STAATLICH ANERKANNTE HOCHSCHULE

DIE UNGELIEBTE DSGVO

und was wir daraus für unsere eigene Sicherheit im Internet lernen können

SRH FERNHOCHSCHULE
The Mobile University

Prof. Dr. Wolfram Behm

1

SRH FERNHOCHSCHULE
The Mobile University

2018: PLÖTZLICH DSGVO

2

STAATLICH ANERKANNTE HOCHSCHULE

DIE GESCHICHTE DER DSGVO

SRH FERNHOCHSCHULE
The Mobile University

3

SRH FERNHOCHSCHULE
The Mobile University

1977: BUNDESDATENSCHUTZGESETZ (BDSG)

Es regelte zunächst nur den Umgang von Behörden mit personenbezogenen Daten und betraf noch keine privatwirtschaftlichen Unternehmen.

Gleiches galt für die Landesdatenschutzgesetze der Bundesländer.

Allerdings wird das Allgemeine Persönlichkeitsrecht, ebenso wie auch andere Grundrechte, auch als Schutzauftrag an den Staat verstanden. Dieser muss Rahmenbedingungen schaffen, dass der Einzelne auch Eingriffen Dritter (zum Beispiel Unternehmen) in seine Privatsphäre nicht schutzlos ausgeliefert ist.

Moderne Datenschutzgesetze (auch BDSG) enthielten daher auch umfangreiche Regelungen über den Umgang nichtöffentlicher Stellen mit personenbezogenen Daten.

4

1995: DATENSCHUTZRICHTLINIE 95/46/EG

„Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“: Regelungsinstrumente, die nicht unmittelbar gelten, sondern zunächst von den Mitgliedsstaaten in nationales Recht umgesetzt werden müssen.

Die Bundesrepublik Deutschland hat diese Richtlinie umgesetzt, indem sie ihre Vorgaben in das deutsche BDSG aufgenommen hat.

Trotz der Datenschutzrichtlinie 95/46/EG verblieben große Unterschiede in den Datenschutzgesetzen der EU-Mitgliedstaaten.

5

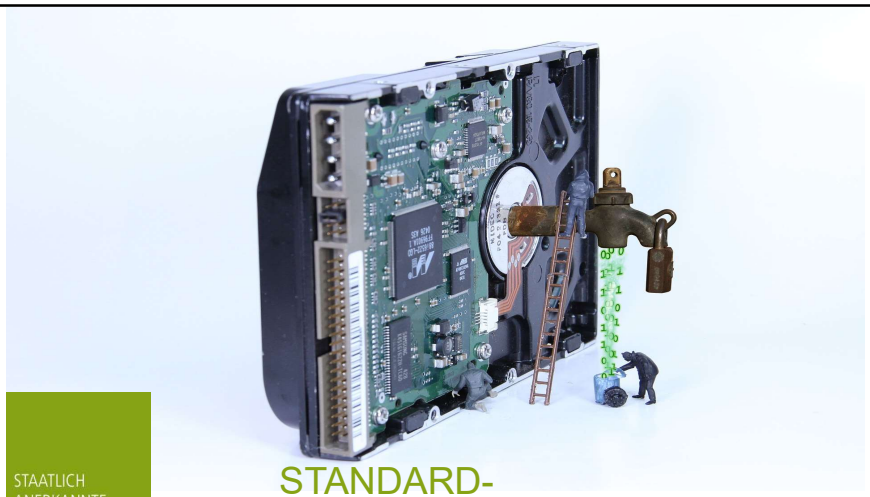
2016/2018: DSGVO

Die EU wählte daher ein neues Regelungsinstrument und verabschiedete 2016 die Datenschutz-Grundverordnung (DSGVO), die im Mai 2018 nach einer Umsetzungsperiode von zwei Jahren in Kraft trat.

Als Verordnung gilt sie wie ein Gesetz unmittelbar und zwingend in allen Mitgliedstaaten, ohne dass sie zunächst in nationales Recht umgesetzt werden muss.

