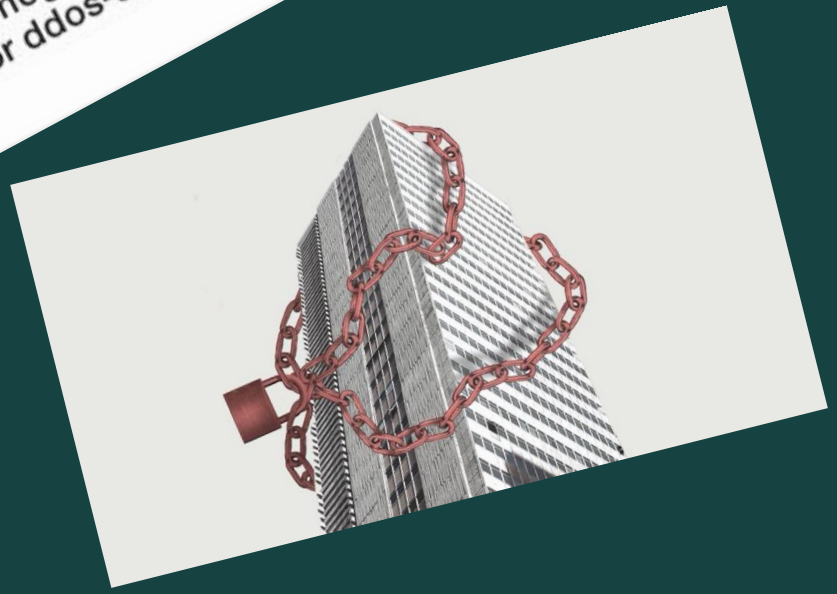
Cybersecurity

Nog hele week geen netwerk op TU Eindhoven, tentamens week uitgesteld

VIER VRAGEN

Waarom worden onderwijsinstellingen plots tegelijkertijd getroffen door cyberaanvallen?

Computernetwerk hogeschool Fontys urenlang onbereikbaar door ddos-aanval



Evelyn de Graaf **24-02-2025**

© De Graaf Project Management

Nuchter en praktisch

- Informatiebeveiliging en Privacy
- Projectmanagement
- Training en workshops
- Functionaris Gegevensbescherming
- Audits en consultancy

Evelyn de Graaf

Privacy en Kwaliteit in Een

Doel voor vandaag

- Behandelen basisprincipes van cybersecurity

- Leren hoe je **de organisatie** en jezelf kunt beschermen tegen de meest voorkomende digitale dreigingen.

© De Graaf Project Management

Agenda

Informatiebeveiliging

Privacy

Interactief

Cyberrisico's

Cybersecurity

Vragen

Filmpjes

© De Graaf Project Management

Feiten cybercriminaliteit

- **Kosten** van cybercriminaliteit voor 2025 wereldwijd geschat op $10,5 biljoen
- **Misverstand**: Ik ben toch niet interessant (als organisatie of als persoon)
- Een hacker denkt in **schakels**: gaatje zoeken om binnen te komen, dan dieper
- Zelden gericht: 9 van de 10 keer **TOEVAL**: wie klikt….
- Hoe herken ik een hacker?

© De Graaf Project Management

Cybersecurity

‘Cybersecurity’

- Cybersecurity is het **beschermen** van systemen, netwerken en gegevens tegen **digitale aanvallen**, **schade** of **ongeautoriseerde toegang**.

- In de digitale wereld van vandaag is cybersecurity **essentieel** voor zowel individuen als organisaties.

© De Graaf Project Management

Waarom cybersecurity regelen?

- Toenemende inzet **technologie**
- Onderwijs beschikt over steeds **meer data**
- Data **gedeeld** met meer samenwerkingspartners

-> **Meer risico op cyberaanvallen**

- Gegevens leerlingen / medewerkers op straat
- Systemen niet meer benaderbaar: continuïteit onderwijs

© De Graaf Project Management

Big Data miljardenhandel!

