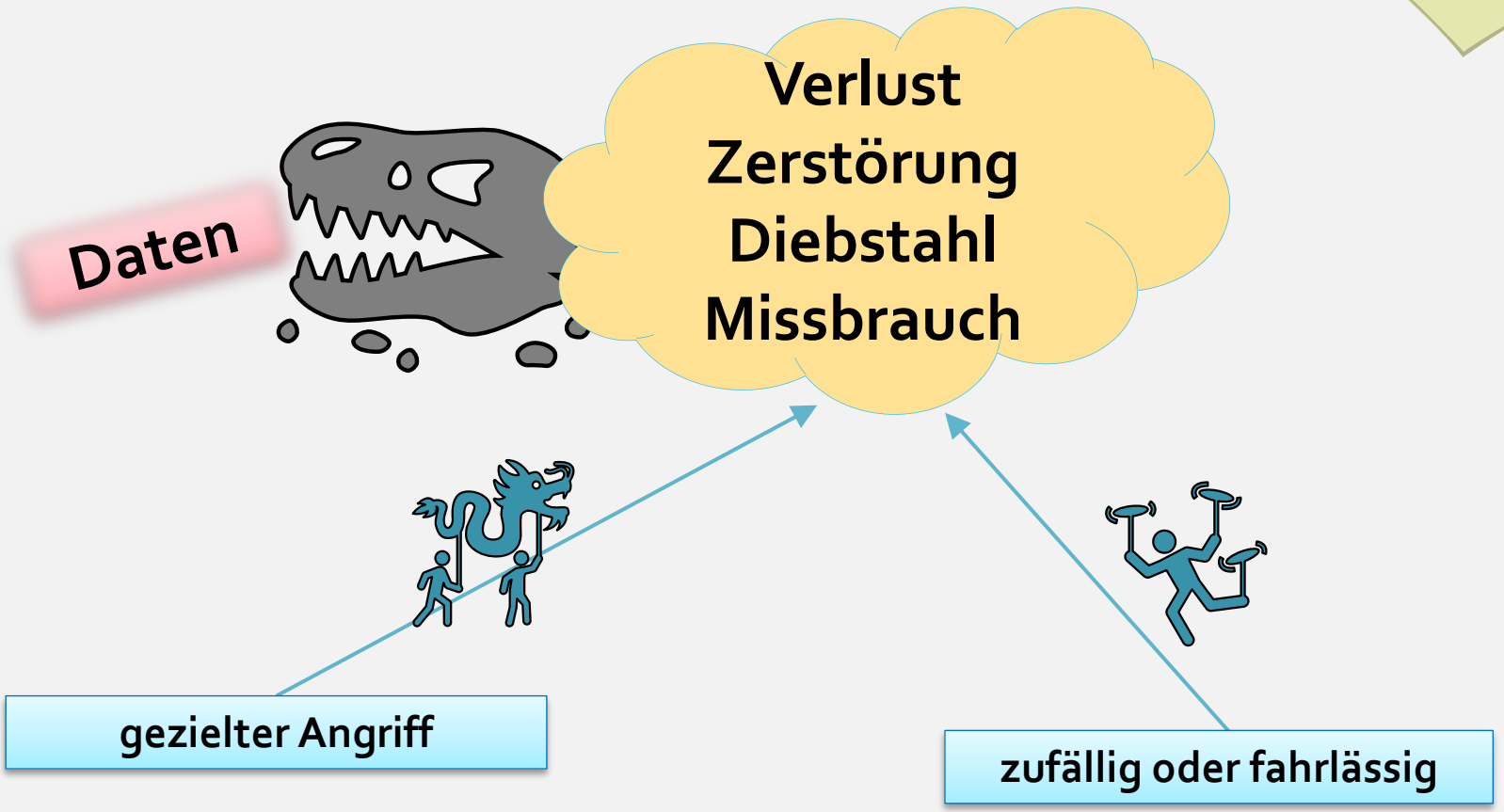
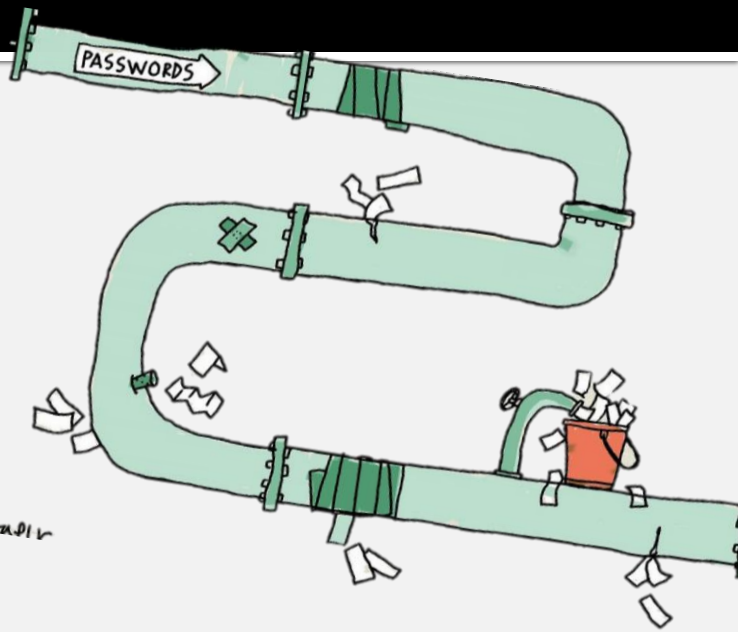
