



e-learning Informatiebeveiliging en Privacy voor alle medewerkers

5.1.2.e

en

5.1.2.e

Vastgesteld in DB-2024-1008

projectnummer

19 september 2024

samenvatting Het DB wordt gevraagd een e-learning Informatiebeveiliging en Privacybescherming verplicht te stellen voor alle medewerkers

trefwoorden e-learning Informatiebeveiliging en Privacy

1. Inleiding

In de huidige digitale wereld is cybercriminaliteit een steeds grotere bedreiging voor organisaties. De mens, vaak de zwakste schakel in de IT-beveiliging, wordt vaak als doelwit gebruikt om toegang te krijgen tot de systemen. Hackers en andere kwaadwillende worden steeds slimmer en de methodes die ze gebruiken om toegang te krijgen tot informatie worden steeds geavanceerder maar ook het beschikbaar stellen van diensten, zoals Ransomware as a Service, zorgt ervoor dat organisaties steeds vaker doelwit zijn van cybercriminelen.

Naast Informatiebeveiliging is privacybescherming van essentieel belang voor het CBS. De samenleving moet erop kunnen vertrouwen dat het CBS zorgvuldig omgaat met de gegevens die verstrekt worden voor statistische doeleinden en dat verwerking van deze gegevens niet ten koste mag gaan van de rechten en vrijheden van burgers. Waar cybercriminaliteit een bedreiging van buitenaf is, is een onvoldoende privacybescherming een risico van binnenuit. In beide gevallen speelt bewustzijn en gedrag van medewerkers een belangrijke rol in het beschermen tegen cybercriminaliteit en het borgen van een adequate privacybescherming.

Een van de belangrijkste manieren om CBS hiertegen te beschermen is door te investeren in bewustwordingstrainingen. Met zo'n training leer je medewerkers de risico's te kennen van online dreigingen en hoe ze zich hiertegen kunnen beschermen. Ook leren medewerkers wanneer er risico's ontstaan bij gegevensverwerkingen en hoe daarmee dient te worden omgegaan. Deze trainingen kunnen leiden tot een significant verminderd risico op datalekken, phishing-aanvallen en andere cyberincidenten en draagt bij aan een betrouwbaar en veilig CBS waar burgers en bedrijven hun gegevens aan kunnen verstrekken zodat het CBS statistieken kan blijven maken in de toekomst.

Zonder dit vertrouwen zullen burgers en bedrijven geen gegevens meer willen verstrekken aan het CBS.

Voor Informatiebeveiliging is de afgelopen jaren een e-learning opgezet. Sinds augustus 2023 maken alle nieuwe interne medewerkers bij indiensttreding de e-learning Informatiebeveiliging. In navolging van deze e-learning is er momenteel ook een e-learning voor privacybescherming in ontwikkeling. Het voorstel is om beide e-learnings CBS breed verplicht te stellen.

2. Waarom is een organisatie brede training noodzakelijk?

Door de CBS medewerkers te trainen in cyberbeveiliging en privacybescherming kunnen we:

- *het risico verminderen op datalekken.* Medewerkers spelen een belangrijke rol in de beveiliging van een organisatie. Door ze te trainen in het herkennen en vermijden van online dreigingen, en de kennis van een juiste wijze van het omgaan van gegevens te vergroten, kun je het risico op datalekken aanzienlijk verkleinen;
- *weerbaarheid vergroten tegen phishing-aanvallen.* Phishing is een populaire methode die cybercriminelen gebruiken om gevoelige informatie te stelen, zoals wachtwoorden en creditcardnummers. Door je medewerkers te leren hoe ze phishing-aanvallen kunnen herkennen, kun je het aantal slachtoffers binnen je organisatie verminderen;
- *voorkomen van afname van de productiviteit.* Cyberincidenten kunnen leiden tot downtime en productiviteitsverlies. Door je medewerkers te trainen in cyberbeveiliging, kun je het risico op dit soort incidenten verminderen en de productiviteit in stand houden;
- *naleving wet- en regelgeving beter waarborgen.* Veel wet- en regelgeving vereist dat organisaties hun medewerkers trainen in cyberbeveiliging. Door organisatie-brede security trainingen te implementeren, kun je ervoor zorgen dat je organisatie aan deze eisen voldoet. In de AVG en de Wet CBS is bovendien vastgelegd dat je als organisatie alle technische en organisatorische maatregelen moet nemen die mogelijk wordt verwacht kan worden om gegevens te beschermen. Een bewustwordingstraining is een organisatorische maatregel. De medewerkers bij het CBS hebben een groot aandeel in de effectiviteit van cyberbeveiliging en privacyborging aangezien een groot deel van de medewerkers op grote schaal (persoons)gegevens verwerkt;
- *bewustzijn verhogen.* bewustwordingstrainingen kunnen het bewustzijn van je medewerkers over cyberbeveiliging en privacybescherming vergroten. Dit kan leiden tot een meer waakzame en proactieve benadering van IT-beveiliging en privacyborging binnen de hele organisatie.

