07.10.21 Datenschutz & Datensicherheit

Donnerstag, 7. Oktober 2021 08:20

Datenschutz -> Missbrauch von personenbezogenen Daten verhindern
-> garantiert "jedem Bürger Schutz vor missbräuchlicher Datenverarbeitung, das Recht auf informationelle Selbstbestimmung und den Schutz der Privatsphäre."
DSGVO
IT - Sicherheitsgesetz
Bundesdatenschutzgesetz

- Rechenschaftspflicht
- Schutz vor Veränderung
- Schutz vor Veränderung

Datensicherheit -> Datenintegrität und Betrieb gewährleisten
-> Datensicherheit hat das technische Ziel, Daten jeglicher Art in ausreichendem Maße gegen Manipulation, Verlust, unberechtigte Kenntnisnahme durch Dritte oder andere Bedrohungen zu sichern

Personenbezogene Daten

Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person

Grundsätzlich gilt, dass alle Informationen, über die irgendwie ein Personenbezug hergestellt werden kann, auch unter den Begriff der personenbezogenen Daten fallen.

Statische und dynamische IP-Adressen -> Personenbezogene Daten
Provider sind gesetzlich verpflichtet 10 Wochen Daten zu speichern

11.10.21 RAID

Montag, 11. Oktober 2021 08:16

-> Redundant Array of Independent (Inexpansive) Disks

Leistungsmerkmale:

- Laufwerk-Kopplung: mehrere Laufwerke können zu einem "Laufwerkbuchstaben" zusammengefasst werden
- Datensicherheit: Daten werden gespiegelt oder über zusätzliche Bits nach Ausfall wieder verfügbar gemacht
- Geschwindigkeit: Schreib-/Lesevorgänge werden intelligent auf mehrere Laufwerke verteilt, allerdings mehrere Kanäle notwendig (Parallelität)
- Ersatzplatte: unter Umständen im laufenden Betrieb Wechselmöglichkeit (insofern Lesekopf sich nicht dreht)
- Ausbau: zusätzliche Schnittstellen verfügbar

-> Fachausdrucke:

- Chaining: mehrere Festplatten so zusammenhängen, dass sie als eine große Festplatte erscheinen
- Hot -Plug / Hot -Swap austauschen im laufenden Betrieb von Festplatte(n)
- Hot -Fix / Hot- Spare automatisches Ersetzen einer defekten Platte durch eine im System befindliche
- Redundant: eine Komponente darf ausfallen, ohne das gesamte System zu beeinflussen (eigentlich: überflüssig)
- Dediziert: fest zugewiesen
- MTBF: Man Time Between Failure durchschnittliche Zeit zwischen zwei Ausfällen statistische Größe

RAID - Level

- RAID 0 - Data Striping

Die Daten werden über alle am RAID beteiligten Festplatten verteilt. Das parallele Lesen respektive Schreiben auf mehreren Laufwerken steigert zwar die Durchsatzrate, senkt jedoch die Sicherheit der Daten: Fällt eine Platte des Verbunds aus, sind alle Daten verloren

Kleinste Sektorgröße - MBR 512Byte
Viele große Dateien aber kleine Sektoren -> viele Streifen

- RAID 1 - Mirroring

Bei RAID 1 werden die Daten auf mehrere Festplatten gespiegelt.
Da die Daten mehrfach vorhanden sind ist ein Festplattenausfall kein Problem mehr.

- RAID 5 - Data (Sector) Striping mit Parity Information

RAID 5 verteilt alle Daten und zusätzliche Paritätsinformationen gleichmäßig über die Festplatten. Dadurch steigen die Lese- und Schreibraten, obwohl die Datenverfügbarkeit gewährt bleibt.

