HEIDELBERGER AKADEMIE
DER WISSENSCHAFTEN
Akademie der Wissenschaften
des Landes Baden-Württemberg

Informationssicherheit

Handreichung für Beschäftigte

Zum internen Gebrauch

Version 1.0

Inhaltsverzeichnis

1 Einleitung

1.1 Versionshistorie

Stand	Version	Änderungen
Oktober 2024	1.0	Neukonzeption auf Basis des IT-Sicherheitskonzepts vom 24.3.2024

1.2 Allgemeine Angaben

Titel des Dokuments: Informationssicherheit – Handreichung für Beschäftigte
Autor: Georg Wolff, Referent im Referat für Wissenschaft und Digitale Infrastruktur
Klassifikation: Intern
Berechtigte: Alle Beschäftigten und Ehrenamtlichen der HAdW

1.3 Zielsetzung

Informationssicherheit geht jeden etwas an.
Ziel dieser Handreichung ist es, einen Überblick über gängige Informationssicherheitspraktiken an der HAdW zu informieren und Anleitung zu deren Umsetzung zu geben. Sie basiert auf dem IT-Sicherheitskonzept der Akademie. In der Summe gewährleistet die Einhaltung der Sicherheitsmaßnahmen:

- verlässliches Handeln der HAdW und ihrer Vertreter
- den guten Ruf der HAdW in der Öffentlichkeit
- den Fortbestand der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte
- die Sicherung sonst möglicherweise unwiederbringlicher Informationen und Daten
- die Erfüllung gesetzlicher Anforderungen
- den Schutz einzelner Personen

1.4 Adressatenkreis

Diese Handreichung richtet sich an alle Beschäftigten und Ehrenamtlichen (ab hier: „Beschäftigte“) der HAdW. *Alle* Beschäftigten haben ein hohes Maß an Verantwortung und Verpflichtung, zur Informationssicherheit beizutragen bzw. diese nicht zu gefährden. Sie sind verpflichtet, den eigenen Arbeitsplatz, die eigene Arbeit, Geräte, Systeme und Accounts sicher zu halten. **Prävention ist der beste Schutz gegen Cyberangriffe und Informationsverluste**.
Die hier vorgetragenen Maßnahmen sind ohne größeren zeitlichen oder technischen Aufwand im Arbeitsalltag umsetzbar und gewährleisten einen effektiven Schutz auf individueller Ebene.

2 Was sind schützenswerte Informationen?

Damit Sie Informationen angemessen schützen können, muss deren Bedeutung für die HAdW und den jeweiligen Geschäftsbereich (z.B. die eigene Forschungsstelle) definiert sein. Der folgende Abschnitt stellt ein Schema zur Einstufung vor.

2.1 Klassifikation

Generell lassen sich Informationen nach drei verschiedenen Dimensionen klassifizieren. Wie schützenswert eine einzelne Information ist, hängt vom größten Risiko in den drei Dimensionen ab. Beispielsweise wäre eine öffentliche verfügbare Information immer noch schützenswert, wenn an sie hohe Anforderungen im Bereich der Integrität gestellt werden (z.B. Website).

Vertraulichkeit

Vertrauliche Informationen müssen geschützt werden und je nach Bereich strengen Sicherheitsanforderungen genügen. Sie dürfen **nicht unautorisiert verbreitet** werden. Es wird unterschieden zwischen streng vertraulichen, vertraulichen, internen und öffentlichen Informationen.

Streng vertraulich oder vertraulich sind Informationen insbesondere dann, wenn deren **Offenlegung zu schweren Folgen** für den Weiterbestand des Geschäftsbereichs oder zu dessen Zusammenbruch (streng vertraulich, z.B. Dokumente zu Rechtsstreitigkeiten), oder erheblichen Beeinträchtigung (vertraulich, z.B. Finanzinformationen, Vertragsverhandlungen, personenbezogene Daten, geistiges Eigentum, etc.) führen würde. Personenbezogenen Daten sind auch dann vertraulich, wenn die Herausgabe zwar nicht die Institution schädigen, aber die Herausgabe die gesellschaftliche oder wirtschaftliche Stellung des Betroffenen beeinträchtigen würde.

Intern sind Informationen, wenn diese nur für den internen Gebrauch bestimmt sind (z.B. Richtlinien, Arbeitsprozesse, Forschungsrohdaten) oder aufgrund rechtlicher Bestimmungen nicht an Dritte gelangen dürfen, deren Herausgabe aber zu keinen schweren Schäden für den Geschäftsbereich führt.