© De Graaf Project Management

Cyberrisico’s

‘Cyberrisico’

De waarschijnlijkheid dat een slechte gebeurtenis plaatsvindt in de informatiesystemen van de organisatie, wat leidt tot verlies van **beschikbaarheid, integriteit en vertrouwelijkheid** van informatie .

Schade uit een **inbreuk op de informatiesystemen** als gevolg van **cyberaanvallen** of **menselijke fouten**

© De Graaf Project Management

De 5 Grootste cyberrisico's

Welke?

© De Graaf Project Management

De 5 Grootste cyberrisico's

1. **Phishing en social engineering**
2. Ransomware en malware-aanvallen
3. Onveilige toegangspunten en zwakke wachtwoorden
4. Onveilige apparaten en BYOD-risico's
5. Gebrek aan bewustzijn en opleiding

© De Graaf Project Management

Vraag:

Hoeveel personen jaarlijks slachtoffer van cybercriminaliteit in NL?

Antwoorden

A. 500.000

B. 1,6 mjn

C. 7 mjn

© De Graaf Project Management

1. Phishing

CEO Fraude

Pathé voor 19 miljoen euro opgelicht door nepmails

10 nov. 2018 in BINNENLAND

© De Graaf Project Management

Wat is phishing?

Phishing is het **misdrijf** waarbij cybercriminelen proberen met valse berichten je **geld**, **persoonsgevoelige gegevens** of **beveiligingsinformatie** te stelen.

"Phishing is de eenvoudigste soort cyberaanval en tegelijk de meest gevaarlijke en effectieve".

© De Graaf Project Management

Enkele kengetallen

- Jaarlijks 2,1 mjn nieuwe phishingsites ontdekt
- 1 op de 6 Nederlanders slachtoffer
- 42% van de Nederlanders heeft ermee te maken gehad
- 20% van de werkende Nederlanders klikt op een phishingmail
- Jongeren (< 35 jaar) vaker slachtoffer (21,5%) dan ouderen (13,1%)

Steeds professioneler en persoonlijker, sneeuwbal effect!

© De Graaf Project Management

De risico’s van phishing

- Onderwijsinstellingen verwerken **zeer persoonsgevoelige gegevens**
- Deze gegevens zijn **beveiligd**, maar **afhankelijk van menselijk handelen**
- Geef je een van beiden af/op dan is er onder andere risico op:

- Datalekken
  - Diefstal, heling, shaming
  - Identiteitsfraude
  - Nog “betere” phishing
- Ransomware
  - Data niet meer toegankelijk
  - Imagoschade
  - Mogelijke financiële schade

© De Graaf Project Management

Vormen van phishing

Phishing kan via ieder type apparaat, zowel **ZAKELIJK** als **PRIVÉ**

- E-mails in allerlei vormen (94%)
- Sms-berichten
- WhatsApp-berichten
- Telefoongesprekken
  - Social engineering (manipulatietechniek om gegevens te krijgen)
  - Helpdeskfraude (”hallo, u spreekt met uw energiemaatschappij X of bank Y”)

