2 SNE Security Essentials 21-22

# H1 Cybersecurity teams

**Cybersecurity** : technieken die gebruikt worden om integriteit van de beveiligingsarchitectuur van een organisatie te beschermen

**GDPR:**  General Data Protection Regulation

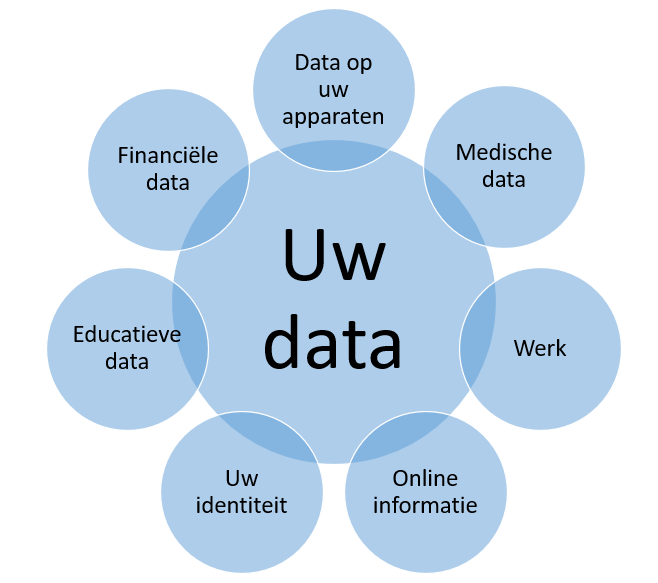
## Threats

* Voor eindgebruikers
* Persoonlijke data
* Internet service
* Belangrijke industriële diensten

**Eindgebruikers**

* Identiteit diefstal
* Carrière of persoonlijke relaties
* Kleine organisaties > grote organisaties

**Persoonlijke data**



**Internet service**

* Primaire doelen
  + Routering
  + IP Adressering
  + Domein namen
  + Database management
* Sniffing
  + Gevoelige data
  + Username & password
  + Creditcard info

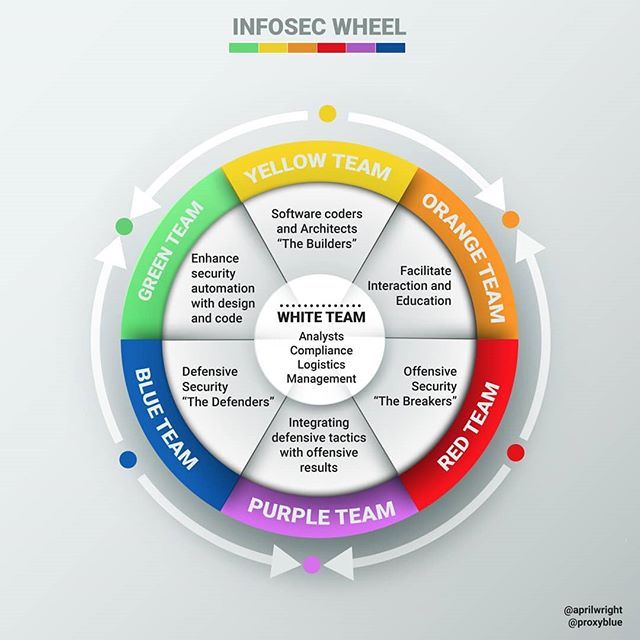
**Belangrijke industriële diensten**

* Infrastructuur systemen
  + Productie
  + Energie
  + Communicatie
  + Vervoer

## Pro’s en Con’s van de aanvaller

|  |  |  |
| --- | --- | --- |
| **Aanvaller** |  | **Verdediger** |
| moet maar 1x slagen |  | moet het elke keer juist hebben |
| kan zwakste plek kiezen |  | moet ALLES verdedigen |
| kan gebruik maken van zero-day attacks |  | kan zich enkel verweren tegen gekende aanvallen |
| kan vals spelen |  | moet zich aan de regels houden |

## INFOSEC WHEEL



**Werking infosec wheel**

**3 Primaire kleuren Rood, Blauw & Geel**

**Secundaire kleuren: paars, groen & oranje**

* Rood + blauw = paars
* Blauw + geel = groen
* Rood + geel = oranje

Ten slotte nog het witte team

**Rode team :**

* Ethical hackers
* Moeten wel toestemming hebben van de betreffende organisatie
  + Pen-test
  + Physical hacks
  + Social engineering
* Zoeken naar beveiligingslekken

Naam : The attackers / Breakers

**Blauwe team :**

* Verantwoordelijk voor beschermende maatregelen
* Damage control
* Incident response
* Zoeken / jagen op de bedreigers
* Data forensics

