Datenschutz im Verein (Teil 2)
Technisch Organisatorische Maßnahmen (TOM)

Erstellen eines IT-Sicherheitskonzeptes

Kurze Vorstellung

- Matthias Müller
- Information Security Officer bei Siemens seit 2005
- Über 30 Jahren ehrenamtlich in versch. Organisationen
  - Bayerische Sportjugend (bsj) Unterfranken
  - DJK Sportverband Unterfranken
  - DJK Salz e.V.
  - Rhönklub Zweigverein Salz e.V.

Wichtige Information!!!

- Ich bin kein Jurist
- Praxisnahe Orientierungshilfe – keine Rechtsberatung
- Weitergabe von eigenen Erfahrungen bzw. eigenem Wissen

5 Jahre DSGVO – Resümee

- Riesen Hype 2018 mit großer Verunsicherung
- In den Vereinen nicht immer nachhaltig umgesetzt (2020 Corona)
- Durch hohe Fluktuation von Ehrenamtlichen
  ➔ regelmäßige Infos notwendig
- Zeit nehmen zum Prüfen, denn Einhaltung von gesetzl. Anforderungen
- Bisher keine Strafen gegen Vereine bekannt, aber …

DSGVO = Datenschutz-Grundverordnung

Agenda

- Einige Grundlagen zum Datenschutz aus Teil1
- Anforderungen an ein IT-Sicherheitskonzept
- Praktische Tipps für Umsetzung im Verein

Grundlagen (aus Teil 1)

- Ein bisschen Theorie muss sein

Grundlagen

- **Datenschutzgesetz** sollen den Einzelnen davor schützen, dass er durch Umgang mit seinen personenbezogenen Daten in seinen **Persönlichkeitsrechten** beeinträchtigt wird
- Umsetzung von EU-Recht 2018 mit Neuordnung und teilweiser Verschärfung des alten Rechts (BDSG), das in der Vergangenheit viele sorglos „ignoriert“ haben
- Alle **Vereine betroffen** als „Verarbeiter“ von personenbezogenen Daten
- Vereine gleichgestellt wie „Unternehmen“
- Kein Unterschied zwischen Hauptberuf oder Ehrenamt
- „Verantwortlicher“ unabhängig von der Rechtsform der/die Vorsitzende

Personenbezogene Daten

Daten sind **personenbezogen**, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann.

Zum Beispiel:

- Name, Adresse
- Geburtsdatum
- Mailadresse
- Kontonummer

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. **Sie sind besonders schützenswert.**

Rechtmäßigkeit

Grundsätzlich keine Datenverarbeitung ohne Einwilligung oder eine andere Rechtsgrundlage

Rechtsgrundlagen, für die keine Einwilligung erforderlich ist:

- Verarbeitung von Daten, die zur Vertragserfüllung notwendig sind (Art. 6 Abs. 1 lit. b. DSGVO)
- „zur Wahrung berechtigter Interessen des Verantwortlichen“ (Art. 6 Abs. 1 lit. f. DSGVO)

Zum Beispiel:

Verein ist Mitglied in Dachverband

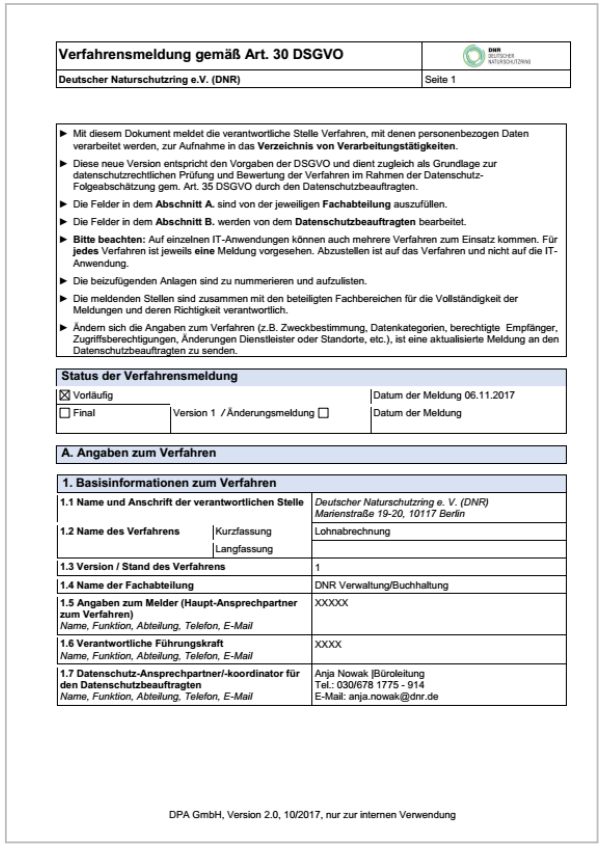
➔ *Notwendige Weitergabe von Daten*

Grundsätze

- **Treu und Glauben:** Geschützt werden müssen alle Daten über die persönlichen oder sachlichen Verhältnisse, die einer bestimmten Person zugeordnet werden können
- **Transparenz:** Rechenschaftspflicht gegenüber der zuständigen Aufsichtsbehörde und dem Betroffenen
- **Zweckbindung:** nur für vorher konkret festgelegte Zwecke
- **Datensparsamkeit:** nur notwendige und begründete Daten
- **Speicherbegrenzung, Integrität, Vertraulichkeit:** Daten müssen sachlich richtig sein, aktualisiert werden, sicher gespeichert werden und auch wieder gelöscht werden

Verfahrens-Verzeichnis

- Aufstellung aller im Verein verwendeter SW
- Bei Kontrollen/Beschwerden ist es wichtig, hier etwas vorweisen zu können
- Verschiedene Formen, auch tabellarisch
- Beschreibung des IT-Sicherheitskonzeptes
  - ➔ Technische und Organisatorische Maßnahmen (TOM)



Verfahrensmeldung gemäß Art. 30 DSGVO | Seite 1

Deutscher Naturschutzring e.V. (DNR)

- Mit diesem Dokument meldet die verantwortliche Stelle Verfahren, mit denen personenbezogen Daten verarbeitet werden, zur Aufnahme in das **Verzeichnis von Verarbeitungstätigkeiten**.
- Diese neue Version entspricht den Vorgaben der DSGVO und dient zugleich als Grundlage zur datenschutzrechtlichen Prüfung und Bewertung der Verfahren im Rahmen der Datenschutz-Folgeabschätzung gem. Art. 35 DSGVO durch den Datenschutzbeauftragten.
- Die Felder in dem **Abschnitt A.** sind von der jeweiligen **Fachabteilung** auszufüllen.
- Die Felder in dem **Abschnitt B.** werden von dem **Datenschutzbeauftragten** bearbeitet.
- **Bitte beachten:** Auf einzelnen IT-Anwendungen können auch mehrere Verfahren zum Einsatz kommen. Für **jedes** Verfahren ist jeweils **eine** Meldung vorgesehen. Abzustellen ist auf das Verfahren und nicht auf die IT-Anwendung.
- Die beizufügenden Anlagen sind zu nummerieren und aufzulisten.
- Die meldenden Stellen sind zusammen mit den beteiligten Fachbereichen für die Vollständigkeit der Meldungen und deren Richtigkeit verantwortlich.
- Ändern sich die Angaben zum Verfahren (z.B. Zweckbestimmung, Datenkategorien, berechtigte Empfänger, Zugriffsberechtigungen, Änderungen Dienstleister oder Standorte, etc.), ist eine aktualisierte Meldung an den Datenschutzbeauftragten zu senden.

