Datenschutz

Eine Checkliste für Vereine und Verbände

Wesel, 2017-11-11 - Tiemo Krüger

tiemo.krueger@gmx.de

Vorbemerkung

- Dies ist keine Rechtsberatung und ersetzt keine Rechtsberatung.
- Diese Präsentation hat keinen Anspruch auf Vollständigkeit.
- Gesetze und deren Anwendung ändern sich im Laufe der Zeit.

Einführung - Daten

- Was sind personenbezogene Daten?

  z.B.:

  - Name und Adressen, Geburtsdatum, Telefon ...
  - Standort und Bewegungsdaten …
  - Bilder, Unterschriften, Atteste …
  - Kontodaten
  - Zugangsdaten (eMail, Username, Passwort)
  - IP-Adressen und Uhrzeiten

App-Entwicklung:
Speichert bitte nur „Hashes“ der Passwörter mit einem angemessenen „Salt“, nie die Passwörter selbst.

- Achtet grundsätzlich auf Datensparsamkeit!
  - Entscheidet bei allen erhobenen Daten, ob ihr sie wirklich benötigt.

Datenschutzbeauftragter

- Benötigen wir einen Beauftragten?
  - Ein Datenschutzbeauftragter ist dann zu bestimmen, sobald **mehr als neun Personen** die Daten der Vereinsmitglieder erheben, verarbeiten oder nutzen. Hierbei spielt es **keine Rolle**, ob es sich dabei um Angestellte, freie Mitarbeiter, Voll- oder Teilzeitbeschäftigte, Auszubildende, Leihpersonal, ehrenamtliche Mitarbeiter oder Mitarbeiter von externen Dienstleistern handelt.

  - Einen Datenschutzbeauftragten **müssen** Vereine bestellen, die in der Regel mehr als vier Arbeitnehmer mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigen (§ 4 f Absatz 1 Satz 1,3 BDSG).

Datenschutzbeauftragter

- Benötigen wir einen Beauftragten?
  - Ein Datenschutzbeauftragter muss immer bestellt werden, wenn besonders sensible Daten genutzt werden!
    - Das sind z.B. Gesundheitsdaten eines Mitglieds!
    - Oder im Verein gibt es Videoüberwachung!
    - Oder Türschlösser mit biometrischer Überprüfung – Fingerabdrücke!
  - Der Datenschutzbeauftragte kann ein Vereinsmitglied sein. Auch ein externes Unternehmen oder eine Einzelperson kann zum Datenschutzbeauftragten bestellt werden.

Datenschutzbeauftragter

- Welche Aufgaben hat der Beauftragte?

  Unter anderem:

- Wie sieht ein datenschutzgerechtes Antragsformular inkl. Einwilligungsklausel aus?
- Welche Daten darf ein Verein gemäß seiner Satzung von seinen Mitgliedern erheben?
- Wie sieht die Datenschutzerklärung in der Vereinssatzung aus?
- Wann darf ein Verein die Mitgliedsdaten an Dachorganisationen und vereinsnahe Organisationen weitergeben?
- Wann darf ein Verein die Mitgliedsdaten an Sponsoren weitergeben?
- Wann darf ein Verein die Mitgliedsdaten an die Presse weitergeben?

Datenschutzbeauftragter

- Welche Aufgaben hat der Beauftragte?

  Unter anderem:

- Darf ein Verein Telefonnummern seiner Mitglieder sammeln?
- Wann dürfen Mitgliedsdaten im Internet veröffentlicht werden?
- Wann dürfen Mitgliedsdaten im in Aushängen und Vereinspublikationen veröffentlicht werden?
- Wann dürfen Mitgliederdaten an andere Vereinsmitglieder übermittelt werden?
- Wann dürfen Mitgliederdaten an Versicherungsunternehmen im Rahmen von Gruppenversicherungsverträgen weitergegeben werden?
- Dürfen sportgerichtliche Entscheidungen im Internet veröffentlicht werden?

Datenschutz

- Wie arbeitet eine Datenschutzbeauftragter (DSB)?

- **Der DSB löst NICHT eure Probleme!**
- Er analysiert die aktuellen Fälle in denen Daten genutzt werden.
- **Er zeigt Lücken und Probleme auf** und empfiehlt gegebenenfalls Gegenmassnahmen.
- Für die Ausführung/Umsetzung sind jedoch immer Vorstände, Mitarbeiter und Ehrenamtliche zuständig.
- Werden neue Arbeitsprozesse eingeführt, so ist in der Planung der DSB mit einzubeziehen und seine Einwände sind zu berücksichtigen.
- **Verantwortlich bleibt IMMER der Vorstand nach BGB.**

Datenschutz

- Wo werden meine Fragen weiter beantwortet?

  Auf den Webseiten der Landes-Datenschutzbeauftragen gibt es meist spezielle Informationen für Vereine, z.B.:

- https://www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein/ Sehr aktuell!
- https://www.lfd.niedersachsen.de/themen/vereine/datenschutz-im-verein-56043.html
- https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Vereine/Inhalt/Datenschutz_im_Verein/Datenschutz_im_Verein1.pdf

Datenschutz

- Wie arbeiten wir, wenn wir keinen Datenschutzbeauftragten (DSB) haben/benötigen?

- **Wir beachten alle Gesetze und Regelungen im gleichen Maße!**
- Natürlich gelten die Gesetze für alle und immer.
- Es sind trotzdem alle Regeln zum Schutz der Daten umzusetzen.

Datenschutz-Praxis

- Anmeldung/Eintritt des Mitglieds
- Auf dem Anmeldeformular sind die Daten nach notwendigen und optionalen Daten zu trennen.
- Die notwendigen Daten wie Name, Adresse, Geburtsdatum benötigen keine Datenschutzbestimmung (abgedeckt durch BDSG §28).
- Die Datenschutzbestimmung für optionale Daten oder die Veröffentlichung im Internet muss auf dem Formular deutlich abgesetzt oder auf einem separaten Blatt (extra unterschrieben) mitgeteilt und akzeptiert werden!
- Geburtsdatum nur erfassen, wenn zum Beispiel für Altersklassenzuordnung notwendig!
- Die Daten dürfen jeweils nur für den unmittelbar genannten Zweck genutzt werden.
- Eltern unterschreiben zusätzlich bei Kindern!

