INTERNATIONALE HOCHSCHULE

Datenschutz & IT-Sicherheit
SoSe 2024

DSBDSITS01

DATENSCHUTZ UND IT-SICHERHEIT

Virtuell in Bielefeld,
Leipzig, Hannover
uvm.

AGENDA

Begriffsbestimmungen und Hintergründe	**01**	04./05.04.
Grundlagen des Datenschutzes	**02**	12./19./26.04./02./03.05.
Grundlagen der IT-Sicherheit	**03**	17./31.05.
Standards und Normen der IT-Sicherheit	**04**	07.06.
Erstellung eines IT-Sicherheitskonzeptes auf Basis von IT-Grundschutz	**05**	14.06
Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte	**06**	20./21.06.
Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen	**07**	28.06./05.07.
Recap, Q&A, Besprechung der Übungsklausur	**08**	12.07.

03

GRUNDLAGEN DER IT-SICHERHEIT

THEMEN

- Paradigmen der IT-Sicherheit
- Modelle der IT-Sicherheit
- Rechtliche Vorgaben der IT-Sicherheit

“WER DIE FREIHEIT AUFGIBT, UM SICHERHEIT ZU GEWINNEN, WIRD AM ENDE BEIDES VERLIEREN.“

- BENJAMIN FRANKLIN

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, …

- … welche Paradigmen der IT-Sicherheit zugrunde liegen
- … welche grundlegenden Modelle der IT-Sicherheit es gibt
- … welche rechtlichen Vorgaben es für die IT-Sicherheit gibt

3.1

INTERNATIONALE HOCHSCHULE

PARADIGMEN DER IT-SICHERHEIT

EINFÜHRUNG

- **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** für einen IT-Verbund planen, einführen und kontrollieren ist ein komplexes Anliegen

- Wissenschaftlicher Konsens über gewisse **Annahmen und Vorstellungen**, die für dieses Anliegen Lösungen anbieten
  → spiegeln sich in sogenannten Paradigmen wider, z.B. „Muster“ oder „Vorbilder“

- Modell der IT-Sicherheit eines IT-Verbundes geht noch einen Schritt weiter:
  - beschreibt **Zustände** und ihre **Übergänge**
  - unterscheidet sichere von unsicheren Zuständen
  - erklärt, unter welchen Umständen sichere Zustände erreicht werden

- Aufgabe der „IT-Sicherheit“: Kunden davon zu überzeugen, dass ein IT-Verbund sicher ist

- Klassische rechtliche Vorgaben der IT-Sicherheit: eher Reaktion als Prävention
  - Umdenken in den letzten Jahren und Gesetzen

PARADIGMEN DER IT-SICHERHEIT

ACL – Access Control List (Zugriffsliste)

- Für jeden Nutzer und für jedes Objekt des IT-Verbundes wird einzeln vermerkt, welche Nutzungsrechte (Lesen, Schreiben, Einschalten, Konfigurieren, …) am Objekt dem Nutzer eingeräumt werden.
- Man unterscheidet DAC von MAC, in Abhängigkeit von der Verbindlichkeit der Pflege.

Discretionary Access Control (DAC)

- Man überlässt es dem Besitzer bzw. Erzeuger eines Objektes, die Nutzungsrechte festzulegen. Beispiele: UNIX-artige Betriebssysteme, soziale Netzwerke

Mandatory Access Control (MAC)

- Die ACL wird zentral gepflegt und automatisch erzwungen

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

PARADIGMEN DER IT-SICHERHEIT

ACL Beispiel

- Bei Dateien und Geräten gibt es beispielsweise die Nutzungsoptionen READ, WRITE und EXECUTE und die Freigabe einer dieser Nutzungsoptionen wird dann je Nutzer in einer ACL wie folgt explizit festgelegt

- In den Zeilen werden dabei die Nutzer und in den Spalten die Objekte aufgelistet: An den Schnittpunkten werden dann die Nutzungsrechte vermerkt.

