

KENMERK: B/2024/99/OH DATUM: 08-03-2024
ONDERWERP: Elementen cybersecurity awareness training

KvK Haaglanden 52988368
IBAN: NL20TRIO0212407368
BIC: TRIONL2U

Elementen cybersecurity awareness training

Artikel 13 lid 6 van de Digital Operational Resilience Act (DORA) schrijft voor dat pensioenfondsen bewustmakingsprogramma's op het gebied van ICT-beveiliging ontwikkelen. Ook ontwikkelen pensioenfondsen opleidingen inzake digitale operationele weerbaarheid als verplichte modules in de opleidingsprogramma's voor het personeel.

Welke elementen opgenomen kunnen worden in zo'n bewustmakingsprogramma en/of opleiding, staan hieronder beschreven. Elk pensioenfonds is uniek en dient daarom die onderwerpen te kiezen die zij relevant vindt. Dit document is opgesteld met hulp van de Pensioen ISAC en het Verbond van Verzekeraars.

Bij vragen, neem contact op met Otto Hulst (otto.hulst@pensioenfederatie.nl).

Categorie	Onderwerp	Omschrijving
Internet gebruik	Sterke wachtwoorden en multifactor authenticatie	Gebruik multifactor authenticatie of complexe wachtwoorden en vermijd in ieder geval default instellingen en het gebruik van voor de hand liggende informatie zoals geboortedata of namen.
	Gebruik up-to-date beveiligingssoftware	Zorg voor betrouwbare antivirus- en antimalware software en houd deze up-to-date.
	Houd software en besturingssystemen actueel	Installeer regelmatig updates voor alle software en besturingssystemen in gebruik om bekende beveiligingsproblemen te voorkomen.
	Vermijd openbare wifi voor gevoelige transacties	Voer geen financiële transacties uit of log niet in op persoonlijke accounts wanneer verbonden met openbare wifi-netwerken.

Categorie	Onderwerp	Omschrijving
	Wees voorzichtig met het delen van persoonlijke of bedrijfsgevoelige informatie	Geef nooit persoonlijke-, bedrijfsgevoelige- of financiële informatie vrij, tenzij je zeker weet dat je te maken hebt met een betrouwbare entiteit.
	Bezoek veilige websites	Let op het 'https' voorvoegsel en het slotpictogram in de adresbalk, wat aangeeft dat de website een veilige verbinding gebruikt.
	Download met voorzichtigheid	Download alleen software of bestanden van bekende en betrouwbare bronnen.
	Wees alert op e-mailbijlagen	Open geen bijlagen in e-mails van onbekende afzenders, aangezien deze malware kunnen bevatten.
	Leer en informeer	Blijf op de hoogte van de nieuwste cyberdreigingen en deel deze informatie met collega's.
	Maak regelmatig (persoonlijke) back-ups	Zorg ervoor dat regelmatig back-ups worden gemaakt van belangrijke bestanden en gegevens om verlies te voorkomen.
	Log uit na gebruik	Log uit bij online accounts wanneer gereed.
Phishing	Zorg voor een duidelijke en begrijpbare definitie van phishing	Wat is phishing precies? En wat zijn de verschillende soorten phishing-aanvallen zoals spear phishing, vishing en smishing?
	Deel herkenningstekens van een phishing-poging	Let op verdachte e-mailadressen, spelfouten, urgente of dreigende taal en verzoeken om persoonlijke of financiële informatie.
	Deel de gevolgen van phishing	Benadruk de potentiële schade die kan ontstaan door op een phishing-link te klikken, zoals malware-infecties, financieel verlies en reputatieschade.

Categorie	Onderwerp	Omschrijving
	Veilig gedrag	Niet klikken op verdachte links, geen bijlagen openen van onbekende afzenders en geen persoonlijke informatie verstrekken zonder verificatie.
	Hoe te reageren op een phishing-poging	De juiste stappen ondernemen wanneer een phishing-e-mail is ontvangen, zoals het melden bij de IT-afdeling/contactpersonen.
	Delen voorbeelden van phishing-pogingen	De methoden en technieken van cybercriminelen evolueren voortdurend. Zorg ervoor dat trainingen up-to-date blijven met de nieuwste tactieken.
	Voer simulaties uit	Gebruik gesimuleerde phishing-aanvallen om in een gecontroleerde omgeving te testen.
Veilig uitwisselen van data	E-mail	Op welke manier werkt e-mail en op welke manieren is dit onveilig? Wat kun je hieraan doen?
	Tooling	Heeft de organisatie tooling geïmplementeerd die de gebruiker kan gebruiken om veilig data over te zetten of uit te wisselen?
	Ad hoc versus structureel	Uitwisseling van data op structureel niveau vraagt om een structurele oplossing. Hoe wissel je eenmalig data uit met partijen. Blijft de data daar opgeslagen, hoe borg je dan dat data daar veilig blijft?
	Aanvallen op data	Welke vormen van aanvallen heb je op data uitwisseling (bijvoorbeeld aanval op netwerk, man-in-the-middle etc)?
Basiskennis cybersecurity	Basiskennis fysiek/social engineering	Gebruik voorbeelden van social engineering zodat duidelijk wordt hoe makkelijk het is en hoe echt het is.

