IT-Sicherheit (WS 2016/17)

Kapitel 1: Grundlagen

Stefan Edelkamp

edelkamp@tzi.de

(Based on slides provided by Andreas Heinemann)

Einführung

teaser-of-the-day

09.04.2015 05:36

Islamisten hacken TV5 UPDATE

Kurz vor 22 Uhr gingen Mittwochabend alle Kanäle des Fernsehunternehmens TV5Monde in Frankreich offline. Die Website sowie die Präsenz auf Facebook verbreiteten kurzfristig islamistische Drohungen. Unter anderem sollen dort Lebensläufe und Ausweisdokumente von Angehörigen französischer Soldaten veröffentlicht worden sein. Die Islamisten drohen diesen Zivilisten, weil die Soldaten militärisch gegen islamistische Verbrecher vorgehen.

Parallele Angriffe auf mehreren Ebenen

Die IT-Chefin des betroffenen Medienunternehmens, Hélène Zemmour, gab francetvinfo noch in der Nacht ein kurzes Interview. Sie berichtete, dass die Angreifer gleichzeitig die internen IT-Systeme und die Sendeanlagen von TV5Monde unbrauchbar gemacht sowie die Kontrolle über die Webseite erlangt hätten.

- Quelle: http://www.heise.de/security/meldung/Islamisten-hacken-TV5-2597578.html

Motivation

Beinahe täglich werden sicherheitskritische Schwachstelle von und Angriffe auf informationsverarbeitende Systeme veröffentlicht. Beispiele

- Anfang 2015: Malware auf Kassensystemen von US-Handelsketten greifen Kreditkarteninformationen ab
  http://blogs.cisco.com/security/talos/POSeidon
- Mitte 2014: Programmierfehler in OpenSSL (Heartbleed) kann zur Ausspähung von Passwörter genutzt werden
  http://heartbleed.com/
- Anfang 2014: 18 Millionen E-Mail-Konten unter Nutzung von Botnetzen gestohlen
  https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Neuer_Fall_von_Identitaetsdiebstahl_07042014.html

Motivation für Angreifer

- Klassische Angreifer
  - White-Hat: Aufdecken von Sicherheitslücken
  - Geheimdienste: Spionage, Sabotage und Überwachung
  - Unternehmen: Wirtschaftsspionage (Zusammenarbeit mit Geheimdiensten)

- Neuere Entwicklungen
  - Etablierung einer stark professionalisierten Schattenwirtschaft (Black-Hat, Auftragshacking)
  - Veröffentlichung geheimer Informationen (Whistleblower)
  - politisch motivierte Angriffe

Motivation für Angreifer (Fortsetzung)

Schattenwirtschaft:

- Mit erfolgreichen Angriffen lässt sich viel Geld verdienen
  - Fälschung von PayTV-Karten
  - Abgreifen von Kreditkarteninformationen (Warenkreditbetrug)
  - Phishing-Angriffe im Bereich Online-Banking

- Darüber hinaus gibt es einen etablierten Schwarzmarkt für Verwundbarkeiten von IT-Systemen (Exploits)

Angriffsarten - Überblick / Beispiele

- Ungezielte Angriffe z.B. über Massen-E-mails, mit denen Viren, Würmer und Trojaner versandt oder Phishing-Angriffe durchgeführt werden
- Gezielte Angriffe, z.B. zur Sabotage und Spionage, die auf bestimmte Institutionen gerichtet sind (DDoS-Angriffe auf staatliche Infrastrukturen)
- Skalpelartige Angriffe, z.B. gezielte Sabotage auf bestimmte IT-Systeme (Beispiel Stuxnet) oder auf Zertifikatediensteanbieter (Beispiel Fälschung von SSL-Zertifikaten der niederländischen Firma DigiNotar im Juli 2011, hiervon war auch das Serverzertifikat von google.com betroffen).

Schwachstellen in Software

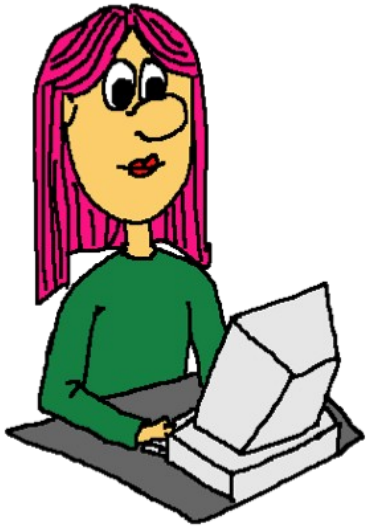
Einer der Gründe für erfolgreiche Angriffe ist die Fehleranfälligkeit von Software

- Heutige Betriebssysteme haben ca. 86.000.000 Zeilen Source-Code
- Untersuchungen zeigen: Fehlerquote liegt bei ca. 0.25%
- Also ca. 200.000 potentiell ausnutzbare Fehler
- Hinzu kommt die Anwendungssoftware

DAS
Kommunikationsmodell der IT-Sicherheit

DAS Kommunikationsmodell der IT-Sicherheit

- Akteure: Alice, Bob und Mallory



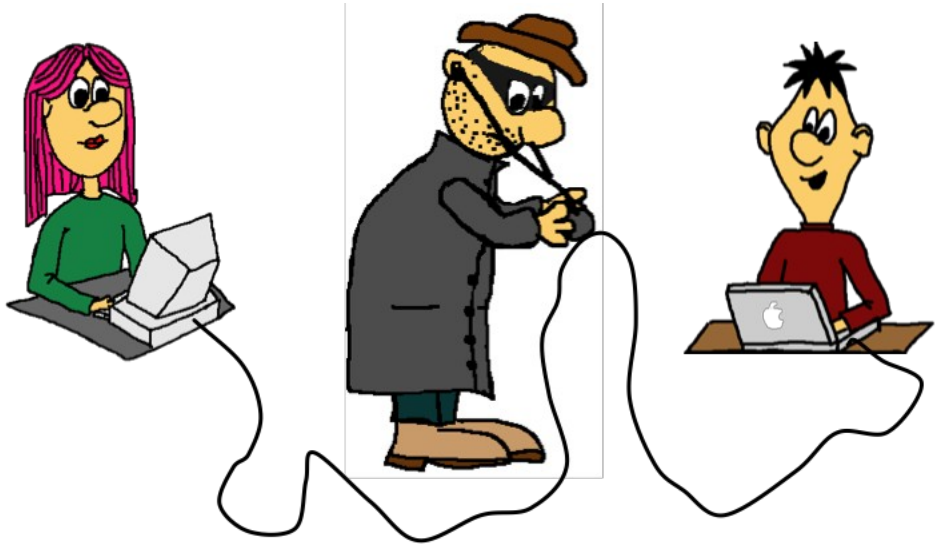
Alice

Bob

Mallory

DAS Kommunikationsmodell der IT-Sicherheit

- Alice und Bob tauschen Nachrichten über einen unsicheren Kommunikationskanal aus
- Mallory versucht alles, um die Kommunikation zwischen Alice und Bob anzugreifen.