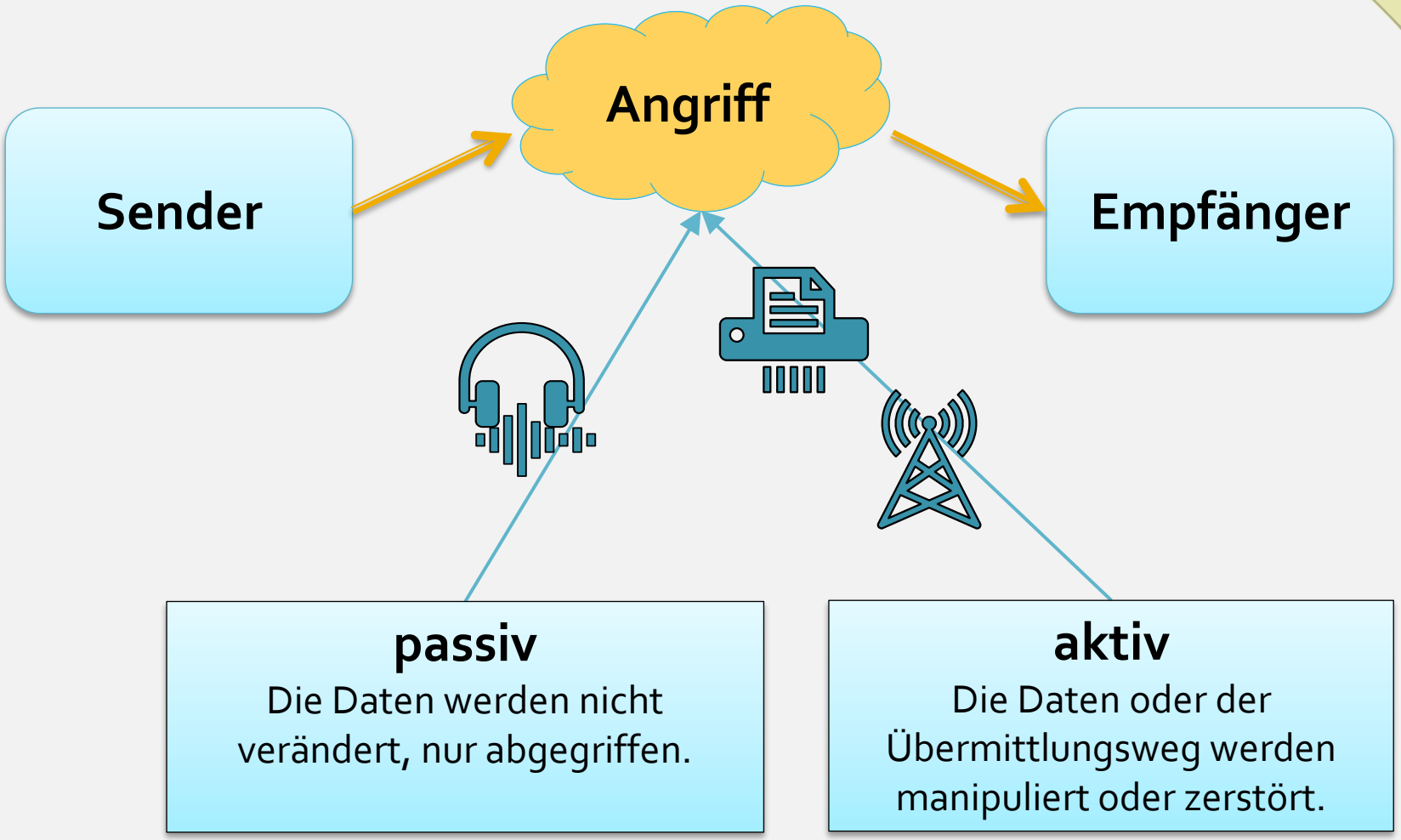
Datensicherheit - Gefährdungen



