese Einstellungen alleine nicht ausreichen. Du musst grundsätzlich bedacht agieren, sobald Du Dich im Internet bewegst:

- bspw. beim Öffnen von E-Mail-Anhängen und -Links
- oder bei der Installation von Drittanbieter-Software.

Konkrete Maßnahmen zur Sicherung der privaten Endgeräte:

- Backups aktivieren und durchführen
- Auf Updates prüfen und ggf. durchführen
- Passwortschutz für Benutzerkonten
- Integrierten Viren- und Ransomware-Schutz aktivieren
- Festplatten-Verschlüsselung aktivieren
- Datenschutz bei der Anwendungsnutzung aktivieren
- (Fortgeschritten): Separaten Administrator-Account verwenden
- (Fortgeschritten): Benutzerkontensteuerung falls notwendig anpassen

2.4.2 Erste Maßnahmen an Lisas MacBook

Abb. 14: Maßnahmen: Backups aktivieren und durchführen

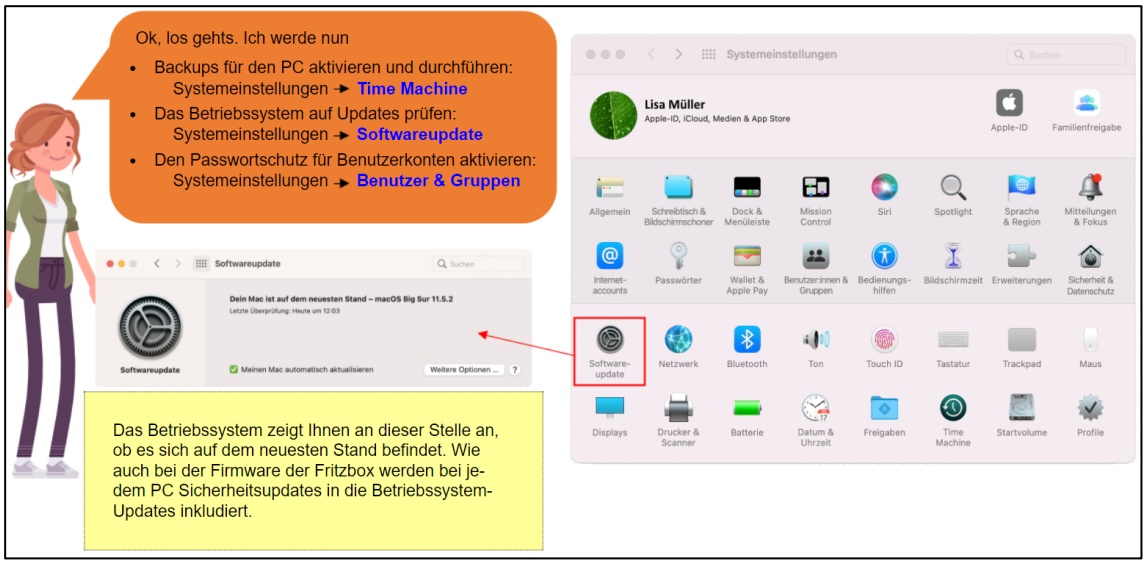


Abb. 15: Maßnahmen: Betriebssystem auf Updates prüfen

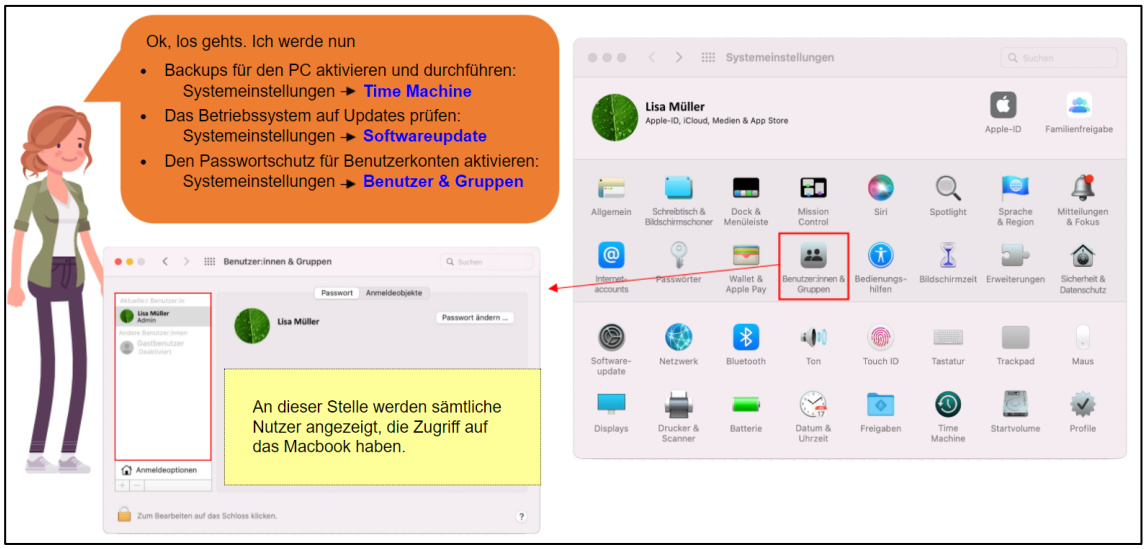


Abb. 16: Maßnahmen: Passwortschutz aktivieren

2.4.3 Weitere Systemeinstellungen

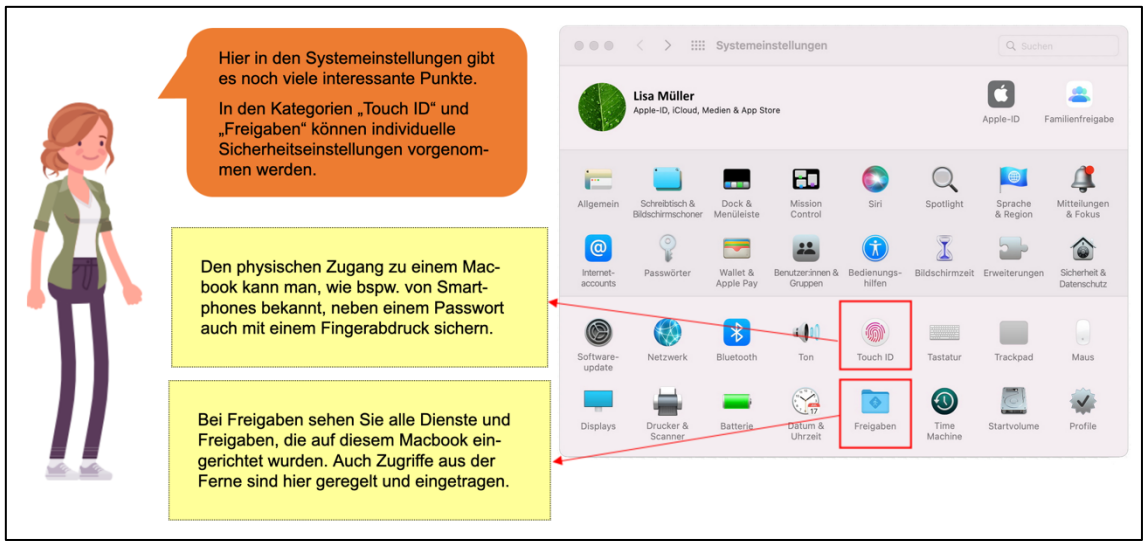


Abb. 17: Weitere Systemeinstellungen

2.4.4 Maßnahmen zum Viren- und Datenschutz an Lisas MacBook

Anette:

> Super, Lisa! Du hast jetzt für alle unsere Apple-Geräte Backups eingerichtet, diese auf Updates überprüft und Passwort-Schutzmechanismen eingerichtet.
>
> Wie sehen denn die Maßnahmen zum Viren- und Datenschutz bei macOS-basierten Computern aus?

Lisa:

Ah gut, dass Du es sagst! Das wäre mir jetzt beinahe entfallen. Gut, schauen wir uns schnell noch die Maßnahmen an. Die finden wir in den Systemeinstellungen unter Sicherheit & Datenschutz. Folgende Einstellungen sollten wir vornehmen:

- Festplatten-Verschlüsselung aktivieren
- Integrierten Viren- und Ransomware-Schutz sowie Firewall aktivieren
- Datenschutz bei der Anwendungsnutzung

Auf den nächsten Seiten zeige ich Euch, wie diese Einstellungen vorzunehmen sind.

2.4.5 Festplatten-Verschlüsselung aktivieren

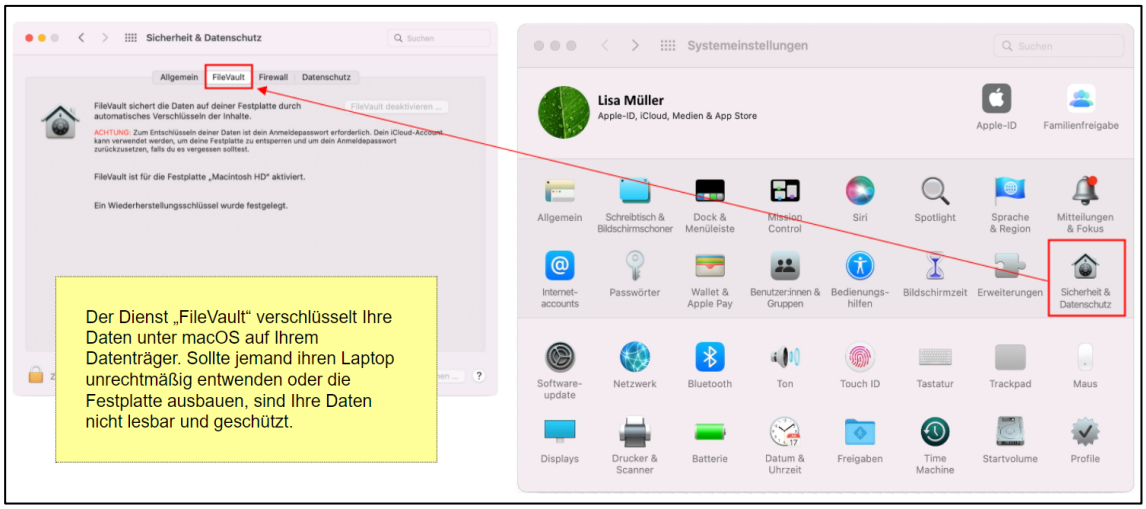


Abb. 18: Festplatten-Verschlüsselung aktivieren

2.4.6 Integrierten Viren- und Ransomware-Schutz sowie Firewall aktivieren

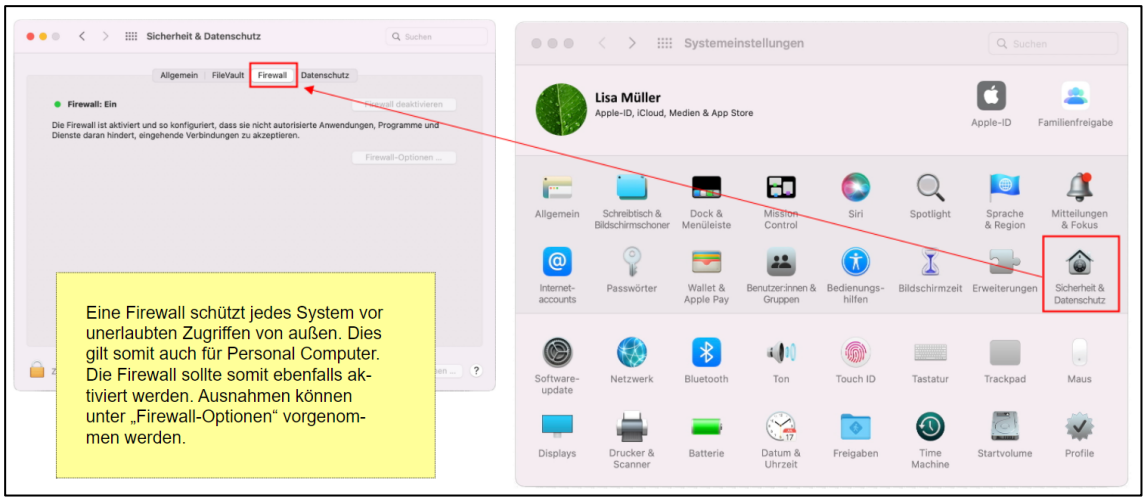


Abb. 19: Integrierten Viren- und Ransomware-Schutz sowie Firewall aktivieren

2.4.7 Datenschutz bei der Anwendungsnutzung

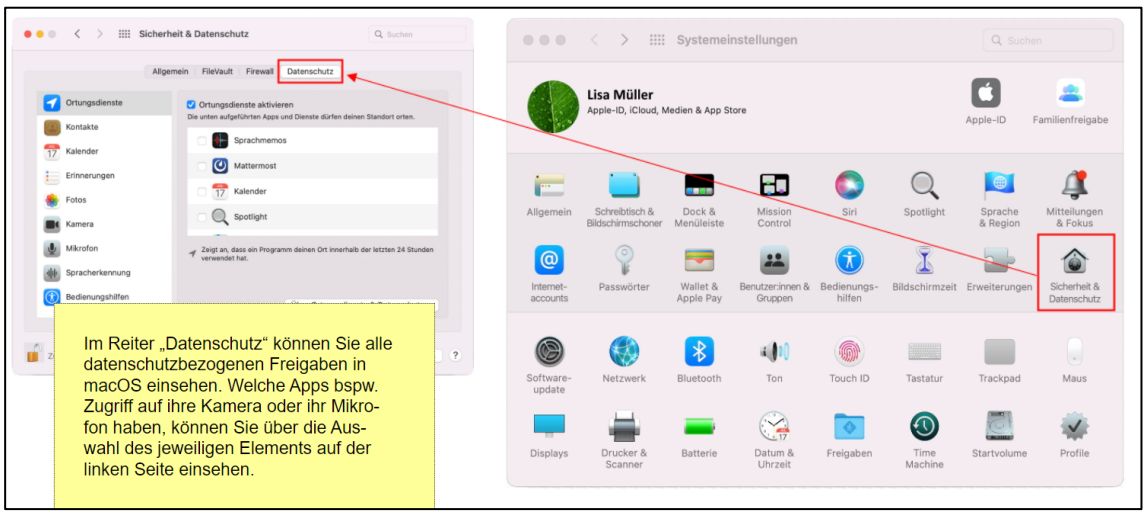


Abb. 20: Datenschutz bei der Anwendungsnutzung

2.4.8 Umgesetzte Maßnahmen am MacBook von Lisa Müller

Lisa:

> Ich habe nun einige relevante Sicherheitsmaßnahmen an meinem MacBook durchgeführt.
>
> Es gibt darüber hinaus weitere (fortgeschrittene) Einstellungsmöglichkeiten, welche die Sicherheit von privaten Endgeräten zusätzlich erhöhen.

