



**BRIGHT PEOPLE
SMART SOLUTIONS**

Risico = Kans x Ellende



Arno

Van Boggelen
Manager Support & Beheer

Toename activiteit cybercriminelen
gebruikers

Wonincor

Cybercriminelen raken meer werk
taleb in 2023: cybercriminelen

organisaties doen melding
Eredivisie en Keuken

Cyber
Kans Minimaal 2
gehackte bedrijven
rijfsleven snoeihard: 139

Ka
ransomware
na ransomware-

T-Mobile getroffen door twee
compromitteren klantgegevens
gericht op Microsoft 365-



Break-out sessie

- Informatiebeveiliging
- Risicoanalyse
- Bedrijfsbeleid
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)



Doelstellingen

- Met deze break-out sessie zou ik uw organisatie kort mee willen nemen in de wereld van risicomanagement en informatiebeveiliging.
- Vandaag zou ik graag bij u bewustzijn creëren en het eerste aanzetje geven om dit ingewikkelde onderwerp in uw organisatie op te gaan pakken en niet langer af te wachten.

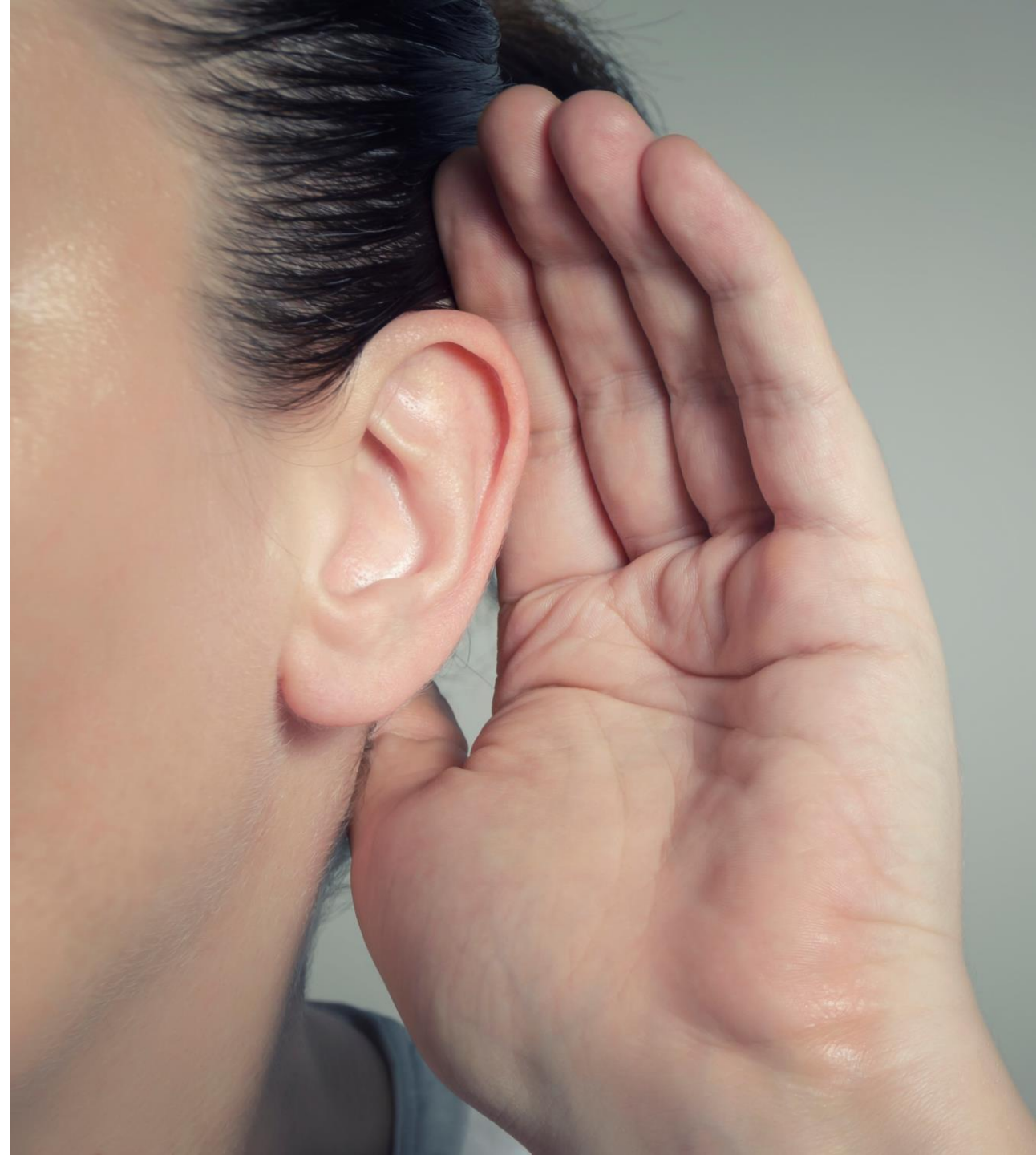
Informatiebeveiliging

Data of informatie?

