Cybersecurity toegepast op uw kantoor

Waarom de brancheorganisaties cybersecurity nu op #1 zetten

SRA

Waarom cybersecurity nu op #1 zetten

Cyber security is voor veel accountants een abstract en ongrijpbare onderwerp. Het heeft het imago geen directe bijdrage te leveren aan de kwaliteit van de dienstverlening van het kantoor en wordt daardoor vaak beschouwd als een bijzaak, een hinderlijke drempel of een separaat traject wat wordt overgelaten aan de (externe) IT-manager.

De digitale weerbaarheid van accountantskantoren staat onder druk door een toenemende complexiteit en connectiviteit in het IT-landschap, nieuwe ontwikkelingen en door te weinig aandacht voor digitale veiligheid bij nieuwe, innovatieve projecten. Om de digitale weerbaarheid van het kantoor te vergroten, is stilstaan is geen optie.

Het IT-landschap

SRA

Verschillende omgevingen

SRA

On-Premises

Ongoing Costs

- Apply patches, upgrades
- Downtime
- Performance tuning
- Rewrite customizations
- Rewrite integrations
- Upgrade dependent applications
- Ongoing burden on IT (hardware)
- Maintain/upgrade network
- Maintain/upgrade security
- Maintain/upgrade database

Cloud Computing

Ongoing Costs

- Subscription fees
- Training
- Configuration
- System Administration

"Tech support says the problem is located somewhere between the keyboard and my chair."

Source: http://www.glasbergen.com/

Vijf belangrijke IT-trends

- Cyber security
- Cloud / …-as-a-service
- Data & Business Intelligence
- Digitale transformatie
- Thuiswerken

Waarom cybersecurity nu op #1 zetten?

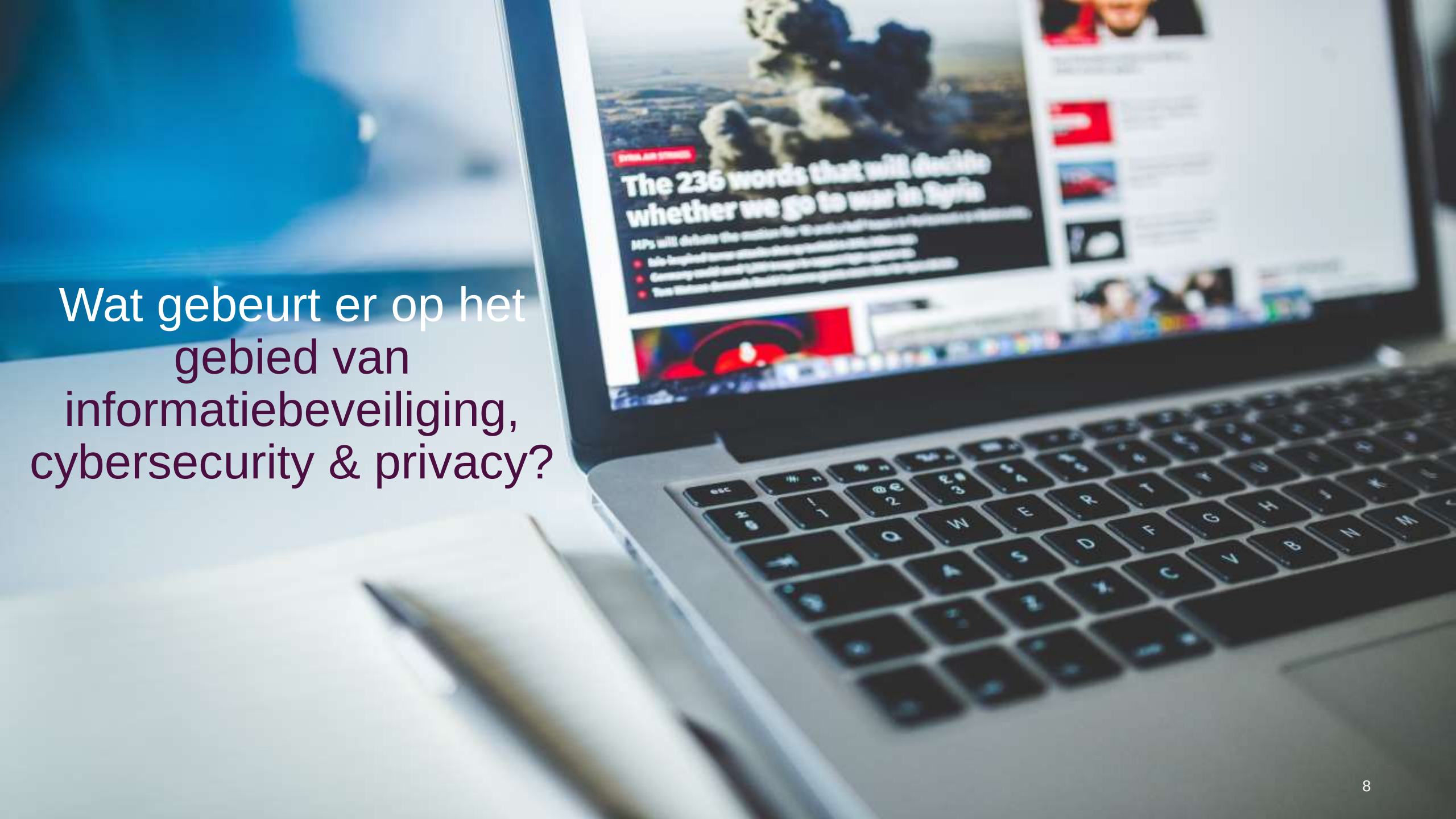
Grootste uitdagingen op IT-gebied

1. **Informatiebeveiliging & Cybersecurity**
2. Beheersing van kosten
3. Migratie naar de cloud
4. Grip op data
5. Kennis van medewerkers
6. Innovatief vermogen van de organisatie
7. **AVG / Privacy**

Investeren in de komende twee jaar

1. Data-analyse / Process Mining
2. **Informatiebeveiliging, Cybersecurity & Privacy**
3. Vervanging van bestaande software
4. Elektronisch ondertekenen
5. Cloud / outsourcing
6. Workflow
7. Dashboards ontwikkelen voor klanten

Bron: SRA IT Benchmark 2021



Wat gebeurt er op het gebied van informatiebeveiliging, cybersecurity & privacy?

Cybersecuritybeeld Nederland

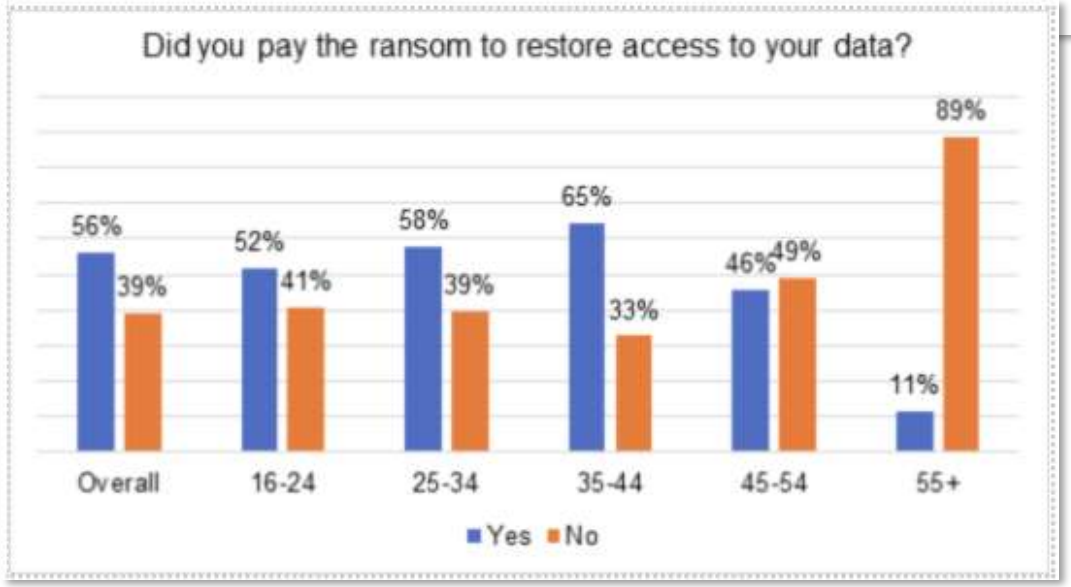
- Digitale dreiging is permanent; digitale risico's zijn onverminderd groot en niet fundamenteel veranderd
  - Sabotage en spionage (door statelijke actoren)
  - Cyberaanvallen door cybercriminelen
  - Afpersing door ransomware
- Digitale weerbaarheid is nog niet overal op orde
  - Basismaatregelen onvoldoende op orde
  - Complexiteit van IT (in de keten) neemt toe
  - Gebruikers gedragen zich 'onveilig'
- Digitale risico's staan niet los van ander risico's
- Vergroting van de weerbaarheid is het belangrijkste instrument
  - Technische, procedurele of organisatorische maatregelen
  - Wetgeving (o.a. AVG)

Bron: https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

Onderzoek ransomware consumenten

Momenteel beweren ongeveer vier op de tien (39%) van de ondervraagden dat ze de afgelopen 12 maanden op de hoogte waren van ransomware. Het is belangrijk dat dit aantal stijgt naarmate werken op afstand productiever wordt. Om consumenten beter te helpen zichzelf te beschermen terwijl ze meer te weten komen over deze vorm van cyberaanval, is het essentieel dat ze begrijpen waar ze op moeten letten en wat ze moeten doen als ze ransomware tegenkomen.