Naam: The defenders

**Gele team :**

* Ontwerpen en bouwen van software, systemen en integraties
* Doel : bedrijf efficiënter maken
  + App-dev
  + Software-engineers
  + Systeem architecten
* Focus ligt op: vereisten, functionaliteit, gebruikerservaring & back-endprestaties

Naam: The builders

Paarse team :

* Primaire doel : resultaten van red-team te maximaliseren en de blue-team capaciteiten te verbeteren
* Deze samenwerking verbetert de veiligheidspositie van een testscope om een betere verdediging te bouwen op basis van ontdekte zwakheden
* Gangbare term voor activiteiten waarbij rode en blauwe teams worden gecombineerd.

Oranje team :

Codeerders (geel) inspireren met aanvallers (Rood)

De reden voor veel beveiligingsfouten in software

Niet kwaadwillende programmeurs

Meer een gebrek aan beveiligingsbewustzijn binnen soft-dev teams en architecten.

Doel van het oranje team is om yellow team te:

Inspireren om veiliger te werk te gaan

Hun beveiligingsbewustzijn te vergroten door onderwijs te geven ten behoeve van softwarecode en ontwerpimplementatie

Je wilt dat je Oranje team je ontwikkelaars (geel) leert denken als aanvallers

**Groene team :**

* Verbeter de verdediging (blauw) met codeurs (geel)
* Blue team is niet altijd op de hoogte van zaken die het geel team heeft toegevoegd: alle frameworks bibliotheken, systemen van derden…
* In het geval van een incident beschikt het blauwe team mogelijk niet over de gegevens die nodig zijn om **geschonden systemen te onderzoeken of te verdedigen**
* Groene team bestaat uit doorlopende gestructureerde interacties tussen het blue team en leden van yellow team (coders)
* Doel : het **verbeteren van op code gebaseerde en ontwerp gebaseerde verdedigingsmogelijkheden** voor detectie, incidenttrespons en dataforensisch onderzoek

**White team**

* Alle kleuren samen brengen
* Alwetende, neutrale derde partij die:
  + De regels bepalen
  + Andere teams organiseren
  + Strategie bepalen
  + Risicobeoordeling uitvoeren
  + Vooruitgang monitoren
* White team leden bevatten elementen van compliance, management, analisten, logistiek en meer
* White team is net zo essentieel als bouwers, aanvallers en verdedigers. White team omvat en beheert alle kleuren zonder direct een van hen te zijn

Naam : the game masters

**CEH :** certified ethical hacker professionele hacker

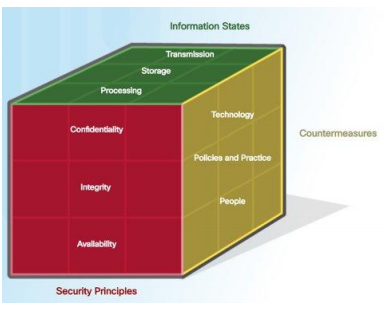
# H2 Security cube

**Cybersecurity cube**

* Is een veelgebruikt framework binnen cybersecurity
* Voorziet bescherming van
  + Netwerken
  + Domeinen
  + Internet
* Uitgevonden door John McCumber

De security cube heeft 3 dimensies

* Security Piniciples (goals)
* Information states
* Countermeasures



**Security principles**

* **CIA triad (1e dimention)**
  + Confidenttiality : privacy , onbevoegde toegang, toeganscontrole, encryptie: AAA
    - AAA: authentication, authorization, accounting
  + Integrity : accuraat, betrouwbaar, consistent (niet veranderen)
    - Hoe zorgen voor integrity
      * Backups toeganscontrole, data valideren
      * Afbeelding met tekst

        Automatisch gegenereerde beschrijving
  + Availability: backups, redundate systemen, betere veerkracht van systemin, disaster recovery

**The states of data**

* **PST: processing, storage, transmission (2e dimention)**
  + Data at rest (DAR)
    - Hoofddoelwit voor hackers
    - Data opslaan
      * Databases
      * Spreadsheets
      * Hardeschijf , tape…
    - Beschermen :
      * Encryptie & backups
  + Data in transit
    - data die verstuurd wordt
      * over publieke networks
      * private networks (VPN, LAN)
      * bedraad
      * sneaker net (removable media)
  + Data in use
    - Initiële ingave
      * Handmatige ingave
      * Gescande formulieren
      * File uploads
    - Wijziging
      * Encoding / decoding
      * Compression / decompression
    - Berekeningen op data
    - Output