Konkrete Maßnahmen zur Sicherung der privaten Endgeräte

- ✓ Backups aktivieren und durchführen
- ✓ Auf Updates prüfen und ggf. durchführen
- ✓ Passwortschutz für Benutzerkonten
- ✓ Integrierten Viren- und Ransomware-Schutz aktivieren
- ✓ Festplatten-Verschlüsselung aktivieren
- ✓ Datenschutz bei der Anwendungsnutzung aktivieren
- (Fortgeschritten): Separaten Administrator-Account verwenden
- (Fortgeschritten): Benutzerkontensteuerung falls notwendig anpassen

2.5 Windows: Maßnahmen zur Sicherung der persönlichen Computer

2.5.1 Windows: Umsetzung konkreter Maßnahmen

Anette:

> Okay Lisa, Du hast nun unsere macOS-basierten PC deutlich sicherer eingerichtet. Klasse! Ich will nun das Gleiche bei unserem Windows-basierten PC umsetzen.
>
> In den Systemeinstellungen meines Windows-PCs lassen sich konkrete Maßnahmen zur individuellen Sicherheit durchführen.

Lisa:

> Super, Mama. Vergiss aber nicht, dass diese Einstellungen alleine nicht ausreichen. Du musst grundsätzlich bedacht agieren, sobald Du Dich im Internet bewegst:
>
> - bspw. beim Öffnen von E-Mail-Anhängen und -Links
> - oder bei der Installation von Drittanbieter-Software.

Konkrete Maßnahmen zur Sicherung der privaten Endgeräte

- Backups aktivieren und durchführen
- Auf Updates prüfen und ggf. durchführen
- Passwortschutz für Benutzerkonten
- Integrierten Viren- und Ransomware-Schutz aktivieren
- Festplatten-Verschlüsselung aktivieren
- Datenschutz bei der Anwendungsnutzung aktivieren
- (Fortgeschritten): Separaten Administrator-Account verwenden
- (Fortgeschritten): Benutzerkontensteuerung falls notwendig anpassen

2.5.2 Erste Maßnahmen an Anettes Microsoft Windows PC

Ok, los gehts. Ich werde nun für unsere Windows-basierten PC

- die Backups für den PC aktivieren und durchführen:
  Einstellungen → Update und Sicherheit → Sicherung
- Das Betriebssystem auf Updates prüfen:
  Einstellungen → Update und Sicherheit → Windows Update
- Den Passwortschutz für Benutzerkonten aktivieren:
  Einstellungen → Konten → Anmeldeoptionen

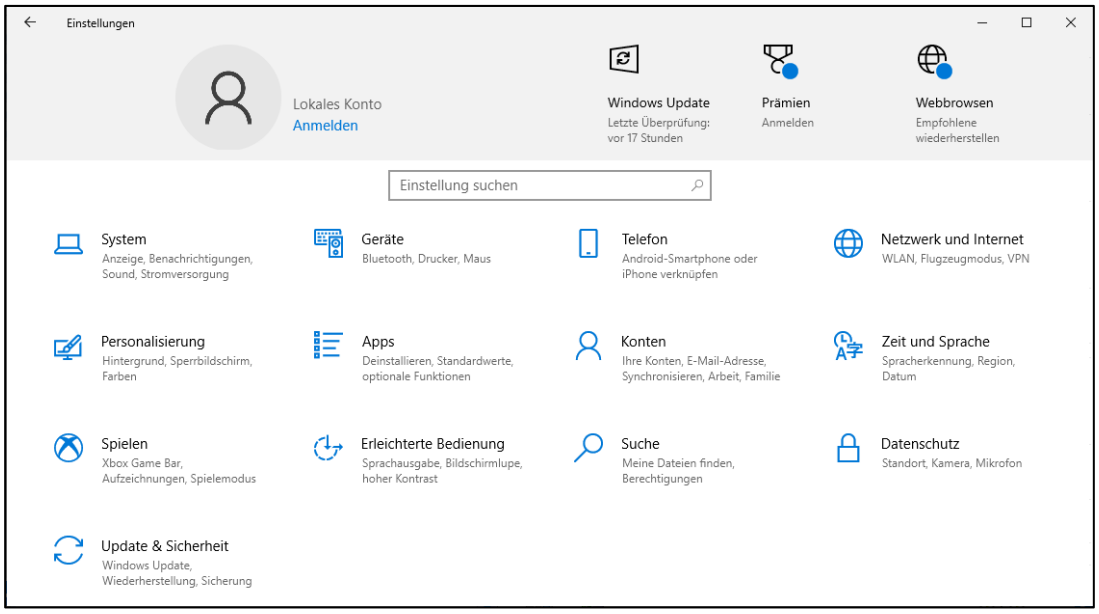


Abb. 21: Windows-Einstellungen

Das Fenster „Einstellungen“ ermöglicht unter Windows die Durchführung der meisten sicherheitsrelevanten Einstellungen.

Die Bereiche „Datenschutz“, „System“, „Konten“ und „Update und Sicherheit“ sind dabei besonders relevant.

2.5.3 Backups aktivieren

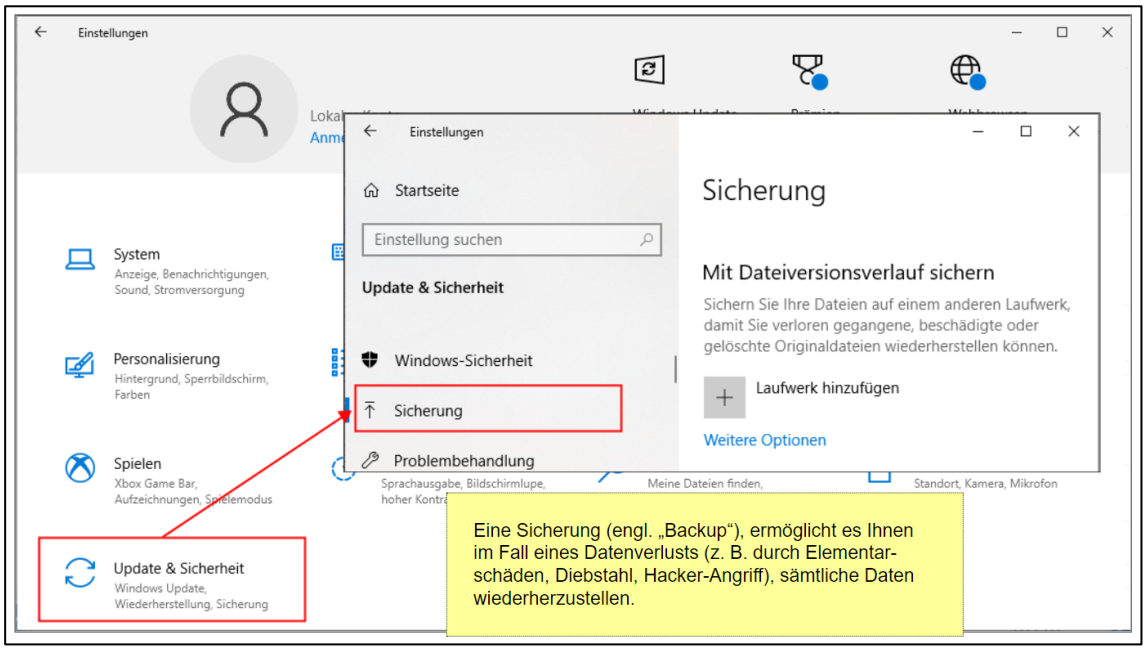


Abb. 22: Backups aktivieren

2.5.4 Das Betriebssystem auf Updates prüfen

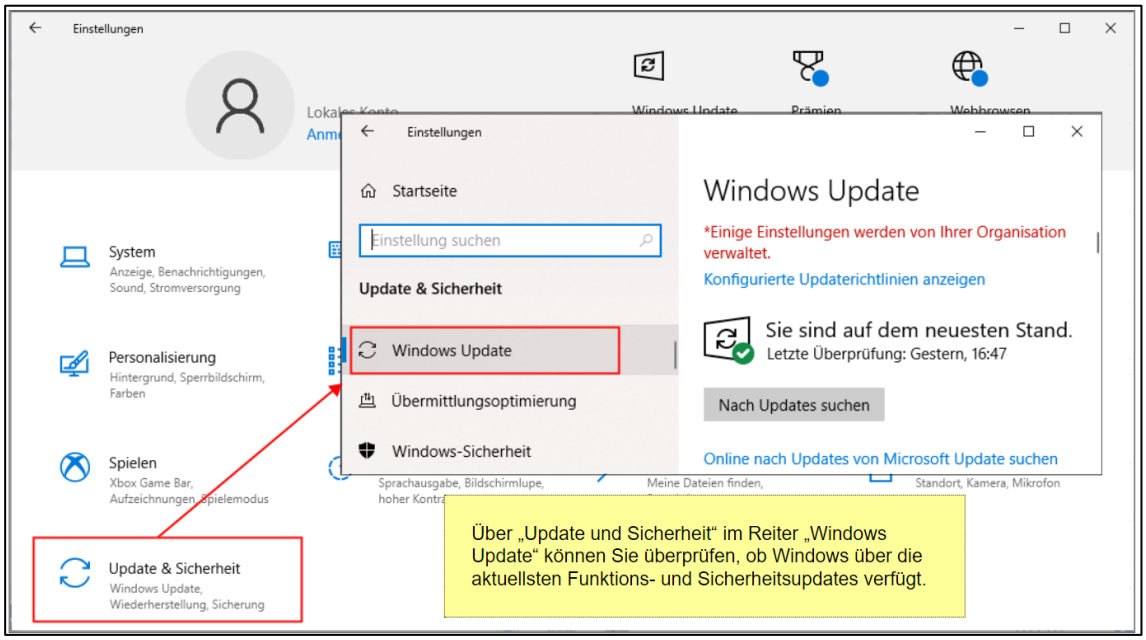


Abb. 23: Das Betriebssystem auf Updates prüfen

2.5.5 Passwortschutz für Benutzerkonten aktivieren

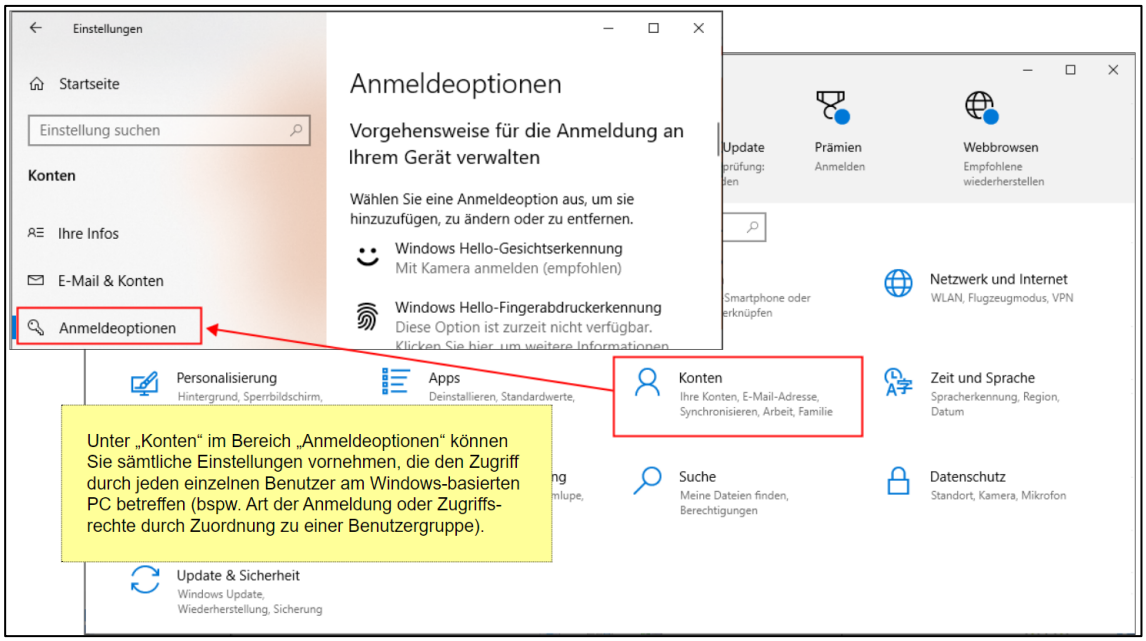


Abb. 24: Passwortschutz für Benutzerkonten aktivieren

2.5.6 Maßnahmen zum Viren- und Datenschutz an Anettes Windows-PC

Lisa:

> Super, Mama, Du hast jetzt für alle unsere Windows-Geräte Backups eingerichtet, diese auf Updates überprüft und Passwort-Schutzmechanismen aktiviert.
>
> Wie sehen denn die Maßnahmen zum Viren- und Datenschutz bei Windows-basierten Computern aus?

Anette:

> Ah gut, dass Du es sagst! Das wäre mir jetzt beinahe entfallen. Gut, schauen wir uns schnell noch die Maßnahmen zum Viren- und Datenschutz an. Folgende Einstellungen sollten wir vornehmen:
>
> - Integrierten Viren- und Ransomware-Schutz sowie Firewall aktivieren
> - Datenschutzeinstellungen bei der Anwendungsnutzung
>
> Auf der nächsten Seite zeige ich Euch, wie diese Einstellungen vorzunehmen sind.