Mindestplattenanzahl bei RAID 5: 3 Festplatten

- RAID 10 - Striped Mirror

RAID 10 ist eine Kombination aus RAID 1 und 0 . Dabei werden wie bei RAID 1 die Festplatten gespiegelt, diese Daten jedoch anschließend bei RAID 0 mittels Striping über die Festplatten verteilt. Die Perfomance ist insgesamt gesteigert obwohl die Daten gesichert sind bei RAID 1.

Aufgabe: Erstellen Sie eine Wertetabelle mit 3 Eingangsvariablen und einem Ausgang und ermitteln Sie die Werte am Ausgang für eine logische XOR - Verknüpfung!

Beispiel:

Laufwerk1	Laufwerk2	Laufwerk3	Parität
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Rekonstruierbar bei einer Fehlerhaften Platte. Unmöglich bei 2

- RAID 7 - Proprietär(Herstellergebunden)

14.10.21 Datenschutzbeauftragte

Donnerstag, 14. Oktober 2021 08:16

Stellung des Datenschutzbeauftragten

- Unabhängigkeit und organisatorische Einordnung
- Abberufungsschutz, Kündigungsschutz und Benachteiligungsverbot
- Anspruch auf Einbindung, Unterstützung und Fortbildung

Kernaufgabe des Datenschutzbeauftragten neben der Unterrichtung und Beratung ist die Überwachung der Einhaltung des Datenschutzes

Internationaler Datenschutz

Probleme beim internationalen Datenschutz

- Anwendbares Recht
  - Wurde ein bestimmtes Recht vereinbart bzw. kann mit dem jeweiligen Land vereinbart werden?
- Internationaler Gerichtsstand
  - Vor welchen Gerichten welches Landes kann geklagt oder angeklagt werden?
- Internationale Behördenzuständigkeit
  - Welche Aufsichtsbehörde ist zuständig?
- Grenzüberschreitender Datenverkehr
  - Wie ist der Umgang mit personenbezogenen Daten bei Datenexport und bei anderen grenzüberschreitenden Sachverhalten geregelt?

Vertraulichkeit	Schutz von Informationen gegenüber unbefugten Zugriffen Dritter
Integrität	Schutz von Informationen gegenüber Veränderungen durch Unbefugte
Verfügbarkeit	Ressourcen und Dienste stehen legitimen Benutzern tatsächlich zur Verfügung
Authentifizierung	ich bin der als der ich mich ausgebe
Verbindlichkeit	Möglichkeit, den Inhalt und den Absender von Informationen gegenüber einem an der Kommunikation nicht beteiligten Dritten zu beweisen
Autorisation	Beschränkung des Zugriffs auf eine Ressource auf bestimmte Benutzer

Das Schutzziel der Vertraulichkeit gilt als verletzt, wenn geschützte Daten von unautorisierten Subjekten eingesehen werden können.

Das Schutzziel der Integrität gilt als verletzt, wenn Daten von unautorisierten Subjekten unbemerkt verändert werden können.

Das Schutzziel der Verfügbarkeit gilt als verletzt, wenn ein Angreifer die Dienst- und Datennutzung durch legitime Anwender eingeschränkt bzw. verhindert.

Authentisierung

- Bezeichnet das Nachweisen einer Identität.

Authentifizierung

- Die Authentifizierung stellt eine Prüfung der behaupteten Authentisierung dar. Bei der Authentifizierung ist nun der Prüfer an der Reihe.
- Bezeichnet Prüfung der obigen Identität.

Autorisierung

- Die Autorisierung ist das Einräumen von speziellen Rechten.
- Bezeichnet das gewähren von Rechten für die obig authentifizierte Identität

Sonntag, 16. Januar 2022 19:21

IT 10 -
5 Sicherheitsregeln
Netzformen
Schutzmaßnahmen
Wartung & Instandhaltung

06.12.21 USV

Sonntag, 16. Januar 2022 19:33

Frequenz im Stromnetz: 50Hz (Periodendauer 20ms)
-> USV muss innerhalb der 20ms zuschalten