DAS Kommunikationsmodell der IT-Sicherheit

- Fähigkeiten von Mallory

Mallory kann die Leitung abhören („passiver Angriff“)

DAS Kommunikationsmodell der IT-Sicherheit

- Fähigkeiten von Mallory

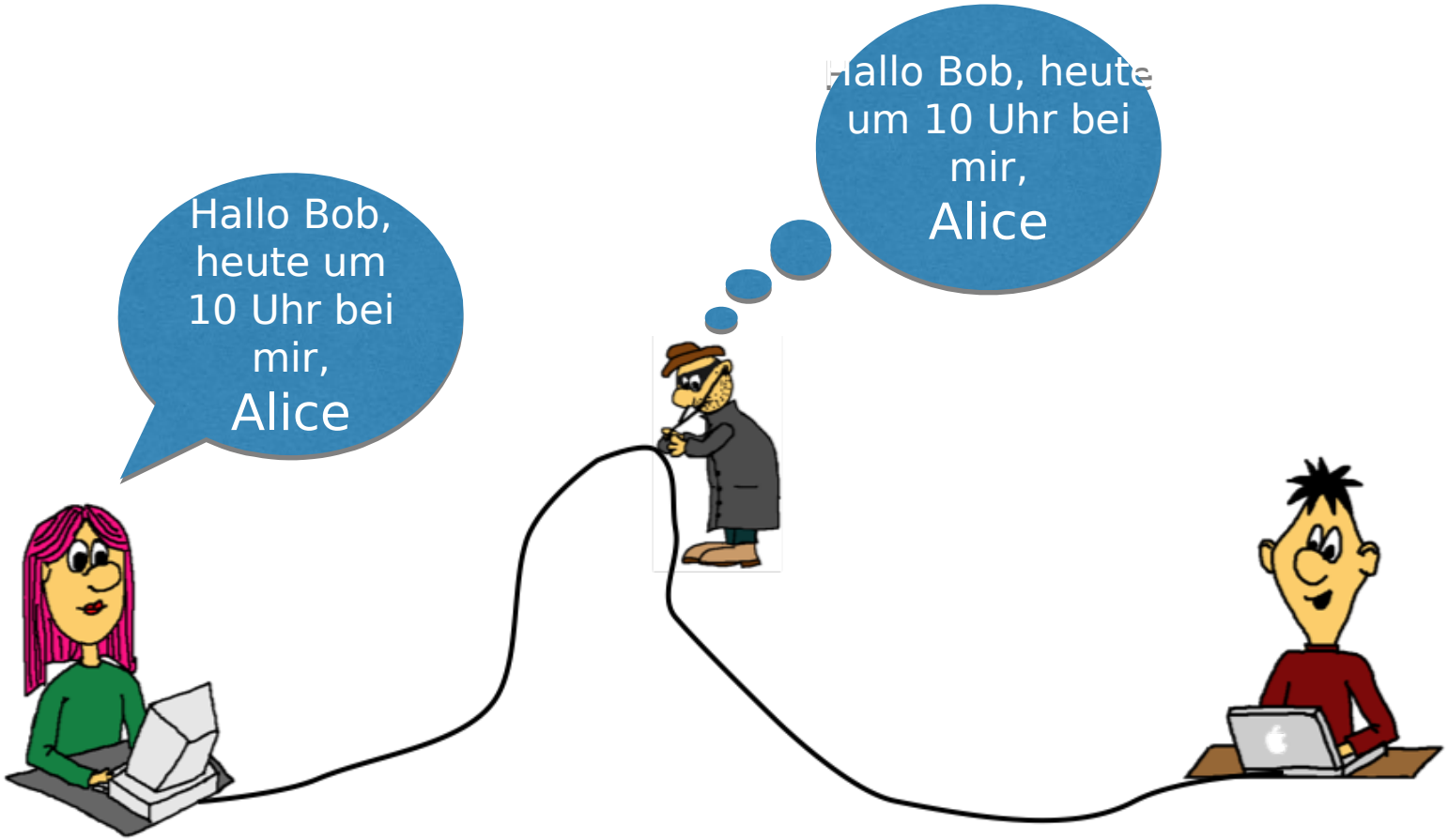
Mallory kann die Leitung manipulieren („aktiver Angriff“)

DAS Kommunikationsmodell der IT-Sicherheit

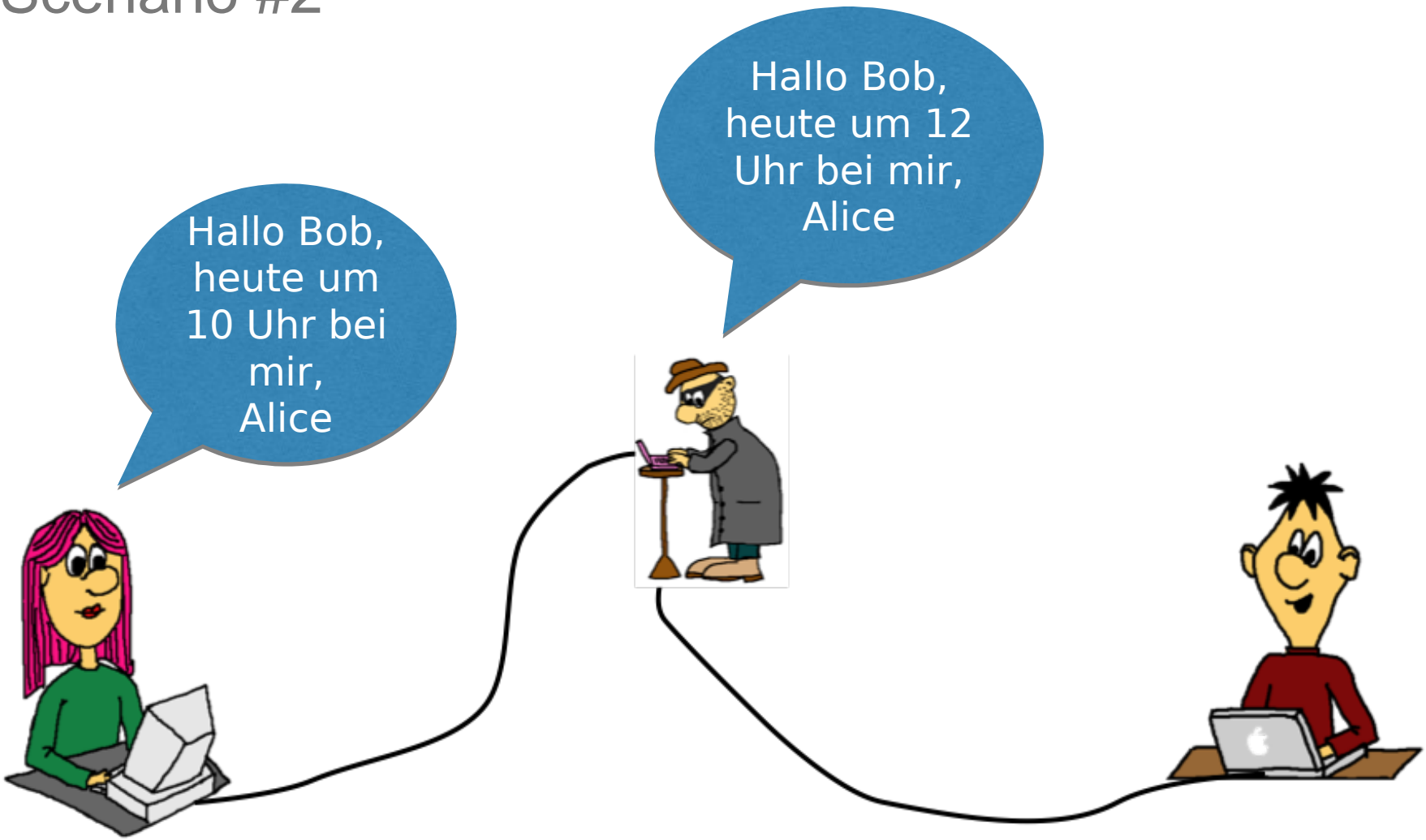
- Fähigkeiten von Mallory

Mallory kann die Leitung kappen („aktiver Angriff“)