2.5.7 Umsetzung der Maßnahmen zum Viren- und Datenschutz

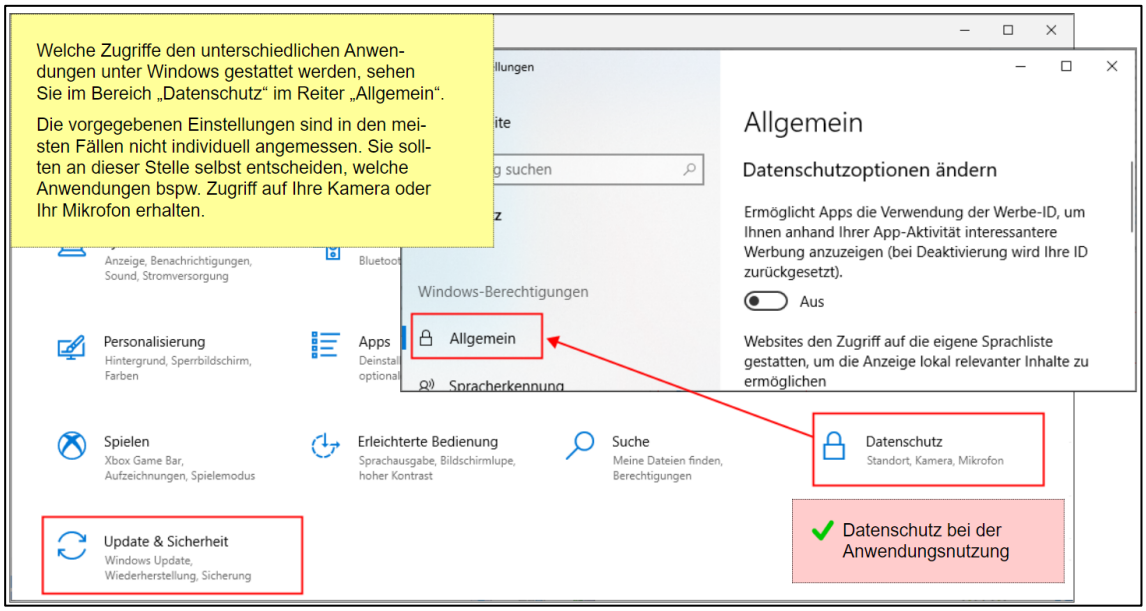


Abb. 25: Umsetzung der Maßnahmen zum Datenschutz

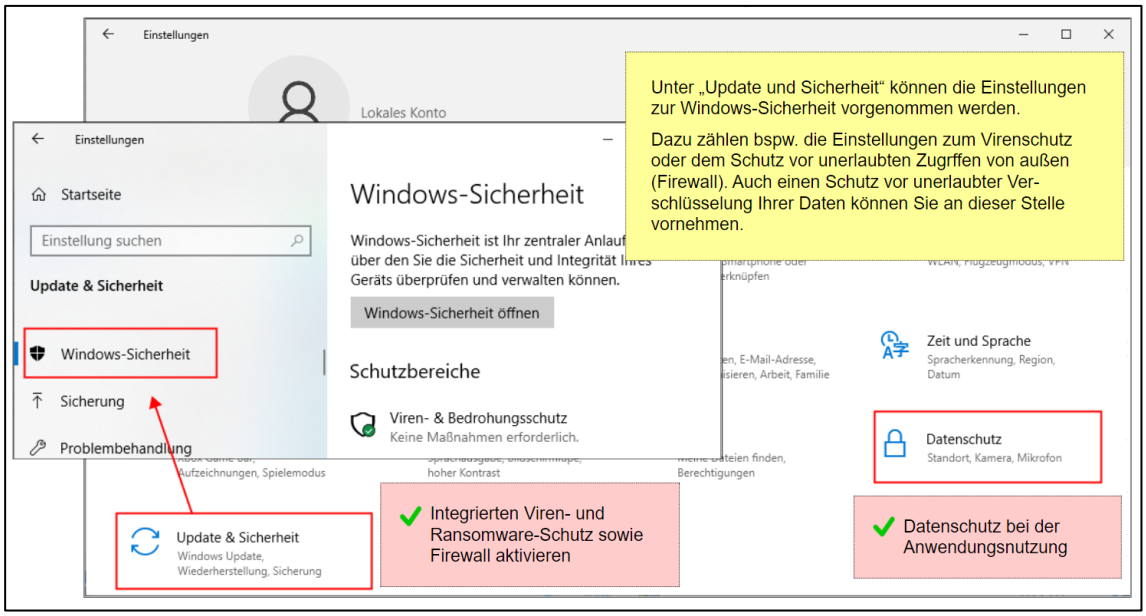


Abb. 26: Umsetzung der Maßnahmen zum Virenschutz

2.5.8 Maßnahmen zur Festplattenverschlüsselung an Windows-basierten Computern

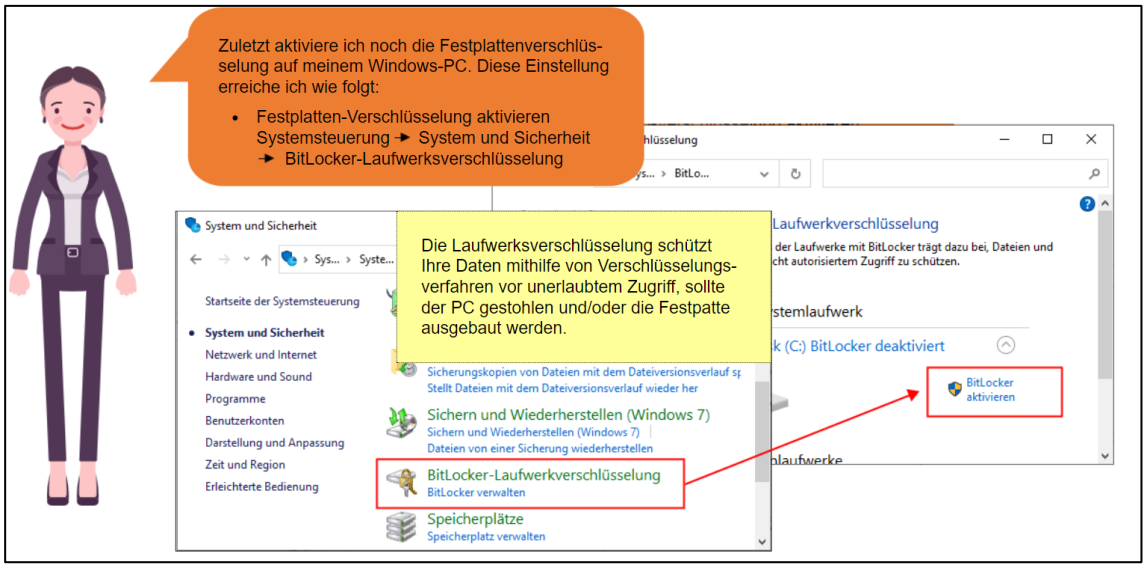


Abb. 27: Maßnahmen zur Festplattenverschlüsselung an Windows-basierten Computern

2.5.9 Umgesetzte Maßnahmen am Microsoft Surface von Anette Müller

Anette:

> Ich habe nun einige relevante Sicherheitsmaßnahmen an meinem Windows-PC durchgeführt.
>
> Es gibt darüber hinaus weitere (fortgeschrittene) Einstellungsmöglichkeiten, welche die Sicherheit von privaten Endgeräten zusätzlich erhöhen.

Konkrete Maßnahmen zur Sicherung der privaten Endgeräte

- ✓ Backups aktivieren und durchführen
- ✓ Auf Updates prüfen und ggf. durchführen
- ✓ Passwortschutz für Benutzerkonten
- ✓ Integrierten Viren- und Ransomware-Schutz aktivieren
- ✓ Festplatten-Verschlüsselung aktivieren
- ✓ Datenschutz bei der Anwendungsnutzung aktivieren
- (Fortgeschritten): Separaten Administrator-Account verwenden
- (Fortgeschritten): Benutzerkontensteuerung falls notwendig anpassen

2.5.10 Genug für heute!

Familie Müller:

> Okay super, unser privates Netzwerk haben wir nun deutlich besser vor Angriffen von außen geschützt. Dabei haben wir uns besonders unseren Router und unsere persönlichen Computer angesehen. Unsere private IT-Sicherheit ist dadurch enorm gestiegen.
>
> Für heute machen wir Feierabend und gehen noch eine Pizza essen.
>
> Morgen informieren wir uns darüber, wie wir die Geräte in unserem Smart Home bestmöglich schützen können.

3 IT-Sicherheit im Eigenheim – Smart Home

3.1 IT-Sicherheit am Beispiel der Familie Müller

3.1.1 Was Sie bisher wissen ...

In WBT 1 haben Sie die Grundlagen zum Thema IT-Sicherheit kennengelernt. Dabei haben Sie erfahren, warum es notwendig ist, sich mit IT-Sicherheitsmaßnahmen zu befassen.

Zudem haben Sie erfahren, was unter den Begriffen „Computersicherheit“, „Datensicherheit“, „Datensicherung“ und „Datenschutz“ verstanden wird.

Des Weiteren haben Sie gelernt, welche Bereiche es zu schützen gilt. Dabei wurden insbesondere die Bereiche „Privates Netzwerk“, „Smart Home“, „Einkaufen und Bezahlen im Internet“, „Cloud-Dienste“, „Wichtige Daten“ und „Soziale Netzwerke“ betrachtet.

In vorangegangenen WBT 2 haben Sie am Beispiel von Familie Müller erfahren, wie die IT-Sicherheit im Eigenheim zu unterstützen ist. Dabei hat sich Familie Müller zunächst mit ihrem privaten Netzwerk auseinandergesetzt.

Konkrete Maßnahmen zur Erhöhung der Sicherheit des privaten Netzwerks wurden am Beispiel des Routers und der PCs der Familie Müller durchgeführt.

3.1.2 Familie Müller

Familie Müller:

> Hallo, wir sind die Müllers.
>
> Wir sind Hans, Anette, Timo und Lisa.
>
> Wir wohnen in einem Einfamilienhaus und haben über die Zeit eine ganz schöne Menge an Geräten und Haushaltsgegenständen angesammelt und nutzen viele verschiedene Online-Dienste wie Web Shops, Cloud-Speicher und soziale Netzwerke.
>
> Auch hat sich bei uns inzwischen eine nicht zu unterschätzende Menge an wichtigen Dokumenten digital angesammelt. Dazu gehören beispielweise Ausweisdokumente, Urkunden oder auch Familienfotos.
>
> Leider haben wir jedoch ein wenig den Überblick verloren, wie es dabei um die IT-Sicherheit bestellt ist. Gerade erst haben wir von Bekannten erfahren, wie prekär es sein kann, wenn man Opfer eines IT-Sicherheitsvorfalls wird. Man hat auf einmal mit ungeahnten Problemen zu tun. Unsere Freunde erhielten beispielsweise Post von Inkasso-Büros, Anwälten und von Web Shops bzgl. nicht bezahlter Rechnungen, obwohl sie nichts bestellt hatten.
>
> Wir sind uns in einem sicher – wir müssen uns um unsere private IT-Sicherheit kümmern, damit uns so etwas nicht auch passiert.

3.1.3 Maßnahmen zur Steigerung der persönlichen IT-Sicherheit

Aus WBT 1 wissen wir, wo wir ansetzen sollten, um die persönliche IT-Sicherheit zu stärken.

Die Möglichkeiten und Maßnahmen zur Steigerung der persönlichen IT-Sicherheit können sehr umfangreich und vielfältig sein. Um den Überblick nicht zu verlieren, sollte deshalb geplant und strukturiert vorgegangen werden. So kann es hilfreich sein, einzelne Maßnahmen anhand von praktischen Anwendungen zu betrachten.

Aus diesem Grund zeigen wir anhand unserer Familie, wie wir im Privaten mit dem Thema IT-Sicherheit umgehen. Heute fokussieren wir uns auf die Sicherheit unseres Smart Home.

3.1.4 Die verschiedenen Anwendungsbereiche

In WBT 1 haben wir die sechs Anwendungsbereiche kennengelernt, die uns helfen können, unsere private IT-Sicherheit in den Griff zu kriegen.

Diese sechs Anwendungsbereiche schauen wir uns im Detail an und werden sie mit konkreten Maßnahmen sicherer gestalten.

Im vorangegangenen WBT 2 haben wir uns bereits um den ersten Anwendungsbereich „Das private Netzwerk“ gekümmert. In diesem WBT beschäftigen wir uns mit dem zweiten Anwendungsbereich: „Smart Home“.

3.2 Das Smart Home der Familie Müller

3.2.1 Der Anwendungsbereich: Das Smart Home

Kommen wir nun zum nächsten Anwendungsbereich: Unserem „Smart Home“.

Auch bei uns haben sich bereits einige „intelligente“ Geräte angesammelt. So setzen wir unter anderem eine Überwachungskamera, fernsteuerbare Lampen und Steckdosen ein. Derzeit überlegen wir zudem, uns einen intelligenten Kühlschrank und Staubsauger anzuschaffen.

Wie wir in WBT 1 gelernt haben, versteht man unter dem „Smart Home“ alle Geräte im eigenen Haushalt, die über den Router mit dem Internet bzw. Netzwerk verbunden sind, untereinander selbstständig kommunizieren, Daten austauschen und Aktionen ausführen.

Diese Geräte sind besonders anfällig für IT-Sicherheitsvorfälle, da bei diesen Geräten oftmals der Fokus auf der Funktionsvielfalt und dem Komfort liegt und nicht auf deren IT-Sicherheit.

3.2.2 Geräte in einem Smart Home

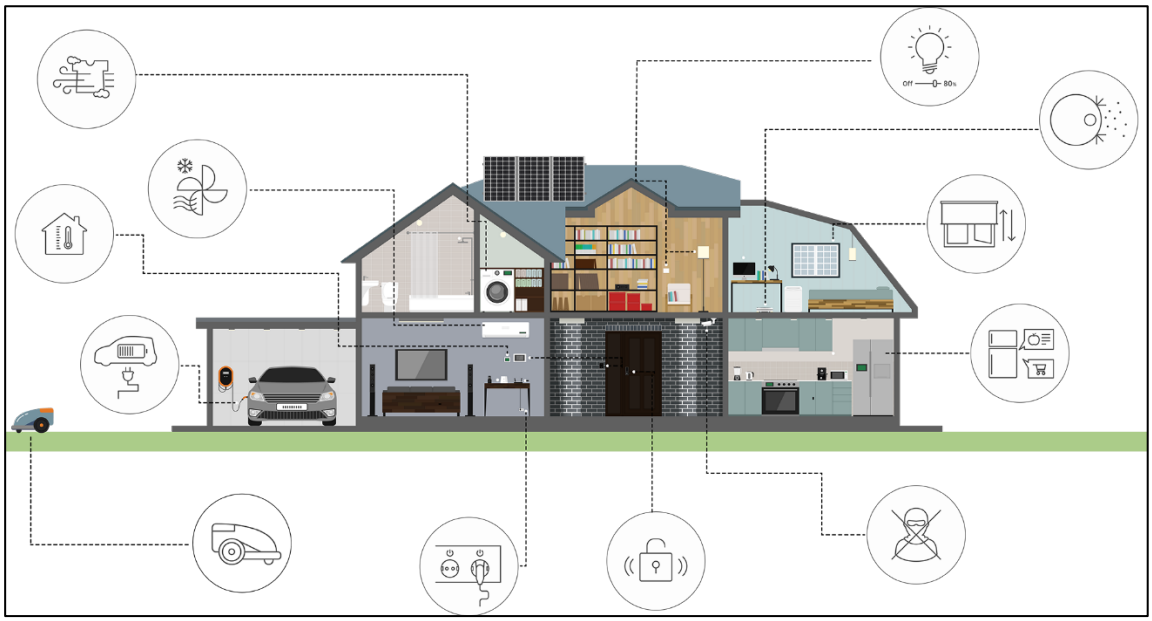


Abb. 28: Geräte in einem Smart Home

Smarte Waschmaschinen:

> Immer mehr Waschmaschinen verfügen inzwischen standardmäßig über eine Internet-Anbindung. Sie lassen sich per App oder Sprachassistenten steuern und helfen, die Wäsche komfortabler und effizienter zu waschen.
>
> Beispielsweise kann die Waschmaschine eine Push-Benachrichtigung an das Smartphone senden, sobald die Wäsche fertig ist. Auch kann man die Waschmaschine über Fernzugriff von unterwegs aus anschalten, damit die Wäsche fertig ist, sobald man Zuhause ist.