Datenschutz-Praxis

- Meldung an LKVs/DKV und Landessportbünde
- Hier ist die Übermittlung durch BDSG §28 abgedeckt, wenn:

- Die Daten ummittelbar für die Vereins-/Verbandsorganisation notwendig sind, wie z.B. das Ausstellen des DKV-Ausweis.

- Für statistische Erhebungen der Verbände dürfen nur anonymisierte Daten erhoben werden.

Datenschutz-Praxis

- Vereins-/Verbandsverwaltung
- Auf welchen Rechnern werden diese eingesetzt?
- Sind diese Rechner verschlüsselt? -> Windows Pro mit Bitlocker!
  - Auch wenn das Programm die DS-Richtlinien erfüllt! Warum?
  - Bei Datenexporten enstehen Dateien ausserhalb des Programms!
  - Angriffe können eingeschränkt werden.
- Wer hat Zugriff auf diese Rechner? Zugang beschränken!
  - Familienmitglieder dürfen keinen Zugriff bei privaten Rechnern haben!
  - Bei Vereinsrechnern sind die Berechtigungen ebebnfalls ainzuschränken!
- Virenschutz – Gegen Datendiebstahl und Datenverlust
  - Setzt aktuelle Virenschutzprogramme ein
- Verpflichtung
  - Lasst Eure Mitarbeiter/Ehrenamtliche eine Verpflichtung hierzu und zum Datenschutz unterschreiben. Verpflichtet sie zur Einhaltung
- Beendigung einer Mitarbeit
  - Scheidet ein MA aus, so ist dafür zu sorgen, dass er/sie keinen Zugriff mehr auf die Daten hat!

Datenschutz-Praxis

- Nutzung von PCs/Notebooks/Smartphones
  - Auch andere Mitarbeiter/Ehrenamtliche erhalten Daten, z.B. Mitgliederlisten oder ähnliches oder verarbeiten Mitgliedsdaten innerhalb ihrer Sparte wie Atteste, Fotos, Anti-Doping-Erklärungen…
  - Wie müssen Geräte hierbei und bei der Vereinsverwaltung genutzt werden?

- Geräte immer verschlüsseln und immer mit User/Passwort oder „Pin“ freischalten/booten.
  - Windows Pro: BitLocker, MacOS: FileVault, Linux: LUKS, iOS: Version >=7, Android: Version >= 6.0
  - Bitte stellt sicher, dass die Verschlüsselung auch eingeschaltet ist!
- Datensicherungen ebenfalls nur auf verschlüsselten Datenträgern!
- Übertragung von unverschlüsselten Dateien nur auf sicheren Wegen:
  - Über SSH-Verbindungen, HTTPS-Webseiten
  - Nicht über FTP, HTTP!

Datenschutz-Praxis

- Kommunikation
  - Wir müssen kommunizieren! Wie tauschen wir Daten sicher aus?
- Daten verschlüsseln!
  - z.B. mit PGP / GPG, dies sind offen erhältliche Programme.
  - Keine unsicheren Methoden verwenden:
  - ZIP Datei mit Passwort ist nicht sicher!
  - Word/Excel Datei mit Passwort ist nicht sicher!
- Ist eMail-Made-in-Germany sicher?!
  - Nur innerhalb des Verbunds wird mit TLS-Mandatory verschickt!
  - NEIN, ihr wisst nicht, ob ein Empfänger eMails zu unsicheren Anbietern weiter leitet.
- Einstellung im eMail-Programm:
  - Achtete darauf, dass die Konteneinstellung zum Abruf und Senden auf TLS, StartTLS oder SSL steht
- Webmailer:
  - Greift nur über https-Verbindungen auf Webmailer zu

Datenschutz-Praxis

- Papier – sind das Daten oder nicht?!
  - Häufig wird erzählt, dass ausgedruckte Dokumente oder handschriftliche Listen nicht unter den Datenschutz fallen!
  - Grund: Etliche Gesetze beziehen sich auf digitale Daten.
  - Die Rechtsprechung sieht das durchweg anders und behandelt Daten immer gleich!
  - Insbesondere wenn Daten zur späteren Verarbeitung auf einem Rechner gesammelt werden oder ausgedruckt verbreitet werden.

- Welche Daten zählen dazu?
  - Natürlich die Listen/Daten, die der Verein einem MA zur Verfügung stellt, z.B. eine Teilnehmerliste eines Kurses.
  - Aber auch Listen, die ein MA erstellt, z.B. eine Anwesenheitsliste.
  - Aber auch interne Daten, z.B. eine Liste mit Daten zur Kommunikation innerhalb eine Gruppe, z.B. eines Kurses (eMail/Telefon)
  - Diese dürfen nie Personen zugänglich gemacht werden, die sich nicht im zugestimmten Verteiler befinden!
  - Alle Personen, denen diese Liste zugänglich ist, sollten mit einem entsprechenden Hinweistext auf der Liste und ihrer Unterschrift zur Geheimhaltung verpflichtet werden.
  - Unabhängig davon gelten die Gesetze trotzdem!