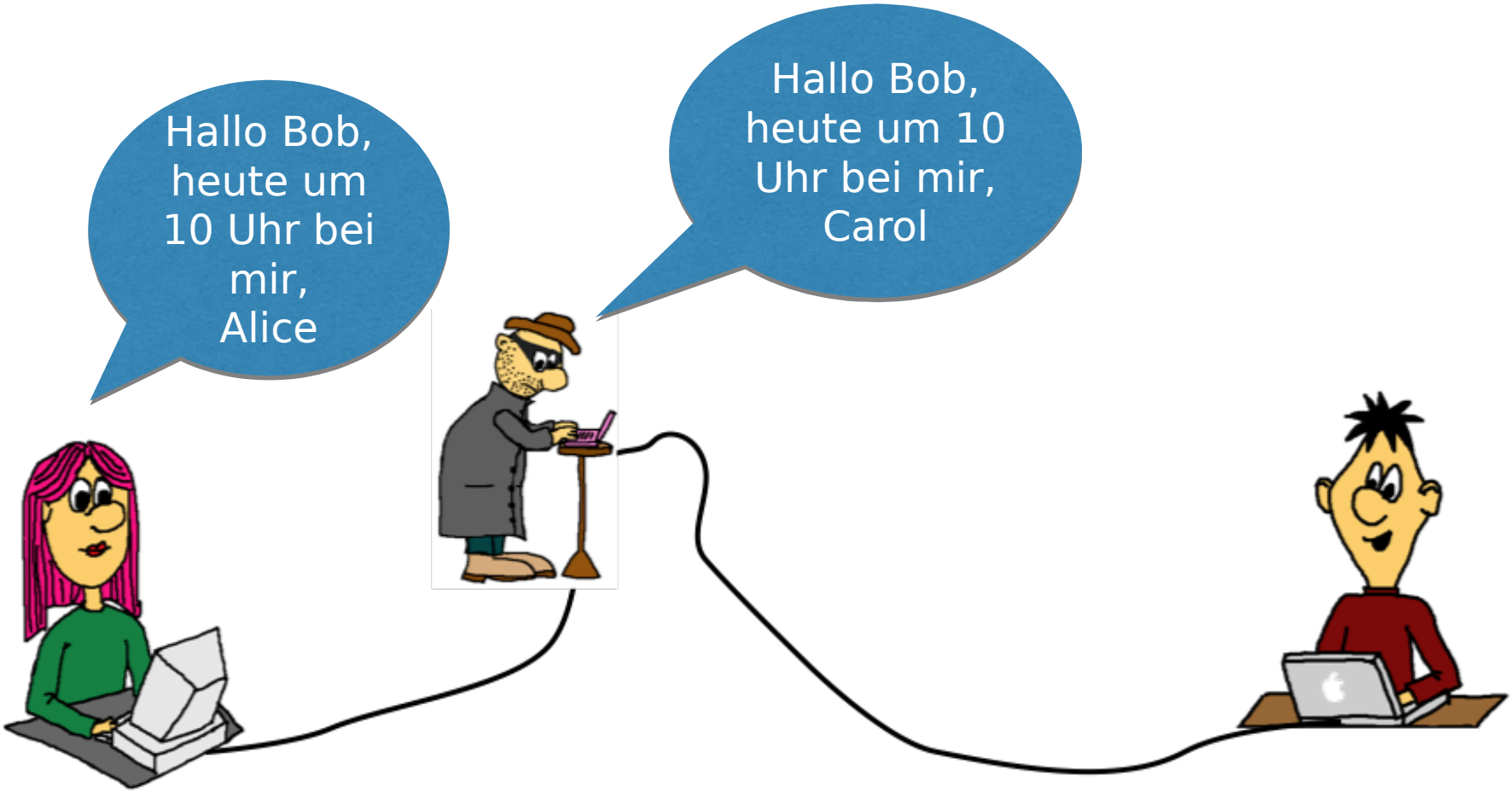
Szenario #1


Hallo Bob, heute um 10 Uhr bei mir,
Alice
Hallo Bob, heute um 10 Uhr bei mir,
Alice