**Countermeasures**

* **TPP : Technology, Policies & practice, People (3e dimension)**
  + Technologies
    - Software-based : software firewalls, portscanning, analyze network traffic, files loggen
    - hardware-based : firewall, intrusion detection systems, intrusion prevention system, content filtering
    - network-based : VPN , NAC(network access control)
    - cloud-based : Saas, Paas, Iaas, (on prem)
  + Education, awareness and training
    - Menselijke factor, persoonlijke trainingen, online trainingen, nieuwe gebruiker wegwijs maken binnen de organisatie. Security awareness
  + Cybersecurity policies & procedures
    - Standards
      * Policies voor afhandelen incidenten
      * Identificatie en authenticatie policies
      * Password policies
      * Remote access
      * Netwerkbeheer
    - Guidelines
    - Activity

# H3 Protecting secrets

**Cryptologie:** leer van het maken en berekenen van geheime codes

**Cryptografie:**  Ontwikkelen / schrijven en gebruiken van de codes

**Cryptanalyse:**  Het analyseren en bestuderen van codes en ze vervolgens kraken

**Steganografie:** Wetenschap / kunst van het verbergen van de berichten in andere informatiebronnen

**Steganalyse:** Technologie die de verborgen informatie probeert te detecteren en vervolgens eruit te halen (extraheren)

**Plaintext:** originerel tekst / bericht.

**Encryptie:**  het versleutelen van plaintext voordat die verzonden wordt. Resultaat is ciphertext

**Key:** sleutel die enkel gedeeld is tussen zender en ontvanger, hiermee kan je de ciphertext ontsleutelen tot plaintext

**Decryptie:** ontsleutelen van de ciphertext met een key. Resultaat = plaintext

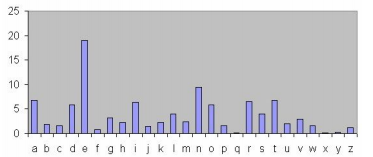
**Encoding:** geen encryptie! = coderen van een boodschap, encryptie is geheim houden, BV binair , HEX

## Klassieke Cyptografie

* **Substitutie**
* **Transpositie**
* **One-time pad**
* **Kerckhoffs principe**

### Substitutie

* Karakters vervangen (karakters, cijfers, letters, symbolen)
* 2 Soorten
  + Eenvoudige substitutie
    - Karakter per karakter
  + Polygrafische substitutie
    - Karakters groeperen en vervangen
* Nadeel
  + Berekenbaar via frequentieanalyze
  + Zoek veelgebruikte letters in ciphertext en vervang door populaire letters in je taal



**Types:**

* Monoalfabetische substitutie (naïf):
  + Caeserrotatie: volgens een formule vast aantal tekens verder shiften.
  + Atbash: vervang bijvoorbeel ‘x’ door ‘a’, ‘y’ door ‘b’,…
* Homofone substitutie (beter)
  + De E komt bijvoorbeeld vaak voor 🡺 laat E vervangen door meer dan 1 symbool
* Polygrafische substitutie
  + Combineer karakters tot een groep en vervang de groep
  + Gebruik gemaakt van verschillende versleutelingsalfabetten, meestal in de vorm van de tabellen
  + Complexere manier: verschillende alfabetten

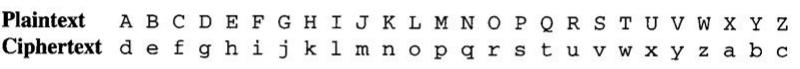
**Caeserrotatie**

Vervang iedere letter door een letter 3 plaatsen te verschuiven in het alfabet

‘A’ wordt ‘D’ **(ROT 3)**

Maak daarna hoofdletters klein

‘D’ wordt ‘d’

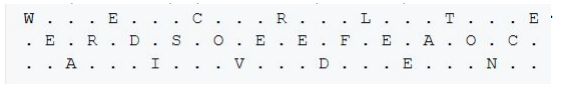


Oefenen in Excel!

### Transpositie

**Rail Fence:**

Stel een key in: is een nummer ‘X’ dus dan maak je X aantal rijen en kijk of je links of rechts vanboven of vanonder moet starten.



Ciphertext: begin met de 1e rij en zo naar de volgende en het aan elkaar plakken

Ciphertext : Afbeelding met tekst

Automatisch gegenereerde beschrijving

**Regular columnar**

* Stap 1 : verzin een KEY, liefst letters die maar 1x voorkomen : bv ‘zebras’ en niet ‘eten’
* Nummer dan de letters navenant hun alfabetische volgorde.