Kaspersky Consumer IT Security Risks Report 2021



Bron: media.kasperskydaily.com

- Betaal geen losgeld
- Schakel een security expert in
- Klik niet op onbekende, onveilige links
- Open geen onbekende bijlage
- Bezoek geen onbekende website
- Gebruik geen onbekende USB-sticks
- Maak regelmatig een back-up
- Installeer beschermingssoftware

YOUR COMPUTER HAS BEEN LOCKED!

Opzet, Bestaan & Werking!

COMPUTABLE

Artikelen

Achtergrond | Security

Juist op die uiterst belangrijke toegang was de twee-factorauthenticatie uitgezet

Schade hack bij Hof van Twente loopt op

Negen op de tien gemeentes vrezen ook slachtoffer te worden

6 april 2021 12:10 | Alfred Monterie

Topic Security

De gemeente Hof van Twente gaat minimaal drie à vier miljoen euro schade lijden als gevolg van de aanval met ransomware waardoor massaal basisdata verloren gingen. Per bewoner is dat zeker honderd euro verlies. De uiteindelijke strop kan nog behoorlijk oplopen.

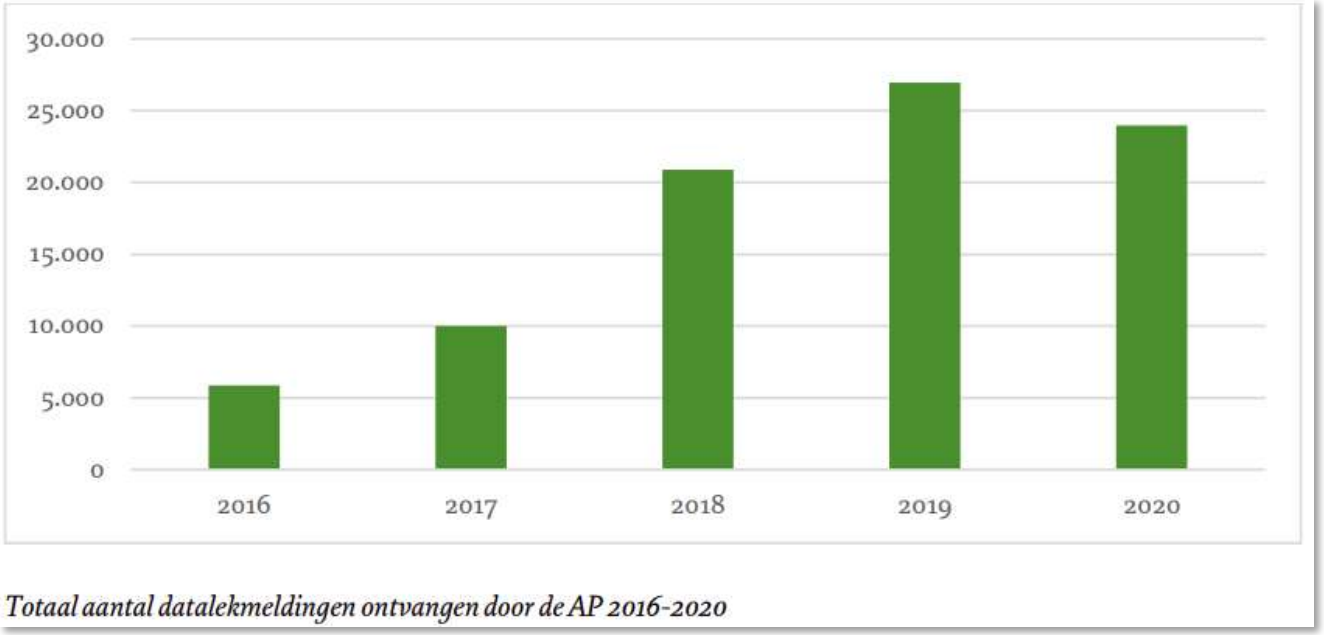
Bewustzijn

Op papier leek alles behoorlijk goed te kloppen.

you should enter the digits resulting code, which is
on the back of your in the payment form and press
OK (if you have several codes, enter them one after the other and press
OK).

Het wachtwoord (Welkom2020) was te zwak.

Datalekken - feiten & cijfers



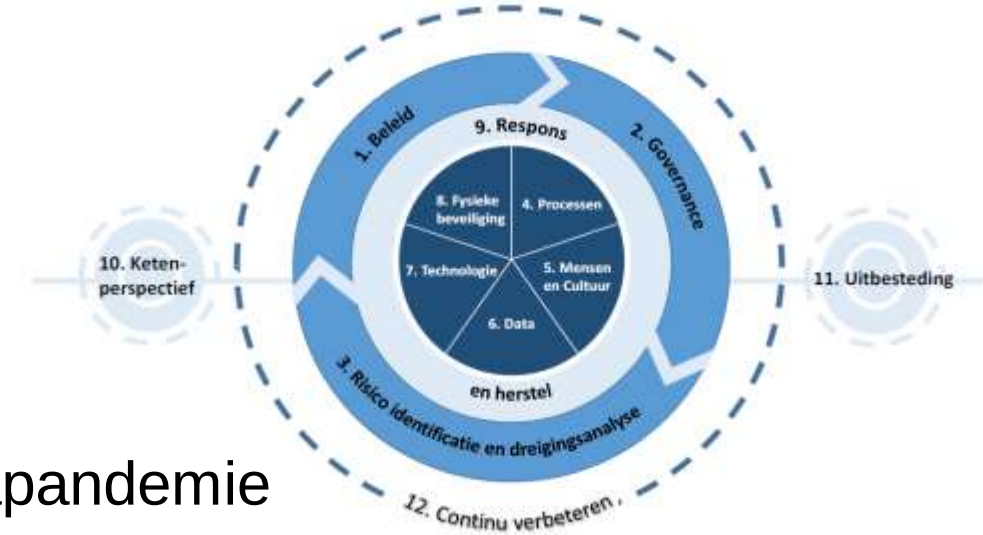
Totaal aantal datalekmeldingen ontvangen door de AP 2016-2020

- Nederland in Top-3
- Toename door:
  - Hacking
  - Malware
  - Phishing
- Thema: MFA

Bron: Autoriteit Persoonsgegevens

Trends

- AFM “Principes voor Informatiebeveiliging”
- Uitvraag WTA-vergunninghouders
- NOREA IT-auditverklaring
- ISO 27001 certificering verplicht
  (bijvoorbeeld ARBO diensten)
- Enorme toename cybercrime tijdens de coronapandemie
- Veranderingen in wet- en regelgeving



Richtsnoeren AVG voor accountants, belastingadviseurs en salarisprofessionals

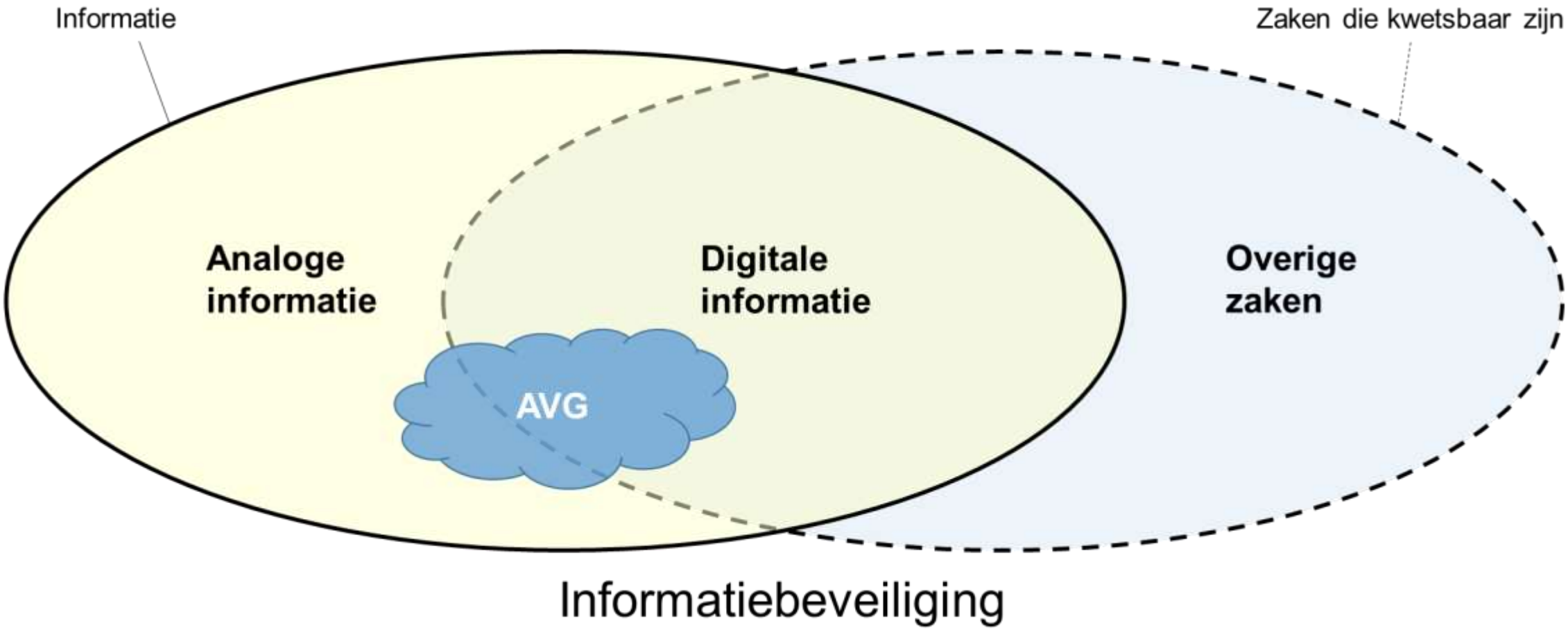
met betrekking tot de status als ‘verwerkingsverantwoordelijke’ of als ‘verwerker’ als bedoeld in de (Uitvoeringswet) Algemene verordening gegevensbescherming bij het verlenen van diensten aan klanten.