Status der Verfahrensmeldung

☒ Vorläufig		Datum der Meldung 06.11.2017
☐ Final	Version 1 / Änderungsmeldung ☐	Datum der Meldung

A. Angaben zum Verfahren

1. Basisinformationen zum Verfahren

1.1 Name und Anschrift der verantwortlichen Stelle		*Deutscher Naturschutzring e. V. (DNR) Marienstraße 19-20, 10117 Berlin*
1.2 Name des Verfahrens	Kurzfassung	Lohnabrechnung
	Langfassung	
1.3 Version / Stand des Verfahrens		1
1.4 Name der Fachabteilung		DNR Verwaltung/Buchhaltung
1.5 Angaben zum Melder (Haupt-Ansprechpartner zum Verfahren) *Name, Funktion, Abteilung, Telefon, E-Mail*		XXXXX
1.6 Verantwortliche Führungskraft *Name, Funktion, Abteilung, Telefon, E-Mail*		XXXX
1.7 Datenschutz-Ansprechpartner/-koordinator für den Datenschutzbeauftragten *Name, Funktion, Abteilung, Telefon, E-Mail*		Anja Nowak |Büroleitung Tel.: 030/678 1775 - 914 E-Mail: anja.nowak@dnr.de

DPA GmbH, Version 2.0, 10/2017, nur zur internen Verwendung

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen
Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de
Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer/ Sozialabgaben	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	• Name und Adressen • Eintrittsdatum • Sportbereiche	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept

Muster–Verzeichnis

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten" gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Bayerisches Landesamt für Datenschutzaufsicht

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	• Auszahlung der Löhne/Gehälter • Abfuhr Sozialabgaben u. Steuern	Beschäftigte	• Name und Adressen der Beschäftigten • ggf. Religions-zugehörigkeit • Eindeutige Kennzahlen zur Steuer/ Sozialabgaben ...	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	• Name und Adressen • Eintrittsdatum • Sportbereiche ...	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	28.02.2018	Außendarstellung	• Mitglieder • Webseitenbesucher	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@ waldmuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@ waldmuehler-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...	...	...	...	...	...	...	...	...	...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Forderung aus DSGVO: IT-Sicherheitskonzept erstellen

- Technische Maßnahmen zur Verbesserung des Datenschutzes (derzeit gültige Standards)
- IT-Sicherheit durch aktuelle Hard- und Software
- Sichere Kommunikation/Kollaboration gewährleisten, speziell mit elektronischen Medien
- Pseudonymisierung und Verschlüsselung
- Regelmäßige Backups
- Löschkonzept vorhanden

Anforderungen an ein IT-Sicherheitskonzept

- Wie erstelle ich ein Konzept?

IT-Sicherheitskonzept

- Definition des Geltungsbereichs – Wer nutzt welche Daten im Vereinsumfeld?
- Welche IT-Verfahren sind vorhanden und müssen berücksichtigt werden?
- Definition des Schutzbedarfs
  (Vertraulichkeit, Integrität, Verfügbarkeit)
- Maßnahmenkatalog festlegen
- Aktualisierung und Fortschreibung

Auflistung der Daten

Wer nutzt diese Daten?

Inventur der Datenverarbeitung

- Welche Daten werden im Verein erfasst?
- Wer hat Zugriff auf die Daten?
- Zu welchem Zweck werden die Daten erhoben?
  - Mitgliederverwaltung, Beitragswesen
  - Meldung an Verbände
  - Versenden von Informationen an Mitglieder
  - Passwesen/Spielerlisten
  - Whatsapp-Gruppen zur Erreichbarkeit
  - Datenerfassung für spezielle Vereinsveranstaltungen (Vereinsausflug, Zeltlager, Herzsport, …)

Basis Verfahrensverzeichnis

Beispiel Mitgliederdaten

Beispiel eines Lebenszyklus von Daten	Wer ist involviert?
Anmeldung eines Mitglieds mit einem Beitrittsformular	Abteilungsleiter
Eingabe der Daten in Mitglieder-Verwaltungsprogramm	Schriftführer
Verteilen der Mitgliederliste	Vorstand/ Abteilung
Meldung der Mitglieder an Dachverband	Schriftführer
Abbuchung der Beiträge	Kassier
Gratulieren zum runden Geburtstag	Vorsitzender
Austritt oder Tod (Änderung in Mitgliederverwaltung)	Schriftführer

Löschfristen definieren!

Kontrollieren der Prozesse

- Wie werden die Daten im Verein übertragen?
  ➔ Mail, USB-Stick, Papierlisten
- Wo werden die Daten gespeichert bzw. weiterverarbeitet?
  ➔ Vereins-PC, private PCs, USB-Medien
- Müssen alle Verantwortliche die kompletten Informationen haben?
  ➔ z.B. Abteilung bekommt die komplette Mitgliederliste
- Wechsel eines Vorstandmitglieds/Funktionäre
  ➔ Löschung/Vernichtung aller personenbezogenen Daten
- Gibt es gesetzliche Anforderungen?
  ➔ Gesetzliche Aufbewahrungspflichten für finanzielle Transaktionen

Informationsverteilung überprüfen!
Nur notwendige Daten verteilen!

IT-Verfahren auflisten

Sind die Daten immer sicher?

Wer nutzt IT-Verfahren?

Mitgliederverwaltung	Mitgliederdaten	Schriftführer
Beitragswesen	Abbuchung der Beiträge	Kassier
Buchungsprogramm	Buchhaltung	Kassier
Datenschnittstelle Dachverband	Meldung von Mitgliedern	Schriftführer
Mail (Outlook, Thunderbird, …)	Kollaboration/Kommunikation	kompl. Vorstand
Microsoft Office, OpenOffice, …	Mitgliederlisten, Rechnungen	kompl. Vorstand
USB-Medien	Verteilen von Infos	kompl. Vorstand
Backup-Programm	Sicherung von wichtigen Daten	Kassier, Schriftführer
Homepage	Informationsplattform	Admin
Social-Media	Terminkoordination	kompl. Vorstand

Beispiel für IT-Verfahren im Verein

Empfehlungen

- Am besten eigene Vereins-PCs – zumindest für die essentiellen Daten, z.B. Mitgliederverwaltung, Buchhaltung, Beitragswesen
- Bei privaten PCs notwendige Schulung/Info
  ➔ Wer nutzt diesen PC noch?
- Kennen alle Betroffenen das IT-Sicherheitskonzept des Vereins?
- Nachweis über erfolgte Aufklärung (Sorgfaltspflicht)

Schutzbedarf ermitteln

Wie wichtig sind die Daten?

