tethisIT
Kluge IT für Unternehmer

UGP Workshop
Datensicherheit & Datenschutz

Christian Toller, tethis IT e.U.
www.tethis-it.at

Inhalt

Tag 1

- Wogegen wir Daten schützen müssen
- DSGVO: Grundlagen & Ziele
- Das Verfahrensverzeichnis
- Risikoeinschätzung
- Einwilligungserklärungen
- Auftragsverarbeiter-Verträge
- Mitarbeitervereinbarungen
- Regelmäßige Überprüfung

Tag 2

- Technische Schutzmaßnahmen
  - Passwörter
  - Verschlüsselung
  - Datensicherung
  - Virenscanner und Firewall
  - HTTPS
  - Webseite sichern
- Organisatorische Schutzmaßnahmen
- Datenschutzerklärung
- Zusammenfassung / F & A

Dies ist keine Rechtsberatung!

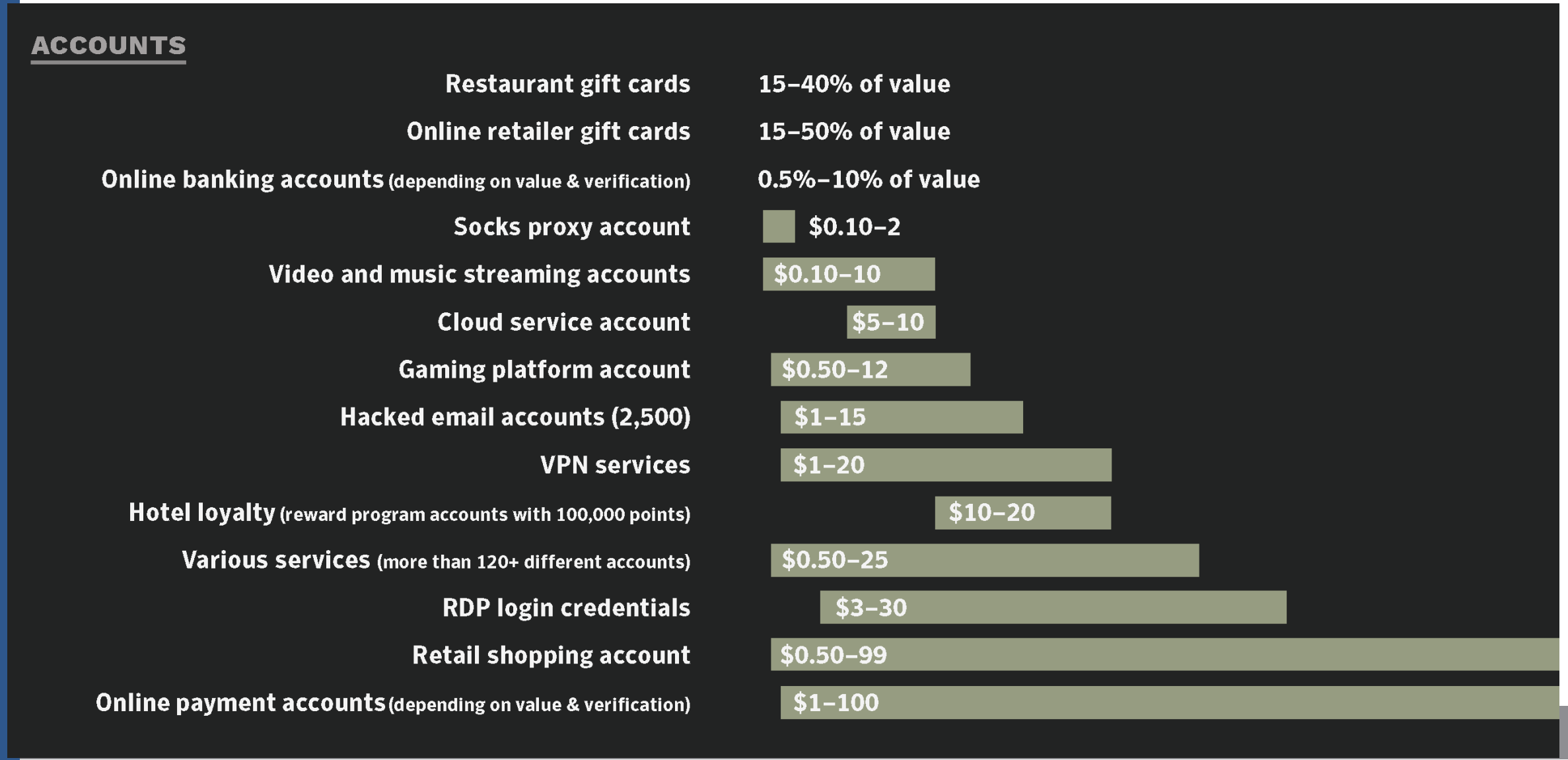
tethisIT
Kluge IT für Unternehmer

- Ich bin kein Anwalt, sondern IT Spezialist
- Dieser Workshop ersetzt keine Rechtsberatung
- Im Zweifel: Fragt einen Anwalt oder die WKO!
- Die WKO hat diesbezüglich zahlreiche Förderprogramme

- Ansonsten gilt: Gesunder Menschenverstand hilft ☺

Bedrohungen © Symantec Internet Security Threat Report 2019

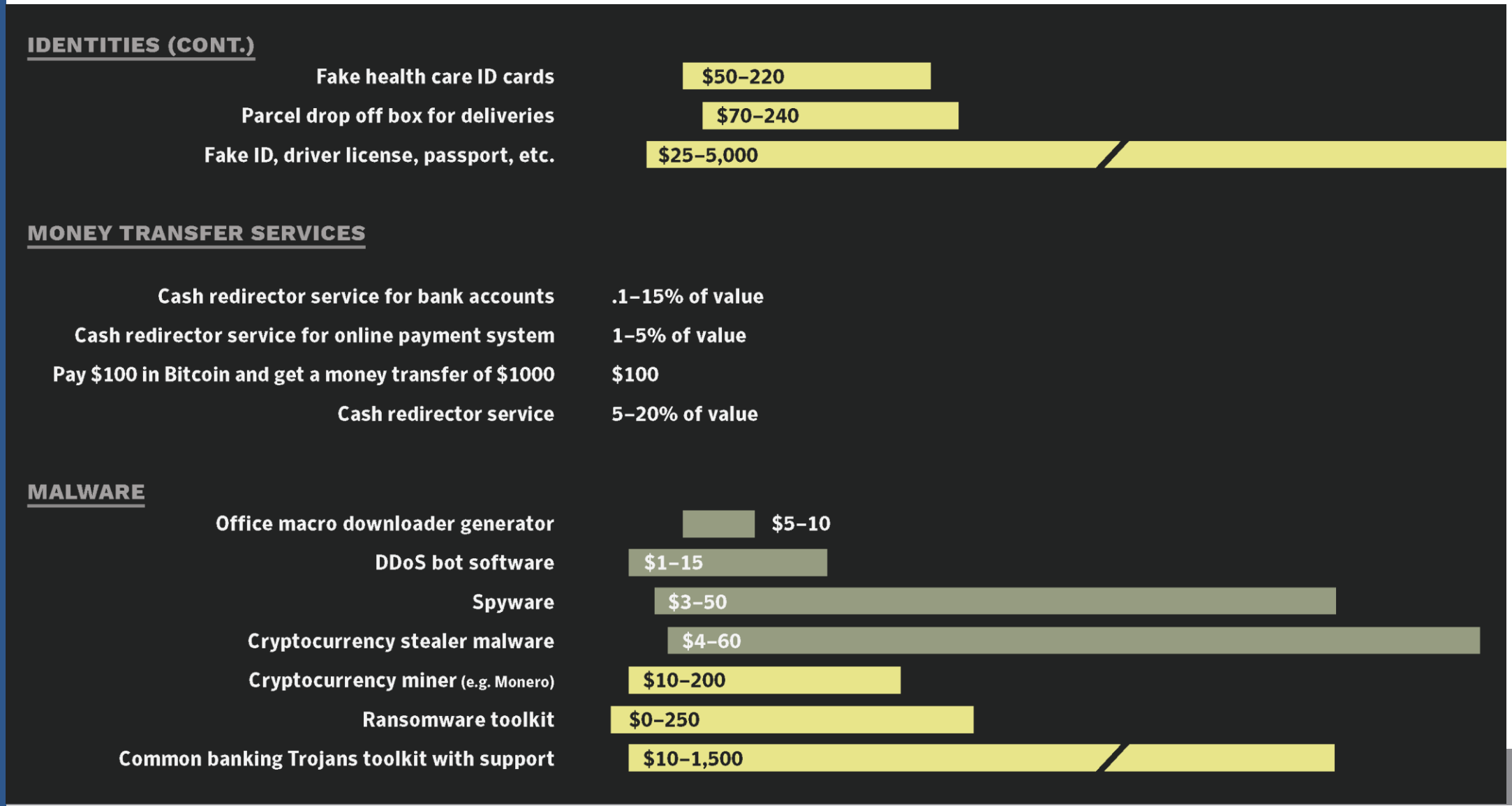
tethisIT
Kluge IT für Unternehmer



Bedrohungen

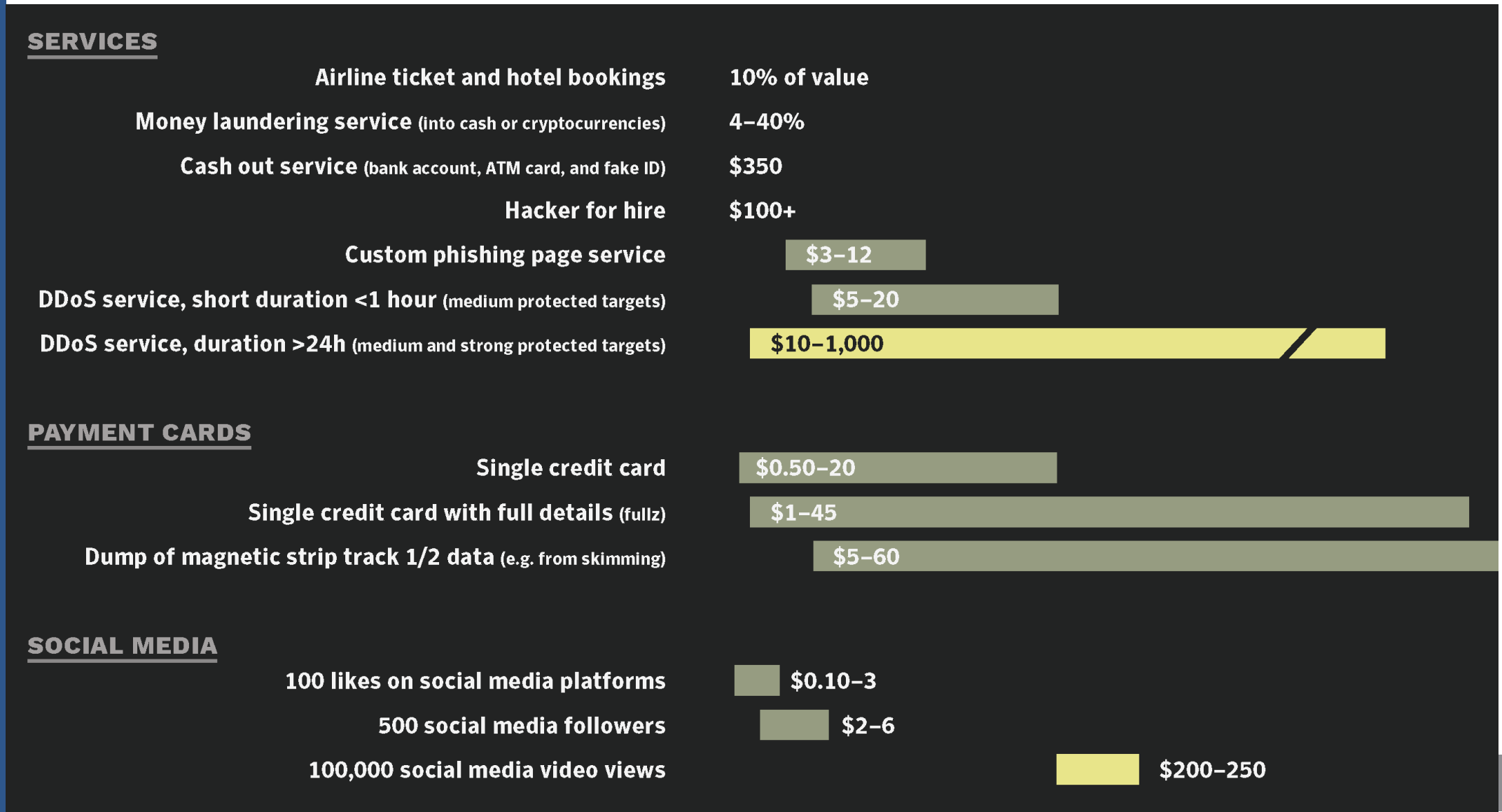
© Symantec Internet Security Threat Report 2019

tethisIT
Kluge IT für Unternehmer



Bedrohungen © Symantec Internet Security Threat Report 2019

tethisIT
Kluge IT für Unternehmer



Bedrohungen

- Datendiebstahl:
  - Daten werden in großem Stil gehandelt
  - Viren & Trojaner
  - Einbruch in Systeme
  - Schadsoftware verhält sich ruhig, versteckt sich
  - Key-Logger protokollieren jeden Tastendruck
  - Infektion über E-Mails, Webseiten, Downloads, USB-Sticks
- Ransomware
  - Verschlüsselt die komplette Festplatte
  - Erpressung: Entschlüsselung nur gegen Geld (oder auch nicht)

Bedrohungen

- Defekte an Hard- oder Software
  - Festplatten sind „Verbrauchsmaterial“ mit begrenzter Lebensdauer
  - Software kann Daten zerstören
  - Ausfälle kündigen sich in der Regel nicht an
  - Redundanz kann helfen
  - Cloud-Lösungen sind weniger Anfällig
- Diebstahl von Geräten und Datenträgern
  - Handys, Laptops und Tablets werden gerne gestohlen
  - Bei Einbruch könnte auch die Sicherung gestohlen werden
  - Kann der Dieb auf Daten zugreifen?

Bedrohungen

Bedrohungen

- Feuer und Naturkatastrophen
  - Zerstört Geräte und Datensicherungen

- Menschliches Versagen
  - Versehentliche Änderungen
  - Überschreiben (Speichern statt Speichern unter…)
  - Versehentliches Löschen
  - Versehentliches Veröffentlichen (Reply-All statt Reply)

Bedrohungen

Daten sind ein wertvolles Gut!

„*Wenn man für ein Produkt nichts zahlt, ist man selbst das Produkt*“

Geschäftsmodelle von Google, Facebook, Instagram usw. basieren auf der Nutzung von personenbezogenen Daten zu Werbezwecken.
=> Daten bewusst weitergeben. Oder auch nicht.

DSGVO Grundlagen

Die EU Datenschutz-Grundverordnung (DSGVO)

engl.: EU General Data Protection Regulation (GDPR)

Worum geht es?

Ziel:

Mehr Kontrolle über die eigenen Daten

Verpflichtung zum Schutz der Daten

DSGVO definiert Grundsätze und Regeln

für gesetzeskonforme Datenverarbeitung

Die Gesetze

- Bisher: Datenschutzgesetz (DSG) 2000
- EU Datenschutzgrundverordnung (DSGVO)
- Österreichische Anpassungen: DSG 2018
- E-Commerce Gesetz, Telekommunikationsgesetz
- Gewerbeordnung 1994

DSGVO in Kraft seit 24.5.2016, verpflichtend seit 25.5.2018
Strafen: 2% / 10 Mio. €, in schweren Fällen 4% / 20 Mio. €
Datenschutzbehörde verhängt Strafen

Österreichische Anpassungen

Am 14. April 2018 hat das österreichische Parlament folgende Änderungen beschlossen:

- Angemessene Bestrafungen (Verhältnismäßigkeit)
- Beim ersten Verstoß wird nur verwarnt
- Günstigere Regelung (alt / neu) wird angewendet
- Behörden bleiben praktisch straffrei, keine Doppelbestrafung
- Keine Strafen für Spione
- Schadenersatzforderung durch Organisationen nicht möglich
- DSGVO gilt nicht für Journalisten
- Videoüberwachung zulässig

Gültigkeitsbereiche

Gilt für personenbezogene Daten lebender Personen

Gilt für alle Unternehmen, die „am EU Markt teilnehmen“

Gilt nicht für:

- Anonymisierte Daten
- Daten verstorbener Personen
- Daten aus der Familie / dem Freundeskreis

Keine relevanten Ausnahmen für kleine Firmen!