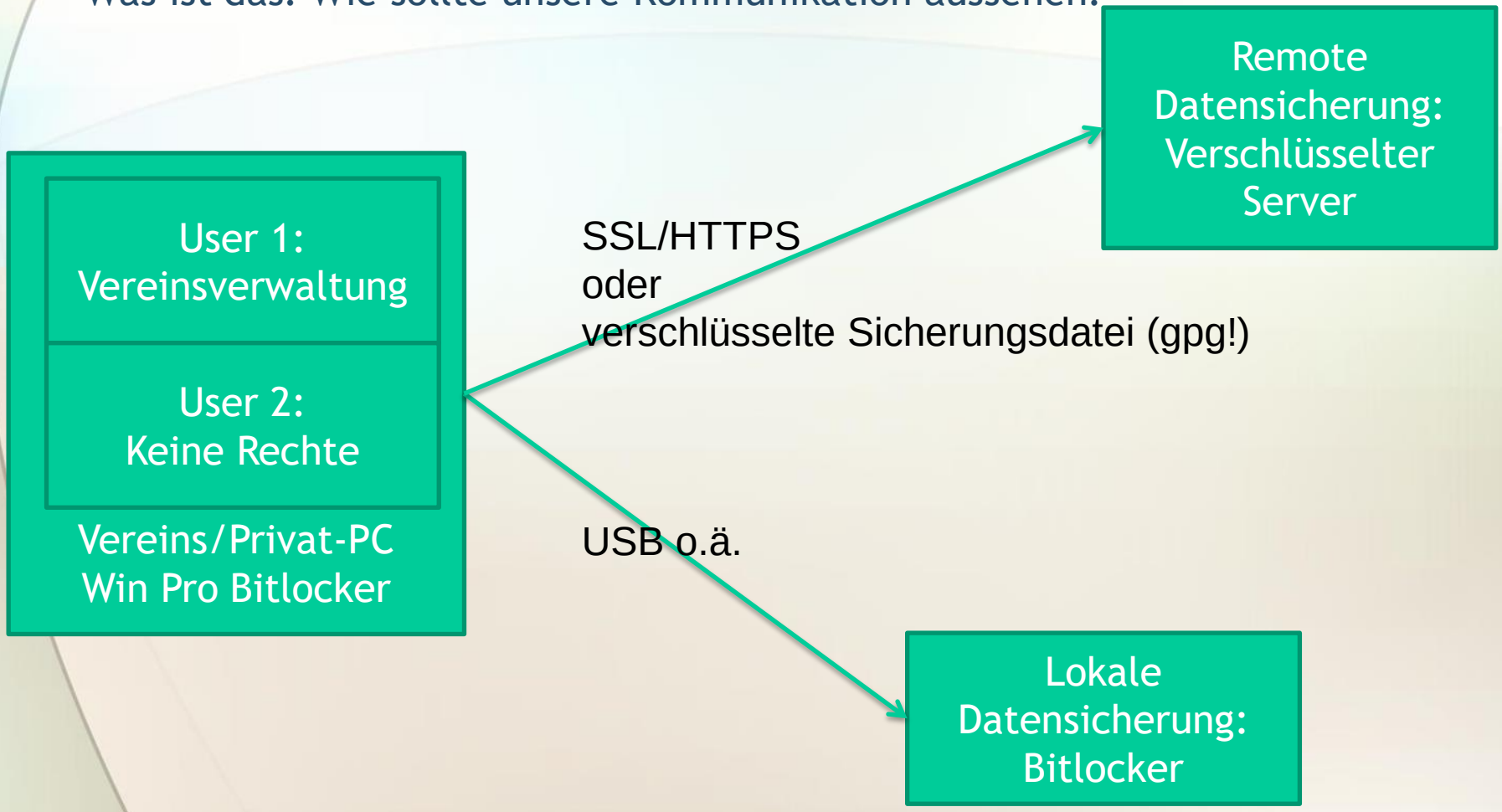
Datenschutz-Praxis

- Messenger
  - Wir benutzen heute alle Messenger wie WhatsApp, doch welche sind wie sicher?

- Welche Messenger sollte ich benutzen?
  - WhatsApp bietet inzwischen Ende-zu-Ende Verschlüsselung, für den normalen Gebrauch sicher, aber nicht ausreichend für Datenaustausch, da nicht ausreichend dokumentiert.
  - Telegram bietet keine standardmäßige Ende-zu-Ende Verschlüsselung, daher ist wegen der Gefahr von Einrichtungsfehlern hier abzuraten.
  - Threema ist vermeintlich sicher. Leider legt der Anbieter wichtige Punkte nicht offen, daher kann Threema nicht als sicher betrachtet werden.
  - Signal legt Quelltext und Architektur offen, hier ist von einer durchgängigen Sicherheit auszugehen! Derzeit der sicherste Messenger und zur Kommunikation von Daten ausreichend!

Datenschutz-Praxis

- Chain-of-Trust
- Was ist das? Wie sollte unsere Kommunikation aussehen?



Datenschutz-Praxis

- Chain-of-Trust
- Was ist das? Wie sollte unsere Kommunikation aussehen?

Datenschutz-Praxis

- Chain-of-Trust
- Was ist das? Wie sollte unsere Kommunikation aussehen?

USB-Stick:
verschlüsselte Datei (gpg!)
oder
verschlüsseltes Medium
(Bitlocker oder LUKS)

Datenschutz-Praxis

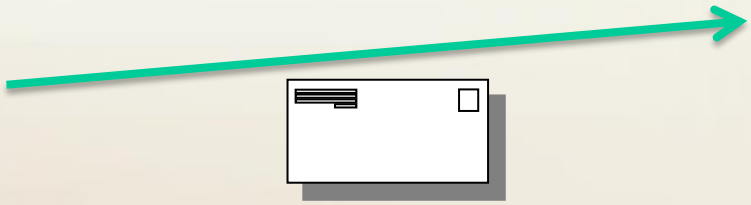
- Dropbox, Google-Drive, iCloud, OneDrive…
- Daten werden auf Cloud-Speichern abgelegt.

