

Cybersecurity Awareness

Cyberboswachters

Tim Dams

Deze cursus werd gemaakt met hulp van AI-assistentie. Sommige afbeeldingen zijn door AI gegenereerd.



WAAROM AWARENESS?

68%

van de datalekken heeft een **menselijke factor** (Verizon DBIR 2024)

klikken op een phishing-link

zwak wachtwoord

onveilig wifi-netwerk



Technische maatregelen alleen zijn **niet voldoende.**

Medewerkers moeten begrijpen **waarom** een maatregel bestaat en hoe ze die toepassen in hun dagelijkse werk.

Jouw rol als cybersecurity-professional

Je bent meer dan een technicus: je bent een **bewustzijnsambassadeur**.



Vertalen

Complexe technische risico's omzetten naar begrijpelijke taal voor collega's en management.



Signaleren

Potentiële risico's identificeren. Afwijkingen en verdachte gebeurtenissen snel en duidelijk rapporteren.



De hele keten

Denk aan de **McCumber kubus**: de menselijke dimensie is even belangrijk als technologie en procedures.

DEEL 1

Awareness-campagnes

Kort, terugkerend en afgestemd op het bedrijf.

Het doel van een campagne

 **Niet**

“Je mag dit niet.”

Regels opleggen zonder uitleg.

vs

 **Wel**

“Hier is waarom dit gevaarlijk is.”

Inzicht geven in de risico's en de gevolgen van bepaald gedrag.

Einddoel: autonome medewerkers

- ✓ Ze leggen zelf de link tussen **gedrag en risico**
- ✓ Ze kiezen bewust voor veilige werkmethoden
- ✓ Ze herkennen en melden nieuwe risico's, ook in onbekende situaties
- ✓ Veilig handelen is een **routine**, geen verplichting

"Waarom moet ik ...?"

Medewerkers moeten deze vragen **zelf** kunnen beantwoorden.



Geen publiek wifi?

Onversleuteld: aanvallers kunnen meekijken (*sniffing*).



Steeds MFA?

Een gestolen wachtwoord alleen volstaat dan niet meer om binnen te raken.



Laptop vergrendelen?

Anders kan een collega of bezoeker toegang krijgen.

Methoden die werken

Micro-trainingen

Kort en frequent: betere retentie, geen overload

Phishing-simulaties

Directe feedback op je eigen gedrag

Gamification

Quizzen en dashboards verhogen de motivatie

Posters & nieuwsbrieven

Visuele reminders in de werkomgeving

Leiderschap

Het management geeft het goede voorbeeld

Geen *one size fits all*: sluit aan bij de **dagelijkse context** van de medewerkers. Gratis

bronnen:

SANS Institute

CISA

GoPhish

Less is more

Een awareness-poster hoeft geen ellenlange tekst te bevatten.

Grappige of uitdagende posters worden **sneller opgemerkt** én onthouden.



Awareness posters hoeven geen ellenlange teksten te bevatten.

GEDRAGSVERANDERING

Je bereikt ze niet door te straffen, maar door te **motiveren en inspireren.**

Gedragsverandering is vaak de moeilijkste uitdaging binnen cybersecurity.

Wat elke medewerker moet kennen



Wachtwoorden & toegang

Sterke, unieke wachtwoorden in een **wachtwoordmanager**. Altijd **MFA** aan.



Apparaatbeheer

Automatische updates, antivirus actief, laptop vergrendelen als je weggaat.



Documenten & netwerken

Geen onbekende USB-sticks of kabels, enkel vertrouwde wifi, regelmatig **backups** (fysiek én digitaal).