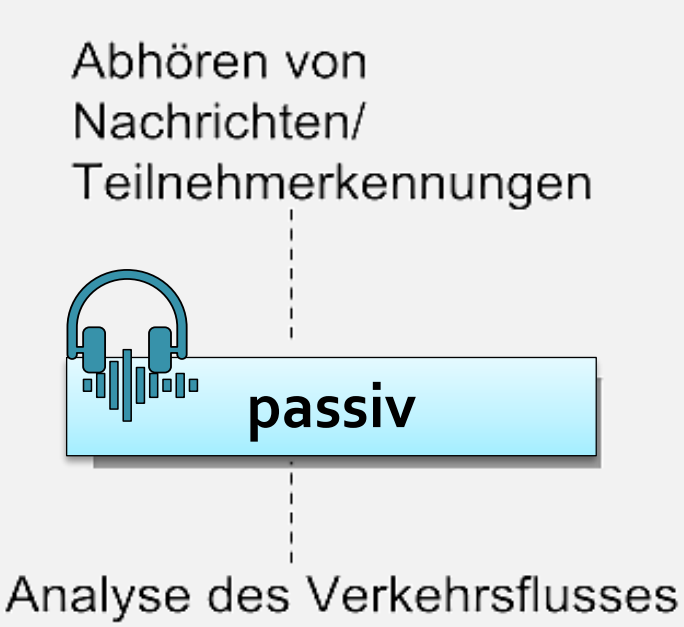
Beispiele für Gefährdungen

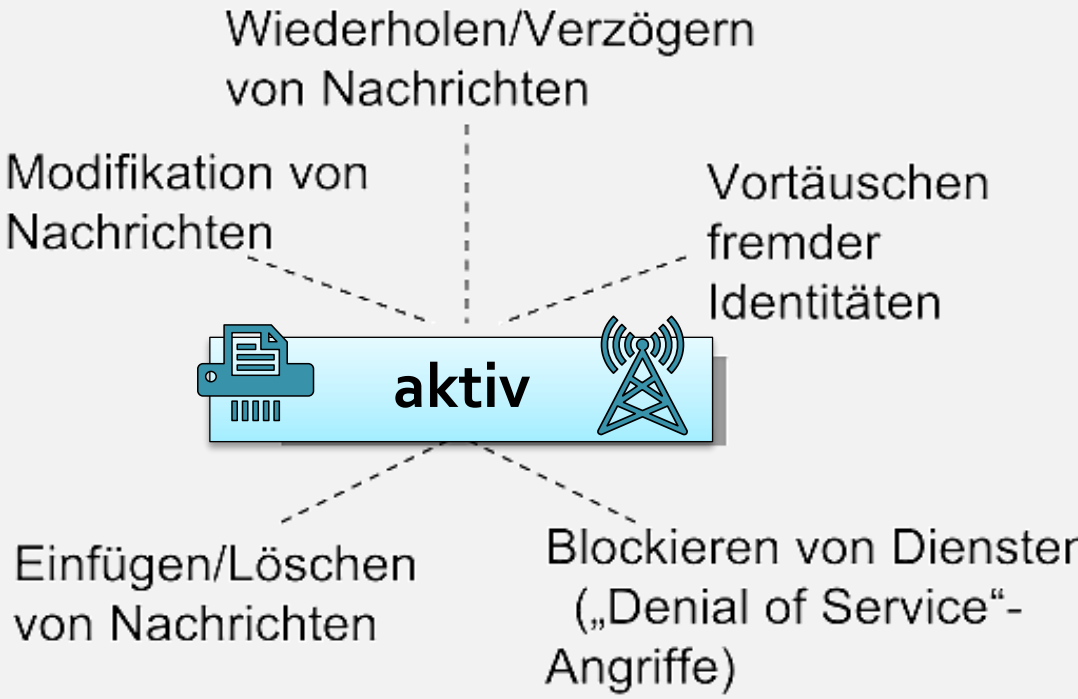


Angriffe allgemein



Angriffe (Beispiele)





Anforderungen an die Sicherheit

Schutzziele für den Umgang mit Daten

Schau dir bitte jetzt das folgende Video an!

Video 1

Anforderungen an die Sicherheit

Nimm am Basketballquerformat!