Afbeelding met tekst, klok

Automatisch gegenereerde beschrijving

* Stel de boodschap in bv “ik heb geen zin in de examens”
* Kies een karakter voor spaties, of om kolom op te vullen bv: ‘&’
* Vul dan je tekst in in het raster

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Z | E | B | R | A | S |
| 6 | 3 | 2 | 4 | 1 | 5 |
|  |  |  |  |  |  |
| i | k | & | h | e | b |
| & | g | e | e | n | & |
| z | i | n | & | i | n |
| & | d | e | & | e | x |
| a | m | e | n | s | & |

**Ga dan de kolommen af via alfabetische volgorde.**

Enies&eneekgidmhe&&nb&nx&i&z&a

* **Decyptie**
  + **Gegeven de key ‘zebras’**
  + **En de ciphertext:** Enies&eneekgidmhe&&nb&nx&i&z&a
* Bepaal het aantal oorspronkelijke rijen
  + Aantal tekens ciphertext / aantal tekens key = 30 / 6 = 5 dus 5 rijen
  + Plaats nu de ciphertext in de colomen volgens alfabet gelijk de key.

**OTP = One time pad**

* Probleem met caeserROT13 🡪 elk karakter heeft dezelfde shift
* Otp heeft verschillende shift voor elk karakter
  + In theorie onmogelijk te kraken
  + Wordt ook gebruikt in moderne crypto
* De Key moet minstens even lang als de boodschap zijn
* Key wordt maar 1x gebruikt en is volledig random.

Afbeelding met tekst, tijd, dag, dak

Automatisch gegenereerde beschrijving

De cijfers onder de tekst is de plaats in het alfabet

Doe dan de som van de 2.

Als de som groter is dan 25 (dus 26 of meer)

Doe dan de som – 26

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Decrytion::

Cipher tekst – key



Als er een getal kleiner is da 0. Tel er dan 26 bij



## Moderne cryptografie

### XOR



Bijvoorbeeld

01100111

11010101

XOR

10110010

### Machten

2^0=1

2^1=2

2^2=4

…

Met letters g^3= g\*g\*g

g^n = g\*g\*g\*…\*(n)

### Modulo

= restwaarde

26 mod 12 = 2 want 12 gaat 2x in 26 dan heb je 24 en is de restwaarde 2

Afbeelding met tekst, klok, hand, tijd

Automatisch gegenereerde beschrijving

### Priemgetal

* Een getal is ofwel een priemgetal of samengesteld getal
* Priemgetal
  + Is een natuurlijk getal en enkel deelbaar door 1 en zichzelf
    - 2,3,5…
  + Onbreekbaar (ondeelbaar)
* Samengesteld getal
  + Natuurlijk getal, minsten 2x deelbaar door een priemgetal
    - 15 = 3\*5
    - 49 = 7\*7
  + == Breekbaar (deelbaar)

Afbeelding met tekst, gekoppeld, apparaat, meter

Automatisch gegenereerde beschrijving

### Encryptie standard

* **Des**
  + Geschreven door IBM + NSA
  + Niet meer veilig sinds 1995
  + Lengte 64 bits (56 bits + 8 controle bits)
* **3DES**
  + Doet 3x DES en gebruikt 3 keys van elk 56 bits
  + 3x trager dan DES
* iets sneller nodig dan 3DES en minstens even veilig
* **AES : Advanced encryption standard**
  + Rijdael algoritme
    - Geschreven door 2 belgen; Vincent Rijmen & Joan Daemen

### AES

128 bits = 10 rondes

192 bits = 12 rondes

256 bits = 14 rondes

Voorbeeld lookup table

01011101 => 11001001

11111111 => 10100010

… (nog 254 extra waarden)

Wat mag niet in zo’n lookup table:

01011101 => 01011101 (🡪 dit is hetzelfde)

00001111 => 11110000 (🡪 gefilpte bits, dus dat alle 1’s allemaal 0’en worden en dat alle 0’en allemaal 1’s worden)

Row shift

1ste rij: doe je niets

2de rij schuif je 1 op naar links:

1 2 3 4 🡪

2 3 4 1

3de rij schuif je 2 op naar links

5 6 7 8 🡪

7 8 5 6

4de rij: schuif je 3 op naar links

Kolom shift

De waardes van 1 kolom ga je op een manier mengen (permutatie)

Deze beschouw je als een vector (4x1) en vervolgens doe je een matrixvermenigvuldiging 🡪 moet je niet kunnen/kennen