Weitere Funktionen wie Waschprogrammempfehlung, Fehlerdiagnosen oder automatische Waschmitteldosierung ermöglichen die Integration der Waschmaschine in ein smartes Zuhause.

Smarte Klimaanlagen:

Klimaanlagen haben grundsätzlich einen sehr hohen Energieverbrauch. Intelligente Klimaanalgen sollen möglichst effizient arbeiten und dadurch Energie und Kosten sparen. Außerdem lassen sie sich über eine entsprechende App oder einen Sprachassistenten sehr komfortabel bedienen. Funktionen wie die ortsabhängige Steuerung oder die automatische „Fenster-Offen-Erkennung“ sorgen dafür, dass die Klimaanlage nur dann läuft, wenn sie auch benötigt wird.

Außerdem wird die aktuelle Raumtemperatur sowie die Wettervorhersage berücksichtigt, um unnötigen Energieverbrauch zu vermeiden.

Smarte Heizkörperthermostate:

Auch Heizkörper benötigen, genauso wie Klimaanlagen, sehr viel Energie. Um diesen Energieverbrauch möglichst gering und effizient zu halten, eignen sich smarte Heizkörperthermostate. Mittlerweile gibt es viele verschiedene Anbieter dieser smarten Geräte. In ihrer Funktion sind sich jedoch alle Thermostate sehr ähnlich. Sie lassen sich über eine App auf dem Smartphone oder über Sprachassistenten steuern und haben zahlreiche Zusatzfunktionen, wie zum Beispiel eine Energie-Report-Erstellung oder die automatische Ortserkennung des Nutzers. So wird die Heizung beispielsweise erst dann automatisch eingeschaltet, wenn sich der Bewohner auf dem Nachhauseweg befindet.

Dies spart Energie, Kosten und ist sehr komfortabel, vor allem bei größeren Gebäuden.

Smarte Heizkörperthermostate:

Auch Heizkörper benötigen, genauso wie Klimaanlagen, sehr viel Energie. Um diesen Energieverbrauch möglichst gering und effizient zu halten, eignen sich smarte Heizkörperthermostate. Mittlerweile gibt es viele verschiedene Anbieter dieser smarten Geräte. In ihrer Funktion sind sich jedoch alle Thermostate sehr ähnlich. Sie lassen sich über eine App auf dem Smartphone oder über Sprachassistenten steuern und haben zahlreiche Zusatzfunktionen, wie zum Beispiel eine Energie-Report-Erstellung oder die automatische Ortserkennung des Nutzers. So wird die Heizung beispielsweise erst dann automatisch eingeschaltet, wenn sich der Bewohner auf dem Nachhauseweg befindet.

Dies spart Energie, Kosten und ist sehr komfortabel, vor allem bei größeren Gebäuden.

Das Auto:

Auch Autos lassen sich mittlerweile digital in das Eigenheim integrieren. So kann man sich beispielsweise bei E-Autos den aktuellen Ladestand via App anzeigen lassen oder wird benachrichtigt, wenn die Ladung zur Neige geht oder das Auto vollständig geladen ist. Auch Ladestationen kann man über Apps finden, wenn man unterwegs ist. Sprachassistenten sind inzwischen fester Bestandteil vieler Autos. So kann man beispielsweise das Garagentor öffnen, sich Verkehrsnachrichten mitteilen lassen oder Essen bestellen, wenn man sich auf dem Heimweg befindet.

Ist kein Sprachassistent in dem Auto integriert, gibt es auch Möglichkeiten, diesen einfach nachzurüsten oder das Smartphone mit dem Auto zu koppeln. Somit ist es möglich, beispielsweise Amazons Sprachassistent "Alexa" auch unterwegs zu nutzen.

Smarter Mähroboter:

Mähroboter erleichtern vielen Menschen die Arbeit, indem sie dafür sorgen, dass der Rasen gepflegt bleibt. Dafür arbeiten sie selbstständig und völlig automatisch. Einmal richtig eingestellt, bedarf es keiner Kontrolle oder manuellen Eingabe mehr. Der Rasenroboter startet zu festgelegten Zeiten und findet bei niedrigem Akkustand alleine in die Ladestation zurück. Sollte man doch einmal das Mähen unterbrechen wollen, lässt sich dies einfach in der App oder per Sprachassistent erledigen.

Dabei gibt es unterschiedliche Geräte, die sich hauptsächlich in der Eignung für bestimmte Flächengrößen des Rasens unterscheiden.

Smarte Steckdosen:

Ein wesentlicher Bestandteil eines Smart Homes sind smarte Steckdosen. Diese kleinen Geräte fungieren als Adapter zwischen Geräten und der herkömmlichen Steckdose und können somit jedes Gerät „smart“ machen. Zwar beschränken sich die Funktionen meist auf das einfache An- und Ausschalten der Geräte, jedoch lassen sich so auch Geräte ohne eigenen Internet-Zugang steuern. So ist es beispielsweise möglich, die Kaffeemaschine per App anzuschalten oder per Sprachbefehl eine Lampe auszuschalten.

Oft bieten diese Steckdosen Zusatzfunktionen, wie eine Messung des Energieverbrauchs oder eine Timer-Funktion.

Aufgrund ihrer einfachen Bedienbarkeit und leichten Installation stellen sie oft eine kostengünstige und einfache Alternative gegenüber teureren smarten Geräten dar.

Smarte Türsteuerung:

Eine intelligente Türsteuerung ermöglicht es, mit dem Smartphone die Haustür aufzuschließen oder die Haustür über eine Kamera zu überwachen. Trifft unerwarteter Besuch ein, ist es auch möglich, die Tür von unterwegs aus zu öffnen.

Smarte Sprechanlagen und Türklingeln übertragen ein Live-Video auf das Handy oder auf Amazon Echo und versuchen so, das eigene Zuhause sicherer zu machen. Auch Fingerabdruck-Sensoren als Ersatz für einen Schlüssel werden dabei oft eingesetzt.

Smarte Sicherheitssysteme:

Smarte Sicherheitssysteme können aus verschiedenen Bestandteilen bestehen. Am häufigsten sind es intelligente Videokameras, Bewegungs- und Fenstersensoren, Rauchwarnmelder und Alarmanlagen, die das eigene Zuhause sicherer machen sollen. Dabei gibt es oft ganze Sicherheitspakete von einem einzigen Anbieter, die sich dann über eine App zentral steuern lassen und bei Auffälligkeiten sofort eine Benachrichtigung senden. Meistens lässt sich der Status des Sicherheitssystems auch über den Sprachassistenten abfragen.

Smarte Kühlschränke:

Smarte Kühlschränke sind mit WLAN, Kameras und oft sogar Tablets als Bedienelement ausgestattet. Beispielsweise dienen die Innenraumkameras dazu, ein Bild beim Schließen der Kühlschranktür aufzunehmen, damit man im Supermarkt via App den aktuellen Bestand seiner Lebensmittel sehen kann. Einige Kühlschränke können auf Grundlage der verfügbaren Lebensmittel auch Rezepte vorschlagen oder Produkte auf die Einkaufsliste setzen, sollte nicht mehr genügend vorrätig sein.

Weitere Funktionen wie Ferndiagnose, Temperaturkontrolle oder eine Verbindung mit dem Sprachassistenten sind mittlerweile auch im Standardfunktionsumfang vieler Kühlschränke enthalten.

Smarte Rollladensteuerung:

Smarte Rollläden lassen sich bequem vom Smartphone oder per Sprachassistenten steuern. So kann man zu flexiblen Zeiten jederzeit von unterwegs aus die Rollläden fernsteuern oder feste Uhrzeiten festlegen, um jeden Abend zur selben Zeit die Rollläden automatisch herunterzulassen.

Mittlerweile sind die Kosten für Nachrüstlösungen relativ gering, sofern man bereits elektrische Rollläden hat. Somit lassen sich smarte Rollläden sehr einfach in das Smart Home integrieren. Dies bietet Schutz vor Einbrechern, Unwettern und spart Energie.

Smarte Staubsauger:

Smarte Staubsauger halten das Zuhause sauber. Mittels eingebauter Sensoren und einem Lasernavigationssystem erstellen Saugroboter eine virtuelle Karte der Räume und fahren diese anschließend ab, um den Boden zu reinigen. Dabei erreichen die Geräte auch schwierige Stellen der Wohnung und weichen Hindernissen automatisch aus. Das erleichtert den Alltag für viele Menschen.

Über eine App lässt sich genau nachvollziehen, welche Stellen der Roboter schon abgearbeitet hat. Viele der smarten Geräten lassen sich auch über einen Sprachassistenten steuern. Notwendig ist dies jedoch nicht, da der Staubsauger zur Ladestation fährt, wenn der Akkustand zu niedrig ist. Ist der Akku geladen, fährt der Staubsauger selbstständig wieder los.

Smarte Lampen:

Smarte Beleuchtung findet man immer häufiger in Häusern und Wohnungen. Diese Lampen bieten einfache, vielseitige und kostengünstige Möglichkeiten, um die Atmosphäre in der eigenen Wohnung möglichst angenehm zu gestalten. Dabei lassen sich die Lichter einfach per App oder auf Befehl von einem Sprachassistenten steuern.

Neben dem einfachen An- und Ausschalten gibt es auch die Möglichkeit, ganze Szenerien, bestehend aus mehreren Lichtern und unterschiedlichen Farben, festzulegen und abzurufen. Auch das automatische Steuern von Lampen, beispielsweise mittels Bewegungssensoren oder zu einer bestimmten Uhrzeit, ist möglich.

3.2.3 Theorie: Das Smart Home

Bei einem „Smart Home“ wird das Internet of Things dafür verwendet, intelligente Wohnhäuser und Wohnungen zu schaffen. Dies geschieht, indem das Zuhause durch Informations-, Sensor- und Aktortechnik vielseitig vernetzt wird.

Beispielsweise werden dafür automatisch gesteuerte Heizungen, Lüftungen, Türen, Fenster oder Lampen in das Gebäude integriert. Dies nennt man Gebäudeautomation. Außerdem kann man smarte Gegenstände, wie zum Beispiel intelligente Kühlschränke, Staubsauger, Kaffee- und Waschmaschinen oder Rasenmäher einsetzen. Dies bezeichnet man als (Haushalts-) Geräteautomation.

Dabei werden in der Regel alle Gegenstände im Haus über ein zentrales Gerät gesteuert. In den meisten Fällen geschieht dies über ein Smartphone, ein Tablet oder über Sprachassistenten wie zum Beispiel „Amazon Echo“ oder „Apple HomePod“.

Ein Smart Assistent bzw. Sprachassistent ist ein Software-Produkt, welches versucht, Kommunikation in möglichst natürlicher, menschlicher Sprache zu führen. Dabei kann es Informationen übermitteln, Befehle ausüben oder einfache Dialoge führen.

Meist ist dieses Software-Produkt in Smartphones und Tablets integriert oder in sogenannten Smart Speakern vorzufinden. Das sind Lautsprecher, welche über das Internet gesteuert werden können und oft zur Steuerung eines Smart Homes verwendet werden.

In den letzten Jahren haben sich Amazons Echo mit dem Sprachassistenten „Alexa“ (Bild unten), Googles „Home“ und Apples „HomePod“ am Markt etabliert.

Lisa:

Das Smart Home wird immer beliebter! In Deutschland gibt es bereits mehr als 10 Millionen Haushalte, die mit „smart things“ ausgestattet sind.

3.2.4 Das Smart Home als Einfallstor für Angreifer

Timo:

Die Geräte in einem Smart Home sollen uns dabei unterstützen, den Alltag einfacher und komfortabler zu gestalten. Aber all diese Vorteile und Komfortfunktionen können auch Nachteile haben.

Werden die Geräte und Funktionen nicht sicher installiert und konfiguriert, können Angreifer über die Smart Home Geräte in das private Netzwerk eindringen. Ist einem Angreifer der Weg in das privaten Netzwerk gelungen, so kann er bspw. das Haus durch die Überwachungskameras selber überwachen oder auch erheblichen physischen Schaden anrichten.

Lisa:

Auch wir besitzen einige intelligente Geräte und damit ein Smart Home. Davon sollten einige bereits ziemlich sicher sein. Andere wiederum fokussieren eher den Nutzerkomfort, und sind ein mögliches Einfallstor für Angriffe in unser privates Netzwerk. Deswegen sollten grundsätzlich alle Geräte im Smart Home via Gastzugang mit unserem privaten Netzwerk verbunden sein.

Einige unserer Smart Home Geräte und deren Sicherheitseinstellungen gucken wir uns nachfolgend gemeinsam an.

3.3 Überwachungskameras im Smart Home

3.3.1 Allgemeine Maßnahmen im Smart Home

Anette:

Bevor wir zu den konkreten Maßnahmen an den einzelnen Geräten im Smart Home kommen, schauen wir uns zunächst die allgemeinen Maßnahmen an.

Allgemeine Maßnahmen vor dem Kauf:

- Produkte von Markenherstellern statt günstige No-Name-Ware wählen
- Werden zukünftig (Sicherheits-) Updates durch den Hersteller bereitgestellt?
- Bewusstsein über Sensoren und aufzuzeichnende Daten der Geräte stärken

Allgemeine Maßnahmen bei unseren Geräten im Smart Home:

- Updates einspielen und aktivieren
- Werkseitige Passwörter in individuelle und sichere Passwörter ändern
- Ist der Zugriff auf die Geräte von außerhalb des Eigenheims notwendig? Wenn ja, VPN-Zugang nutzen.
- Geräte-/Datenschutzeinstellungen überprüfen
- Universal Plug-and-Play (UPnP) im Router ggf. deaktivieren
- (Fortgeschritten): Separates Netzwerk für alle IoT-Geräte einrichten

3.3.2 Überwachungskamera: Umsetzung konkreter Maßnahmen

Nachdem wir uns die allgemeinen Maßnahmen angeschaut haben, kommen wir nun zur Umsetzung konkreter Maßnahmen bei unseren Überwachungskameras.