Was wird geregelt?

Für erlaubte Verarbeitungen regelt die DSGVO z.B.

- Rechtsgrundlagen
- Rechte und Pflichten
- Verpflichtung zum Schutz der Daten
- Rollen in Hinsicht auf Datenschutz
- Regelmäßige Überprüfung

Rollen in der DSGVO

tethisIT
Kluge IT für Unternehmer

Betroffene(r)	Verantwortliche(r)
Derjenige, dessen Daten verarbeitet werden. In der Regel ein Kunde, Lieferant, Mitarbeiter	Derjenige, der die Daten verarbeitet. In der Regel Ihr!
Empfänger	**Auftragsverarbeiter**
Jemand, an den der Verantwortliche Daten weitergibt und der Sie dann eigenverantwortlich verarbeitet	Jemand, der die Daten im Auftrag des Verantwortlichen verarbeitet, aber keine Verantwortung übernimmt.

Auftragsverarbeiter

Verantwortlicher:
Entscheidet über Zwecke und Mittel der Datenverarbeitung.

Auftragsverarbeiter:
Verarbeitet Daten im Auftrag / im Interesse / zugunsten eines Auftraggebers.

Vor allem wer über den Zweck entscheidet, ist verantwortlich.

Das können auch beide sein!

Besser für den Auftraggeber: geteilte Verantwortung!

Auftragsverarbeiter

Auftragsverarbeiter: Mailchimp, Microsoft Office 365, Webhoster, DropBox, Cloud Datensicherung

Verantwortlicher: Banken, Steuerberater, Versanddienstleister sind „Verantwortlich im Sinne der DSGVO“

Regelungen im Auftrag / Vertrag sind zur Unterscheidung wichtig.

Der Verantwortliche muss sich von Auftragsverarbeiter **schriftlich** zusichern lassen, dass dieser die DSGVO einhält

Es muss dokumentiert werden, welche Daten zu welchem Zweck an den Auftragsverarbeiter übermittelt werden.

Verhältnismäßigkeit

Die DSGVO beachtet

Verhältnismäßigkeit!

Perfekter Schutz wird NICHT gefordert

Gefordert sind nur Maßnahmen die in Hinsicht auf

- Kosten und Aufwand der Unternehmensgröße
- dem Risiko

angemessen sind

Sensible Informationen

Besonders schützenswert sind „Daten besonderer Kategorien“:

- Daten von Kindern (bis 14 Jahre)
- Sensible Daten:
  - Ethnische Herkunft
  - Politische Meinungen
  - Religiöse o. weltanschauliche Überzeugungen
  - Gewerkschaftszugehörigkeit
  - Genetische oder biometrische Daten
  - Gesundheitsdaten
  - Sexualleben oder sexuelle Orientierung

Die DSGVO Grundsätze

Rechtmäßig und Transparent

– Daten müssen rechtmäßig beschafft werden.
– Bei Kauf von Daten: Verkäufer muss die Einstimmung zur Nutzung der Daten für den geplanten Zweck bereits eingeholt haben.
– Betroffene Personen können Auskunft über die gespeicherten Daten verlangen

Die DSGVO-Grundsätze

tethisIT
Kluge IT für Unternehmer

Rechtsgrundlagen für die Verarbeitung von nicht-sensiblen Daten:

Lt. DSGVO	Bedingung
Art 6 Abs 1 lit a	Mit Einwilligung des Betroffenen
Art 6 Abs 1 lit b	Zur Erfüllung eines Vertrages
Art 6 Abs 1 lit c	Aufgrund rechtlicher Vorschriften
Art 6 Abs 1 lit d	Aus lebenswichtigen Interessen
Art 6 Abs 1 lit e	Bei öffentlichem Interesse
Art 6 Abs 1 lit f	Bei berechtigten Interessen des Verantwortlichen, sofern Rechte des Betroffenen nicht überwiegen (nicht bei Kindern)
Art 9 Abs 2 lit e	Daten wurden vom Betroffenen veröffentlicht

Die DSGVO-Grundsätze

tethisIT
Kluge IT für Unternehmer

Rechtsgrundlagen für sensible Daten:

Lt. DSGVO	Bedingung
Art 9 Abs 2 lit a	Mit Einwilligung des Betroffenen
Art 9 Abs 2 lit b	Aufgrund Arbeits-/Sozialrecht, Kollektivvertrag, Betriebsvereinbarung
Art 9 Abs 2 lit c	Aus lebenswichtigen Interessen
Art 9 Abs 2 lit e	Daten wurden vom Betroffenen veröffentlicht
Art 9 Abs 2 lit f	Zur Geltendmachung von Rechtsansprüchen
Art 9 Abs 2 lit h	Für Zwecke der Gesundheitsvorsorge / medizinischen Behandlung
Art 9 Abs 2 lit g,i,j	Bei erheblichem öffentlichem Interesse (Gesundh., wissensch., histor.)

Die DSGVO Grundsätze

Nur mit Zweckbindung

– Bei der Zustimmung muss der Zweck der Datenverarbeitung genannt werden.
– Verarbeitung zu anderen Zwecken erfordert separate Zustimmung

Beispiel: Nur weil jemand ein Kunde ist, darf ich ihm/ihr noch keinen Newsletter schicken.

Die DSGVO Grundsätze

So wenig wie möglich

– Es dürfen nur die Daten gesammelt und verarbeitet werden, die für diesen Zweck nötig sind.

Beispiel: Bei der Newsletter-Anmeldung sollten keine Telefonnummer abgefragt werden, Namen nur als optionale Angabe.

Die DSGVO Grundsätze

Nur so lange wie nötig

– Daten dürfen nur für eine bestimmte Dauer gespeichert werden, z.B. „solange Kundenbeziehung besteht + Aufbewahrungsdauer“ oder „bis zur Kündigung des Newsletters“
– Im Zweifel haben die gesetzlichen Aufbewahrungsfristen Vorrang
– Nach Ablauf dieser Frist müssen die Daten gelöscht werden
– Ob Löschung aus Datensicherungen angemessen ist, ist noch nicht geklärt
– Betroffene Person kann Löschung der Daten verlangen.
– Löschung ist zu dokumentieren

Die DSGVO Grundsätze

Korrekt und sicher (Privacy by Design & Privacy by default)

Integrität und Vertraulichkeit muss sichergestellt sein

– Die Daten müssen gegen versehentlichen Verlust oder Beschädigung geschützt werden
  => Datensicherung ist Pflicht

– Die Daten müssen vertraulich bleiben
  => Zugangsschutz
  => Verschlüsselung
  => Pseudonymisierung

– Zugriff auf die Daten nur wenn nötig / im Auftrag
  => Vertragliche Vereinbarung mit Mitarbeitern

Rechte des Betroffenen

Recht auf Information

Der Betroffene hat das Recht über folgende Punkte informiert werden:

– Welche Daten werden zu welchem Zweck verarbeitet
– Quelle der Daten (falls nicht direkt vom Betroffenen, z.B. Telefonbuch)
– Die rechtliche Grundlage der Verarbeitung
– Dauer der Aufbewahrung und Kriterien für Löschung
– Weitergabe der Daten (ins Ausland?)
– Die Betroffenenrechte

Rechte des Betroffenen

Recht auf Auskunft

- Betroffene Personen haben das Recht auf Auskunft in klarer einfacher Sprache
- Ergebnisse eigener Arbeit und geistiges Eigentum müssen nicht herausgegeben werden.
- Alle Kontaktdaten, E-Mails, CRM Daten sind herauszugeben
- Die Auskunft muss kostenlos sein, zumindest solange die Auskunftspflicht nicht missbraucht wird.

Rechte des Betroffenen

Recht auf Berichtigung, Löschung und Einschränkung

- Der Betroffene hat das Recht die gespeicherten Daten zu korrigieren.
- Er kann fordern, dass die Daten gelöscht werden.
  Ausnahme: Die Daten müssen aus gesetzlichen oder vertraglichen Gründen gespeichert werden.
- Die Verwendung der Daten kann auf bestimmte Zwecke eingeschränkt werden.

Rechte des Betroffenen

Recht auf Datenübertragung

– Der Betroffene kann die Übergabe von gespeicherten Daten an ein anderes Unternehmen fordern
z.B. an einen anderen Webhoster oder Mailprovider, an einen anderen Arzt

Rechte des Betroffenen

Recht auf Widerspruch

– Ein einmal gegebenes Einverständnis zur Datenverarbeitung kann jederzeit widerrufen werden.

– Nach einem Widerspruch müssen die entsprechenden Daten gelöscht werden.

Rechte des Betroffenen

Umsetzungsfristen

– Für die Umsetzung dieser Rechte gilt eine Frist von 1 Monat
  Sie kann um 2 Monate verlängert werden

Ausnahmen

– Sollte es vertragliche oder gesetzliche Gründe, oder berechtigte Interessen geben, die die Interessen des Betroffenen überwiegen, müssen Daten nicht gelöscht bzw. ein Widerspruch nicht akzeptiert werden

Pflichten des Verantwortlichen

Umsetzung der Betroffenenrechte

– Die Rechte der Betroffenen müssen umgesetzt werden

Informationspflicht

– Die Informationspflichten sind zu erfüllen.
Spezielle Formvorschriften gibt es nicht, aber die Informationen müssen dem Betroffenen bei Beginn der Datenverarbeitung zugänglich sein
=> Eine Datenschutzerklärung ist notwendig

Pflichten des Verantwortlichen

Umsetzung von Maßnahmen zum Datenschutz

– Es sind technische und organisatorische Maßnahmen zum Schutz der Daten zu treffen
– Die getroffenen Maßnahmen sind zu dokumentieren und regelmäßig (in der Regel jährlich) zu überprüfen
– Auch die Prüfungen und resultierende Anpassungen sind zu dokumentieren.

Pflichten des Verantwortlichen

Privacy by Design

– Eingesetzte Technologien sollten bereits mit Blick auf den Datenschutz entwickelt oder ausgewählt werden

– Voreinstellungen sollten so gesetzt werden, dass sie dem Datenschutz gerecht werden

Beispiel:

– Bei der Auswahl von Cloud-Speicher sichere Anbieter wählen

– Outlook so konfigurieren, dass die komplette Adresse angezeigt wird

Pflichten des Verantwortlichen

Risikoanalyse & Datenschutzfolgeabschätzung

- Besteht durch die Verarbeitungen ein hohes Risiko für die Rechte und Freiheiten der Betroffenen?

- Die Einschätzung erfolgt anhand einer Liste mit nicht riskanten Verarbeitungen (DSB) oder eines Fragenkataloges (WKO)

- Besteht ein hohes Risiko, muss eine Datenschutzfolgeabschätzung erstellt werden:
  Risikoanalyse, Eintrittswahrscheinlichkeit, Abschätzung der Folgen, Gegenmaßnahmen

Pflichten des Verantwortlichen

Datenschutzfolgeabschätzung

1. Datenarten & Rechtsgrundlagen sammlen
2. Werden Datenschutz-Prinzipien eingehalten?
3. Verarbeitungsvorgänge beschreiben
4. Mögliche Risiken beschreiben
5. Mögliche Folgen des Eintritts analysieren
6. Bereits getroffene Schutzmaßnahmen auflisten
7. Soll-Ist-Vergleich anstellen
8. Zusätzlichen Maßnahmen planen

Pflichten des Verantwortlichen

Meldung von Datenschutzverletzungen

- Sollte eine Datenschutzverletzung auftreten, ist dies innerhalb von 72 Stunden der Aufsichtsbehörde zu melden, sofern ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht.
- Sollte ein hohes Risiko bestehen, ist auch die betroffene Person zu informieren.
- Eine Datenschutzverletzung wäre z.B. ein Hackerangriff, der Verlust eines Datenträgers, der Diebstahl eines Handys oder Laptops.

Pflichten des Verantwortlichen

Zusammenarbeit mit der Datenschutzbehörde

– Dokumentation muss zwecks Prüfung zur Verfügung gestellt werden

Ernennung eines Datenschutzbeauftragten

– Überwacht den Datenschutz und ist dabei nicht an die Anweisungen des Unternehmers gebunden. Mitarbeiter oder Externer.

– Nur für Firmen die sich primär mit der *Verarbeitung von sensiblen Daten* oder der *regelmäßigen und systematischen Überwachung* beschäftigen.

– Für kleinere Firmen eher nicht relevant.

Pflichten des Verantwortlichen

Dokumentationspflicht

– Die Datenverarbeitungsprozesse müssen dokumentiert werden
  => Es wird ein „Verfahrensverzeichnis“ geführt

– Unternehmen unter 250 Mitarbeitern müssen das nur, wenn
  – Daten nicht nur gelegentlich verarbeitet werden
  – sensible Daten verarbeitet werden
  – ein Risiko für Rechte und Freiheiten besteht

=> In der Praxis ist jeder dazu verpflichtet

Was ist zu Dokumentieren?

Intern (Datenschutzbehörde kann Einsicht verlangen)

- Verfahrensverzeichnis (welche Daten werden wie verarbeitet?)
- Liste der technischen und organisatorischen Maßnahmen (TOMs)
- Auftragsverarbeiter-Verträge
- Risikoanalyse & Datenschutzfolgeabschätzung
- Entscheidung, dass (kein) Datenschutzbeauftragter ernannt wird
- Mitarbeitervereinbarungen
- Regelmäßige Überprüfung

Extern (Dokumente müssen veröffentlicht oder Kunden zur Verfügung gestellt werden)

- Datenschutzerklärung
- Einwilligungserklärungen

Datenverarbeitung im Ausland

Verarbeitung außerhalb der EU nur möglich…

- Wenn ein „Angemessenheits-Beschluss“ der EU Kommission vorliegt
  Norway, Liechtenstein, Iceland, Andorra, Argentina, Canada, Faroer Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay, Großbritannien
- USA wenn Anbieter Mitglied im Data Privacy Framework ist
  - Kann auf https://www.dataprivacyframework.gov/s/participant-search geprüft werden
- Wenn die EU Standard-Vertragsklauseln vereinbart werden (im Auftragsverarb.-Vertrag)
- Wenn geeignete Garantien vorliegen (ISO Zertifizierung)
- Wenn ein Grund für eine Ausnahme vorliegt
  - Ausdrückliche Einwilligung
  - Erfüllung eines Vertrages
  - Geltendmachung von Rechtsansprüchen
  - Lebenswichtige Interessen des Betroffenen
  - Öffentliches Interesse

Zusammenfassung

Rechtskonforme Datenverarbeitung bedeutet (stark vereinfacht):

- Nur mit gültiger Rechtsgrundlage
- Nur so wenig wie möglich, so lang wie nötig speichern
- Schutz der Daten vor Verlust, Änderung, Diebstahl
- Verträge mit Auftragsverarbeitern
- Dokumentation und jährliche Prüfung
- Anliegen von Betroffenen nachkommen
- Meldung von Datenschutzverletzungen
- Information der Betroffenen durch Datenschutzerklärung

Umsetzung - Vorgehensweise

1. Verfahrensverzeichnis erstellen
2. Technische & organisatorische Maßnahmen auflisten
3. Verbesserungsbedarf identifizieren
4. Risikoabschätzung
5. Datenschutzerklärung erstellen
6. Einwilligungserklärungen formulieren
7. Auftragsverarbeiter-Verträge einsammeln
8. Weisungen an Mitarbeiter, etc.
9. Regelmäßige Prüfung / Verbesserung

Verfahrensverzeichnis

- Name des Verantwortlichen
- Name und Zweck der Verarbeitung
- Kategorien der verarbeiteten Daten
- Kategorien der betroffenen Personen
- Kategorien der Empfänger
- Übermittlung an Drittländer?
- Fristen für Löschung (wenn möglich)
- Allg. Beschreibung der TOMs (wenn möglich)
- Rechtsgrundlage (nicht von der DSGVO gefordert)
- Auftragsverarbeiter (nicht von der DSGVO gefordert)

Verfahrensverzeichnis

Wie kommt man an die Liste der Verarbeitungen?