Sie verdrängt in ihrem Anwendungsbereich zum einen die ältere Datenschutzrichtlinie, zum anderen aber auch nationale Gesetze, die denselben Regelungsgegenstand haben. Das bisherige nationale BDSG wurde damit obsolet. Auch für die Zukunft können Mitgliedstaaten grundsätzlich keine nationalen Gesetze erlassen, die im Widerspruch zur DSGVO stehen.

6



STAATLICH ANERKANNTE HOCHSCHULE

STANDARD-DATENSCHUTZMODELL

Generischen Maßnahmen zur Umsetzung der Gewährleistungsziele

SRH FERNHOCHSCHULE The Mobile University

7

SRH FERNHOCHSCHULE The Mobile University

DAS STANDARD-DATENSCHUTZMODELL

Gemäß Art. 5 DSGVO lassen sich **wesentliche Grundsätze** für die Verarbeitung personenbezogener Daten auflisten: Die Verarbeitung muss

- rechtmäßig,
- nach Treu und Glauben,
- nachvollziehbar,
- zweckgebunden,
- auf das notwendige Maß beschränkt,
- auf der Basis richtiger Daten,
- vor Verlust, Zerstörung und Schädigung geschützt
- die Integrität und Vertraulichkeit wahrend

stattfinden.

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 5

8

SRH FERNHOCHSCHULE
The Mobile University

DAS STANDARD-DATENSCHUTZMODELL

Wesentliche Grundsätze

Die Einhaltung der Grundsätze gemäß Art. 5 DSGVO muss nachweisbar sein – es besteht eine „Rechenschaftspflicht“.

„Das Standard-Datenschutzmodell (SDM) bietet geeignete Mechanismen, um diese rechtlichen Anforderungen der DSGVO in technische und organisatorische Maßnahmen zu überführen.“ Dazu werden im SDM die rechtlichen Anforderungen in Form der Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit formuliert.

Das SDM überführt mit Hilfe dieser Gewährleistungsziele die rechtlichen Anforderungen der DS-GVO in die von der Verordnung geforderten technischen und organisatorischen Maßnahmen.

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 5

9

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

In Kapitel 7 SDM „werden generische Datenschutz-Schutzmaßnahmen aufgeführt, die in der Datenschutzprüfpraxis vieler Datenschutzaufsichtsbehörden seit vielen Jahren erprobt sind.“

Es wird deutlich, dass sich die Datenschutzanforderungen grundsätzlich sinnvoll strukturieren lassen. Dies erleichtert es Unternehmen eine systematische Umsetzung.

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 22

10

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHE MAßNAHMEN

a) Datenminimierung

Der Zweck einer Daten-verarbeitung begrenzt auch den Umfang der Daten, die in ihrem Rahmen verarbeitet werden dürfen.

Nicht notwendige Daten bedürfen einer zusätzlichen Rechtsgrundlage.

Bild: Pixabay.com

11

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

a) Datenminimierung

Typische Maßnahmen:
Reduzierung von erfassten Attributen der betroffenen Personen
Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
Bevorzugung automatisierter Verarbeitungsprozessen (nicht Entscheidungsprozessen), => weniger Kenntnisnahme verarbeiteter Daten und weniger Einflussnahme gegenüber im Dialog gesteuerten Prozessen
Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren
Regelungen zur Kontrolle von Prozessen zur Änderung von Verarbeitungstätigkeiten

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 22

12

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHE MAßNAHMEN

b) Verfügbarkeit

Auf die Daten muss genau dann zugegriffen werden können, wenn dies erforderlich ist. Hierzu müssen sie auffindbar und von den eingesetzten Programmen interpretierbar sein. Dies ist beispielsweise gefährdet bei Serverausfällen durch höhere Gewalt oder Hackerangriffe.

Bild: Pixabay.com

13

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

b) **Verfügbarkeit**

Typische Maßnahmen:
Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts
Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
Dokumentation der Syntax der Daten
Redundanz von Hard- und Software sowie Infrastruktur
Umsetzung von Reparaturstrategien und Ausweichprozessen
Vertretungsregelungen für abwesende Mitarbeitende

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 22

14

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHE MAßNAHMEN

c) Integrität

Die Daten sind gegen Manipulationen geschützt, also unversehrt, vollständig und aktuell.

