tethisIT
Kluge IT für Unternehmer

UGP Online Workshop
Datensicherheit & Datenschutz

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

Technisches

- Alle Mikrofone (außer meinem) sind abgeschaltet
- Bei Fragen: Im Chat „Hand heben“, ich öffne dann Dein Mikro
  Alternativ: Frage in den Chat schreiben
- Eure Kameras bleiben aus, ich schalte Sie nur am Anfang zum Testen und bei Fragen kurz ein
- Fragen die im Workshop nicht beantwortet werden können, beantworte ich per Mail an alle TeilnehmerInnen
- Link zu Download für alle Vorlagen, Slides etc. schicke ich nachher

Inhalt

1. Bedrohungen für die Daten
2. DSGVO: Grundlagen & Ziele
3. Das Verfahrensverzeichnis
4. Andere Dokumente
5. Verarbeitung im Ausland
6. Cloud Dienste & WhatsApp
7. Schutzmaßnahmen & Webseite
8. Dokumentation der Maßnahmen
9. Datenschutzerklärung

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

- Datendiebstahl (Trojaner, Keylogger, gehackte Webseite, …)
- Diebstahl von Geräten und Datenträgern
- Ransomware
- Defekte an Hard- oder Software
- Feuer und Naturkatastrophen
- Menschliches Versagen

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)

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

Verhältnismäßigkeit ist gefordert, nicht Perfektionismus!

Österreichische Anpassungen

Am 14. April 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

Worum geht es?

Ziel:

Mehr Kontrolle über die eigenen Daten

Verpflichtung zum Schutz der Daten

DSGVO definiert Grundsätze und Regeln

für gesetzeskonforme Datenverarbeitung

Gültigkeitsbereiche

Gilt für personenbezogene Daten lebender, natürlicher Personen, die irgendwie geordnet abgelegt werden.

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!

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

Auftragsverarbeiter: Mailchimp, Microsoft Office 365, Webhoster, DropBox, Cloud Datensicherung
=> Verarbeitet Daten im Auftrag / im Interesse / zugunsten eines Auftraggebers

Verantwortlicher: Ihr selbst, Banken, Steuerberater, Versanddienstleister sind „Verantwortlich im Sinne der DSGVO“
=> Entscheidet über Zwecke und Mittel der Datenverarbeitung

Regelungen im Auftrag / Vertrag sind zur Unterscheidung wichtig.

Der Verantwortliche muss sich von Auftragsverarbeiter **schriftlich** zusichern lassen, dass dieser die DSGVO einhält (Auftragsverarbeiter-Vereinbarungen: https://www.blogmojo.de/av-vertraege/)

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

Transparent

– Über jede Verarbeitung muss informiert werden, nichts darf im geheimen passieren.

– Betroffene Personen können Auskunft über die gespeicherten Daten verlangen

Rechtmäßig

– Datenverarbeitung ist nur mit Rechtsgrundlage erlaubt! (nächste Slides)

– Daten müssen rechtmäßig beschafft werden.

– Bei Kauf von Daten: Verkäufer muss die Einstimmung zur Nutzung der Daten für den geplanten Zweck bereits eingeholt haben.

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.)

Andere DSGVO Grundsätze

- Nur mit Zweckbindung
- So wenig wie möglich
- Nur so lange wie nötig
- Korrekt und sicher (Privacy by Design & Privacy by default)
  - Virenschutz
  - Passwörter
  - Datensicherung
  - Verschlüsselung
  - Zugriffbeschräkungen

Rechte des Betroffenen

- Recht auf Information => Datenschutzerklärung
- Recht auf Auskunft => Was wissen Sie über mich, was machen Sie damit?
- Recht auf Berichtigung, Löschung und Einschränkung
- Recht auf Datenübertragung
- Recht auf Widerspruch

Umsetzungsfrist: 1 Monat, 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
- Maßnahmen zum Datenschutz
- Privacy by Design
- Risikoanalyse
- Meldung von Datenschutzverletzungen
- Zusammenarbeit mit der Datenschutzbehörde
- Ernennung eines Datenschutzbeauftragten
- Dokumentationspflicht