Schutzziele für den Umgang mit Daten

- Schutz der Vertraulichkeit
- Schutz der Integrität
- Schutz der Verbindlichkeit
  - Authent-izität
  - Unabstreit-barkeit
- Schutz der Verfügbarkeit

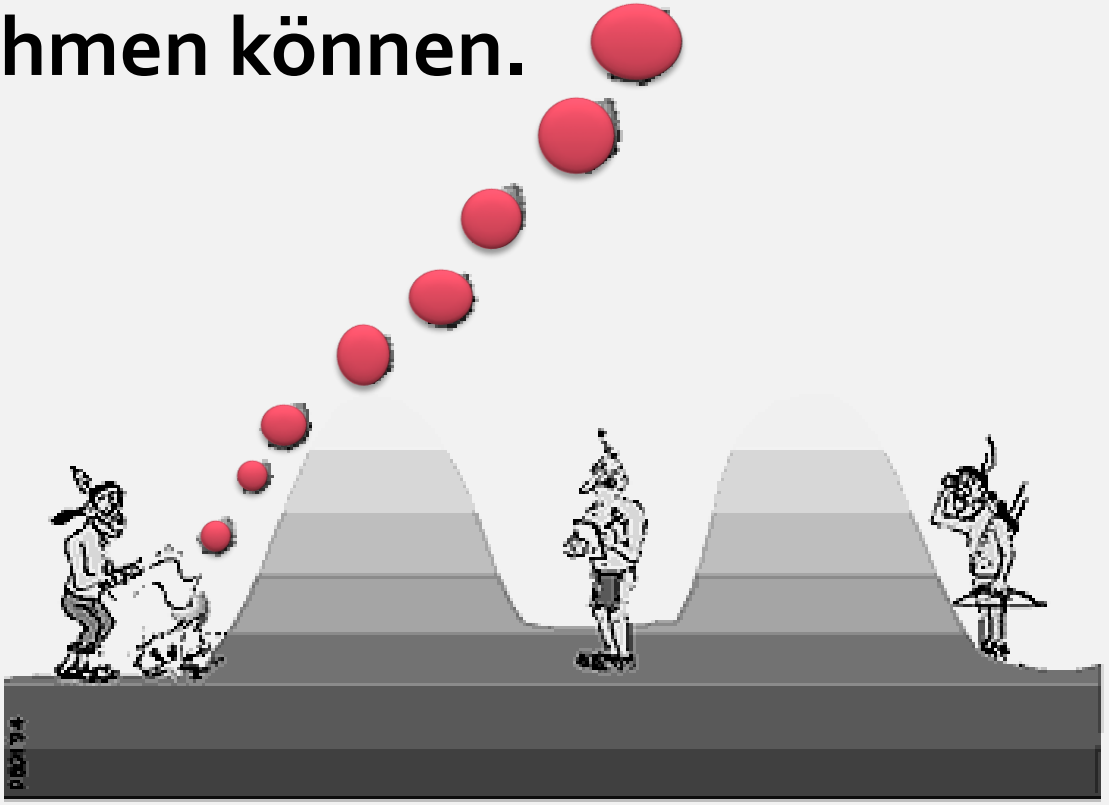
Ergänze hier die Infos auf dem nächst. Seiten und aus dem Videos!

Vertraulichkeit

Informationen sind nur für Berechtigte zugänglich.

Vertraulichkeit

Informationen dürfen nur für den Berechtigten lesbar sein. Es darf nicht möglich sein, dass am Transport der Informationen Beteiligte vom Inhalt Kenntnis nehmen können.