Blijf leren

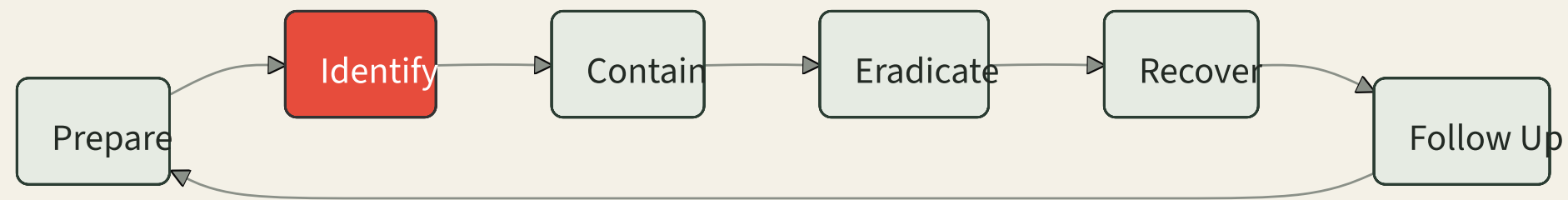
Deel kennis actief binnen je team en blijf op de hoogte van nieuwe dreigingen.

DEEL 2

Incident response

Incident response

Een goed **incident response-plan** minimaliseert schade en voorkomt herhaling.



De 6 stappen

1. Prepare

Procedures definiëren, medewerkers trainen, plan up-to-date houden.

2. Identify

Verdachte activiteiten **herkennen en melden**. Hier speelt awareness het meest.

3. Contain

Getroffen systemen isoleren, verdachte accounts blokkeren.

4. Eradicate

Het incident volledig verwijderen.

5. Recover

Systemen en data herstellen.

6. Follow Up

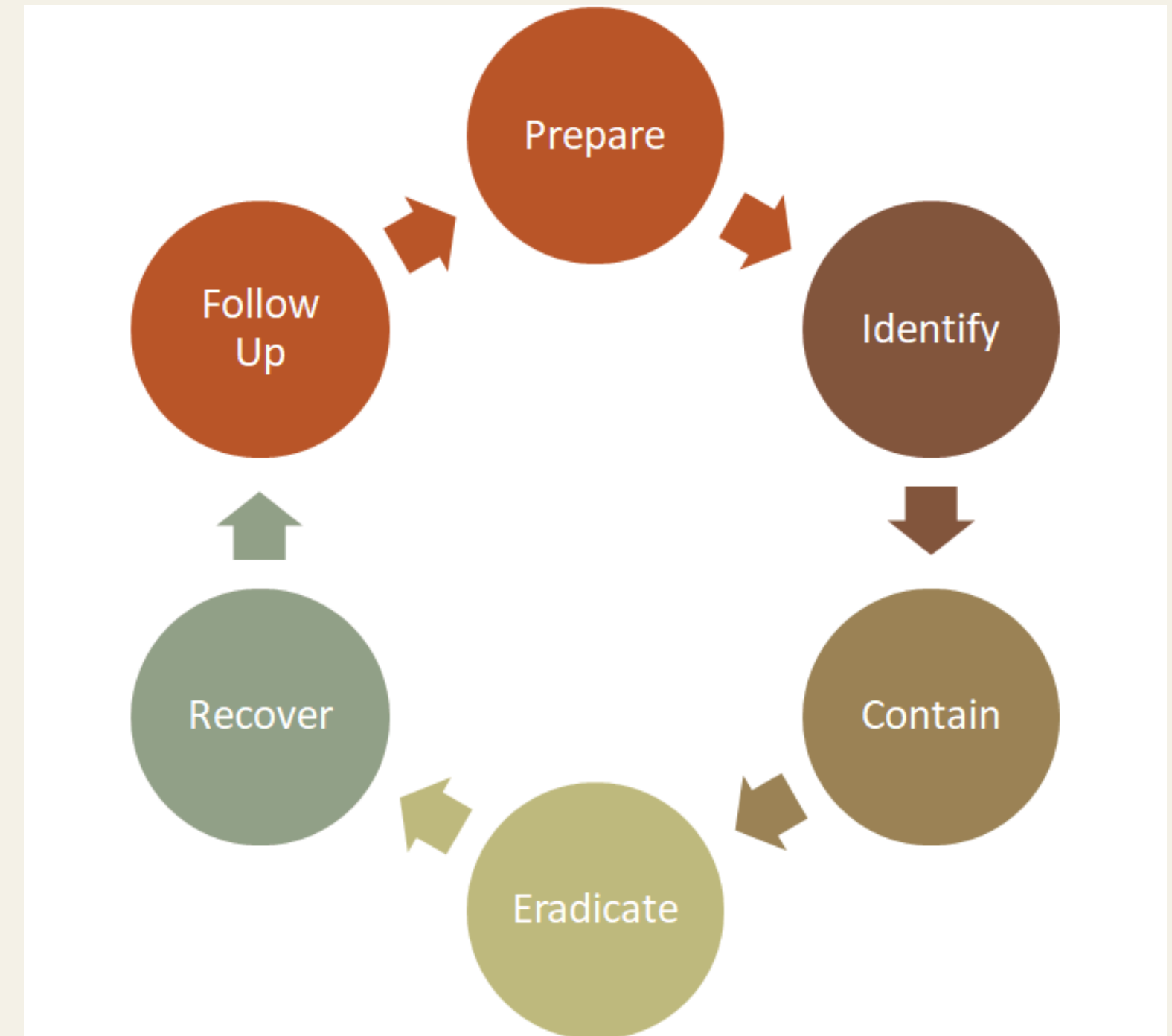
Oorzaak analyseren, processen verbeteren.