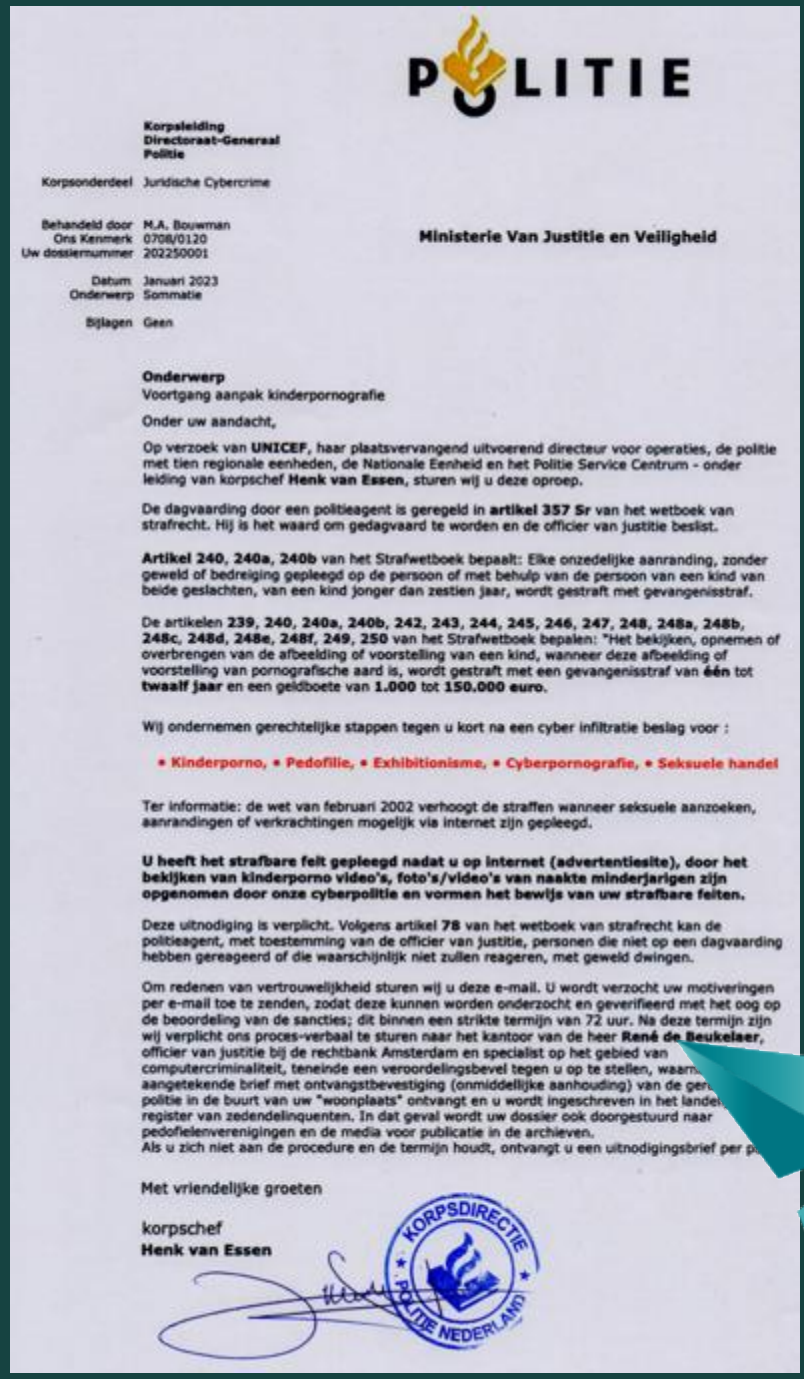
- **Combinatie** (meerdere vormen worden gecombineerd)

© De Graaf Project Management

Andere voorbeelden

Steeds echter…

- Je hebt een prijs, waardebon of cheque gewonnen of
- Je kan een creditcard met lage of geen rente krijgen of
- Je hebt teveel betaald voor iets en hebt recht op restitutie of
- Je bent vergeten je rekening te betalen of
- Je account is gedeactiveerd om beveiligingsredenen, “activatie vereist”



POLITIE

Korpsleiding
Directoraat-Generaal
Politie

Korpsonderdeel Juridische Cybercrime

Behandeld door M.A. Bouwman
Ons Kenmerk 0708/0120
Uw dossiernummer 202250001

Ministerie Van Justitie en Veiligheid

Datum Januari 2023
Onderwerp Sommatie

Bijlagen Geen

Onderwerp
Voortgang aanpak kinderpornografie

Onder uw aandacht,

Op verzoek van **UNICEF**, haar plaatsvervangend uitvoerend directeur voor operaties, de politie met tien regionale eenheden, de Nationale Eenheid en het Politie Service Centrum - onder leiding van korpschef **Henk van Essen**, sturen wij u deze oproep.