- Data zijn ruwe feiten of observaties, terwijl informatie de betekenisvolle interpretatie en presentatie van die data is.
- Data wordt omgezet in informatie door het te organiseren, analyseren en te voorzien van context.
- Voor de ontvanger heeft informatie toegevoegde waarde en de losse data niet.

Classificaties

- Geheim
- Vertrouwelijk
- Persoonsgegevens
- Intern
- Publiek





Informatiebeveiliging

- **Authenticiteit:** de oorsprong
- **Integriteit:** de betrouwbaarheid
- **Beschikbaarheid:** op het juiste moment beschikbaar
- **Privacy:** beschermen van persoonsgegevens
- **Veiligheid:** beschermen van informatie



AVG en ISO27001

- AVG is wetgeving ter bescherming van persoonsgegevens.
- ISO is een hulpmiddel voor informatiebeveiliging.

Risicoanalyse



Is er binnen uw
organisatie een
risicoanalyse gedaan
m.b.t.
informatiebeveiliging?

Risicoanalyse

- Bedreigingen
- Kans
- Ellende
- Risicoscore
- Risicobereidheid
- Beheersmaatregelen



Kans versus Ellende

- Risico's worden vaak uitgedrukt in de **kans** dat het voorkomt en de **ellende** (impact) die het heeft op de organisatie.
- De kunst van risicomanagement is om een evenwicht te vinden tussen het **verkleinen van de Kans** en het **minimaliseren van de Ellende**.

Bedreigingen

- Menselijk gedrag
- (Technische) storingen
- Kwetsbaarheden en cyberaanvallen
- Datalek
- Inbraak
- Natuurrampen
- Brand



Is een zwak wachtwoord
wat de medewerker instelt
menselijk handelen of een
gebrek aan beleid?

"Risicobeheer is een cultuur, geen afdeling"
John H. Vande Vate



Voorbeeld risicobepaling



Datacorruptie door stoomstoring

- Kans: 2x per jaar
- Ellende: bedrijfsvoering en herstel van data kosten € 6.000,- per gebeurtenis
- Risicoscore: € 12.000,- per jaar

Risicoacceptatie	Risicovermindering	Risicomijding
Geen maatregelen	Beperkte maatregelen Voorbeeld: <ul style="list-style-type: none">• UPS Accu	Veel maatregelen Voorbeeld: <ul style="list-style-type: none">• UPS Accu• Installatie na laten kijken• Regelmatig onderhoud• Generatoren plaatsten

Zwak wachtwoord

- Kans: continu
- Ellende: bedrijfsinformatie wordt gestolen en misbruikt **wordt**
- Risicoscore: hoog (90 op een schaal van 100)

Risicoacceptatie	Risicovermindering	Risicomijding
Geen maatregelen	Beperkte maatregelen Voorbeeld: <ul style="list-style-type: none">• Afdwingen sterk wachtwoord	Veel maatregelen Voorbeeld: <ul style="list-style-type: none">• Afdwingen sterk wachtwoord• Regelmatig laten wijzigingen• 2FA• Minimaliseren van rechten• Encryptie van data

Cijfers en feitjes

- In 2021 waren zijn 4.332 datalekken gemeld (AVG)
- Phishing is de meest voorkomende methode van cyberaanvallen
- 1/3 van de bedrijven heeft te maken gehad met een cyberaanval (CBS)
- 5 geslaagde cyberaanvallen per maand op Nederlandse bedrijven (NBIP)
- In 2019 zijn de totale kosten van cybercriminaliteit geschat op 10 miljard euro
- Volgens studies is het nemen van maatregelen op langere termijn voordeliger
- Meebewegen met veranderingen is een noodzaak
- Banken en verzekeraars passen de dienstverlening aan (ABN AMRO)

Bedrijfsbeleid

Bedrijfsbeleid

- Focus
- Beslissingen
- Naleven
- Draagvlak



Business Continuity Plan (BCP)



Is er binnen uw
organisatie een Business
Continuity Plan?

Business Continuity Plan

Een BCP is een strategisch plan dat de procedures, richtlijnen en acties beschrijft die een organisatie moet nemen om de bedrijfscontinuïteit te waarborgen tijdens en na een calamiteit.





Business Continuity Plan

- Blijven functioneren
- Beperken van financiële verliezen
- Beperken van (reputatie)schade
- Nakomen van contractuele verplichtingen
- Veerkracht van de organisatie verhogen
- Verzekeringen
- Afspraken maken met IT en Software leveranciers