Dit is een fijnere versie van de **4 NIST-fasen** uit H2: *Contain*, *Eradicate* en *Recover* vormen samen NIST-fase 3.

Een cyclus, geen rechte lijn

Vaak wordt het plan getoond als een **lineaire sequentie**.

Na de *Follow Up* moet er altijd informatie terugstromen naar de *Prepare*-fase. Zo leren we uit elk incident.



Meldcultuur

Awareness helpt vooral bij **Identify**: hoe sneller een incident herkend wordt, hoe kleiner vaak de schade.

- ✓ Duidelijke meldprocedures: **wie meldt wat, aan wie, hoe snel?**
- ✓ Meldkanalen zijn **laagdrempelig en toegankelijk**
- ✓ Niemand mag bang zijn om een incident te melden



Een complex incident response-plan dat niemand kent, is **nutteloos**.

Oefen het plan regelmatig en zorg dat medewerkers weten wat **hun** rol is. Het plan is een levend document, geen map in de kast.

DEEL 3

Social engineering

De aanvaller heeft geen tools nodig, enkel een goed verhaal.

Technieken van de stropers



Pretexting

Verzint een geloofwaardig scenario, vaak als “collega” of “IT-medewerker”.



Tailgating

Loopt achter een medewerker een beveiligd gebied binnen.



Vishing

Voice phishing via de telefoon. AI imiteert stemmen steeds beter.



Baiting

Lokt met een USB-stick, gratis Spotify, ... vol malware.



Quid pro quo

‘Voor wat hoort wat’: iets aanbieden in ruil voor gevoelige informatie.



Combinatie

Meestal gebruiken aanvallers meerdere technieken tegelijk.

Ontmaskeren met een challenge



Beller: “*Uw bank is KBC.*” Jij: “Neen hoor.” Beller: “*Oh excuses, ik bedoelde Argenta.*”

Phishing herkennen

Afzender	Vergelijk met eerdere communicatie of de website
Links	Hover zonder te klikken: waar leidt de link echt naartoe?
Bijlagen	Van onbekenden nooit openen zonder verificatie
Urgentie	“Onmiddellijk actie vereist!” is een klassiek manipulatiemiddel
Gevoelige info	Een vraag via mail of telefoon is bijna altijd verdacht
Twijfel	Bel terug via een gekend nummer, niet via het nummer in de mail



Bij twijfel: **niet klikken.**

Melden is altijd beter dan niets doen, ook als het uiteindelijk vals alarm blijkt.

Conclusie

- ✓ Bij **68%** van de datalekken speelt de mens mee: awareness is een noodzaak
- ✓ Goede campagnes leggen uit **waarom**, niet alleen wat
- ✓ Varieer: trainingen, simulaties, gamification, posters
- ✓ Een incident response-plan werkt alleen als medewerkers het kennen
- ✓ Social engineering herken je door te **challengen en te verifiëren**