https://www.nba.nl/nieuws-en-agenda/nieuwsarchief/2019/oktober/nba-nirpa-nob-novak-en-rb-publiceren-richtsnoeren-avg/

SRA


Informatiebeveiliging
Cybersecurity
Cobit
Risicomanagement
ISAE3402
ITIL
FG
Pentest
Audit
Security
ISO27001
AVG
Compliance
Privacy
Awareness

Kader - Informatiebeveiliging, Cyber Security & AVG



Informatiebeveiliging, Cyber Security & AVG

- Informatiebeveiliging kampt met imago
  - Meer dan ICT → Mens, Organisatie en Techniek
  - Beveiliging draagt onvoldoende bij aan de dienstverlening
- Inzicht in risico's niet integraal
  - Informatie over incidenten en maatregelen verspreid in de organisatie
  - Afhankelijkheid van externe partijen
  - Bekende risico's krijgen overmatig veel aandacht (AVG)
- Aanvallen succesvol door ontbreken basismaatregelen en bewustwording
- Onvoldoende risicomanagement; waan van de dag regeert
- Toenemende complexiteit en connectiviteit in het ICT-landschap
  - Schaduw-IT
  - Noodzaak voor multidisciplinaire aanpak en eigenaarschap

Beveiliging in vijf stappen

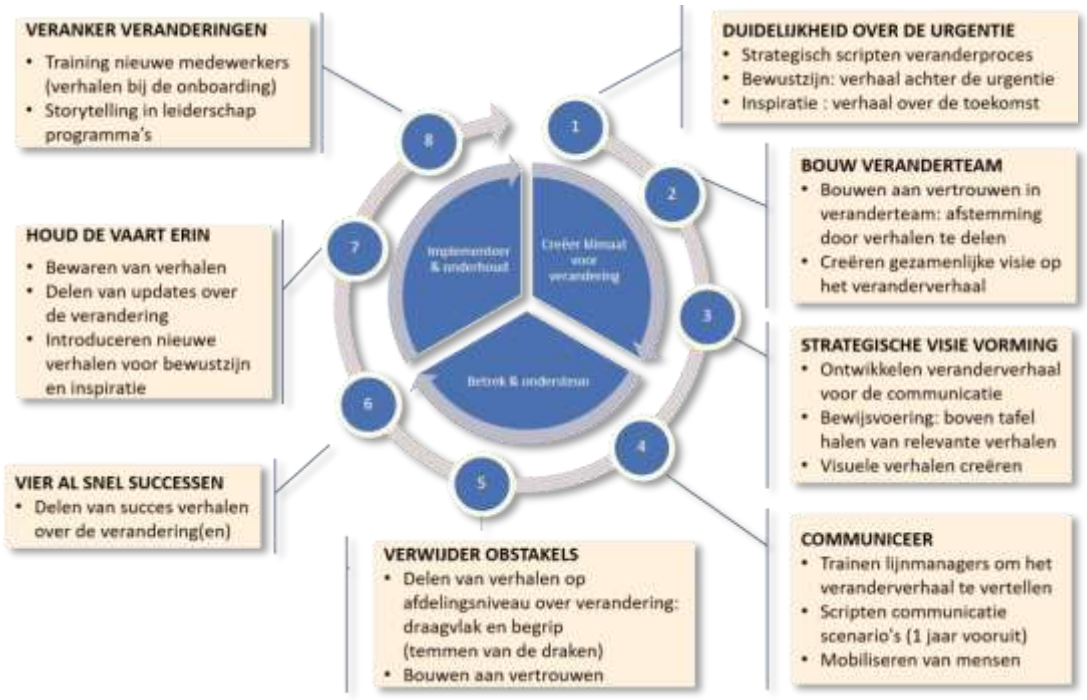
1. Stel het (beleids)kader vast; verdeel verantwoordelijkheden, bevoegdheden en taken
2. Breng risico's in kaart, bepaal het volwassenheidsniveau
3. Bepaal de gewenste maatregelen voor mens, techniek en organisatie
4. Omgaan met uitbesteden van IT-diensten
5. Beheersen en verbeteren

Selecteer de juiste hulpmiddelen en tools om in zetten


GOVERNANCE

Informatie(beveiligings)beleid

- Directieverantwoordelijkheid
- Uitgangspunten en risicobereidheid vaststellen (in lijn met organisatiebeleid en –doelstellingen)
- Eisen ten aanzien van:
  - Beschikbaarheid
  - Integriteit
  - Vertrouwelijkheid
- Periodieke evaluatie
- Beveiligingsbewustzijn bevorderen



Beleid en doelstellingen

- Bepaal het gewenste niveau
  - Management → Continue betrokkenheid / draagvlak
  - Cultuurverandering → Informatieveiligheid moet tweede natuur worden

- Inventariseer hoe ver u van het doel bent verwijderd
  - Meldingen als indicator
  - Proef op de som nemen (nulmeting)

- Bepaal hoe u de ‘awareness gap’ gaat overbruggen.
  - Basisgebieden: kennis, houding en gedrag
  - Gebruik momentum
  - Let regels uit

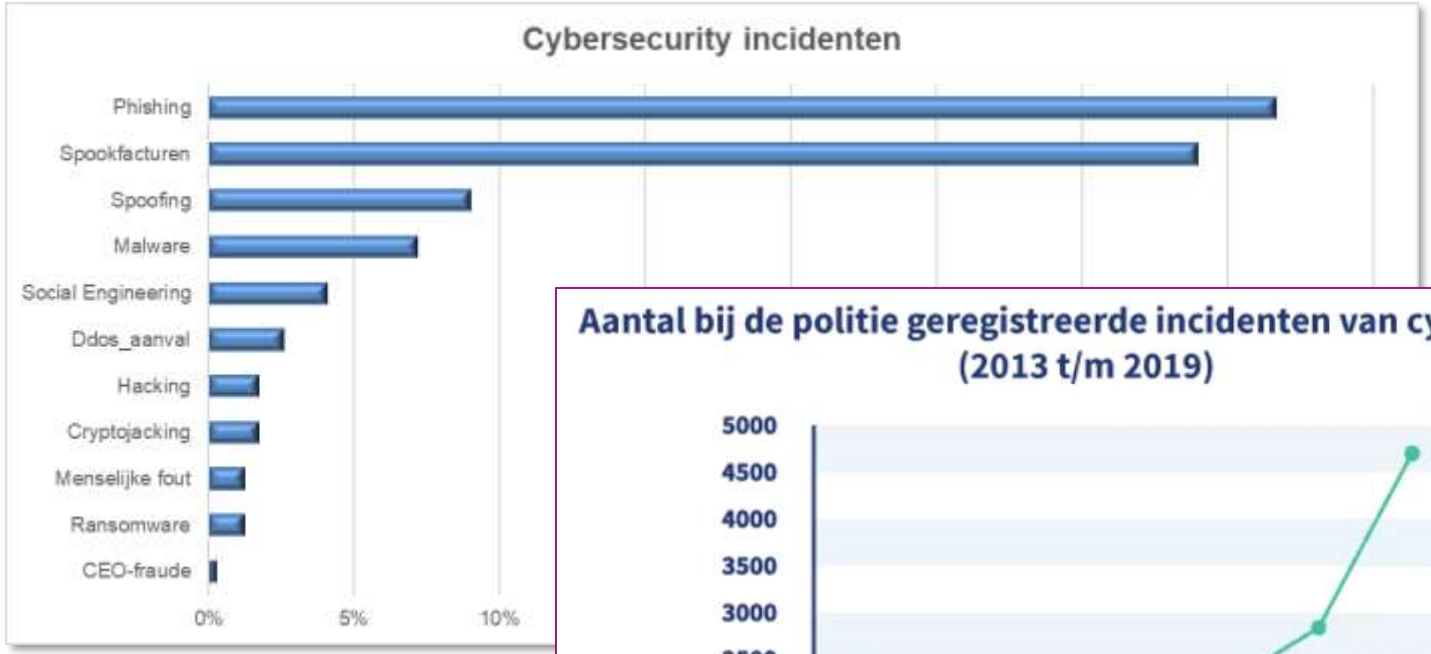
- Plan activiteiten
  - Communiceer (per doelgroep)
  - Varieer (vb: awareness games, informele bijeenkomsten)
  - Beloon positief gedrag; security is niet vrijblijvend.