Maßnahmen zur Vertraulichkeit

- **Informationen**, die vertraulicher als „intern“ eingeschätzt werden, sollten Sie entsprechend **kennzeichnen**, z.B. bei Papierdokumenten auf dem Deckblatt/Aktenordner, bei elektronischen Dokumenten etwa in der Fußzeile des Dokuments, bei Mailverkehr im Betreff oder in der ersten Zeile des Inhalts.
- Werden Sie hellhörig, wenn Sie mit einem (augenscheinlich) plausiblen Grund um die Herausgabe von vertraulichen Informationen wie z.B. Ihrem Passwort oder Bankdaten gebeten werden. Mehr dazu unter dem Punkt „**Social Engineering**“

Integrität

Informationen müssen **vollständig und richtig** verfügbar sein. Integre Informationen enthalten also keine nicht genehmigten Veränderungen. Besonders schützenswert sind Informationen, wenn gefälschte Daten z.B. zu Fehlbuchungen, inhaltlich falschen Förderentscheidungen oder fehlehrhaften Publikationen führen könnten.
Bei einer typischen elektronischen Datenübertragung kann eine Veränderung der Daten in der Regel nicht verhindert werden. Ziel ist es also, veränderte Daten erkennen zu können.

Maßnahmen zur Integrität

- Verwenden Sie **durchdachte und einheitliche** Ordnerstrukturen.
- **Benennen** Sie Ordner und Dateien nach einer **fest definierten Syntax**.
- Arbeiten Sie bei der Benennung von Dateien mit **Daten und Versionierungen** (z.B. „23-11-09_Handreichung-Informationssicherheitsrichtlinien_v1_GW“). So können leichter **Änderungen rückverfolgt** werden.

Verfügbarkeit

Informationen müssen für die Beschäftigten, die mit Ihnen arbeiten, **jederzeit verfügbar** sein. Besonders schützenswert sind solche Informationen, **ohne die die zentralen Funktionen des Geschäftsbereichs nicht erfüllt** werden können (z.B. Datenbanken), die **zeitkritische Prozesse** betreffen (z.B. Antragsdaten), oder bei denen **nur kurze Ausfallzeiten** toleriert werden können (z.B. Veranstaltungstechnik).

Maßnahmen zur Verfügbarkeit

- **Sichern Sie wichtige Daten** so, dass diese möglichst auf mehreren Datenträgern (z.B. Festplatte, Cloud) an mehreren Orten verfügbar sind (**Redundanz**).
- Klären Sie wo möglich, wer Ihre Aufgaben im **Krankheits- oder Verhinderungsfall** übernehmen kann und sorgen Sie dafür, dass diese Person auch tatsächlich technisch und inhaltlich in der Lage ist.

3 Gefahrenquellen

3.1 Schadsoftware

Abb. 1: The mother of all suspicious files, © xkcd.com

Als Schadsoftware wird **Software oder Code** bezeichnet, die auf das Endgerät des Opfers (PC, Tablet, Smartphone, etc.) gelangt und dieses für **kriminelle Zwecke** missbraucht. Oft bemerkt das Opfer die Infektion mit Schadsoftware nicht oder zu spät. In diese Kategorie fallen etwa **Trojaner** (als normale Software getarnte Schadprogramme), **Viren** (Schadcode, der sich in immer mehr Programme und Dateien einnistet) und **Würmer** (eigenständige Schadsoftware).
Schadsoftware kann sich unter anderem über infizierte Datenträger (USB-Sticks, externe Festplatten, CDs, etc.), E-Mail-Anhänge, Downloads aus unseriösen Quellen, infizierte Websiten (z.B. Werbebanner) o.Ä. verbreiten.
Egal, in welcher Verbreitungsart ein Schadprogramm auf den Rechner kommt: Sobald es sich eingenistet hat, arbeitet es in der Regel **autonom** weiter, lädt zum Beispiel weitere Schadprogramme auf das Gerät oder verbindet sich mit einem Server, von dem es zentral für ein Botnetz missbraucht wird.
Weit verbreitet ist auch Schadsoftware, die eine sogenannte **Backdoor-Funktion** im Gepäck hat: Solche Programme öffnen für Cyber-Kriminelle eine Hintertür, die einen **heimlichen Fernzugriff** auf das betroffene System ermöglicht. So können z.B. auch große **Datenmengen verschlüsselt** werden und für deren Entschlüsselung ein Geldbetrag erpresst werden (**Ransomware**).

Maßnahmen zu Schadsoftware

- Seien Sie **vorsichtig beim Öffnen von E-Mails** – insbesondere, wenn Sie Links und Anhänge anklicken und wenn es sich um die unerwartete Nachricht und/oder die eines unbekannten Absenders handelt. Aber auch bei vermeintlich bekannten Absendern ist Vorsicht geboten. Deaktivieren Sie am besten die Anzeige im HTML-Format und das Laden externer Inhalte.
- Deaktivieren Sie das automatische Ausführen von **Makros** und **Skripts**.
- Nutzen Sie **nur vertrauenswürdige Quellen**, um Dateien herunterzuladen.
- Schließen Sie **keine Datenträger unbekannter Herkunft** an Ihren PC an (z.B. USB-Sticks von Gästen, die etwas ausdrucken oder präsentieren möchten)
- Legen Sie **regelmäßig Backups** wichtiger Daten an, um sich vor deren Verschlüsselung zu schützen und verlorene Daten selbst wiederherstellen zu können.
- Verwenden Sie **Benutzerkonten mit reduzierten Rechten**, damit Schadprogramme keine Administratorrechte und damit Zugang zum gesamten System haben.
- Führen Sie in Absprache mit der EDV regelmäßig und zeitnah zur Verfügung stehende **Updates** durch – von Ihrem Betriebssystem und Programmen auf allen Geräten, um Sicherheitslücken zu schließen.
- Installieren Sie in Absprache mit der EDV ein **Virenschutzprogramm und eine Firewall**, um Schadprogramme möglichst beim ungewollten Download zu erkennen. Unter Windows nutzen Sie am besten die vorinstallierte Windows-Firewall und Windows Defender.

