# 10-PUNKTE-PLAN AUF PRIVATHAUSHALT ANWENDEN

Modul 231

Name, Name

# Inhalt

# Einleitung

In dieser Dokumentation werden wir den ISSS 10-Punkte-Plan für Klein- und Mittelbetriebe auf den Privathaushalt von der Familie Däppen anwenden. Dafür werden wir zuerst den Sachverhalt vor den getroffenen Massnahmen erläutern und diesen auch teilweise grafisch darstellen. Danach werden wir den oben genannten Sachverhalt analysieren und auswerten. Anhand dieser Auswertung werden wir Massnahmen treffen, diese umsetzen und Dokumentieren. Zum Schluss werden wir das Endergebnis aufzeigen und die Umsetzung der getroffenen Massnahmen auswerten. In dieser Doku werden wir ausschliesslich auf die ersten 10 Punkte des 10-Punkte-Plans eingehen. Auf die Punkte für mehr Vertraulichkeit und mehr Verfügbarkeit werden wir nicht eingehen.

Die Familie besteht aus 5 Personen, wovon sich 3 nicht wirklich gut mit Technik und Informationssicherheit auskennen. Deshalb sind wir zuversichtlich, dass wir mithilfe des 10-Punkte-Plans und den getroffenen Massnahmen die Informationssicherheit in diesem Haushalt erhöhen können. [1]

[2]

# Was ist der 10-Punkte-Plan?

Der 10-Punkte-Plan ist ein 10-Punkte-Programm, welches für mehr Informationssicherheit in Klein- und Mittelbetrieben sorgen soll. Dieser unterliegt seit der Auflösung von InfoSurance im Mai 2016 dem Copyright von ISSS auch bekannt als Information Security Society Switzerland). Der 10-Punkt-Plan enthält 10 Massnahmen, um einen wirkungsvollen Grundschutz zu erhalten. Ausserdem enthält der 10-Punkte-Plan noch 5 weiter Punkte für mehr Vertraulichkeit und mehr Verfügbarkeit. Zu jedem dieser insgesamt 20 Punkten werden die Grundsätze genannt, der Punkt erläutert und Tipps & Tricks genannt. Wenn man die 10 ersten Punkte des 10-Punkte-Plans korrekt befolgt, sollte laut dem Schweizerischen Gewerbeverband [3] ein wirkungsvoller Grundschutz entstehen. Ausserdem sollen bei der Umsetzung des 10-Punke-Plans keine grossen Kosten entstehen. [4]


*[5]*

# Sachverhalt vor Anwendung des 10-Punkte-Plans

## IT-Infrastruktur beschrieben

Der Haushalt besitzt einen Swisscom-Router mit eingebauter Firewall, über welchen man ins Internet kommt. Die oben genannte Firewall kann beliebig konfiguriert werden und wird jede Woche, wenn möglich auf den neusten Stand gebracht. An dem oben genannten Router sind Access-Points welche auch als Router dienen angeschlossen. Beide Access-Points verfügen über WPA2. Bei beiden Access Points ist WPS auch bekannt als Wi-Fi Protected Setup deaktiviert. Die Namenskonvention wurde sehr schlicht gehalten. Bei Laptops und PCs wird einfach das Gerät (Laptop oder PC) und danach der Vorname des Besitzers für den Namen gewählt wie z.B. «Laptop Name». Bei Handys, Tablets und Spielkonsolen wird nur das Modell des Gerätes als Name verwendet wie z.B. «OnePlus 8 Pro». [1]

Access Point 1 hat eine versteckte SSID, ein mehr als 24 Zeichen langes Passwort und die Firmware wird monatlich vom ältesten Sohn auf Updates überprüft. Auf den oben genannten AccessPoint sind die Geräte des ältesten Sohns und seiner Freundin verbunden. Dass sind folgende Geräte: 2 Handys, ein Tablet, 2 Spielkonsolen, 2 Laptops (Windows) und 2 PCs (Windows). Auf den Laptops und PCs läuft ein Antivirenprogramm von Kaspersky Lab [6]. Der Administrator für alles was in diesem Netz ist, ist Name der älteste Sohn. [1]

An Access Point 2 sind die Geräte der restlichen Familie angehängt. Dazu gehören 3 Handys, eine Spielkonsole, ein Tablet, ein PC (Windows) und 3 Laptops (Windows). Access Point 2 hat eine sichtbare SSID welche jedoch nicht auf den Besitzer hindeutet. Ausserdem hat der oben genannte Access Point ein Passwort welches weniger als 24 Zeichen hat und die Firmware wird nur ein- bis zweimal pro Jahr aktualisiert. Wie auch schon im ersten Netz haben alle Laptops und PCs ein Antivirenprogramm von Kaspersky Lab [6]. Einen richtigen Fernseher hat die Familie nicht mehr da man eigentlich alles im Internet anschauen kann. Der Vater der Familie ist der Administrator für alles was sich im Netz von Access Point 2 befindet. [1]

