cara.
connecté à ma santé

Best Practices der IT-Sicherheit

Warum ist IT-Sicherheit so wichtig?

- **...um Ihre Arbeit sicherzustellen**
  Bei einem Sicherheitsproblem können Sie lange Zeit nicht mehr mit Ihrer IT-Ausrüstung und Ihren Daten arbeiten.

- **...um die Daten der Personen zu schützen, die Ihnen vertrauen**
  Vertrauen ist grundlegend. Die Personen, die Ihnen ihre Daten anvertraut haben, verlassen sich darauf, dass Sie ihre Daten schützen.

- **...um Ihr vertragliches Engagement gegenüber CARA zu erfüllen**
  Sie haben sich bei Ihrem Anschluss an CARA dazu verpflichtet, die minimalen Sicherheitsvorgaben einzuhalten.

- **...weil diese grundlegenden Regeln noch viel zu oft vernachlässigt werden**
  Es gilt also nicht bloss, diesen Leitfaden zu lesen – sein Inhalt muss von Ihrer Organisation und Ihren Nutzerinnen und Nutzern auch tatsächlich umgesetzt werden.

20 Best Practices zur Steigerung der Sicherheit Ihrer Informationen

Sie können Ihre Sicherheit wirklich und effizient steigern, indem Sie die nachstehenden 20 Best Practices anwenden, die in sechs Bereiche unterteilt sind:

A. Material
B. Usermanagement
C. Praktiken
D. Passwörter
E. Aufmerksamkeit und Vorsicht
F. Sensibilisierung

A. MATERIAL

Best Practice Nr. 1
Führen Sie regelmässig Software-Updates durch und aktualisieren Sie regelmässig Ihr Betriebssystem (Windows, MacOS, Android, iOS) und den Webbrowser, mit dem Sie auf das EPD zugreifen. So können Sie Sicherheitslücken vermeiden.

Wenn eine Firma Ihre IT verwaltet, bitten Sie diese um regelmässige Aktualisierungen, im Idealfall jedes Mal, wenn eine neue Version verfügbar ist.

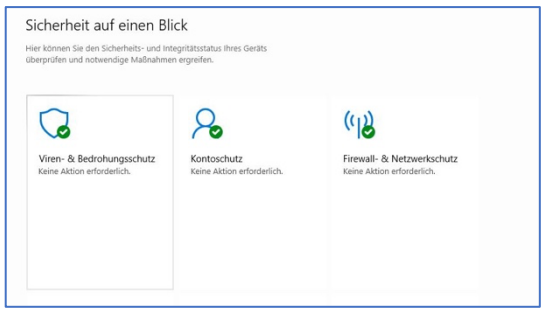
Best Practice Nr. 2
Verwenden Sie eine Anti-Virus-Software auf dem neuesten Stand.

Sie können Ihr Anti-Virus-Programm öffnen, um das Update-Datum zu überprüfen und allenfalls automatische Updates zu erlauben.

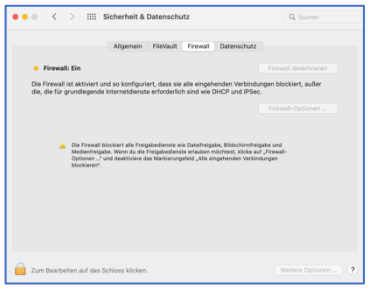
Best Practice Nr. 3
Verwenden Sie eine Firewall.

Sie können beispielsweise die Firewall Ihres Betriebssystems verwenden. Diese muss aktiviert werden.

Beispiel auf Windows



Beispiel auf Mac



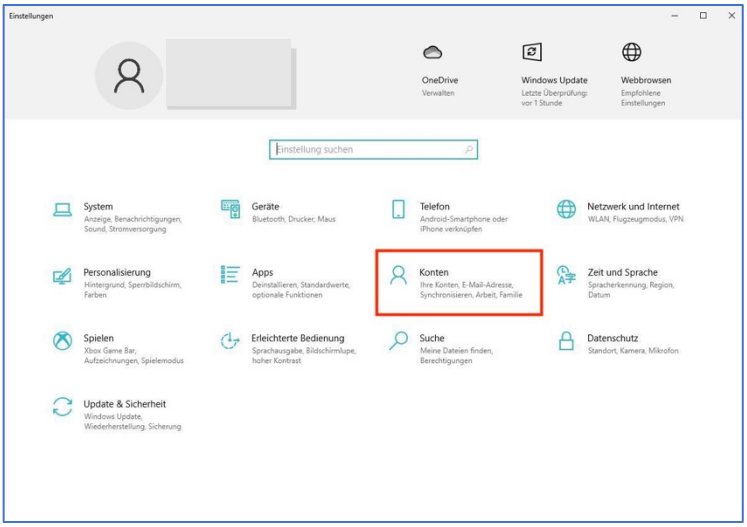
Sie können auch eine physische Firewall oder eine Firewall auf Ihrem Moden einrichten.

