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. **+14.06.**
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	20.06 / 21.06.
Bewährte Schutz- und Sicherheitskonzepte für IT-Geräte	06	28.06.
Ausgewählte Schutz- und Sicherheitskonzepte für IT-Infrastrukturen	07	05.07.
Recap, Q&A, Besprechung der Übungsklausur	08	12.07.

07

AUSGEWÄHLTE SCHUTZ- UND SICHERHEITS-KONZEPTE FÜR IT-INFRASTRUKTUREN

THEMEN

- Objektschutz
- Schutz vor unerlaubter Datenübertragung
- Schutz vor unerwünschtem Datenverkehr
- Schutz durch Notfallplanung

“Der Status der IT-Sicherheit lässt sich gut mit dem Besuch beim Zahnarzt vergleichen, denn auch hier gilt: Vorbeugen ist besser als heilen.“

- Damian Izdebski

(CEO der techbold technology group)

LERNZIELE

Nach der Bearbeitung dieser Lektion werden Sie wissen, …

- … wie – auf konzeptioneller Ebene – wesentliche Teile von IT-Infrastrukturen sicher beschafft, konfiguriert und betrieben werden können.
- … wie unerlaubte Datenübertragung verhindert werden kann.
- … was Notfallpläne für Datenschutz und IT-Sicherheit leisten können.

Prism

EINFÜHRUNG

- **Prism** ist ein System, mit dessen **Hilfe staatliche Einrichtungen die Internetaktivitäten von Menschen überwachen** können
  - die Daten all jener, die Produkte und Dienstleitungen von u. a. Google, YouTube, Facebook, Microsoft, Skype, AOL, Yahoo und Apple nutzen
  - **Aufgedeckt** hat Prism der Whistleblower Edward Snowden **im Jahre 2013**

- staatliche Einrichtung schickt einfach einen **Gerichtsbeschluss mit der Datenanforderung**, in dem der Firma zugleich unter Strafandrohung verboten wird, diese Datenübermittlung publik zu machen

BEISPIEL FÜR SICHERHEITSPROBLEME

- Unsichere Besucherausweisregelung und **fehlende Beaufsichtigung von Handwerkern/Reinigungskräften**
- **Fehlerhafte Konfiguration einer Firewall** Freitagnachmittag ohne korrekte Freigabe
- **Nicht funktionierende Wirkungskette zwischen USV und Notstrom** aufgrund nie getesteter/berücksichtigter Überlast

7.1

INTERNATIONALE HOCHSCHULE

OBJEKTSCHUTZ

OBJEKTSCHUTZ

- Objektschutz ist der **Schutz von Gebäuden, Räumen und Inventar vor Ereignissen**, die einen Verlust oder Schaden verursachen können
  - Schutz vor Feuer, Naturkatastrophen, Einbrüchen, Diebstahl, Vandalismus und Terrorismus

- **Schützenswerte Räume** einer IT-Infrastruktur sind z. B. der Serverraum, das Datenträgerarchiv und die Klimazentrale
  - Diese Räume sollten **niemals Hinweise auf ihre Nutzung** tragen.

  →Türschilder wie „SERVERRAUM“ geben einem potenziellen Angreifer wertvolle Hinweise, um seine Aktivitäten gezielter und damit Erfolg versprechender durchzuführen.

- **Zutritt zu schützenswerten Räumen ist verbindlich zu regeln und lückenlos zu kontrollieren**
  - nach Tageszeiten, Orten und Rollen zu differenzieren
  - Systeme zur Zutrittskontrolle reichen dabei von einem einfachen Schloss bis zu aufwendigen Zutrittssystemen etwa mit Fingerabdruckscannern
  - Grundsatz: **einfache und praktikable Lösungen** oft ebenso effizient sind wie aufwendige Technik
  - Zutrittskontrolle müssen **gegen Manipulationen geschützt** werden

OBJEKTSCHUTZ

Beispiel

- In einem Serverraum sollten sich auf keinen Fall Geräte befinden, die den Zutritt für einen großen Benutzerkreis erforderlich machen, wie z. B. Drucker oder Fotokopierer

- Unnötige Brandlasten wie Druckerpapier oder Kartonagen sollten ebenfalls nicht in einem Serverraum gelagert werden.