Mehr Informationen:
Bundesamts für Sicherheit in der Informationstechnik: Informationsbroschüre „Schadprogramme – so schützen Sie sich“, Weblink (pdf).

3.2 Social Engineering

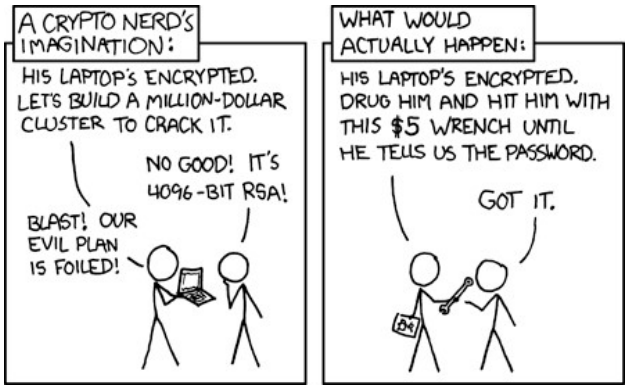

Abb. 2: Security, © xkcd.com

Als Social Engineering wird der Versuch bezeichnet, nicht durch die Überwindung technischer Hindernisse (Firewall o.Ä.), an Informationen zu gelangen, sondern durch **Manipulation des Opfers** („Schwachstelle Mensch“).

Bekannt geworden ist z.B. der „**Enkel-Trick**“, bei dem v.a. ältere Personen dazu genötigt werden, von sich aus Geld für eine nur behauptete Notlage auf die Konten der Betrüger zu überweisen, die sich als die Enkel oder andere Verwandte/Bekannte der Opfer ausgeben.

Eine beliebte Form des Social Engineering ist auch das **Phishing**, bei dem gefälschte E-Mails von Unternehmen und Institutionen versendet werden (z.B. PayPal, Amazon, Finanzamt, etc.), über die die Opfer verleitet werden sollen, Links anzuklicken, unter denen sie zur Eingabe persönlicher Daten (Accountname und -passwort o.Ä.) aufgefordert werden.

Angreifende nutzen also Techniken der **sozialen Manipulation**, um bei der Zielperson bestimmte **Emotionen auszulösen** oder sie zu **unüberlegten Handlungen**, z.B. zur Herausgabe sensibler Daten, zu bewegen. Sie drohen mit Konsequenzen, wenn die Daten nicht preisgegeben werden. Dabei geben Sie sich als Vorgesetzte/Verwandte/Bekannte/Techniker/Kollegen/Institutionen etc. aus. Oft haben Sie durch vorherige Recherche oder Observation schon Informationsfetzen erhalten, die diese Identität glaubhaft(er) machen.

Maßnahmen zu Social Engineering

- Geben Sie **keine nicht-öffentlichen Informationen** heraus, wenn ihr Gegenüber **nicht eindeutig identifizierbar** ist.
- Auch **unscheinbare Daten** wie Telefonnummern, Adressen, Geburtstage, etc. können Angreifern bei der Planung helfen, z.B. um Sicherheitsfragen zu knacken.
- Die Beschäftigten der Akademie, der Universitäten, der Universitätsrechenzentren oder seriöser Geschäftspartner werden Sie **nie** um die **Herausgabe sensibler Informationen** wie Passwörter, Kontodaten, etc. bitten.
- **Misstrauen** Sie Personen, die Sie durch **Druck** zu einer Handlung bewegen wollen.
- Vergewissern Sie sich ggf. z.B. über einen **Rückruf** über offizielle Verzeichnisse über die Identität der anderen Person.
- **Beenden Sie im Zweifelsfall Gespräche** oder Mailverkehr und halten Rücksprache mit der Leitung Ihres Geschäftsbereichs.

Mehr Informationen:

Cybersicherheitsagentur Baden-Württemberg: Fact Sheet „Phishing E-Mails“, Weblink (pdf).

Cybersicherheitsagentur Baden-Württemberg: Fact Sheet „Social Engineering“, Weblink (pdf).

IBM: „Social Engineering – How Bad Guys Hack Users“, Weblink (YouTube-Video).