- Den Arbeitstag verdeutlichen
- Teams und verwendete Tools auflisten
- Vorlagen und Beispiele (z.B. wko, Deutschland)
- Tools, die bei der Dokumentation unterstützen (z.B. Audatis)

Die DSGVO schreibt keine Granularität vor

=> Grob anfangen und später besser werden

Verfahrensverzeichnis

tethisIT
Kluge IT für Unternehmer

Zweck und Bezeichnung der Verarbeitung	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten	Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden	Ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation	Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO	Rechts-grundlage der Daten-verarbeitung	Auftrags-verarbeiter
Finanz-buchhaltung	Namen, Anschrift, Bank-verbindungen, Umsatzsteuer-Identifikationsnummer von Debitoren und Kreditoren	Weitergabe – soweit gesetzlich erforderlich – an die Finanz-verwaltung weitergegeben. Eine Weitergabe der Daten erfolgt auch an Steuerberater und Wirtschafts-prüfer.	Keine.	Buchhaltungsdaten werden für eine Dauer von 7 Jahren aufbewahrt. Nach Ablauf dieser gesetzlichen Aufbewahrungspflicht werden die Daten gelöscht.	Siehe Beschreibung der Technischen & organisatorischen Maßnahmen	DSGVO Art 6 Abs 1 lit a (Einwilligung) DSGVO Art 6 Abs 1 lit b (Vertragserfüllung)	FastBill GmbH, Deutschland

Verfahrensverzeichnis

Zwecke der Verarbeitung	Betrieb einer Webseite zum Marketingzwecken und statistische Analyse der Nutzung
Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten	- IP Adressen (Google Analytics: nur anonymisierte IP Adressen) - Bei Nutzung des Kontaktformulars: Name, E-Mail-Adresse, Tel.Nr., IP Adresse - Cookies - Betroffene Personen: Besucher der Webseite
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden	- Webhoster - Dienstleister für Nutzungsanalyse (Google Analytics) - Facebook (Facebook Pixel ohne erweiterten Abgleich)
Ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation	Dienstleister für Nutzungsanalyse in den USA (Google Analytics und Facebook, beide Mitglied des Privacy Shield)
Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien	- IP Adressen beim Webhoster werden nach 3 Monaten gelöscht - Google Analytics Daten werden nach einem Jahr gelöscht
Allgemeine Beschreibung der TOMs	Siehe separate Dokumentation der technischen und organisatorischen Maßnahmen (TOM)
Rechtsgrundlage der Datenverarbeitung	Art 6 Abs 1 lit f DSGVO (berechtigte Interessen)
Auftragsverarbeiter	tethis IT (Webhosting) Mailchimp Facebook

Verfahrensverzeichnis

Los geht‘s:

Wir erstellen ein beispielhaftes Verfahrensverzeichnis

Im Handout folgt jetzt die Dokumentation der TOMs

Wird jetzt übersprungen, weil wir uns morgen auf die technischen Schutzmaßnahmen konzentrieren!

Risikoeinschätzung

- DSB liefert Liste mit Verarbeitungen die keine Folgeabschätzung erfordern: https://www.dsb.gv.at/verordnungen-in-osterreich (Datenschutz-Folgenabschätzung-Ausnahmenverordnung und dazugehörige Erläuterungen)
- Sind die eigenen Verarbeitungen enthalten? Dann kein hohes Risiko, keine Folgeabschätzung nötig
- Falls nicht, übrige Verarbeitungen anhand der Checkliste der WKO prüfen
- Sollte sich ein hohes Risiko ergeben, Datenschutzfolgeabschätzung erstellen. Hinweise dazu bei der WKO: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Ablaufplan-Datenschutz-Fo.html

Normalerweise ist für ein EPU KEINE Folgeabschätzung nötig!

Risikoeinschätzung (Liste der DSB)

- Bild- und Akustikdatenverarbeitung in Echtzeit
- Bild- und Akustikverarbeitungen zu Dokumentationszwecken
- Patienten-/Klienten-/Kundenverwaltung und Honorarabrechnung einzelner Ärzte, Gesundheitsdienstanbieter und Apotheken
- Rechts- und Beratungsberufe
- Archivierung, wissenschaftliche Forschung und Statistik
- Unterstützungsbekundungen
- Aktenverwaltung (Büroautomation) und Verfahrensführung
- Organisation von Veranstaltungen
- Preise und Ehrungen
- Kundenverwaltung, Rechnungswesen, Logistik, Buchführung
- Personalverwaltung
- Mitgliederverwaltung
- Kundenbetreuung und Marketing für eigene Zwecke
- Sach- und Inventarverwaltung
- Register, Evidenzen, Bücher
- Zugriffsverwaltung für EDV-Systeme
- Zutrittskontrollsysteme
- Stationäre Bildverarbeitung und die damit verbundene Akustikverarbeitung zu Überwachungszwecken (Videoüberwachung)

Risikoeinschätzung (Kriterien der WKO)

tethisIT
Kluge IT für Unternehmer

- Wird bewertet?
- Automatisierte Entscheidungsfindung?
- Systematische Überwachung?
- Vertrauliche oder höchst persönliche Daten?
- Datenverarbeitung in großem Umfang?
- Daten von Kindern, Patienten, Senioren, Arbeitnehmer, …?
- Neue Technologien (z.B. Biometrie)
- Wird ein Recht oder Vertrag verhindert?

Treffen zwei Kriterien zu, besteht wahrscheinlich ein hohes Risiko

Risikoeinschätzung

- Einschätzung anhand der Ausnahmenliste der DSBO oder WKO Fragenliste
- Falls hohes Risiko => Datenschutzfolgeabschätzung

- Einschätzung ob Datenschutzbeauftragter nötig ist (siehe oben)

- Ergebnis Dokumentieren

Im Handout folgt jetzt Datenschutzerklärung.

Wird jetzt übersprungen, die Diskussion erst nach dem Thema Webseite Sinn macht

Auftragsverarbeiter Verträge

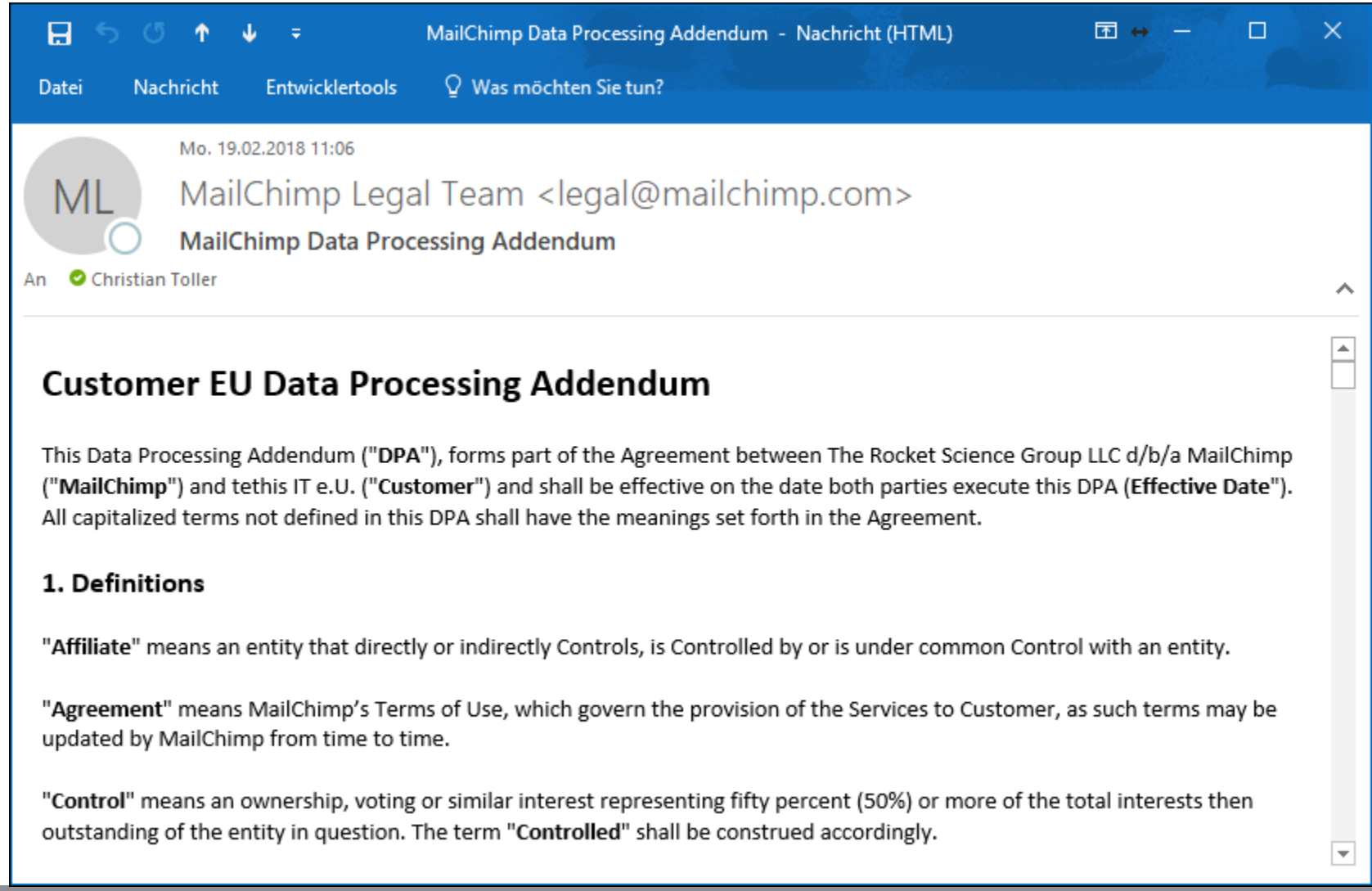
Ein Vertrag mit einem Auftragsverarbeiter muss folgende Punkte enthalten:

- Bindung an den Verantwortlichen
- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der verarbeiteten Daten
- Kategorien der betroffenen Personen (sensible Daten?)
- Rechte und Pflichten des Verantwortlichen

Auftragsverarbeiter Verträge

Einfach danach fragen!

Falls nicht vorhanden, Vorlage der wko ausfertigen lassen.



Auftragsverarbeiter Verträge

Sehr gute Liste:

https://www.blogmojo.de/av-vertraege/

https://av-vertrag.org/

Einwilligungserklärungen

Laut Gesetz ist eine Einwilligung..

„… jede freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung durch die betroffene Person in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.“

Einwilligungserklärungen

Eine korrekt Einwilligungserklärung muss

- keiner bestimmten Form folgen
- dokumentierbar sein (also eher schriftlich, elektronisch)
- Freiwillig erfolgen (keine Abhängigkeiten)
- Für einen bestimmten Fall erfolgen (Zweck nennen)
- In informierter Weise erfolgen (nicht verstecken, klare Sprache)

Vorausgefüllte Erklärungen (gesetzter Haken) sind nicht zulässig.

„Kopplungsverbot“ beachten!

Einwilligungserklärungen

Freiwilligkeit ist insbesondere dann zweifelhaft:

- wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert Einwilligungserklärungen erteilt werden können, obwohl es im Einzelfall angebracht ist
- wenn die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung des Vertrages nicht erforderlich ist (Koppelungsverbot),
- wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht (z.B. wenn es sich bei dem Verantwortlichen um eine Behörde handelt).

Einwilligungserklärungen

tethisIT
Kluge IT für Unternehmer

- ✓ Ich möchte regelmäßig per E-Mail Informationen rund um die Humanenergetik und zu neuen Workshops erhalten. Bitte senden Sie mir Ihren Newsletter an folgende E-Mail-Adresse:

- ✓ Ich möchte Sitzungen per Skype durchführen und stimme der Übermittlung meines Namens und meiner E-Mail-Adresse an Skype sowie der Übertragung des Gespräches mittels Skype zu. Skype ist eine Dienstleistung der Microsoft Corp., USA. Die Daten werden in die USA übertragen.

Einwilligungserklärungen

✓ Cookie-PopUps auf Webseite (z.B.: post.at)

✓ Ich möchte per E-Mail kommunizieren und stimme der Übermittlung von persönlichen und/oder vertraulichen Daten per unverschlüsselter E-Mail zu. Mir ist bewusst, dass die Inhalte dieser E-Mails auf dem Übertragungsweg möglicherweise in Drittstaaten übertragen und von Dritten eingesehen werden können.

Einwilligungserklärungen

- ✓ Ich bin damit einverstanden, dass Bilder von Kurseinheiten an denen ich / mein Kind teilgenommen hat, in sozialen Medien oder auf unserer Webseite xyz.at veröffentlich werden.
- ✓ Ich bin damit einverstanden, dass Name, Alter, Anschrift, Tel.Nr. und E-Mail-Adresse meines Kindes zum Zwecke der Planung und Durchführung des Unterrichts verarbeitet werden. Die Daten werden nicht an Dritte weitergegeben
- ✓ Ich möchte zusätzlich per WhatsApp kommunizieren. Mir ist bekannt das dazu meine Telefonnummer an WhatsApp Ireland Limited übermittelt werden muss. Es gelten die Datenschutzbestimmungen von WhatsApp: https://www.whatsapp.com/legal/#privacy-policy

Weisung an die Mitarbeiter

Mitarbeiter vertraglich zur Einhaltung der DSGVO verpflichten:

- Daten nur auf Anweisung verwenden
- Geheimhaltung
- Keine unbefugte Beschaffung, Übermittlung o. Verarbeitung
- Gilt auch nach Ende des Arbeitsvertrages

Muster gibt es bei der WKO und in den Unterlagen

Regelmäßige Prüfung

Einmal jährlich muss geprüft werden:

- Ist das Verarbeitungsverzeichnis vollständig?
- Haben sich die Risiken verändert?
- Wurden die TOMs umgesetzt?
- Sind die TOMs noch angemessen?

Die jährliche Prüfung ist zu dokumentieren

TOMs

Fragebogen auf https://itsafe.wkoratgeber.at/, Ausfüllhilfe von Stephan Hansen-Oest

Sind Cloud-Dienste sicher?

tethisIT
Kluge IT für Unternehmer

1. Man vertraut die Daten einem fremden Firma an!
   Ist diese Firma vertrauenswürdig?
2. Unsere Pflicht: Sicherheit schriftlich zusichern lassen
3. Nur Anbieter aus sicheren Ländern
4. Reputation ist wichtig
5. Erhöhte Redundanz / Fehlertoleranz
6. Mehr Überwachung, mehr Know-How
7. Räumliche Trennung ist gegeben
8. Zum Teil Versionierung, verbesserte Teamarbeit

Das Thema WhatsApp

- Das Problem: WhatsApp verschickt bei der Installation das komplette Telefonbuch des Handys. D.h. Nutzung auf einem Handy mit Kunden-Tel. Nummern ist nicht legal.
- Dazu ist die Einwilligung aller Personen, die im Telefonbuch gespeichert sind, notwendig
- Keine Tel. Nr. speichern, Einwilligung einholen, Handy benutzen, das separate Telefonbücher erlaubt (z.B. Blackberry)
- Alternative Apps: Threema, Signal oder SMS
- Oder: Mit Hilfe einer Mobile-Device-Management Lösung den Zugriff von WhatsApp auf das geschäftliche Telefonbuch verhindern: https://www.miradore.com/de/ oder https://www.manageengine.com/mobile-device-management/

TOMs – Ziele lt. DSG 2018

1. Zugangskontrolle (Schlösser, Alarmanlage)
2. Datenträgerkontrolle (verschlüsselte USB Sticks und Handys)
3. Benutzerkontrolle (Berechtigungen, Rollen)
4. Zugriffskontrolle (Passwörter, Passwortregeln)
5. Übertragungskontrolle (Regeln für die Weitergabe von Daten)
6. Eingabekontrolle (Protokollierung von Zugriffen)
7. Transportkontrolle (HTTPS, verschlüsselte E-Mails)
8. Wiederherstellung (Datensicherung)
9. Datenintegrität (Virenschutz)

Passwörter sind Pflicht!