Categorie	Onderwerp	Omschrijving
	Malware	Geef inzicht in manieren waarmee malware wordt gebruikt om toegang te verkrijgen, waarbij ook gebruik wordt gemaakt van social engineering.
	Hacking	Hoe denkt een hacker en hoe komt hij binnen (simpele voorbeelden)?
Gedrag en social media	Online gedrag	Koppeling met malware en onveilige sites. Hoe onveilig gedrag zoals klikken op foute links voor grote gevolgen zorgt.
	Social media	Informatie van Facebook, Instagram, X en LinkedIn en hoe dit gebruikt kan worden in aanvallen.
	Reputatieschade	Hoe online gedrag voor grote consequenties kan zorgen. Beleid van organisatie volgen.
	Procedures bij medewerkers en externen onder de aandacht brengen	Bij elke medewerker hoort duidelijk te zijn waar een (vermoeden) van een incident gemeld kan worden. De organisatie moet weten wat als datalek bij de AP/betrokkene gemeld moet worden.
Mobiele apparaten	Gebruik	Wat is geoorloofd gebruik, mag je apps downloaden, kan je je eigen instellingen beheren, mag de gebruiker zijn mobiele apparaat afgeven?
	Risico's	Makkelijk aanloggen op onveilige netwerken, onbeheerd achterlaten van devices, korte afstand hacks (bluetooth, RFID).
	Verlies en diefstal	Beschrijf wat te doen wanneer een mobiel apparaat kwijt is.
Instellingen controleren (gebruiker)	Applicatie en browser	Inschakelen 'Do Not Track'-opties, beperk de toegang van applicaties tot locatiegegevens, contacten, camera,

Categorie	Onderwerp	Omschrijving
		microfoon, etc., tenzij strikt noodzakelijk. Blokkeer ongewenste cookies en houd browser up-to-date.
	Sociale media	Profielen privé of "alleen voor vrienden", beperk de te delen hoeveelheid persoonlijke informatie, schakel geotagging uit en voorzichtig met het delen van jouw locatie.
	Advertentie voorkeuren	Opt-out van gepersonaliseerde advertenties waar mogelijk, gebruik hulpmiddelen om advertentie trackers te blokkeren.
	Mobiele apparaat	Beperk applicatietoestemmingen tot het noodzakelijke minimum, schakel Bluetooth uit wanneer niet in gebruik, vermijd het automatisch verbinden met openbare wifi-netwerken.
	E-mail	Uitschakelen optie om afbeeldingen automatisch te downloaden in e-mails, omdat dit tracking pixels kan activeren, beperk de toegang van derden tot persoonlijke mailbox/agenda.
	Macro's/scripts	Schakel macro's en scripts (zoals powershell) altijd uit/schakel alleen goedgekeurde macro's/scripts van bekende bronnen in.
	Besturingssysteem	Inschakelen automatische updates voor besturingssysteem, beperk delen van bestanden en schakel onnodige services uit.
	Netwerk	Schakel onnodige netwerkdiensten uit.
	Digitale assistenten en smart devices	Beperk de toegang en dataverzameling door digitale

Categorie	Onderwerp	Omschrijving
		assistenten, update regelmatig de firmware van slimme apparaten.
	Netwerk	Firewalls, ingress- en egress-filtering, VPN
Instellingen controleren (IT)	Endpoint	Antivirus- en antimalware-software, persoonlijke firewalls.
	Patches en updates	Besturingssystemen en alle software.
	Toegangscontrole	Sterke authenticatie (bijv. multifactor authenticatie). Maak gebruik van principes als: <ul style="list-style-type: none"> - 'least' privileges - Role based access control - Conditional access control
	Server	Best practices toepassen en daardoor hardenen van servers, uitschakelen van niet-essentiële services.
	Monitoring en logging	Maak gebruik van het loggen van netwerkverkeer en systeemlogs. Breng dit samen in een SIEM (Security Information and Event Management) systeem.
	Draadloos	Sterke encryptie, aanpassing standaard inloggegevens voor draadloze routers.
	Applicaties	Stel een Software Development Lifecycle op (SDLC), maak gebruik van secure coding praktijken bij het ontwikkelen van software.
	Backup en recovery	Herstelprocedures.
	Inzage in 'scope' incident verkrijgen	Op basis van SIEM, SOC en of andere log events inzage verkrijgen in de reikwijdte van het (potentiële incident). Verkrijg inzicht in de impact op de gehele keten en leg deze vast.

Categorie	Onderwerp	Omschrijving
Acties bij (mogelijk) incident	Vastlegging volgorde­lijkheid	Leg vanaf de start van het incident vast: <ul style="list-style-type: none"> – Wie/wat iets heeft gedetecteerd – Welke vervol­gactie is uitgevoerd – Wie betrokken is bij besluitvorming.
	Mogelijke oplossings­richtingen	Bij een mogelijk (groot) incident, overweeg de volgende acties: <ul style="list-style-type: none"> – Beperken toegang tot het onderdeel van de omgeving welke mogelijk gecompromitteerd is; – Bepaal vooraf welke personen in de organisatie de bevoegdheid hebben een besluit te nemen welke impact heeft op de continuïteit van de dienstverlening, zoals bijvoorbeeld het uitschakelen van elke internetconnectiviteit in een deel van de infrastructuur.
	‘Veilig valideren’ van wijzigingen in applicaties	Gebruik voor het testen van wijzigingen binnen applicaties zoveel mogelijk data welke niet herleidbaar is tot personen. Een kopie van een productieomgeving is niet altijd nodig. <p>Bepaal vooraf welke personen in een organisatie mogen besluiten een afwijking hierop te accepteren.</p> <p>Met bovenstaande maatregelen wordt het risico op een datalek verminderd. Per ongeluk gebruik van een e-mailadres van een klant voor testdoeleinden kan dan simpelweg minder makkelijk voorkomen.</p>