3.3 Identitätsdiebstahl

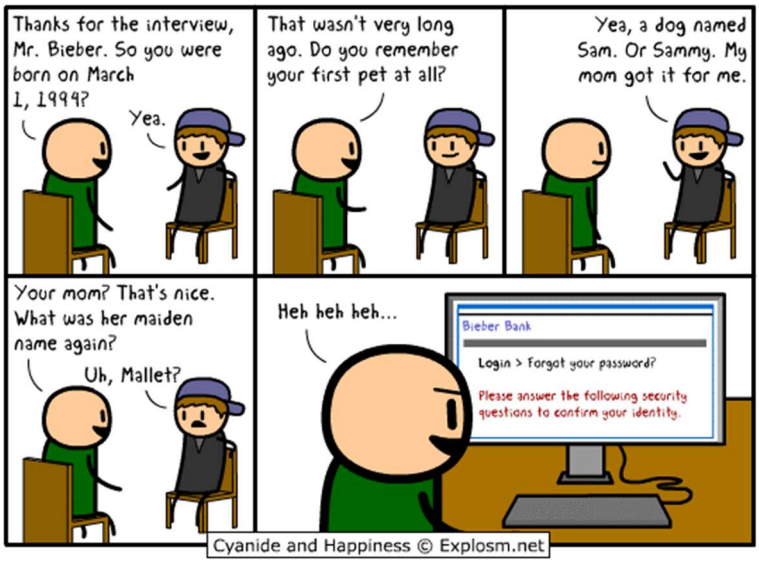

Abb. 3: Cyanide & Happiness #2919

Unter Identitätsdiebstahl versteht man, wenn Kriminelle sich v.a. im Internet als eine andere Person ausgeben. Die Folgen können schwerwiegend sein – von **finanziellen Schäden** über **Rufschädigung** bis zu **strafrechtlichen Konsequenzen**. Cyberkriminelle verschaffen sich mitunter unbefugt Zugriff zu einem **fremden Account**: Etwa mithilfe von Phishing-Mails oder Datenlecks greifen sie **Login-Daten** ab. Anschließend können sie sich einloggen und den Account übernehmen.
Um sich im Internet als eine andere Person auszugeben, müssen Cyberkriminelle jedoch nicht zwingend ein fremdes Konto übernehmen. Eine andere Strategie ist, einen neuen **Account in fremdem Namen** zu erstellen. Zuvor sammeln sie Bilder und private Daten wie Geburtsdatum und Beruf. Damit befüllen sie zum Beispiel ein Social Media-Profil, das täuschend echt aussehen kann und nutzen dieses, um z.B. Teammitglieder oder Geschäftspartner des Opfers hinters Licht zu führen.

Maßnahmen zu Identitätsdiebstahl

- Nutzen Sie **starke Passwörter** und verwenden Sie z.B. einen **Passwort-Manager** (s.u.).
- Verwenden Sie **für jeden Dienst ein eigenes Passwort**. Sollte zum Beispiel Ihr privates Social Media-Konto gehackt werden, ist so etwa Ihr dienstliches E-Mail-Konto nicht mitbetroffen.
- Nutzen Sie, wo möglich, **Zwei-Faktor-Authentifizierung**.
- Geben Sie online nur so viel wie unbedingt notwendig über sich preis.
- Nutzen Sie privat **unterschiedliche Nutzernamen** auf unterschiedlichen Plattformen. So erschweren Sie es Cyberkriminellen, ein Gesamtprofil über Sie zu erstellen.
- Verwenden Sie für Geräte wie Laptop, Smartphones oder Tablets eine **Displaysperre**. Lassen Sie sich zudem nicht bei der Eingabe von Passwörtern beobachten.
- Seien Sie vorsichtig im Umgang mit **öffentlichen WLAN-Netzwerken** (verwenden Sie z.B. unterwegs wo möglich eduroam) und meiden Sie diese am besten ganz. So vermeiden Sie die unverschlüsselte Übertragung von Daten.
- Nutzen Sie Ihre **Dienstadresse nicht für private Kommunikation** und umgekehrt.

Weitere Informationen:
Cybersicherheitsagentur Baden-Württemberg: Fact Sheet „Zwei-Faktor-Authentifizierung“, Weblink (pdf).

4 Sicher im Arbeitsalltag

4.1 E-Mail

Abb. 4: Der Drei-Sekunden-Sicherheitscheck © Can Yesil / fotolia.com; BSI

Für Sicherheit im Mailverkehr müssen Sie keine zusätzliche Software installieren. Viele E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können (z.B. exchange oder SoGo beim URZ Heidelberg). Wichtig ist, auf eine **verschlüsselte Verbindung** (HTTPS) zum Postfach zu achten, um von den Schutzmechanismen Ihres Browsers zu profitieren. Achten Sie darauf, dass die Verschlüsselung nicht nur für den Login-Vorgang, sondern **während der gesamten Webmail-Nutzung** aktiviert ist.
Falls Sie erweiterte Anforderungen an Komfort und Funktionalität bei der Arbeit mit E-Mails haben, sollten Sie einen aktuellen und verbreiteten **E-Mail-Client** (z.B. Outlook, Mozilla Thunderbird) auswählen und diesen **sicher konfigurieren**, um z.B. ein zusätzliches Einfallstor zur Ausführung von Schadcode auf Ihrem Rechner auszuschließen.
Achten Sie bei der Nutzung von E-Mail-Programmen darauf, dass **Übertragungsprotokolle** (POP3S, IMAPS, SMTPS) verwendet werden (Standard bei den HAdW-Dienstadressen und Mailclients). Sie können auch ein **digitales Zertifikat** einrichten. Mit diesem können Sie dann Ihre ausgehenden E-Mails signieren, sodass der Empfänger zweifelsfrei feststellen kann, ob eine E-Mail tatsächlich von Ihrem Account versendet wurde. Wenn sowohl Absender als auch Empfänger ein solches Zertifikat eingerichtet haben, ist es sogar möglich, die Mails zu **verschlüsseln**. Dann können diese, selbst wenn Sie unterwegs abgefangen werden, nicht ausgelesen werden.