Spannung im Netz: 230V Effektivwert (Nicht Spannungsspitze!)
-> Effektivwert ist quasi Vergleichsgröße, weder Spitze noch Mittelwert Leistungsabnehmer erbringt bei Anschluss aus Netz gleiche Leistung wie bei Anschluss an 230V Betriebsspannung

Bestandteile: Batterie / Akku
Gleichrichter (Wechselspannung -> Gleichspannung)
Wechselrichter (Gleichspannung -> Wechselspannung)
Elektro-mechanisches Schaltrelais(Kontrolle Umschalten von Netz- auf Akkubetrieb)

Netzstörungen

1. Netzausfälle
2. Spannungschwankungen
3. Spannungsstöße
4. Unterspannungen
5. Überspannungen
6. Blitzeinwirkungen
7. Spannungsspitzen
8. Frequenzschwankungen
9. Spannungsverzerrung
10. Spannungsoberschwingungen

-> typische Prüfungsfrage: Wovor schützen USV - Anlagen ?
VFD: 1-3
VI: 1-5
VFI: 1-10

USV-Klassifizierungen nach IEC 62040-3:

Stufe 1: Abhängigkeit des USV - Ausganges vom Netz
Stufe 2: Spannungskurvenform des USV-Ausganges
Stufe 3: Dynamische Toleranzkurve des USV - Ausganges

Unterschied USV zu Notstromversorgung:
Notstromversorgung schaltet nicht sofort / unterbrechungsfrei
Notstromaggregat ist für längeren Zeitraum vorgesehen

Stufe 1: Abhängigkeit des USV Ausganges vom Netz

-> VFI
Voltage and Frequency independant
-> USV Ausgang ist abhängig vom Netz
-> Ausgangsspannung ist unabhängig von allen Netzspannungs & Frequenzschwankungen

-> VI
Voltage independent

-> USV Ausgang ist abhängig von der Netzfrequenz
-> wird aber durch aktive & passive Regeleinrichtungen innerhalb bestimmter Grenzen aufbereitet

-> VFD
Voltage and frequency dependent

-> USV Ausgang ist abhängig von Änderungen der Netzspannung und Netzfrequenz,
Wenn die USV keine Maßnahmen zur Verbesserung durch Anzapftransformatoren, EMV Filter oder Varistoren hat

Anwendungsbereiche:

VFI:
- Sicherheitssysteme
- Sensible Server & IT Anwendungen
- Kleine Netzwerke
- Messtechnische & Industrielle Anlagen
- Steuersysteme

VI
- PC & Workstation
- TK - Anlagen
- Kassensysteme
- Kleine Server
- Netzwerkkomponenten

VFD
- PC und Workstations
- Homeoffice

17.01.22 Kryptographie

Montag, 17. Januar 2022 08:13

[…] (noch teil nachzuholen)

Symmetrische Verschlüsselung

- Bei der symmetrischen Verschlüsselung wird für das verschlüsseln, wie auch für das Entschlüsseln derselbe Schlüssel verwendet. Meist ist es nützlich, eine Notation für Klartext, Chiffretext und Schlüssel zur Hand zu haben

  Beispiele: DES, Twofish, MARS, AES (Rijndael)

Asymmetrische Verschlüsselungssysteme

- Verschlüsselungssystem asymmetrisch -> Schlüssel öffentlich (public key)
  - Jeder der den Schlüssel kennt, kann Nachrichten verschlüsseln

- Nur Besitzer eines private key's kann entschlüsseln
  - Schlüssel muss nicht geheim übertragen werden

- Schlüssel muss jedoch richtig sein

  Beispiele: RSA (Wurzel ziehen), Rabin (Quadratwurzel), McEliece

  Vorteile:
  - Relativ hohe Sicherheit
  - Weniger Schlüssel benötigt, dadurch weniger Aufwand der geheimhaltung
  - Public Key ist für jeden ohne Probleme zu erreichen
  - Möglichkeit der Authentifikation durch elek. Unterschriften (digitale Signatur)

  Nachteile
  - Asymm. Verfahren arbeiten ca. 10 000 Mal langsamer als symmetrische
  - Große benötigte Schlüssellänge
  - Probleme bei mehreren Empfänger, Msg muss immer neu verschlüsselt werden

  Hybride Verfahren
  - Sicherheitsrisiko durch für jeden zugänglichen Public Key
    - Man in the Middle

Was ist besser?