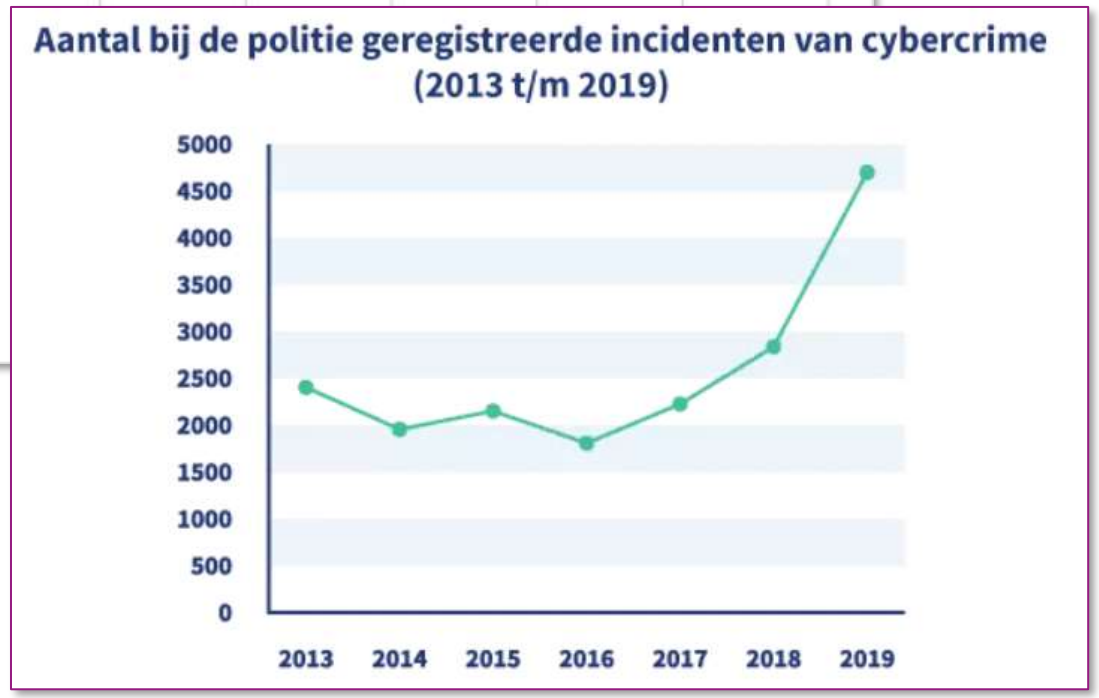
- Evalueer, stel bij en herhaal.


Risk Assessment
Severity
obability
Disaster
High
Medium
Minimal
Regularly
Critical
Critical
High
Medium
robable
Critical
High
Medium
Medium
asional
Critical
High
Low
rely
High
Medium
Medium
bable

Veelvoorkomende dreigingen op een rij

- Phishing
- Ransomware
- Netwerkaanvallen
- CEO-fraude
- Spoofing
- Cryptojacking
- DDoS-aanvallen





Voorbeeld

Hoe ontvang ik mijn vernieuwde betaalpas?

Door direct zelf uw aanvraag te bevestigen, voorkomt u extra kosten en ongewenste blokkade van uw huidige betaalproduct. Bevestig direct de aanvraag van uw vernieuwde betaalpas door de QR-code hiernaast te scannen met de camera van uw smartphone. Vervolgens ontvangt u binnen 5 werkdagen uw vernieuwde betaalpas kosteloos thuis.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,
ABN Amro Bank N.V.

Geachte relatie,

Wij nemen contact met u op om u te laten weten dat wij met ingang van 1 januari 2020 enkele wijzigingen hebben doorgevoerd in ons privacybeleid. Deze wijzigingen weerspiegelen de striktere privacy en wetgeving eisen van de Algemene Gegevensbescherming (bekend als de AVG) die banken in Nederland moeten voldoen.

Als bank mogen wij onze producten en dienstverlening alleen openstellen voor klanten van wie wij de identiteit hebben vastgesteld. Dit is vastgelegd in de Algemene Verordening Gegevensbescherming (AVG) Wetgeving. Deze wet helpt ons om onze klanten te beschermen en hun veiligheid te waarborgen.

Uit ons klantenbestand is naar voren gekomen dat uw contactgegevens niet compleet zijn. Het is belangrijk dat wij uw meest actuele contactgegevens in bezit hebben, zodat wij u kunnen bereiken indien het nodig is.

Wij verzoeken u om de juiste contactgegevens aan ons door te geven. Doet u dit niet, dan kunt uw rekening geblokkeerd worden: u kunt dan niet meer betalen of geld van opnemen. Klik hier om uw contactgegevens bij te werken. Is uw rekening al geblokkeerd? Dan is het van noodzaak om uw te identificeren, zodat u weer volledig gebruik kunt maken van uw rekening.

Heeft u nog vragen?
Meer informatie vindt u op rabobank.nl/privacy. Staat het antwoord er niet bij? Neem dan contact met ons op. Wij helpen u graag!

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groet,
Rabobank

SRA

Dit bericht lijkt gevaarlijk

Het bericht bevat een verdachte link die is gebruikt om persoonlijke informatie van mensen te stelen. Klik niet op links en beantwoord het bericht niet met persoonlijke informatie.

Linda van Dijk | SRA

Van: Linda Van Dijk <lvandijk@sra.lu>
Verzonden: donderdag 5 november 2020 15:56
Aan: Tony van Oorschot | SRA <tvanoorschot@sra.nl>
Onderwerp: Sollicitatiepagina probleem

Hoi Tony,

Lukt het voor jou om deze pagina te laden? Voor mij lukt het, maar voor een potentiële sollicitant dan weer niet..

Met vriendelijke groet,

Linda Van Dijk
HR Adviseur

Rijnzathe 14
3454 PV Utrecht
www.sra.nl

T 030 656 60 60

E lvandijk@sra.nl

Let op:

- Afzender
- Aanhef
- Open geen onbekende bijlage(n)
- Klik niet op onbekende, onveilige links
- Bezoek geen onbekende website
- Taalgebruik en –fouten
- Urgentie
- Vraag naar persoonlijke gegevens

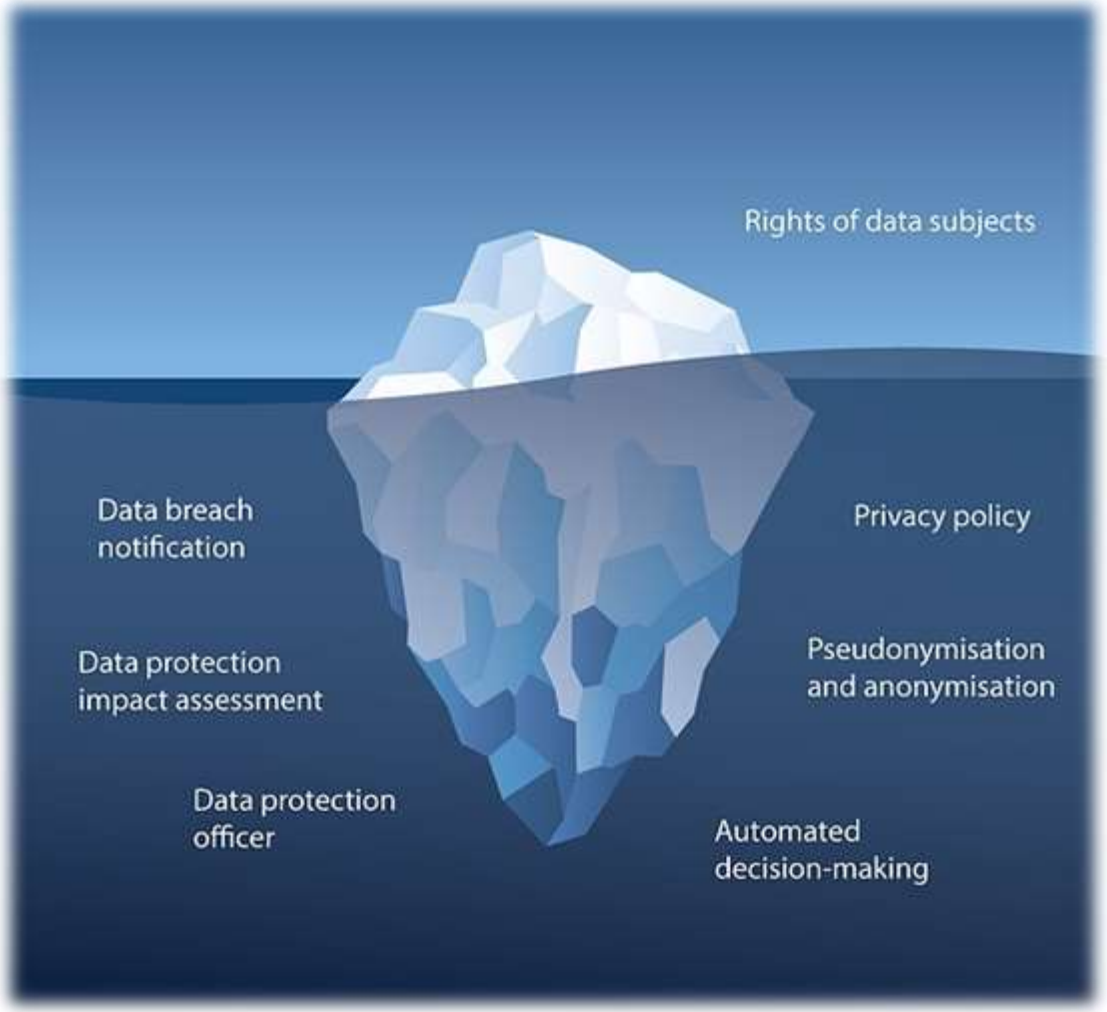
Heeft u al eens te maken gehad met een datalek?

De juiste volgorde

- Risico-analyse
  - Mitigeren
  - Delen (‘cyberriskverzekering’)
  - Vermijden (stoppen)
  - Accepteren (inclusief onbekende risico’s)

- Maatregelen:
  - Controls op de belangrijkste risico’s
  - Dataclassificatie
  - Disaster recovery plan

- Tools



Risico-analyse

- Impact analyse
  - Hoe belangrijk is deze informatie / dit systeem voor de organisatie?
  - Wat is de impact voor de organisatie bij een probleem?