Kategorien Schutzbedarf

- **Vertraulichkeit (Datenschutz)**
  - nur autorisierte Personen haben Zugriff auf Informationen
  - Maßnahmen: Zugriffskontrolle, Verschlüsselung, Sicherheitsrichtlinien
- **Integrität**
  - Informationen müssen richtig und vollständig sein / nicht unbefugt manipuliert
  - Maßnahmen: digitale Signaturen, Protokollierung von Änderungen
- **Verfügbarkeit**
  - berechtigte Nutzer können jederzeit auf Informationen zugreifen
  - Maßnahmen: Redundanz, Backups, regelmäßige Updates der Systeme

Schutzbedarf ermitteln (Beispiel)

Mitgliederverwaltung	Mitgliederdaten	DS-I-V
Beitragswesen	Abbuchung der Beiträge	DS-I
Buchungsprogramm	Buchhaltung	DS-I-V
Datenschnittstelle Dachverband	Meldung von Mitgliedern	DS
Mail (Outlook, Thunderbird, …)	Kollaboration/Kommunikation	DS
Microsoft Office, OpenOffice, …	Dokumente, Rechnungen, Mitgliederlisten	DS-I-V
USB-Medien	Verteilen von Infos	DS
Backup-Programm	Sicherung von wichtigen Daten	DS-I-V
Homepage	Informationsplattform	V
Social-Media	Terminkoordination	DS

DS = Datenschutz (Vertraulichkeit) / I = Integrität / V = Verfügbarkeit

Kontrollieren der Prozesse

- Alle Daten mit **Datenschutz-Relevanz**
  ➔ sicher abspeichern und sicher übertragen, Zugriff einschränken, Verschlüsselung der Daten

- Alle Daten mit **Integritäts-Anforderung**
  ➔ regelmäßige Kopien

- Alle Daten mit **Verfügbarkeits-Anspruch**
  ➔ regelmäßige Backups, möglichst an unterschiedl. Orten ablegen
  ➔ vereinsrelevante Daten an einer zentralen Stelle

Schutzkonzept erstellen

Maßnahmen definieren

IT-Schutzkonzept – Teil 1

- **Aktuelles Betriebssystem** mit automatischen Security-Updates einsetzen
- Aktuellen Web-Browser verwenden
- Software immer auf dem neusten Stand halten – regelmäßige Kontrolle der SW
- Daten / Software nur aus vertrauenswürdigen Quellen herunterladen
- Auf allen PCs **Virenschutz und Firewall** aktivieren
- PCs mit Bitlocker verschlüsseln
- **Sichere Passwörter** verwenden und die wichtigsten regelmäßig ändern
- Unterschiedliche Passwörter mit **Passwortsafe** nutzen
- **Unterschiedl. Benutzerkonten** anlegen (eingeschränkter User) – speziell bei „**Familien-PC**“
- Regelmäßige verschlüsselte Sicherungen und **Backups anlegen** – möglichst an unterschiedlichen Stellen aufbewahren
- **Löschfristen definieren** und einhalten – sicheres Löschen!
- Wichtige Vereins- und Zugangsdaten zentral und sicher hinterlegen

Beispiel für IT-Schutzkonzept

IT-Schutzkonzept – Teil 2

- Papier-Aktenvernichter für personenbezogene Daten vorhanden
- Abschließbaren Schränke für personenbezogene Daten nutzen
- **Vereins-WLAN absichern** mit aktuellster Verschlüsselung (mind. WPA2) – gilt auch für Heimnetzwerke
- Nur notwendige Daten an erforderliche Personen verteilen
- **Verschlüsselte Kommunikation** von personenbezogenen Daten mit passwortgeschützter ZIP-Datei – besser Mail-Verschlüsselung einrichten
- Auf Whats-App als offizielle Vereinskommunikation verzichten (Daten liegen auf amerikanischen Servern)
- Regelmäßige Info / Schulungen für Mitarbeiter
- Prozess zur **Einarbeitung von neuen Mitarbeitern** im Verein festlegen
- **Checkliste für ausscheidende Mitarbeiter** mit personenbezogenen Daten erstellen
- **Unterschriebene Verpflichtungserklärung** aller Mitarbeitern einholen
- Meldewege für Datenschutzpanne definieren und kommunizieren

Beispiel für IT-Schutzkonzept

Maßnahmen definieren und dokumentieren

- Erfassung aller PCs auf die erforderliche Hardware und Software-Ausstattung
  ➔ neue Hardware oder SW anschaffen bzw. zumindest in die Budgetplanung aufnehmen
- (verpflichtende) Schulungen für die Anwender anbieten
  ➔ (regelmäßige) Schulung der Mitarbeiter evtl. auch extern bei SW-Hersteller
- Löschfristen festlegen und kommunizieren
- Wichtige Vereinsdaten (z.B. Buchhaltung, Mitgliederverwaltung, Rechnungen) speziell mit gesetzl. Anforderungen zentral ablegen – evtl. Vereins-PC anschaffen
- Archivieren von besonderen Vereinsereignissen an einer zentralen Stelle (Ehrungen, Jubiläen, Auszeichnungen, …)

Beispiel-Maßnahmen

Verpflichtungserklärung

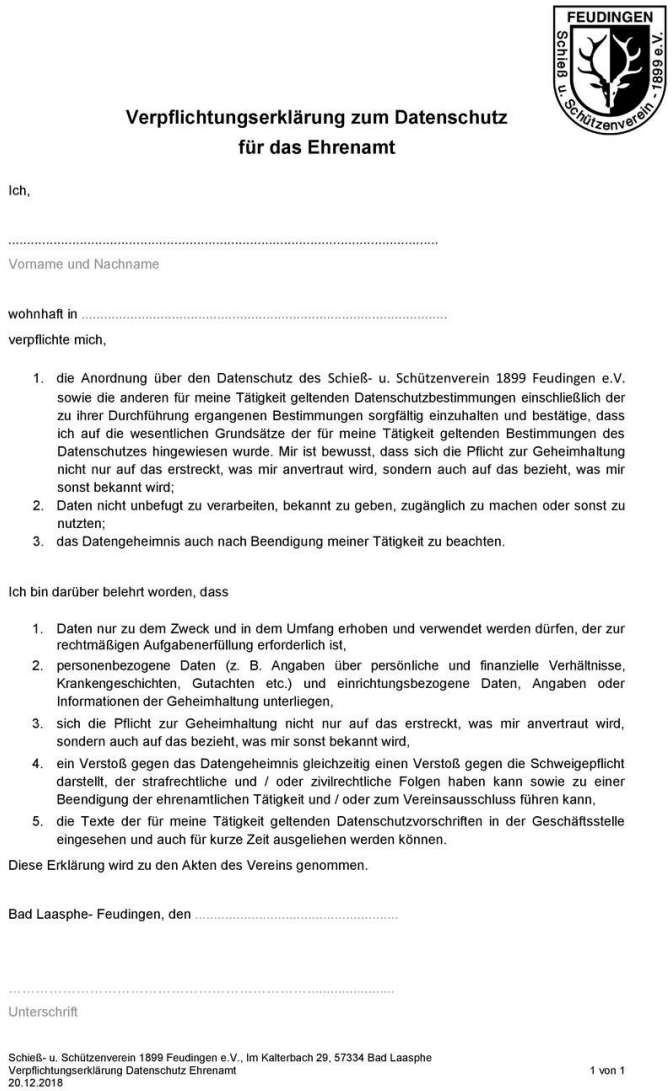
alle Mitarbeiter unterschreiben

Sicherheit der Datenverarbeitung

- Info aller Mitarbeiter (auch ehrenamtliche), die mit personenbezogenen Daten arbeiten
- Hinweis auf das IT-Sicherheitskonzept des Vereins zum sicheren Umgang
- **Umgang mit Gesundheitsdaten o.ä. erfordert besondere Beachtung!**

Muster-Datenschutzverpflichtung

- Datenschutzverpflichtung der Mitarbeiter muss nachweisbar sein, aber nicht zwingend schriftlich
  ➔ z.B. unterschriebene Teilnehmerliste mit Agenda
- Verantwortlich (i.d.R. der/die Vorsitzende) müssen die Einhaltung der Grundsätze nachweisen
  (Art. 5 Abs. 2 DSGVO)



Verpflichtungserklärung zum Datenschutz
für das Ehrenamt

Ich,

.....