Best Practice Nr. 4

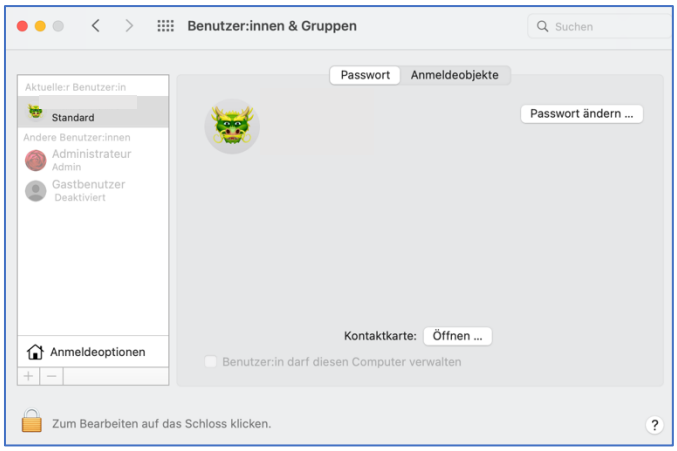
Arbeiten Sie nicht von einem Benutzerkonto mit Administratorenrechten aus.

Sie können auf Ihrem Computer unter verschiedenen Benutzerkonten arbeiten. Von einem Benutzerkonto mit Administratorenrechten aus können Sie funktionale oder betriebliche Änderungen an Ihrem Computer vornehmen. Das ist von einem Standard-Benutzerkonto aus nicht möglich. Um die Installation von Malware zu verhindern, ohne dass Sie dem zugestimmt haben, sollten Sie von einem Benutzerkonto aus arbeiten, bei dem Sie nicht Administrator sind. Das ändert nichts an Ihrer laufenden Arbeit. Sollte aber eine Softwareinstallation oder ein Update nötig sein, müssen Sie zuerst ein Administratoren-Passwort eingeben. Auf diese Weise haben Sie eine bessere Kontrolle darüber, was auf Ihrem Gerät installiert wird.

Beispiel auf Windows



Beispiel auf Mac



Best Practice Nr. 5
Greifen Sie nur von Computern aus auf die Plattform CARA zu, die nach den oben genannten Punkten gesichert wurden.

B. USERMANAGEMENT

Best Practice Nr. 6
Denken Sie daran, die Zugriffsrechte von Personen, die Ihre Organisation verlassen, zu sperren.

Best Practice Nr. 7
Informieren Sie auch CARA, wenn Nutzerinnen und Nutzer Ihre Organisation verlassen. Das können Sie über folgendes Online-Formular tun: https://forms.cara.ch/institution/staff-mutation. Dadurch wird die User-Liste auch auf der Plattform CARA aktualisiert.

Best Practice Nr. 8
Erteilen Sie Ihren Nutzerinnen und Nutzern lediglich die Zugriffe, die zum Erledigen ihrer Aufgaben nötig sind.

C. PRAKTIKEN

Best Practice Nr. 9
Nutzen Sie eine sichere Internetverbindung.

- Stellen Sie sicher, dass Sie sich mit einem Netzwerk verbinden, das Sie kennen.
- Stellen Sie sicher, dass Ihr übliches Netzwerk passwortgeschützt ist (siehe Kapitel D).
- Stellen Sie sicher, dass nur Sie selbst und Ihre Kolleginnen und Kollegen Zugriff auf dieses Netzwerk haben.

Best Practice Nr. 10
Loggen Sie sich immer aus, wenn Sie das EPD verlassen, auch wenn es nur für kurze Zeit ist.

Best Practice Nr. 11
Schliessen Sie keine externen Datenträger (z.B. Harddisk oder USB-Stick), die von Personen von ausserhalb Ihrer Organisation stammen, an Ihren Computer an.

Best Practice Nr. 12
Lassen Sie keine unbefugte Dritte in Ihre Nähe, wenn Sie auf die Plattform CARA oder auf Ihr klinisches Informationssystem (z.B. Praxissoftware) zugreifen.

