Beste collega,

Wij hebben jou nodig! Wist je dat één Belgische onderneming op twee vandaag wordt geconfronteerd met **cybercriminaliteit**?

Een medewerker van een Belgische kmo maakte deze pijnlijke ervaring mee. Door één enkele klik op een **bijlage besmet met een virus**. Zijn computer werd **volledig versleuteld** waardoor de bestanden van de onderneming niet meer konden worden geopend, zelfs niet via de back-up. Alles ging **heel snel** en de kosten liepen op: verlies van belangrijke gegevens, vraag om 10.000 bitcoins aan losgeld, klachten van klanten, … Een rechtstreekse, werkelijke kost van 35.000 euro.

Jou overkomt het niet? Jij bent voorzichtig en ze hebben je niet snel liggen? Dat dacht hij ook…

Daarom willen wij het met jou graag hebben over de **3** meest voorkomende en meest gevreesde **cyberaanvallen**:

* Het hacken van **wachtwoorden** waardoor de veiligheid van al onze professionele en privéaccounts in het gedrang komt.
* **Phishing**waarbij iemands identiteit wordt misbruikt om via e-mail toegang te krijgen tot onze bedrijfs- of bankgegevens.
* **Social engineering of social hacking** dat misbruik maakt van het vertrouwen van de medewerkers, om op oneerlijke wijze aan belangrijke informatie te geraken of om een geldtransfer te bekomen.

Je hebt deze vorm van internetfraude zeker al zien voorbijkomen op het nieuws. Zin om hier meer over te weten te komen?

Laten we samen nadenken over de beste manier om:

* Aanvallen te **ontmaskeren**
* De **juiste reflexen** aan te nemen
* Snel te **waarschuwen** en te **reageren**

In de komende weken zal je via e-mail **interactieve informatie ontvangen** met onlinetesten, video’s en scenario’s van echte gevallen van cyberaanvallen. Vervolgens delen we onze **ervaringen** tijdens een participatieve en gezellige ‘breakfast meeting’.

Wij hopen op jouw medewerking voor de veiligheid van ons allemaal.

Met vriendelijke groeten,