OBJEKTSCHUTZ

- Perimeterschutz
- Zutrittskontrolle
- Stromversorgung
- Klimatisierung
- Brandschutz
- …

OBJEKTSCHUTZ

Sicherheits-Zonen	Funktion	Kennzeichnung (Beispiel)
1	Grundstück	weiß
2	Halböffentlicher Bereich, angrenzende Büroflächen	grün
3	Operating-Bereiche, Nebenräume der IT	gelb
4	Technische Anlagen zum Betrieb der IT	blau
5	IT- und Netzwerkinfrastruktur	rot

– Quelle Abbildung: BITKOM, 2017

7.2

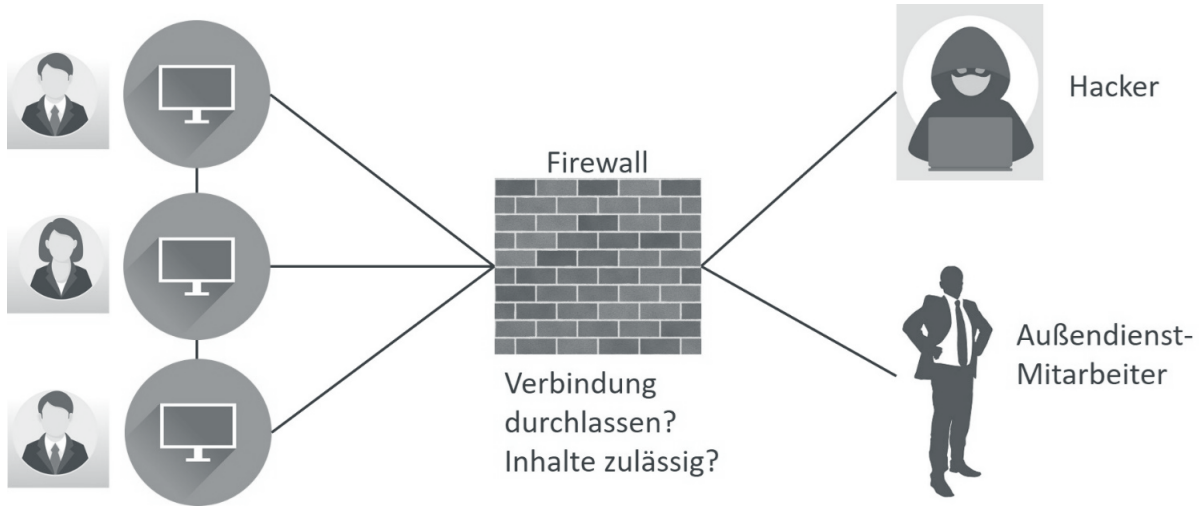
INTERNATIONALE HOCHSCHULE

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

- In TCP/IP-Netzwerken ist eine **Firewall** (i.e.S.) wie ein Router **ein eigenständiges Gerät**, das mehrere (einheitliche) **Netzwerke miteinander verbindet**.

- Zusätzlich zu den Funktionalitäten eines Routers bietet aber eine Firewall auch Schutz vor unerlaubter Datenübertragung, indem sie **jedes ein- und ausgehende Datagramm analysiert** und – entsprechend vordefinierter Regeln – die **Weiterleitung des Datagramms vornimmt oder unterbindet**.



„Ein **Sicherheitsgateway** (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten.
Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer Sicherheitsrichtlinie als ordnungsgemäß definierte Kommunikation“

Quelle: https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/S/Sicherheitsgateway.html

„Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden.“

Quelle: https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/S/Sicherheitsgateway.html

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

INTERNATIONALE HOCHSCHULE

- Eine **DMZ (Demilitarisierte Zone)** ist ein Zwischennetz, das an Netzübergängen gebildet wird und sowohl von innen als auch von außen erreichbar ist.
  - weniger stark gesichert als das interne Netz,
  - besser vom äußeren Netz aus erreichbar.