Vorname und Nachname

wohnhaft in .....

verpflichte mich,

1. die Anordnung über den Datenschutz des Schieß- u. Schützenverein 1899 Feudingen e.V. sowie die anderen für meine Tätigkeit geltenden Datenschutzbestimmungen einschließlich der zu ihrer Durchführung ergangenen Bestimmungen sorgfältig einzuhalten und bestätige, dass ich auf die wesentlichen Grundsätze der für meine Tätigkeit geltenden Bestimmungen des Datenschutzes hingewiesen wurde. Mir ist bewusst, dass sich die Pflicht zur Geheimhaltung nicht nur auf das erstreckt, was mir anvertraut wird, sondern auch auf das bezieht, was mir sonst bekannt wird;
2. Daten nicht unbefugt zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzten;
3. das Datengeheimnis auch nach Beendigung meiner Tätigkeit zu beachten.

Ich bin darüber belehrt worden, dass

1. Daten nur zu dem Zweck und in dem Umfang erhoben und verwendet werden dürfen, der zur rechtmäßigen Aufgabenerfüllung erforderlich ist,
2. personenbezogene Daten (z. B. Angaben über persönliche und finanzielle Verhältnisse, Krankengeschichten, Gutachten etc.) und einrichtungsbezogene Daten, Angaben oder Informationen der Geheimhaltung unterliegen,
3. sich die Pflicht zur Geheimhaltung nicht nur auf das erstreckt, was mir anvertraut wird, sondern auch auf das bezieht, was mir sonst bekannt wird,
4. ein Verstoß gegen das Datengeheimnis gleichzeitig einen Verstoß gegen die Schweigepflicht darstellt, der strafrechtliche und / oder zivilrechtliche Folgen haben kann sowie zu einer Beendigung der ehrenamtlichen Tätigkeit und / oder zum Vereinsausschluss führen kann,
5. die Texte der für meine Tätigkeit geltenden Datenschutzvorschriften in der Geschäftsstelle eingesehen und auch für kurze Zeit ausgeliehen werden können.

Diese Erklärung wird zu den Akten des Vereins genommen.

Bad Laasphe- Feudingen, den .....

.....

Unterschrift

Schieß- u. Schützenverein 1899 Feudingen e.V., Im Kalterbach 29, 57334 Bad Laasphe
Verpflichtungserklärung Datenschutz Ehrenamt
20.12.2018

1 von 1

Quelle: www.ssv-feudingen.de

Fortschreibung

regelmäßige Updates

Regelmäßige Updates

- **Regelmäßiges Fortschreiben des IT-Sicherheitskonzeptes notwendig**
  - **Veränderte IT-Standards ➔ outdated Software**
  - **Prozesse im Verein ändern sich**
  - **Satzungsänderung**
  - **…**

Fragen bis hierher???

Praktische Tipps to go

- Wir sind alle betroffen!

Sicherer PC, Notebook

regelmäßige Zeit nehmen

Experten und Computerlaien

Top 5 Sicherheits-Maßnahmen

Aktuelle Software

Aktuelles Betriebssystem verwenden

➔ Windows 7 ist seit Januar 2020 abgekündigt!!!

"Grob fahrlässig"

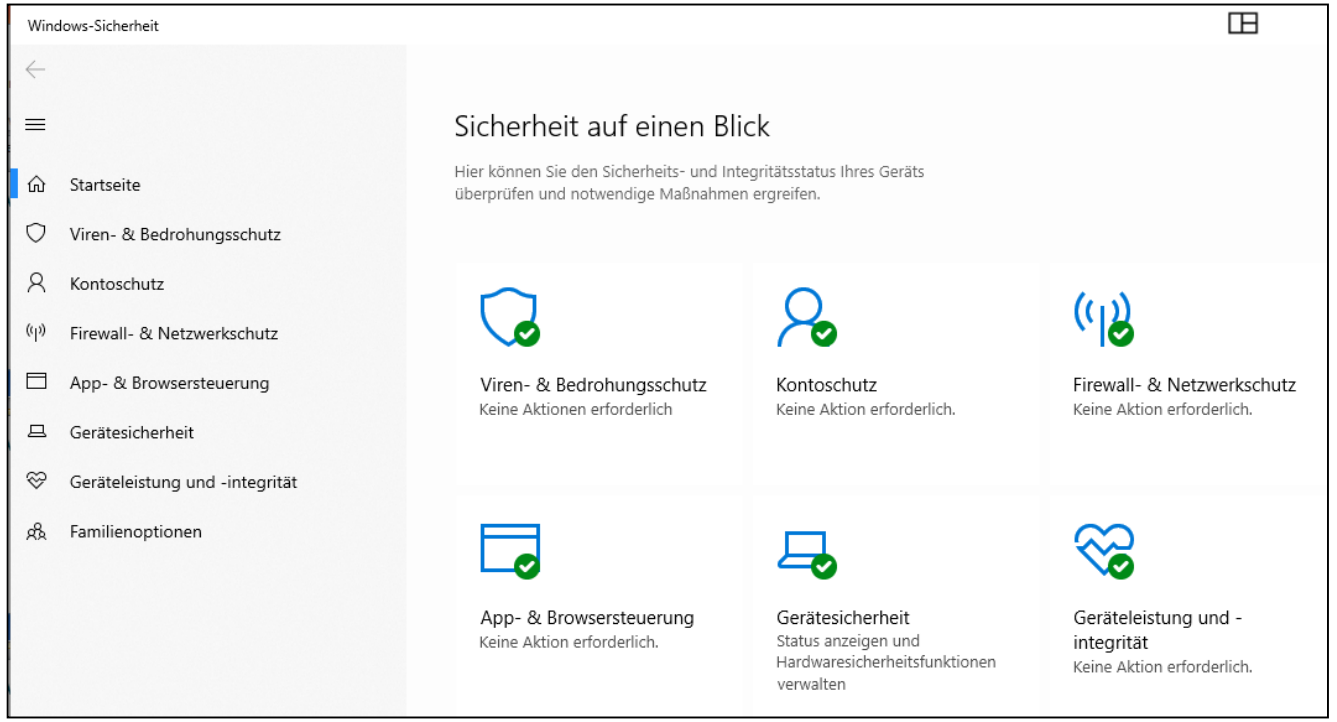
Millionen PCs laufen mit veraltetem Windows

Wer eine solche Nachricht angezeigt bekommen hat, sollte schleunigst handeln.
(Foto: picture alliance / NurPhoto)