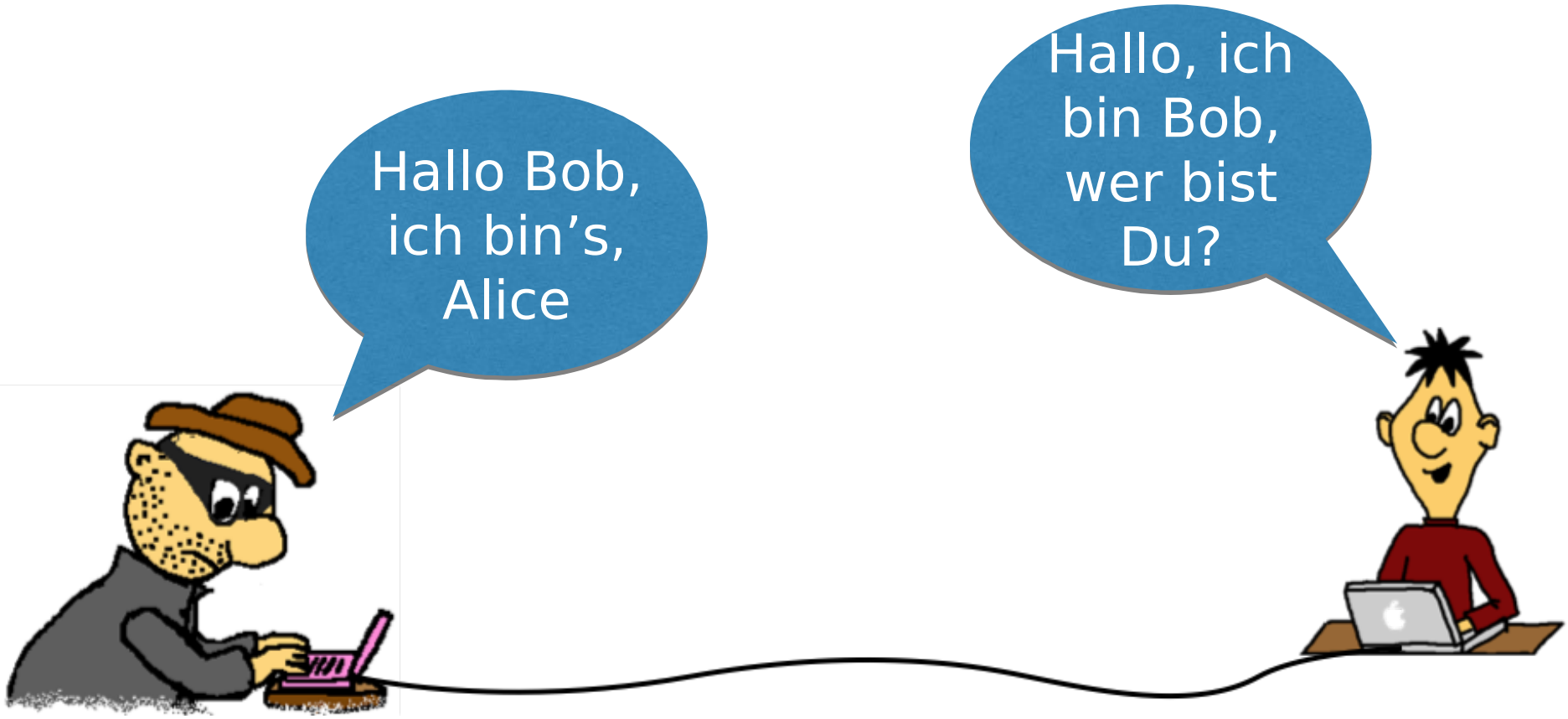
Scenario #2


Hallo Bob, heute um 10 Uhr bei mir, Alice
Hallo Bob, heute um 12 Uhr bei mir, Alice

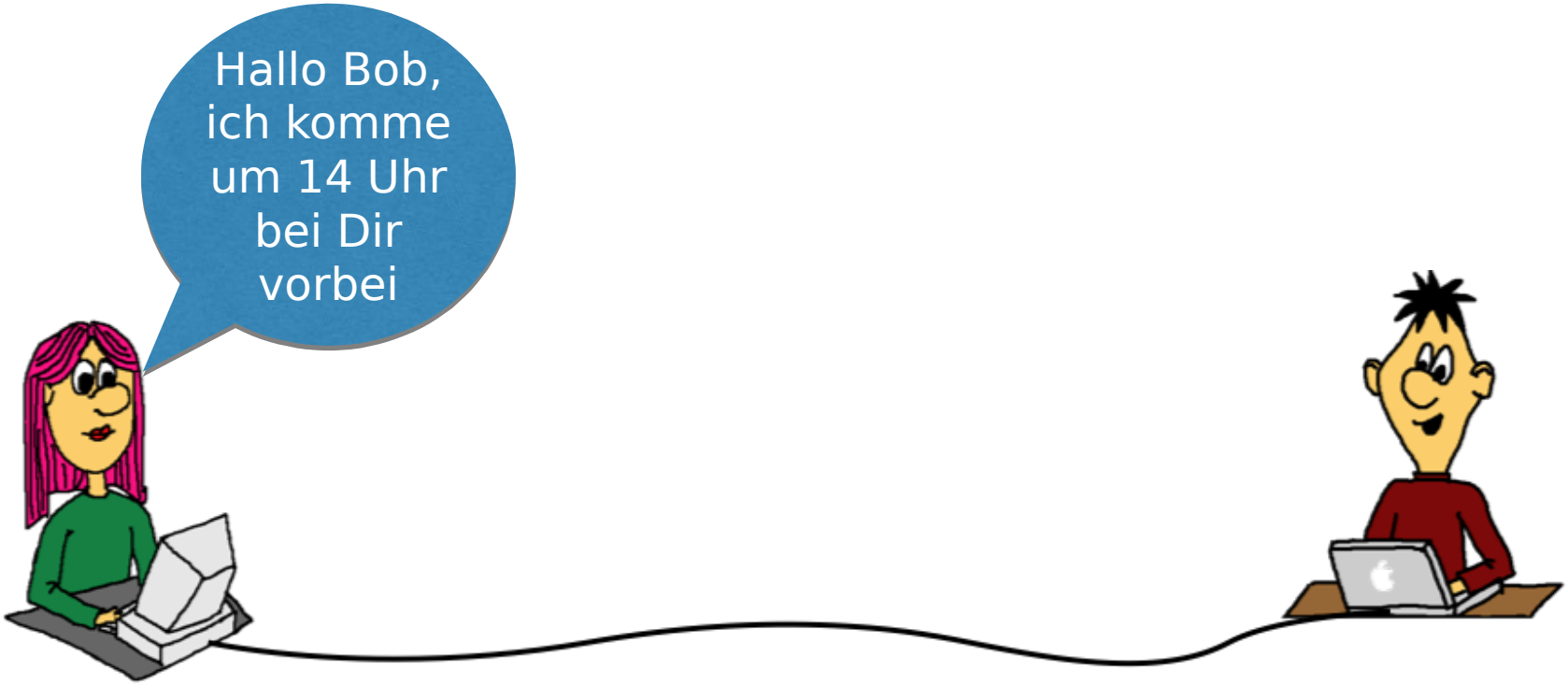
Szenario #3


Hallo Bob, heute um 10 Uhr bei mir, Alice
Hallo Bob, heute um 10 Uhr bei mir, Carol

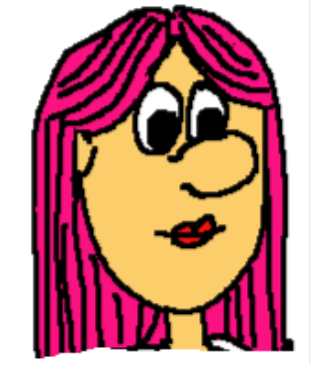
Szenario #4



Szenario #5 (1/2)



Szenario #5 (2/2)