Gefahren für die IT-Infrastruktur von diesem Privathaushalt sind auf den ersten Blick der jüngste Sohn, die Mutter und die Freundin des ältesten Sohnes da diese sehr unvorsichtig im Internet unterwegs sind und gerne mal wieder auf irgendwelche Links in E-Mails klicken und irgendwelche Daten eingeben. Eine weitere Gefahr ist das WLAN-Netzwerk von Access

Point 2 da dieser eine Sichtbare SSID hat und was noch schlimmer ist, ist das sehr kurze und schlechte Passwort. [1]

### IT-Infrastruktur dargestellt (Netzwerkplan)

Musste entfernt werden

# Analyse der zu den 10 Punkten

## Erstellen Sie ein Pflichtenheft für IT-Verantwortliche!

Da die Familie keinen IT-Verantwortlichen besitzt existiert auch kein Pflichtenheft für diesen. Jedoch gibt es kleinere Richtlinien mit dem Umgang von technischen Geräten. Man darf nicht willkürlich Links anklicken und auch nicht auf kuriosen Website Login- oder sonstige Daten eingeben. [1]

## Sichern Sie Ihre Daten regelmässig mit Backups!

Im ganzen Haushalt wird eigentlich mit einer Cloud von Apple oder Microsoft gearbeitet. Das heisst alles was auf iPhones und iPads einen bestimmten Grad an Wichtigkeit hat wird in die iCloud gespeichert und alles was wichtig ist und auf eine PC oder einem Laptop ist wird in die OneDrive gespeichert. Alles was auf einem OnePlus ist, ist sich selbst überlassen und wird im Ernstfall verloren sein. Trotzdem gibt es Dinge welche mit einer lokalen Sicherung der Daten gesichert werden. Im Haushalt der Familie Däppen wird die Buchhaltung einmal im Monat und die Daten auf dem PC von Name einmal pro Woche auf externe Festplatten gespeichert. [1]

## Halten Sie Ihr Antivirus-Programm aktuell!

Das Antivirenprogramm wie auch ein Teil anderer Software auf den privaten Geräten werden wöchentlich aktualisiert. Die Geräte sind also nicht länger als eine Woche nicht auf dem neusten Stand des Antivirenprogramms. Ausserdem versendet Kaspersky Lab selbst E-Mails und Desktop-Benachrichtigungen, falls eine neue Version des Antivirenprogramms verfügbar ist. [1]

## Schützen Sie Ihren Internetzugang mit einer Firewall!

Im Swisscom Router befindet sich eine eingebaute Firewall, welche vom ältesten Sohn verwaltet wird. Die Firewall ist mit einem starken Passwort geschützt welches mehr als 24 Zeichen lang ist. Ausserdem wird die Konfiguration der Firewall regelmässig gespeichert. [1]

## Aktualisieren Sie Ihre Software regelmässig!

Die Software auf den Geräten, welche an Access Point 1 angeschlossen sind, wird fast täglich aktualisiert. Dafür wird von Name selbst auch ein Log geführt, wann welche Software auf welche Version aktualisiert wurde. Jedoch ist auch mit Nachfragen bei den anderen Familienmitgliedern nicht genau bekannt, ob dies auch bei den Geräten im Netz von Access Point 2 der Fall ist. [1]

## Verwenden Sie starke Passwörter!

Grundsätzlich werden überall starke Passwörter verwendet da die Familie sich darauf geeinigt hat, dass ein Passwort mindestens 14 Zeichen lang sein muss und Zahlen, Sonderzeichen, Gross- und Klein Buchstaben enthalten sollte. Ausserdem dürfen die Passwörter der Familie nicht aus Namen, Kürzel oder Wörtern bestehen. Nur bei den 2 PCs, allen iPhones und iPads werden noch 6-stellige Pins zur Entsperrung des Gerätes verwendet. [1]

## Schützen Sie Ihre mobilen Geräte!

Beide Access Points verfügen über einen MAC-Filter, das heisst dass nur die registrierten Geräte, also die der Familie sich mit dem WLAN verbinden dürfen. Jedoch gibt es auch da ausnahmen da der älteste Sohn gerne auch mal ein Gerät von einem Kollegen registriert damit dieser bei Ihm zuhause Internetzugriff hat. Sehr private Daten werden jedoch nur mit Hilfe eines VPN über WLAN übertragen. Die Familie nutzt dazu NordVPN [8]. Die Handys und Tablets sind jedoch nicht mit einem Antivirenprogramm ausgestattet. [1]