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

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

Aufgabe

1. Bitte erstelle eine Zeile des Verarbeitungsverzeichnisses, und zwar für einen Zweck, der für Dich spezifisch ist (also Dein „Tagesgeschäft“)
2. Benötigst Du eine Einwilligung (was ist die Rechtsgrundlage?)
3. Falls ja, formuliere die Frage und schreibe sie im letzten Feld auf

Ein leeres Formular und Beispiele schicke ich per Mail.

Das Resultat bitte per E-Mail an christian.toller@tethis-it.at

Bei Fragen: Bitte im Chat melden

Nach der Pause besprechen wir ein paar Beispiele

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!

Einwilligungserklärungen

Eine korrekte 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!

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 (USA: AV-Vertrag mit SCC‘s)
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

Datenverarbeitung im Ausland

Verarbeitung außerhalb der EU nur möglich…

- Wenn ein „Angemessenheits-Beschluss“ der EU Kommission vorliegt z.B. Kanada, Schweiz, Neuseeland, Japan (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)
- Wenn geeignete Garantien vorliegen (ISO Zertifizierung)
- Wenn ein Grund für eine Ausnahme vorliegt
  - Ausdrückliche Einwilligung
  - Auftragsverarbeiter-Vertrag, der die „Standardvertragsklauseln“ (SCC‘s) enthält
  - etc.

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
- Handy mit zwei getrennten Telefonbüchern (Blackberry, Samsung Knox)
- 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/

Maßnahmen zum Datenschutz

tethisIT
Kluge IT für Unternehmer

Technische Maßnahmen

Passwörter
Datensicherung
Verschlüsselung
Virenscanner

Organisatorische Maßnahmen

Vergabe von Zugriffsrechten
Information / Weiterbildung
Auswahl von Kommunikationsmedien

Passwörter sind Pflicht!

– Passwörter auf allen Geräten und 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 nutzen: lastpass.eu, 1password.com, keepass.info

Auf https://haveibeenpwned.com/ und https://sec.hpi.de/ilc/ checken ob Passwort geklaut wurde

Wenn möglich, 2-Faktor-Authentisierung nutzen! (SMS, Fingerabdruck)

Geräte / Speicher verschlüsseln

tethisIT
Kluge IT für Unternehmer

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

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
- „Let‘s Encrypt“ Zertifikate sind kostenlos und automatisch
- Google Ranking ist besser, Browser warnen nicht

=> Webseite unbedingt mit https beginnen, sonst umstellen!

Ist die Webseite DSGVO-konform?

tethisIT
Kluge IT für Unternehmer

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, Werbung
- 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 oder berechtigtes Interesse: Info reicht aus

Interesse des Besuchers überwiegt => Einwilligung

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

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

Cookies

tethisIT
Kluge IT für Unternehmer

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 Compliance, Borlabs Cookie, WP DSGVO Tools