Passwörter auf allen Geräten!

Bildschirmschoner mit Passwort

Lieber lange Passwörter als komplexe

Wichtig: Für jede Anwendung ein eigenes Passwort!

Tipp: Immer der gleiche Anfang, am Schluss variieren

!mmerDasGle1chefacebook!

Passwortmanager sind eine große Hilfe:

Bitwarden (https://bitwarden.com), 1Password https://1password.com, keePass (https://keepass.info, LastPass (https://lastpass.eu/

Passwort-Diebstahl

Auf https://haveibeenpwned.com/ und https://sec.hpi.de/ilc/ prüfen, ob das eigene Passwort bekannt geworden ist

Falls ja, sind alle Dienste, bei denen man sich mit der betroffenen Kombination aus Benutzername & Passwort anmeldet, gefährdet.

⇒ Sofort Passwort ändern

⇒ Im Zweifel: Alle wichtigen Passwörter ändern!

2-Faktor Authentisierung

Benutzt mehrere „Faktoren“

Etwas das Du…

…kennst	…hast	…bist
Benutzername	Handy / Smartphone	Fingerabdruck
Passwort	Hardware-Token	Gesicht
E-Mail Adresse	Zugriff auf E-Mails	Netzhautscan

- Ist sicherer als nur ein Passwort.
- Login ist aufwendiger als nur ein Passwort
- Wenn möglich für alle kritischen Accounts verwenden

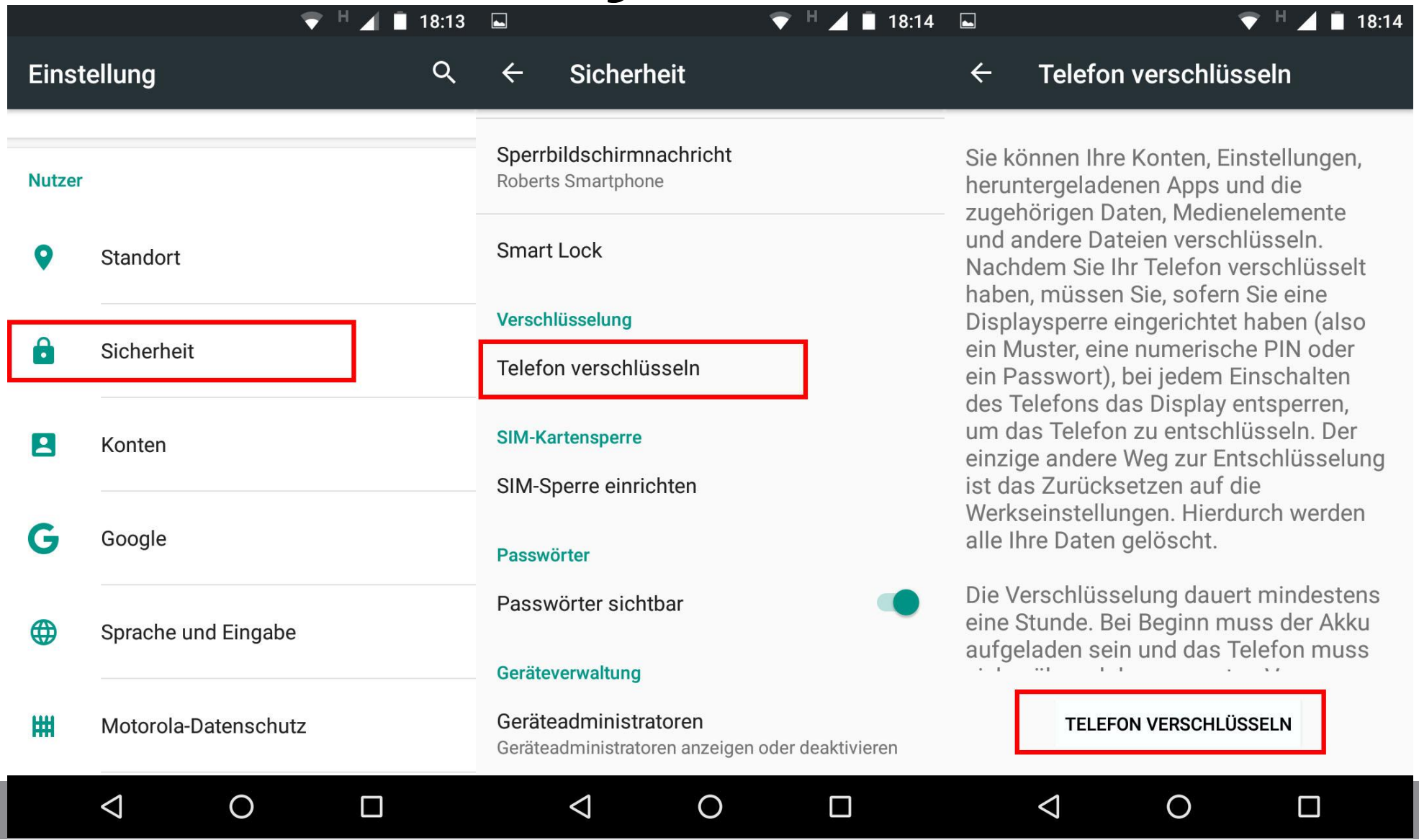
Geräte / Speicher verschlüsseln

Verhindert, dass Geräte unbefugt ausgelesen werden

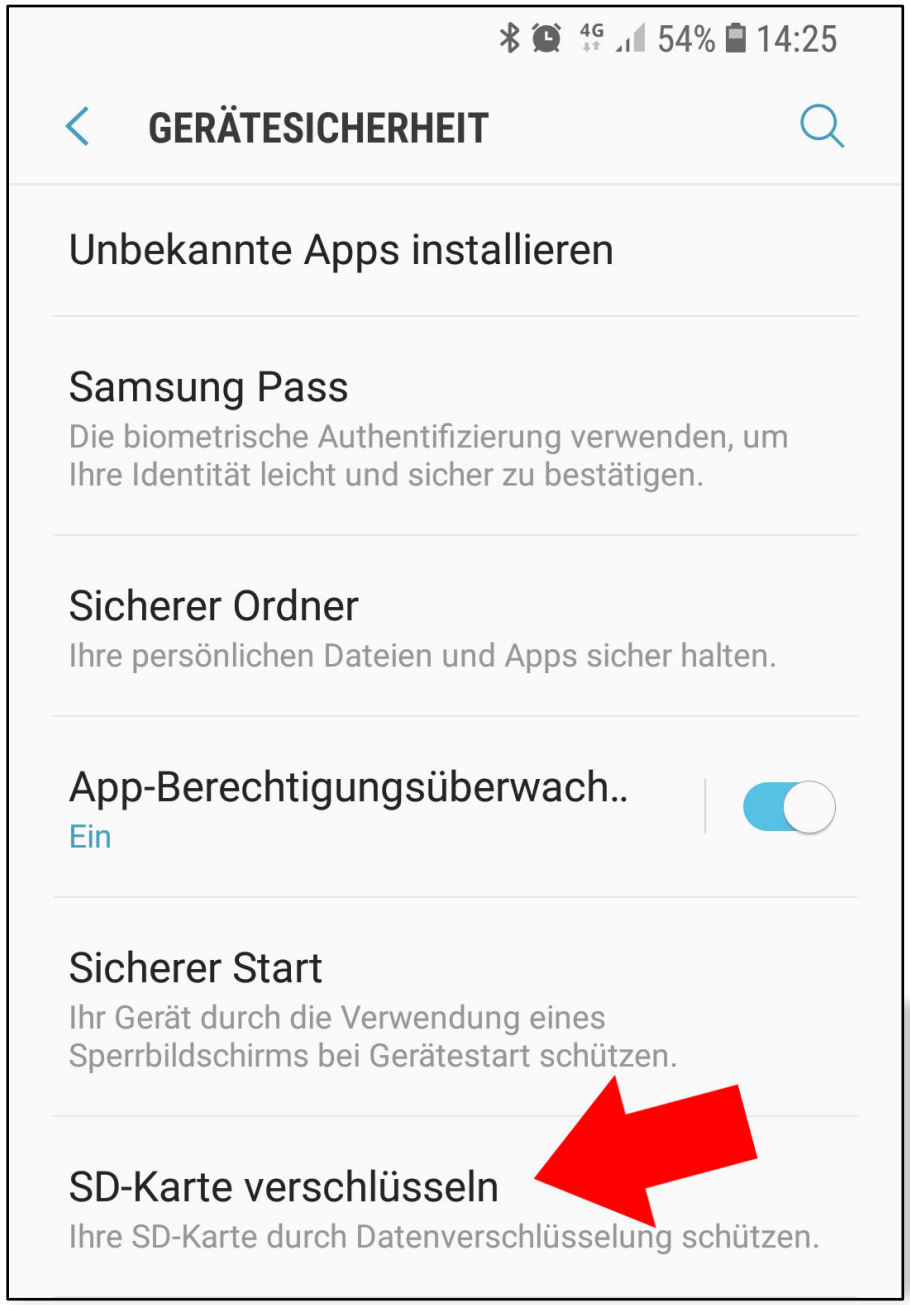
Schützt bei Diebstahl

	Handy	Computer und USB
Apple	per default eingeschaltet	Festplatten-dienstprogramm FileVault
Windows / Android	Einstellungen Sicherheit Verschlüsseln	Bitlocker (Win 10 Pro) Veracrypt