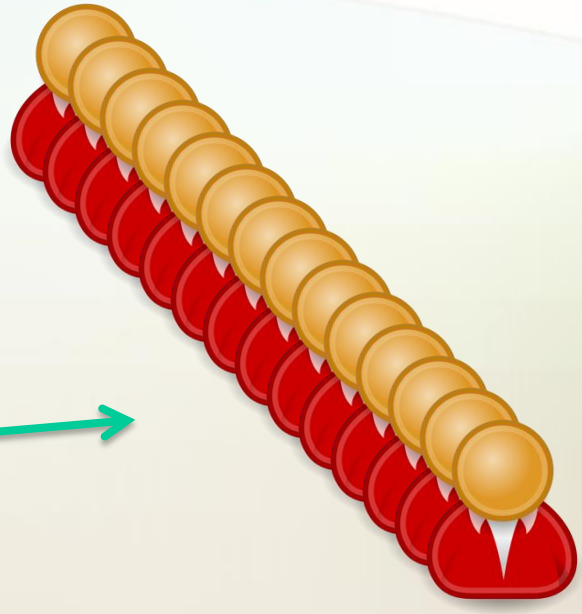
- Grundsätzlich können diese Dienste kritisch sein und bekommen keine Empfehlung!
- Benutzt nur europäische oder deutsche Anbieter!
- Bei den o.g. internationalen Anbietern immer mit einem deutschen Account über eine deutsche Seite des Anbieters anmelden.
- Immer im Kleingedruckten Ausnahmen kontrollieren!

Datenschutz-Praxis

- Newsletter und andere Rundschreiben
- typischerweise per eMail versandt

Die Empfänger einer solchen eMail werden in das Empfänger-Feld: BCC eingetragen!



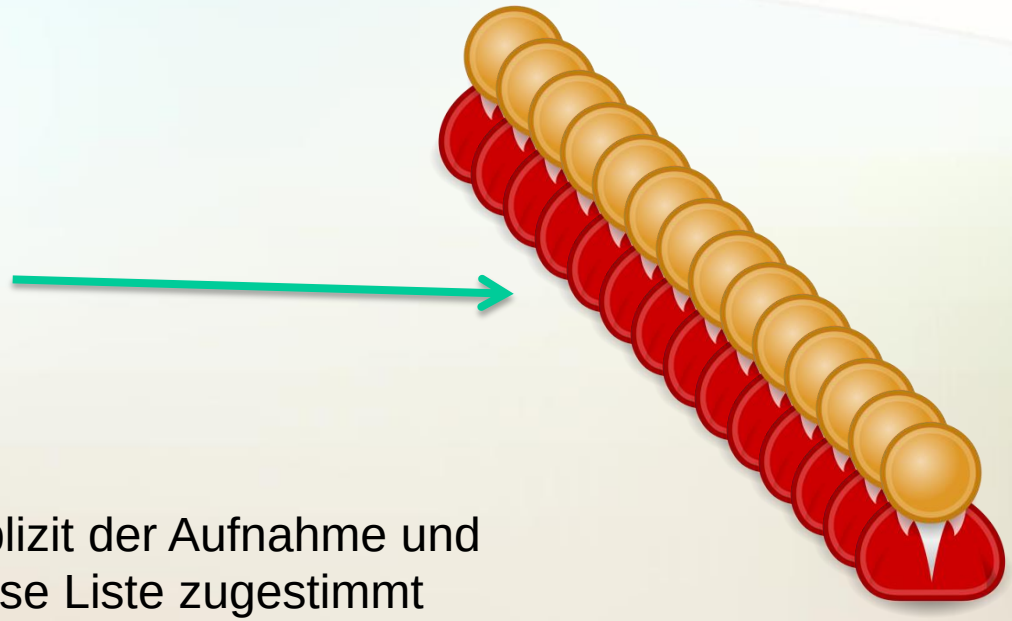


BCC steht für „Blind Carbon Copy“, andere Empfänger dieser eMail können diese Empfänger nicht in der Email sehen!

Datenschutz-Praxis

- Mitgliederlisten, Kontaktlisten an Mitglieder
- Für die Organisation des Austauschs

Der Verein veteilt
eine Liste zur Kontakt-
aufnahme untereinander
an die Mitglieder:



Nur Mitglieder, die explizit der Aufnahme und Veröffentlichung in diese Liste zugestimmt haben, dürfen hier auftauchen!

Datenschutz-Praxis

- Die Daten verlassen nie die Chain-of-Trust!
- Passworte sind hart genug!
- Passworte und Überprüfungen zu Schlüsseln werden IMMER auf separatem Weg ausgetauscht/geprüft!
- Ausgeschiedenen Benutzern werden Rechte entzogen!

dkv-datenbank.de

- Datenschutzbestimmung kommt hier vom DKV.
  - Daten NICHT zusätzlich im Verein auf Rechnern verwalten, nur die Hardcopies im Verein sicher ablegen (verschlossenes Vorstandsbüro).
- Anlegen eines neuen Sportlers:
  - Sportler immer zuerst das separat ausgefüllte Formular (Download auf der Seite) unterschreiben lassen. Eltern bei Minderjährigen zusätzlich!
  - Erst dann den Sportler im System anlegen! Atteste nach Jahresfreischaltung des Sportlers löschen!
  - Die Vorgehensweise in der Datenbank einen Sportler anzulegen und dann das vorausgefüllte Formular auszudrucken, ist rechtlich NICHT OK!
  - Keine Bilder hochladen.
  - Vereinsadresse statt Privatadresse des Sportlers angeben.

Sportveranstaltungen

- Anmeldung von Sportlern: Datenübermittlung an Dritte

  - Dies ist evtl. durch den Zweck des Vereins abgedeckt: „ … und die Teilnahme an Sportveranstaltungen …“
  - Evtl. kann auch durch den grundsätzlichen Beitritt und den damit geschlossenen Rechtsvertrag das Vorhaben zur Teilnahme an Veranstaltungen implementiert werden UND
  - Die übermittelten Daten gehören typischerweise zu den Pflichtdaten. Daraus lässt sich wieder §28 BDSG herleiten.

  - Zur Sicherheit sei bei den Pflichtdaten im Beitrittsformular ein abgesetzter Hinweis empfohlen, z.B.
  - „Die obigen Daten werden zur Vereinsverwaltung und zur Teilnahme am Sportbetrieb und an Veranstaltungen genutzt.“

Eigene Berichterstattung

- Ergebnisse/Berichte im Internet
  - Ergebnisse/Ergebnislisten sind durch BDSG §28 abgedeckt.