Maßnahmen zur E-Mail-Sicherheit

- Nutzen Sie bei eingehenden Mails den **Drei-Sekunden-Sicherheitscheck**.
- Richten Sie ein **Zertifikat,** z.B. über das Universitätsrechenzentrum Heidelberg ein.
- **Melden Sie E-Mails** beim geringsten Verdacht der EDV-Abteilung und befolgen Sie deren Anweisungen.
- **Verzichten** Sie auf die Darstellung und Erzeugung von E-Mails im **HTML-Format**.
- **Deaktivieren** Sie die Anzeige von **externen Inhalten**.

Weitere Informationen:
URZ Heidelberg: S/MIME-Zertifikat (mit Anleitung), Weblink.

4.2 Videokonferenzen

Videokonferenzen ermöglichen uns, auch über Distanzen im Team zusammenzuarbeiten, Daten zu teilen und Inhalte zu präsentieren. Sie sollten aber darauf achten, dass beim Teilen des Bildschirms (Screensharing) oder Ihre Webcam keine sensiblen Informationen sichtbar sind. Wenn Unbefugte an Videokonferenzen teilnehmen, können diese ggf. vertrauliche Informationen mitlesen und -hören.

Maßnahmen zu Videokonferenzen

- Verwenden Sie nach Möglichkeit einen **virtuellen Hintergrund oder Weichzeichner**.
- **Entfernen Sie Informationen** von Flipcharts, Tafeln, etc. in Ihrem Büro, bevor Sie einer Videokonferenz beitreten.
- Schalten Sie **Sprachassistenzsysteme** („Alexa" o.Ä.) während der Arbeit, vor allem aber während Besprechungen **aus und entfernen** Sie diese aus dem Zimmer.
- Lassen Sie Teilnehmerinnen und Teilnehmer, die ohne Kamera an einer Videokonferenz teilnehmen, sich **identifizieren**.
- Geben Sie **keine Passwörter** ein, während Sie einen Bildschirm teilen.
- **Schließen** Sie generell **alle nicht benötigten Tabs und Programme** (v.a. Passwort-Manager o.Ä.), bevor Sie einen Bildschirm teilen.
- **Deaktivieren** Sie während des Screensharing **Pop-Ups**, z.B. von Mailprogrammen oder Messengerdiensten.

4.3 Arbeiten im Büro

Ausgedruckte Dokumente, Akten, Unterlagen und handschriftliche Notizen sammeln sich schnell am Arbeitsplatz an. Eine **mangelnde Ordnung**, ob auf dem Schreibtisch oder auf dem Desktop, kann ein **Einfallstor für Angriffe** sein und die Werte Vertraulichkeit (Daten sind einsehbar), Integrität (Durch Unordnung werden falsche Versionen o.Ä. versendet) oder Verfügbarkeit (Daten gehen verloren) beeinträchtigen. Außerdem kann auch die **DSGVO** verletzt werden. Ein **unaufgeräumter Desktop** wiederum erleichtert es Cyberkriminellen, **unbemerkt Schadsoftware** o.Ä. auf Ihrem PC abzulegen.
Auch sollte Ihr Büro **nie gleichzeitig unbesetzt und unverschlossen** sein. Dabei spielt es keine Rolle, wie lange Sie den Platz verlassen – schon bei kurzen Pausen besteht die Möglichkeit einer Sicherheitsgefährdung.

Maßnahmen zum Arbeiten im Büro

- Legen Sie **sensible Dokumente nur bei unmittelbarem Bedarf** auf Ihren Schreibtisch und schließen Sie diese unverzüglich nach Gebrauch wieder weg.
- **Drucken Sie nur die nötigsten Dokumente** aus und lassen Sie **keine Dokumente im Drucker** liegen.
- **Sperren Sie Ihren Bildschirm** beim Verlassen des Büros und reinigen Sie Flipcharts o.Ä. Das gilt auch schon bei kurzfristigen Abwesenheiten (Gang zur Teeküche etc.)
- Verwenden Sie Ihren **Desktop nur für die wichtigsten**, häufig verwendeten Programme und Dateien.
- Legen Sie (aktuell) nicht benötigte Dateien nach einer festen Struktur ab oder löschen Sie sie.
- Folgen Sie einer **einheitlichen Syntax bei der Benennung** von Dateien und verwenden Sie Daten und Versionierungen.
- **Löschen Sie unbekannte Dateien** oder lassen Sie diese auf Schadsoftware überprüfen.

Weitere Informationen:

Cybersicherheitsagentur Baden-Württemberg: Fact Sheet „Clean Desk und Clean Desktop“, Weblink (pdf).