**Symmetric Encryption**

* Voordelen
  + Relatief eenvoudig
  + Sneller en efficiënter dan asymmetrische encryptie
  + Kan meer en grotere data aan
* Nadelen
  + Key management is moeilijker
    - Zender & ontvanger moeten op veilige manier key delen
    - Oplossing 🡪 key samen opbouwen via Diffie-hellman of ECC
  + Moeilijk om identiteit te bewijzen
    - Meerdere personen kunnen de key kennen

**Asymmetric encryption**

* Public key: voor encryptie
* Private key: voor decryptie en identificatie van bron
* Algoritmes (zijn bekend, maar keys zorgen voor veiligheid)
  + RSA

**RSA : Rivest-Shamir-Adleman**

* Product van 2 zeer grote priemgetallen (priemgetal tussen de 100 tot 200 cijfers lang)
  + Maakt gebruik van de moeilijke ontbindbaarheid
* Moeilijk grondtal berekenen

Afbeelding met tekst, apparaat, gekoppeld, meter

Automatisch gegenereerde beschrijving

Gebruikt in browsers voor veilige connecties

**Keys genereren**

Bob naar alice

Bob doet 4 stappen voor een public & private key te genereren

* Public key voor alice
* Private key voor bob zelf
  + Doe dit per bericht

1. Priemfactoren voor de keys
   1. Kies 2 grote priemgetallen ‘p’ & ‘q’
   2. N = p \* q
   3. N is makkelijk te berekenen
   4. Maar N is moeilijk in priemfactoren te ontbinden
2. Definieer Eulerindicator (totiënt) φ(N) = (p-1)\*(q-1)
3. Public key (bestaat uit 2 stukken N & e)
   1. N= p \* q
   2. E = gekozen exponent voor de encryptie
      1. Kies e zodat
         1. Grootste gemene deler van e en φ(N) is 1
         2. Ggd (e, φ(N) ) = 1
         3. Via uitgebreide algoritme van euclides
            1. Meerder oplossingen voor e mogelijk.
4. Private Key (bestaat uit 2 stukken N & d)
   1. N = p \* q
   2. Gebruik φ(N)= (p-1) \* (q-1) om private key te berekenen
      1. Dus een hacker wil p en q kennen.
   3. d: exponent voor decryptie
      1. Er geldt: e \* d = (veelvoud van φN)) + 1
      2. d = (k \* φ(N) + 1) / e
         1. d berekenbaar (voor natuurlijke getallen, niet voor kommagetallen) en geheim

**RSA encryptie**

M: message (boodschap),

Is grondtal hier (bits van tekst vormen zogezegd een getal

🡪Moeilijk te achterhalen

E: public key

N: product van 2 priemgetallen (p & q)

C: Ciphertext (geëncrypteerde boodschap)

Afbeelding met tekst, elektronica

Automatisch gegenereerde beschrijving

**RSA Decryptie**

* RSA decryptie (ontvanger gebruikt zijn eigen private key)
  + Ciphertext zijn bits als getal beschouwen.
  + Getal tot macht private key nemen, daarna modulo N.
  + Geeft oorspronkelijke message terug.
    - Reden: Euler’s Theorem

Afbeelding met tekst

Automatisch gegenereerde beschrijving

**Diffie-Hellman** key exchange

Op een veilige manier private key uitwisselen

* Publikie variablen uitwisselen en combineren met private key
* Om samen dezelfde key op te bouwen
  + SSL, TLS, SSH, IPsec

A : private key alice

G: generator

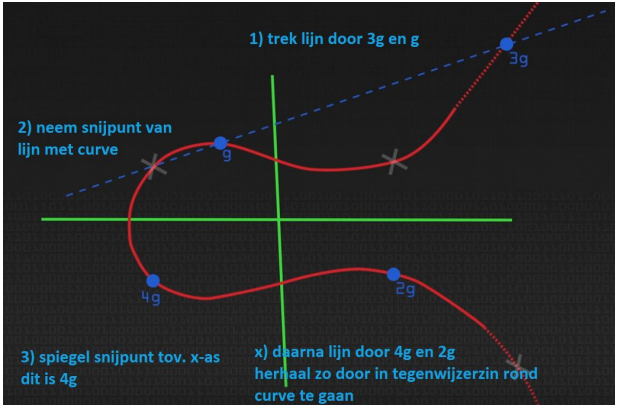
N: groot priemgetal 4000 bits

B: private key bob

A^g mod n b^g mod n

(G^b)^a mod n (g^a)^b mod n

**Elliptic Curve**

****

Veelvoud van g is ons private getal

Ag (a veelvoud van g) a :private alice

Bg (b veelvoud van g) b: private bob

Gedeelde key is abg

**WPA3**

Afbeelding met tafel

Automatisch gegenereerde beschrijving

Afbeelding met tafel

Automatisch gegenereerde beschrijving

WPA3 personal: user stelt zelf ww in, extra beveiliging, beschermd data verkeer zelfs nadat password gekraakt is