	…	**Objekt-1**	**Objekt-2**	**…**
…	…	…	…	…
Nutzer-1	…	READ, WRITE	EXECUTE	…
…	…	…	…	…

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

PARADIGMEN DER IT-SICHERHEIT

Probleme

- Egal ob DAC oder MAC, die Pflege einer ACL wird schnell allein schon wegen der Größe und der Dynamik eines IT-Verbundes problematisch
  - Lösungsansatz: Nutzer und Objekte bestimmten **Gruppen** zuzuordnen und dann nur noch für diese Gruppen Nutzungsrechte festzulegen

- Beispiel: Mitglieder der Gruppe „Praxispersonal“ dürfen Dateien der Gruppe „Patientendaten“ einsehen (READ) und verändern (WRITE)

- Gruppen können dabei auch Teile von anderen Gruppen sein. Hier geht man meist von einer sogenannten „Rechtevererbung“ aus.
  → Gefahr widersprüchlicher Nutzungsrechte

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

PARADIGMEN DER IT-SICHERHEIT

Role Based Access Control (RBAC)

- Dieses Konzept vergibt Nutzungsrechte auf Grundlage des aktuellen Arbeitsprozesses. Nutzern werden Rollen zugeordnet (etwa: Administrator, Gast, etc.)

- Nutzer können dabei formal zwar mehrere Rollen besitzen, aber stets nur in einer Rolle handeln

- Rollen können hierarchisch gegliedert sein. An eine Rolle sind oft auch eine oder mehrere Gruppenzugehörigkeiten (mit den eingeräumten Nutzungsrechten) gebunden
  - Rechtevererbung aber keine Rollenvererbung

- Je nach der aktuellen Rolle des Nutzers erteilt oder sperrt das System dann das Nutzungsrecht für ein Objekt (oder eine Gruppe von Objekten) auf Basis einer entsprechenden ACL

- Beispiel: Microsoft Active Directory

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

PARADIGMEN DER IT-SICHERHEIT

Role Based Access Control (RBAC) - Beispiel

- In der Arztpraxis Dr. med. Heilemacher könnte man die Rollen Praxisinhaber (PI), Praxispersonal (PP) und Dienstleister (DL) definieren, wobei sinnvollerweise die Rolle PI die Rolle PP umfasst.

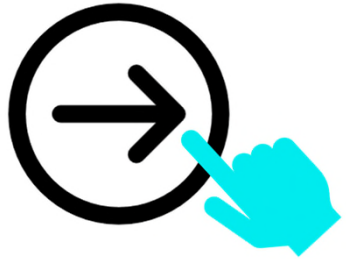
- Für Notfälle mag dem Praxisinhaber neben der Rolle PI auch die Rolle eines DL fest zugeordnet sein, damit er gegebenenfalls auch Wartungsaufgaben durchführen kann.

- Dies bedeutet aber nicht, dass er in seiner Rolle als PI Wartungsaufgaben durchführen kann.
  - Er muss dazu explizit die Rolle PI ablegen und die Rolle DL annehmen, was – typisch – ein Abmelden als PI und dann ein Anmelden als DL erfordert.
  - In der Rolle PI sind Wartungsaufgaben NICHT durchführbar, sehr wohl aber alle Aufgaben, die der Rolle PP zugeordnet sind.

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

PARADIGMEN DER IT-SICHERHEIT

Übung: Access Control List



30 Minuten - Gruppenarbeit

(Password: DaSchu_ITS_24)

Durchsuchen Sie Ihr Betriebssystem nach existierenden Rechten und Access Control Lists.

Hier finden Sie ein mögliches Vorgehen für Windows:
Abrufen von Informationen aus einer ACL - Win32 apps | Microsoft Learn

Haben Sie diese Art der Einstellungen schon verwendet? In welcher Form bzw. wozu? Welche Rolle spielt ACL bei Ihrem Praxispartner oder bei angebotenen Softwarelösungen Ihres Praxispartners?

Diskustieren Sie verschiedene für Sie relevante Aspekte in Ihrer Gruppe.

3.2

INTERNATIONALE HOCHSCHULE

MODELLE DER IT-SICHERHEIT

MODELLE DER IT-SICHERHEIT

- Für eine feingranulare Steuerung von Nutzungsrechten sind die bisher vorgestellten Ansätze manchmal nicht ausreichend
  - beispielsweise die Anforderung „Labordaten der letzten drei Kalenderjahre dürfen nur vom Praxisinhaber gelöscht werden“ nicht unmittelbar abbildbar