## Machen Sie Ihre IT-Benutzerrichtlinien bekannt!

Genaue Benutzerrichtlinien gibt es eigentlich nicht. Die einzige klar festgelegte Richtlinie ist die oben bei Punkt «Verwenden Sie starke Passwörter!» genannte Passwortrichtlinie. Ausserdem gilt: man darf nicht einfach irgendwelche Programme aus dem Internet herunterladen, man darf nicht einfach auf einer zwielichtigen Website Login- oder andere Daten eingeben und man muss die Software regelmässig aktualisieren. [1]

## Schützen Sie die Umgebung Ihrer IT-Infrastruktur!

Das Haus ist immer abgeschlossen, auch wenn jemand zuhause ist. Der Swisscom-Rauter befindet sich in einen abgeschlossenen, gut klimatisierten Raum im Keller wo nur der älteste Sohn und der Vater der Familie Zugang haben. Dass Zimmer vom ältesten Sohn wird immer abgeschlossen falls sich niemand im Raum befindet. Zugriff haben nur der älteste Sohn und seine Freundin. Somit ist der Zugriff zum Access Point 1 gut geschützt. Vom Access Point 2 kann man dies nicht behaupten da dieser frei zugänglich im Wohnzimmer steht. [1]

### Ordnen Sie Ihre Dokumente und Datenträger!

Alle ausgedruckten Dokumente werden im Kellerarchiv der Familie nach Datum und Thema geordnet bei guten Luftbedingungen gelagert. Dort werden auch die externen Festplatten der Buchhaltung gelagert. Zugriff zu diesem Archiv hat nur der Vater der Familie. Elektronische Daten, welche nicht benötigt werden, werden nur von dem ältesten Sohn und dem Vater überschrieben. Die anderen Familienmitglieder löschen die Daten in dem sie «DELETE» oder einen Löschen-Button drücken oder die Dateien einfach in den Mülleimer ziehen. [1]

# Auswertung

## Was war gut?

- Eine Passwortrichtlinie festgelegt
- Dass fast alle wichtigen Daten in einer Cloud gespeichert sind und von Verlust geschützt sind
- Dass physische Ausgedruckte Daten archiviert werden.
- MAC-Filter bei WLAN-Netzwerken

## Was war nicht so gut (Massnahmen erforderlich)?

- 6-stellige Pins für PCs, iPhones und iPads
- Dass Software nur wöchentlich oder sogar über längeren Zeitraum nicht aktualisiert wird
- Dass Mobile Geräte wie Handys und Tablets über kein Antivirenprogramm verfügen.
- Dass es keine genauen Nutzungsrichtlinien gibt, vor allem wenn es Personen im Haushalt gibt welche nur über wenig Erfahrung mit dem Umgang mit Technik und Internet verfügen
- Access Point 2 verfügt über ein schwaches Passwort und die SSID ist sichtbar, auch wenn diese nichts über den Besitzer des WLAN-Netzwerkes aussagt

# Massnahmen

Die getroffenen Massnahmen wurden aufgrund der obenstehenden Aufwertung der Analyse zu 10-Punkt-Plan getroffen. Die Massnahmen, welche von uns getroffen wurden, sind für uns sinnvollsten, um die Datensicherheit in diesem Haushalt zu erhöhen.