De dagvaarding door een politieagent is geregeld in **artikel 357 Sr** van het wetboek van strafrecht. Hij is het waard om gedagvaard te worden en de officier van justitie beslist.

Artikel 240, 240a, 240b van het Strafwetboek bepaalt: Elke onzedelijke aanranding, zonder geweld of bedreiging gepleegd op de persoon of met behulp van de persoon van een kind van beide geslachten, van een kind jonger dan zestien jaar, wordt gestraft met gevangenisstraf.

De artikelen **239, 240, 240a, 240b, 242, 243, 244, 245, 246, 247, 248, 248a, 248b, 248c, 248d, 248e, 248f, 249, 250** van het Strafwetboek bepalen: "Het bekijken, opnemen of overbrengen van de afbeelding of voorstelling van een kind, wanneer deze afbeelding of voorstelling van pornografische aard is, wordt gestraft met een gevangenisstraf van **één** tot **twaalf jaar** en een geldboete van **1.000** tot **150.000 euro.**

Wij ondernemen gerechtelijke stappen tegen u kort na een cyber infiltratie beslag voor :

• Kinderporno, • Pedofilie, • Exhibitionisme, • Cyberpornografie, • Seksuele handel

Ter informatie: de wet van februari 2002 verhoogt de straffen wanneer seksuele aanzoeken, aanrandingen of verkrachtingen mogelijk via internet zijn gepleegd.

U heeft het strafbare feit gepleegd nadat u op internet (advertentiesite), door het bekijken van kinderporno video's, foto's/video's van naakte minderjarigen zijn opgenomen door onze cyberpolitie en vormen het bewijs van uw strafbare feiten.

Deze uitnodiging is verplicht. Volgens artikel **78** van het wetboek van strafrecht kan de politieagent, met toestemming van de officier van justitie, personen die niet op een dagvaarding hebben gereageerd of die waarschijnlijk niet zullen reageren, met geweld dwingen.

Om redenen van vertrouwelijkheid sturen wij u deze e-mail. U wordt verzocht uw motiveringen per e-mail toe te zenden, zodat deze kunnen worden onderzocht en geverifieerd met het oog op de beoordeling van de sancties; dit binnen een strikte termijn van 72 uur. Na deze termijn zijn wij verplicht ons proces-verbaal te sturen naar het kantoor van de heer **René de Beukelaer,** officier van justitie bij de rechtbank Amsterdam en specialist op het gebied van computercriminaliteit, teneinde een veroordelingsbevel tegen u op te stellen, waarn aangetekende brief met ontvangstbevestiging (onmiddellijke aanhouding) van de ger politie in de buurt van uw "woonplaats" ontvangt en u wordt ingeschreven in het lande register van zedendelinquenten. In dat geval wordt uw dossier ook doorgestuurd naar pedofielenverenigingen en de media voor publicatie in de archieven.
Als u zich niet aan de procedure en de termijn houdt, ontvangt u een uitnodigingsbrief per p

Met vriendelijke groeten

korpschef
Henk van Essen

KORPSDIRECTIE POLITIE NEDERLAND

Herkennen van phishing

- Onverwacht contact
- Dwingend karakter: snelheid vereist
- Let op: steeds minder spelfouten
- Aanhef: op naam of algemeen
- Klik op afzender: bekend of dubieus e-mailadres
- Verzoeken om (persoonsgevoelige/beveiliging) gegevens
- Wees extra alert op meegestuurde bijlagen: Let op bij: *.exe, .zip, .docm of .xlsm*

  Nooit openen bestanden die eindigen op: *.js, .lnk, .wsf, .scr of .jar*

Vraag je af

- Is de communicatie relevant (heb je wel iets besteld..?)
- Kan ik de **communicatie valideren**? via een **andere route** (website/bellen)?

© De Graaf Project Management

Vraag:
De site mijn-ing.nl is voorzien van een groen slotje, de site bankierenrabobank.nl niet. Wat zegt dat?