WPA3-enterprise : maakt gebruik van Protected management frames. 192bit mode

**Key management :** beheren van cryptografische sleutels

* + - Symmetrische sleutels
    - Asymmetrische sleutels
* Omvat het volgende
  + Genereren
  + Beschermen
  + Opslaan
  + Uitwisselen
  + Vervangen
  + Verwijderen

1. Zorg dat de key veilig is
2. Veilige verdeling ven de sleutels
3. Keys worden gebruikt in cryptografische operaties
   1. Opslaan voor latere decryptie
4. Sleutel niet meer bruikbaar 🡪 vervangen
5. Als sleutel gekraakt is
   1. Sleutel intrekken
   2. Sleutel vernietigen

**PKI :** public key infrastructure (authenticatie door certificaten)

* Client communiceert met server
* Client krijgt certificaat en valideert op authenticiteit
* Asymmetrische encryptie om verkeer naar en van server te versleutelen
* Digitaal certificaat bevat
  + Geldigheidsperiode
  + Uitgever
  + Certificaat houder
  + Public key

Wordt gebruikt in:

* TLS/SSL
* SSH
* VPN
* Bitcoin

Maakt gebruik van X.509 certificaten

**Cryptool2**

**Stego**

# H4 Protecting integrity

## Hashing

Waarom hashing, zorgen dat data onveranderd blijft 🡪 betrouwbaar

Hashing is onomkeerbaar!

**Salting**

Extra random string toevoegen aan plaintext

Tekst : hello

Salting :hello3ara

En op die string wordt de hash functie uitgevoerd

Elke user heeft eigen salt!

**Toepassingen**

* Password hashing
* Integriteit van files
* Message digest
* Cryptocurrency
* Digitale handtekening
* HMAC/KHMAC (key-hash message authentication code)

**Hashes kraken**

* Rainbow table attack
* Brute force
* Dictionary

Rainbow table

* Precomputed table van passwords en hun hashes
* Start vanuit hashed tekst en doe lookuo in de tabel
* Werkt puur offline en gedane werk kan hergebruikt worden
* Kan je nog uitbreiden via brute forcing

Onveilige algoritmes:

* MD5
* SHA-1,2,3

Veilige algoritmes

* Bcrypt
* Scrypt
* Argon2
* PBKDF2

# H5 (praktijk)

# H6 Protecting security domains

**Role-based Access control :** strategie gebaseerd op functies van werknemers, in grote organisaties met honderden gebruikers

**Mandatory Access control :** Strategie die beveiligings labels gebruikt : topsecret, geheim, vertrouwenlijk.. op veiligheidsclassificatie van het object en het label dat aan de gebruiker is bevestigd

**Rule-based Access Control :** Strategie gebaseerd op toegangscontrolelijsten (Access control lists)

**Discretionary Access control :** eigenaar bepaalt welke onderwerpen toegang hebben tot dat object en welke specifieke toegang ze hebben.

**5 nines : 99,999% uptime**

Afbeelding met tafel

Automatisch gegenereerde beschrijving

Afbeelding met tafel

Automatisch gegenereerde beschrijving

**Waar wordt 5 nine toegepast**

* Financiële sector
* Gezondheidszorg
* Publieke veiligheid
* Detailhandel
* Media-industrie

**Bedreigingen voor beschikbaarheid**

* Natuurrampen
* Menselijke fouten
* Hardware fouten
* Sabotage
* Softwareaanvallen
* Softwarefouten
* Diefstal
* Stoomstoring

**Redundancy**

N+1 redundancy (altijd een reserve onderdeel hebben)

* Raid
* Stp (spanning tree)
* Etherchannel
* Router redundancy
* Location redundancy

**Asset identification**

* Inventarisatie van de aanwezige hard & software

Elk component dat een security risico kan zijn

* Hardware systeem
* Besturingssysteem
* Hardware-netwerkapparaat
* Besturingssysteem van een netwerkapparaat
* Softwaretoepassing
* Alle firmware

**4 Stappen**

1. Bepaal categoriën
2. Bepaal verantwoordelijkheden
3. Bepaal de criteria voor de classificatie (top secret, secret, confidential, public trust, unclassified)
4. Implementer een classificatieschema