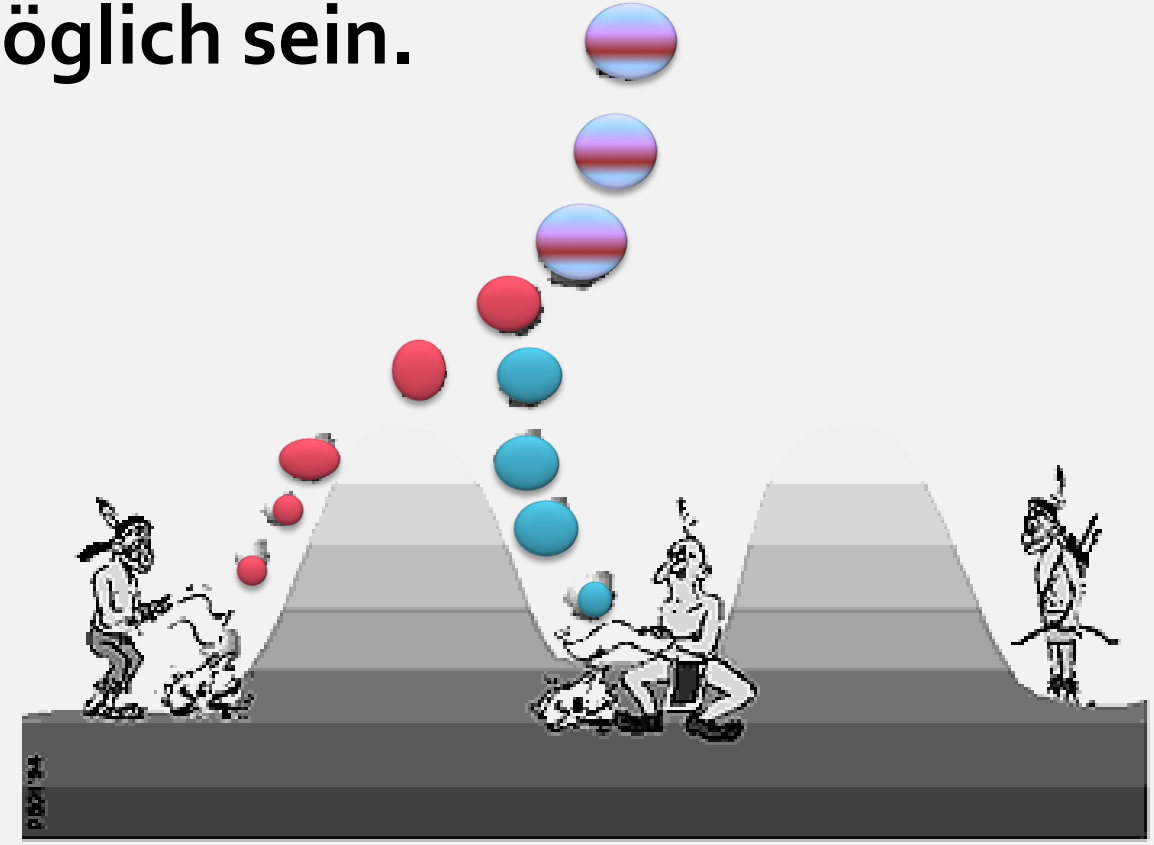


Integrität

Unversehrtheit der gesendeten bzw. gespeicherten Daten.

Integrität

Eine Veränderung oder Verfälschung von Nachrichten auf dem Übermittlungsweg darf nicht möglich sein.



Verbindlichkeit

Nachweis der Identität der Informationsquelle
(Authentizität)

+

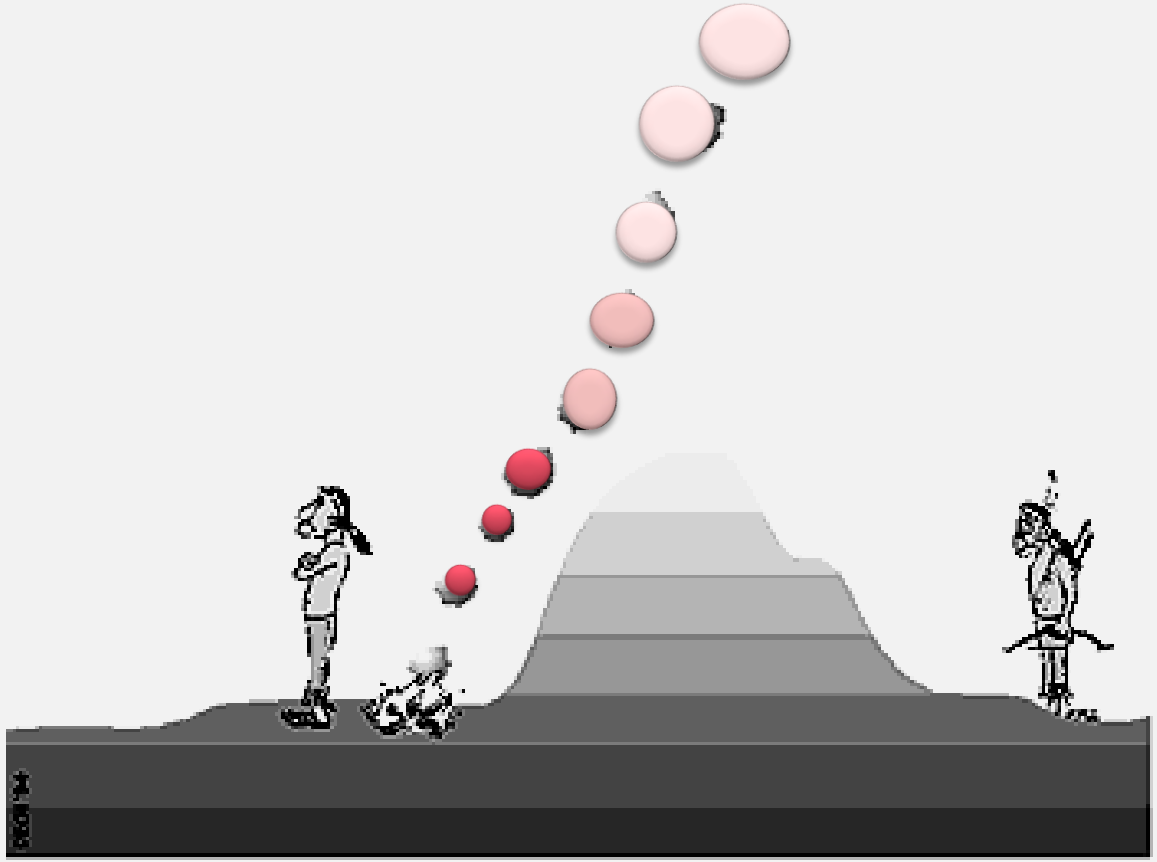
Nachweis für die Ausführung der Handlung
(Nichtabstreitbarkeit)