Abweichungen müssen ausgeschlossen werden oder zumindest erkennbar sein, damit sie korrigiert werden können.

Bild: Pixabay.com

15

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

c) Integrität

Typische Maßnahmen:
Einschränkung von Schreib- und Änderungsrechten
Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts
dokumentierte Zuweisung von Berechtigungen und Rollen
Prozesse zur Aufrechterhaltung der Aktualität von Daten
Festlegung des Sollverhaltens von Prozessen und regelmäßige Tests zur Feststellung und Dokumentation der Ist-Zustände, der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 23

16

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHE MAßNAHMEN

d) Vertraulichkeit

Vertraulichkeit bedeutet im Zusammenhang mit der Verarbeitung von Daten, dass Unbefugte von diesen Daten nicht Kenntnis nehmen können.

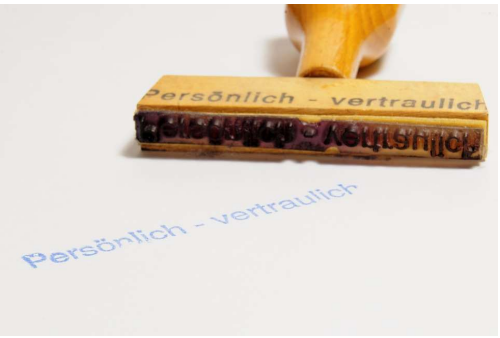


Bild: Pixabay.com

17

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

d) Vertraulichkeit (1)

Typische Maßnahmen:
Festlegung eines Rechte- und Rollen-Konzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle
Implementierung eines sicheren Authentisierungsverfahrens
Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zu-gelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen
Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 23

18

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

d) Vertraulichkeit (2)

Typische Maßnahmen:
spezifizierte, für das Verarbeitungstätigkeit ausgestattete Umgebungen (Gebäude, Räume)
Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheits-vereinbarungen etc.)
Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept)
Schutz vor äußeren Einflüssen (Spionage, Hacking)

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 23

19

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHE MAßNAHMEN

e) Nichtverkettung

Personenbezogene Daten dürfen ausschließlich zu festgelegten Zwecken verarbeitet werden.

Bild: Pixabay.com

20

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

e) Nichtverkettung (1)

Typische Maßnahmen:
Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
programmtechnische Unterlassung bzw. Schließung von Schnittstellen bei Verarbeitungsverfahren und Komponenten
regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
Trennung nach Organisations-/Abteilungsgrenzen
Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 23-24

21

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

e) Nichtverkettung (2)

Typische Maßnahmen:
Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle
Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten
geregelte Zweckänderungsverfahren

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 23-24

22

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHE MAßNAHMEN

f) Transparenz

Das Ziel der Transparenz bedeutet unter anderem, dass nachvollziehbar ist, welche Daten zu welchen Zwecken verarbeitet werden. Dies gilt vor allem für Betroffene. Eine heimliche Datenverarbeitung, mit der die Betroffenen nicht rechnen müssen, ist regelmäßig nicht gestattet.

Bild: Pixabay.com

23

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

f) Transparenz (1)

Typische Maßnahmen:
Dokumentation von Verarbeitungstätigkeiten insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Beschreibungen von Verarbeitungstätigkeiten, Zusammenspiel mit anderen Verarbeitungstätigkeiten
Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verarbeitungstätigkeiten
Dokumentation der Verträge mit den internen Mitarbeitenden, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 24

24

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

f) Transparenz (2)

Typische Maßnahmen:
Dokumentation von Einwilligungen und Widersprüchen
Protokollierung von Zugriffen und Änderungen
Nachweis der Quellen von Daten (Authentizität)
Versionierung
Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts
Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 24

25

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHE MAßNAHMEN

g) Intervenierbarkeit

Die Rechte des Betroffenen aus Art. 15ff. DSGVO (wie zum Beispiel Auskunft und Löschung der Daten) muss jederzeit umgesetzt werden können.