- Fotos im Internet
  - Primar gelten hierzu die Regeln zum „Recht am eigenen Bild“.
  - Dies ist primär eine Medienthema, hier gelten primär das KunstUrhG, StGB und BGB.
  - Fotos von Veranstaltungen sind grundsätzlich zulässig.
    - Das gilt auch für Kinder!
    - Dabei muss sich der Bildinhalt auf die Veranstaltung beziehen.

Eigene Berichterstattung

- Adressen/Geburtstage im Internet
  - Innerhalb kleiner Vereine oder wenn im Zweck noch Begriffe wie „Geselligkeit“ auftauchen, sind diese Listen teilweise erlaubt.
  - Veröffentlichungen in Vereinszeitungen im Internet fallen nicht mehr unter diese Erlaubnis.
- Vereinszeitungen (PDF …) im Internet
  - Achtet auch hier auf die Mitgliedsdaten
  - Was innerhalb eines kleinen Vereins O.K. sein kann:
    - Kontaktdaten
    - Geburtstagsliste, Jubiläen

    hat im Internet ohne Zustimmung nichts zu suchen, deshalb vor Veröffentlichung des PDFs im Internet schwärzen oder Seiten entfernen!

Löschen von Daten

- Irgendwann sind Daten nicht mehr notwendig
  - Ein Mitglied verlässt den Verein.
    - Daten löschen, sobald alles geregelt ist
  - Backups sind überholt.
    - Löschen oder vernichten
  - Datenträger werden aussortiert.
    - Löschen oder vernichten
  - Rechner werden verkauft/verschrottet.
    - Festplatten löschen oder vernichten
- Setzt Löschfristen und dokumentiert diese
  - z.B. auf der ersten Vorstandssitzung nach der Hauptversammlung wird ein Löschprotokoll abgearbeitet.
  - In diesem vermerkt ihr vorher welche Daten es wo gibt und welche Fristen hier gesetzt sind.

Löschen von Daten

- Wie lösche ich richtig?
  - Festplatten (HDD)
    - Einmal komplett überschreiben reicht für den normalen Gebrauch.
    - Mehrfaches Überschreiben ist für unseren Gebrauch nicht notwendig.
  - USB-Sticks, SSDs
    - Einmal komplett überschreiben reicht für den normalen Gebrauch.
    - Daten werden hier zwar beim Überschreiben im Vergleich zur HDD direkt unlesbar gemacht, aber Flash-Speicher Technologien haben häufig (temporär) ungenutzte Bereich, auf denen Daten theoretisch in seltenen Fällen erhalten bleiben. Risiko: gering
  - Ich bin mir nicht sicher!
    - Frag jemanden, der sich auskennt
    - Beauftrage einen Fachbetrieb für Datenvernichtung
    - Zerstöre den Datenträger mit sinnloser Gewalt… ;-)

Webseiten und Web-Applikationen

Prolog


SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

SPORT Schlagzeilen | Wetter | DAX 10.630,12 | TV-Programm | Abo

Nachrichten > Sport > Sonstiges > Doping > Robert Harting und Christina Obergföll: Wada-Hack betrifft auch deutsche Sportler

Attacke auf Wada-Account

Daten von Harting und Obergföll gehackt

Die russische Hackergruppe "Fancy Bears" legt nach: Sie hat die Namen von 25 Sportlern veröffentlicht, die bei der Antidoping-Agentur Ausnahmegenehmigungen beantragt haben. Darunter sind prominente Deutsche.

- 150-300 Millionen Userdaten werden jedes Jahr gehackt.
- Kleine Firmen in Deutschland mussten im letzten Jahr im Schnitt 10-15 T€ für Anwälte und Absicherung nach einem erfolgreichen Hack ausgeben. Vereine sind von der Größe vergleichbar.
- Auch im Kanusport wurden im letzten Jahr mehrere Angriffsvektoren gefunden!

Einführung - Rechtslage

- Auszug aus TMG §13
- Diensteanbieter haben(…) sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist.

- Diese (Einrichtungen)
  a)gegen Verletzungen des Schutzes personenbezogener Daten und
  b)gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind.

- Vorkehrungen (…) müssen den Stand der Technik berücksichtigen.
- Eine Maßnahme (…) ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Einführung - Rechtslage

- Wichtige Gesetze
  - TMG - Telemediengesetze

    Insbesondere
    - §§ 5,6 – Info-Pflichten: Impressum/Verantwortliche
    - §§13,15 – Verwendung und Verschlüsselung der Daten
    - §15a Meldung, wenn Dritte unberechtigt Daten erlangen

  - BDSG – Bundesdatenschutzgesetz

    Insbesondere
    - §§4, 4g – Datenschutzbeauftragter
    - §34 – Auskunft an Betroffene
    - §42a – Meldung, wenn Dritte unberechtigt Daten erlangen

Einführung - Erwartung

- Webseiten, Social Media, Apps, Foren und viele andere digitale Kommunikationsformen nutzen personenbezogene Daten.
- In der Vereinsverwaltung werden Daten erhoben.
- Grundsätzlich sind diese Daten als schützenswert anzusehen.
- Ein User hat grundsätzlich die Erwartung und das Recht, dass diese Daten geschützt werden.

Checkliste

- Die folgenden Punkte sollten geprüft und im Zweifel umgesetzt werden.
- Detaillierte Informationen zu den einzelnen Themen findet Ihr auch im Internet, eine gute Quelle ist zum Beispiel: https://www.e-recht24.de/

Standort des Servers?

- Ihr betreibt eine Webseite?
  - Steht der Server in der EU?
    (Das erfahrt ihr bei Eurem Anbieter)
    - Ja: Damit fällt er unter den EU-Datenschutz. ✓
    - Nein: Der Server steht nicht in der EU. ✘
  - Gegenmassnahme:
    - Die Webseite zu einem anderen Anbieter umziehen!

Impressum und Datenschutzerklärung

- Überprüft Euer Impressum auf Vollständigkeit
  - https://www.e-recht24.de/impressum-generator.html ✓
- Fügt eine Datenschutzerklärung ein!
  - https://www.e-recht24.de/muster-datenschutzerklaerung.html ✓

Muss ich meine Webseite verschlüsselt übertragen?