Überwachungskameras können meist entweder über eine eigene Anwendung oder wie im Falle der Fritzbox über eine Administrationsoberfläche im Web-Browser angesteuert werden. Bei uns steht eine Oberfläche im Web-Browser bereit, um die Einstellungen der Überwachungskamera einsehen und anpassen zu können.

Folgende konkrete Maßnahmen sollten wir bei unseren Überwachungskameras durchführen:

- Auf Updates prüfen und ggf. durchführen
- Sichere und individuelle Passwörter wählen
- Fernzugriff einschränken
- Datenschutzeinstellungen anpassen

3.3.3 Einstellungen an der Überwachungskamera

Unsere Überwachungskamera ist von der Marke AXIS. Ich kann diese im Browser über eine eigene Administrationsoberfläche ansteuern. Dort kann ich die verschiedenen Funktionen anpassen und Einstellungen vornehmen.

Im Anschluss zeige ich, wie Firmware-Upgrades installiert und ein individuelles Passwort gesetzt werden kann.

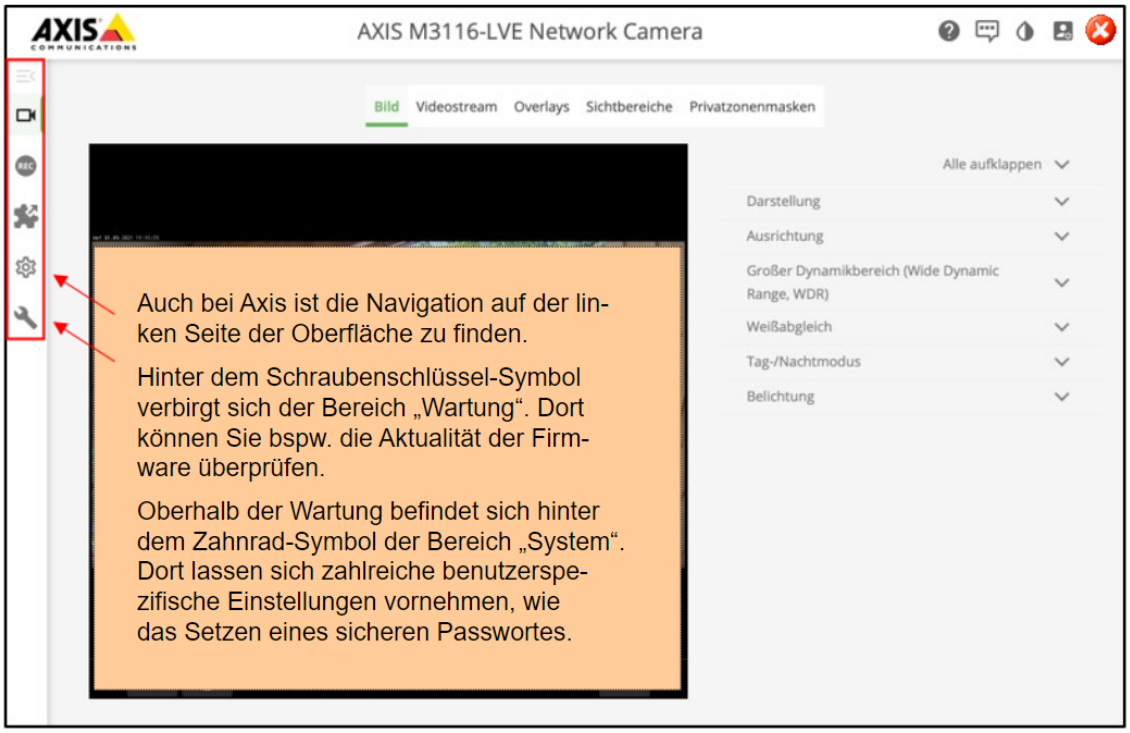


Abb. 29: Einstellungen an der Überwachungskamera

3.3.4 Firmware-Upgrade an der Überwachungskamera

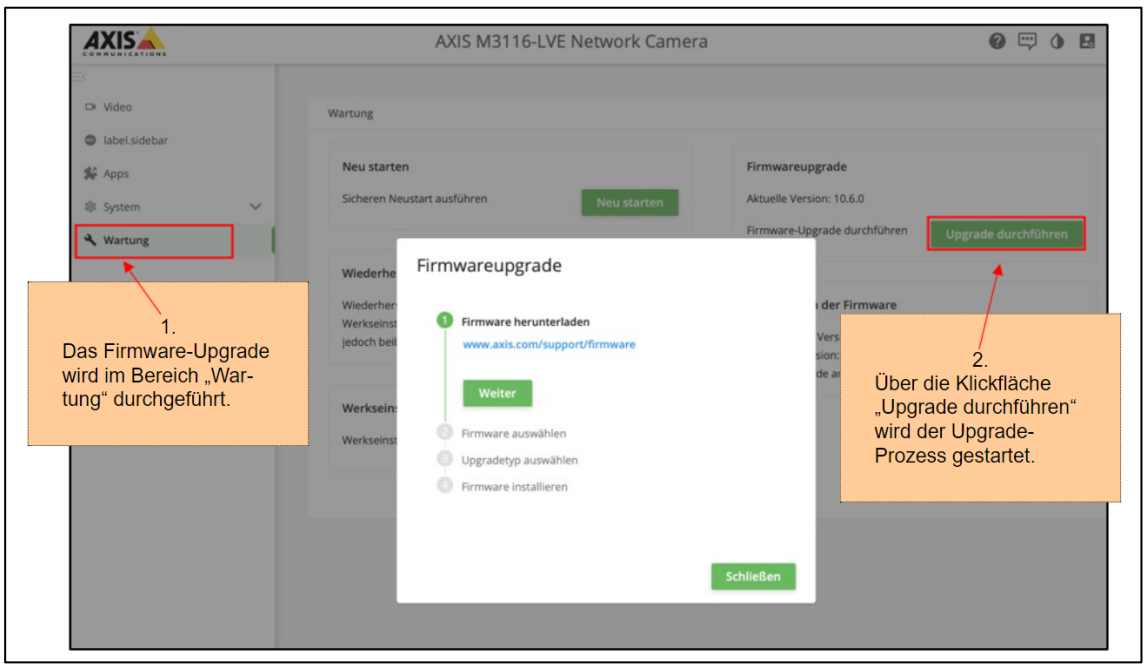


Abb. 30: Firmware-Upgrade an der Überwachungskamera

3.3.5 Sicheres Passwort für die Überwachungskamera

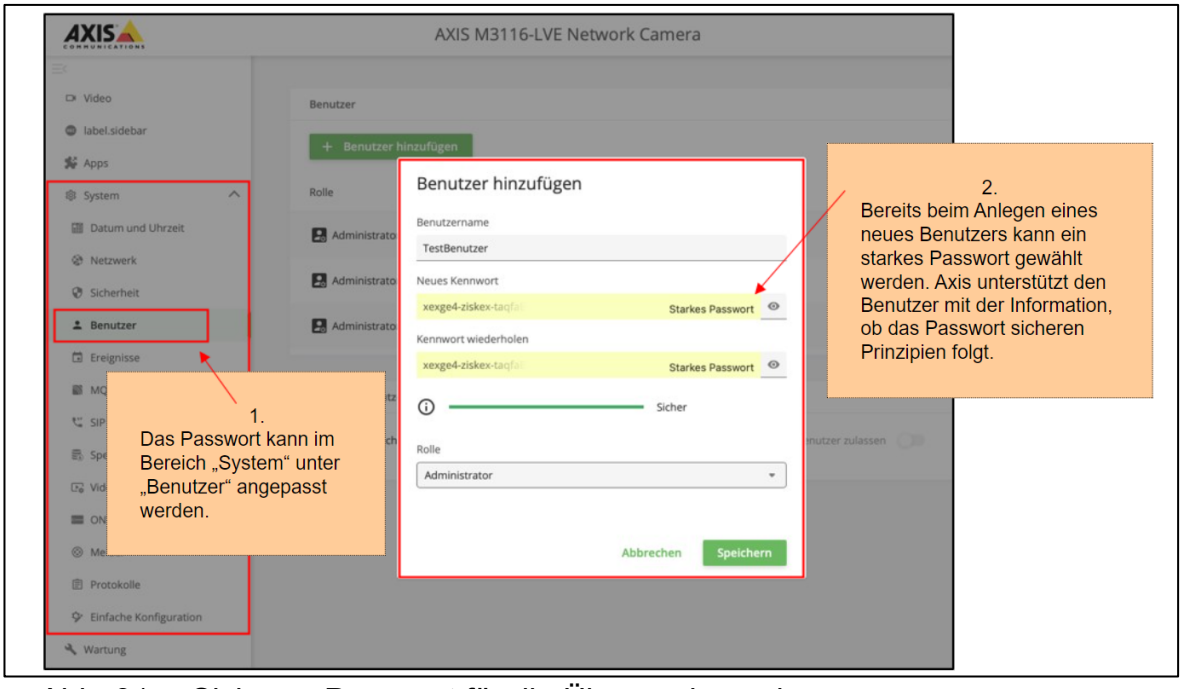


Abb. 31: Sicheres Passwort für die Überwachungskamera

3.3.6 Fernzugriff an der Überwachungskamera deaktivieren

Hans:

Nun schaue ich, ob ein Fernzugriff auf die Kamera eingerichtet ist und deaktiviere diesen. Denn ich möchte nur aus unserem privaten Netzwerk auf die Überwachungskamera zugreifen können.

Somit ist ein (unberechtigter) Zugriff auf unsere Überwachungskameras außerhalb unseres privaten Netzwerks nicht möglich.

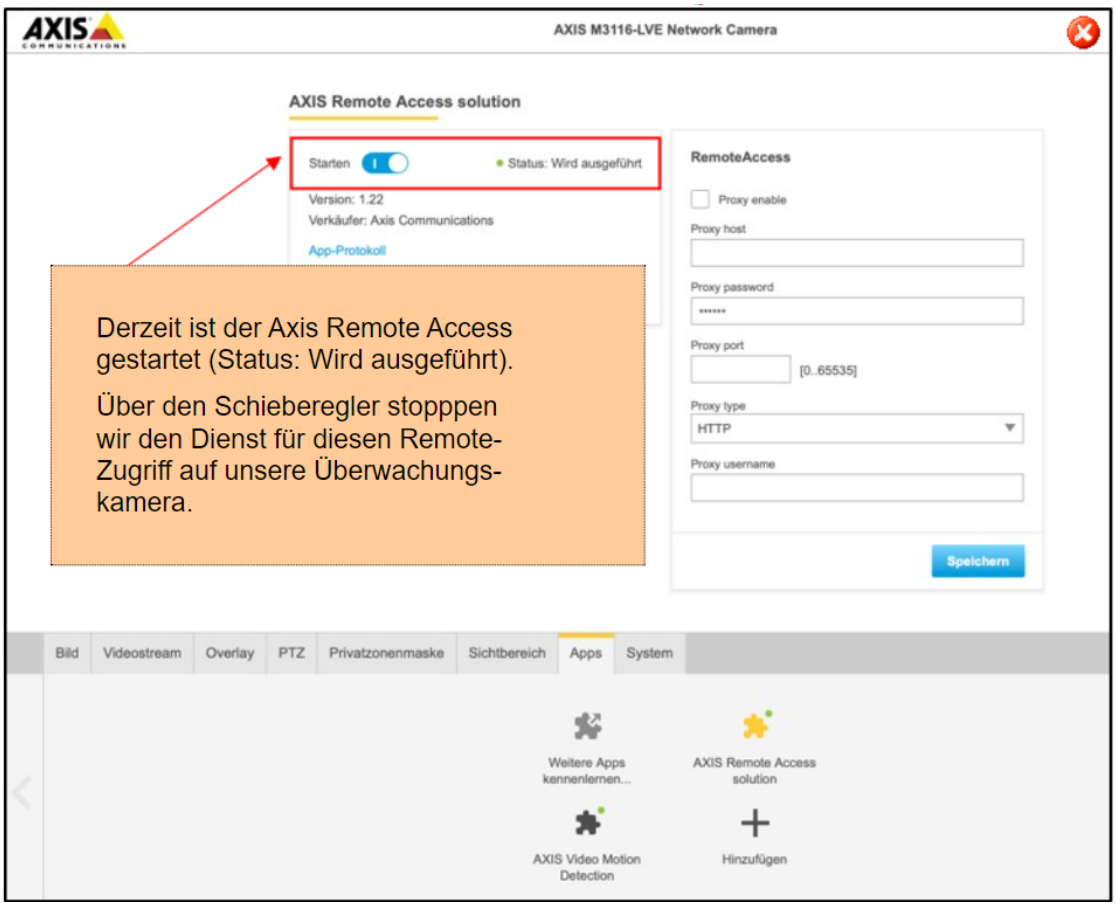


Abb. 32: Fernzugriff an der Überwachungskamera deaktivieren

3.3.7 Datenschutz der Überwachungskamera

Hans:

Zuletzt überprüfe ich die werkseitigen Datenschutz-Einstellungen unserer Überwachungskamera und prüfe, welche Daten gesammelt und übertragen werden (Telemetrie-Einstellungen).