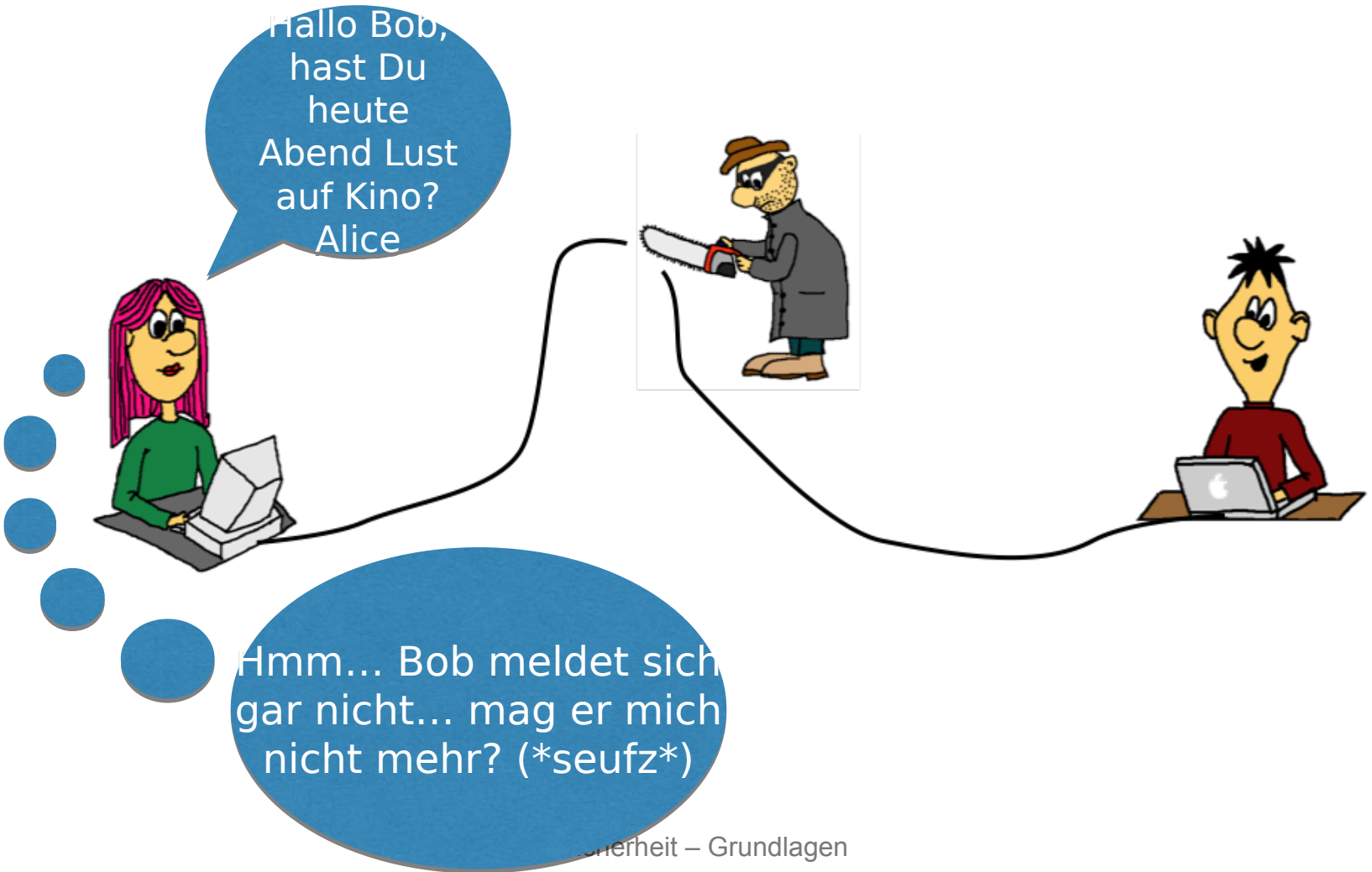


Hallo Bob, da bin ich!

Ähh, hmm… stimmt doch gar nicht. Wir haben doch 16 Uhr ausgemacht

HALLO (*grumpfl*), DU BIST 2 STUNDEN ZU SPÄT!!! WAS SOLL DAS??? ICH HABE DIE GANZE ZEIT GEWARTET!!!

Szenario #6


Hallo Bob, hast Du heute Abend Lust auf Kino? Alice
Hmm... Bob meldet sich gar nicht... mag er mich nicht mehr? (*seufz*)

Zwischenfazit

Aus den Szenarien #1 bis #6 können wichtige Schutzziele der IT-Sicherheit abgeleitet/formuliert werden.

//www.heise.de/security/meldung/Angriffe-auf-kritische-Luecke-Flash-Patch-ist-da-3165410.html

teaser-of-the-day

Adobe liefert einen Notfall-Patch für Flash aus, der 24 Sicherheitslücken stopft. Eine davon soll derzeit unter Windows aktiv ausgenutzt werden, um Erpressungs-Trojaner auszuliefern.

Wer den Flash Player unter Windows nutzt, sollte schleunigst die installierte Version prüfen. Denn die Versionen bis jeweils einschließlich 21.00.197 (Windows und OS X), 18.0.0.333 (Extended Support Release Windows und OS X) und 11.2.202.577 (Linux) sind verwundbar, warnt Adobe.

Grundlegende Begriffe

Grundlegende Begriffe

- Information und Daten
- IT-System und IT-Verbund
- Sicherheit (Betriebs- und Informationssicherheit)
- Schutzziele
- Bedrohung, Gefährdung, Angriff, Risiko

Information

- Definition des Begriffs nach deutschem Duden:
  - das Informieren; Unterrichtung über eine bestimme Sache; Kurzwort: Info
  - [auf Anfrage erteilte] über alles Wissenswerte in Kenntnis setzende, offizielle, detaillierte Mitteilung über jemanden, etwas
  - Äußerung oder Hinweis, mit dem jemand von einer [wichtigen, politischen] Sache in Kenntnis gesetzt wird
- Eine Information hat für den Empfänger **i.d.R.** einen Neuigkeitsgehalt
  - Ihre Form kann unterschiedlich sein: gesprochen, geschrieben, gedacht, elektronisch

Informationen als schützenswerte Güter

- Verlust des informationellen Selbstbestimmungsrechts (Datenschutz): Informationen über Krankheiten, Einkommen etc.
- Finanzielle Verluste: Geschäftsgeheimnisse, Verträge, Zugangsdaten zum Online-Banking etc.
- Persönliche Unversehrtheit: Fehlfunktionen medizinischer Überwachungsgeräte, Verkehrsleitsysteme etc.
- Die Betrachtung/Beurteilung hinsichtlich IT-Sicherheit erfolgt meist ausgehend von den schützenswerten Informationen

Daten

- Daten in der Informatik sind Repräsentationen von Informationen, z.B.
  - als Bytefolge gespeichert auf einer Festplatte
  - als Netzwerkpaket bei der Übertragung über das Internet

- Der Begriff der Datensicherheit ist also spezieller als Informationssicherheit zu verstehen
  - Datensicherheit: Beschäftigt sich mit der Sicherheit von Daten
  - Informationssicherheit: Beschäftigt sich mit der Sicherheit von Informationen (und damit auch von Daten, die die Informationen repräsentieren)

IT-System

- Ein IT-System ist ein dynamisches technisches System mit der Fähigkeit zur Verarbeitung und Speicherung von Daten
- Beispiele
  - Computer, Smartphones, Tablet-PCs
  - Drucker, Scanner
  - Router, Switch, Firewall

IT-Verbund

- Ein Informationsverbund (IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten, die der Aufgabenerfüllung in einem bestimmen Anwendungsbereich der Informationsverarbeitung dienen.
- Unterschiedliche Ausprägungen möglich. Beispiele
  - eine gesammten Institution (Firma, Behörde)
  - einzelne Bereiche einer Institution, die
    - in organisatorische Strukturen (Abteilung) gegliedert sind oder
    - gemeinsame Geschäftsprozesse bzw. Anwendungen haben

Sicherheit

- Allgemein versteht man unter Sicherheit den Schutz vor negativen Konsequenzen aus vorsätzlichen und berechtigten Handlungen
- In Bezug auf IT-Systeme unterscheidet man zwei Arten von Sicherheit
  - Schutz vor negativen Konsequenzen aus berechtigten Handlungen: Betriebssicherheit / Funktionssicherheit (*safety*)
  - Schutz vor negativen Konsequenzen aus vorsätzlichen / unberechtigten Handlungen: Informationssicherheit (*security*)

Prävention

- Kernbestandteil von Betrachtungen über Sicherheit ist in erster Linie Prävention von vorsätzlichen Handlungen
- Beispiele
  - Physikalische Sicherheitsmerkmale auf Geldscheinen (Fälschungssicherheit), wie z.B. Wasserzeichen, Sicherheitsfaden, Infrarot- und UV-Farben
  - Physikalische und kryptographische Sicherheitsmerkmale bei hoheitlichen Dokumenten (Fälschungs- und Verfälschungssicherheit)
  - Härtung von IT-Systemen durch Penetrationstests
  - Verschlüsselung von Dokumenten, E-Mails