- Häufig werden Webseiten verschlüsselt mit dem https-Protokoll übertragen, muss ich das auch?

- Nein, prinzipiell ist das für eine normale Webseite nicht zwingende notwendig. ✓
- Notwendige Ausnahmen werden im Folgenden erläutert.
- Grundsätzlich kann eine Umsetzung empfohlen werden.
- Weitere Infos siehe Anhang

Verwendet Ihr Cookies?

- Nein, 100% nicht! ✓
- Ich bin nicht sicher. ✘
- Wir verwenden ein CMS (z.B. Joomla, Wordpress). ✘
- Wir verwenden plugins von facebook, Wetter oder ähnliches. ✘
- Ja! ✘
- Gegenmassnahme:
    - Datenschutzbestimmungen z.B. im Impressum erweitern!

Einverständnis zu Cookies?

- Auf vielen Webseiten muss ich heute beim ersten Besuch ein Einverständnis zur Nutzung von Cookies anklicken. Ist das auch für unsere Webseite notwendig?
  - Nein, grundsätzlich ist dies zwar durch ein EU-Gesetz gefordert, aber nicht in deutsches Recht umgesetzt. ✓
  - Theoretisch könnte das Gesetz in Deutschland noch umgesetzt werden, aber aktuell geht man davon aus, dass das in Deutschland geltende Recht gilt, nach dem ein Hinweis in AGB oder Datenschutzbedingungen ausreicht.

Log-Files

- Führt Euer Server-Anbieter oder Eure Webseite Log-Files/Statistiken über die Besucher?
  - Nein, 100% nicht! ✓
  - Ich bin nicht sicher. ✗
  - Wir verwenden ein CMS (z.B. Joomla, Wordpress). ✗
  - Ja! ✗

- Gegenmassnahme:
  - Datenschutzbestimmungen um den Abschnitt Server-Log-Dateien erweitern!
    - Beispiele auf https://www.e-recht24.de/

Google Analytics

- Verwendet Ihr Google Analytics?
  - Nein! ✓
  - Ja! ✗
- Gegenmassnahme:
  - Datenschutzbestimmungen um den Abschnitt Google-Analytics erweitern! (https://www.e-recht24.de/)
  - IP-Anonymize im Analytics Code deiner Webseite aktivieren (zwingend nach geltendem Recht)
  - Opt-Out Links und Cookie setzen in den Datenschutzbestimmungen erwähnen.

Wenn Du nicht weißt wie, dann entferne Analytics und lass die Finger davon!

Andere Analyse-Dienste

- Neben Google Analytics gibt es auch andere Analyse-Dienste wie Piwiks, eTracker oder Erweiterungen, die im CMS installiert sein können.
- Es gelten die gleichen/ähnlichen Bedingungen wie für Google-Analytics. Auch hier müssen die Datenschutzbestimmungen passend erweitert werden.
- Beispieltexte zu den notwendigen Formulierungen findet Ihr häufig bei den Diensteanbietern oder auch auf https://www.e-recht24.de/ s