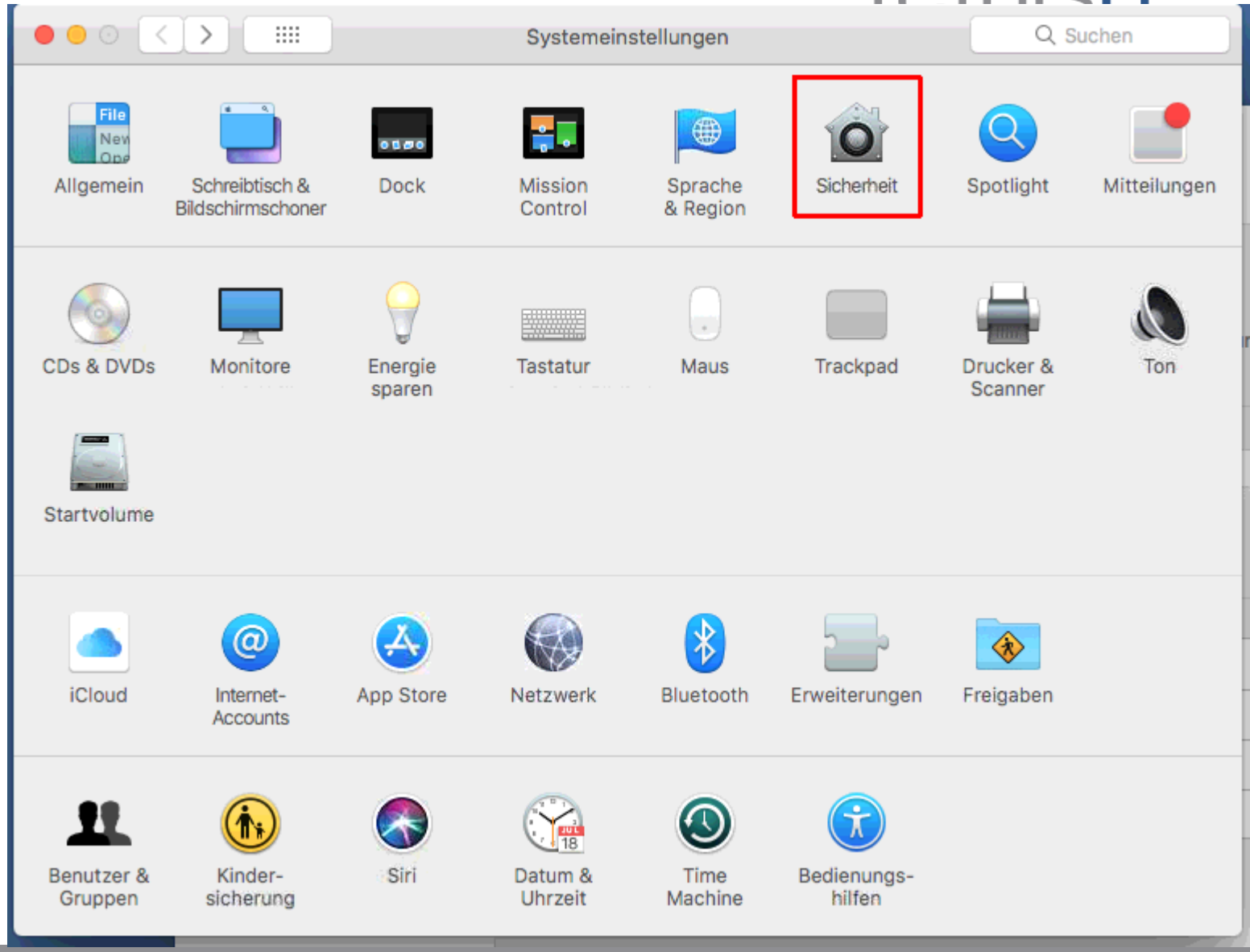
Android: Handy verschlüsseln



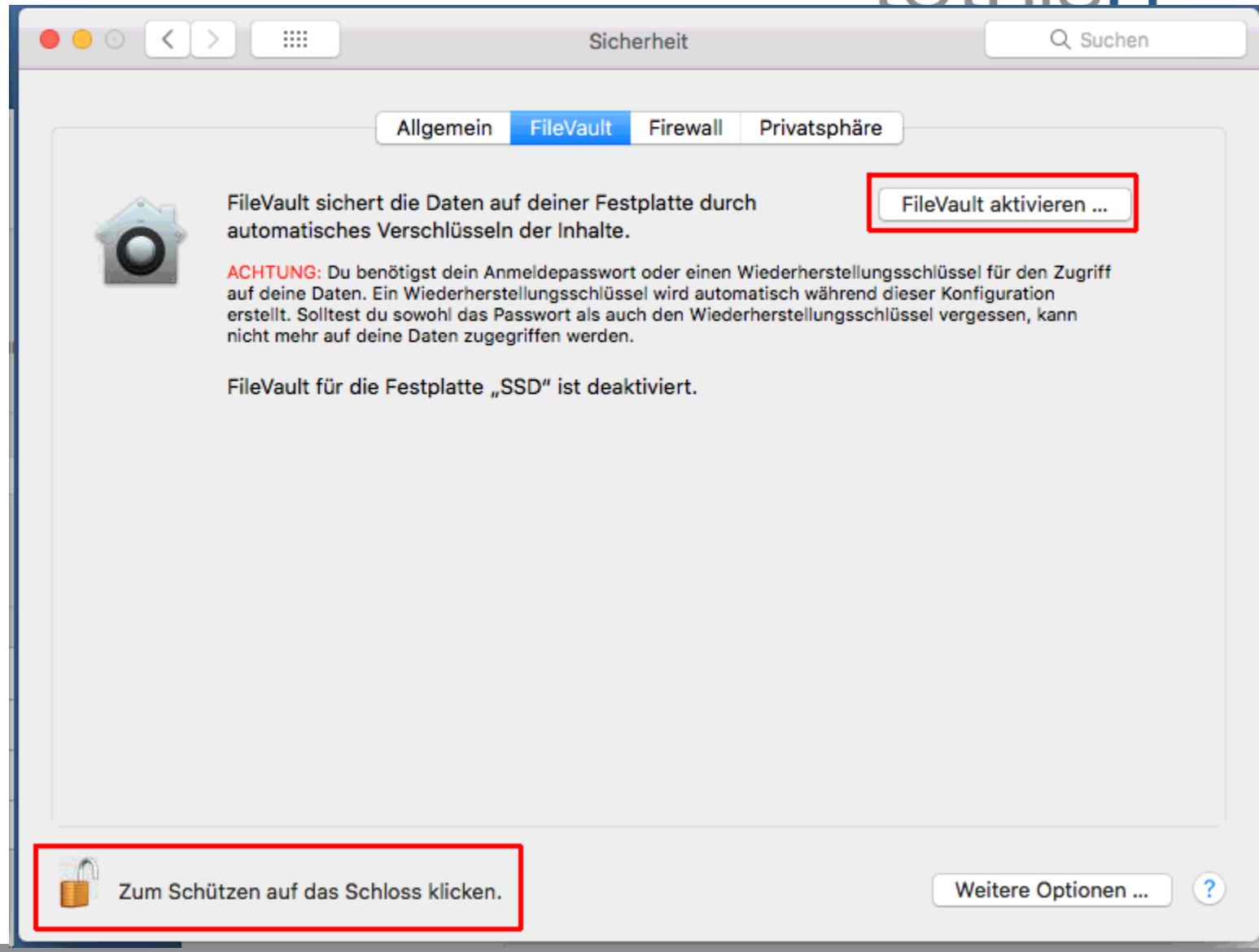
Android: SD Karte verschlüsseln

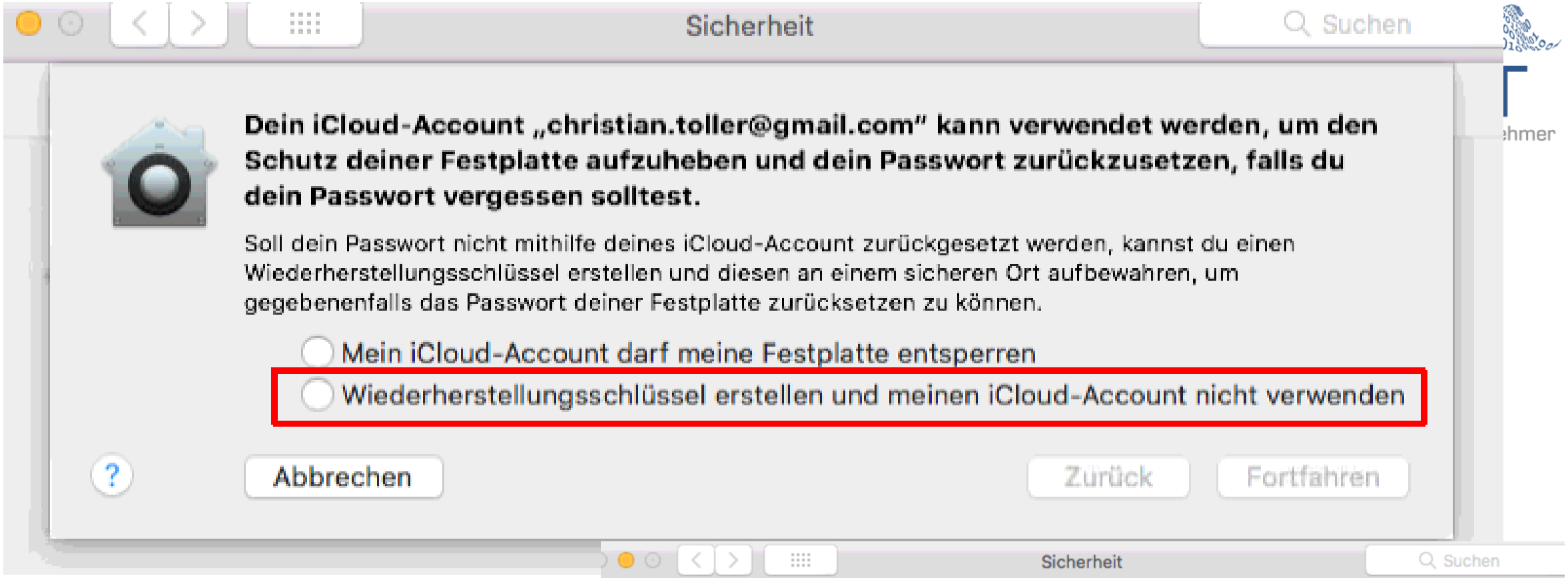


Mac: Festplatte(n) verschlüsseln

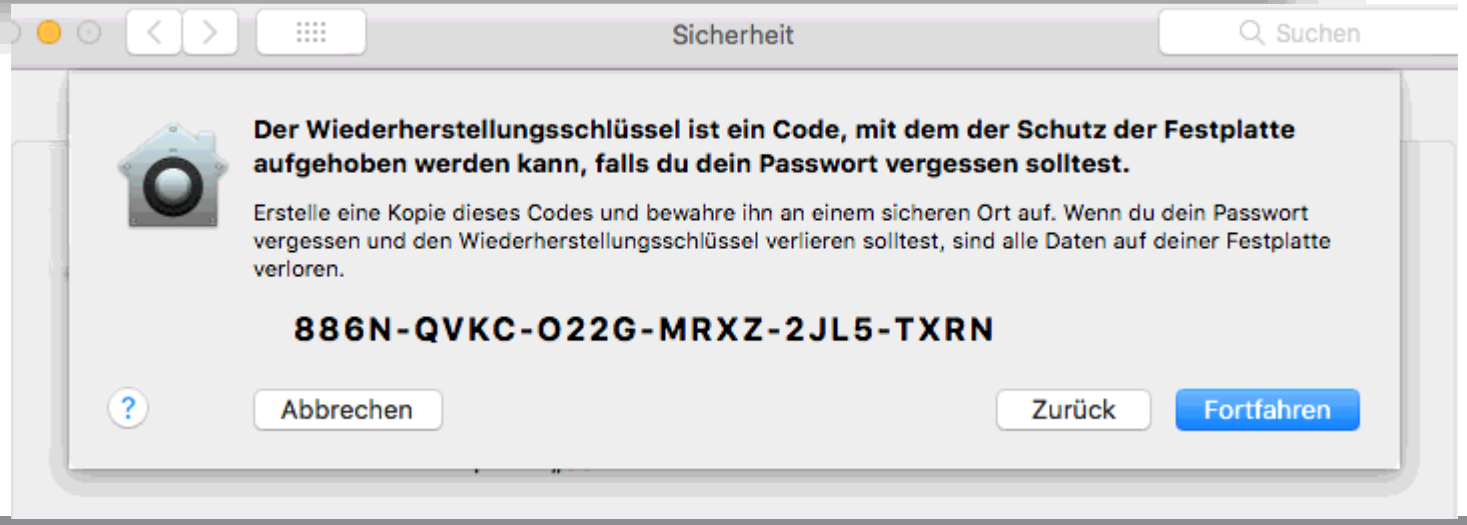


Mac: Festplatte(n) verschlüsseln



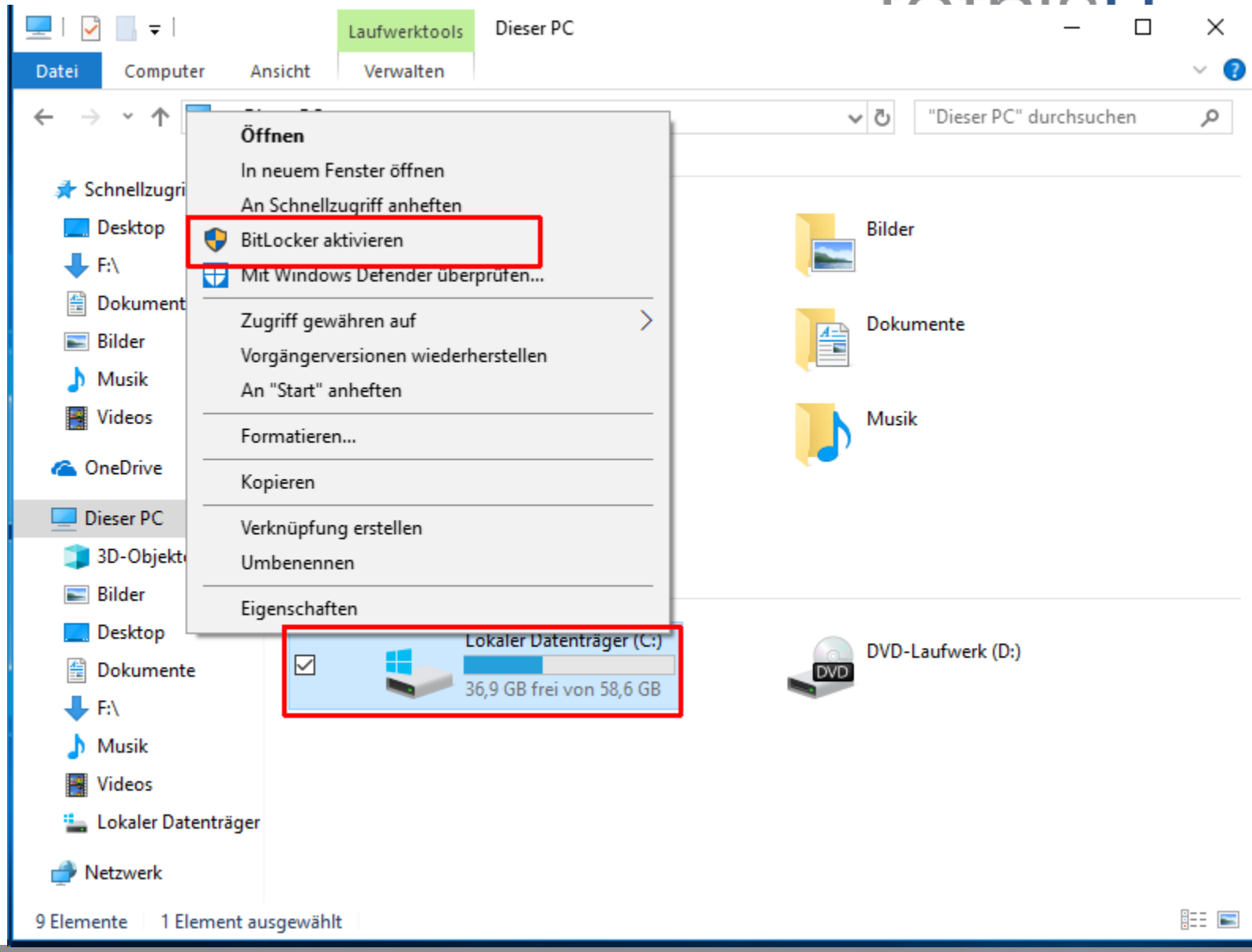


Mac: Festplatte(n) verschlüsseln



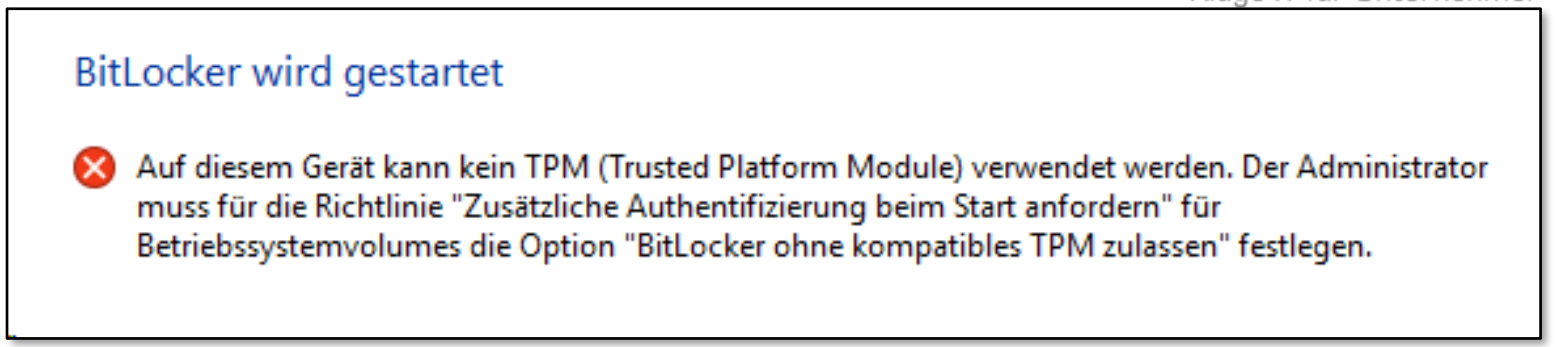
PC: Festplatte(n) verschlüsseln

erfordert Win10 Pro



PC: Festplatte(n) verschlüsseln

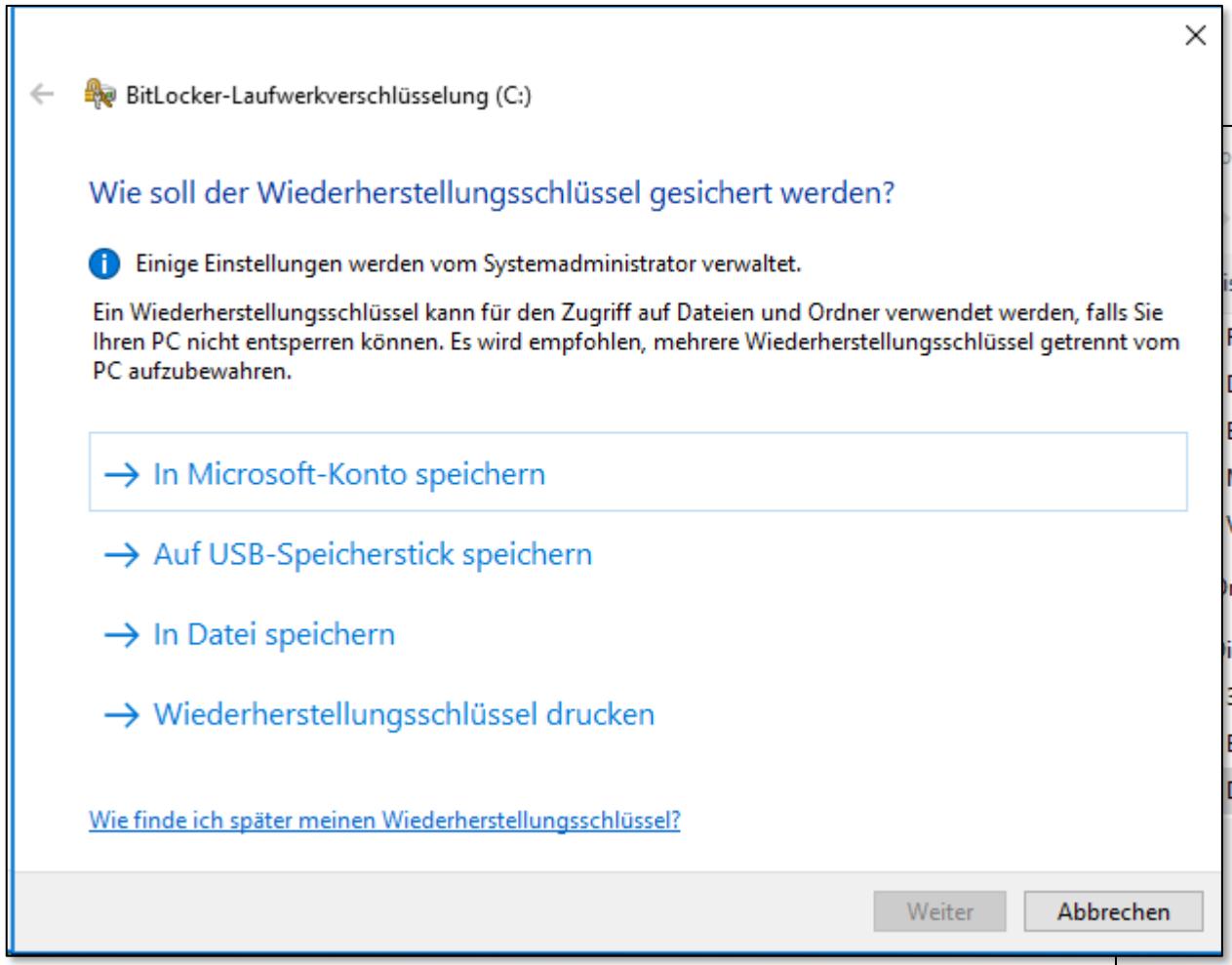
Fehler bei älteren Computern

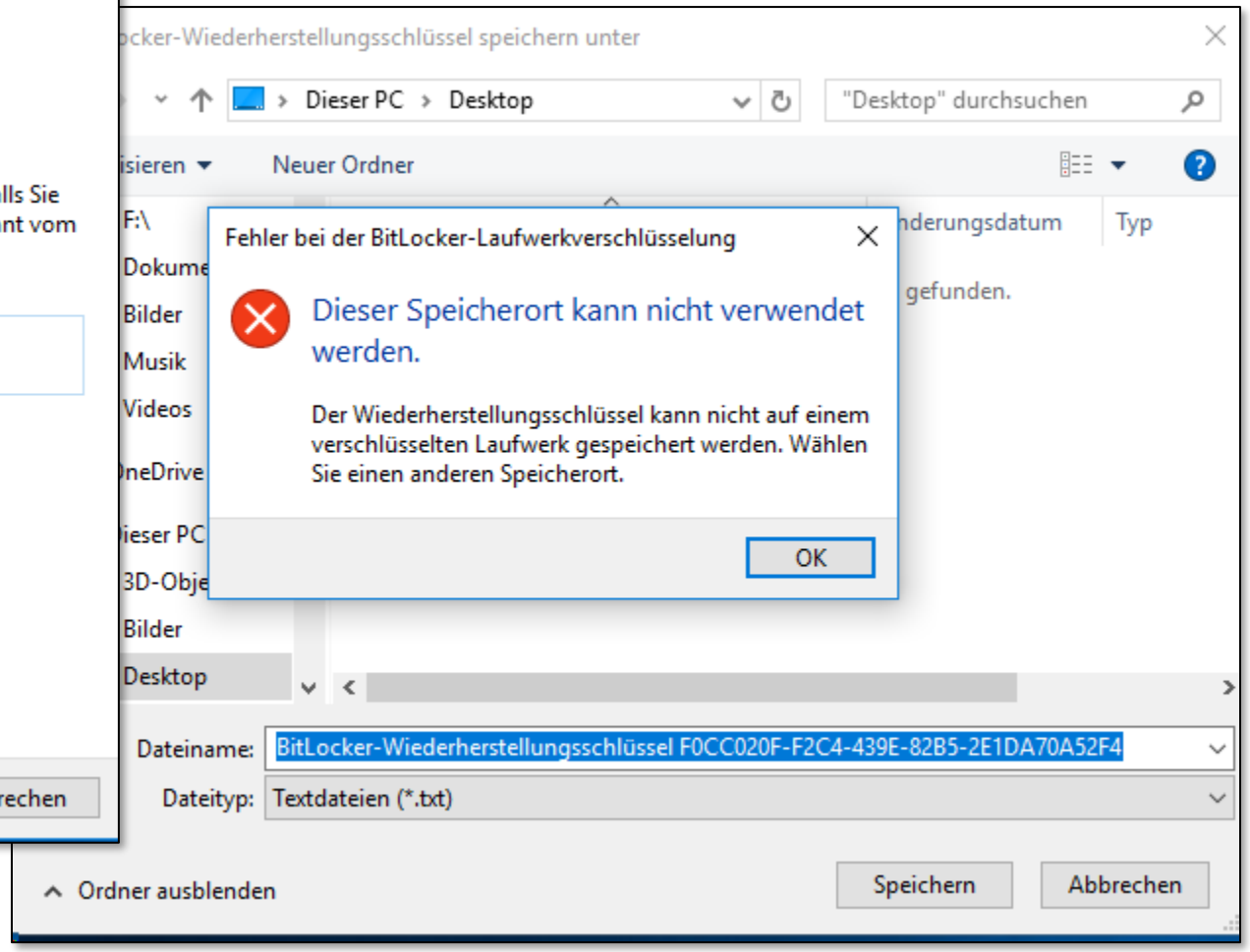


Windows + R drücken
gpedit.msc eingeben, RETURN
Der „Group Policy Editor“ öffnet sich
Links auswählen
Computerkonfiguration
Administrative Vorlagen
Windows Komponenten
Bitlocker-Laufwerksverschlüsselung
Betriebssystem-Laufwerke
Rechts „Zusätzliche Authentifizierung beim Starten anfordern“ doppelt anklicken
Aktivieren anklicken