Verbindlichkeit-Authentizität

Für den Empfänger einer Nachricht muss erkennbar und nachweisbar sein, wer die Informationsquelle ist. Der Empfänger muss sich sicher sein, dass nicht ein anderer in dessen Namen handelt.

Verbindlichkeit- Unabstreitbarkeit

Absicherung, dass der Empfang der Nachricht vom Empfänger nicht abgestritten werden kann.

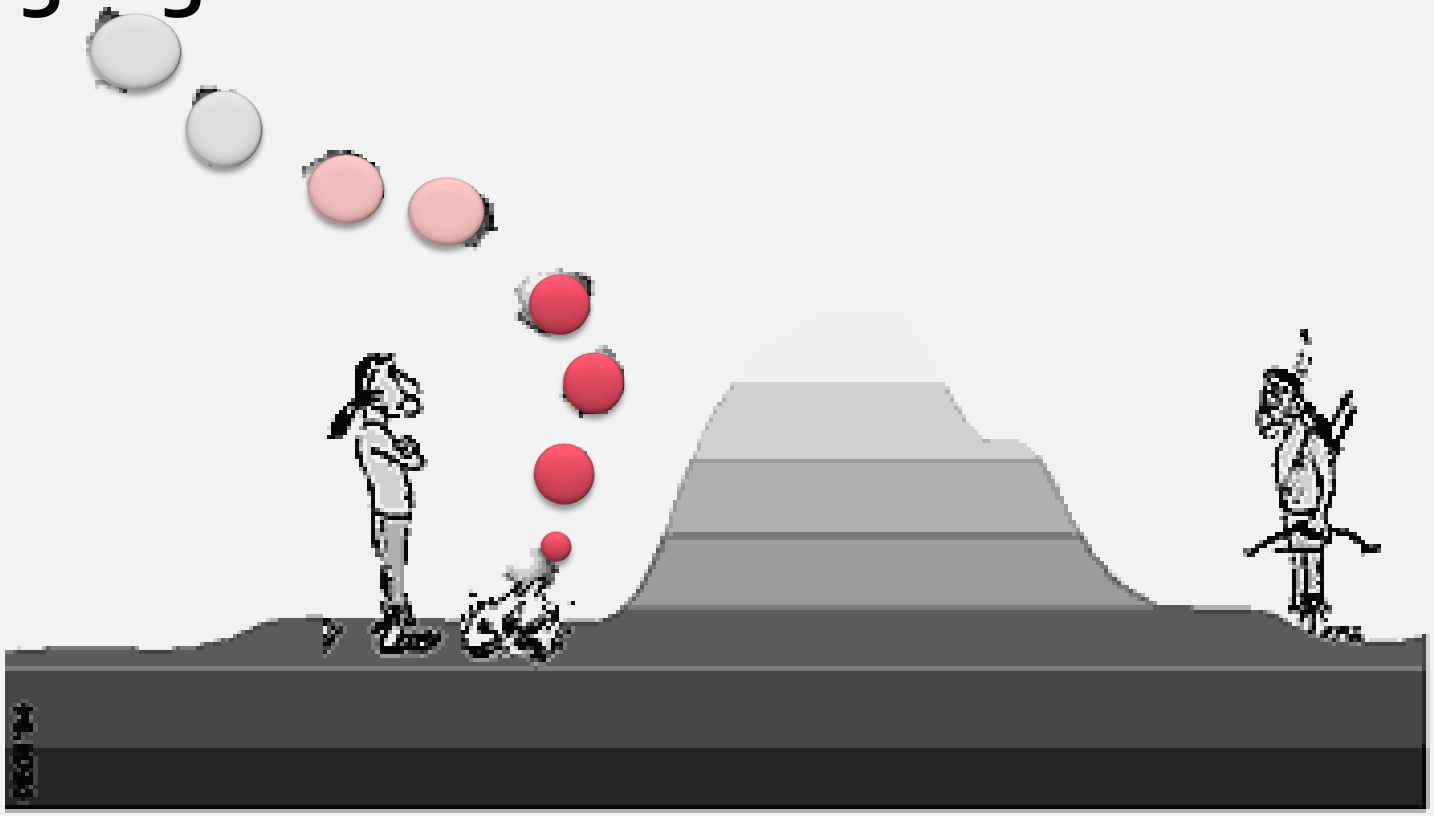


Verfügbarkeit

Daten stehen zuverlässig zur Verfügung, wenn sie benötigt werden.

Verfügbarkeit

Absicherung, dass alle erforderlichen Daten zum richtigen Zeitpunkt am richtigen Ort zur Verfügung stehen.



Zigtausende Täter-Daten wie Fingerabdrücke sind im Landeskriminalamt Sachsen-Anhalt gelöscht worden. Foto: dpa

Durch einen Löschfehler sind 42.000 von rund 60.000 erkennungsdienstlichen Daten von Straftätern seit Januar auf einen Schlag weg.

Von Matthias Fricke ›

Magdeburg I Als Ermittler eines Revieres in Sachsen-Anhalt es im Februar mit einem Raub zu tun haben, sind sie ganz sicher, dass sie den Täter kennen. Sie lassen ihre gesicherten Spuren im Polizeilichen Informationssystem (INPOL) gegenlaufen, doch der Abgleich ergibt auch nach mehrmaligem Versuch keinen Treffer. Erst eine Nachfrage im Landeskriminalamt (LKA) bringt es ans Licht: Die Daten sind gelöscht, obwohl es sich um einen Serientäter handelt. „Skandalös ist, dass man uns nicht informiert hat", sagt ein Kriminalist, der nicht genannt werden will.

Von rund 60.000 Datensätzen sind 41.875 gelöscht worden. Das bestätigt LKA-Sprecher Michael Klocke der Volksstimme und spricht von einer „Fehlerkette", die zur Löschung geführt habe. Betroffen sei der erkennungsdienstliche Teil des Informationssystems, in dem unter anderem Fingerabdrücke, Porträtaufnahmen, Tätowierungen