- Sie **dient der Schaffung eines zusätzlichen Sicherheitsbereichs** für Dienste (z. B. E-Mail, Web) oder Proxys
  - die von externen Netzen aus nutzbar sein sollen
  - aus Sicherheitsgründen nicht im internen Netz platziert werden dürfen.

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

INTERNATIONALE HOCHSCHULE

- Eine Firewall besteht aus einer Softwarekomponente, die Netzwerkpakete lesen und auswerten kann.

- Die Software kann
  - auf einer zu schützenden Hardwarekomponente selbst oder
  - auf einer separaten, nur für die Firewall vorgesehenen Hardware installiert sein.

- Innerhalb der Software sind Regeln definiert, welche Datenpakete durchgelassen werden und welche zu blockieren sind.

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

Was kann eine Firewall?

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

Was kann eine Firewall?

- Prüfung des Datenverkehrs auf Basis von Regeln und Richtlinien
- Protokollierung und Alarmierung
- Abwehr von Einbruchsversuchen
- Abwehr von Denial of Service Angriffen (DoS)

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

Was kann eine Firewall NICHT?

- Vor bösartigen Insidern schützen,
- Vor Verbindungen schützen, die nicht über sie geführt werden,
- Endgeräte-Sicherheit ersetzen,
- Sichere Kommunikationsverfahren ersetzen (Verschlüsselung etc.),
- Sich selbst richtig konfigurieren ….

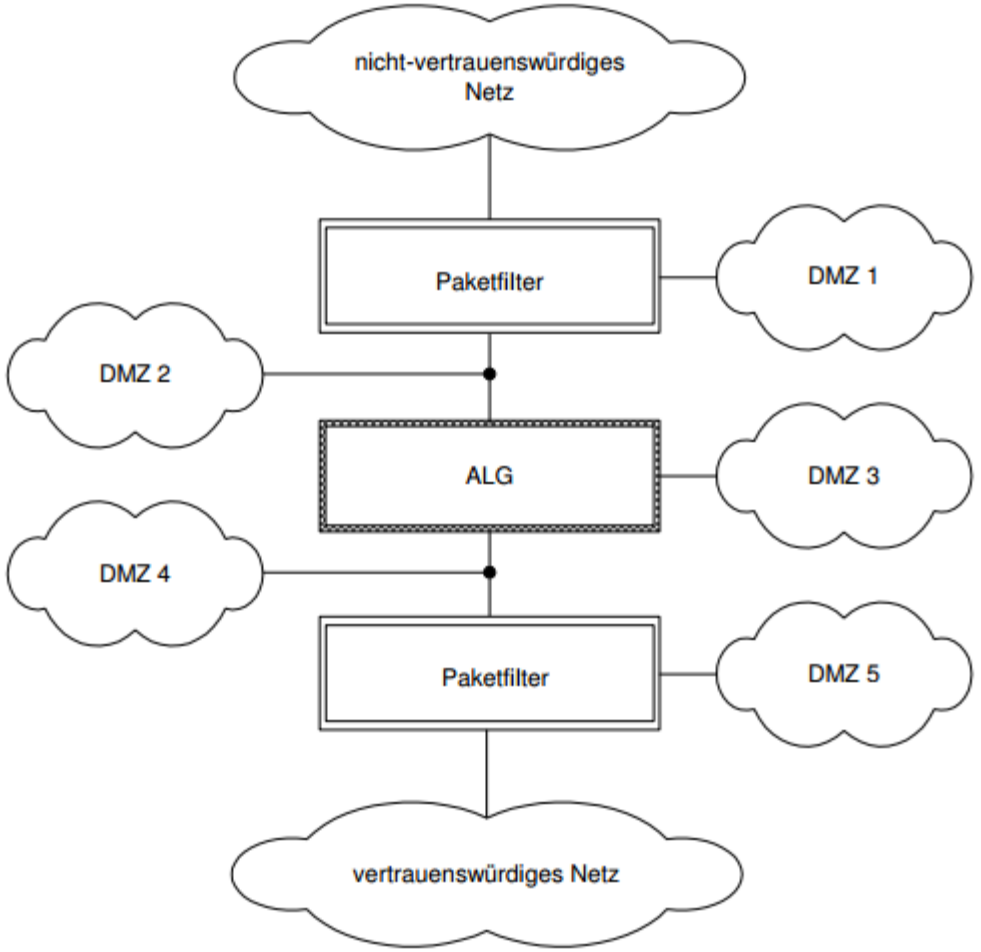
SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

- Ist die Software auf einer separaten, nur für die Firewall vorgesehenen Hardware installiert, wird die Firewall auch als **externe oder als Hardware-Firewall** bezeichnet.