4.4 Mobiles Arbeiten – Zuhause

Das mobile Arbeiten, insbesondere von Zuhause, ist inzwischen in der Akademie fest verankert. Im Gegensatz zur geschützten Büroumgebung sind **Sie in den eigenen vier Wänden selbst dafür verantwortlich**, dass der Schutz von Informationen gewährleistet ist. Ein **sorgloser Umgang** bei Aufbewahrung oder Transport von Arbeitsmaterialien, Zugänglichkeit durch Besuch oder Familienmitglieder, Vermischung von Privatem und Dienstlichem etc. **kann neue Sicherheitsrisiken** hervorrufen.

Maßnahmen zum mobilen Arbeiten I

- **Schließen Sie Türen und Fenster** beim Verlassen des Raums und telefonieren Sie nicht über Lautsprecher.
- Verwahren Sie **Papierunterlagen verschlossen** auf.
- Informieren Sie Ihr Umfeld, dass zufällig aufgeschnappte **Informationen vertraulich** zu behandeln sind.
- Schalten Sie **Sprachassistenzsysteme („Alexa" o.Ä.) während der Arbeit aus** und entfernen Sie diese aus dem Zimmer.
- Verwenden Sie, wo möglich, auch im mobilen Arbeiten die **Dienstgeräte**.
- Schließen Sie **keine privaten Geräte an den Dienstrechner** an oder umgekehrt.
- **Sperren Sie den Bildschirm** beim Verlassen des Arbeitsplatzes.
- Hinterlassen Sie Ihren Arbeitsplatz **aufgeräumt** und stellen Sie sicher, dass **keine sensiblen Informationen** einsehbar sind.
- Entsorgen Sie vertrauliche Dokumente **nicht im Hausmüll**.

Weitere Informationen:
Cybersicherheitsagentur Baden-Württemberg: Fact Sheet „Homeoffice", Weblink (pdf).
Bundesamt für Sicherheit in der Informationstechnik: „Tipps für sicheres Mobiles Arbeiten", Weblink (pdf).

4.5 Mobiles Arbeiten – Unterwegs

Beim mobilen Arbeiten unterwegs (z.B. im Zug) tun sich eine Menge **zusätzlicher Gefahrenquellen** auf. So können z.B. **Papierdokumente**, die sensible Informationen unverschlüsselt enthalten, von Unbefugten leicht eingesehen werden; über **öffentliche WLANs** können Dritte Zugriff auf übermittelte Daten erhalten oder Malware einschleusen. **Diebe** können Geräte und/oder Informationen entwenden oder diese können einfach verlorengehen/liegengelassen werden.

Maßnahmen zum mobilen Arbeiten II

- Schätzen Sie ab, ob Ihre momentane Umgebung ein **risikoarmes Arbeiten** zulässt und verschieben Sie ggf. sensible Arbeiten auf einen **späteren Zeitpunkt**.
- Telefonieren Sie **nicht über Lautsprecher**.
- Benutzen Sie ein **Headset** und sprechen Sie keine sensiblen Informationen laut aus. Verschieben Sie ggf. Telefonate auf einen **späteren Zeitpunkt**.
- Benutzen Sie **Bildschirmfolien** oder sitzen Sie mit dem **Rücken zur Wand**, um das Auslesen über die Schulter oder durch **Videoüberwachungssysteme** zu erschweren.
- **Vermeiden** Sie die mobile Arbeit mit **Papierdokumenten**.
- Verwenden Sie, wo möglich, auch im mobilen Arbeiten die **Dienstgeräte**.
- Schließen Sie **keine privaten Geräte an den Dienstrechner** an oder umgekehrt.
- **Sperren Sie den Bildschirm** beim Verlassen des Arbeitsplatzes.
- Hinterlassen Sie Ihren Arbeitsplatz **aufgeräumt** und stellen Sie sicher, dass **keine sensiblen Informationen** einsehbar sind.
- Entsorgen Sie vertrauliche Dokumente nicht unterwegs.
- **Vermeiden** Sie das Arbeiten in **öffentlichen Netzwerken** und schalten Sie die **automatische Verbindung** zu WLANs unterwegs ab.
- Besuchen Sie über öffentliche Netzwerke **nur sichere Verbindungen** (https)
- Greifen Sie auf dienstliche Daten nur über **VPN-Verbindungen** zu.

Weitere Informationen:
Bundesamt für Sicherheit in der Informationstechnik: „Tipps für sicheres Mobiles Arbeiten“, Weblink (pdf).