Mogelijke risico's

Voor de organisatie

- Negatieve publiciteit en imagoschade.
- Dwangmaatregelen en/of boetes opgelegd door de toezichthouder.
- Schadeclaims door betrokkenen.
- Hogere kosten bij het achteraf nemen van privacy maatregelen.
- Slechte datakwaliteit leidt tot slechtere performance van de business.
- Datalekken leiden tot wantrouwen.
- Ziekte van medewerkers
- Rem op innovatief vermogen
- Personeelstekort

Bij uitbesteding van IT

- Verlies van kennis en skills van medewerkers
- Afname flexibiliteit
- Verlies van contact met eindgebruikers
- Bepalen van de toegevoegde waarde
- Interpretatieverschillen over contract / SLA
- Kosten voor issues buiten contract / SLA
- Afhankelijkheid ('vendor lock-in')
- Verkeerde verwachtingen over geleverde (niveau) van diensten
- Uit elkaar groeien van partijen; botsende visies en culturen

Risico’s waar we vaak niet aan denken

- Bestanden belanden in de prullenbak
- Chaos op de (thuis)werkplek
- Delen van mailboxen en wachtwoorden
- Een eenvoudig centraal wachtwoord voor iedereen voor alles
- Gastvrijheid op het kantoor “Kom binnen!”
- Gebruik van privé USB-sticks, externe harde schijven, enz
- Gebruik van persoonlijke e-mailaccounts voor het werk
- Incidenten en datalekken verzwijgen
- Ontbreken van voorwaarden in contracten over data en privacy
- Onduidelijkheid over bewaartermijnen
- Te veel informatie verstrekken (via de telefoon)

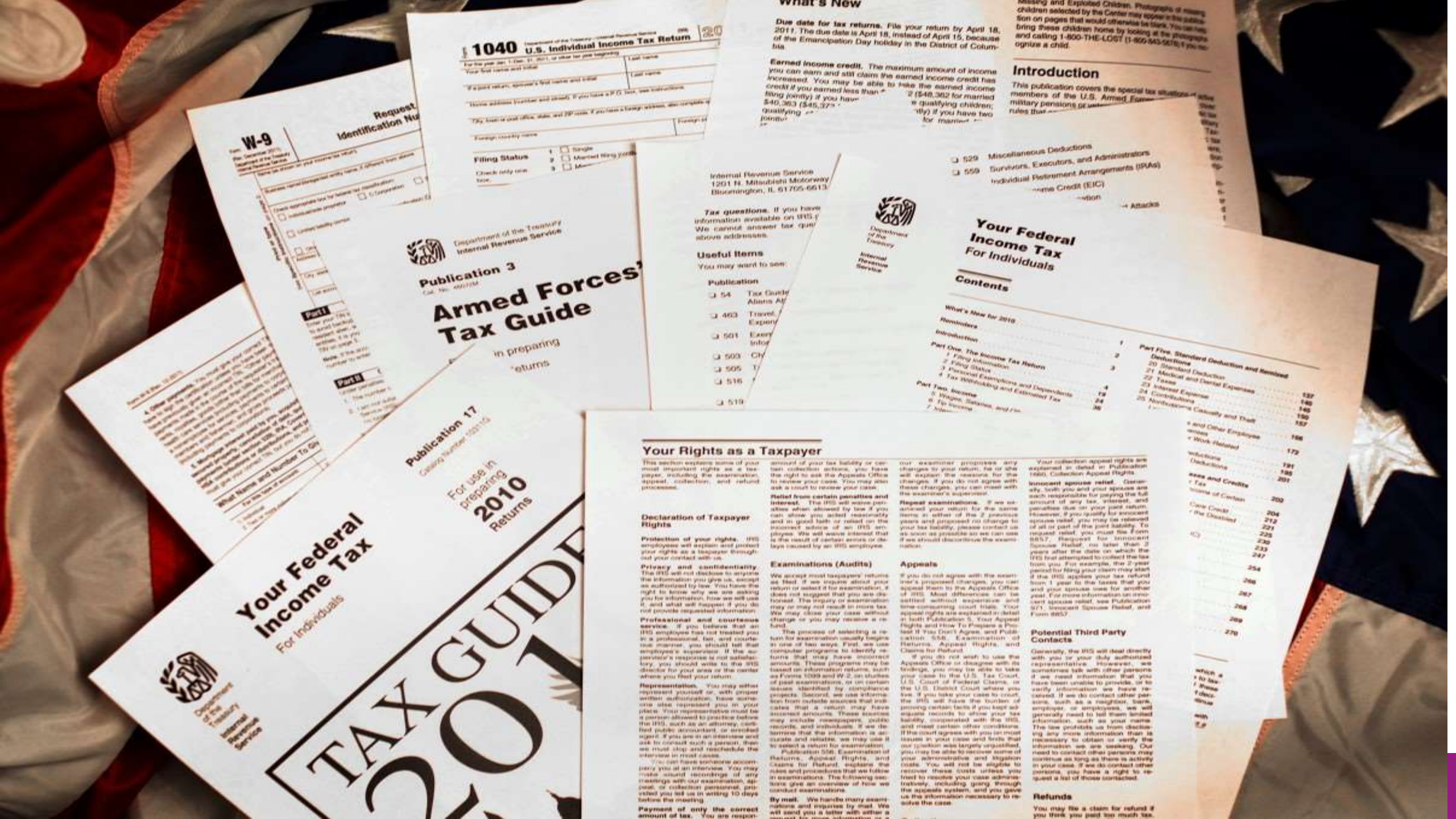
Risico-analyse

SRA

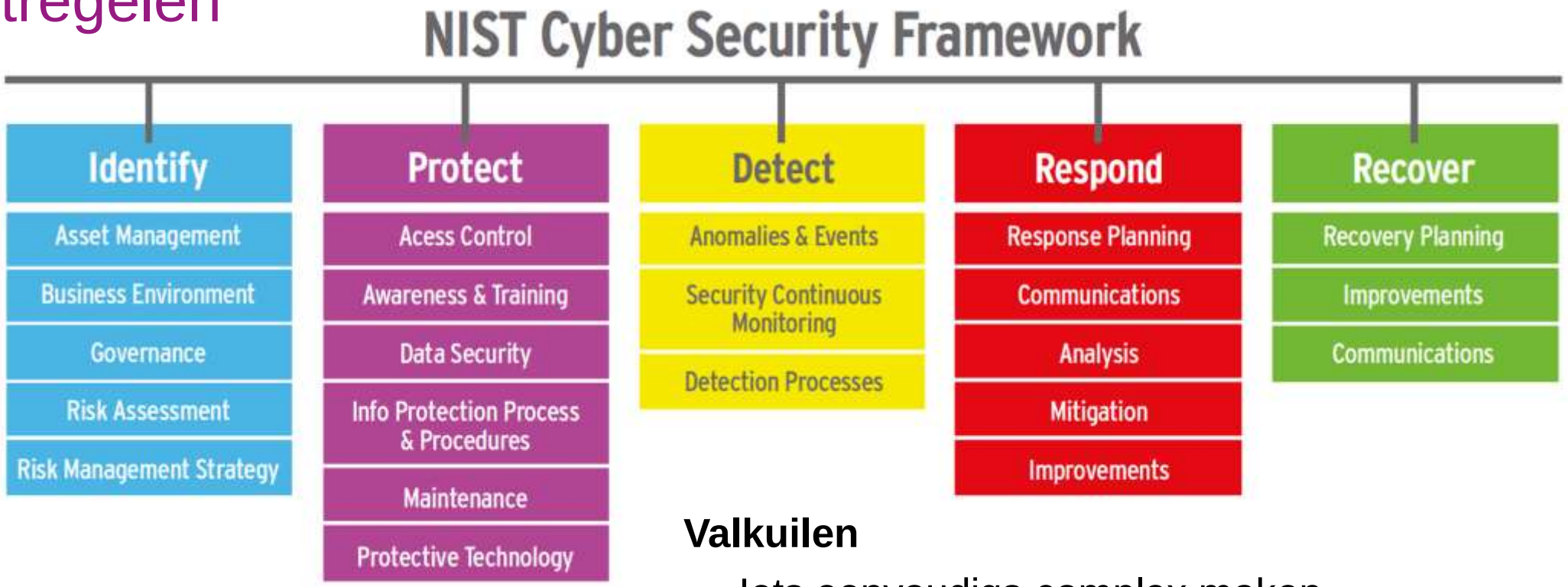
- Impact analyse
  - Hoe belangrijk is deze informatie / dit systeem voor de organisatie?
  - Wat is de impact voor de organisatie bij een probleem?