- Häufig sind **Firewalls an Netzwerkgrenzen** zwischen einem internen und einem externen Netzwerk platziert. An dieser zentralen Stelle kontrollieren Sie den ein- und ausgehenden Datenverkehr.

In der Regel kontrolliert eine Firewall den Datenverkehr an besonders kritischen Stellen in Netzwerken zum Einsatz. Als somit zentralem Bestandteil einer sicheren IT-Infrastruktur muss der Beschaffung, der Konfiguration und dem Betrieb einer Firewall besondere Aufmerksamkeit zukommen.

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG



SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

- Um zudem unerlaubte Datenübertragungen auch über verschlüsselte Tunnel zu erkennen, ist die Fähigkeit des **Aufbrechens von TLS/SSL-Verbindungen durch eine Firewall** mit anschließender Regelanwendung heutzutage meist unverzichtbar.

- Im Betrieb muss eine Firewall die Möglichkeit bieten, die **Vertraulichkeit der durchgeleiteten Daten sicherzustellen**.

- Dazu muss sie Verschlüsselungen mit modernen Algorithmen und sicheren Parametern ermöglichen. Sie muss zudem die Möglichkeit bieten, dass Sende- und Empfangsaktivitäten nur nach einer „starken“ Authentisierung des Anwenders gestattet werden.

- Der Zugang zur **Konfiguration der Firewall** muss durch verschiedene Maßnahmen **besonders geschützt** werden.

SCHUTZ VOR UNERLAUBTER DATENÜBERTRAGUNG

INTERNATIONALE HOCHSCHULE

Bundesamt für Sicherheit in der Informationstechnik

NET.3: Netzkomponenten

NET.3.2: Firewall

1 Beschreibung

1.1 Einleitung

Eine Firewall ist ein System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basierte Datennetze sicher zu koppeln. Dazu wird mithilfe einer Firewall-Struktur der technisch mögliche Informationsfluss auf die in einer Sicherheitsrichtlinie als vorher sicher definierte Kommunikation eingeschränkt. Sicher bedeutet hierbei, dass ausschließlich die erwünschten Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden.

– Quelle Abbildung: BSI, 2022

7.3

INTERNATIONALE HOCHSCHULE

SCHUTZ VOR UNERWÜNSCHTEM DATENVERKEHR

SCHUTZ VOR UNERWÜNSCHTEM DATENVERKEHR

- **DoS (Denial of Service)-Angriffe** zielen darauf ab, Netzwerke und damit auch die in den Netzwerken angebotenen Dienste lahmzulegen.
  - Dies wird typisch dadurch erreicht, dass ein im anzugreifenden Netzwerk angebotener Dienst so stark mit Anfragen „bombardiert“ wird, dass er regulären Anfragen nicht mehr nachkommen kann.
  - oft Datenraten von über 300 Gigabit pro Sekunde beobachtet

- Bei **Distributed DoS-Angriffen (DDoS)** wird ein DoS-Angriff von mehreren Teilnehmern gleichzeitig ausgeführt.
  - DDoS-Angriffe können auch von einem **Bot-Netz** ausgeführt werden.
  - Meistens wissen die Besitzer gar nicht, dass ihre Geräte Teil eines Bot-Netzes sind.

- DoS- und DDoS-Angriffe sind nach deutschem Recht strafbar (§ 303b StGB Computersabotage)

7.4

INTERNATIONALE HOCHSCHULE

SCHUTZ DURCH NOTFALLPLANUNG

SCHUTZ DURCH NOTFALLPLANUNG

INTERNATIONALE HOCHSCHULE

- Zu der **Notfallplanung** eines IT- bzw. Informationsverbundes gehört **jegliche Vorsorge zur Aufrechterhaltung oder Wiederherstellung** von IT-Anwendungen im Falle unvorhergesehener Ereignisse oder Störungen.

