Cyber Security
Voor Ondernemers

KBC

Toelichting Bedrijvenpark Waregem-Zuid

Bert Bleukx

Cybercriminaliteit
is een sterk
geïndustrialiseerde
zwarte economie geworden

Het gevolg is dat niet alleen banken of overheden het doelwit zijn, maar OOK KMO's en kleine zelfstandigen

Om je daar tegen te wapenen:

1) Manage je ICT
   (je kan wel je ICT outscourcen, maar niet je verantwoordelijkheid over ICT)
2) Neem je personeel mee in de strijd

The Art of Cyber Security

Om je onderneming te beschermen tegen cybercriminelen, dien je te werken aan kennis en betrokkenheid

Kennis en betrokkenheid van je medewerkers (zie volgende pagina)

Betrokkenheid vanuit de CEO tav ICT
Kennis van ICT over de business prioriteiten van de onderneming: wat zijn de 'kroonjuwelen' en wat is minder belangrijk om te beschermen. Daardoor kan je gerichter investeren en spreiden in de tijd.

CEO: Prepare your ICT for the battle

Niet vanuit een motie van wantrouwen "ze doen het niet goed"
Noch vanuit een 'gemakkelijkheidshouding': "Ik snap daar toch niets van"
WEL vanuit een visie van 'good management'
"Je kan wel je ICT outscourcen,
maar niet de verantwoordelijkheid over je ICT"

Cybersecurity is een continue investering
- SPREEK met je ICT
- Bepaal samen met hen de prioriteiten

IT-security is cruciaal
- organiseer regelmatig een neutrale security assessment op je ICT

Personeel Scanning:

Hoe goed is de Security-kennis van je personeel?

Via misleidende mails medewerkers verleiden tot het openen van een attachment of klikken op een link

Laat u NIET misleiden door een logo of door de ondertekening (= 2 minuten Google)

Kijk naar het afzend-adres
Kijk naar het adres achter de link
Bedenk: verwacht ik dit van deze afzender?

Geef je medewerkers opleidingen:

- Eenvoudige tips waarmee ze valse mails kunnen doorprikken

Train je medewerkers

- Stuur zelfgemaakte phishingmails uit als test en meet hoe vaak er op geklikt wordt

Geef je medewerkers een meldpunt:

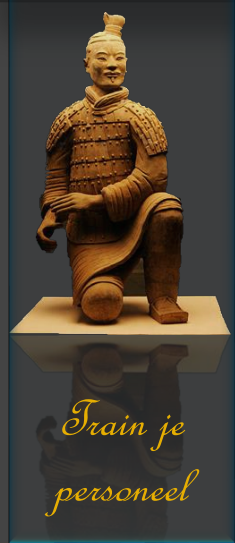
- Wanneer ze zo'n valse mail ontvangen: waar moeten ze ermee naartoe?

BETREK je medewerkers in de strijd tegen cybercriminelen:

- Leg hen geen (in hun ogen) zinloze regels op, die zullen ze trachten te omzeilen
- Maar leg uit WAAROM dit nodig is.
- Geef hen tips om security regels zonder teveel inboeting op gebruiksgemak effectief toe te passen.

Voorbereiding:

Vecht je personeel MEE of TEGEN je?



- Paswoorden
  - Het geheim van goede paswoorden
    - Geen herbruik
      - Als ze 1 toepassing kraken, proberen ze dat paswoord op al je andere toepassingen
      - Dwz: Als ze 1 toepassing kraken zoals bv LinkedIn, dien je
        - voor jezelf te controleren waar je datzelfde paswoord nog gebruikt
        - en ook in die toepassingen je paswoord te wijzingen
    - Tip om zonder veel complexiteit toch steeds een ander paswoord te hebben:

      bv Wachtwoord = "Wachtwoord"
      Vervang steeds 3e letter door 1e letter van de toepassing

      ➔ Wachtwoord 'Dropbox' = "WaDhtwoord"
      ➔ Wachtwoord 'Gmail' = "WaGhtwoord"
      ➔ Wachtwoord 'Facebook' = "WaFhtwoord"