Schutzziele

- Klassische Schutzziele:
  - **C**onfidentiality (Vertraulichkeit)
  - **I**ntegrity (Integrität)
    - Authentizität (engl. Authenticity)
    - Nichtabstreitbarkeit (engl. Non-Repudiation)
  - **A**vailability (Verfügbarkeit)

- Schutzziele bzgl. Datenschutz
  - Anonymität
  - Pseudonymität

Schutzziel *Vertraulichkeit*

- Vertraulichkeit soll sicherstellen, dass Informationen nur autorisierten Personen zugänglich sind.
- Maßnahmen zur Umsetzung des Schutzziels Vertraulichkeit:
  - Kryptographische Verschlüsselungsverfahren
  - Überbringen von Dokumenten durch vertrauenswürdigen Kurieren
  - Zutrittsregeln (Gebäudesicherung, Raumsicherung)
  - Zugriffskontrollen (geeignete Leserechte für gespeicherte Dateien/Verzeichnisse)

Schutzziel *Integrität*

- Unter Integrität versteht man die Vollständigkeit und Unverfälschtheit der Daten für den Zeitraum, in dem sie von einer autorisierten Person erstellt, übertragen oder gespeichert wurden. Darin sind sowohl absichtliche als auch unabsichtliche, z. B. durch technische Fehler verursachte, Veränderungen enthalten.
- Maßnahmen zur Umsetzung des Schutzziels Integrität
  - Kryptographische Hashfunktionen
  - Sichere Aufbewahrung von Kopien zum späteren Abgleich mit dem Original
  - Zugriffs- und Zutrittsregeln

Schutzziel *Daten- und Nachrichtenauthentizität*

- Die Authentizität von Daten/Nachrichten ist gewährleistet, wenn der Urheber der Daten vom Empfänger eindeutig identifizierbar und seine Urheberschaft nachprüfbar ist. Dies beinhaltet auch die Integrität der Daten.

- Maßnahmen zur Umsetzung des Schutzziels Datenauthentizität
  - elektronische Signaturen
  - händisches Unterschreiben eines Dokumentes
  - persönliche Übergabe von Daten

Schutzziel *Instanzauthentizität*

- Ein Objekt oder Subjekt wird als authentisch bezeichnet, wenn dessen Echtheit und Glaubwürdigkeit anhand einer eindeutigen Identität und charakteristischer Eigenschaften überprüfbar ist.

- Maßnahmen zur Umsetzung des Schutzziels Instanzauthentizität:
  - Benutzername/Passwort
  - Challenge-Response-Protokolle
  - Abgleich der Identität auf Basis hoheitlicher Dokumente (Reisepass, Personalausweis)

Schutzziel *Nichtabstreitbarkeit (Verbindlichkeit)*

- Die Nichtabstreitbarkeit von Daten ist gewährleistet, wenn der Ersteller der Daten die Erzeugung im Nachhinein nicht abstreiten kann (gerade auch gegenüber Dritten)

- Maßnahmen zur Umsetzung des Schutzziels Nichtabstreitbarkeit:
  - elektronische Signaturen
  - händische Unterschrift
  - Nutzung vertrauenswürdiger Zeugen (z.B. Notar)

Integrität vs. Authentizität vs. Nichtabstreitbarkeit

Abgrenzung der Begriffe

- Offensichtlich gilt:
  - Aus der Nichtabstreitbarkeit folgt die Authentizität
  - Aus der Authentizität folgt die Integrität

- Die Umkehrung gilt im Allgemeinen nicht:
  - Sicheres Aufbewahren einer Kopie zum späteren Abgleich sorgt für die Integrität, es kann damit aber nicht festgestellt werden, wer die Daten erzeugt hat.
  - Bei einer persönlichen Übergabe weiß der Empfänger, von wem er die Daten hat, kann dies aber gegenüber einem Dritten nicht nachweisen.

Authentisierung vs. Authentifizierung

Abgrenzung der Begriffe

- Authentisierung: Nachweis der Identität
  - Ich weise mich durch Eingabe meines Benutzernamens/Passwortes aus
  - Ich weise mich mit meinem Personalausweis aus
- Authentifizierung: Prüfung des Nachweises
  - Benutzername/Passwort wird geprüft
  - Personalausweis und Verknüpfung mit meiner Person werden geprüft
- Nach der Authentifizierung ist/wird das Subjekt autorisiert entsprechend seiner Berechtigungen zu arbeiten

Schutzziel *Verfügbarkeit*

- Ein IT-System gewährt Verfügbarkeit, wenn autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können
- Die Messung der Verfügbarkeit erfolgt üblicherweise nach folgender Formel:

$$\text{Verfügbarkeit} = \frac{\text{Gesamtlaufzeit} - \text{Ausfallzeit}}{\text{Gesamtlaufzeit}}$$

- Maßnahmen zur Umsetzung der Verfügbarkeit
  - Datensicherung
  - Vertretungsregeln
  - redundante Auslegung von Komponenten

Beispiel Verfügbarkeit von Cloud Diensten

Cloud-Speicherdienste im Vergleich

Ausgewählte Ergebnisse einer Untersuchung des Hasso-Plattner-Instituts (HPI)

	Amazon S3	Google Cloud Storage	Hewlett Packard Cloud Object Storage	Rackspace Cloud Files	Windows Azure
Speicherkosten in US-Dollar pro GB/Monat	0,055*	0,054*	0,09	0,075*	0,037*
Garantierte Verfügbarkeit in %	99,9	99,9	99,95	99,9	99,95
Datenverschlüsselung möglich	✓	✓	✓	✗	✓
Datenzugriff nach Vertragsende	✓	✗	✓	✗	✓
Mindestens ein Standort in der EU	✓	✓	✗	✓	✓
Nutzerseitiges Eigentumsrecht an den Daten	✓	✓	✗	✓	✓
Insolvenzfall geklärt	✗	✗	✗	✗	✗

Ja ✓
Nein ✗

*Angabe beschreibt niedrigst zu erreichenden Preis. Die Preise hängen von geografischer Region und genutztem Speicher- und Transfer-Volumen ab.

Der Test wurde von November 2012 bis Juli 2013 durchgeführt. Ausführliche Informationen im Technischen Bericht Nr. 84, erschienen im Universitätsverlag Potsdam, ISBN 978-3-86956-274-2.

“On the Internet, nobody knows you’re a dog”

- Cartoon, Peter Steiner, The New Yorker, July 5, 1993
- Internet wird in einer breiteren Masse der Bevölkerung wahrgenommen
- unterstreicht die damalige Anonymität bei der Dienstenutzung im Internet

Quelle: Wikipedia

Schutzziel *Anonymität* und *Pseudonymität*

- Anonymität
  Personenbezogene Daten werden so verändert, dass diese nicht oder nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können.

- Pseudonymität
  Personenbezogene Daten werden so verändert, dass diese nur unter Kenntnis der Zuordnungsvorschrift einer Person zugeordnet werden können.