Quelle: www.n-tv.de

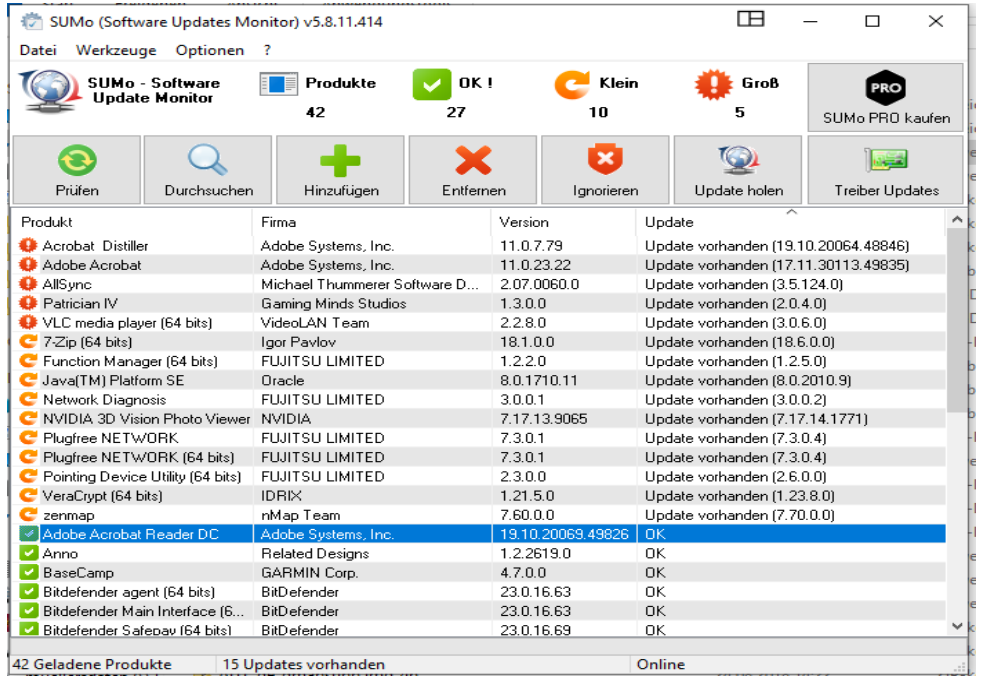
Geräte-Sicherheit

- Virenscanner immer aktuell
- Firewall aktivieren
- Regelmäßige Sicherheitskopien anlegen
  ➔ z.B. externe Festplatte



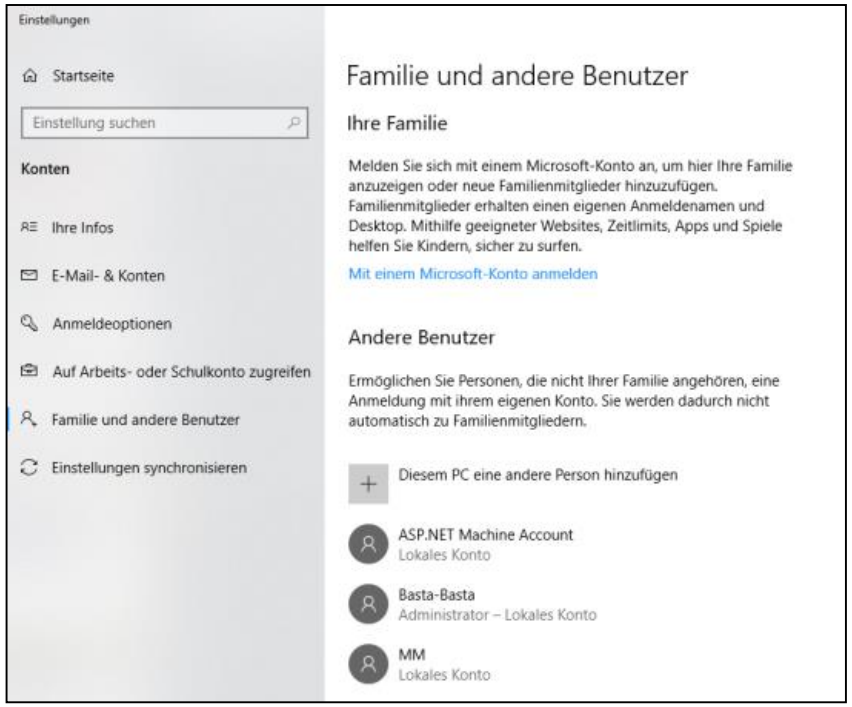
Aktuelle Software

- Software aktuell halten, speziell Browser
  ➔ SUMo (Software Update Monitor)
- Veraltete, unsichere und unbenutzte Software deinstallieren
- Daten/Software nur aus vertrauenswürdigen Quellen herunterladen



Eingeschränkten User anlegen

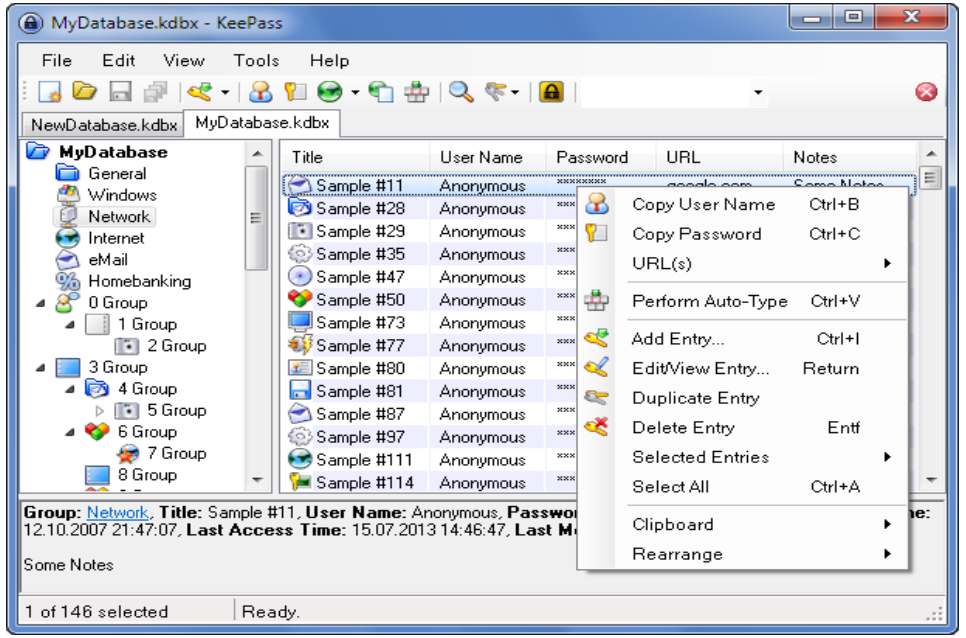
- Admin-Konto nur für administrative Zwecke nutzen
- Eingeschränkten User anlegen
  ➔ bei Mehrfachnutzung (Familie) separate Konten
- Für alle Konten komplexe Passwörter verwenden



Quelle: http://www.howtogeek.com/227763/how-to-completely-delete-your-microsoft-account/