und Auffälligkeiten bei Personenbeschreibungen (z.B. Narben) gespeichert sind. Diese Datei-Gruppe ist erst vor kurzem vom Bundeskriminalamt (BKA) an die Länder rückübertragen worden. Nötig wurde dies durch ein kompliziertes System von unterschiedlichen gesetzlichen Löschfristen nach einem Urteil des Bundesverwaltungsgerichtes, so Klocke.

Montag, 1. März 2021

NACHRICHTEN

SACHSEN-ANHALT

42.000 Täterdaten bei Polizei gelöscht

MAGDEBURG – Aus einer Datenbank der Polizei sind versehentlich rund 42.000 Datensätze zu Straftätern aus Sachsen-Anhalt gelöscht worden. Die Datensätze enthalten Fingerabdrücke, Porträtaufnahmen sowie Besonderheiten wie Tätowierungen und Narben von Tätern. Eine Fehlerkette, die im Landeskriminalamt (LKA) in Magdeburg geendet habe, führte zur Löschung, erklärte ein Sprecher am Samstag. Aus der Landespolitik kam am Wochenende die Forderung nach Aufklärung des Vorfalls. Zudem kritisierten innenpolitische Sprecher mehrerer Landtagsfraktionen, aus dem Medien davon erfahren zu haben. Eine Rettung ist aber wahrscheinlich: Im Bundeskriminalamt existiere eine Datenbanksicherung, aus der die gelöschten Daten wiederhergestellt werden könnten, so das LKA. lpga

Im konkreten Fall standen alle Daten zur Lösch-Prüfung an, weil die Fristen überschritten waren. Diese hätten deshalb längst an die jeweils vor Ort ermittelnden Dienststellen weitergeleitet werden müssen, um zu kontrollieren, ob der Täter erneut straffällig wurde, beziehungsweise eine negative Rückfallprognose hat. Ist das der Fall, kann die Löschfrist verlängert werden. Klocke: „Bisher ist unklar, in welchem Umfang eine vorherige Prüfung der zu löschenden Gruppen vorgenommen wurden." Dies müsse geklärt werden.