Abgrenzung Anonymität und Pseudonymität

Abgrenzung der Begriffe

- Beispiele für Anonymität sind
  - Aliase/*nicknames* in Foren, Chaträumen, die keine Anmeldung erfordern oder keine personenbezogenen Daten erheben

- Beispiele für Pseudonymität sind
  - Matrikelnummern
  - Aliase/*nicknames* in Webdiensten wie ebay, amazon (diese erheben personenbezogene Daten)

IT-Sicherheit

- Ziel der IT-Sicherheit ist die Verfügbarkeit der Daten, Dienste und Anwendungen zu gewährleisten, sowie die Integrität und Vertraulichkeiten der Daten sicher zu stellen.

- Wichtige Begriffe
  - Gefahr, Bedrohung, Gefährdung
  - Schwachstelle
  - Angriff
  - Schadensszenario
  - Risiko

Gefahr

- Eine Gefahr ist ein Sachverhalt, bei dem ohne konkreten zeitlichen, räumlichen oder personellen Bezug bei ungehindertem Ablauf des zu erwartenden Geschehens in absehbarer Zeit mit hinreichender Wahrscheinlichkeit ein Schaden für ein schutzwürdiges Gut eintreten wird.

- Beispiele
  - Hochwasser (Gefahr für Leib und Leben, finanzieller Verlust)
  - Pest (Gefahr für Leib und Leben)

Bedrohung

- Eine Bedrohung ist eine Gefahr mit zeitlichem, räumlichem oder personellem Bezug zu einem Schutzziel.

- Beispiele
  - Hochwasser ist eine Bedrohung für Leib und Leben von Menschen an der Oder (aber nicht in Darmstadt)
  - Pest ist eine Gefahr für Leib und Leben, aber keine Bedrohung (der Pesterreger ist ausgestorben)

Gefährdung

- Eine Gefährdung bezieht sich ganz konkret auf eine bestimmte Situation oder auf ein bestimmtes Objekt und beschreibt die Wahrscheinlichkeit, mit der eine potenzielle Gefahr (d.h. Bedrohung) zeitlich oder räumlich auftritt.

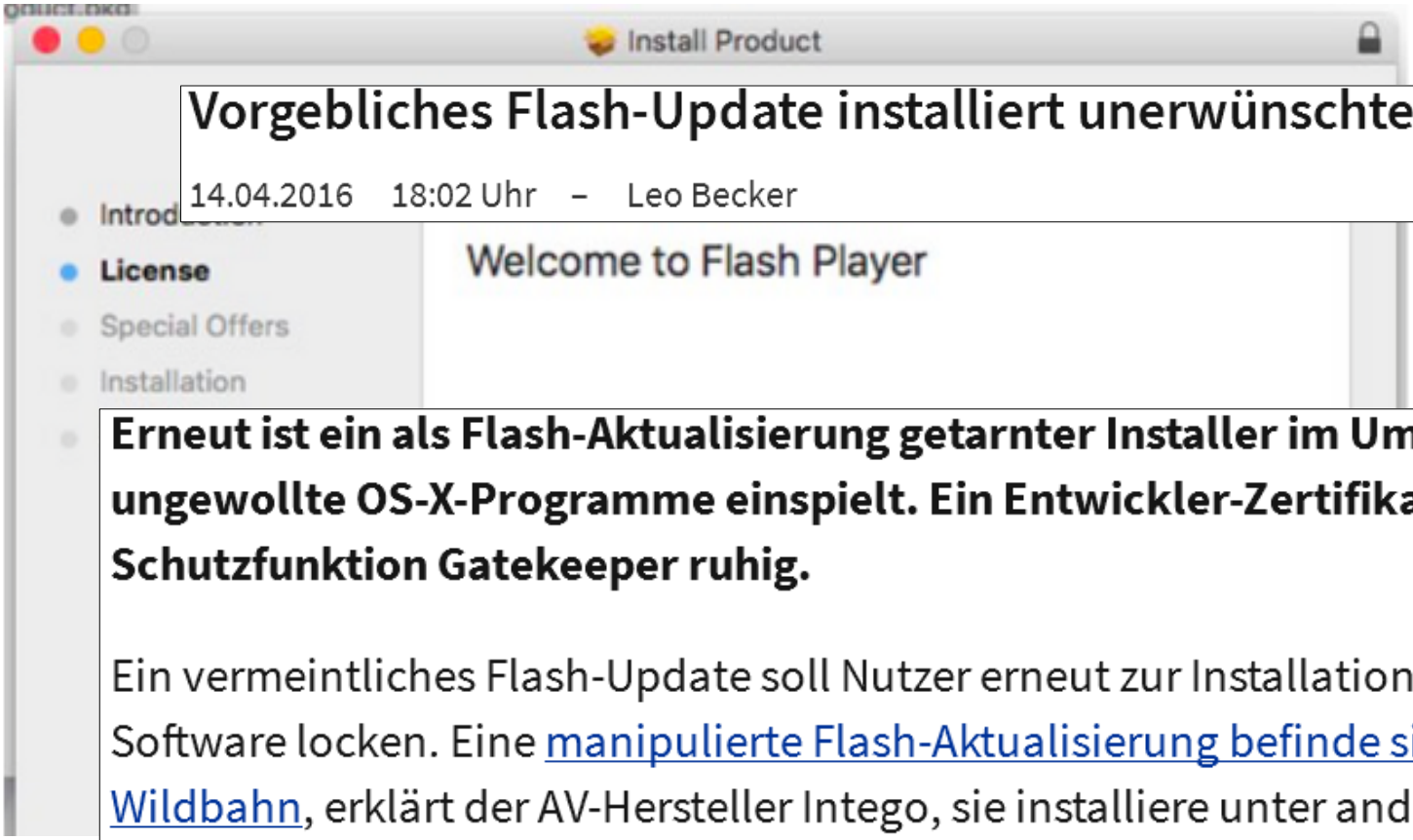
- Anders ausgedrückt: Trifft eine Bedrohung auf eine Schwachstelle (z.B. technische oder organisatorische Mängel), so entsteht eine Gefährdung
- Beispiel
  - Bei zu niedrigen Deichen im Gebiet der Oder sind steigende Wasserpegel eine Gefährdung

Gefährdungskategorien

- Höhere Gewalt (z.B. Hochwasser, Blitzeinschlag, globaler Stromausfall)
- Technische Fehler (z.B. defekte Datenträger, Ausfall einer Datenbank)
- Fahrlässigkeit (z.B. Nichtbeachtung von Sicherheitsmaßnahmen, ungeeigneter Umgang mit Passwörtern)
- Organisatorische Mängel (z.B. fehlende oder unzureichende Regelungen, nicht erkannte Sicherheitsvorfälle)
- Vorsätzliche Handlungen (z.B. Abhören und Manipulation von Leitungen, Schadprogramme, Diebstahl)

/www.heise.de/security/meldung/Vorgebliches-Flash-Update-installiert-unerwuenschte-Mac-Programme-3174793.html

teaser-of-the-day



Vorgebliches Flash-Update installiert unerwünschte Mac-Programme

14.04.2016 18:02 Uhr – Leo Becker

vorlesen

Erneut ist ein als Flash-Aktualisierung getarnter Installer im Umlauf, der ungewollte OS-X-Programme einspielt. Ein Entwickler-Zertifikat stellt die Schutzfunktion Gatekeeper ruhig.