Bild: Pixabay.com

26

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

g) Intervenierbarkeit (1)

Typische Maßnahmen:
differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verarbeitungstätigkeiten sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 24-25

27

SRH FERNHOCHSCHULE
The Mobile University

GENERISCHEN MAßNAHMEN

g) Intervenierbarkeit (2)

Typische Maßnahmen:
Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen
Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte
Einrichtung eines Single Point of Contact (SPoC) für Betroffene
operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten

Das Standard-Datenschutzmodell, V.1.1 –Erprobungsfassung, S. 24-25

28

STAATLICH ANERKANNTE HOCHSCHULE

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

SRH FERNHOCHSCHULE
The Mobile University

29

SRH FERNHOCHSCHULE
The Mobile University

INHALTSVERZEICHNIS

Bild: Pixabay.com

30

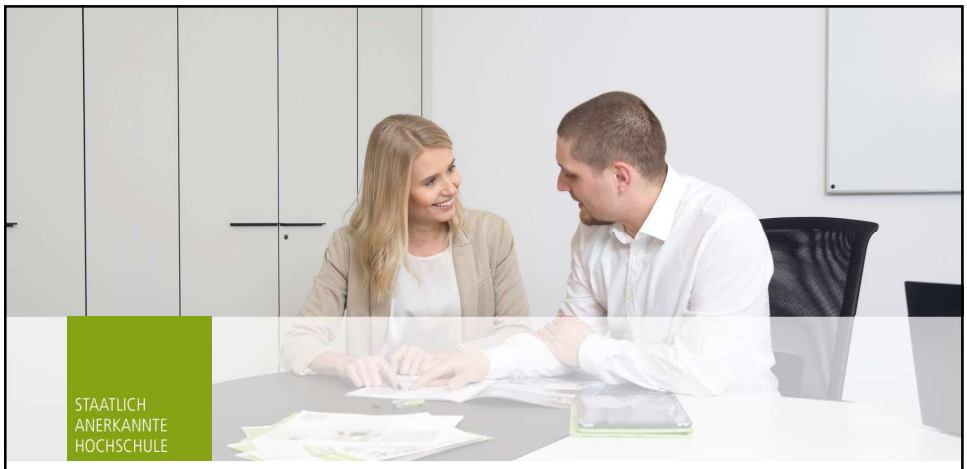
SRH FERNHOCHSCHULE
The Mobile University

INHALTSVERZEICHNIS

3. Verfügbarkeit und Belastbarkeit
   - Verfügbarkeitskontrolle
4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
   - Datenschutz-Maßnahmen
   - Incident-Response-Management
   - Datenschutzfreundliche Voreinstellungen
   - Auftragskontrolle (Outsourcing an Dritte)

Bild: Pixabay.com

31



AUFTRAGSVERARBEITUNG

SRH FERNHOCHSCHULE
The Mobile University

32

SRH FERNHOCHSCHULE
The Mobile University

INHALTSVERZEICHNIS

1. Präambel
2. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung
3. Anwendungsbereich und Verantwortlichkeit
4. Pflichten des Auftragnehmers
5. Pflichten des Auftraggebers
6. Anfragen betroffener Personen
7. Nachweismöglichkeiten
8. Subunternehmer
9. Haftung und Schadensersatz

Bild: Pixabay.com

33

Zwischenfazit

SRH FERNHOCHSCHULE
The Mobile University

34

STAATLICH
ANERKANNTE
HOCHSCHULE

BEDROHUNGEN

SRH FERNHOCHSCHULE
The Mobile University

35

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

Computer- Viren

bösartige Software (auch Malware genannt), die Rechner infizieren und dort Schaden anrichten. Ein Virus benötigt einen Wirt, also ein Programm, in das er seinen Code hineinkopiert und dadurch seine Funktionen verändert.

Bild: Pixabay.com

36

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

Computer- Viren

Viren gelangen auf einen Rechner über verseuchte E-Mail-Anhänge oder den Aufruf verseuchter Programme von einem Datenträger, aus dem lokalen Netzwerk oder dem Internet.