Passwörter sicher verwalten

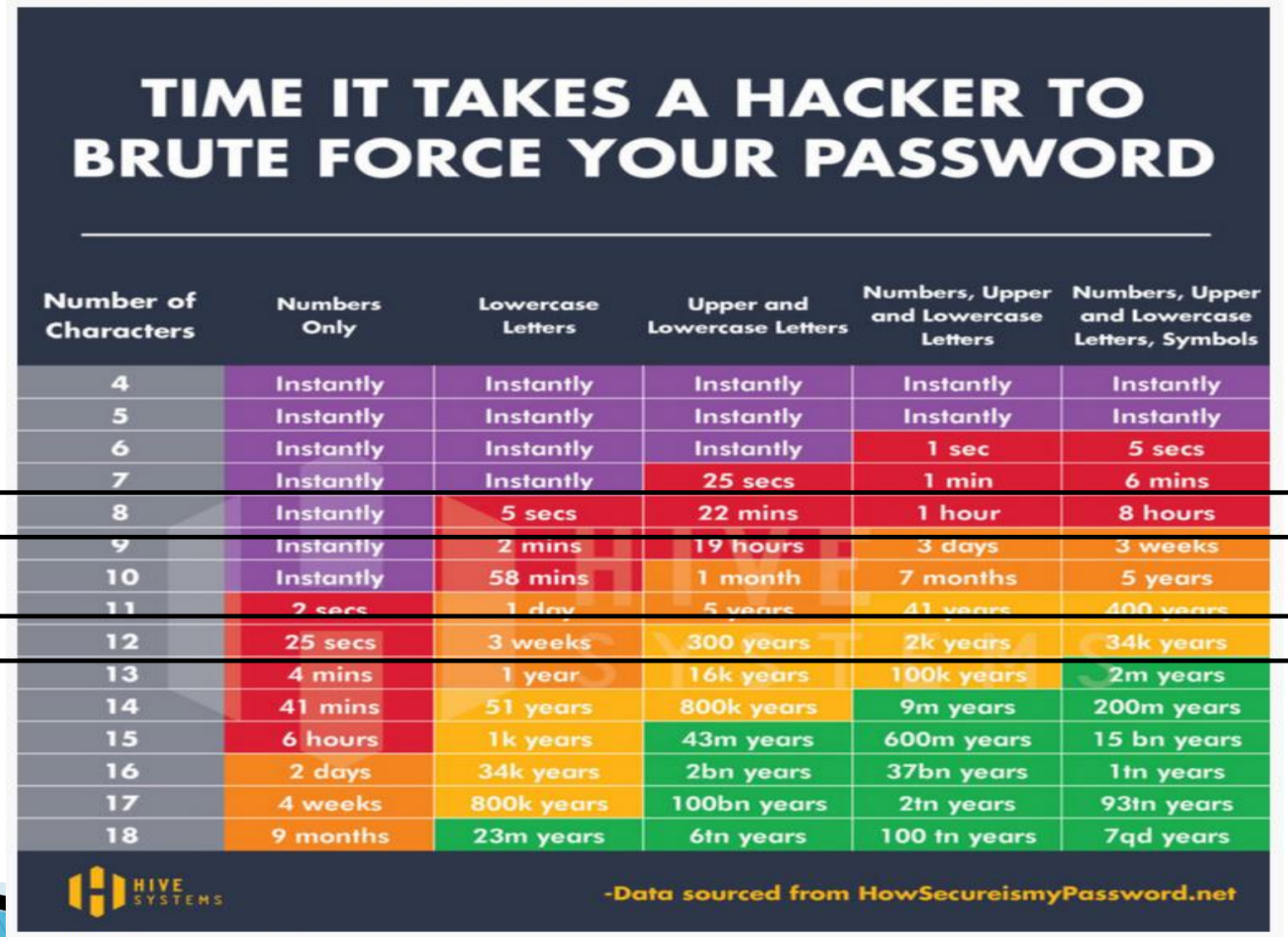
- **Passwörter nie unverschlüsselt speichern!!!**
- Empfehlung: KeePass oder anderer PW-Manager
- Verwaltungsprogramm für Zugangsdaten und andere sensible Informationen (Kreditkartendaten usw.)
- Erstellt auch selbst
  beliebig lange und komplizierte Passwörter
- Teilweise Browser-Integration möglich
- Auch für Handy verfügbar



Sichere Passwörter verwenden

- **Nicht zu simpel** – 12345678 / Passwort
- **Keine Namen** – Haustier / Spitznamen / Straßennamen
- **Buchstaben UND Ziffern** – Groß-/Kleinschreibung, wenn möglich **Sonderzeichen**
- **Eselsbrücken** – Anfangsbuchstaben von Sätzen oder gleich ganze Sätze verwenden
- **Länger ist sicherer** – mind. 12 Zeichen
- **Keine Notizen** – außer an einem sicheren Ort!
- **Möglichst nicht mehrfach benutzen** – für die wichtigen!
- **Ab und zu mal ändern** – für die ganz wichtigen (Mail, …)

Dauer für Passwort knacken



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

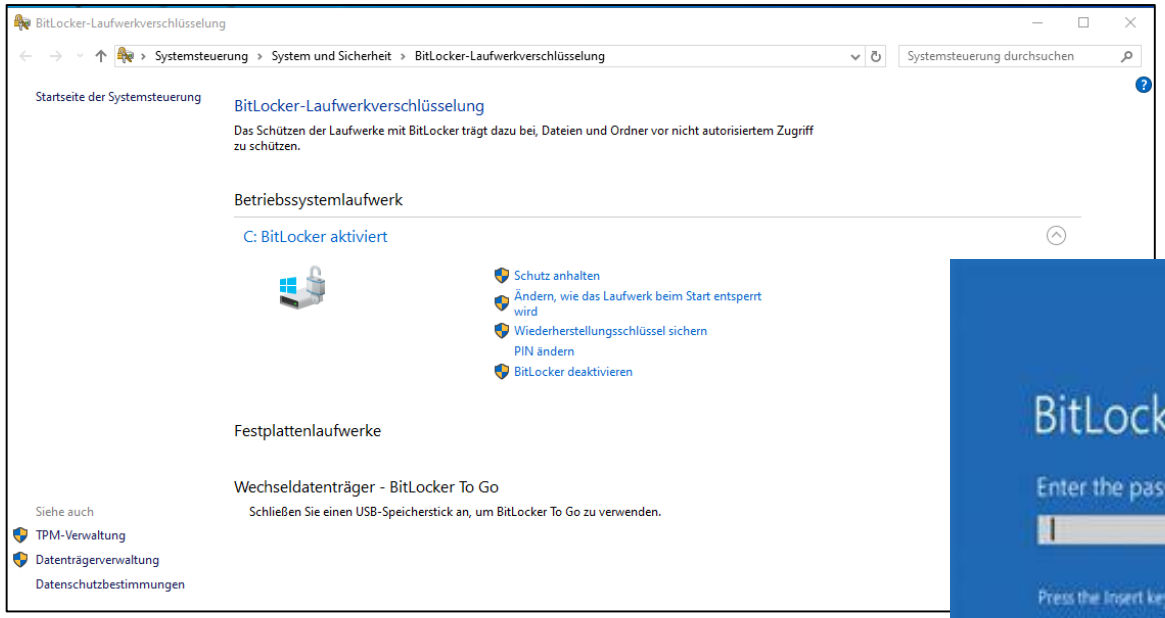
HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

Quelle: hivesystems.io/blog/are-your-passwords-in-the-green

PC verschlüsseln

- Bitlocker aktivieren (außer Windows Home)



https://support.microsoft.com/de-de/windows/aktivieren-der-geraeteverschluesselung