-> **Hybridsysteme**:
- Nachricht wird symmetrisch verschlüsselt
- Der verwendete Schlüssel wird asymmetrisch verschlüsselt
- verschlüsselte Nachricht wird mit dem verschlüsselten Schlüssel versandt

Anwendung:

- Digitale Signatur
- Verschlüsselung von Informationen
- Zahlungssysteme

Softwaresysteme:

- Pretty good Privacy (PGP)
- GNU Privacy Guard (GPG)

Kryptoanalyse:

- Geheimtextangriff (schwierigste, probieren aller möglichen Schlüssel) Brute Force
- Klartextangriff (leistungsfähiger, Teile des Textes werden vermutet)
- Angriff mit ausgewählten Klartext
- Angriff mit adaptiv ausgewähltem Klartext (wiederholter Angriff auch in Abhängigkeit der bisherigen Kryptoanalyse)

Merkmale des Hash-Wertes

- Die Funktion ist nicht umkehrbar!
- Aus dem Hash-Wert kann also nicht auf die zu Grunde liegende Datei geschlossen werden
- Es gibt keine 2 Dateien mit dem gleichen Hash-Wert

Folgende Eigenschaften:

- Die Eingabe kann beliebig lang sein
- Die Ausgabe hat eine feste Länge
- H (x) ist für ein gegebenes x relativ leicht zu berechnen
- H (x) ist ein Weg und nicht reversibel
- H (x) ist kollisionsfrei, dh. zwei verschiedene Eingabewerte führen zu unterschiedlichen Hash-Werten

Elektronische Signatur
- Kennzeichnet den Urheber
- Unverschlüsselt
- Nicht vertraulich

Fortgeschrittene elektronische Signatur
- Verschlüsselt
- Empfänger muss den Nachweis eines sicheren Zertifikats erbringen

Qualifizierte elektronische Signatur
- Urheber wird durch qualifiziertes Zertifikate nachgewiesen
- Ist einer natürlichen Person zuzuordnen
- Ist einer handschriftlichen Unterschrift gleich gestellt

20.01.22 Firewall

Donnerstag, 20. Januar 2022 08:10

Definition:

- Eine Firewall stellt eine dauerhaft kontrollierte Verbindung zwischen zwei logischen Netzen her. Die Firewall überwach den durch sie hindurch laufenden Datenverkehr und entscheiden anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht.

Auf diese Weise versuch die Firewall das private Netzwerk bzw. das Netzsegment vor unerlaubten Zugriffen zu schützen.

Zb. Zwischen einem privaten Netz (LAN) und dem Internet (WAN)

Firewalltypen

- Paketfilter (Schicht 3 und 4 OSI - Modell)
- Application - Gateways (Schicht 7)
- Desktop - Firewalls
    - Funktionskomponenten klassischer Firewalls
        - Paketfilter (Basisfunktion)
        - Network Address Translation
        - URL-Filter
        - Content-Filter
        - Proxyfunktion
        - Virtual Private Networks (VPN)
        - Stateful Packet Inspection
        - Deep Packet Inspection
    - Next Generation Firewalls (NGFW)
        - Intrusion Detection System
        - Intrusion Prevention System
        - TLS / SSL und SSH Inspection
        - Website - Filter
        - Antivirus Inspection
        - Malwareerkennung
        - QoS Management