* Krietieke informatie -> zwaartste beveiliging

**Asset standardization :** inventaris van hard&software in organisatie

**Threat identification :**  identificatie van de bedreigingen begin met maken van CVE-identificatie

**CVE:** Common vulnerabilities and exposure

**Risico analyse**

Analyseren van gevaren voor de activa van de organisatie

4 Doelen

1. Identificeer activa en hun waarde
2. Identificeer kwetsbaarheden en bedreigingen
3. Kwantificeer de waarschijnlijkheid en de impact van de geïdentificeerde bedreigingen
4. Breng de impact van de bedreiging in evenwicht met de kosten van de tegenmaatregel

Kwantitatieve risicoanalyse

Een kwantitatieve analyse brengt cijfers toe aan het risicoanalyseproces

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Single loss exectancy activawaarde (vervangwaarde) \* blootstellingsfactor

* Is een subjectieve waarde uitgedrukt als een percentage dat een activum verliest als gevolg van een bepaalde dreiging (totaal verlies van activa = 1)
* Annualized rate of occurrence: hoefeel % kans is er dat er geduurende het jaar verlies zal optreden (>100% = verlies kan meer dan 1x per jaar optreden)
* Annual loss Expectancy: enige richtlijn over wat het zou moeten uitgeven om het actief te beschermen
* Fysieke items kan een waarde worden toegekend voor kwantitatieve analyse.

Afbeelding met tafel

Automatisch gegenereerde beschrijving

**Simplicity:** Vermijd complexe oplossingen die gebruikers niet kunnen begrijpen of om problemen op te lossen / beveiliginsoplossingen die van binnen uit eenvoudig zijn, maar vanbuiten complex.

**Obscurity:** geen informatie vrijgeven die cybercriminelene kunnen gebruiken om erachter te komen welke versie van het besturingssyteem een server gebruikt / bepaalde soorten informatie verbergen

**Limiting:** De mensen van de marketingafdeling geen toegang geven tot de loonadministratie / een werknemer verbieden gevoelige documenten uit het pand te verwijderen

**Diversity**: Verschillende versleutelingsalgoritmen of authenticatiesystemen gebruiken om gegevens in verschillende staten te beschermen.

**Incident Response (NIST)**

1. **Voorbereiding op noodgevallen**
2. **Herhaalbaar proces**
3. **Coördinatie**
4. **Leg gaten/ kwetsbaarheden bloot**
5. **Behoudt essentiële kennis**
6. **Oefening baart kunst**
7. **Documentatie en aansprakelijkheid**

**CSIRT : Computer security incident response team**

**4Fasen**

* Voorbereiding
* Detective & analyse
* Inperking, uitroeiing & herstel
* Follow up

**SANS :** privé organisatie voor onderzoek en training van security

SANS incident response plan

1. Voorbereiding
   1. Beleid
   2. Responseplan
   3. Team
2. Identificatie
   1. Monitoring
   2. Analyseer events
   3. Breng CSIRT leden op de hoogte
3. Insluiting
   1. Insluiting op korte termijn
   2. Systeemback-up nemen om te analyseren
4. Uitroeiing
   1. Reimaging
   2. Voorkomen van de hoofdzaak
   3. Toepassen best practices
   4. Scannen op malware
5. Herstel
   1. Bepaal tijd en datum voor herstel
   2. Testen en verifiëren
   3. Monitoring
6. Les geleerd
   1. Documentatie voltooien
   2. Stel een benchmark op om te vergelijken
   3. Bijeenkomst over geleerde lessen

## Endpoint security

**Hosthardening**

* Operating system security
  + Firewall
  + (guest) accounts
  + Updates
* Antimalware
  + Antivirus programma
  + Adware bescherming
  + Phishing bescherming
  + Spywarebescherming
* Patches zijn code-updates die fabrikanten bieden om te voorkomen dat een nieuw ontdekt virus of worm een succesvolle aanval uitvoert
* Patchmanagement
  + Het beslissen welke patches geschikt zijn voor bepaalde systemen
  + Ervoor zorgen dat de patches correct zijn geplaatst
  + Het testen van systemen na de patches
* Firewall & inbraakdetectiesysteemen (IDS)
  + Ongewenst verkeer tegenhouden & analyseren
* Beveiligde communicatie
  + VPN
  + HTTPS

**Protection of devices**

* Security kabels
* Sloten
* Logout timers
* Gps tracking
* Inventartis RFID tags
* Content control software

**Server hardening**

* Beveiligde toegang op afstand
  + Ssh
  + Scp
  + Rdp
* Administratieve maatregelen
  + Beveiliging poorten
  + Accounts
  + Group policies
* Schakel logboeken en waarschuwingen in

**Fysieke beveiliging**

* Voldoende stroom
* Reserve stroom
* HVAC, (heating ventilation & air conditioning)
* Hardware monitoring
* Beveiligd?
* Wat bij brand?