Antwoorden

A. Alleen de site met groene slotje is veilig
B. Ze zijn beide onveilig
C. Bankierenrabobank.nl klinkt niet betrouwbaar en dan maakt het groene slotje niets uit

© De Graaf Project Management

Makkelijk herkenbaar

© De Graaf Project Management

Maar....

- Wat als jouw ICT afdeling in een mailtje vraagt om vanwege een probleem je wachtwoord te wijzigen met een linkje...?

© De Graaf Project Management

Identiteitsfraude

- PAS OP!

- Kopie ID gevraagd bij valse personeelsadvertentie voor thuiswerken
- Hotels/campings

- Huis op jouw naam met wietplantage

© De Graaf Project Management

Hoe te handelen

Better safe than sorry!

- **Wel doen**
  - Markeer externe/malafide e-mails/WhatsApp berichten als spam
  - Blokkeer malafide (mobiele) telefoonnummers
  - **Meld verdachte activiteit bij leidinggevende/collega's** (die ze zelf waarschijnlijk niet door hebben)
  - **Valideer via een andere route!**
- **Niet doen**
  - Op linkjes klikken
  - Ingaan op ongewenste telefoontjes
  - E-mails/berichten doorsturen
  - (persoonsgevoelige/beveiligings-) gegevens verstrekken
  - Software installeren (computer noch mobiel)

© De Graaf Project Management

Wat te doen als het toch is misgegaan

Het kan de besten overkomen… blijf kalm

- **Wel doen**
  - Neem direct contact op met ICT
  - **Koppel** een eventuele computer in kwestie **tijdelijk los van internet (Wi-Fi uit, kabel los)** totdat er contact met ICT geweest is (ook als je niet zeker bent of het is misgegaan)
  - Overleg noodzaak tot wijzigen wachtwoorden en bijwerken 2-staps verificatie en andere te ondernemen acties
- **Niet doen**
  - Blijven e-mailen of WhatsAppen/bellen met de malafide partij
  - Verwijder geen relevante gegevens voor onderzoek zoals e-mails, WhatsApp berichten, belhistorie, …
  - Zet een eventuele computer in kwestie **niet** uit

© De Graaf Project Management

De 5 Grootste cyberrisico’s

1. Phishing en social engineering
2. **Ransomware en malware-aanvallen**
3. Onveilige toegangspunten en zwakke wachtwoorden
4. Onveilige apparaten en BYOD-risico’s
5. Gebrek aan bewustzijn en opleiding

© De Graaf Project Management

2 Ransomware en malware

- Ransomware: gijzelsoftware op je computer waardoor je niet meer bij bestanden kunt totdat losgeld is betaald.

- Malware is kwaadaardige software die activiteiten uitvoert op je computer, zoals het stelen van gegevens of het verstoren van systeemfunctionaliteit.

© De Graaf Project Management

Wat doe je als organisatie?

- Betalen JA of Nee?
- Organisatie nadenken over: kan ik verder zonder betalen?
- Is er een draaiboek: weet je hoe te handelen?
- Let op: gemiddeld pas na 207 dagen ontdekt!

© De Graaf Project Management

Hoe voorkomen?

Ransomware

- Regelmatig back-ups draaien
- Update je software regelmatig om beveiligingslekken te dichten

Malware

- Gebruik een betrouwbare antivirussoftware.
- Wees voorzichtig met het downloaden van software van onbekende bronnen.