- Modelle der IT-Sicherheit können helfen
  - Zwei Modelle werden skizziert:
    - das **Bell-LaPadula-Modell** mit dem Sicherheitsziel der Vertraulichkeit von gemeinsam genutzten Objekten
    - das **Biba-Modell** mit dem Sicherheitsziel der Integrität von Objekten
  - Modelle, sind nicht automatisch „richtig“, sondern beschreiben die Grundkonzepte, die in bestimmten Situationen angewendet werden können, in anderen nicht
    - in ihrer Reinform passen sie nur sehr selten
    - In der Praxis: als Ausgangspunkt nehmen und dann punktuell öffnen
      →Risiko, dass dann die nachweisbaren Sicherheitseigenschaften nicht mehr vollumfänglich gelten

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

MODELLE DER IT-SICHERHEIT

Bell-LaPadula (Schutzziel: Vertraulichkeit)

- Ein Subjekt darf nur Objekte niedrigerer oder gleicher Sicherheitseinstufung lesen (no-read-up) und nur Objekte höherer oder gleicher Einstufung schreiben (no-write-down).

Biba (Schutzziel: Integrität)

- Ein Subjekt darf nur Objekte niedrigerer oder gleicher Sicherheitseinstufung schreiben (no-write-up) und nur Objekte höherer oder gleicher Einstufung lesen (no-read-down).

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

MODELLE DER IT-SICHERHEIT

Bell-LaPadula-Modell

- Festlegungen der Nutzungsrechte in einer ACL um eine generelle Zugriffsregel zu erweitern, die bei jedem Zugriff eines Nutzers auf ein Objekt ebenfalls durchgesetzt wird
  - Nutzer und Objekte in Sicherheitsstufen eingeteilt
  - die in einer Ordnung zueinanderstehen, das heißt, dass sie gleich sind oder die eine „höher“ als die andere ist
  - spiegeln für Objekte eine Einstufung hinsichtlich der Vertraulichkeitsanforderungen wider

- Beispiele:
  - von derartigen Sicherheitsstufen für Patientendaten sind etwa „öffentlich<individuell< privat<intim“, je nachdem welcher Sphäre diese Daten entstammen.
  - Beim Militär o.ä. findet man z. B. Sicherheitsstufen wie „öffentlich<vertraulich<geheim<streng geheim“.

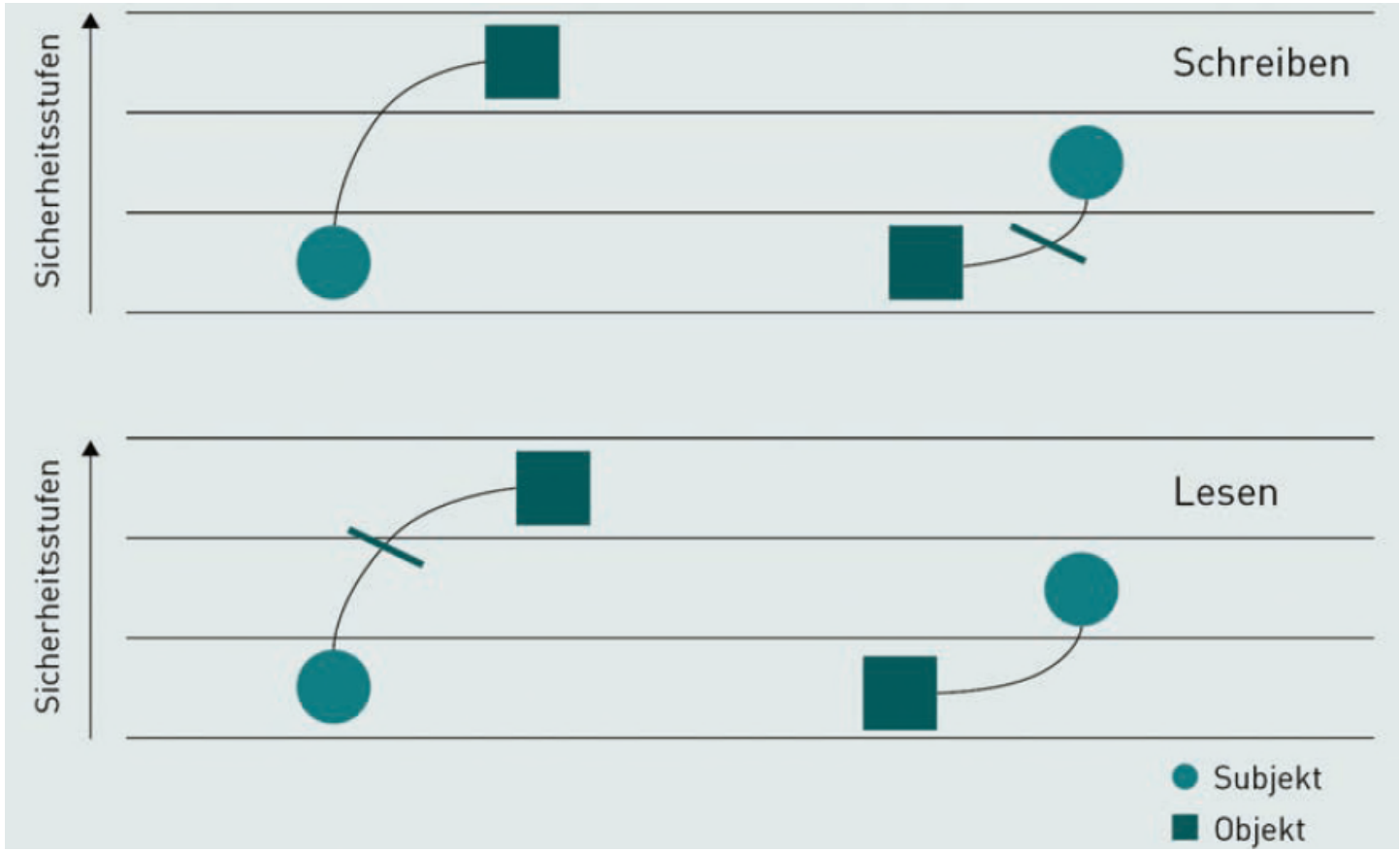
Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