**Endpoint security**

* Endpoint security beveiligt apparaten van eindgebruikers
  + Mobile apparaten
  + Laptop’s /pc’s
  + Servers
* Deze apparaten kunnen worden beschoud als een toegangspunt tot het netwerk
  + 80% van attacks -> naar de endpoints

**Mogelijke gevaren:**

* Malware
  + Worms
  + Viruses
  + Tronjan horses
  + Logic bombs
  + Ransomware
  + …
* Attacks
  + DDOS
  + Smurf attack
  + Sniffing
  + Spoofing
  + Man-in-the-middle
  + Replay
  + Zero-day
  + Keylogger

**Network access control NAC**

Benadering van security dat het volgende probeert te combineren

* Endpoint security
  + Antivirus
  + Hostintrusion prevention
  + Vulnerability asessment
* Gebruikers- of systeemauthenticatie
* Netwerk security enforcement

**SIEM:** Security incident & event monitoring

Enkele mogelijkheden van siem

* In een vroeg stadium signalen van cybercrime detecteren
* Ondersteuning bieden in onderzoek naar verdachte incidenten, gebruik makend van log-informatie

**Honeypot:** Val voor een hacker

* Een hacker verdoet tijde aan onbelangrijke info
* Informatie verschaffen over de hacker.
* Gebruikt om spam te detecteren

Veel kwetsbaarheden in windows 🡪 10 categorien

1. Remote code execution
2. Buffer/heap overflow
3. DoS
4. Memory corruption
5. Privilege escalation
6. Information Disclosure
7. Security feature bypass
8. XSS
9. Directory traversal
10. XSRf : cross site request forgery

Kwetsbaarheden in adroid

* Laat toe apps te installeren van onbetrouwbare bronnen
* Fysieke diefstal
* Rooting
* Gebrek aan data encryptie
* Uitschakelen van authenticatie
* SQL injection
* Geen endpoint protection
* Update/patching niet vaak uitgevoerd

Kwetsbaarheden macos & IOS

* High sierra
* Macthans
* Jailbraiking
* iCloud geen block na x aantal wachtwoord attempts

**Waarom endpoint security??**

1. Mobiliteit
   1. Veel mensen werken van thuis
   2. Zijn niet beschermd door firewall van organisatie
2. Encryptie
   1. Bijna al de communicatie van en naar het internet is geëncrypteerd
   2. Decrypt bij het endpoint
3. Cybercrime blijft evolueren

Gebreken aan traditionele antivirus

* Malware gericht
* Vertraagde beveiliging
* Slechte systeemprestaties
* Relatief lage effectivtiet

Wat is next-gen endpoint sec?

* Maakt gebruik van AI & machine learning
* Doel: uitgebreide bescherming bieden
* Omvat realtime analyse van gebruikers

**EPP :** Endpoint protection platform

Iets meer traditionele anti-malware scanning

**EDR:** endpoint detection & response

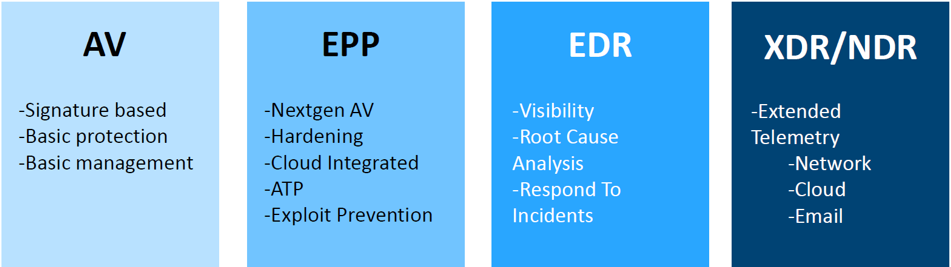
Geadvanceerder

Detecteren en onderzoeken van security incidenten

Herstellen van endpoint tot voor infectie

Ideale situatie = EPP + EDR

**XDR:** Extended detection & response



**Zero trust:**

* Ken elk device op uw netwerk
* Ken elke gebruiker dat toegang vraagt/ krijgt
* Weten hoe bedrijfsmiddelen op en buiten het netwerk kubnt beschermen

# H7 Attacks

**Attack techniques**

* **http flood** 
  + overbelasten van bandbreedte
* **syn flood**
* **port flooding**
  + udp
  + icmp
  + tcp