- Arbeitsweise Paketfilter
    - Es wird überprüft, von welcher Seite das Paket empfangen wird.
    - Auf der Netzzugangsebene werden die Quell- und Ziel-Adresse und der verwendete Protokoll-Typ kontrolliert
    - Auf Netzwerksebene (Schicht 3) wird je nach Protokoll-Typ das Paket anders kontrolliert
    - Auf Transportebene (Schicht 4) findet eine Überprüfung der gesetzten Flags, Optionen und Parameter statt
    - Zusätzlich kann überprüft werden, ob der Zugriff in einem erlaubten Zeitrahmen stattfindet

    - Statische Paketfilter
        - Treffen Entscheidung anhand der Header -Daten der UDP / IP - und TCP /IP - Schichten (z.B. Anhand der IP -Quelladresse, der IP -Zieladresse und der TCP - Flags)
    - Dynamische Paketfilter / Stateful Inspection
        - Erweitern die Funktionalität der statischen Paketfilter um die Möglichkeit zur Betrachtung des Kommunikationskontextes
        - Können auch bei verbindungslosen Protokollen (wie z.B. UDP) eine

Entscheidung treffen
        - Dienste sicher bereitstellen, die nicht mit festen Portnummern verbunden sind

- Private IP - Adressen
    - Werden nicht geroutet (vom Router nicht weitergereicht)
    - Von außen nicht anpingbar
    - Man kann den Router beispielsweise anpingen, aber nicht den Rechner direkt
- Öffentliche IP - Adressen
    - Von außen erreichbar

Vorteile von Paketfiltern
- Transparent für Benutzer und die Rechensysteme.
    - Ausnahmen sind natürlich explizite Authentifizierungen.
- Einfach erweiterungsfähig für neue Protokolle
- Flexibel für neue Dienste

Nachteile von Paketfiltern
- Daten, die oberhalb der Transportebene sind, werden in der Regel nicht analysiert
- Für die Anwendungen (FTP, HTTP, SMTP, …) besteht keine Sicherheit
- Protokolldaten werden nur bis zur Transportebene zur Verfügung gestellt
- Falsch konfigurierte Ports können feindselig ausgenutzt werden

Intrusion-Detection-System
- Heutige IDS bestehen typischerweise aus folgenden Komponenten:
    - Netzsensoren (zur Überwachung des Netzverkehrs an bestimmten Punkten)
    - Hostsensoren (zur Überwachung des Betriebssystems, von Applikationen und oder des hostspezifischen Netzverkehrs)
    - Datenbankkomponenten
    - Managementstation
    - Auswertungsstation

Intrusion-Prevention-System
- Scannt das lokale Netz nach "Besonderheiten"
    - Anomalien werden in Quarantäne geschoben und blockiert

Angriffe
- Angriffsarten
    - Passive Angriffe
        - Der Angreifer gelangt in den Besitz von Informationen, ohne selber in das Geschehen einzugreifen
    - Aktive Angriffe
        - Der Angreifer tritt selbst in Erscheinung, indem er Daten, Informationen oder Dienste fälscht, modifiziert oder löscht bzw. deren Verfügbarkeit sabotiert.

IPv4 Header

Donnerstag, 20. Januar 2022 08:20

Adresse + Port = Socket

TODO: CSMACD

24.01.22 Routing

Montag, 24. Januar 2022 08:08

- Läuft auf:
  - OSI-Model Schicht 3: Network Layer
    - Distance Vector Protokolle
    - Link State Protokolle

- Router benötigen zum Routen:
- Routing: "bester Weg von Router 1 zu Router 2
  - Zieladressen (Destination Address)
  - Quellen, von denen sie lernen
  - Mögliche Wege
  - Den besten Weg
  - Aktuelle Routing - Informationen

Statische Route

- Route, die vom Administrator manuell eingegeben wird

Dynamische Route

- Route, die von einem Routing-Protokoll automatisch erstellt wird (Topologie-und Traffic berücksichtigt)
- COMMAND: /route print
- GoodToKnow: Begriffe zur Datenübertragung
    - Datenaustausch
      - Unidirektional (Senden nur in eine Richtung)
      - Bidirektional (Hin und Zurück Senden)
      - Simplex (Nur senden)
      - Halbduplex (Erst Senden, danach Empfangen)
      - Vollplex (Senden und Empfangen parallel)

- Alle Pakete mit unbekanntem Ziel werden an ein Default-Gateway weitergeleitet. So Muss nicht für jedes Zielnetzwerk ein Eintrag gemacht werden.