Ein vermeintliches Flash-Update soll Nutzer erneut zur Installation ungewollter Software locken. Eine manipulierte Flash-Aktualisierung befinde sich derzeit in freier Wildbahn, erklärt der AV-Hersteller Intego, sie installiere unter anderem die Programme MegaBackup, ZipCloud und MacKeeper. Der Installer bietet offenbar auch Browser-Erweiterungen als "Special Offer" an, die bestimmte Einstellungen in Safari, Chrome und Firefox verändern.

Angriff

- Ein Angriff bezeichnet einen unautorisierten Zugriff bzw. Zugriffsversuch auf ein IT-System oder eine Information
- Technische Angriffe lassen sich in zwei Kategorien unterteilen
  - passive Angriffe: Zielen auf Informationsgewinnung (Schutzziel Vertraulichkeit)
    z.B. durch Abhören von Datenleitungen
  - aktive Angriffe: Zielen auf Informationsveränderung (Schutzziel Integrität und Verfügbarkeit)
    z.B. Vortäuschen einer falschen Identität, um Zugriff auf ein System zu erhalten

Schadensszenario

- Das Brechen der definierten Schutzziele (erfolgreicher Angriff auf ein IT-System durch Ausnutzen einer Schwachstelle) kann unterschiedliche Schäden verursachen.
- Folgende Schadensszenarien sind üblich
  - Verstoß gegen Gesetze, Vorschriften, Verträge
  - Beeinträchtigung des informationellen Selbstbestimmungsrechts
  - Beeinträchtigung der persönlichen Unversehrtheit
  - Beeinträchtigung der Aufgabenerfüllung
  - Negative Innen- oder Außenwirkung
  - Finanzielle Auswirkungen

Risiko (1/3)

- Ein Risiko ist das Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses und dessen Konsequenz, bezogen auf die Abweichung des gesteckten Ziels
  - Risiko = Eintritswahrscheinlichkeit * Schadenshöhe
- In Bezug auf IT-Sicherheit, das Produkt aus
  - Wahrscheinlichkeit dafür, dass ein Schutzziel gebrochen wird, und
  - Höhe des Schades, der sich daraus ergibt
- Die Bestimmung der Risiken hilft bei der Priorisierung umzusetzender Maßnahmen

Risiko (2/3)

Eintrittswahrscheinlichkeit und Schadenshöhe lassen sich nur schwer quantifizieren

- Für Eintrittswahrscheinlichkeit: Welche Mittel wird ein Angreifer einsetzen
  - hängt von seiner Motivation ab
  - nicht nur abhängig von finanziellen Gewinnaussichten, sondern teilweise auch vom persönlichen Ehrgeiz (z.B. Whistleblower)

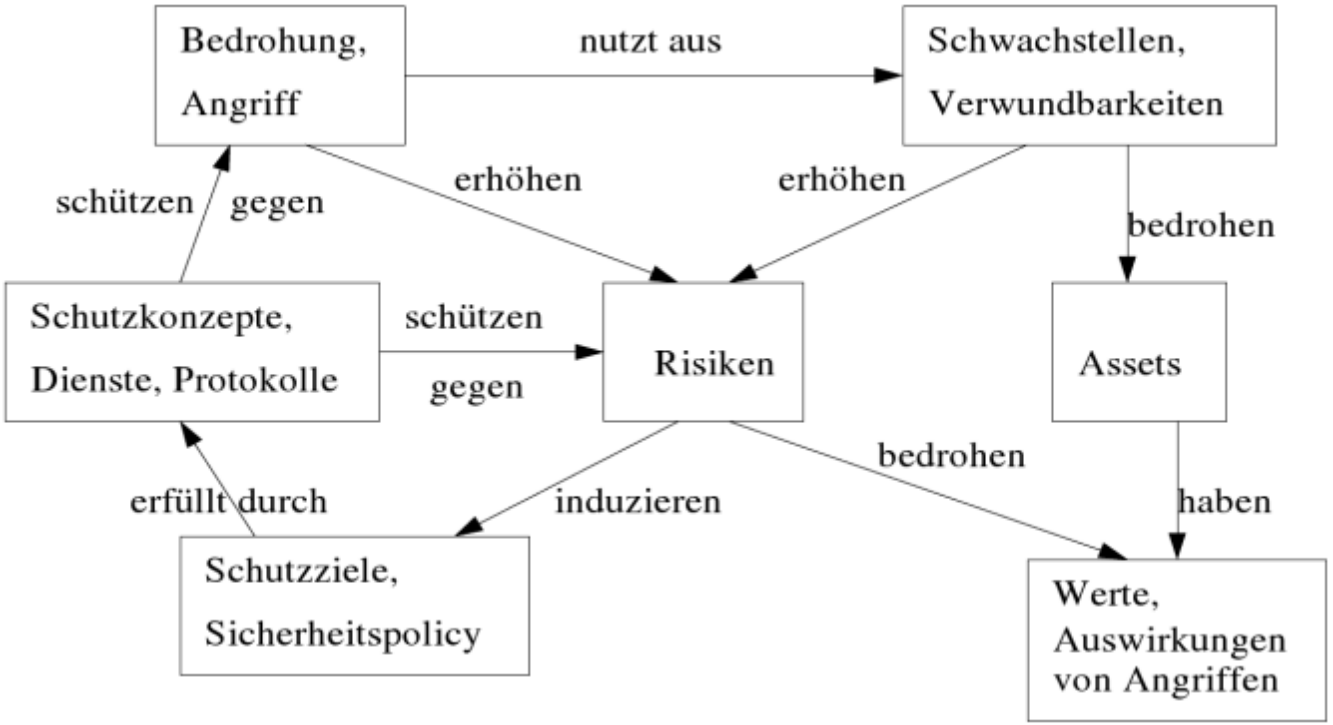
- Für Schadenshöhe: Abschätzung, welche Folgen ein Angriff hat
  - meist sind mehrere Schadensszenarien betroffen
  - hängt von der konkreten Institution ab (für kleine Unternehmen kann ein Verlust von 100.000 Euro existenzgefährdend sein, für Konzerne nicht)

Risiko (3/3)

Folgende Vereinfachung (nicht quantitative, sondern qualitative Bewertung):

- Klassifiziere Eintrittswahrscheinlichkeit in **mittel (1)**, **hoch (2)**, **sehr hoch (3)**
- Klassifiziere Schadenshöhe in **mittel (1)**, **hoch (2)**, **sehr hoch (3)**
- Werte für das Risiko: **1 (unbedeutend)** bis **9 (kritisch)**

Abhängigkeiten eingeführter Begriffe



- Quelle: C. Eckert: IT-Sicherheit, Konzepte-Verfahren-Protokolle, Oldenbourg-Verlag

Zusammenfassung

- IT-Sicherheit unterscheidet *safety* (Betriebssicherheit) von *security* (Schutz vor unerwünschtem Verhalten)
- Betrachtungen zur IT-Sicherheit erfordern Kenntnisse über
  - ⋊ zugrundeliegende System- und Kommunikationsmodelle
  - ⋊ Fähigkeiten des Angreifers
  - ⋊ Schutzziele
- Bestimmung von Risiken in der IT-Sicherheit lassen sich schwer quantifizieren
  - ➜ Trend: *assuming a state of compromise*

    (vgl. L. Levy, RSAConference ASIA PACIFC 2013)