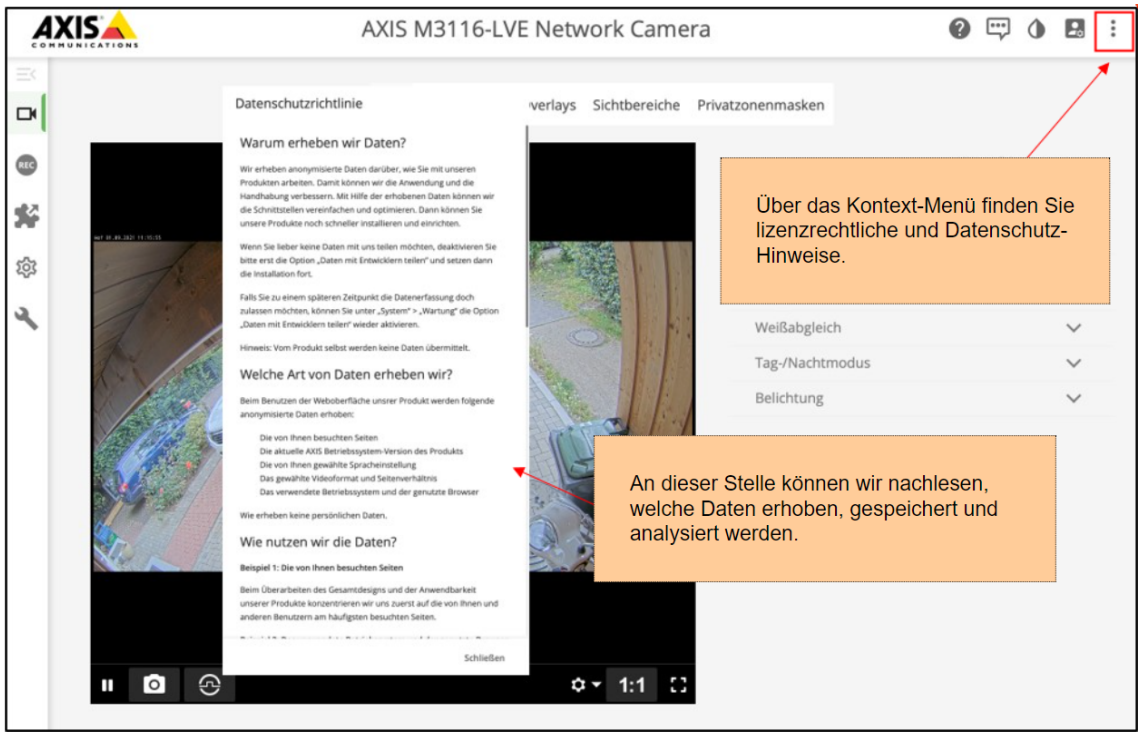


Abb. 33: Datenschutz-Einstellungen der Überwachungskamera

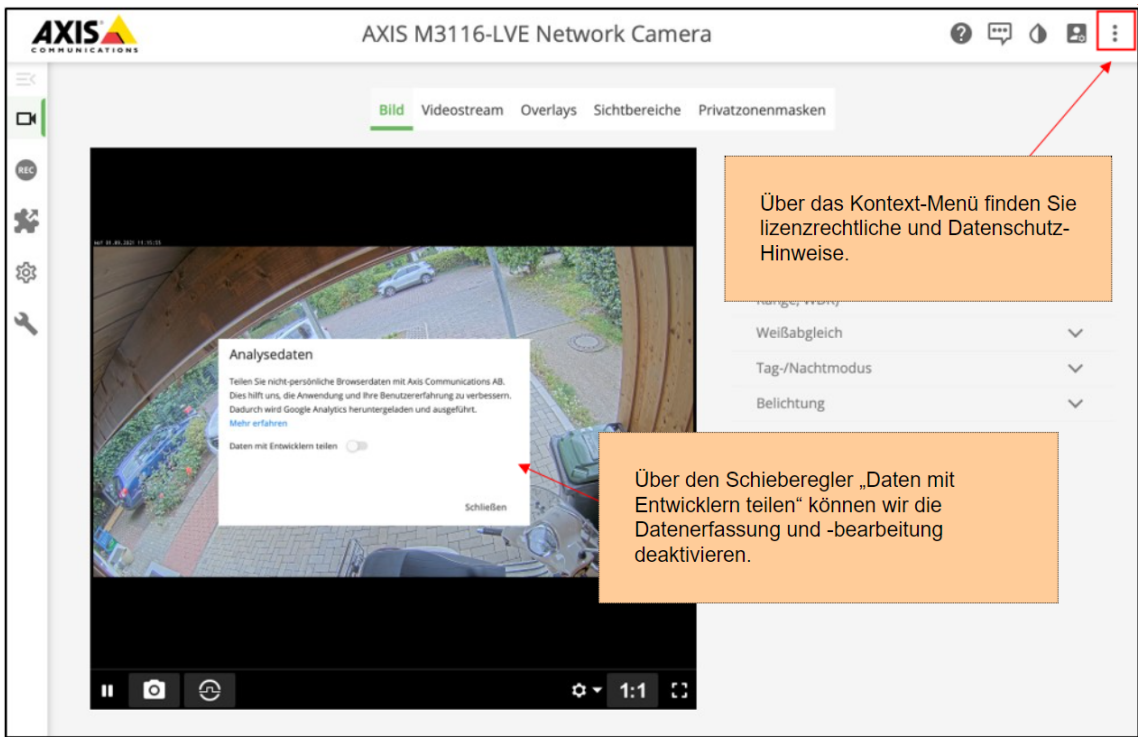


Abb. 34: Telemetrie-Einstellungen der Überwachungskamera

3.3.8 Umgesetzte Maßnahmen an den Überwachungskameras

Hans:

Ich habe nun einige relevante Sicherheitsmaßnahmen an unseren Überwachungskameras durchgeführt.

- ✓ Auf Updates prüfen und ggf. durchführen
- ✓ Sicheres und individuelles Passwort wählen
- ✓ Fernzugriff einschränken
- ✓ Datenschutz anpassen

Als nächstes schauen sich Anette und Lisa unsere smarten Lampen und Steckdosen an.

3.4 Lampen und Rollos im Smart Home

3.4.1 Das Smart Home von Familie Müller

Hans:

Durch die vorgenommenen Einstellungen an der Überwachungskamera ist unser Smart Home bereits viel sicherer geworden.

Anette und Lisa, ihr schaut euch jetzt unsere Lampen, Rollos und Steckdosen an, richtig?

Anette:

Danke Hans! Genau! Wir möchten heute die Sicherheitseinstellungen für unsere smarten Lampen, Rollos und Steckdosen überprüfen.

Lisa, Du startest mal mit den Lampen und Rollos, ok?

3.4.2 Smarte Lampen und smarte Rollos

Lisa:

Na klaro Mama! Unsere smarten Lampen und Rollos habe ich von meinem letzten Einkauf von Ikea mitgebracht. Ikea hat mittlerweile einige smarten Geräte im Angebot.

Die Geräte lassen sich dabei über eine eigene Anwendung von Ikea auf dem Smartphone ansteuern. Wie das geht, zeige ich euch auf dem Weg zum Bus.

Ach stimmt, das habe ich ganz vergessen. Auf die Geräte kann ich gar nicht von unterwegs zugreifen, sondern nur, wenn ich in unserem privaten Netzwerk bin.

Das ist super, denn somit ist der unberechtigte Zugriff auf unsere Lampen und Rollos deutlich erschwert.

3.4.3 Smarte Lampen und smarte Rollos: Umsetzung konkreter Maßnahmen

Lisa:

Okay, jetzt bin ich wieder zuhause.

Folgende konkrete Maßnahmen sollten wir an unseren smarten Lampen und Rollos umsetzen.

- Sicheres und individuelles Passwort wählen
- Prüfen und Einspielen von Firmware-Updates
- Geräte-/Datenschutzeinstellungen überprüfen
- Werkseinstellungen anpassen

3.4.4 Sicheres und individuelles Passwort wählen

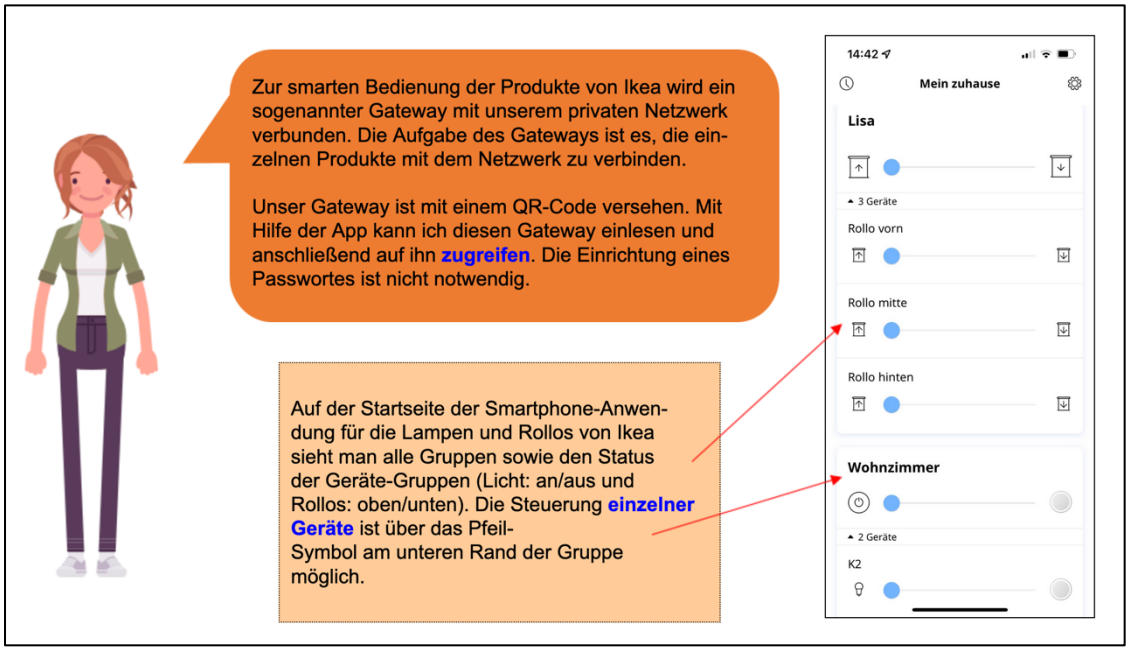


Abb. 35: Sicheres und individuelles Passwort wählen

3.4.5 Prüfen und Einspielen von Firmware-Updates

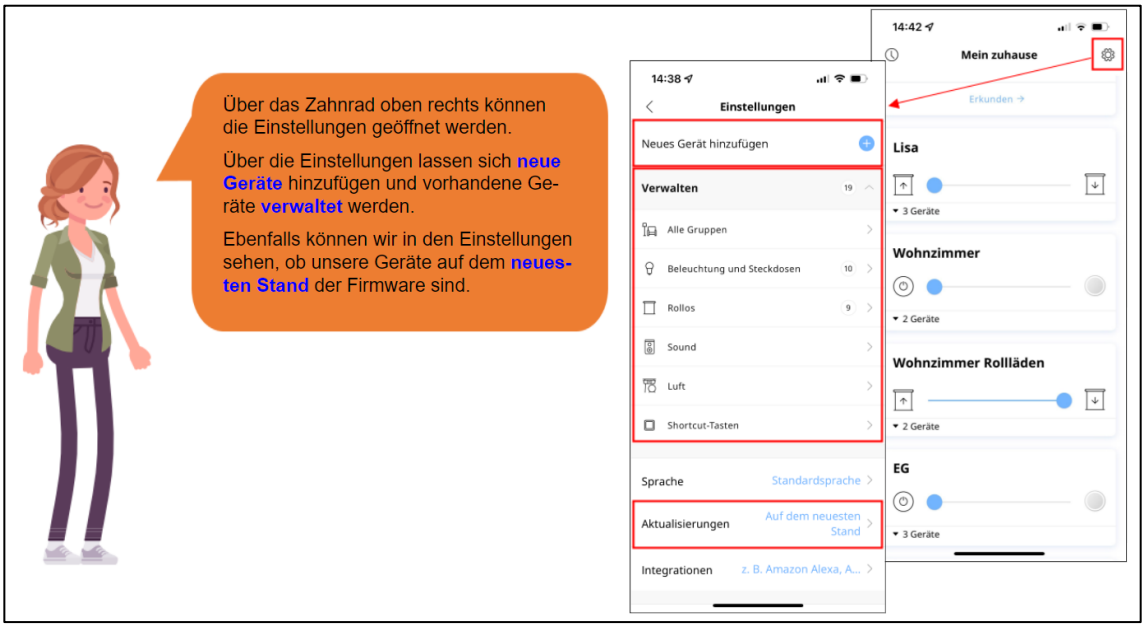


Abb. 36: Prüfen und Einspielen von Firmware-Updates

3.4.6 Geräte-/Datenschutzeinstellungen überprüfen

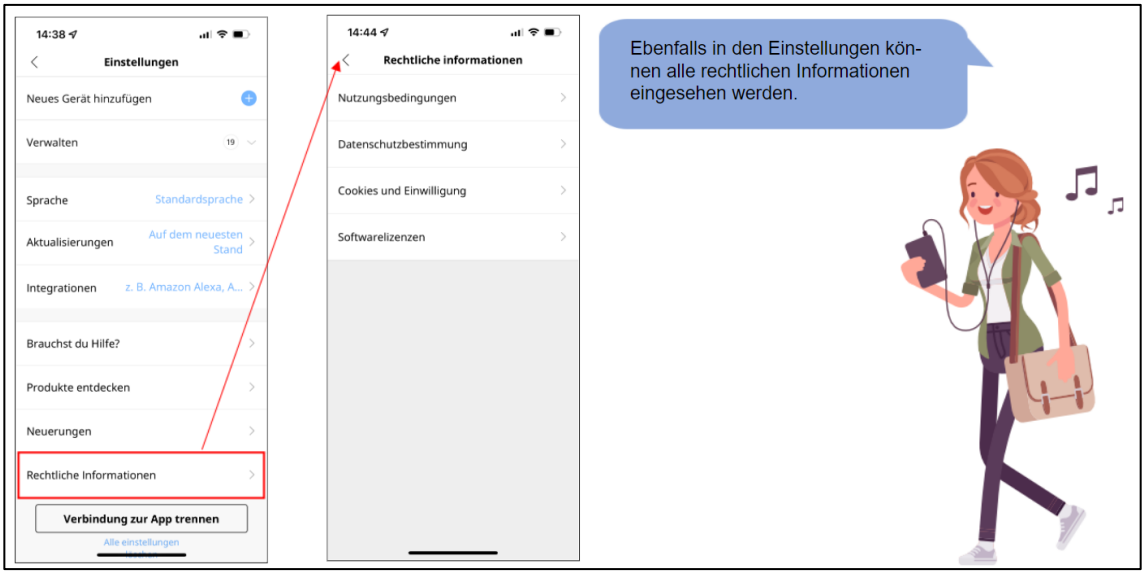


Abb. 37: Geräte-/Datenschutzeinstellungen überprüfen

3.4.7 Timer-Einstellungen anpassen

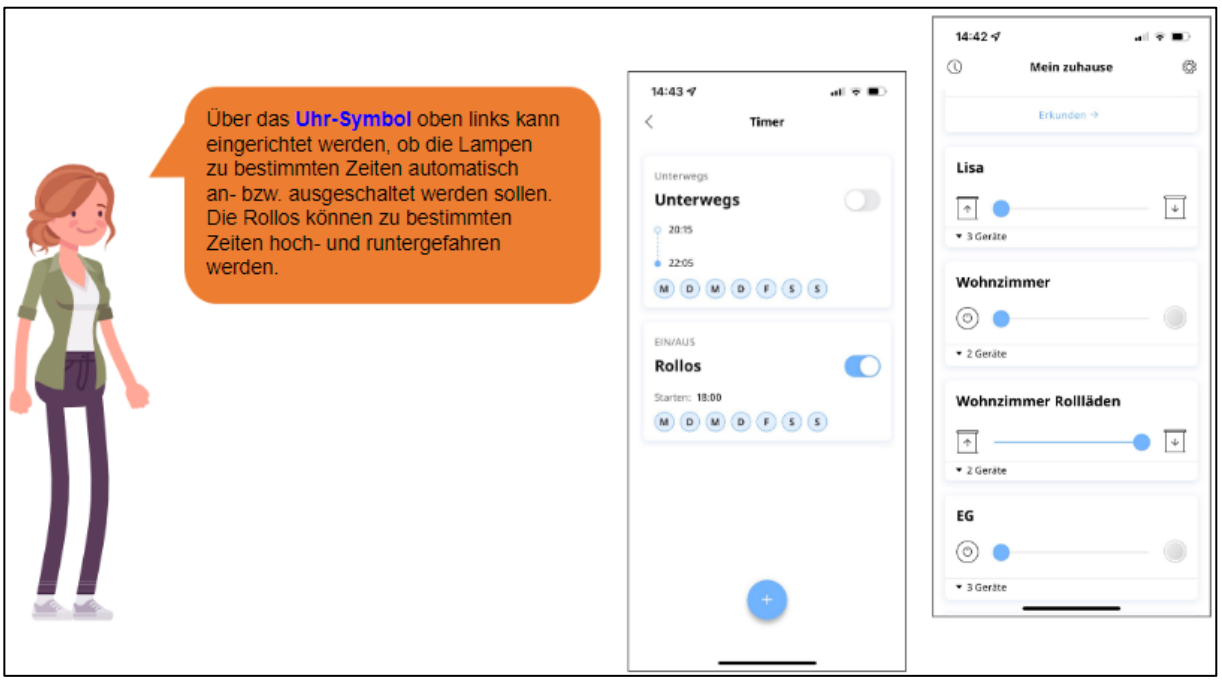


Abb. 38: Timer-Einstellungen anpassen

3.4.8 Umgesetzte Maßnahmen an den Lampen und Rollos

Lisa:

Wir haben nun einige relevante Sicherheitsmaßnahmen an unseren smarten Lampen und Rollos in unserem Smart Home durchgeführt.