- In kaart brengen van de stakeholders en actoren
  - Extern : cybercriminelen, leveranciers en klanten
  - Intern : directie en medewerkers

- De dreigingsanalyse
  - Kans en impact bepalen
  - Bepalen hoe moet worden omgegaan met het risico (incl. het restrisico)
  - Maatregelen:
    - Huidige situatie / huidige maatregelen
    - Gewenste situatie / te nemen acties


1040 U.S. Individual Income Tax Return
W-9
Publication 3
Armed Forces' Tax Guide
Publication 17
For use in preparing 2010 Returns
Your Federal Income Tax
For Individuals
TAX GUIDE
Your Rights as a Taxpayer
Introduction
Contents

Maatregelen



Bron: https://www.nist.gov

Valkuilen

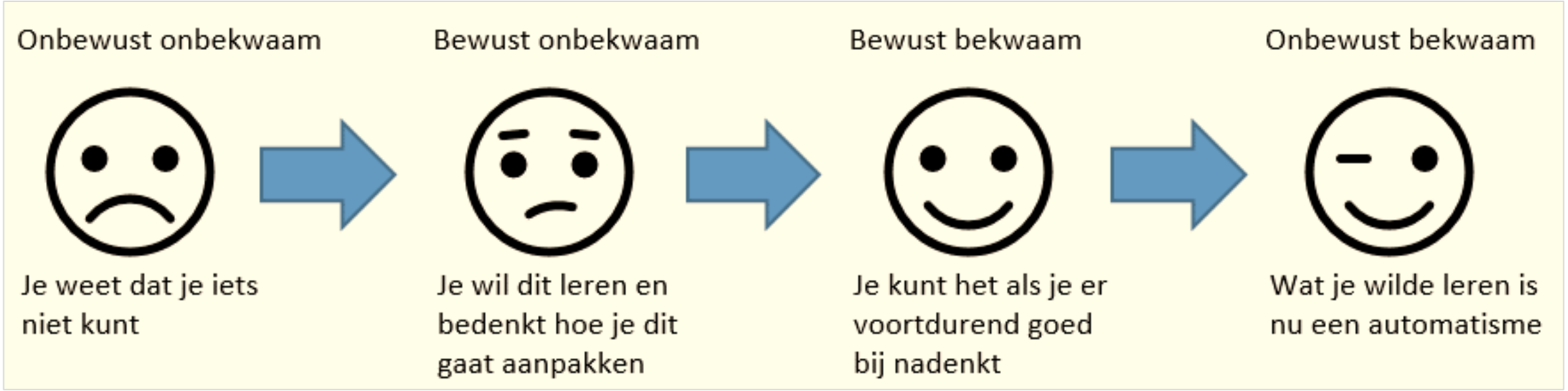
- Iets eenvoudigs complex maken
- Alles willen oplossen
- Niet eens zijn over het risico
- De ultieme oplossing willen hebben
- Te complexe oplossing

Best practices

- Identificeer
  - Awareness, de menselijke firewall
  - Bedrijfscontinuïteit, maak een plan
  - Kroonjuwelen bepalen
- Bescherm
  - Train de medewerkers
  - Zorg voor digitale hygiëne
  - Backup, volgens de 3-2-1-1-0-regel
- Ontdek
  - Installeer detectiesystemen
  - Plaats virtuele struikeldraden
- Reageer
  - Zorg voor een incident-respons plan
  - Wees kalm en betrouwbaar
- Herstel
  - Maak een herstelplan
  - Ontwerp je herstel

Bron: Veeam

Medewerkers



- Vertel de medewerker duidelijk wat deze moet doen.
- Pas op dat je niet ongeduldig wordt als het niet snel genoeg gaat.

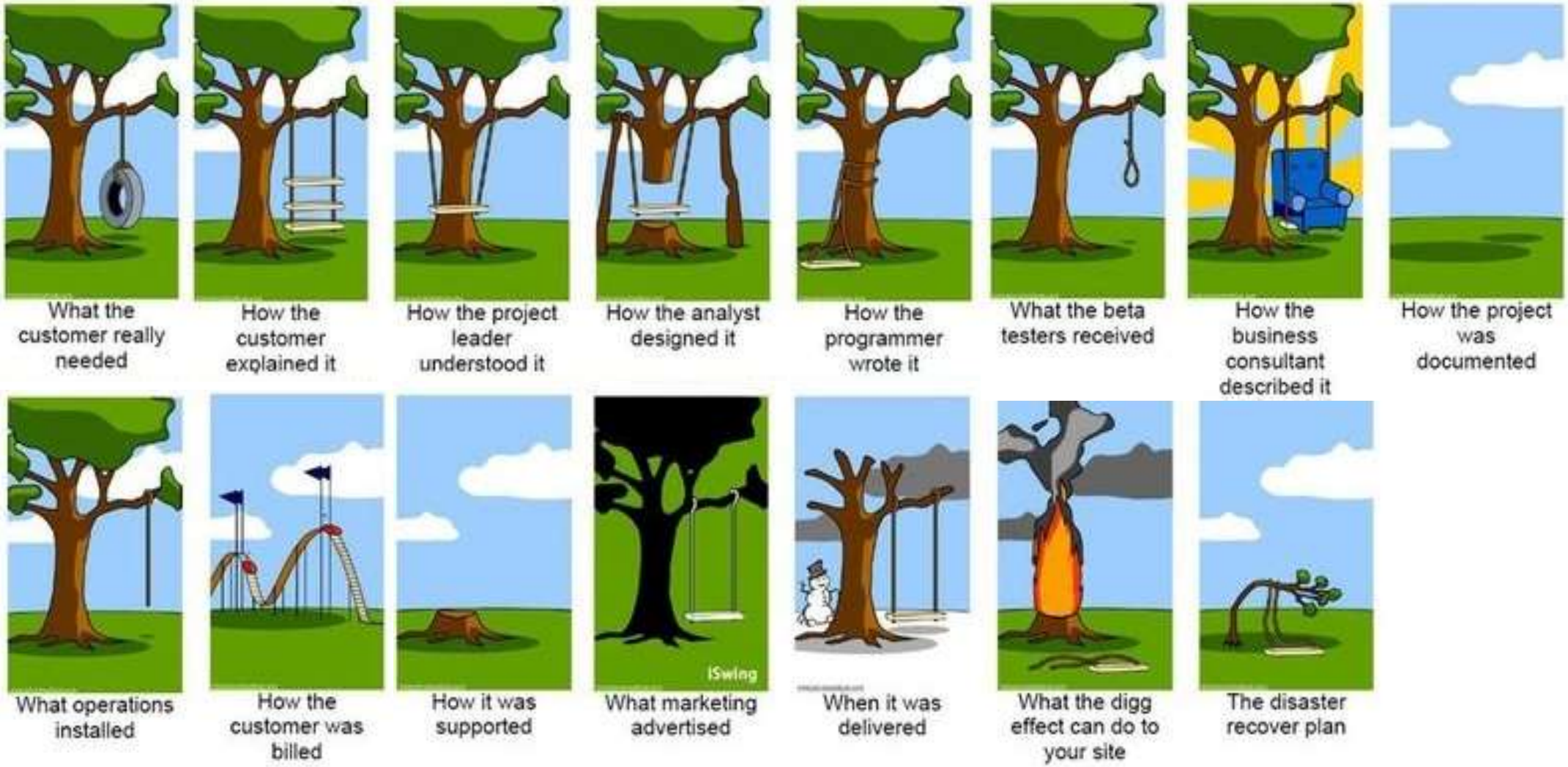
- Coach de medewerker.
- Pas op dat je de medewerker niet betuttelt of niet serieus neemt.

- De medewerker weet wat te doen.
- Pas op met teveel opdrachten omdat deze medewerkers al weten wat ze moeten doen.

- Naar deze medewerker heb je geen omkijken.
- Pas op met teveel vrijheid, dit kan leiden tot verlies aan betrokkenheid.

Dan willen we nu een tool!

SRA



Iedereen heeft z’n eigen perspectief

- Eenvoud
- Voldoen aan administratieve (privacy) verplichtingen
- Verantwoording (“zijn we compliant?”)
- Bescherming van data (encryptie, logische toegang)
- Kennis
- Forensische tooling (“wat is er gebeurd?”)

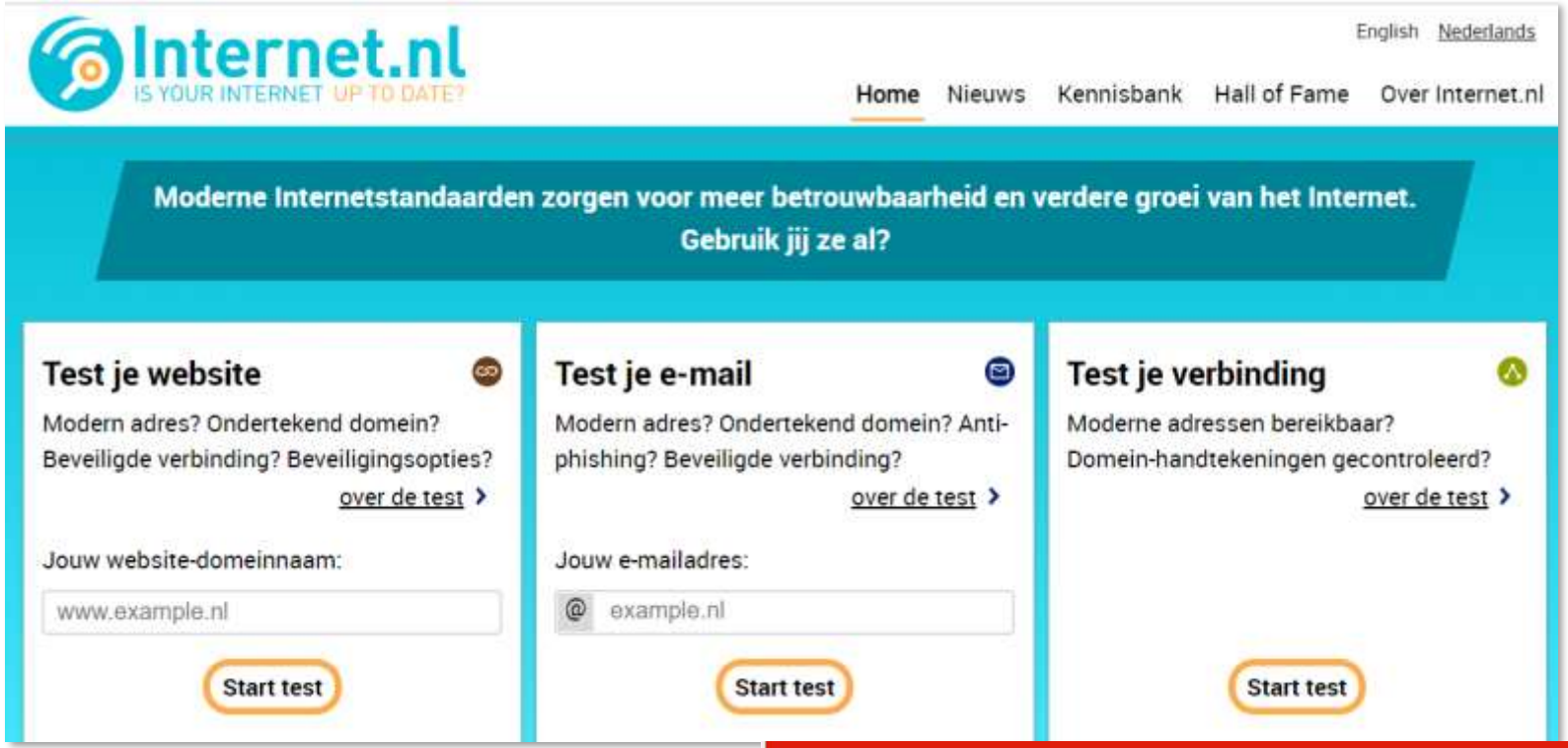
Aandachtspunten

- Veel (nieuwe) marktpartijen
- Terminologie; wat is wat?