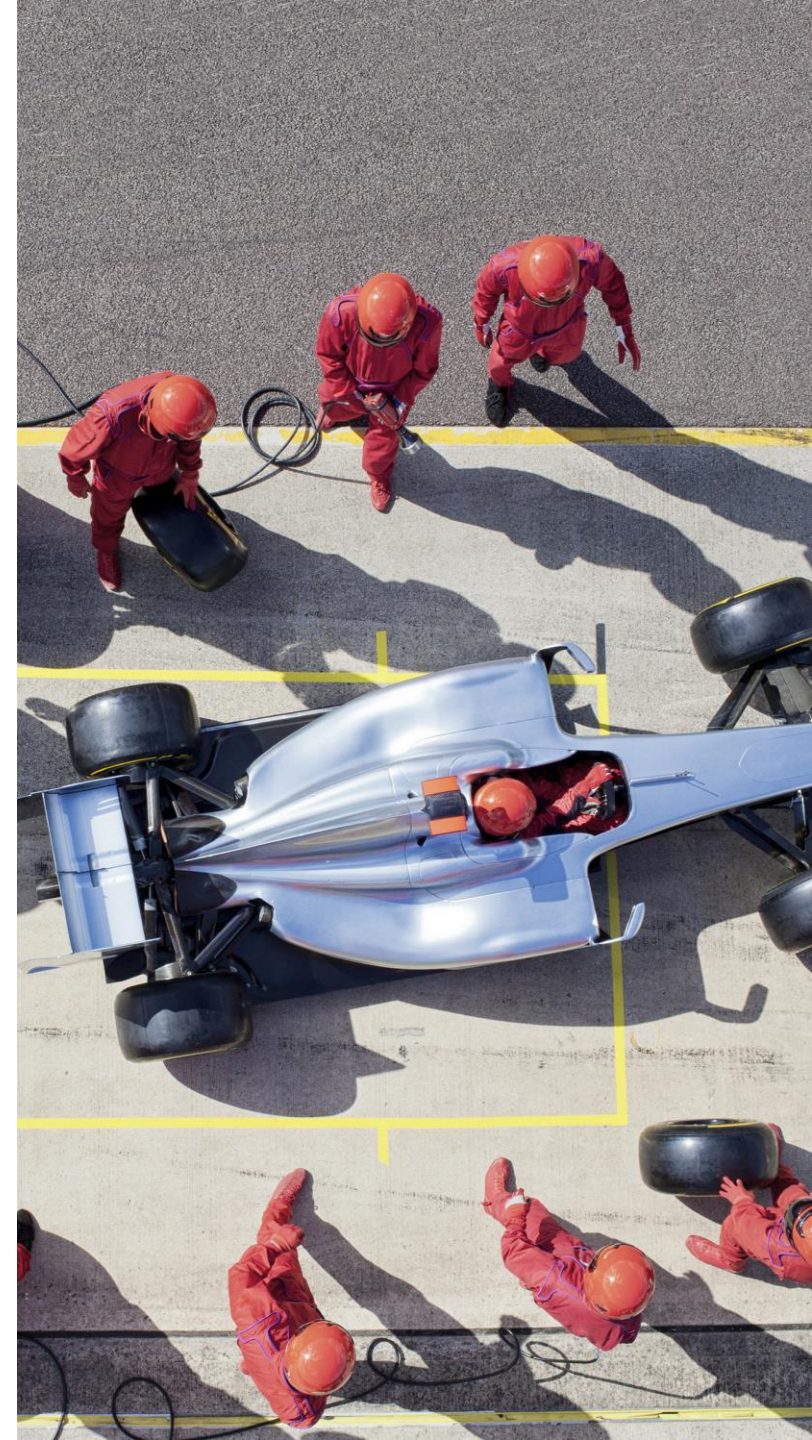
Disaster Recovery Plan (DRP)



Is er binnen uw
organisatie een Disaster
Recovery Plan?

Disaster Recovery Plan

Een DRP is een operationeel plan dat specifiek gericht is op het herstellen van systemen, gegevens en infrastructuur na een calamiteit.





Disaster Recovery Plan

- Minimaliseren van gegevensverlies
- Minimaliseren van downtime
- Beschermen van bedrijfskritische processen
- Procedures afgestemd met IT en software leveranciers

Wat kunt u nu
al doen?

Actie

- Volg een training informatiebeveiliging en/of ISO27001
- Awareness creëren in de organisatie
- PEN testen (ethisch hacker) uit laten voeren
- Informatiebeveiligingsincidenten registeren
- BCP en DRP opstellen
- Heldere afspraken maken met IT en software leveranciers
- Verdiepen in eisen van ISO27001
- Banken en verzekeraars bieden extra diensten



Heeft uw organisatie afspraken voor onderhoud en reparaties op machines? En voor het IT-landschap?

Wat kan AB
betekenen?



Ondersteuning vanuit AB

- Inrichten van rollen en rechten binnen de applicaties
- Inrichten beveiligingsniveaus en documenttypes in e-Synergy
- Alleen gevalideerde wijzingen in de database (ABEI)
- Het testen van updates voordat deze naar productie gaan
- Advies over netwerkaccounts (serviceaccounts)
- Service Level Agreement (SLA)



Service Level Agreement (SLA)

- Kennis
- Capaciteit
- Responsafspraken
- Voorrang bij calamiteiten
- Bereikbaarheid elke dag van 8:30 tot 17:30
- Escalatiemanager

Wilt u meer informatie over een SLA?

Neem gerust contact op met uw accountmanager!



edankt voor uw aandacht!