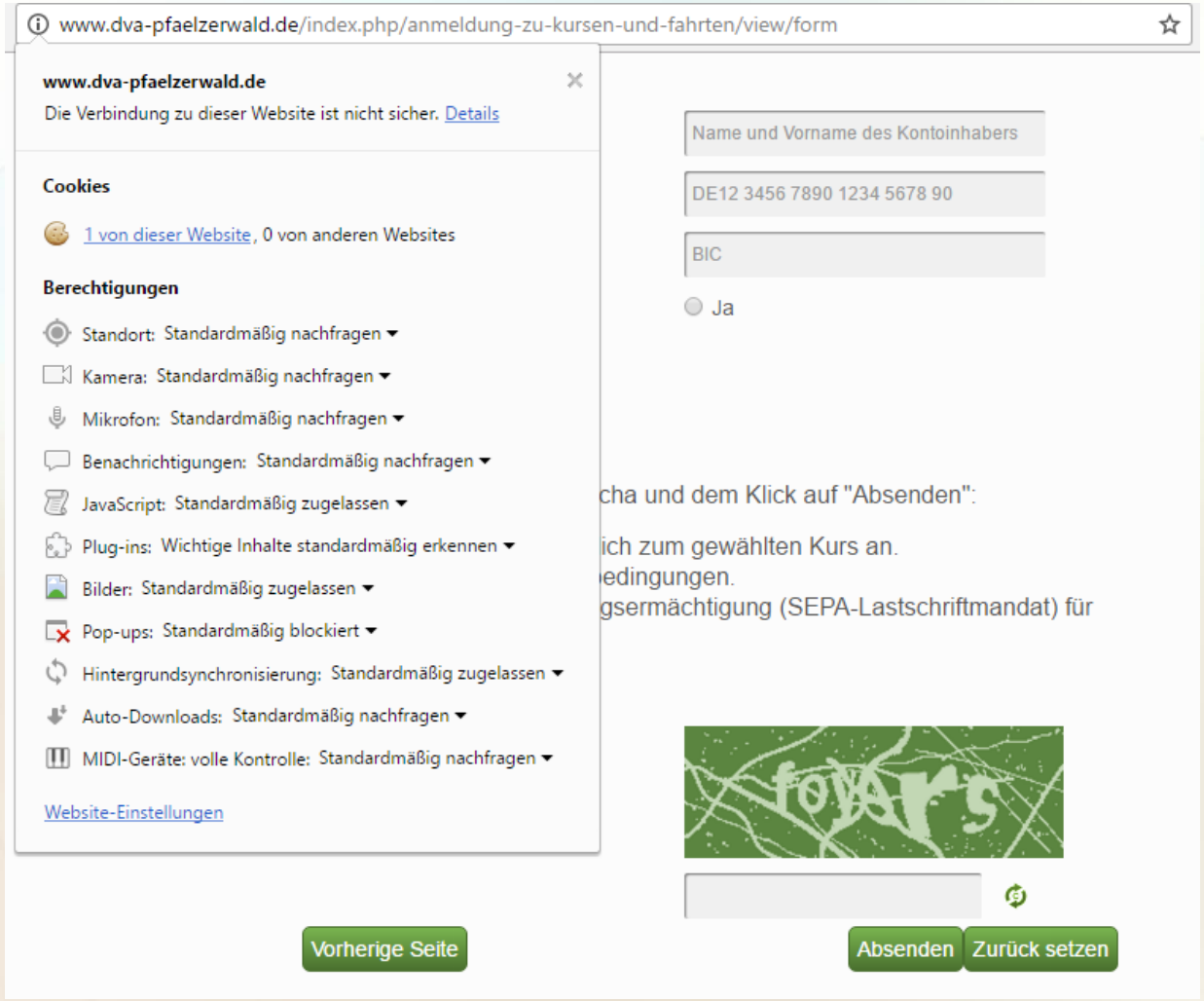
Facebook-Plugins

- Facebook bietet viele Plugins wie Post-Anzeige, Like-Buttons, Video-Integration. Diese werden direkt oder über CMS Module integriert. Mit dem Laden der Seite werden User-Infos an Facebook übermittelt.
  - Verwenden wir nicht! ✓
  - Verwenden wir! ✘
- Massnahmen:
  - Sind nach aktueller Rechtslage in D wahrscheinlich unzulässig!
  - Alternativ Server-seitig mit Facebook-API lösen
  - Alternativ mit 2-Click-Plugin lösen (der User muss das Plugin erst freischalten)

Das gilt sinngemäß auch für G+, pinterest, twitter, instagram …

Formulare

- Erschreckend: Kontodaten ohne Verschlüsselung



Formulare

- Können die Benutzer auf Eurer Seite Formulare (z.B. zur Kontaktaufnahme) verwenden und geben dabei persönliche Daten an?
  - Nein! ✓
  - Ja! ✗
- Massnahmen:
  - Stellt sicher, dass das Formular mittels https sicher übermittelt wird!
  - Überlegt Euch genau, welche Daten der Benutzer wirklich angeben muss!
  - Daten werden nur per eMail vom Server weiter verschickt:
    - Vorsicht: Email ist unsicher!
    - ODER: Stellt sicher, dass nur eine sichere (TLS) Verbindung genutzt wird.
  - Daten werden auch/alternativ auf dem Server hinterlegt:
    - Auch die folgenden Folien müssen berücksichtigt werden!

Datenbanken und Datenablage

- Speichert Ihr auf dem Server personenbezogene Daten?
  - Nein! ✓
  - Ja! ✘
- Massnahmen:
  - Die Website-Verbindungen zur Abfrage und Anzeige müssen verschlüsselt übertragen werden (https)!
  - Die entsprechenden Laufwerke auf dem Server sollten verschlüsselt sein! (Webhosting und Managed Server sind nicht optimal hierfür.)
  - Zugang zu diesen Daten haben nur die berechtigten Personen!
  - Die User müssen einer Datenschutzbestimmung zustimmen, diese muss vollständig über den Umgang und Nutzung der Daten informieren.

Auch Webhoster müssen sich an den EU-Datenschutz halten. Der mögliche Angriffsvektor ist relativ gering.

Die üblichen großen Webhoster in D können als zuverlässig angesehen werden.

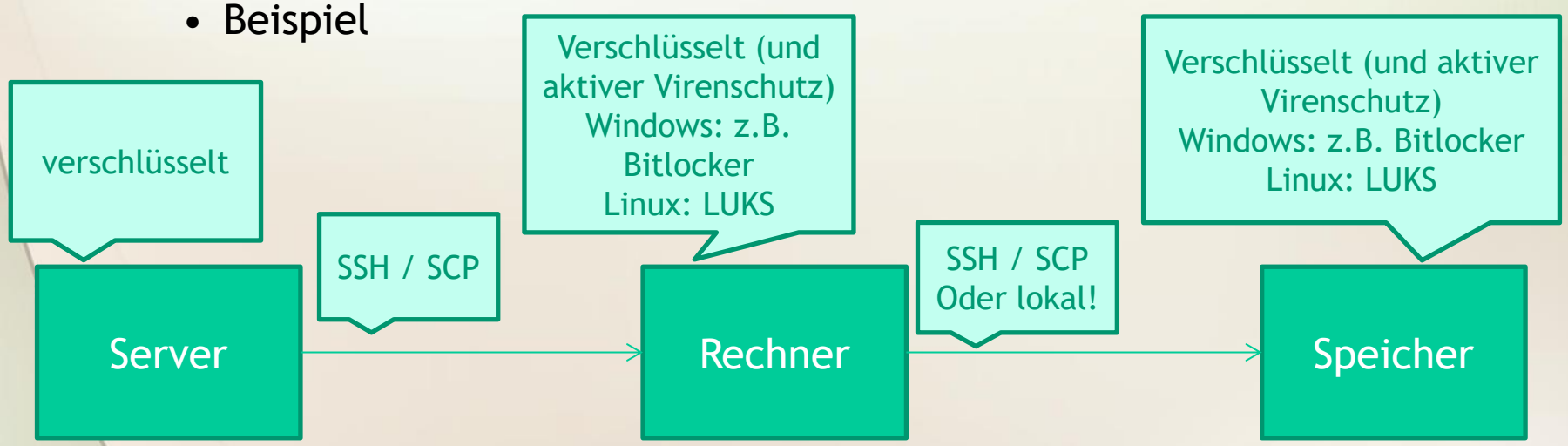
Bei besonders sensiblen Daten kann diese Lösung nicht empfohlen werden.

Datensicherung

- Führt Ihr Sicherungen von personenbezogene Daten durch?
  - Nein! ✓
  - Ja! ✘

Diese Folie gilt sinngemäß auch für Vereins-Verwaltungs-Software!