Tools

- Gebruiksvriendelijkheid; wie zijn de gebruikers?
- Ondersteuning bij implementatie
- Wat kun je met de resultaten?
- Hoe zit het met de kosten?
  - Aanschaf / abonnement
  - Implementatie
  - Gebruik en beheer
- Een hele suite? Ga je alles wel echt gebruiken


PITTSBURGH


Internet.nl
IS YOUR INTERNET UP TO DATE?
English Nederlands
Home Nieuws Kennisbank Hall of Fame Over Internet.nl
Moderne Internetstandaarden zorgen voor meer betrouwbaarheid en verdere groei van het Internet.
Gebruik jij ze al?
Test je website
Modern adres? Ondertekend domein? Beveiligde verbinding? Beveiligingsopties?
over de test
Jouw website-domeinnaam:
www.example.nl
Start test
Test je e-mail
Modern adres? Ondertekend domein? Anti-phishing? Beveiligde verbinding?
over de test
Jouw e-mailadres:
@ example.nl
Start test
Test je verbinding
Moderne adressen bereikbaar? Domein-handtekeningen gecontroleerd?
over de test
Start test

SRA

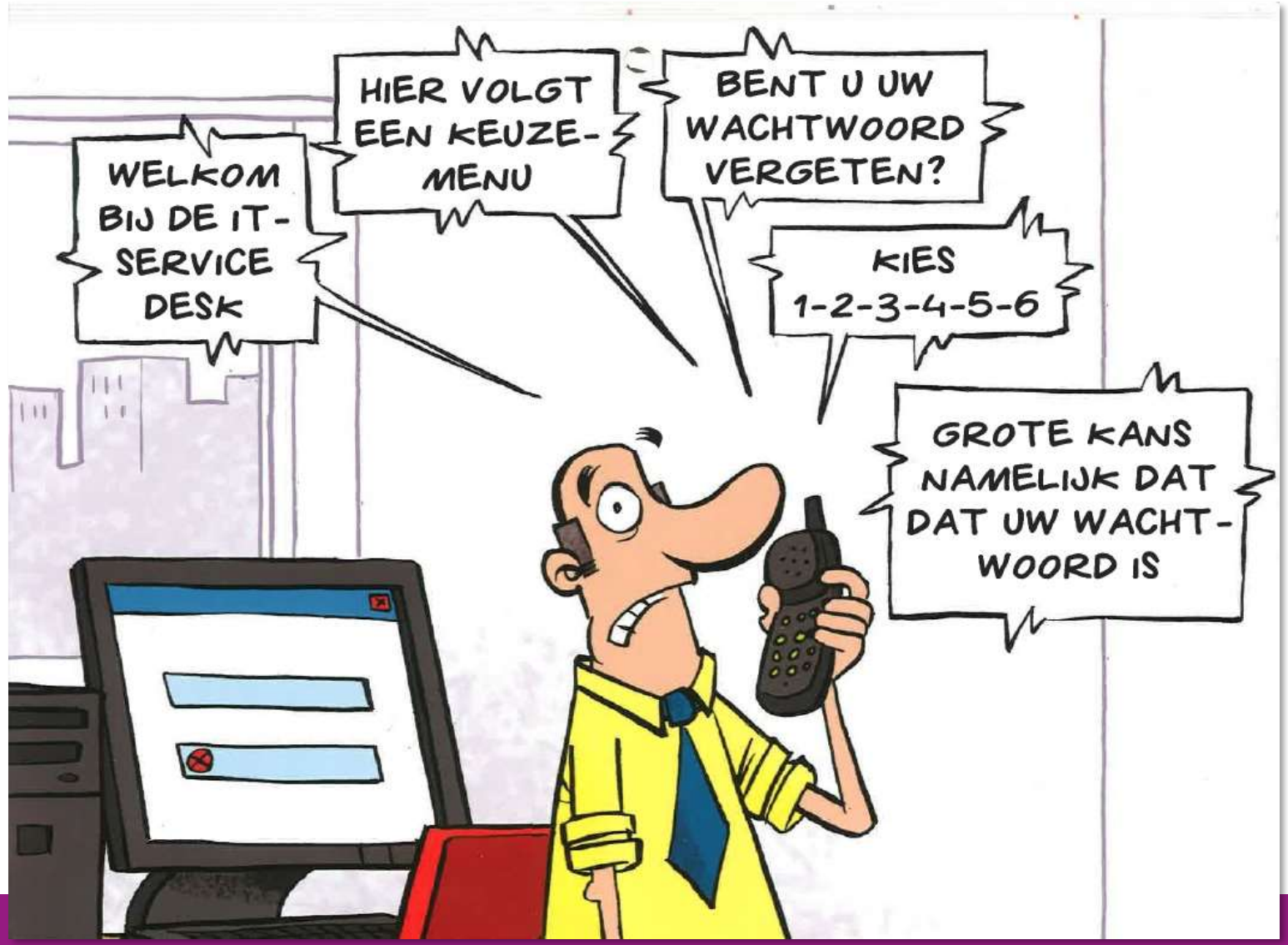

Qualys. SSL Labs
Home Projects Qualys Free Trial Contact
You are here: Home > Projects > SSL Server Test
SSL Server Test
https://www.ssllabs.com/ssltest/
This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.
Hostname:
Submit
Do not show the results on the boards

Ministerie van Economische Zaken en Klimaat

1	**Inventarisatie van Kwetsbaarheden** Het vergroten van de weerbaarheid tegen cyberincidenten begint bij inzicht. Inzicht in de kwetsbaarheden van bedrijfssystemen en de risico's. Begin daarom met een inventarisatie en denk na over wat je wel en niet moet doen bij een cyberincident.	
	Inventarisatie van kwetsbaarheden	
1a	Maak en onderhoud een inventarisatielijst van alle computers, software, clouddiensten, slimme apparaten etc., voorzien van bijbehorende software-versies en serienummers. Zie voor een voorbeeld bijlage 1. Maak deze inventarisatie ook als je zaken hebt uitbesteed aan een leverancier.	Actualiseer minimaal elke 3 maanden.
1b	Controleer of onbekende apparaten en software in de omgeving aanwezig zijn en geef hier opvolging aan.	Controleer in een continue proces en volg indien nodig op.
1c	Maak een inventarisatie van onderdelen en informatie die bedrijfskritisch en gevoelig zijn. Denk hierbij aan eigen vindingen, formules, modellen en andere concurentiegevoelige informatie.	Actualiseer minimaal elke 3 maanden.
	Back-up en recovery Door een cyberincident kan bedrijfsdata verloren gaan of geïnfecteerd raken. Hierdoor kunnen de primaire bedrijfsprocessen stil komen te liggen. Het consequent maken van back-ups, draagt bij aan het snel herstellen van de verloren gegevens, zodat de onderneming vlot weer aan de slag kan.	

https://tools.digitaltrustcenter.nl/check-je-risicoklasse/

Wachtwoorden



Tips over wachtwoorden

- Test je wachtwoord(en)

https://veiliginternetten.nl/wachtwoordkraak-test/

- Gebruik tweetrapsverificatie

. . .

- Gebruik een password manager

. . .