Webseite sichern

tethisIT
Kluge IT für Unternehmer

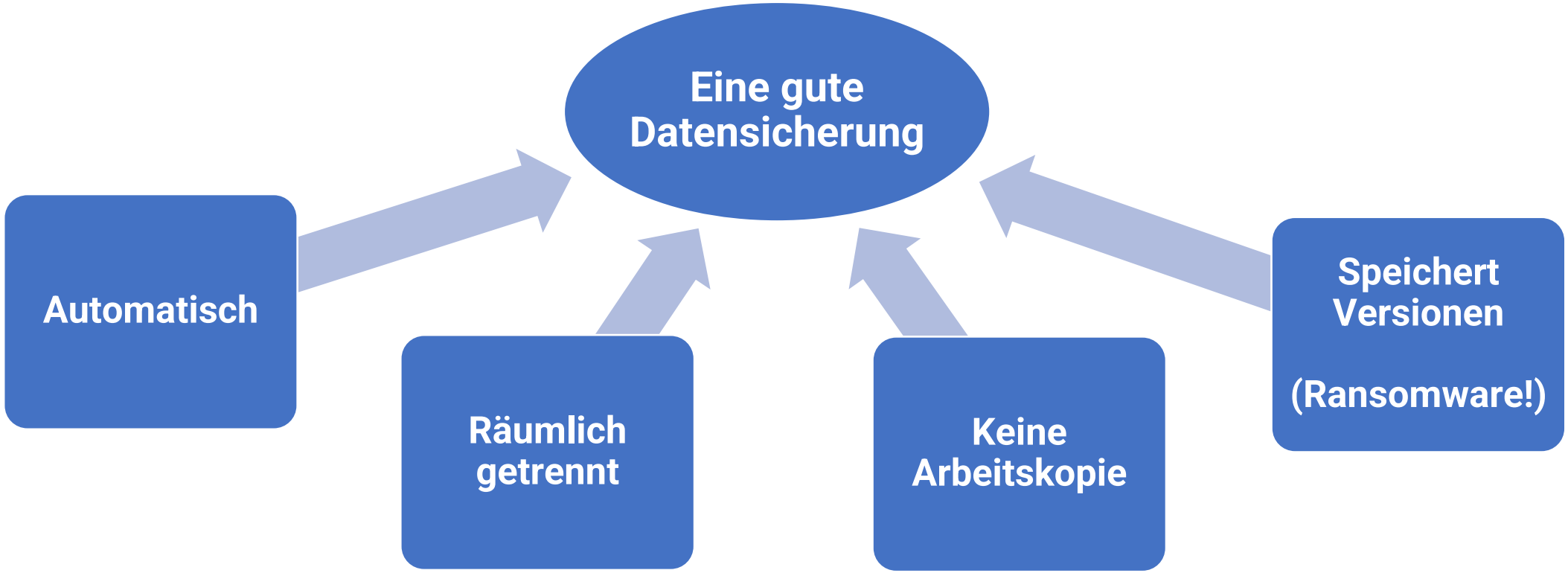
- Webseiten, Webserver, etc. werden ständig angegriffen (Brute-Force-Attacks, Ausnutzung von Exploits)
- Updates, Updates, Updates. Und natürlich BACKUPs! (z.B. Updraft Plus)
- Sichere Passwörter, Benutzername nicht „admin“
- 2-Faktor Authentisierung einrichten (z.B. Google Authenticator, Wordfence, Wordpress 2-step verification, Duo, Rublon, Two Factor Authentication)
- HTTPS
- Sicherheitsplugins können helfen, z.B. Wordfence, WP Cerber Security, Sucuri, 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 (Google oder iCloud Backup)
- E-Mails (IMAP, nicht POP / Mailprogramm sichern)
- Webseite (z.B. mit Updraft Plus)
- 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
  z.B. mit FileVault (Mac) oder Dateiversionsverlauf (Win 10)
  automatisch, Versionen, E-Mails möglich, räumlich getrennt?

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

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

- Zugang zu Daten beschränken (Berechtigungen, wegschließen)
- Clean Desk Policy, keine Aufrufe mit Namen
- Keine fremden Datenträger / USB Sticks
- Sichere Vernichtung von Daten und Datenträgern
- Brandschutz, Alarmanlage
- Mitarbeiter-Vereinbarung
- Plan für den Fall das Mitarbeiter ausscheiden

In den Downloads gibt es eine Checkliste und zwei Vorlagen für TOMs

Datenschutzerklärung

Vorlagen: wko, tethis IT

Generatoren:

https://www.firmenwebseiten.at/datenschutz-generator/

https://www.ratgeberrecht.eu/leistungen/muster-datenschutzerklaerung.html (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

Im Auftrag des AMS
Arbeitsmarktservice Wien

Ihre Meinung ist uns wichtig!

https://oesb.surveymonkey.com/r/UGP-Toller-ON

PAUSE !!

Pause bis 12:50