© De Graaf Project Management

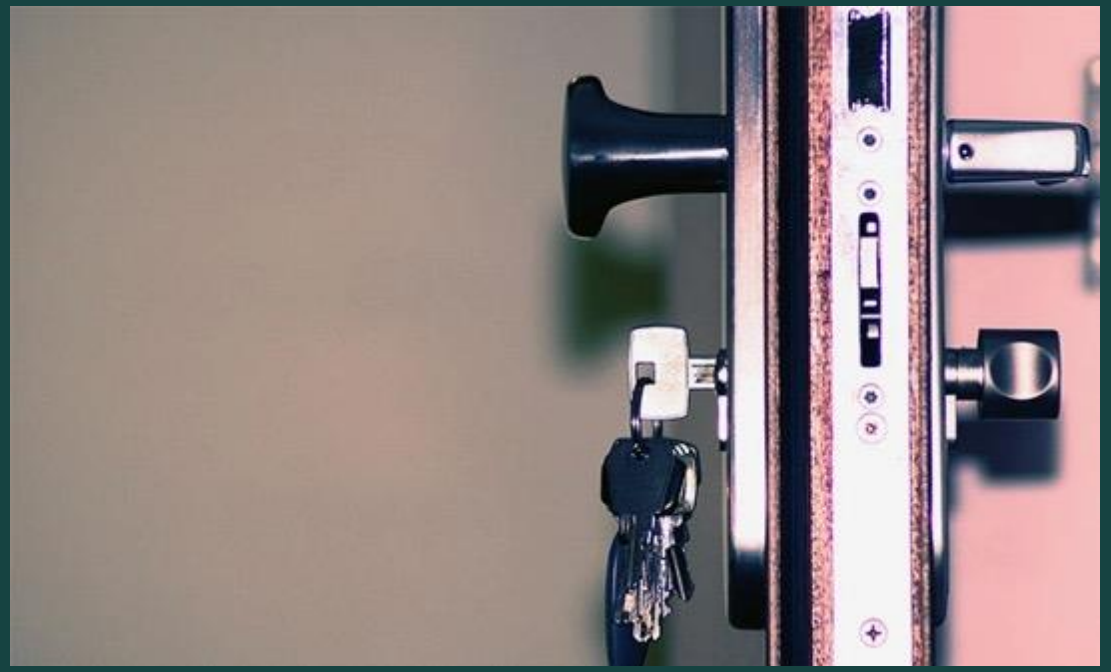
De 5 Grootste cyberrisico’s

1. Phishing en social engineering
2. Ransomware en malware-aanvallen
3. **Onveilige toegangspunten en zwakke wachtwoorden**
4. Onveilige apparaten en BYOD-risico’s
5. Gebrek aan bewustzijn en opleiding

© De Graaf Project Management

3. Toegangsrechten en wachtwoorden

- Authenticatie: verifiëren wie iemand is (wachtwoord, pincode etc.)
- Autorisatie: wie mag wat doen (na inlog)
- Alleen toegang wie dit nodig heeft!
- Wijziging functie:
  - Extra rechten toekennen?
  - Andere rechten afnemen?



© De Graaf Project Management

Wachtwoorden

© De Graaf Project Management

Gebruik sterke wachtwoorden

- Makkelijk te raden
- 6 tekens en letters:
  in 5 seconden
- Wachtzin: jaren!

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

HIVE SYSTEMS

-Data sourced from HowSecureismyPassword.net

Vraag:
Een programma op je computer vraagt om een update, wat doe je?

Antwoorden

A. Ik installeer de update
B. Ik vertrouw dat soort pop-ups niet dus ik open ze niet en installeer niets
C. Als ik alles opnieuw moet opstarten doe ik niets. Als ik tevreden ben met de oude versie hoef ik geen verbeteringen

© De Graaf Project Management

Hou het veilig....

- Gebruik voor elke website een ander wachtwoord (wachtzin met ...)
- Wachtwoordmanager: veiliginternetten.nl
- Updates direct installeren (vanuit pc, niet klikken op link in mail!)
- Gebruik geen openbare wifi netwerken voor gevoelige activiteiten (internetbankieren)
- Stel 2FA in
- Hou je wachtwoord ALTIJD voor jezelf!!!