Thuiswerken - Het kantoor als ontmoetingsplek

Aandachtspunten voor thuiswerken

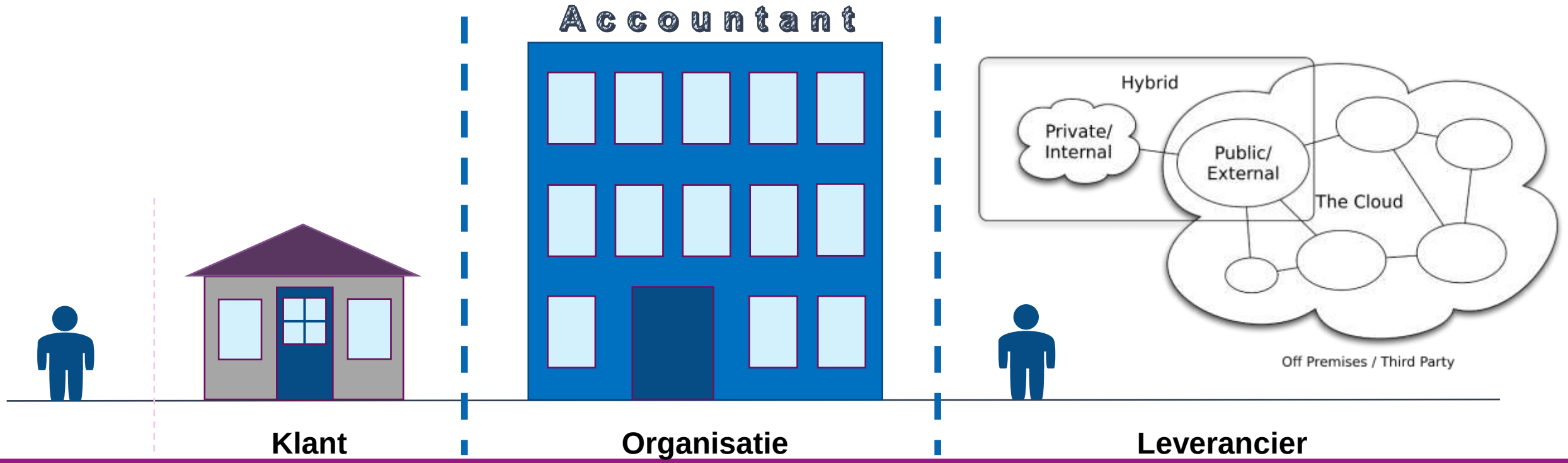
- Gebruik van privé computers en (wifi)netwerk
  - Updates en upgrades
  - Antivirus
- Gebruik van online software en websites
- Toegang tot vertrouwelijke bestanden
- Veilige verbindingen (kantoor en applicaties)
- Procedures en richtlijnen:
  - Wat deel je wel / niet
  - Gebruik van vertrouwelijke bestanden
  - Afsluiten (⊞ + L)
  - Opname videovergaderingen
  - …
- Wees je bewust van valse e-mails / phishing

“Hoe weet ik dat medewerkers via een veilig (wifi) netwerk werken (thuis, bij klanten of elders) of hoe kan dat goed beveiligd worden?”

https://www.digitaltrustcenter.nl/thuiswerken

(Cl)outsourcing

- Integrale ketenbenadering bij het bepalen van informatiebeveiligingsrisico's en beheersmaatregelen
- Afspraken met klanten en leveranciers



Werken in de cloud

Als je gehost bent: wat is dan het hackrisico?
Waar moet je op letten of wat kan je verlangen?

Algemeen

- Multi-factor authenticatie
  - Beheerders
  - Gebruikers
- Rollen en rechten
- Logging
- Alerts
- Verouderde protocollen en applicaties
- Afspraken m.b.t. thuiswerken

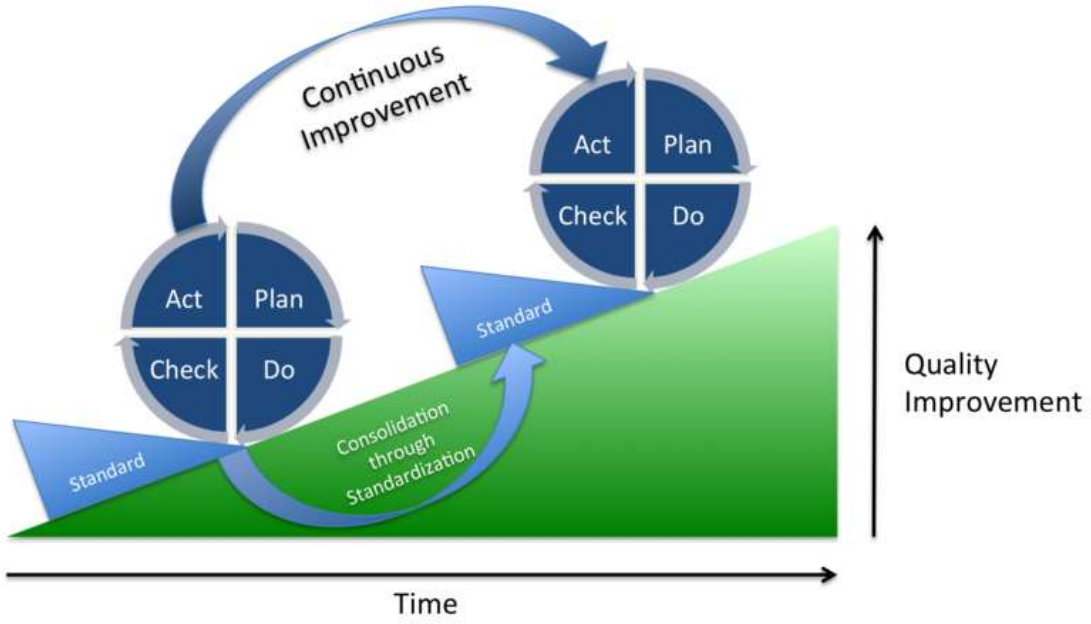
Meer info: https://www.digitaltrustcenter.nl/nieuws/veilig-werken-in-cloud-werkomgevingen

Afspraken met je leverancier

- Uitbestede producten en diensten
- Onderhoudswerkzaamheden
- Getroffen beveiligingsmaatregelen
- Werkplekondersteuning en –beveiliging
- Gegevensbescherming
- Omgaan met incidenten en datalekken
- Service levels en rapportage
- Exit-procedure

Meer info: https://www.digitaltrustcenter.nl/informatie-advies/afspraken-maken-met-een-it-leverancier

Evalueren en verbeteren



- Plan een evaluatie
- Zorg voor inhoud
  - Incidenten en resultaten
  - Impact op het proces
- De juiste mensen aan tafel
- Bepaal de verbeterpunten; maak een lijst (korte en lange termijn)
- Benoem verantwoordelijken voor verbeterpunten
- Communiceer over het oplossen van verbeterpunten
- Plan een (her)test

Tips voor betere cyber weerbaarheid

Alertheid

- Vergroot bewustzijn bij medewerkers
- Volg actuele ontwikkelingen

Preventie

- Organiseer de back-up en test de back-up procedure regelmatig
- Oefen herstelprocedures
- Zorg voor een actief update beleid; voer updates zo snel mogelijk uit
- Beperk toegang tot data; toegang van medewerkers afhankelijk hun rol, functie en daarbij behorende rechten.

Detectie

- Monitor systemen en de dagelijkse operatie
- Test jezelf!

Valkuilen bij selectie van oplossingen / leveranciers

- Aandacht voor security & privacy
- Flexibiliteit / schaalbaarheid
- Ervaring
- Omgaan met hybride omgevingen
- Exit-strategie

Samengevat

SRA

Aan de slag

- Zet informatiebeveiliging op de agenda; benut de kansen vanuit de AVG
- Maak mensen verantwoordelijk
- Budgetteer informatiebeveiliging
- Rapporteer en analyseer incidenten
- Blijf zorgen voor bewustwording
- Zorg voor security by design (en privacy by design)

Geiger-project

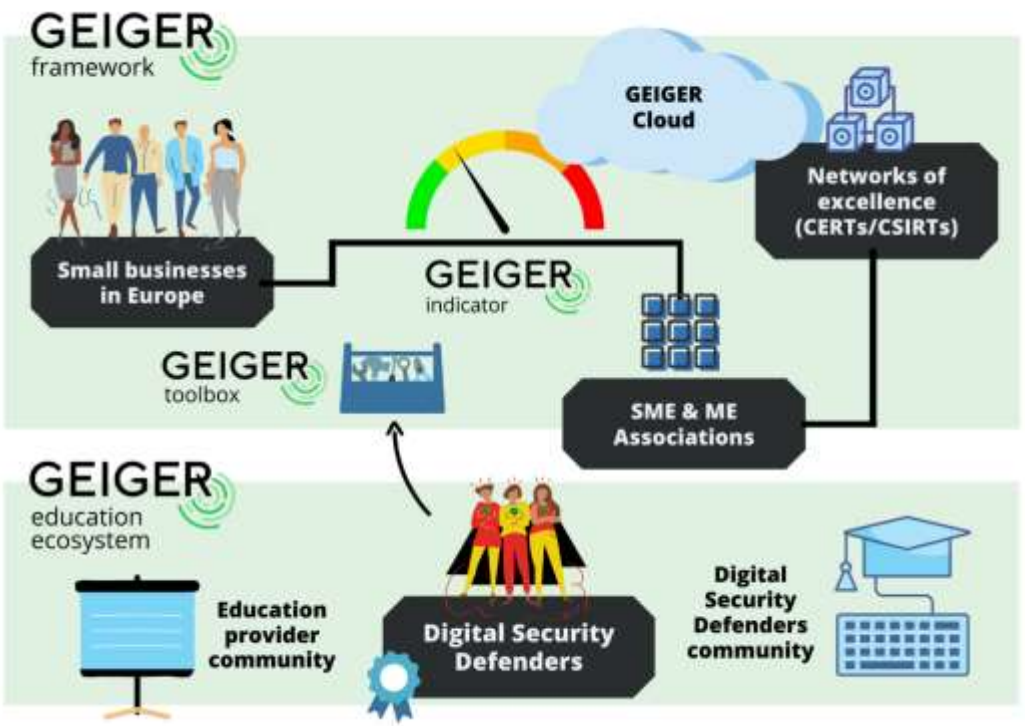
Innovatieproject voor het mkb op het gebied van cyberbeveiliging

- Tool: ‘Geigerteller’ voor cyberbeveiliging
- Opleidingsprogramma

In Nederland

- Accountant als trusted advisor
- Kick-off meeting 18 november

➢ Meer informatie: https://www.sra.nl/geiger/



GEIGER

Bedankt voor uw aandacht.