- ✓ Sicheres und individuelles Passwort wählen
- ✓ Prüfen und Einspielen von Firmware-Updates
- ✓ Geräte-/Datenschutzeinstellungen überprüfen
- ✓ Werkseinstellungen anpassen

3.5 Steckdosen im Smart Home

Hans:

Danke Lisa, die Lampen und Rollos sind jetzt wirklich smart in unserem Zuhause integriert.

Anette, machst Du weiter mit den Steckdosen?

Anette:

Genau! Ich prüfe nun die Sicherheitseinstellungen für unsere smarten Steckdosen.

3.5.1 Smarte Steckdosen: Umsetzung konkreter Maßnahmen

Anette:

Folgende konkrete Maßnahmen sollten wir an unseren smarten Steckdosen umsetzen. Da ich die smarten Steckdosen gekauft und eingerichtet habe, kenne ich mich mit der Administration noch recht gut aus.

Das Vorgehen zur Absicherung von intelligenten Geräte im Smart Home ist für viele Geräte oftmals das Gleiche oder zumindest sehr ähnlich.

- Prüfen und Einspielen von Firmware-Updates
- Geräte-/Datenschutzeinstellungen überprüfen
- Werkseinstellungen anpassen
- Sicheres und individuelles Passwort wählen
- Fernzugriffsoptionen anpassen

3.5.2 Zugriff auf die smarten Steckdosen via Fritzbox

Anette:

Da unsere Steckdosen keine eigene Benutzeroberfläche anbieten, nutzen wir die integrierte Smart-Home-Oberfläche der Fritzbox, um unsere intelligenten Geräte zu verwalten.

Wir erinnern uns: Die Einstellungen und Funktionen in der Administrationsoberfläche der Fritzbox werden über das Menü auf der linken Seite angesteuert. Zur Verwaltung unseres Smart Homes wechseln wir in die Kategorie „Smart Home“.

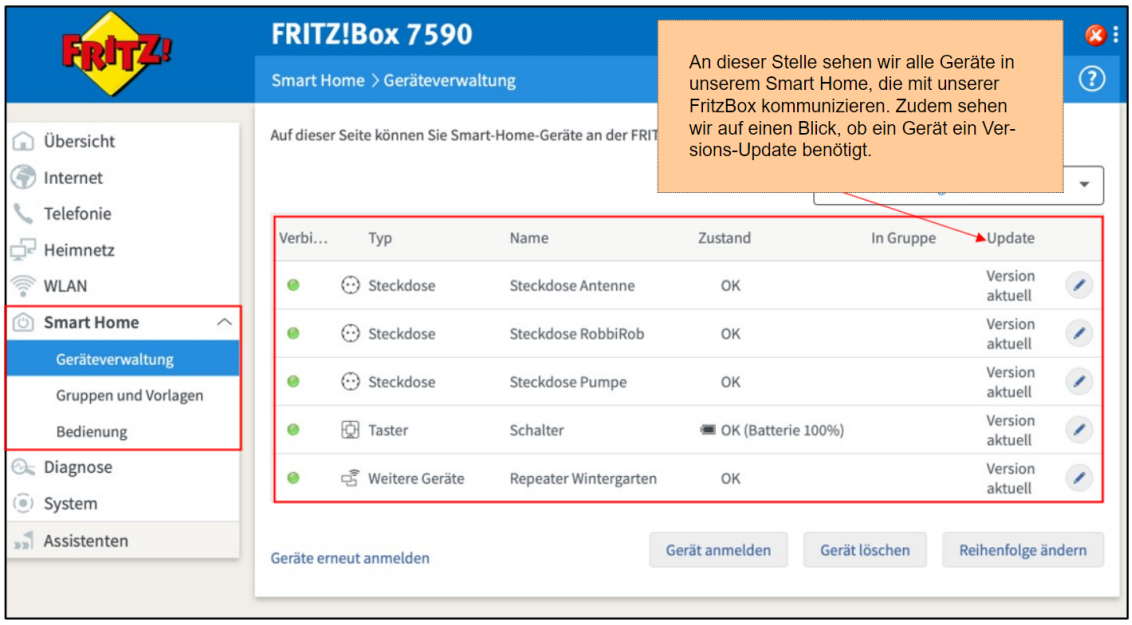


Abb. 39: Smart Home in der Fritzbox

3.5.3 Einstellungen zur Bedienung der Gruppen und Geräte

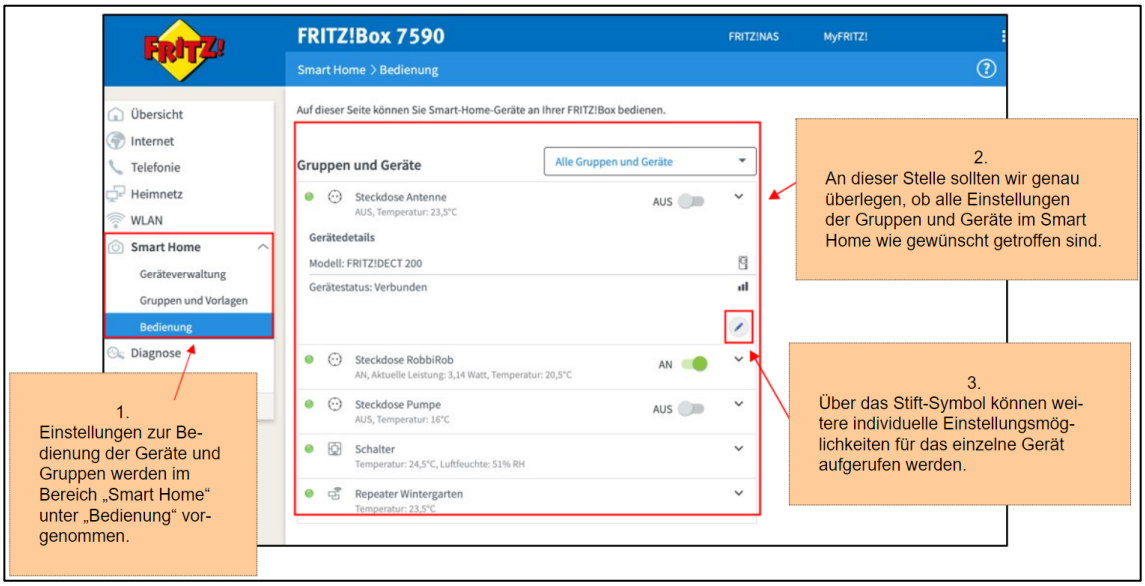


Abb. 40: Einstellungen zur Bedienung der Gruppen und Geräte

3.5.4 Einstellungen zur Bedienung einer smarten Steckdose

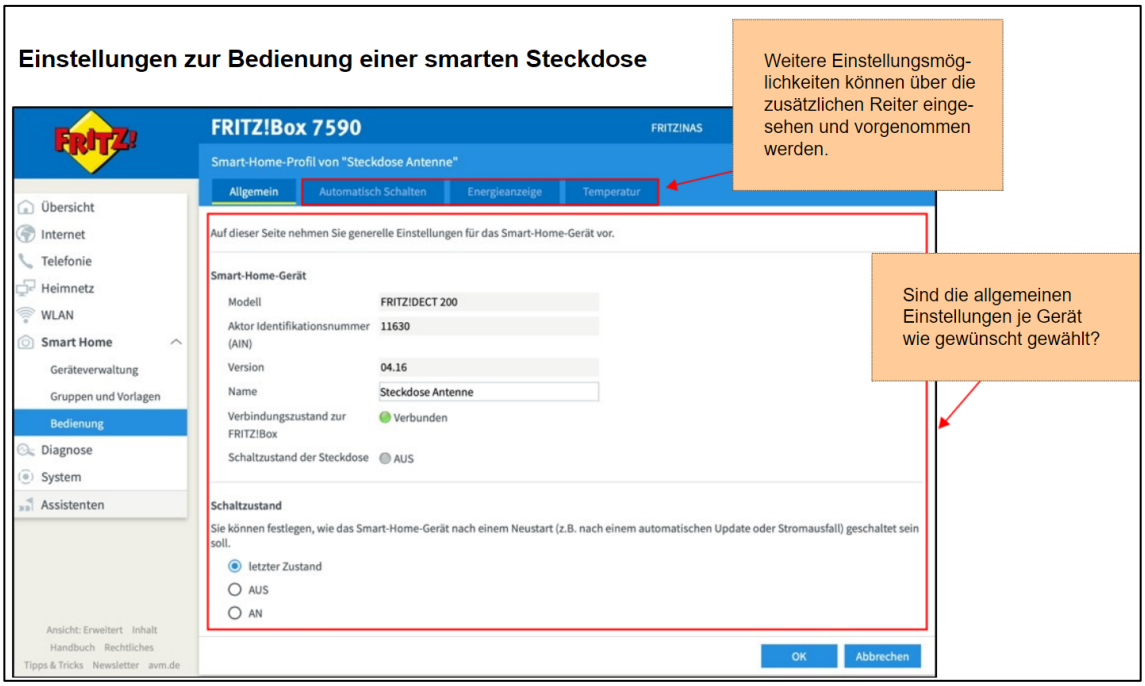


Abb. 41: Einstellungen zur Bedienung einer smarten Steckdose

3.5.5 Automatische Schaltung einer smarten Steckdose

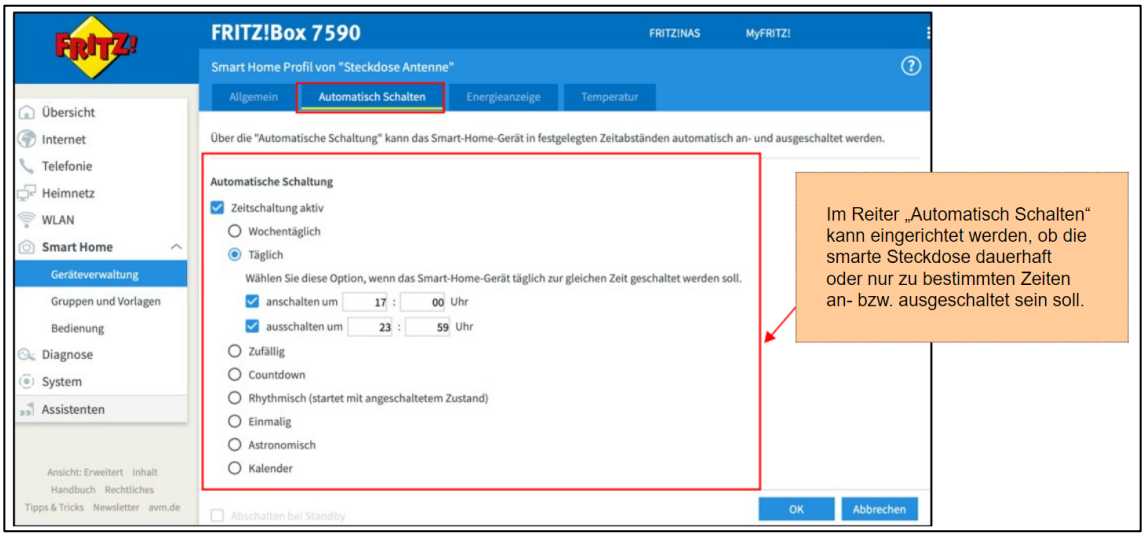


Abb. 42: Automatische Schaltung einer smarten Steckdose

3.5.6 Umgesetzte Maßnahmen an den Steckdosen

Anette:

Wir haben nun einige relevante Sicherheitsmaßnahmen an unseren smarten Steckdosen und damit exemplarisch für andere Geräte in unserem Smart Home durchgeführt.

- ✓ Prüfen und Einspielen von Firmware-Updates
- ✓ Geräte-/Datenschutzeinstellungen überprüfen
- ✓ Werkseinstellungen anpassen

Timo:

Da unsere Steckdosen über die Fritzbox administriert werden, ist deren Zugriff über das Fritzbox-Passwort geschützt. Der Fernzugriff ist ebenfalls nur über die Fritzbox möglich.

Diese Maßnahmen habe ich an der Fritzbox durchgeführt.

- ✓ Sichere und individuelle Passworte wählen
- ✓ Fernzugriffsoptionen anpassen

3.6 Abendessen

Familie Müller:

> Okay super, unsere Geräte im Smart Home sind nun um einiges sicherer und der Zugriff durch Unbefugte ist um einiges unwahrscheinlicher geworden.
>
> Bei der Beschaffung von smarten Geräten werden wir uns von nun an vorab informieren und die Sicherheit der Geräte in den Fokus stellen.
>
> Für heute machen wir Schluss und werfen den Grill an.
>
> Morgen informieren wir uns über unser Verhalten beim Einkaufen und Bezahlen im Internet.