© De Graaf Project Management

De 5 Grootste cyberrisico’s

1. Phishing en social engineering
2. Ransomware en malware-aanvallen
3. Onveilige toegangspunten en zwakke wachtwoorden
4. **Onveilige apparaten en BYOD-risico’s**
5. Gebrek aan bewustzijn en opleiding

© De Graaf Project Management

Defense in depth

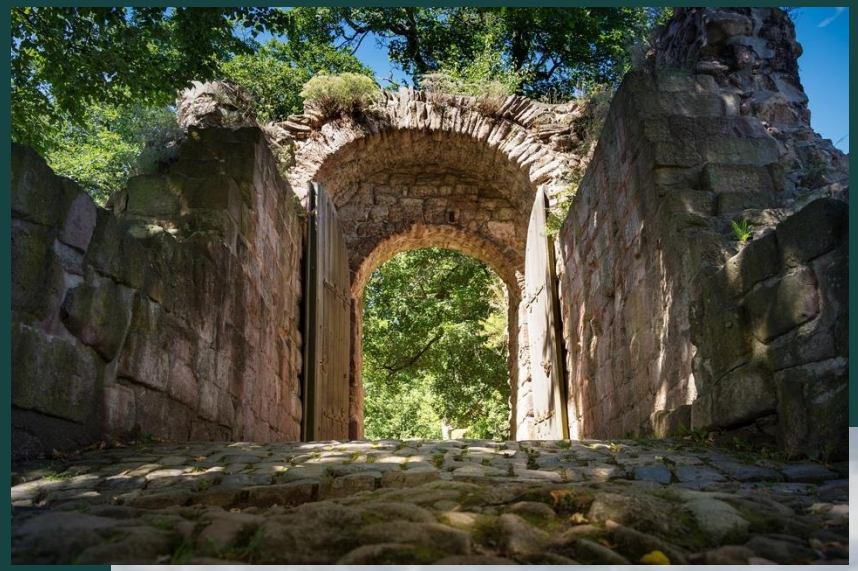
Beveiligingsstrategie waarbij **meerdere verdedigingslagen** rondom het te beveiligen object worden aangebracht.

Het falen van de ene laag wordt opgevangen door de volgende laag.

© De Graaf Project Management

Defense in depth

vroeger



© De Graaf Project Management

Defense in depth

tegenwoordig

Onderwijs digitaal!