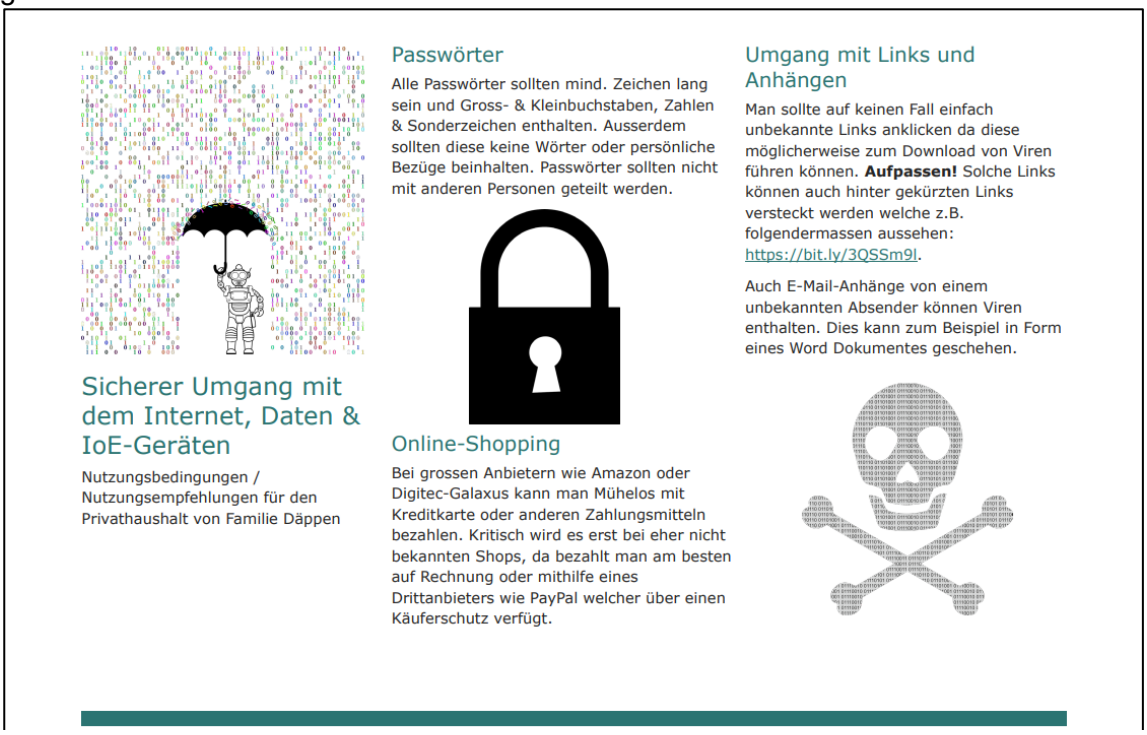
Die erste Massnahme, welche wir getroffen haben, ist die Personen im Haushalt darüber aufzuklären, warum und wieso man die installierte Software aktualisieren muss. Als nächstes

muss Access Point 2 sicherer gemacht werden. Dafür werden wir wahrscheinlich sicher mal das Passwort ändern und evtl., wenn die zuständige Person dies auch einsieht, die SSID verstecken. Ausserdem müssen grundlegende Nutzungsbedingungen aufgesetzt werden. Diese werden wahrscheinlich Passwort- und Pinrichtlinien, Umgang mit dem Internet, Umgang mit gelöschten Daten und Umgang mit technischen Geräten im Allgemeinen beinhalten. Zum Schluss wird endlich auch Virenschutz für die mobilen Geräte zu Verfügung gestellt, falls die Familie dies auch will und die Kosten dafür tragen möchte.

# Umsetzung der Massnahmen

In den untenstehenden Massnahmen wird mehrmals das Wort «wir» in direktem Bezug zur Familie verwendet. Falls jedoch etwas direkt mit jemandem der Familie Mitgeteilt wurde, wurde dies indirekt über Name getan und von allen von uns allen geplant da nur Name vor Ort war.

Wir haben die Massnahme für zu aktualisierende Software und die Massnahme zu fehlenden Nutzungsbedingungen zusammen in eine Lösung gepackt. Dafür haben wir eine kleine Broschüre mit Grundlegenden Nutzungsbedingungen erstellt, diese Ausgedruckt und an jeden der Familie verteilt. Ausserdem hat Name zu jedem PC im Haus noch eine davon dazu gelegt. Wir haben diese Broschüre möglichst einfach formuliert damit hoffentlich jede Person im Haushalt diese versteht und umsetzten kann. Die Vorderseite der Broschüre sieht folgendermassen aus:




[9]

Die gesamte Broschüre kann man unter den Anhängen einsehen.

Als nächstes haben wir den Vater der Familie darüber aufgeklärt, warum man ein starkes Passwort für ein WLAN-Netzwerk wählen soll. Dieser hat dies auch eingesehen und das Passwort geändert. Nach mehrfachem erklären, weshalb man die SSID am besten verstecken soll, wurde dies auch getan. Danach haben wir den Personen, welche mit dem WLAN-Netzwerk von Access Point 2 verbunden sind, erklärt wie sie nun auf dieses Netzwerk zugreifen können.

Zum Schluss haben wir der Familie vorgeschlagen sich auch noch ein Antivirenprogramm für die mobilen Geräte zuzulegen und wir haben der Familie eine kostenloses Antivirenprogramm vorgeschlagen. Wie sich jedoch herausstellte hatte die Familie schon vor sich ein Antivirenprogramm von Kaspersky Lab für die Mobilen Geräte zu kaufen. Dies wurde auch einige Tage nach dem Gespräch getan.

# Quellen & Arbeitsverteilung

## Quellen

[1] Informationen von Name

[2] Bild von IO-Images auf Pixabay

[3] Schweizerischer Gewerbeverband

[4] PDF: 10-Punkte-Plan ISSS oder IET-Gibb Filestash oder Anhang «A1»

[5] KMU Admin

[6] Kaspersky Lab

[7] Erstellt mit Diagrams.net

[8] NordVPN

[9] Anhang «A2»