D. PASSWÖRTER

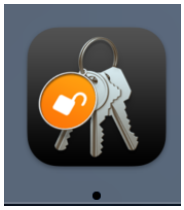
Best Practice Nr. 13
Erstellen Sie für jedes Ihrer Konten komplexe Passwörter aus Grossbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen, die Sie nur für das jeweilige Konto benutzen.

CARA empfiehlt mindestens zehn Zeichen lange Passwörter, die mindestens einen Grossbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten. Sie können beispielsweise einen ganzen Satz verwenden, der für Sie Sinn macht und den Sie sich leicht merken können.

Best Practice Nr. 14
Schreiben Sie Ihre Passwörter niemals auf einen physischen Träger (Post-it, Heft, unter die Tastatur usw.).

Sie können sie hingegen in einer Schlüsselbund-Software auf Ihrem Computer oder Telefon abspeichern, sofern nur Sie selbst darauf Zugriff haben.

Beispiel auf Mac
«Schlüsselbundverwaltung»



Best Practice Nr. 15
Geben Sie Ihre Passwörter nie irgendjemandem bekannt.

CARA und alle seriösen Leistungserbringer werden Sie nie nach Ihrem Passwort fragen –- weder telefonisch noch via E-Mail oder Brief. Wenn CARA, ein Anbieter elektronischer Identitäten (z.B. Hin, GenèveID oder VaudID santé) oder irgendein anderer Leistungserbringer Sie nach etwas fragt, das Ihnen suspekt vorkommt, fragen Sie besser zuerst über die offizielle Telefonnummer auf der entsprechenden Website nach.

Sie erreichen CARA unter der Nummer 021 566 84 51.

Es ist ebenfalls verboten, sein elektronisches Identifikationsmittel an eine Drittperson weiterzugeben – auch nicht innerhalb Ihrer Organisation.

E. AUFMERKSAMKEIT UND VORSICHT

Best Practice Nr. 16
Lassen Sie sich nicht betrügen oder ablenken. Wenn Sie etwas seltsam oder ungewöhnlich finden, seien Sie vorsichtig.

Best Practice Nr. 17
Öffnen Sie keine Anhänge von E-Mails von unbekannten Absendern. Wenn Sie den Absender nicht kennen, Ihren Namen unter den Empfängern nicht sehen oder der Text seltsam geschrieben ist (Fremdsprache, viele Rechtschreibfehler, ungewöhnliche Formulierungen), löschen Sie die E-Mail.

Bei Zweifeln oder wenn Sie den Anhang schon angeklickt haben, kontaktieren Sie sofort Ihren IT-Anbieter oder IT-Verantwortlichen.

Best Practice Nr. 18
Klicken Sie auf keine Links in E-Mails oder Nachrichten, ohne vorgängig die Vertrauenswürdigkeit des Absenders überprüft zu haben. Sie können beispielsweise ohne zu klicken mit der Maus über den Link fahren – so wird die URL angezeigt. Wenn Sie die Website nicht kennen oder Zweifel am Absender hegen, löschen Sie die Mail.

Bei Zweifeln oder wenn Sie den Link schon angeklickt haben, kontaktieren Sie sofort Ihren IT-Anbieter oder IT-Verantwortlichen.

F. SENSIBILISIERUNG

Best Practice Nr. 19
Sprechen Sie mit Ihren Kolleginnen und Kollegen über IT-Sicherheit, vor allem über diese Best Practices.

IT-Sicherheit, namentlich über diese Punkte, erfolgt über gemeinsame Aufmerksamkeit und Vorsicht. Verbreiten Sie diese Punkte und erklären Sie den IT-Usern, dass sie wichtig sind.

Sie können beispielsweise unser Blatt «Sicherheitsregeln» verwenden, um mit Ihren Kolleginnen und Kollegen darüber zu sprechen, und das Blatt direkt in Ihren Räumlichkeiten aufhängen.

Best Practice Nr. 20
Sprechen Sie mit Ihren Kolleginnen und Kollegen, mit Ihren Mitarbeiterinnen und Mitarbeitern regelmässig über IT-Sicherheit.

Denken Sie daran, sie regelmässig daran zu erinnern und dieses Thema mit ihnen zu besprechen, beispielsweise beim Arbeitsbeginn neuer Mitarbeitender oder zweimal jährlich zu festgelegten Daten. Auch wenn diese Regeln einfach und offensichtlich sind, lassen sich eine Vielzahl von Risiken durch besondere Aufmerksamkeit und Vorsicht vermeiden.

Support
Bei Fragen zu den Best Practices stehen wir Ihnen gerne zur Verfügung:
www.cara.ch/de/Support