MODELLE DER IT-SICHERHEIT

Bell-LaPadula-Modell

- Jeder Nutzer und jedes Objekt erhält dann eine Sicherheitseinstufung anhand der Sicherheitsstufen
- dem Nutzer wird also eine Clearance und dem Objekt eine Classification zugeordnet

- **Sicherheitseinstufungen**:
  Regel festgelegt, dass
  - Subjekt nur Objekte niedrigerer oder gleicher Sicherheitseinstufung lesen (no-read-up)
  - nur Objekte höherer oder gleicher Einstufung schreiben darf (no-write-down)



Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

MODELLE DER IT-SICHERHEIT

Bell-LaPadula-Modell - Beispiel

- Der angestellte Arzt in der Praxis Dr. med. Heilemacher darf zum Beispiel bis zur Sicherheitsstufe „privat“ Dokumente lesen, aber keine Dokumente der Sicherheitsstufe „intim“.
  - Damit hat er die Sicherheitsstufe „privat“.
  - Er hätte dann eine höhere Sicherheitsstufe als ein Drucker der Arztpraxis, der nur „öffentliche“ und „individuelle“ Dokumente drucken darf, aber keine „privaten“ oder „intimen“, da er die Sicherheitsstufe „individuell“ hat.

- Der oben genannte, angestellte Arzt dürfte zum Beispiel bei Anwendung von Bell-LaPadula alle Ausgaben des erwähnten Druckers lesen, aber nichts auf diesem Drucker drucken.
  - Damit wird verhindert, dass irgendwelche Objekte Nutzern niedrigerer Sicherheitseinstufungen zur Kenntnis kommen können.
  - Hierdurch wird die Vertraulichkeit in (vor allem) hierarchisch organisierten Arbeitsumgebungen, wie zum Beispiel beim Militär, geschützt.

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

MODELLE DER IT-SICHERHEIT

Bell-LaPadula-Modell in der Praxis

- Bell-LaPadula-Modell wird meist mithilfe von MAC durchgesetzt
  - verhindert es dann aufgrund der MAC ausdrücklich und wirkungsvoll den Informationsfluss „von oben nach unten“

- gelegentlich Objekte von einem höher eingestuften Nutzer gelesen, verändert und zurückgeschrieben werden
  - zurückgeschriebene Objekt muss dann automatisch auf die Schutzstufe dieses Nutzers hochgestuft werden
  - Objekte können also durch den laufenden Betrieb automatisch hoch-, aber nicht heruntergestuft werden
  - Wandern mit der Zeit mehr und mehr Objekte nach oben
    → werden dem Zugriff der darunter angeordneten Nutzer entzogen
    → bis schließlich der IT-Verbund oft nicht mehr funktionsfähig ist
  - Dann müssen von Hand alle die Objekte wieder herabgestuft werden, die „unten“ gebraucht werden