© De Graaf Project Management

Defense in depth

Inlog 2FA

Inlog sterk wachtwoord

Veilige verbinding

Server: firewall

Database: encryptie

© De Graaf Project Management

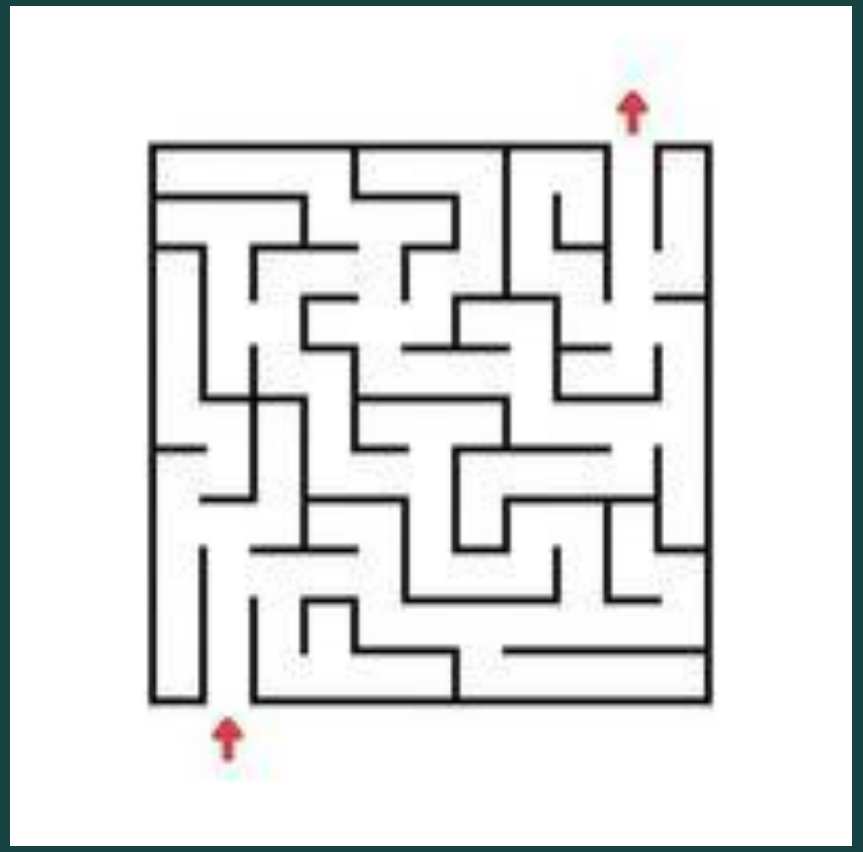
BYOD-risico's

- Maak beleid op Bring Your Own Device (BYOD)
- Wat zijn de afspraken, wat mag wel en niet
- Stel eisen aan de beveiliging

© De Graaf Project Management

KISS

- Keep It Simple and Stupid
  - Te moeilijk, gaan mensen eromheen werken, zoeken de makkelijke weg
    - 1 wachtwoord voor alles
    - Wachtwoord op briefje



© De Graaf Project Management

De 5 Grootste cyberrisico’s

1. Phishing en social engineering
2. Ransomware en malware-aanvallen
3. Onveilige toegangspunten en zwakke wachtwoorden
4. Onveilige apparaten en BYOD-risico’s
5. **Gebrek aan bewustzijn en opleiding**

© De Graaf Project Management

5. Gebrek aan bewustzijn en opleiding

- Cyberrisico's niet direct zichtbaar, niet aan gewend, lastig om gedrag aan te passen

- Let op: lets meer bewustzijn zorgt voor sneller handelen:
  → in 2 uur in de lucht in plaats van in 2 maanden

- Gedragscode veilig internetgebruik
- Meldprocedure voor verdachte activiteiten en datalekken
- Medewerkers regelmatig trainen
- E-learning
- Phishing simulaties
- Nieuwsbrieven/Presentaties

.

© De Graaf Project Management

Gratis apps

- Let op: een gratis app bestaat niet
- 10.000 nieuwe kwaadaardige apps per dag!
  - Telefoon leeg getrokken, contacten, internet bankieren…
  - Aandacht voor kinderen: deze zitten de hele dag op telefoon!
    - lesprogramma

© De Graaf Project Management

Wat kan de organisatie doen

- IBP-beleid, reglementen en protocollen opstellen
- IBP kennis, bewustwording en borging
- ICT beveiliging/gebruiksgemak afwegen

- **Sectorale ontwikkelingen volgen**
  - Normenkader IBP
  - Funderend Onderwijs Referentie Architectuur (FORA: modellen, processen)

© De Graaf Project Management

Bedankt voor jullie aandacht!

© De Graaf Project Management

Gebruik van materiaal privacybewustwordingstraining

Het geheel of gedeeltelijk gebruik van dit materiaal is uitsluitend toegestaan door de rechtmatige afnemer van deze privacybewustwordingstraining. De inhoud van dit materiaal is beschermd door copyright © waardoor het niet is toegestaan om dit materiaal te vermenigvuldigen en/of openbaar te maken door middel van druk, fotokopie, microfilm of op enigerlei wijze zonder nadrukkelijke schriftelijke toestemming van De Graaf Project Management.

Dit materiaal is zorgvuldig en naar beste weten samengesteld. Regel- en wetgeving zijn voortdurend aan verandering onderhevig waardoor De Graaf Project Management niet kan instaan voor de juistheid of volledigheid hiervan. De Graaf Project Management aanvaardt geen enkele aansprakelijkheid voor schade, van welke aard dan ook, als gevolg van handelingen en/of beslissingen die op basis van dit document zijn genomen.

© De Graaf Project Management