4.6 Passwörter

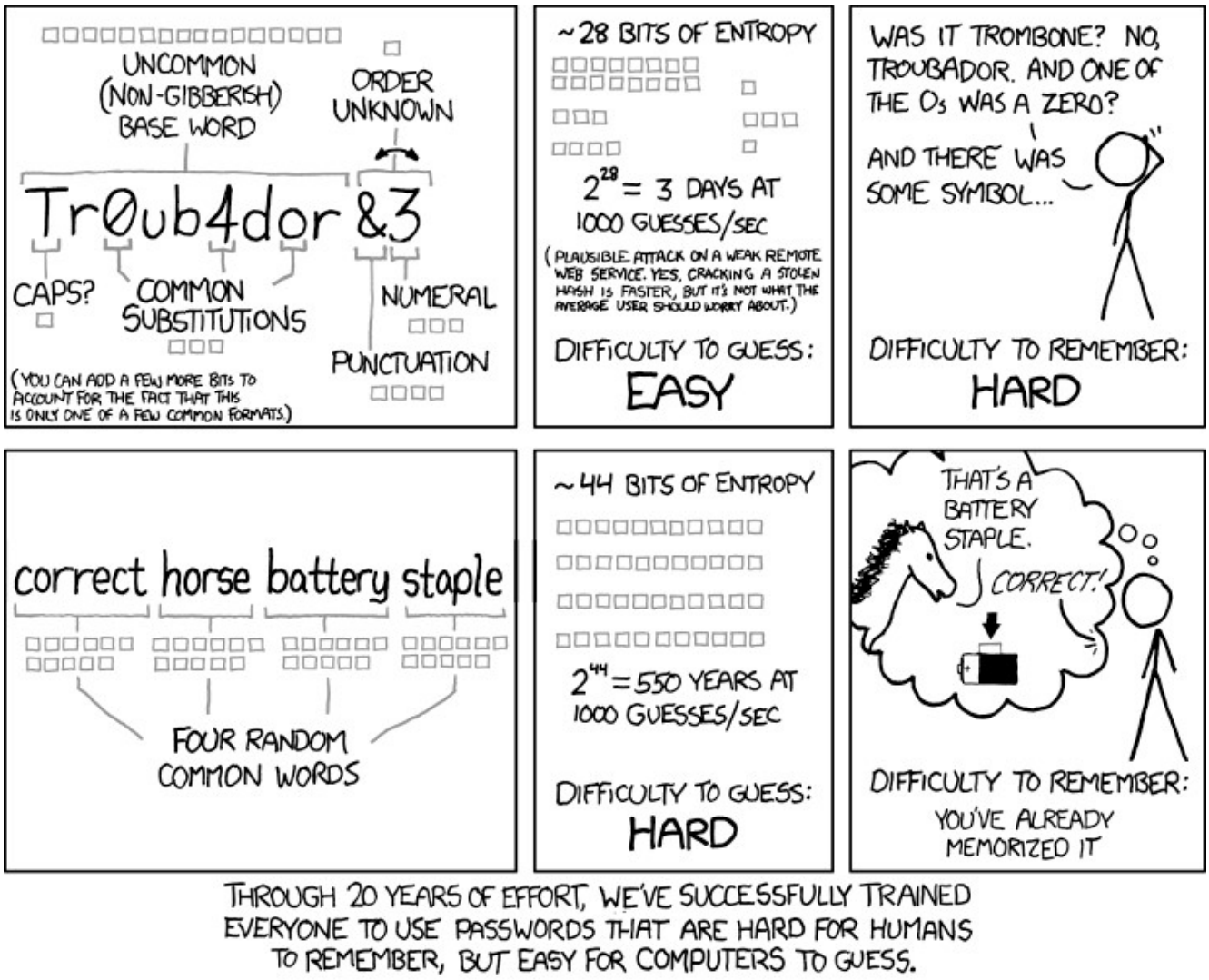

Abb. 5: Password strength, ©xkcd.com

Passwörter sind die **Schlüssel zu unseren Daten** und damit zu unserem digitalen Leben. Schützen Sie Ihre beruflichen und privaten Daten zuverlässig vor ungewollten Zugriffen, indem Sie für jeden Ihrer Zugänge ein **einzigartiges und starkes Passwort** verwenden. Wenn Sie gleiche Passwörter für unterschiedliche Accounts (v.a. im dienstlichen *und* privaten Bereich) verwenden, kann eine Sicherheitslücke in einem der Accounts alle Accounts mit dem gleichen Passwort kompromittieren (z.B. bei ebenfalls gleichem Benutzernamen/hinterlegter Mail-Adresse oder auch durch Aufnahme in Passwörterlisten). **Unsichere Passwörter** können (z.B. nach Datenlecks) von Angreifern schnell geknackt werden.

Selten geworden sind Angriffe, bei denen alle möglichen Passwörter ausprobiert werden (**brute force-Methode**), weil in der Regel Login-Server effektive Schutzmaßnahmen gegen solche Verfahren bereitstellen und der Rechenaufwand (für starke Passwörter) zu groß wäre. Realistischer sind sog. **Wörterbuchangriffe**, bei denen auf Basis bereits bekannter (also zu einem früheren Zeitpunkt entschlüsselter) Passwörter gezielt diese und Variationen ausprobiert werden. Deswegen ist im oben angeführten Beispiel „Tr0ub4dor&3“ zwar sicherer als „troubador“, aber nur eingeschränkt, wenn „troubador“ als Passwort bereits geleakt oder geknackt wurde (gängige Anordnung von Sonderzeichen und Ziffern, gängige Substitutionen).