PC: Festplatte verschlüsseln

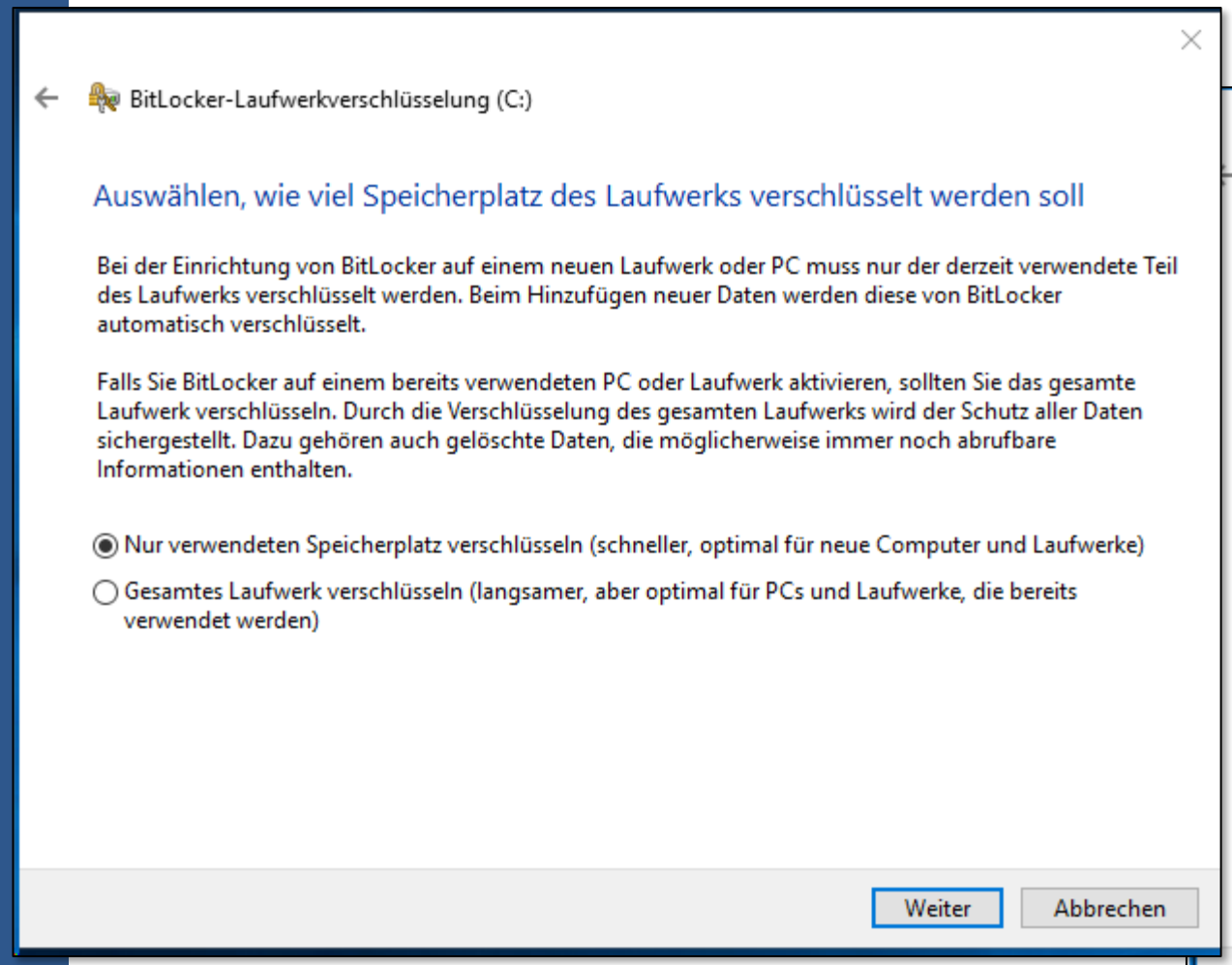
tethisIT
Kluge IT für Unternehmer

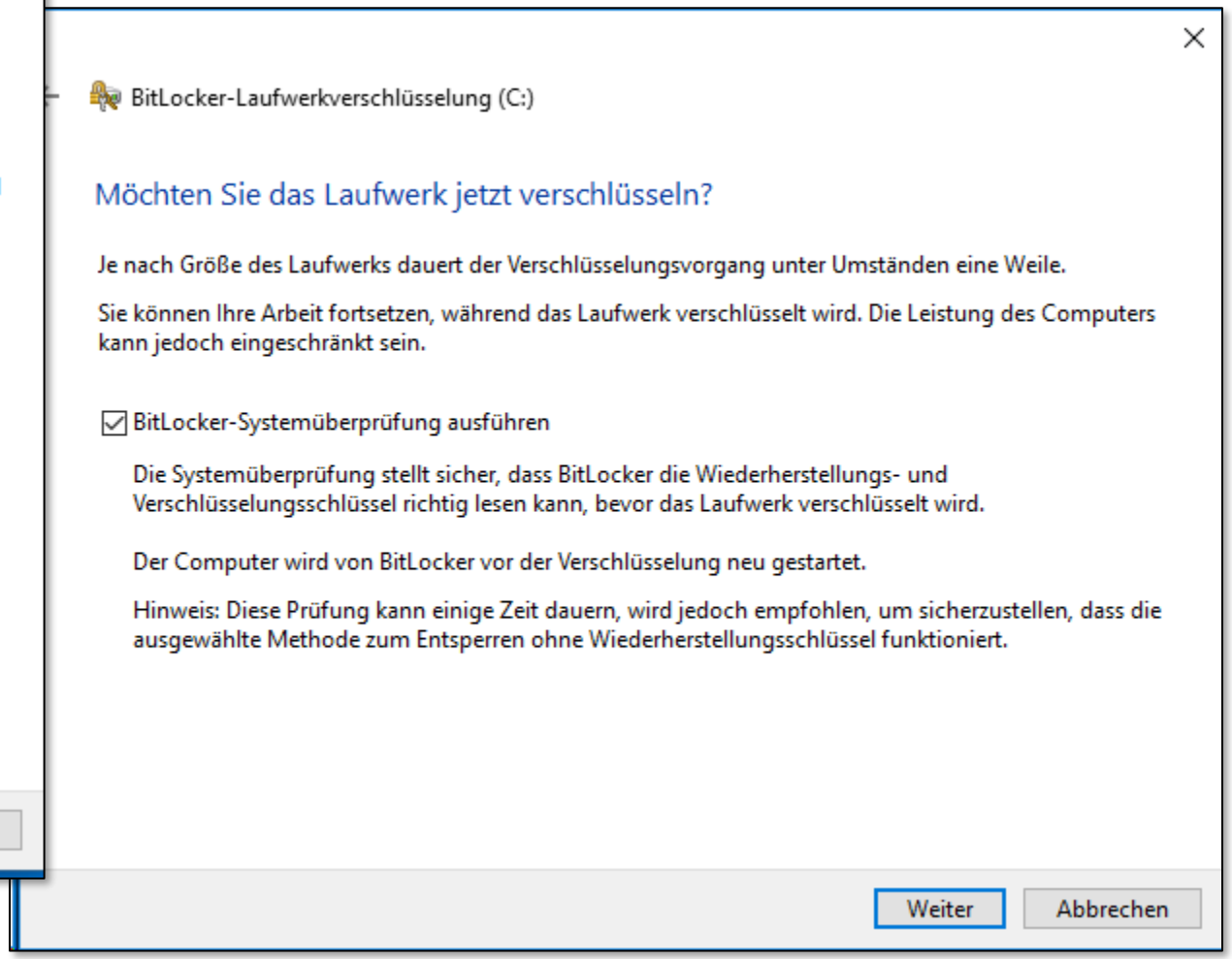




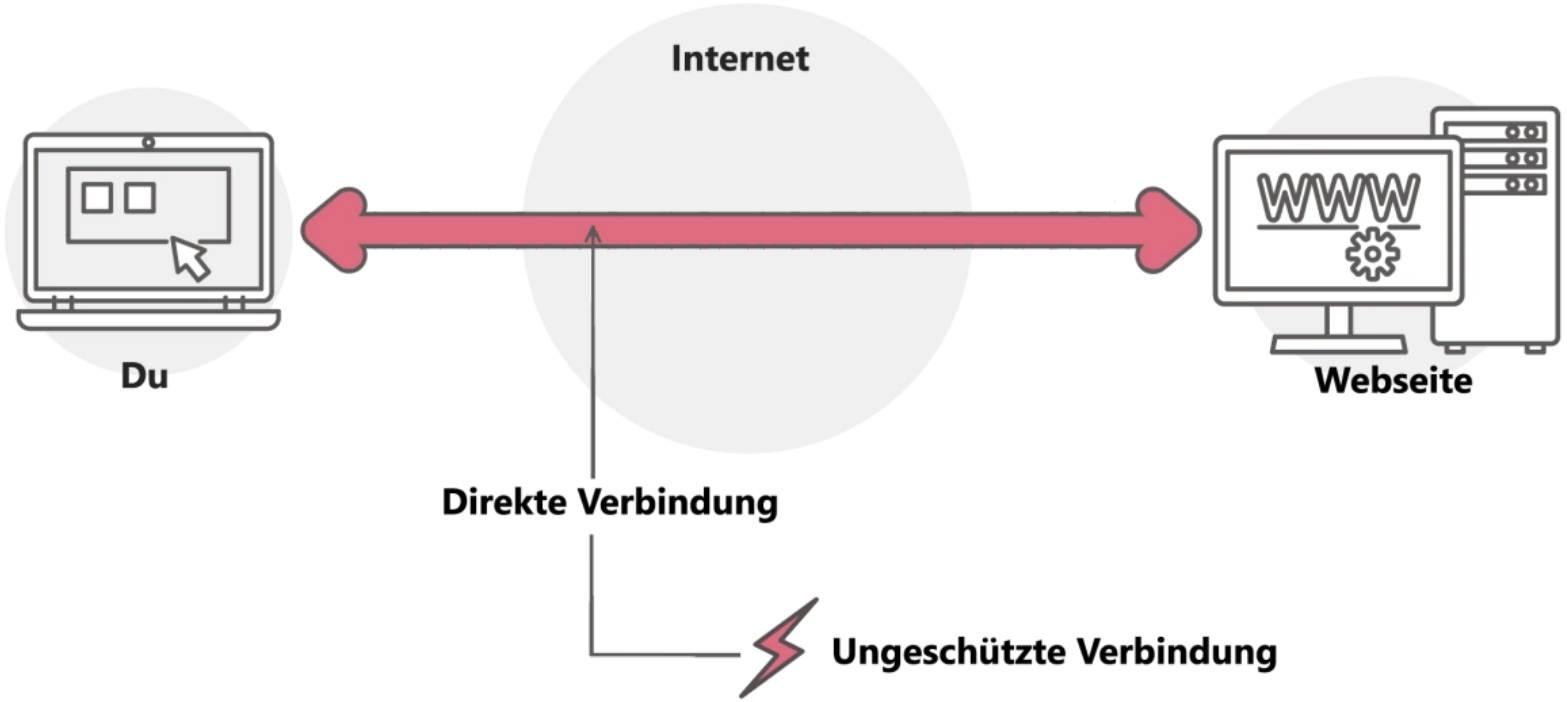
PC: Festplatte verschlüsseln

tethisIT
Kluge IT für Unternehmer



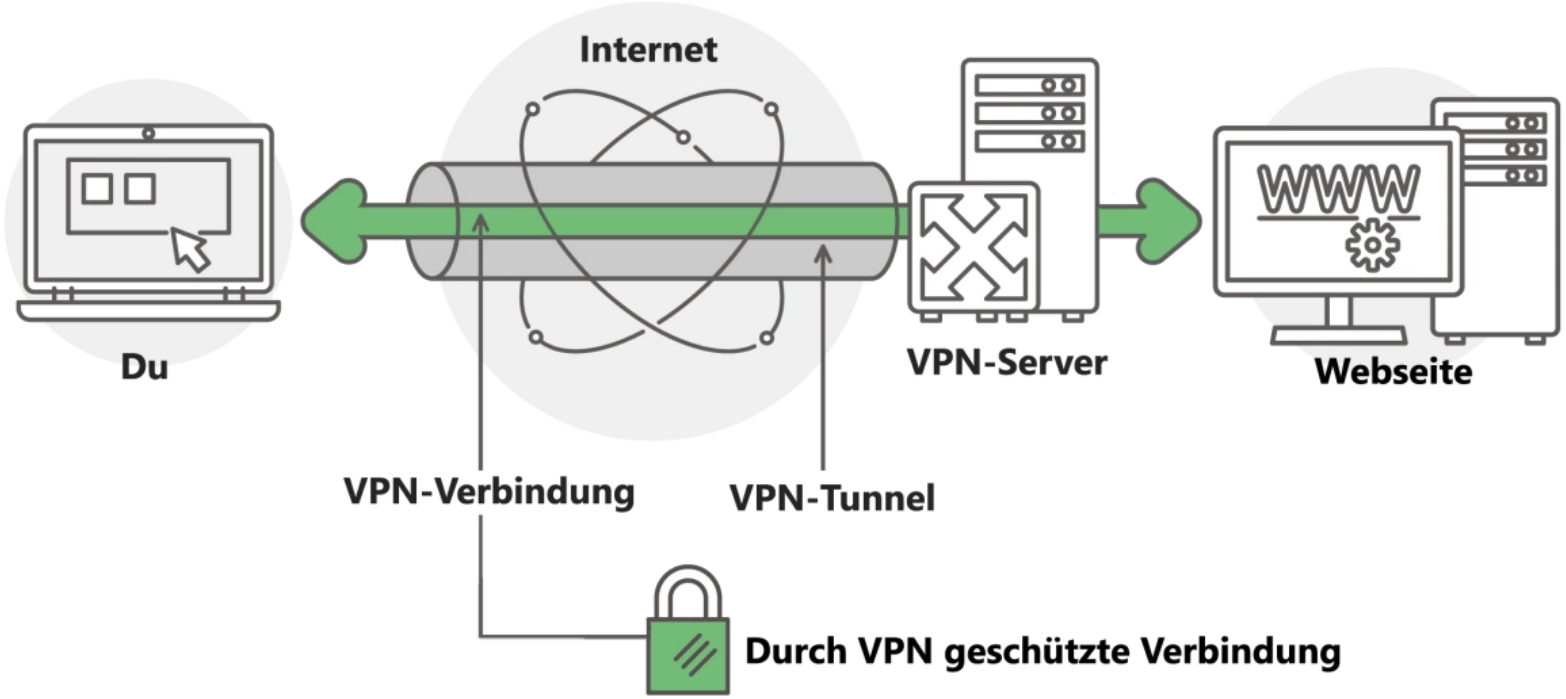


VPN - Normalzustand

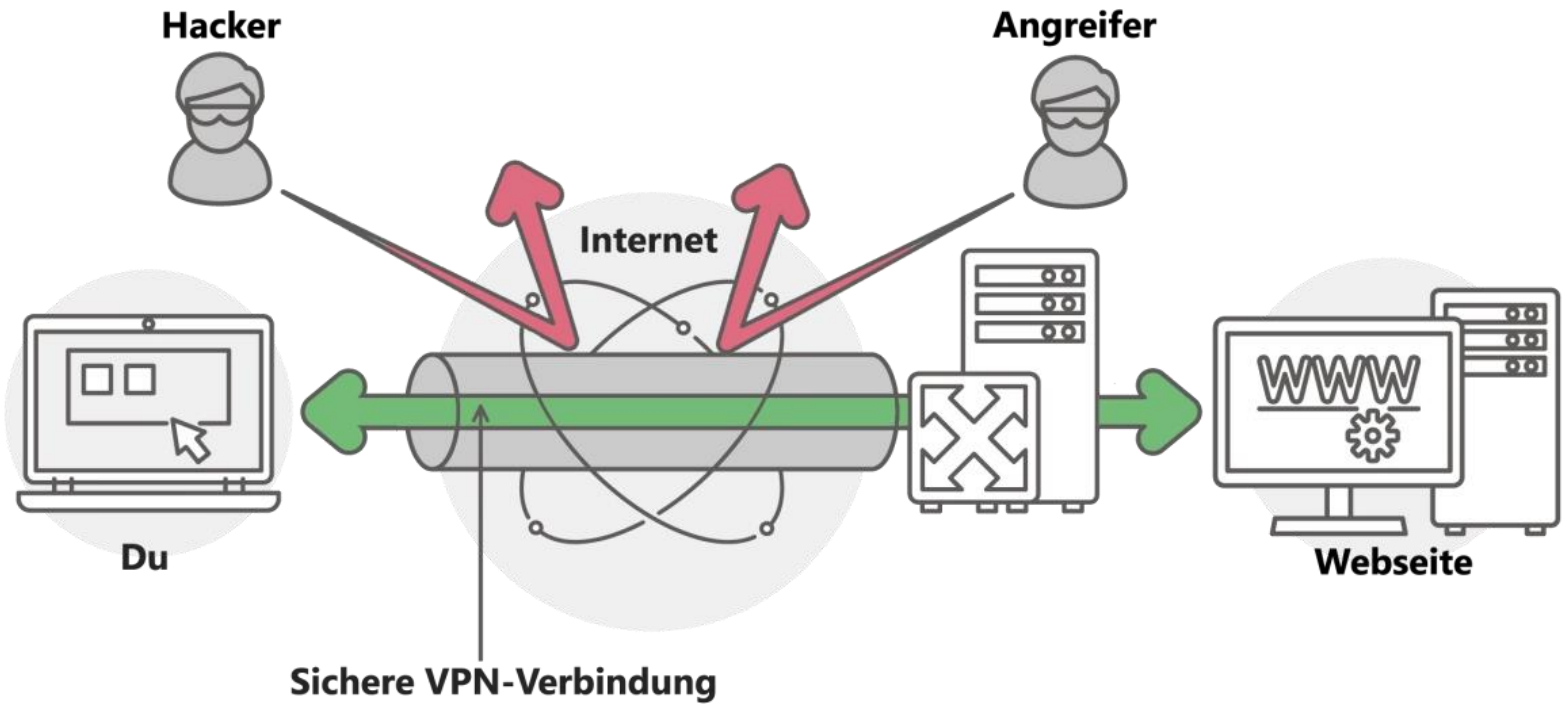


VPN – Mit VPN

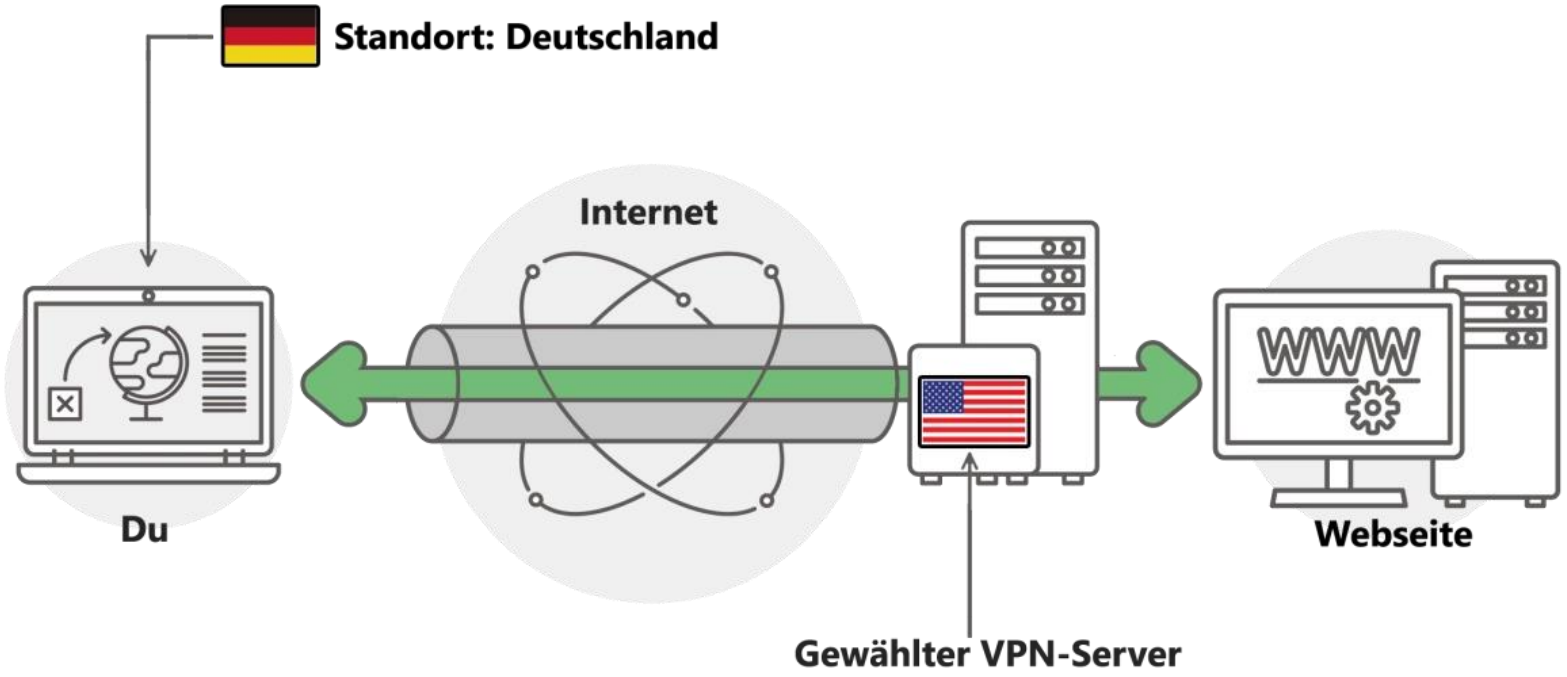
Mit Virtual Private Network



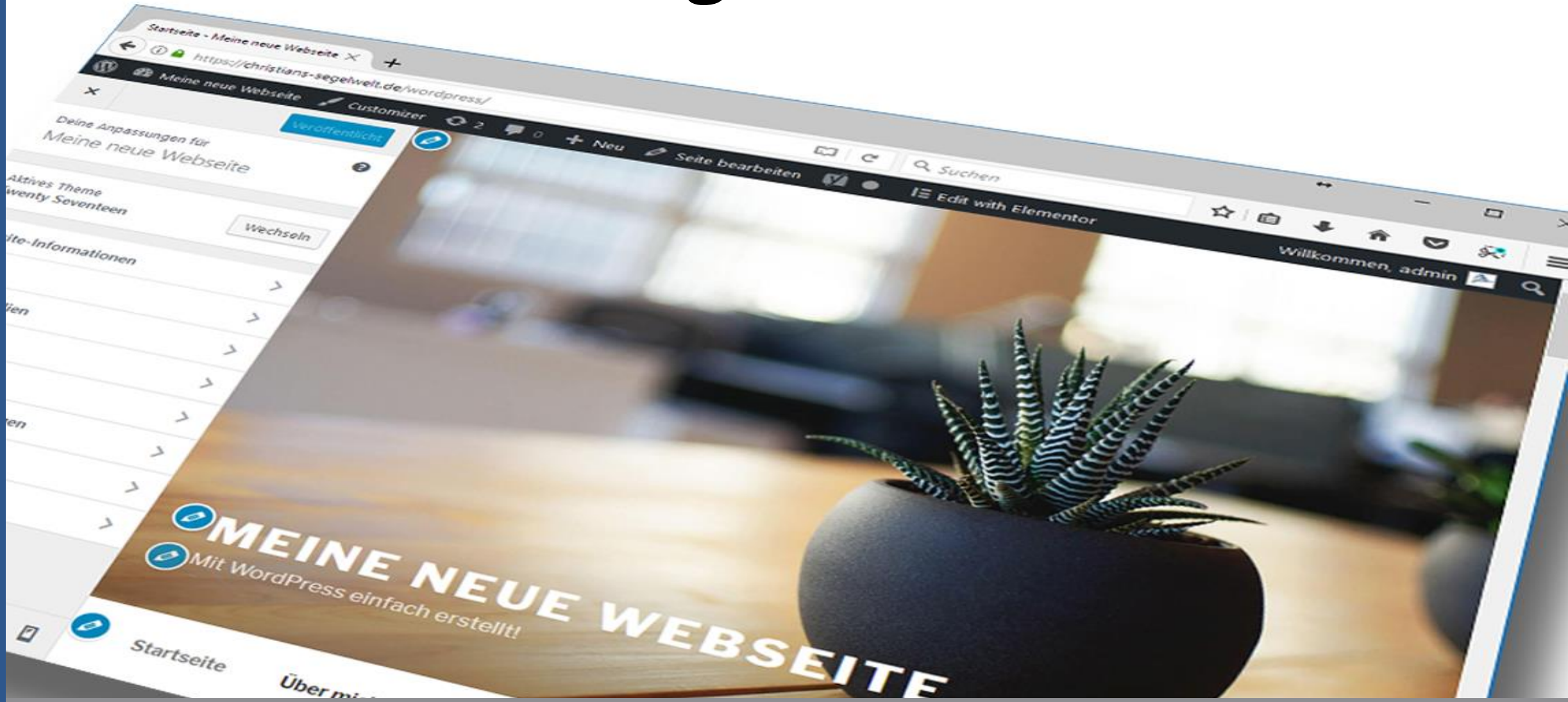
VPN – Schutz vor „Lauschern“



VPN – Umgehung Geoblocking



DSGVO und die eigene Webseite



https: Verschlüsseltes Internet

tethisIT
Kluge IT für Unternehmer

Pflicht, sobald Daten eingegeben werden können

Beweist, das die Seite echt ist. Wenn man kontrolliert!

Daten werden verschlüsselt übertragen

Für https ist ein Zertifikat nötig, „Personalausweis“ für die Seite

Bei der Ausstellung wird Identität überprüft:

- Domain-Prüfung (Zugriff auf den Webserver/E-Mail reicht)
- Organisations-Prüfung (Firmenbuch, Kreditkarte, etc.)
- Extended Validation (Identifikation z.B. per Post, nicht für e.U.)