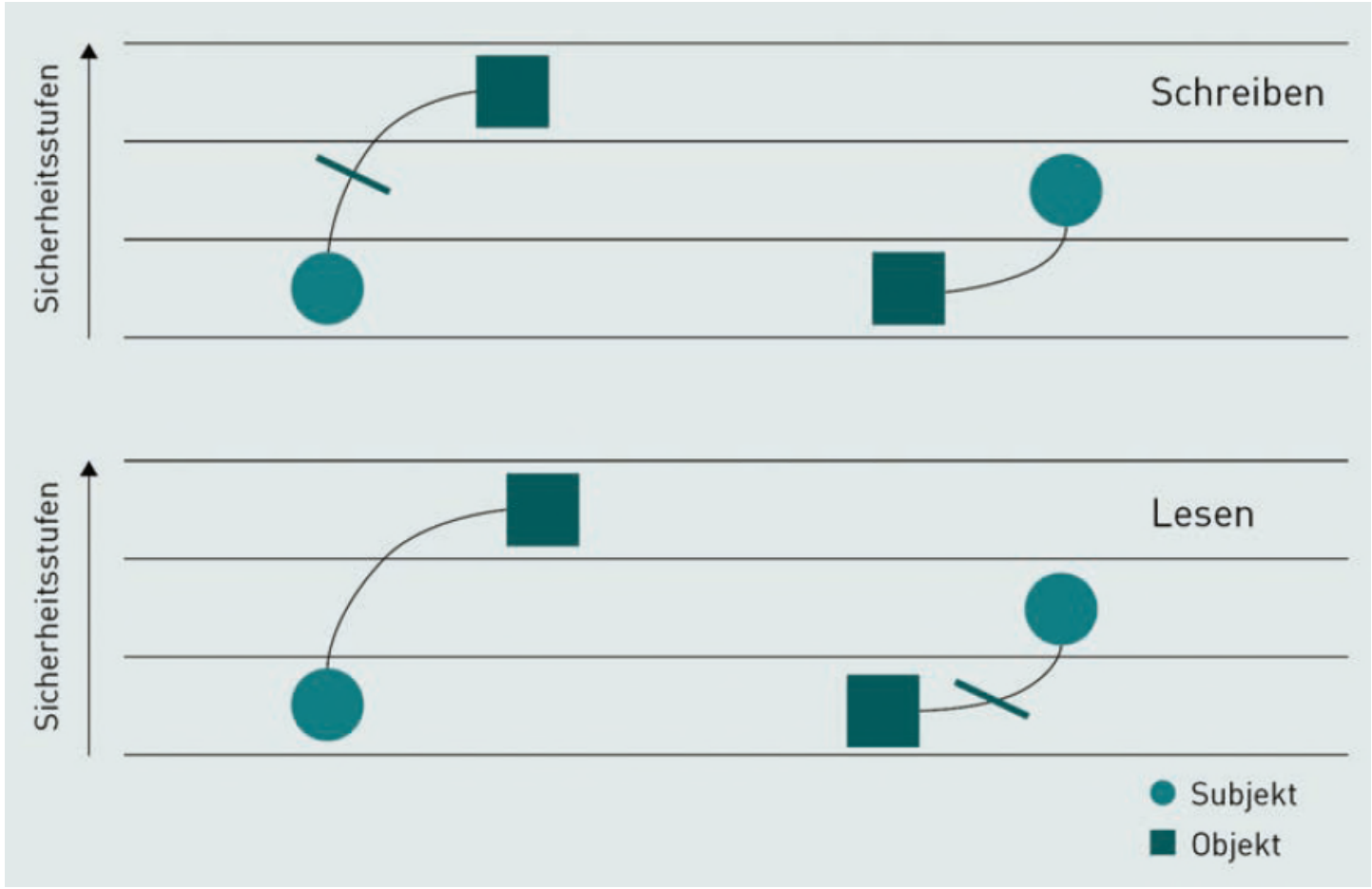
Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