Maßnahmen zu Passwörtern

- Je **länger** (Anzahl Zeichen) und/oder **komplexer** (Groß-/Kleinschreibung, Ziffern, Sonderzeichen) ein Passwort ist, desto schwieriger ist es zu knacken. Faustregel: Ein hochkomplexes (4 Zeichenarten) Passwort sollte mindestens 8 Zeichen lang sein, ein niedrigkomplexes (2 Zeichenarten) mindestens 25 Zeichen lang.
- **Notieren Sie keine Passwörter**, geben Sie diese nicht weiter und geben Sie sie stets **unbeobachtet** ein.
- **Ersetzen Sie schwache, doppelte, geleakte und voreingestellte Passwörter** durch neue, starke Passwörter.
- Verwenden Sie einen **Passwort-Manager**, um sich nicht unnötig viele komplexe Passwörter und deren Zuordnung merken zu müssen. Schützen Sie diesen Manager unbedingt mit einem einzigartigen, starken Passwort.
- Verwenden Sie, wo möglich, **Zwei-Faktor-Autorisierung** (die Einführung am URZ HD läuft).

Weitere Informationen:

Cybersicherheitsagentur Baden-Württemberg: Fact Sheet „Passwortsicherheit“, Weblink (pdf).

Bundesamt für Sicherheit in der Informationstechnik: „Sichere Passwörter erstellen“, Weblink.

Computerphile: „Password Cracking“, Weblink (YouTube-Video).

Computerphile: „How to Choose a Password“, Weblink (YouTube-Video).

Computerphile: „How Password Managers Work“, Weblink (YouTube-Video).

5. Sicherheitsvorfälle

Ein **Sicherheitsvorfall** ist dann eingetreten, wenn mindestens eines dieser **Kriterien** erfüllt ist:

- Die **Vertraulichkeit** von Daten ist verletzt, weil z.B. unberechtigte Personen Zugriff darauf haben oder hatten.
- Die **Integrität** von Daten ist verletzt, weil z.B. Daten unberechtigt und unbemerkt verändert wurden.
- Die **Verfügbarkeit** von Daten ist gestört, weil z.B. ein System ausgefallen ist.

Ein **Sicherheitsrelevantes Ereignis** ist dagegen, wenn einer dieser Werte nur **gefährdet erscheint**.

Anzeichen dafür, dass ein Sicherheitsvorfall im Gange ist, können weiterhin unter anderem sein:

- Korrekte Zugangsdaten funktionieren nicht mehr.
- Warnhinweise von Viren- oder Abwehrprogrammen.
- Programme starten und beenden selbständig.
- Dateien können nicht mehr verändert oder gespeichert werden.
- E-Mails werden selbständig von Ihrem Account versendet.
- Die Darstellung von Programm-Icons ist verändert.
- Die Startseite im Webbrowser verändert sich oder Webseitenanfragen werden umgeleitet.
- Das Webcam-Licht leuchtet bei ausgeschalteter Kamera.
- Der Rechner fährt von selbst herunter.
- Fremde Geräte sind ohne Ihre Kenntnis an Ihrem Arbeitsplatz (z.B. USB-Sticks)

Diese Symptome können aber auch andere Ursachen als Sicherheitsvorfälle haben.

5.1 Verhalten bei Sicherheitsvorfällen

Besteht der Verdacht auf einen Sicherheitsvorfall im Arbeitsumfeld, muss dieser schnellstmöglich gemeldet werden, um im Ernstfall Schlimmeres verhindern zu können – jede Minute zählt. Informieren Sie unverzüglich die beauftragte Person für Informationssicherheit, die IT-Abteilung, Ihre Forschungsstellenleitung oder die Geschäftsführung. Konsultieren Sie ggf. den IT-Notfallplan, um die richtigen Ansprechpartner zu identifizieren.

Verhalten im Sicherheitsfall

- Bewahren Sie **Ruhe**.
- **Stellen Sie die Arbeit** am potentiell infizierten Gerät **unverzüglich ein**, fahren Sie es herunter und **trennen Sie es vom Netz**.
- Leiten Sie nur nach Anleitung **Gegenmaßnahmen** ein.
- Gehen Sie auf keinen Fall auf **Forderungen von Kriminellen** ein.
- **Kontaktieren Sie umgehend** die IT-Abteilung, Informationssicherheitsbeauftragte, Geschäftsführung oder Forschungsstellenleitung (Wer meldet? Welches Gerät/System ist betroffen? Wie haben Sie an dem Gerät zuvor gearbeitet? Was haben Sie beobachtet? Wann ist das passiert? Wo befindet sich das betroffene Gerät?)
- Drucken Sie die **Notfallkarte** „Verhalten bei IT-Notfällen“ (s.u.) aus und hängen Sie diese gut sichtbar in Ihrem Geschäftsbereich aus. Ihre **IT-Notfallrufnummer ist 06221 54 3354**

Weitere Informationen:

Cybersicherheitsagentur Baden-Württemberg: Fact Sheet „Informationssicherheitsvorfall erkennen“, Weblink (pdf).

Allianz für Cybersicherheit/Bundesamt für Sicherheit in der Informationstechnik: Notfallkarte „Verhalten bei IT-Notfällen“, Weblink (pdf).