Man arbeite mit Hochdruck an der Lösung des Problems. Der LKA-Sprecher: „Im Bundeskriminalamt, die die Plattform INPOL bereitstellt, existiert eine Datenbanksicherung, aus der die gelöschten Daten voraussichtlich vollständig wiederhergestellt werden könnten." Ob und unter welchen datenschutzrechtlichen Voraussetzungen dies erfolgen darf, werde noch geprüft. Der Landesbeauftragte für Datenschutz sei „bereits informiert worden". Eine Rettung bleibt also vorerst noch offen.

Olaf Sendel von der Deutschen Polizeigewerkschaft, der erst von der Volksstimme von der Panne erfuhr: „Da hat man uns einen Bärendienst erwiesen." Schwere Straftaten würden oft durch Spuren-Personen-Treffer aufgeklärt. Dies sei nun nicht mehr möglich. Er fürchtet: „Straftäter haben jetzt eine Freifahrkarte."

Angriffe auf Daten im Netzwerk

Vertraulichkeit

Sniffing
= Schnüffeln

Abhören und Auswerten des Datenverkehrs
z.B. Cookies, Echelon → Abhörsystem USA,GB im kalten Krieg

Phishing
= Abfischen

sensible Daten/ Passwörter
z.B. angebliche Emails und Webseiten von Banken

Integrität Authentizität

Spoofing
= Täuschung

Verschleierung und Fälschung der Identität des Absenders
z.B. falsche Absender von, Gewinn-Mails

Video 2

Angriffe auf Daten im Netzwerk

Verfügbarkeit

Denial-of-Service (DoS)

Lahmlegen eines Servers mit Backdoors, Email-Bomben, Spamming

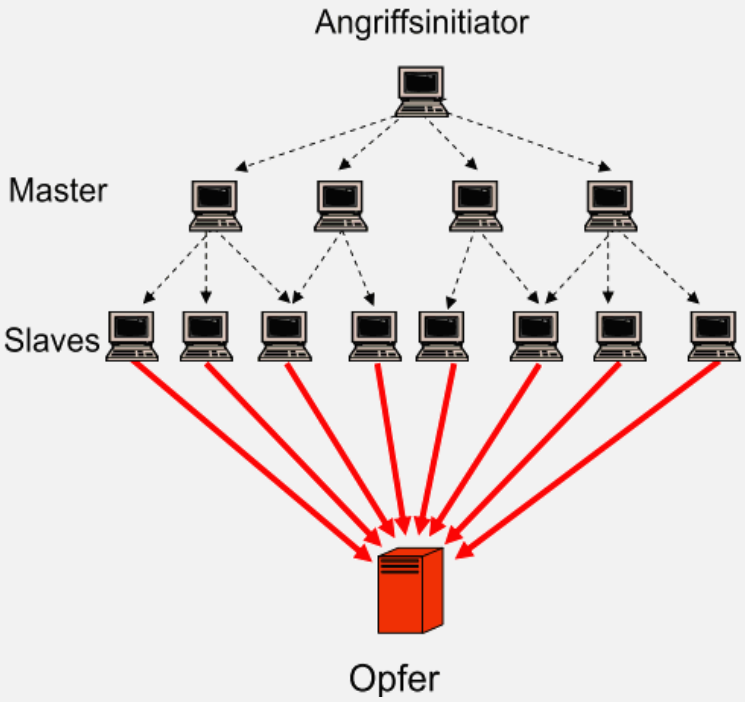
Schadpro-gramme

Viren, Würmer, Trojanische Pferde, Exploits, fehlerhafte Software

Video 3

Angriffe auf Daten im Netzwerk

Was ist ein Denial-of-Service (DoS) - Angriff?



Wird ein DoS ausgeführt,
geschieht das mit der Absicht, einen Server und dessen Dienste arbeitsunfähig zu machen.
-> wirtschaftliche Schäden, Provokation, Cyberterror

Aktuelles Beispiel: Angriffe auf LernSax

Video 4

Anforderungen an die Sicherheit

Schutzziele für den Umgang mit Daten

Schau dir bitte das folgende Video an, dort werden die auf der nächsten Folie angegeben Schutzmaßnahmen einzeln besprochen.
Notiere zu den einzelnen Punkten Beispiele / Erläuterung aus dem Video.

Video 5

Schutzmaßnahmen

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellbarkeit
- Datenintegrität
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennbarkeit

Ein 100% er Schutz ist unmöglich! Wichtig ist ein gesundes Verhältnis zwischen Komfort und Risiko.

So nicht ! ☺
Danke für die Aufmerksamkeit