MODELLE DER IT-SICHERHEIT

Biba-Modell

- verwendet Sicherheitseinstufungen wie bei dem Bell-LaPadula-Modell, der Fokus liegt hier aber auf der Integrität der Objekte
- sozusagen eine Umkehrung des Bell-LaPadula-Modells dar:
  Hier werden Objekte nicht vor der Kenntnisnahme, sondern vor der Manipulation durch Unbefugte geschützt

- höhere Sicherheitseinstufung bedeutet auch eine höhere Integrität:
  - ein Subjekt nur Objekte niedrigerer oder gleicher Sicherheitseinstufung schreiben (no-write-up)
  - nur Objekte höherer oder gleicher Einstufung lesen darf (no-read-down)



Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

MODELLE DER IT-SICHERHEIT

Biba-Modell - Beispiel

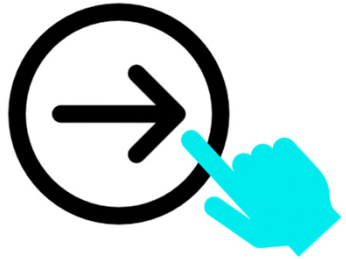
- Hat eine Praxisangestellte etwa die Einstufung „individuell“, dann kann sie bei Anwendung von Biba ein „privates“ Gutachten des angestellten Arztes lesen, jede von ihr veränderte oder auch nur unter einem anderen Namen gespeicherte Version ist aber maximal nur noch „individuell“, hat also eine niedrigere Einschätzung bezüglich der Integrität.

- Das Biba-Modell wird beispielsweise seit Windows Vista bei allen Microsoft-Windows-Desktopbetriebssystemen unter dem Namen MIC (Mandatory Integrity Control) mit den Sicherheitsstufen: Low, Medium, High und System verwendet, da es ja bei Systemdateien vor allem auf Integrität und weniger auf Vertraulichkeit ankommt.

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

MODELLE DER IT-SICHERHEIT

10 Minuten - Gruppenarbeit



(Password: DaSchu_ITS_24)

- Welche Anwendungsfälle aus der Praxis fallen Ihnen zu den beiden Modellen der IT-Sicherheit (Bell-LaPadula, Biba) ein?
  - Gerne dürfen Sie auf die Suche gehen und diese recherchieren

TRANSFERAUFGABE 1 –LÖSUNG

Bell-LaPadula:

Kontrollierter Zugriff auf staatliche Verschlusssachen.

Biba-Modell:

Wird in sicherheitsrelevanten Systemen wie z.B. Firewalls oder auch bei Betriebssystemen eingesetzt, um Angriffe abzuwehren. Ein mögliches Einsatzszenario sind militärische Systeme, bei denen es essentiell ist, dass Befehle in der Kommandokette nicht modifiziert und somit Manipulationen verhindert werden können.

3.3

INTERNATIONALE HOCHSCHULE

RECHTLICHE VORGABEN DER IT-SICHERHEIT

RECHTLICHE VORGABEN DER IT-SICHERHEIT

- Ziel: knapper Überblick über einige derzeit bestehende Schutzpflichten zu geben, die gesetzlich für Betreiber von IT-Verbünden gelten

- Motiv/Konsequenzen:
  - Soweit diese zivilrechtlich begründet sind, führen sie bei schuldhafter Verletzung zur **Haftung des Verantwortlichen**
  - Anforderungen aus dem Strafrecht können bei schuldhafter Verletzung **Geldbußen oder Freiheitsstrafen** nach sich ziehen

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

RECHTLICHE VORGABEN DER IT-SICHERHEIT

Schutzziele der IT-Sicherheit und zugehörige Vorschriften des StGB	
Vertraulichkeit	§ 202a StGB Ausspähen von Daten § 202c StGB Vorbereiten des Ausspähens und Abfangens von Daten § 203 StGB Verletzung von Privatgeheimnissen
Integrität	§ 263a StGB Computerbetrug § 265a StGB Erschleichen von Leistungen § 268 StGB Fälschung technischer Aufzeichnungen § 269 StGB Fälschung beweiserheblicher Daten § 270 StGB Täuschung im Rechtsverkehr bei Datenverarbeitung § 303a StGB Datenveränderung
Verfügbarkeit	§ 303b StGB Computersabotage