„Let‘s Encrypt“ Zertifikate sind kostenlos und automatisch

https: Verschlüsseltes Internet

Vorteile einer https-Webseite:

- Nicht verschlüsselte Webseiten werden nicht mehr angezeigt
- Google Ranking ist besser
- DSGVO-konform (wenn Besucher Daten eingeben können)

⇒Neue Webseite mit https beginnen (einfach, kostenlos)

⇒Bestehende Webseite möglichst umstellen (evtl. aufwendig)

https: Verschlüsseltes Internet

tethisIT
Kluge IT für Unternehmer

Ablauf bei der Umstellung von bestehenden Wordpress-Seiten

1. Backup!
2. Zertifikat installieren (Webhoster)
3. URL unter Einstellungen / Allgemein ändern
4. Umleitung einrichten (.htaccess, Webhoster)
5. Datenbank korrigieren (Better Search Replace)
6. „mixed content“ suchen und korrigieren (Entwicklertools)
7. Google Search Console / Analytics
8. „Likes“ sichern: Yoast og:url setzen und FB von Umleitung ausnehmen

Anl.: https://www.wpbeginner.com/wp-tutorials/how-to-add-ssl-and-https-in-wordpress/
https://www.miss-webdesign.at/wordpress-auf-https-umstellen/

Ist die Webseite DSGVO-konform?