- Eine Notfallplanung erfordert ein **systematisches Vorgehen**.
- Durchgeführt werden sollte zunächst eine **Business Impact Analysis** (BIA):
  - zu verstehen, welche IT-Anwendungen wichtig für die Aufrechterhaltung des Geschäftsbetriebs und damit für die Institution sind und welche Folgen ein Ausfall dieser IT-Anwendungen haben kann
  - Es existieren viele Methoden und Wege, eine BIA durchzuführen
  - Wie die erforderlichen Ergebnisse ermittelt werden, kann jede Institution für sich entscheiden
  - In **BSI-Standard 100–4** (vgl. Bundesamt für Sicherheit in der Informationstechnik 2008) wird beispielsweise eine Methode vorgestellt, die an die Schutzbedarfsfeststellung nach BSI-Standard 200–2 (vgl. Bundesamt für Sicherheit in der Informationstechnik (2017b) angelehnt ist

SCHUTZ DURCH NOTFALLPLANUNG

Business Impact Analysis

- Welche **Geschäftsprozesse sind kritisch** für die Aufrechterhaltung des Geschäftsbetriebs und damit für die Institution?
- Welche **Folgen hat ein Ausfall** dieser Geschäftsprozesse?

- Es ist zu analysieren und zu bewerten, wie sich ein Ausfall von Geschäftsprozessen auf die Institution auswirken und wie sich **Schäden während dieser Zeit entwickeln** können
- Für die Geschäftsprozesse sind die Wiederanlaufparameter zu identifizieren bzw. festzulegen. Dazu zählen:
  - die maximal tolerierbare Ausfallzeit,
  - die Wiederanlaufzeit,
  - das Wiederanlaufniveau und
  - der maximal zulässige Datenverlust.

- Mit den Ergebnissen der BIA erfolgt anschließend eine Risikoanalyse, die eine Maßnahmenauswahl und eine **Priorisierung dieser Maßnahmen** zum Ziel hat. Diese münden in eine **Notfallplanung**, die es umzusetzen gilt.

SCHUTZ DURCH NOTFALLPLANUNG

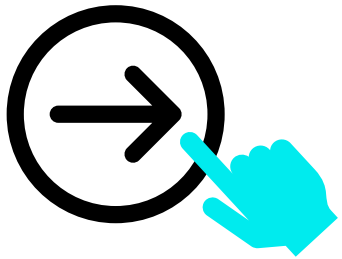
INTERNATIONALE HOCHSCHULE

- Bei der Notfallplanung sind selbstverständlich der **Datenschutz und die IT-Sicherheit zu berücksichtigen.**

- Es ist sicherzustellen, dass im Falle eines Ausfalls, bei der Inbetriebnahme und dem Betrieb von Ausweichlösungen und **bei der Wiederaufnahme** des Normalbetriebs sowohl **Datenschutz als auch IT-Sicherheit** gewährleistet sind.
  - die Gewährleistung der Vertraulichkeit von Daten (z. B. Zugriffsrechte, Verschlüsselung)
  - Einhaltung der Minimalanforderungen an die Datensicherung
  - Einhaltung gesetzlicher Vorgaben

- Die Möglichkeiten zur **Überprüfung der eigenen Notfallplanung** sind vielfältig:
  - Sie reichen von einfachen Überprüfungen von Einzelmaßnahmen bis hin zu komplexen Übungen

Bearbeitung bis 9:45 Uhr



(Password: DaSchu_ITS_Hamburg23)

Suchen Sie sich ein Element der OWASP TOP 10 aus und bennen Sie diese in miro (first come, first serve). →
OWASP Top Ten | OWASP Foundation
Bereiten Sie einen fünfminütigen Vortrag über Definition, Gefahr und Gegenmaßnahme vor.
Vorstellung der Ergebnisse im Plenum

Gibt es zu den bisherigen Inhalten Fragen?