4 IT-Sicherheit im Eigenheim – Einkaufen im Internet

4.1 IT-Sicherheit am Beispiel der Familie Müller

4.1.1 Was Sie bisher wissen ...

In WBT 1 haben Sie die Grundlagen zum Thema IT-Sicherheit kennengelernt. Dabei haben Sie erfahren, warum es notwendig ist, sich mit IT-Sicherheitsmaßnahmen zu befassen.

Zudem haben Sie erfahren, was unter den Begriffen „Computersicherheit“, „Datensicherheit“, „Datensicherung“ und „Datenschutz“ verstanden wird.

Des Weiteren haben Sie gelernt, welche Bereiche es zu schützen gilt. Dabei wurden insbesondere die Bereiche „Privates Netzwerk“, „Smart Home“, „Einkaufen und Bezahlen im Internet“, „Cloud-Dienste“, „Wichtige Daten“ und „Soziale Netzwerke“ betrachtet.

In den vorangegangenen WBT 2 und 3 haben Sie am Beispiel von Familie Müller erfahren, wie die IT-Sicherheit im Eigenheim zu unterstützen ist. Dabei hat sich Familie Müller zunächst mit den beiden Anwendungsgebieten „Privates Netzwerk“ und „Smart Home“ auseinandergesetzt.

4.1.2 Familie Müller

Familie Müller:

> Hallo, wir sind die Müllers.
>
> Wir sind Hans, Anette, Timo und Lisa.
>
> Wir wohnen in einem Einfamilienhaus und haben über die Zeit eine ganz schöne Menge an Geräten und Haushaltsgegenständen angesammelt und nutzen viele verschiedene Online-Dienste wie Web Shops, Cloud-Speicher und soziale Netzwerke.
>
> Auch hat sich bei uns inzwischen eine nicht zu unterschätzende Menge an wichtigen Dokumenten digital angesammelt. Dazu gehören beispielweise Ausweisdokumente, Urkunden oder auch Familienfotos.
>
> Leider haben wir jedoch ein wenig den Überblick verloren, wie es dabei um die IT-Sicherheit bestellt ist. Gerade erst haben wir von Bekannten erfahren, wie prekär es sein kann, wenn man Opfer eines IT-Sicherheitsvorfalls wird. Man hat auf einmal mit ungeahnten Problemen zu tun. Unsere Freunde erhielten beispielsweise Post von Inkasso-Büros, Anwälten und von Web Shops bzgl. nicht bezahlter Rechnungen, obwohl sie nichts bestellt hatten.
>
> Wir sind uns in einem sicher – wir müssen uns um unsere private IT-Sicherheit kümmern, damit uns so etwas nicht auch passiert.

4.1.3 Maßnahmen zur Steigerung der persönlichen IT-Sicherheit

Aus WBT 1 wissen wir, wo wir ansetzen sollten, um die persönliche IT-Sicherheit zu stärken.

Die Möglichkeiten und Maßnahmen zur Steigerung der persönlichen IT-Sicherheit können sehr umfangreich und vielfältig sein. Um den Überblick nicht zu verlieren, sollte deshalb geplant und strukturiert vorgegangen werden. So kann es hilfreich sein, einzelne Maßnahmen anhand von praktischen Anwendungen zu betrachten.

Aus diesem Grund zeigen wir anhand unserer Familie, wie wir im Privaten mit dem Thema IT-Sicherheit umgehen.

4.1.4 Die verschiedenen Anwendungsbereiche

In WBT 1 haben wir die sechs Anwendungsbereiche kennengelernt, die uns helfen können, unsere private IT-Sicherheit in den Griff zu kriegen.

Diese sechs Anwendungsbereiche schauen wir uns im Detail an und werden sie mit konkreten Maßnahmen sicherer gestalten.

In den vorangegangenen WBT 2 und 3 haben wir uns bereits um die ersten beiden Anwendungsbereiche gekümmert. In diesem WBT beschäftigen wir uns mit dem Anwendungsbereich „sicheres Einkaufen im Internet“.

4.2 Einkaufen und Bezahlen im Internet

4.2.1 Einkaufen und Bezahlen im Internet

Familie Müller:

Nachdem wir uns die Geräte und Verbindungen in unserem unmittelbaren Umfeld (unserem privaten Netzwerk) angeschaut haben, werfen wir nun ein Blick auf den Anwendungsbereich „Einkaufen und Bezahlen im Internet“.

Denn auch dieser Anwendungsbereich hat maßgeblich mit unserer privaten IT-Sicherheit zu tun. Wer möchte schon, dass fremde Personen in unserem Namen und mit unserem Geld ungewollt Gegenstände oder Dienstleistungen in Anspruch nehmen?

4.2.2 Allgemeine Maßnahmen zum sicheren Einkaufen und Bezahlen im Internet

Timo:

Auch bei diesem Anwendungsbereich ist es sinnvoll, sich zunächst allgemeine Maßnahmen zur Steigerung der privaten IT-Sicherheit anzuschauen. Lisa zeigt direkt im Anschluss die konkreten Maßnahmen, die wir noch vor dem Einkaufen in einem Web Shop durchführen können. Mama zeigt uns danach, wie wir die IT-Sicherheit während der Nutzung von Web Shops steigern können.

Aber zunächst zur Liste allgemeiner Maßnahmen:

Im Vorfeld:

- Ist das Unternehmen bzw. der Zahlungsanbieter seriös/vertrauenswürdig?
- Ist der Zugang zur Web Site des Shops vor Dritten geschützt (https)?

Während der Nutzung von Online-Shops:

- Sichere und unterschiedliche Passwörter/Passwort-Manager verwenden
- Zusätzlichen Schutz bei der Authentifizierung in den Web Shops aktivieren (2-Faktor-Authentifizierung; 2FA)
- Vorsicht bei E-Mails mit integrierten Links und Anhängen
- Ist die im Benutzerkonto hinterlegte E-Mail-Adresse ebenfalls gut geschützt (sicheres Passwort, 2FA etc.)?
- Wurden Wiederherstellungsinformationen im Web Shop hinterlegt, falls Passwort oder Token verloren gehen?

4.2.3 Einkaufen im Internet: Umsetzung konkreter Maßnahmen

Lisa:

> Super Timo, Danke für den Überblick.
>
> Ich gucke mir nun zurerst konkret an, wie wir im Vorfeld sicherstellen können, dass ein Web Shop vertrauenswürdig ist. Dazu habe ich konkrete Maßnahmen zusammengestellt.

Konkrete Maßnahmen zur Prüfung der Vertrauenswürdigkeit eines Web Shops

- Angaben im Impressum überprüfen.
- Sind Gütesiegel vorhanden?
- Käuferschutz prüfen: trustedshops.de, trustpilot.com etc.
- Ist die Web Site des Shops verschlüsselt?

4.2.4 Überprüfung der Vertrauenswürdigkeit eines Web Shops – Impressum

Nach deutschem Recht muss jeder Web Site-Betreiber ein Impressum auf seiner Web Site veröffentlichen. Das Impressum umfasst alle notwendigen Angaben zu den verantwortlichen Personen und zeigt die Anschrift des Betreibers. Allein diese Maßnahme kann bereits helfen, seriöse Shops von Betrügern zu unterscheiden.

Die Angaben zum Impressum finden Sie zumeist am unteren Ende der Start-Seite des Web Shops.

4.2.5 Überprüfung der Vertrauenswürdigkeit eines Web Shops – Gütesiegel

Waren die Angaben im Impressum nicht eindeutig, können zusätzliche Web Sites helfen, die Vertrauenswürdigkeit eines Web-Shops zu überprüfen. Eine solche Web Site ist beispielweise die der Trusted Shops GmbH. Auf dieser Web Site sind viele verschiedene Web Shops inklusive Nutzerbewertungen gelistet.

4.2.6 Überprüfung der Vertrauenswürdigkeit eines Web Shops – https-Verschlüsselung

Um einen sicheren Einkauf samt Bezahlung im Internet durchführen zu können, ist es essentiell, eine sichere Verbindung über den Web-Browser zum Web Shop aufzubauen.

Unsere Familie wurde erstmals von unserer Bank auf diese Maßnahme hingewiesen. Wir sollen immer sicherstellen, dass in der Adressleiste des Browsers ein Schloss-Symbol zu sehen ist oder die Web-Adressen mit einem "**https**"-Text beginnt. Ein dahinterliegendes Protokoll stellt sicher, dass alle Verbindungen zwischen dem Einkäufer und dem Web Shop verschlüsselt und dadurch vor Außenstehenden geschützt sind.

4.3 Die sichere Nutzung von Web Shops

4.3.1 Konkrete Maßnahmen zur Nutzung von Web Shops

Anette:

Nachdem wir sichergestellt haben, dass der Web Shop vertrauenswürdig und die Verbindung verschlüsselt ist, sollten wir uns an die Maßnahmen im Rahmen der Nutzung des Web Shops kümmern.

Konkrete Maßnahmen zur sicheren Nutzung eines geprüften Web Shops

- Sicheres und einzigartiges Passwort verwenden
- 2-Faktor-Authentifizierung aktivieren (im Shop und in der hinterlegten E-Mail-Adresse)
- Sichere E-Mail-Adresse verwenden
- Konto-Wiederherstellungsinformationen hinterlegen

4.3.2 2-Faktor-Authentifizierung im Web Shop

Anette:

Ich stelle leider fest, dass die Web Shops alle unterschiedlich aufgebaut sind. Auch bietet nicht jeder Web Shop die Möglichkeit, eine 2-Faktor-Authentifizierung zu aktivieren.

Die Verwendung eines sicheren Passwortes ist jedoch bei allen Web Shops möglich.

Hans:

Die Zwei-Faktor-Authentisierung bezeichnet den Identitätsnachweis eines Nutzers mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Faktoren.

Zum Beispiel wird häufig gefordert, den Login per Kennung und geheimen Passwort (1. Faktor) in einer Web Site (Web Browser auf einem Rechner) durch die Eingabe einer PIN oder TAN (2. Faktor) in einer App auf dem Smartphone zu vervollständigen.

4.3.3 Sicheres Passwort im Web Shop

Anette:

Um ein sicheres Passwort setzen und ggf. die 2-Faktor-Authentifizierung aktivieren zu können, melde ich mich zuerst am Web Shop an. Anschließend finde ich die Passwort-Einstellungen meist im Bereich

„Sicherheit“ oder ähnlich bezeichnet.

Schauen wir uns die Umsetzung der konkreten Maßnahmen anhand eines bekannten Web Shops beispielhaft an.

Abb. 43: Sicheres und einzigartiges Passwort verwenden

Abb. 44: 2-Faktor-Authentifizierung aktivieren (im Shop und in der hinterlegten E-Mail-Adresse)

4.3.4 Sichere E-Mail-Adresse zur Verwendung im Web Shop

Anette:

Neben der Sicherheit des Benutzerkontos im Web Shop ist es essentiell, dass auch das hinterlegte digitale Postfach (die E-Mail-Adresse) gut geschützt ist.

Denn wenn ein Angreifer Zugriff auf die hinterlegte E-Mail-Adresse erhält, kann er sich meist mit einem Klick das Passwort des Kontos im Shop zusenden lassen. Daher gilt es, auch die E-Mail-Adresse mit einem starken Passwort und einer 2-Faktor-Authentifizierung zu schützen.

Ich zeige mal, wie das bei meinem E-Mail-Anbieter funktioniert.

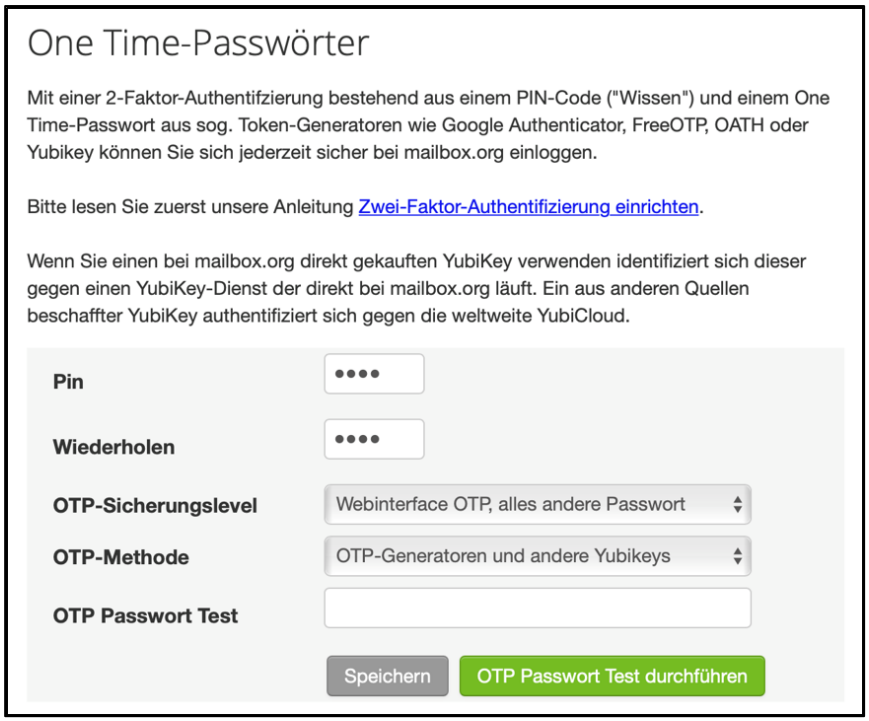


Abb. 45: 2-Faktor-Authentifizierung zum Schutz des E-Mail-Kontos

4.3.5 Betrachtete Maßnahmen zum sicheren Einkaufen im Internet

Lisa:

Wir haben uns nun einige relevante Maßnahmen zum sicheren Bezahlen und Einkaufen im Internet angesehen.

- ✓ Angaben im Impressum überprüfen
- ✓ Sind Gütesiegel vorhanden?
- ✓ Käuferschutz prüfen: trustedshops.de, trustpilot.com, etc.
- ✓ Ist die Web Site des Shops verschlüsselt?

4.3.6 Abendessen

Lisa:

Okay super, unser Verhalten im Internet insbesondere beim Einkaufen in Web Shops ist nun viel bedachter und sicherer.

Für heute machen wir Schluss und werfen den Grill an.

Demnächst informieren wir uns noch über Cloud-Dienste, den Schutz unserer Daten und überdenken unser Verhalten in sozialen Netzwerken.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: http://wi.uni-giessen.de

Herausgeber: Prof. Dr. Axel Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse http://wi.uni-giessen.de/