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

STRAFGESETZBUCH

Ausspähen von Daten

- § 202a StGB: „Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft“

- Zugangssicherung handelt es sich schon, wenn diese den Zugang zu den Daten nicht nur unerheblich erschwert
- Das Gesetz verlangt bewusst nicht, dass Zugangssicherungen erst mit einem bestimmten Aufwand oder bestimmten IT-Kenntnissen überwunden werden können
- Schon das Verschließen eines Raumes reicht aus
- Nur wenn jedermann ohne Weiteres eine Zugangssicherung überwinden kann, genügt sie nicht mehr

- § 202c StGB im Kontext des Umgangs mit Hackertools und Schadsoftware:
  - nur zu Test- oder Prüfzwecken beschafft oder erstellt werden, ist besondere Sorgfalt geboten
  - Weitergabe sollte nur an bekannte und zuverlässige Dritte erfolgen
  - Keinesfalls sollte solche Software einem unbestimmten Empfängerkreis

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

„14 GEBOTE“ DES DATENSCHUTZES

Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte **(Zugangskontrolle)**,
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern **(Datenträgerkontrolle)**,
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten **(Speicherkontrolle)**,
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte **(Benutzerkontrolle)**,
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben **(Zugriffskontrolle)**,
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können **(Übertragungskontrolle)**,
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind **(Eingabekontrolle)**,

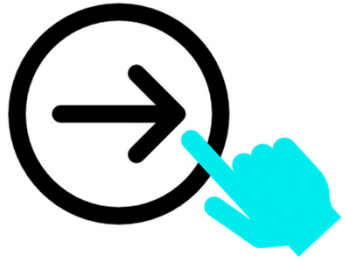
„14 GEBOTE“ DES DATENSCHUTZES

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird **(Transportkontrolle)**,
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können **(Wiederherstellbarkeit)**,
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden **(Zuverlässigkeit)**,
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können **(Datenintegrität)**,
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggeber verarbeitet werden können **(Auftragskontrolle)**,
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind **(Verfügbarkeitskontrolle)**,
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können **(Trennbarkeit)**.

Ein Zweck nach Satz 1 Nummer 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

RECHTLICHE VORGABEN

Übung: BDSG „14 Gebote“



30 Minuten - Gruppenarbeit

(Password: DaSchu_ITS_24)

Finden Sie je vorgenannten „Gebot“ ein Beispiel für eine umsetzende technische-organisatorische Maßnahme.

KRITISCHE INFRASTRUKTUREN (KRITIS)

- IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist ein im Juli 2015 in Kraft getretenes Gesetz
- IT-Sicherheitsgesetz (IT-Sig 2.0) ist im Mai 2021 in Kraft getreten

- Betreiber besonders gefährdeter Infrastrukturen (sogenannte **Kritische Infrastrukturen**) wie Energie, Wasser, Gesundheit oder Telekommunikation verpflichtet, ihre IT-Verbünde besser zu schützen
  - obligatorischen Meldung von IT-Sicherheitsvorfällen
  - Mindeststandards für die IT-Sicherheit bei den Betreibern solcher IT-Verbünde festgelegt
  - jeweiligen Branchen selbst solche Standards entwickeln, die dann vom BSI genehmigt werden müssen
  - Meldepflichten/Meldung von Vorfällen
  - Alle zwei Jahre nachweisen, dass Sie die Anforderungen erfüllen → „Stand der Technik“

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“

Bundesinnenministerium

KRITISCHE INFRASTRUKTUREN (KRITIS)

- Die Sektoren „Medien und Kultur“ sowie „Staat und Verwaltung“ sind von der gesetzlichen Regelung durch das IT-Sicherheitsgesetz nicht betroffen.

- Unterschiedliche Penetration mit Informations- und Kommunikationstechnologie
  - Bsp.: IT-Kompetenz Gesundheitswesen vs. Straßenbau

Quelle Abbildung: Bundesamt für Bevölkerungsschutz, 2022.