Zu beachten ist jede Funktion, die Daten über Besucher sammelt und evtl. (z.B. zur Analyse) weitergibt:

- Server-Protokolle
- Social-Media (Like-Buttons, Share-Buttons)
- Anti-spam oder Sicherheits-Funktionen
- Statistiken, Performance Monitoring
- Ressourcen von anderen Seiten (Videos, Bilder, Fonts)
- Cookies
- Im Zweifel googlen, ob Einwilligung erforderlich ist

Gute Liste für Wordpress: https://www.blogmojo.de/wordpress-plugins-dsgvo/

Webseite: Einwilligung

Vertrag: Info reicht aus

Berechtigtes Interesse des Betreibers => Info und evtl. Opt-Out

Interesse des Besuchers überwiegt => Einwilligung

Berechtigtes Interesse / Vertrag	Einwilligung
WooCommerce Server Logfiles Google Font (aber vermeiden) Google Re-Captcha Kommentare	Google Analytics Facebook Pixel Akismet (AntiSpam) JetPack (alround Plugin) Externe Medien (Videos)

Gute Liste für Wordpress: https://www.blogmojo.de/wordpress-plugins-dsgvo/

Google Fonts

- Wenn Google Fonts normal (also von google) geladen werden, wird die IP-Adresse aller Besucher an Google übertragen!
- Das hat zu ungerechtfertigten Schadenersatzforderungen geführt
- Google sichert zu, die IP-Adresse nicht zu verarbeiten
- Datenschutzbehörden haben sich noch nicht geäußert
- Rechtsgrundlage „berechtigtes Interesse“ ist vertretbar
- Aber: Man kann die Datenweitergabe einfach vermeiden

=> Google Fonts lokal einbinden, dann besteht kein Risiko

Ein paar Tipps dazu: https://tethis-it.at/google-fonts-lokal-einbinden/ oder googeln

Cookies

Cookies speichern Besucher-spezifische Information in dessen Browser. Damit können Besucher auch auf anderen Webseiten wiedererkannt werden.

Für den Betrieb der Seite unbedingt nötige Cookies (Session, Login, Warenkorb)	Andere Cookies (Google Analytics, Tracking, Werbung)
Rechtsgrundlage: berechtigtes Interesse	Rechtsgrundlage: Einwilligung
Cookie-Hinweis nur als Info oder gar nicht (nur Hinweis in Datenschutzerklärung)	Cookie-Hinweis mit Zustimmung / Ablehnung plus Info in Datenschutzerkl.

Einwilligung bedeutet: Erst fragen, dann Cookie setzen!
Wordpress Plugins: GDPR Cookie Consent, GDPR Cookie Compliance, Borlabs Cookie, WP DSGVO Tools

Webseite sichern

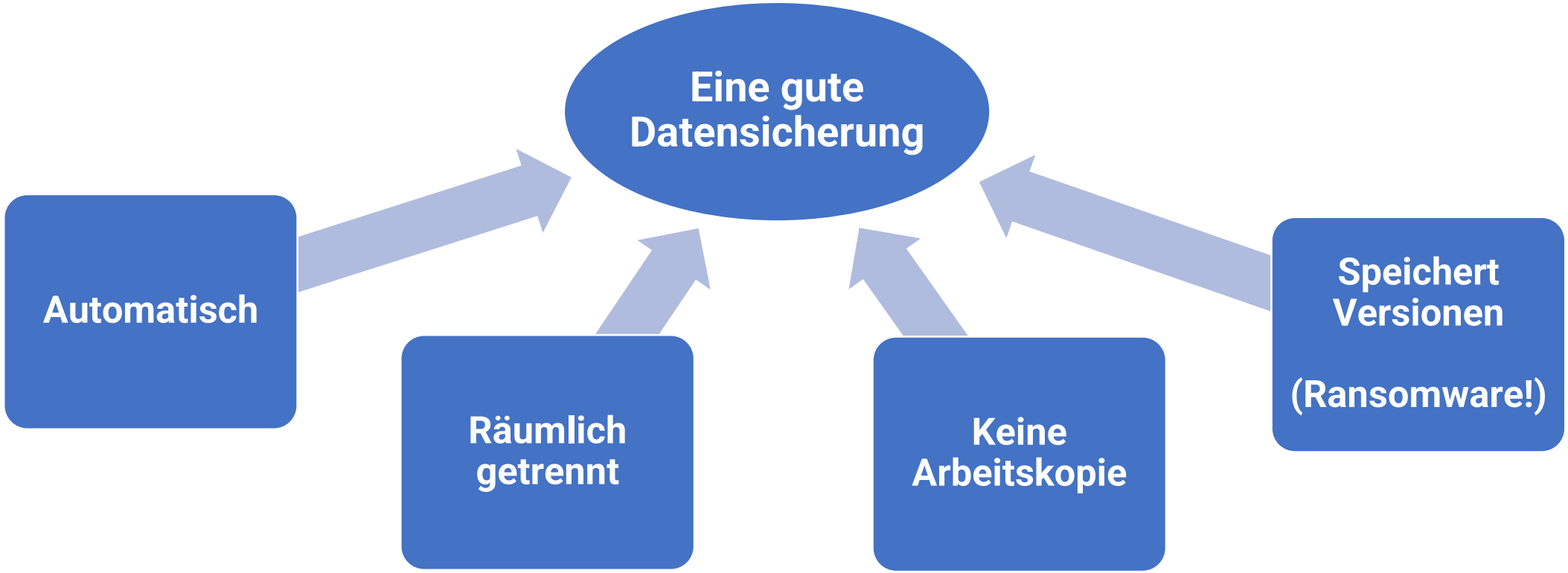
- Webseiten, Webserver, etc. werden ständig angegriffen (Brute-Force-Attacks, Ausnutzung von Exploits)
- Updates!
- Sichere Passwörter UND Benutzernamen (nicht „admin“)
- 2-Faktor Authentisierung einrichten (z.B. Google Authenticator, Wordfence, Wordpress 2-step verification, Duo, Rublon, Two Factor Authentication)
- HTTPS für Admin-Bereich nutzen
- Sicherheitsplugins können helfen, z.B. Wordfence, WPS Hide Login, Disable REST API (aber viel Unsinn am Markt)

Anleitung z.B. http://www.erfolgsrezepte-online.de/wordpress-absichern/

Datensicherung

Frage: Welche Auswirkungen hätte ein Totalverlust?

=> Zeit, Kosten, Reputation



Datensicherung

Was sollte gesichert werden?

- Daten auf dem Computer & NAS (wo sind relevante Daten?)
- Daten auf dem Handy
- E-Mails
- Webseite
- Daten aus Cloudlösungen (Buchhaltung, Online-Galerie, …)
- Daten aus Cloud-Speicher (Dropbox, OneDrive, etc.)

Wichtig: Wiederherstellung testen!

Datensicherung: Optionen

- Kopie auf verschlüsselte externe Festplatte, USB Stick
  nicht automatisch, keine Versionen, E-Mails nicht enthalten, räumlich getrennt?
- Synchronisation mit Cloud-Speicher
  kurze Aufbewahrung, evtl. keine Versionen, Arbeitskopie, keine E-Mails, räumlich getrennt
- Cloud-Backup (tethis CDS, Veeam, Acronis und andere)
  automatisch, Versionen, E-Mails möglich, räumlich getrennt, abhängig vom Internet – sichert auch Daten aus der Cloud, Office 365, Exchange, Datenb.
- Backup auf NAS / Server / externe Platte mit Backup-Programm
  automatisch, Versionen, E-Mails möglich, räumlich getrennt?

Datensicherung: Achtung

- Wo speichert das E-Mail-Programm die E-Mails?
  Diesen Ordner sichern
- Sichert der Webhoster evtl. die E-Mails?
- Cloud-Backup sichert z.T. auch E-Mails (Office 365)
- Wordpress: Plugins benutzen, sichern auf anderen Server
- Sichert der Webhoster? Mit Versionen?
- Regelmäßig komplett herunterladen (Dateien und Datenbank)
- Handy: eingebautes Backup, Backup Apps

Win10: Dateiversionsverlauf

Einrichtung:

- *Einstellungen* / *Update & Sicherheit* / Sicherung
- Externe Festplatte: *Laufwerk hinzufügen*
- Netzwerklaufwerk: *Weitere Optionen* / *Siehe erweiterte Einstel.* / *Netzwerkadresse auswählen* / *Netzwerkadresse hinzufügen*

Wiederherstellung:

- *Einstellungen* / *Update & Sicherheit* / Sicherung / *weitere Optio.*
- Ganz unten: *Daten von einer aktuellen Sicherung wiederherstell.*

Mac: TimeMachine

Einrichtung:

- *Einstellungen / TimeMachine/ Backup-Volume auswählen*
- Externe Festplatte: *Laufwerk auswählen*
- Netzwerklaufwerk: Vorher im Finder *Gehe Zu / Mit Server verbinden /* NAS bzw. TimeMachine (Gerät) auswählen

Wiederherstellung:

- *Im Finder Programme / TimeMachine aufrufen*
- *Rechts Datum auswählen, Datei auswählen,*

Updates, Updates, Updates

tethisIT
Kluge IT für Unternehmer

- Wichtigste Schutzmaßnahme (neben „Augen offen halten“)
- Ständiger Wettlauf zwischen Hackern und Herstellern
- Wann immer möglich: Automatisch installieren!
  Nachteil: kostet Zeit, kann Fehler verursachen
- Webseite: Wordpress (CMS) Updates installieren
  Vorher unbedingt Backup machen!
- Geräte: Modems, Router, Home-Automation nicht vergessen
- Handy: Updates nicht verhindern

Virenscanner

- Auch für Macs und Linux eine gute Idee
- Wichtig ist vor allem der „Echtzeitschutz“
- Regelmäßige Updates sind Pflicht
- Meine persönliche Meinung: Microsoft Defender reicht aus
- Auf Handys gelten Virenscanner als problematisch

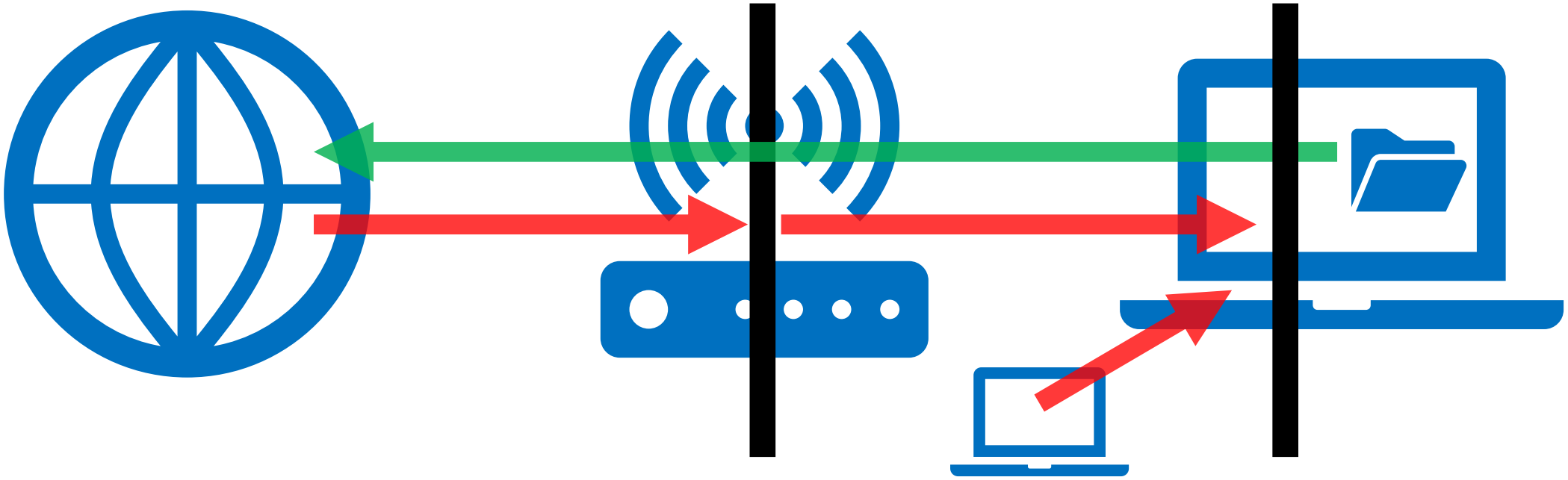
Wenn Virus / Trojaner gefunden wurde:

- Gefundenen Virus im Internet nachschlagen
- Von USB / CD starten und komplett prüfen

Die Augen offen halten!

- Schadsoftware kommt meistens per E-Mail
- Mailprogramm komplette Adresse anzeigen lassen
- Vorsicht mit Anhängen bei unbekannten Absendern
- Warnungen NICHT einfach wegklicken
- Programme nur aus seriösen Quellen herunterladen
- Im Zweifel: Abbrechen
- Nach Infektion: Von sauberem Medium starten, testen, neu installieren

Firewall



Gibt es im Router und in jedem PC / Mac
Unterbindet eingehende Verbindungen aus dem Internet
Ausgehende Verbindungen (und Antworten) sind erlaubt
„UPNP“ abschalten, damit können sich Apps selbst freischalten

Organisatorische Maßnahmen

tethisIT
Kluge IT für Unternehmer

Kommunikationsmittel (für sensible Daten) bewusst wählen

- Unverschlüsselte E-Mails sind nicht sicher
- E-Mail-Verschlüsselung ist einfach, erfordert aber den Austausch von Zertifikaten oder Passwörtern
  Anleitung für Outlook https://outlook-blog.de/9161/e-mails-in-outlook-verschluesseln/
- Alternative 1: Einwilligung einholen
- Alternative 2: Dropbox, OneDrive, SharePoint oder eigene Webseite benutzen

Organisatorische Maßnahmen

- Need-to-know: Zugang zu Informationen beschränken
- Nach der Arbeit vom PC abmelden / sperren
- Clean Desk Policy, keine Aufrufe mit Namen
- Keine fremden Datenträger / USB Sticks
- Regelmäßig alte Daten löschen
  (z.B. im Rahmen der jährlichen Prüfung der DSGVO Dokumentation)

Organisatorische Maßnahmen

- Räume verschließen
- Akten, Datenträger und Geräte verschlossen aufbewahren
- Alte Akten Schreddern
- Brandschutz (Feuerlöscher, Rauchmelder)
- Alarmanlage
- WLAN-Router und LAN-Switch wegschließen

Organisatorische Maßnahmen

- Mitarbeiter-Vereinbarungen abschließen:
  - Verpflichtung zur Geheimhaltung
  - Regelungen für eigene Geräte
  - Einwilligung in Datenverarbeitung

- Bei Kündigungen:
  - Daten löschen (lassen)
  - Rechte entziehen

Dokumentation der TOMs

- Evtl. Fragebogen ausfüllen
- Vorlage der Ärztekammer ist hilfreich

Datenschutzerklärung

- Verantwortlicher
- Welche Daten & Zweck der Verarbeitung
- Quelle, falls nicht selbst eingegeben
- Rechtsgrundlage
- Werden berechtigte Interessen verfolgt? Welche?
- Weitergabe an Drittstaaten? Ist der Empfänger “sicher”?
- Dauer der Speicherung, Kriterien für Löschung
- Werden automatisch Entscheidungen getroffen? Welche?
- Rechte des Betroffenen (Auskunft, Widerspruch, Beschwerde, etc.)
- Datenschutzbeauftragter, Kontaktdaten

Datenschutzerklärung

Vorlagen: wko, tethis IT
Generator:
https://www.adsimple.at/datenschutz-generator/
https://www.xn--generator-datenschutzerklrung-pqc.de/
(auch in EN, FR. Achtung: deutsch)

Für Webseite verpflichtend

Bei Vertragsabschluss kann zusätzlich informiert werden

UGP
Das Unternehmensgründungs-programm des AMS

bit management
member of bit group

ösb Consulting

AMS
Arbeitsmarktservice Wien

Ihre Beobachtungen und Eindrücke sind wertvoll, wir wollen die Qualität unserer Workshops sichern und steigern.

https://shorty.oesb-gruppe.com/toller