- Massnahmen:
  - Alle Strecken und Orte der Datenablage sind verschlüsselt!
  - Beispiel



Vereinsverwaltung

- Verwaltet Ihr die Daten der Vereinsmitglieder mit einer Software?
  - Nein! ✓
  - Ja! ✗
- Massnahmen:
  - Es gelten die gleichen Ansprüche an lokale Verschlüsselungen wie bei den Themen zuvor!
  - Beim Austausch der Daten zwischen berechtigten Personen muss eine Verschlüsselung oder sichere Übergabe sichergestellt sein.
  - Mit dem Aufnahmeantrag ist das Mitglied mit einer Datenschutzerklärung über die Speicherung und Nutzung der Daten zu informieren!

Web-Applikationen

- Ihr betreibt oder plant „Web-Applikationen“ ?
  - Das sind z.B. Mitgliederdatenbanken, Sportlerdatenbanken, Fahrtenbücher, Anmeldesysteme für Veranstaltungen…
  - Nein! ✓
  - Ja! ✗
- Massnahmen:
  - Es gelten grundsätzlich alle Forderungen aus den vorherigen Folien!
  - Ausserdem ist bei der Nutzung oder Implementierung von Software Umsicht und Professionalität in Planung und Erstellung gefordert! Planlose, schlecht dokumentierte Entwicklung führt im Rechtsstreit fast grundsätzlich zur Niederlage. Wichtige Punkte werden auf der folgenden Folie aufgeführt.

Web-Applikationen

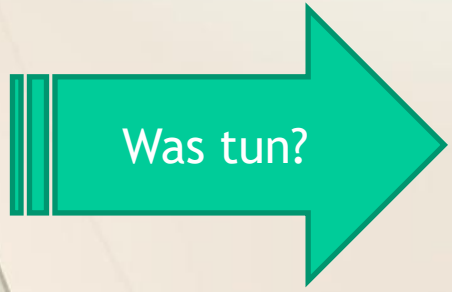
- Debug-Modes müssen in Produktivsystemen IMMER ausgeschaltet sein!
- Es ist IMMER zuerst die User- und Rechteverwaltung umzusetzen und die Anwendung zu planen und richtig einzusetzen!
- Es wird KEINE Funktion implementiert bei der nicht die User/Rechte Prüfung an erster Stelle steht.
- Bei einem Funktionsaufruf sind grundsätzlich die Parameter auf Missbrauch/Fehler zu prüfen!
- Die Implementierung wird grundsätzlich durch eine zweite Partei überprüft.

Grundsätze

- Ihr nutzt irgendeine der vorherigen Funktionen oder Ihr plant deren Einsatz

  UND

- Ihr versteht die hier vorgestellten Anforderungen sachlich oder technisch nicht oder könnt nicht sicher beurteilen, dass es bei Euch richtig läuft.

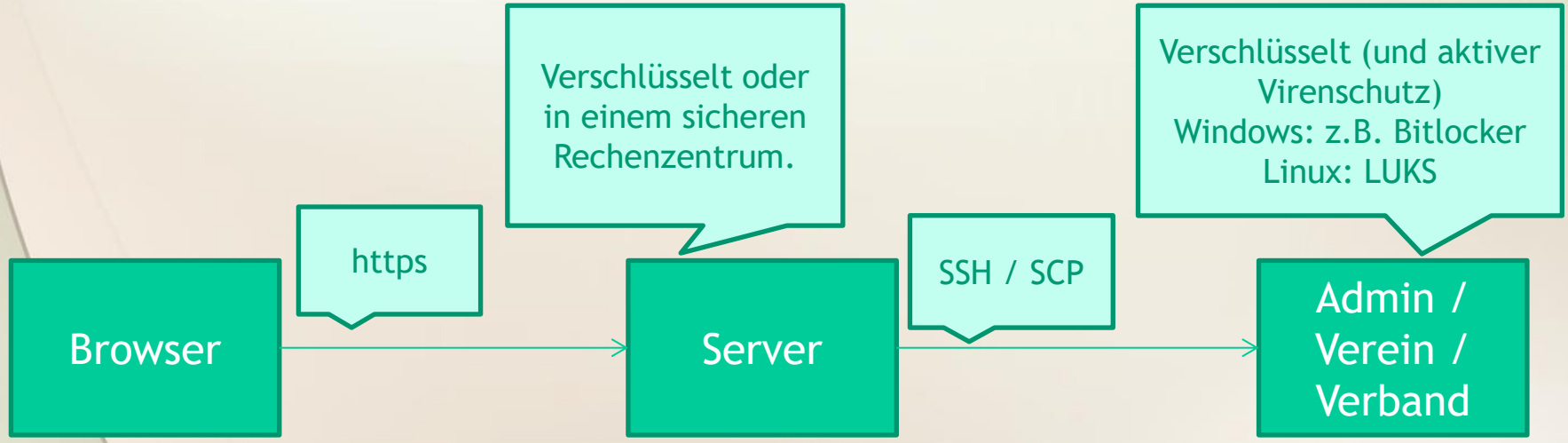


Schaltet es eventuell vorübergehend ab!

Holt Euch professionelle Hilfe!

Grundsätze

- Achtet immer darauf, dass die „Chain-of-Trust“ nicht gebrochen wird.
- Dazu müssen alle Elemente der Datenübermittlung und Datenspeicherung z.B. vom User bis zu Eurem Arbeitsplatz angemessen gesichert sein.



Anhang: https richtig nutzen

- Eine https Verbindung muss nach aktuellem Stand der Technik eingerichtet sein!
  - https bedeutet im Optimalfall:
    - Verschlüsselte Verbindung UND
    - Gegenüber/Webserver ist identifiziert - Stichwort: Zertifikat
  - Stellt IMMER die ganze Seite auf https um (redirect von http!). Damit kommt es erst gar nicht zu Fehlern.
  - Verwendet eine Installation die PFS (Perfect Forward Secrecy) erfüllt.
  - Lasst Euch im Zweifel von Eurem Diensteanbieter/Webhoster helfen.
  - Überprüft Eure Installation über: https://www.ssllabs.com/ssltest/

Kostenlose Zertifikate gibt es bei der Initiative letsencrypt.org

Erreicht dort das Ranking „A“