Routing-Protokolle werden zur Wegewahl zwischen Routern und zur Aktualisierung der Routing Tabelle genutzt.

- Wenn ein Pfad bestimmt wurde, kann ein Router ein "routed"-Protokoll routen.
  - Routed Protokoll: IP
  - Routing Protokolle: IGRP

Distance Vector Routing-Protokolle

- Distance - Wie weit?
- Vector - Welche Richtung?
  - Senden periodisch Kopien der Routingtabelle an Nachbarrouter und nutzen Entfernung und Richtung des Ziels zur Pfadbestimmung (etwa alle 30 Sekunden)
  - Router erlernen den besten Pfad zum Ziel von ihren Nachbarn

  - Routing-Internet-Protocol (RIP)
    - Bandbreite
    - Verzögerung
    - Zuverlässigkeit
    - Last
    - MTU (Maximum transfered Unit)

Routing-Probleme: -> Unendlichkeitsprinzip (Netzwerknummern schaukeln sich hoch)

Router setzen die Entfernung einer Routerzielverbindung auf unendlich

- Lösung:
  - Maximum festlegen

Link-State Routing Protokolle

- Jedes Mitglied(Router) spricht mit jedem anderen - Beispiel WA Gruppe-> alle bekommen eine Nachricht
- Nach anfänglicher Flutung des Netzes, werden nur noch kleine event-getriggerte "Link-State-Updates" zu allen anderen Routern gesendet.
- Periodische Updates (Refresh) alle 30 Minuten

- Hybrid Routing
  - Wahl des Pfades basierend auf "Distance Vector"
    - -> Balanced Hybrid Routing
  - Schnelle Konvergenz durch änderungsbasierte Updates
  - Besitzt Attribute von "Distance-Vector-" und "Link-State-Routing"

Ziele der Routingalgorithmen

- Optimierung beste Route auswählen
- Einfachheit und geringe Belastung
- Robustheit und Stabilität bei unvorhersehbaren Ereignissen
- Schnelle Konvergenz aller Router haben gleiche korrekte Informationen
- Flexibilität
- Skalierbarkeit

27.01.22 VPN

Donnerstag, 27. Januar 2022 08:45

VPN = Virtual Private Network

- Verbindungsarten
  - Site-to-Site (Netz zu Netz
    - Sollen zwei lokale Netze miteinander verbunden werden, wird auf beiden Seiten ein VPN-Gateway verwendet. Diese bauen dann untereinander eine VPN - Verbindung auf, die meist permanent bestehen bleibt. Andere Rechner aus dem lokalen Netz können nun den VPN - Gateway verwenden, um Daten in das andere Netz zu senden.
    - So lassen sich zum Beispiel zwei weit entfernte Standorte einer Organisation oder Firma miteinander verbinden
  - End-to-Site
    - VPNs werden auch oft dazu verwendet, um Mitarbeitern außerhalb einer Organisation oder eines Untern…
- Protokolle
  - IPSec - IP Security Protocol
  - Point-to Point Tunneling Protocol
  - L2TP - Layer 2 Tunneling Protocol
- PAP
  - Das Password Authentification Protocol (PAP) ist ein Verfahren zur Authentifizierung über das Point-to-Point Protocol
  - Passwort und Benutzerkennung werden unverschlüsselt übertragen

- CHAP
  - Mehr Fokus auf Sicher