Sichere Kommunikation

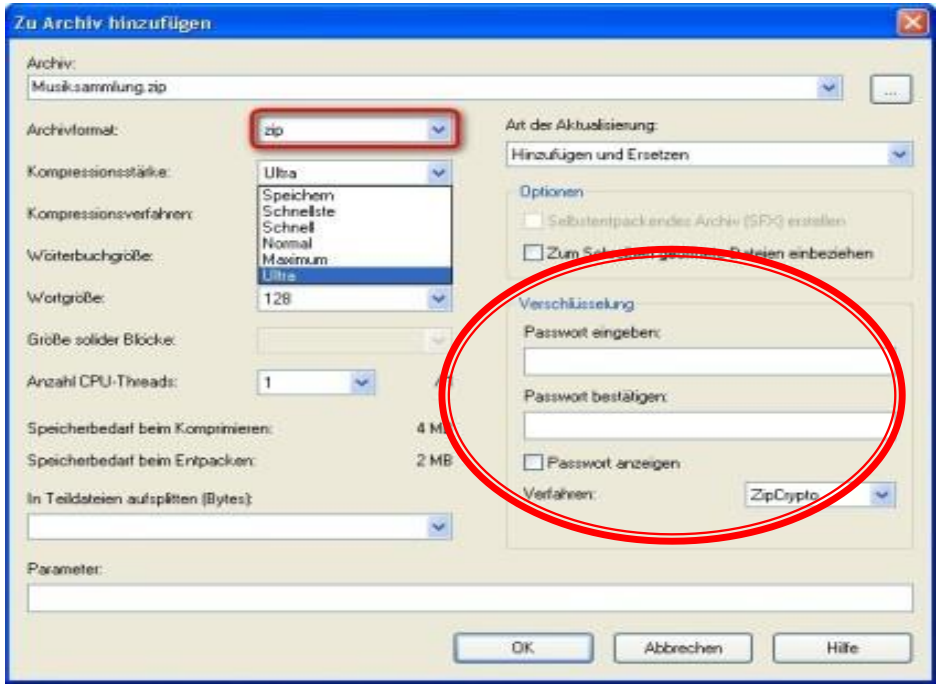
Daten sicher übertragen

Kommunikation mit E-Mail

- Sinnvoll sind Funktions-Mailadressen (Vorsitzender@tsv-musterstadt.de, Kassier@tsv-musterstadt.de, …)
- Bei Wechsel in der Vorstandschaft müssen keine neuen Mailadressen verteilt werden – nur Passwort ändern
- Zugriff auch auf ältere Informationen
- Trennung von privaten und Vereins-Infos

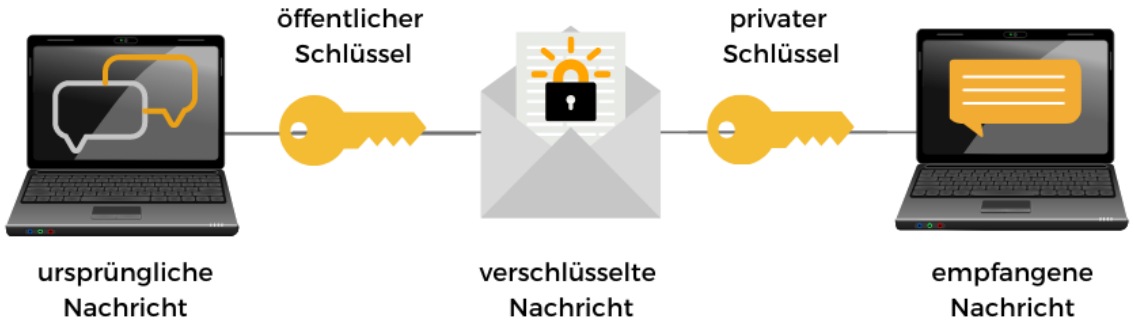
Schützenswerte Daten nur verschlüsselt versenden

- Empfehlung: 7-Zip
- Kann verschlüsselte Zip-Archive erstellen
- Diese können ohne 7-Zip auch mit anderen ZIP-Programmen geöffnet werden
- **Passwort muss auf gesondertem Weg übermittelt werden!!!**



Mail-Verschlüsselung

- E-Mail wie Postkarte – kann von jedem mitgelesen werden
- E-Mail-Verschlüsselung kostenlos und einfach zu installieren/bedienen
- Mailverschlüsselung: Schloss und Schlüssel



Wie funktioniert Mail-Verschlüsselung: https://www.youtube.com/

Erzeugen von PGP-Schlüsseln und Einbinden in das genutzte Mailprogramm Anleitung: https://praxistipps.chip.de/outlook-e-mails-mit-pgp-verschluesseln_29276