KRITISCHE INFRASTRUKTUREN (KRITIS)

- Das Gesetz beantwortet jedoch noch nicht die Frage, welche Unternehmen konkret als Kritische Infrastrukturen im Sinne des Gesetzes gelten

- Definiert diese lediglich abstrakt

- Für die Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr wurden mit der KRITIS-Verordnung Anlagenkategorien und Schwellenwerte definiert, welche Anlagen als kritische Infrastrukturen gelten
  - Schwellenwerte vielfach so definiert, dass sie etwa 500.000 Nutzern oder Kunden entsprechen

Quelle: DLBISIC01 Einführung in Datenschutz und IT-Sicherheit, Fernstudiumsskript Version: 002-2023-0206, IU Internationale Hochschule GmbH

DEFINITION: KRITIS

Beispiel Anlagenkategorien und Schwellwerte Sektor Energie

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Stromversorgung**		
1.1	Stromerzeugung		
1.1.1	Erzeugungsanlage	Installierte Nettonennleistung (elektrisch oder direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil) in MW oder	104
		installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses der Bundesnetzagentur vom 20. Mai 2020, Aktenzeichen BK6-18-249 kontrahiert ist, oder	0
		installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV präqualifiziert ist	36
1.1.2	Anlage oder System zur Steuerung/Bündelung elektrischer Leistung	Installierte Nettonennleistung (elektrisch) in MW oder	104
		installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses BK6-18-249 kontrahiert ist, oder	0
		installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV präqualifiziert ist	36
1.2	Stromübertragung		
1.2.1	Übertragungsnetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3 700

Quelle Abbildung: Bundesministerium der Justiz, 2022.

DEFINITION: KRITIS

Beispiel Anlagenkategorien und Schwellwerte Sektor Energie

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Trinkwasserversorgung**		
1.1	Gewinnung		
1.1.1	Gewinnungsanlage	Gewonnene Wassermenge in Millionen m^3/Jahr	22
1.2	Aufbereitung		
1.2.1	Aufbereitungsanlage (Wasserwerk)	Aufbereitete Trinkwassermenge in Millionen m^3/Jahr	22
1.3	Verteilung		
1.3.1	Wasserverteilungssystem	Verteilte Wassermenge in Millionen m^3/Jahr	22
1.4	Steuerung und Überwachung		
1.4.1	Leitzentrale	Von den gesteuerten/ überwachten Anlagen gewonnene, transportierte oder aufbereitete Wassermenge in Millionen m^3/Jahr	22
2	**Abwasserbeseitigung**		
2.1	Siedlungsentwässerung		
2.1.1	Kanalisation	Angeschlossene Einwohner	500 000
2.2	Abwasserbehandlung und Gewässereinleitung		
2.2.1	Kläranlage	Ausbaugröße in Einwohnerwerten	500 000
2.3	Steuerung und Überwachung		
2.3.1	Leitzentrale	Ausbaugrößen der Anlagen in Einwohnerwerten oder angeschlossene Einwohner der gesteuerten oder überwachten Anlagen	500 000

Quelle Abbildung: Bundesministerium der Justiz, 2022.

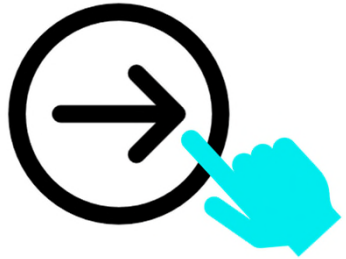
MELDEPFLICHT

Beispiele

- Benennung eines IT-Sicherheitsbeauftragten
- Selbstentwickeltes Werkzeug zur Dokumentation von Sicherheitsvorfällen mit Meldefunktion gemäß IT-Sicherheitsgesetz
- Ticket-System zum Melden/Analysieren von Vorfällen/Schwachstellen
- Abwicklung über den Helpdesk
- Übergreifender Incident-/Krisenmanagement-Prozess
- …

RECHTLICHE VORGABEN

Übung: Kritische Infrastrukturen



90 Minuten - Gruppenarbeit

(Password: DaSchu_ITS_24)

- Bilden Sie zwei Gruppen
- Wählen Sie je Gruppe eine Fallstudie aus dem open-access-Buch „*Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen*“ von U. Lechner et. Al. (abrufbar unter: Case Kritis - Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen (oapen.org))
- Hinterlegen Sie Ihre Wahl in Miro - Fallstudien dürfen nicht von zwei Gruppen bearbeitet werden.
- Stimmen Sie innerhalb der Gruppe ab, wie Sie sich die Fallstudie erschließen und eine Präsentation von fünf Minuten für das Plenum erstellen.
- Erstellen Sie eine Präsentation, die die wichtigsten Aspekte der gewählten Fallstudie darstellen.
- Stellen Sie die Fallstudie dem Plenum vor

Gibt es zu den bisherigen Inhalten Fragen?