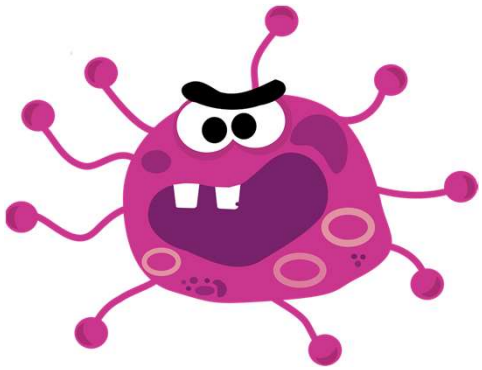


Bild: Pixabay.com

37

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

Trojaner

Schadprogramm, das sich als eine andere, harmlose oder nützliche Datei tarnt und auf diese Weise vom Nutzer auf den Rechner geladen und ausgeführt wird.

Bild: Pixabay.com

38

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

Computer- Wurm

Schadprogramm, das sich selbst weiterverbreiten kann, indem es sich automatisch verschickt, zum Beispiel
über offene Ports, die durch angreifbare Software im Unternehmensnetzwerk betrieben werden.

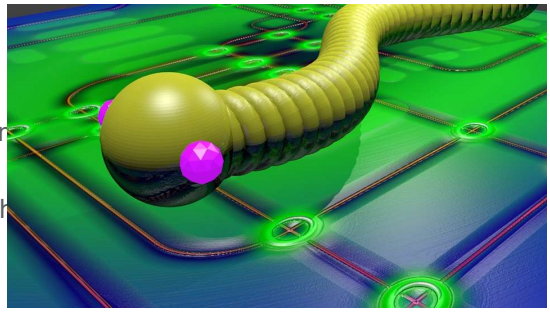


Bild: Pixabay.com

39

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

DDOS-Attacke

Bei einer „Distributed Denial of Service“-Attacke (kurz DDOS-Attacke) versucht ein Angreifer, das System seines Opfers durch eine hohe Zahl von Serveranfragen zu überlasten und lahmzulegen.

Bild: Pixabay.com

40

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

Brute Force-Attacken

sollen einen passwort-geschützten Zugang knacken, indem in kurzer Zeit automatisiert eine große Menge möglicher Passwörter einfach ausprobiert werden.

Bild: Pixabay.com

41

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

Man-in-the-Middle-Angriff

Möglichkeit, eine Kommunikation zwischen zwei Stationen zu belauschen. Dabei werden die Datenpakete über einen dritten Rechner „in der Mitte“ umgeleitet, wo sie mitprotokolliert und gelesen werden können.

Bild: Pixabay.com

42

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

IP-Spoofing

Angreifer fälschen die Absenderadresse; so können sie sich z.B. von außen in ein geschütztes Netzwerk einschleusen, indem sie eine IP-Adresse aus dem geschützten Netzwerk selbst vorgaukeln.

Bild: Pixabay.com

43

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

Cross Site Scripting

ein Angreifer schleust Programmcode auf eine fremde Website. Loggt sich der Nutzer auf dieser Website ein, wird der fremde Code ausgeführt und hat daher alle Privilegien, die der angemeldete Benutzer selbst hat.

Bild: Pixabay.com

44

SRH FERNHOCHSCHULE
The Mobile University

BEDROHUNGEN

Social Engineering

durch Täuschung, Überzeugungskraft, Ausnutzen von Höflichkeit oder Hilfsbereitschaft oder ähnliche Methoden im persönlichen Kontakt mit Menschen werden hilfreiche Informationen oder Zugang zu geschützten Systemen erlangt.

Bild: Pixabay.com

45

STAATLICH ANERKANNTE HOCHSCHULE

KEINE BEDROHUNG, SONDERN REALITÄT

SRH FERNHOCHSCHULE
The Mobile University

46

SRH FERNHOCHSCHULE
The Mobile University

DATA ANALYTICS

Riesige und verschiedenste Datenbestände werden verknüpft und analysiert, um daraus unterschiedlichste Informationen zu gewinnen.

Bild: Pixabay.com

47

SRH FERNHOCHSCHULE
The Mobile University

BEISPIELE

Bild: Pixabay.com

48


100%-ige Sicherheit kann es nicht geben
Die sicherste Technik hilft nichts, wenn wir selbst sorglos Daten verbreiten
Für die DSGVO war es höchste Zeit
Datenschutz ist eine komplexe Herausforderung
SRH FERNHOCHSCHULE
The Mobile University

49