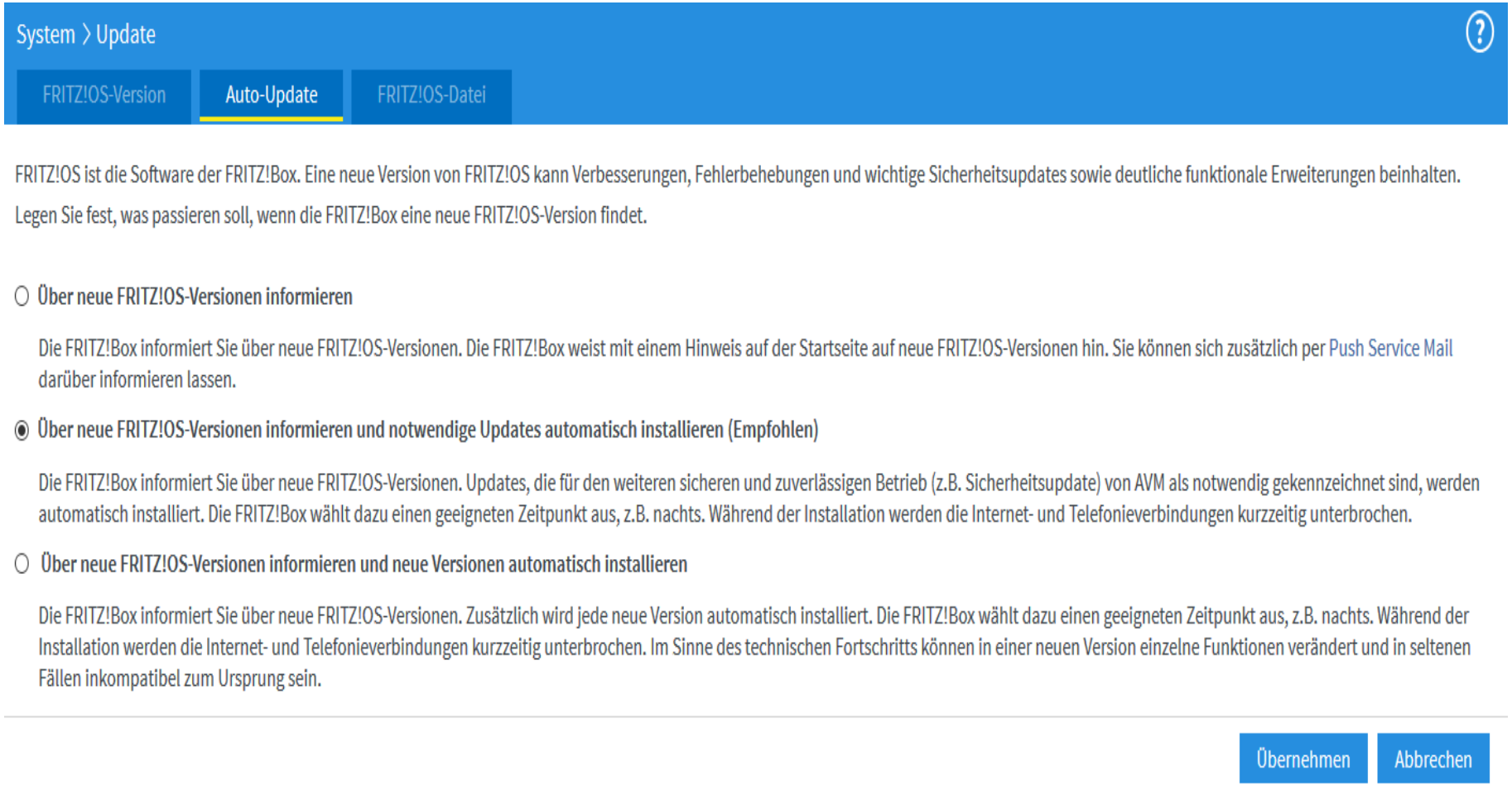
Sicheres Netzwerk

Vereins-WLAN

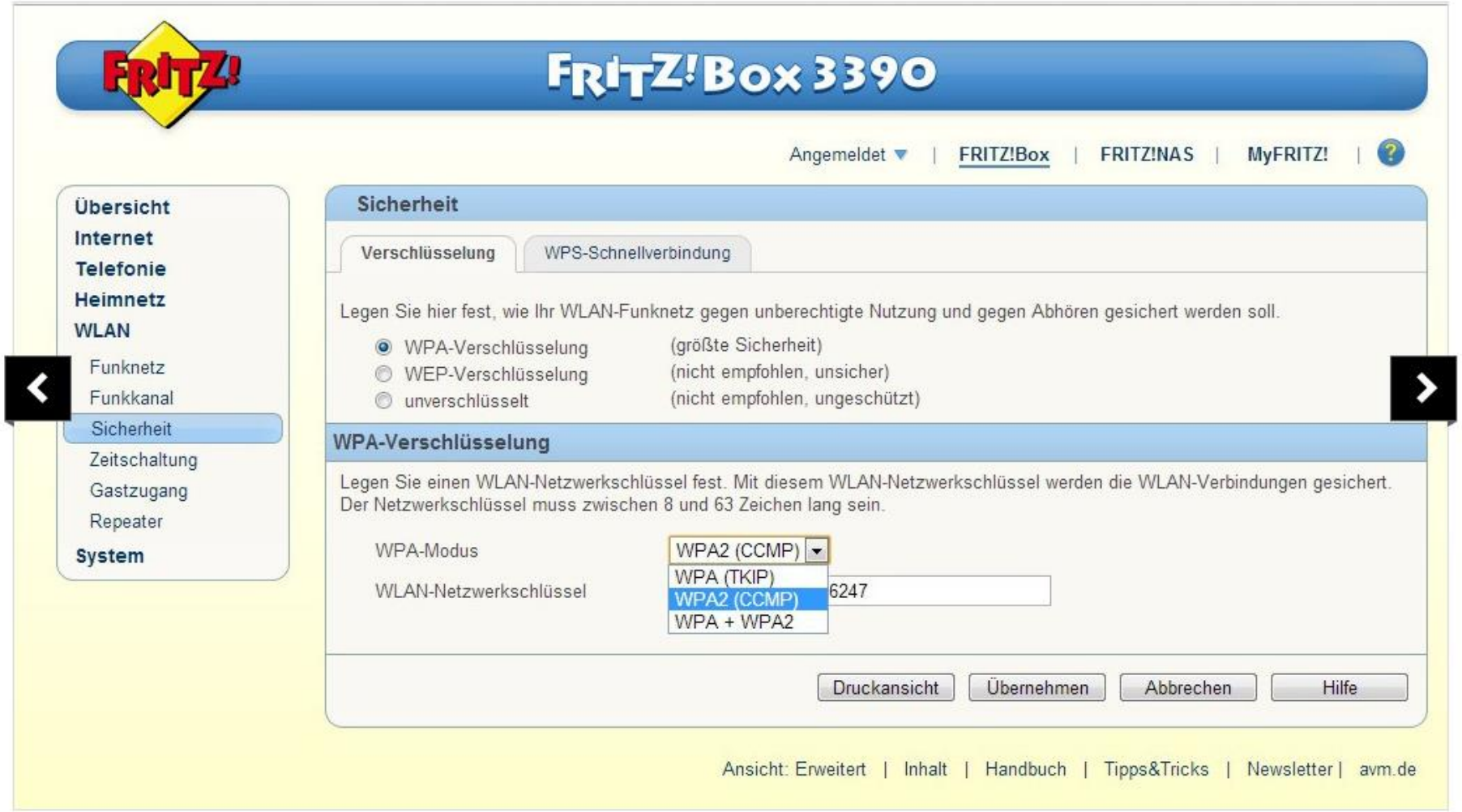
Router sichern – Passwort

Quelle: www.computerbild.de

Router sichern – Auto-Update



WLAN absichern – WPA2



Quelle: www.computerbild.de

Homebanking

- Aber bitte sicher …

Vereinskonto sicher führen

- Eigenes Vereinskonto anlegen
- Online-Banking über Lesezeichen starten oder besser eigene Bank-SW ➔ nie aus einer Mail
- Keine Passwörter oder PIN/TAN speichern
- 2-Faktor-Authentisierung für Online-Banking einrichten und nutzen
- Möglichst getrennte Geräte für Banking und TAN
- Sensible Daten nicht über öffentliche WLANs übertragen

Welches TAN-Verfahren?

- **Externe TAN-Generatoren** sind am sichersten
  ➔ getrennt vom Internet und ausschließlich für das Onlinebanking benutzt

- **pushTAN** am weitesten verbreitet
  ➔ bei richtiger Anwendung gutes Sicherheitsniveau
  (getrennte Geräte für Banking und TAN)

- Generell sind die in Deutschland angewendeten Versionen der TAN-Generierung sicher, solange die Nutzerinnen und Nutzer Banking und **TAN-Erstellung immer auf unterschiedlichen Geräten** durchführen

Quelle: www.bsi.de

Was war das noch alles?

- Ein schneller Überblick

Good to know – Sicher im Internet

1) Alle Software regelmäßig aktualisieren (nicht nur Windows!!!)
2) Aktuellen Web-Browser verwenden
3) Virenschutzprogramm und Personal-Firewall
4) Unterschiedl. Benutzerkonten anlegen (eingeschränkter User, Admin)
5) Unterschiedliche Passwörter verwenden und die wichtigsten regelmäßig ändern
6) Vorsicht bei E-Mails und deren Anhängen ➔ keine Links aus Mails öffnen!!!
7) Daten/Software nur aus vertrauenswürdigen Quellen herunterladen
8) Zurückhaltung bei der Weitergabe von persönlichen Daten
9) Wichtige Daten verschlüsseln
10) Regelmäßige Sicherheitskopien anlegen

www.bsi-fuer-buerger.de

Sicherheit geht alle an!

Danke für die Aufmerksamkeit!

Noch Fragen???

Und zum Schluss …

Es geht nicht um Angst zu schüren!

Bleiben Sie dem Ehrenamt treu!

Anhang

Meldung eines Vorfalls

- Beispiele:
  - USB-Stick mit Mitgliederdaten verloren
  - unverschlüsseltes Laptop mit personenbezogenen Daten im Zug vergessen
  - Großer Mailverteiler in CC
  - Hacker-Angriff
  - Schadsoftware
- Müssen der Aufsichtsbehörde und den Betroffenen gemeldet werden
- Meldung eines Vorfalles innerhalb von 72 Stunden
- Kontaktdaten griffbereit im Datenschutzordner

Meldestelle

Aufsichtsbehörde für Bayern

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Promenade 27, 91522 Ansbach

E-Mail: poststelle@lda.bayern.de

Telefon: 0981/53-1300