Cyber
Weerbaarheidscentrum
Greenport

Concrete instructies voor medewerkers

Medewerkers zien meer dan je denkt. Maar wat doen zij als ze denken dat er iets niet klopt? Als ondernemer is het belangrijk om je personeel te laten weten bij wie ze terecht kunnen als ze denken dat er iets niet klopt. Moedig dit soort meldingen aan! Beter één keer teveel dan slachtoffer worden van bijvoorbeeld ransomware.

De volgende concrete zaken kun je bespreken met je medewerkers:

- Maak een procedure voor het melden van incidenten (of opgemerkte kwetsbaarheden) door eigen medewerkers, klanten, gebruikers enzovoorts.

- Vraag personeel expliciet om met regelmaat alert te zijn op:
    - activiteiten buiten normale werktijden
    - aanwezigheid van onbekende bestanden of programma's
    - onverklaarbare waarschuwingsmeldingen van firewall of antivirusprogramma's
    - onverklaarbare aanpassingen aan toegangsrechten van bestanden of folders'
    - aangepaste bestanden of webpagina's
    - uitvoeren van programma's die normaal niet worden gebruikt
    - wijzigingen in DNS-, netwerkrouter- of firewall-configuraties
    - trage systeemprestaties en onverklaarbare crashes
    - pogingen tot het ontfutselen van vertrouwelijke gegevens

- Als je geen (ICT- of security-) expert binnen het bedrijf hebt, laat dan regelmatig een expert naar je netwerk kijken en laat hem/haar de meldingen van het personeel bekijken.

- Maak melding van cybercrime. Het is belangrijk de juiste instanties op de hoogte te brengen van cybercrime, dit om later de geleden schade te kunnen verhalen bij de crimineel, de verzekering en andere instanties.

- Veel vormen van cybercrime zijn sluimerend en zullen geen directe gevolgen hebben voor je reputatie, de continuïteit van je bedrijfsprocessen of directe schade veroorzaken. Echter in geval van crisis is het beter vooraf een draaiboek klaar te hebben:
    - Bepaal welke informatie en/of systemen je zeker nodig hebt voor je bedrijfsvoering.
    - Wat ga je doen als deze uitvallen?
    - Wie moet je inschakelen om de problemen zo snel mogelijk op te lossen?
    - Wie moet je waarschuwen, in welke volgorde, en wat moet de boodschap zijn (deze is waarschijnlijk anders voor personeel, klant, leverancier)?

- Evaluatie. Leer altijd van voorgaande crises.
    - Wat is er gebeurd?
    - Waarom is dit gebeurd?
    - Wat zijn de gevolgen?
    - Hoe kunnen we dit voorkomen?
    - Hoe hebben we gereageerd?
    - Hoe kunnen we onze respons op een crisis als deze verbeteren?

- Procedure bij verzoek om persoonsgegevens in te zien, te wijzigen en/of te verwijderen:
  Als een van je klanten of zakelijke relaties een verzoek indient om persoonsgegevens in te zien, te wijzigen en/of te verwijderen, ben je verplicht om binnen 4 weken schriftelijk of per e-mail te reageren op dit verzoek. Op de website van de Autoriteit Persoonsgegevens(AP) lees je meer over de

rechten van personen waarvan gegevens verzameld worden en de plichten waaraan je je als verwerker van persoonsgegevens dient te houden.

Dit document is gebaseerd op 'Concrete instructies voor medewerkers' van het Digital Trust Center. Het originele document is te vinden via https://www.digitaltrustcenter.nl/concrete-instructies-voor-medewerkers