3. Wet- en regelgeving en frameworks

Awarenes- trainingen op het gebied van cyberveiligheid en privacybescherming zijn maatregelen die voortvloeien uit huidige wet- en regelgeving en frameworks. Daarnaast zijn er ook een aantal (toekomstige) ontwikkelingen waar we rekening mee moeten houden. Hieronder een overzicht van alle huidige en toekomstige wet-en regelgeving en frameworks.

- **De Wet CBS:** artikel 38 van de Wet CBS verplicht het CBS tot het nemen van de nodige technische en organisatorische voorzieningen ter beveiliging van zijn gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.
- **De NIS2-richtlijn:** de NIS2-richtlijn is een Europese richtlijn die de cybersecurity van kritieke infrastructuur en sectoren wil versterken. De richtlijn wordt in Nederland geïmplementeerd in de Cyberveiligheidswet en verplicht organisaties in deze sectoren om passende maatregelen te nemen om hun IT-systemen en -gegevens te beschermen. Dit omvat het trainen van medewerkers in cyberbeveiliging.

- **De AVG:** de AVG is een Europese verordening die regels stelt voor de verwerking van persoonsgegevens in organisatie. De AVG vereist dat organisaties passende technische en organisatorische maatregelen nemen om de persoonsgegevens die zij verwerken te beschermen.
- **De ISO 27001:** de ISO 27001 is een internationale norm voor informatiebeveiliging. De norm bevat eisen voor het trainen van medewerkers in cyberbeveiliging. De norm stelt het volgende:
 - trainen nieuwe medewerkers: in ieder geval binnen de inwerkperiode, liefst binnen een maand (zie norm);
 - trainen alle medewerkers: jaarlijks (zodat zij op de hoogte zijn en blijven van actueel beleid).
- **Norea Privacy Control Framework (PCF):** het PCF is een raamwerk dat is ontwikkeld om organisaties te helpen bij het implementeren van effectieve privacy controls. SAT01 control schrijft het volgende:
 - ten minste eenmaal per jaar wordt voor alle medewerkers een bewustwordingscursus ten aanzien van privacy en beveiliging georganiseerd. Nieuwe medewerkers, contractanten en anderen wordt verplicht om binnen een maand na aanvang van de overeenkomst een vergelijkbare training te volgen, zodat zij op de hoogte zijn van het privacybeleid van de entiteit en de implicaties hiervan.

Door nu te investeren in organisatie-brede trainingen, zijn we ook voorbereid op de toekomstige eisen die aan ons gesteld zullen worden op het gebied van cyberveiligheid.

4. Waarom moet de training verplicht zijn voor alle medewerkers?

Om de maximale effectiviteit van de training te garanderen, is het belangrijk dat alle medewerkers, zowel interne medewerkers maar ook inhuurkrachten, stagiaires, gastonderzoekers en gedetacheerden enz, de training volgen. Dit zorgt voor:

- een consistent niveau van beveiligingsbewustzijn: alle medewerkers hebben dezelfde basiskennis van cyberbeveiliging en privacybescherming, ongeacht hun functie of afdeling;
- een uniforme benadering van IT-beveiliging en privacybescherming: alle medewerkers weten hoe ze zich moeten gedragen om de IT-systemen en -gegevens van de organisatie te beschermen;
- geringer risico op menselijke fouten: menselijke fouten zijn een belangrijke oorzaak van cyberincidenten en datalekken. Door alle medewerkers te trainen, kun je het risico op fouten die kunnen leiden tot datalekken of andere incidenten verminderen.

5. Duur van de training en beschikbaarheid

De training informatiebeveiliging duurt ongeveer 45 minuten per medewerker, de training Privacybescherming circa 30 minuten. De trainingen wordt door de CBS- Academy beschikbaar gesteld via het 5.1.2.e zodat medewerkers deze op een voor hun passend moment kunnen volgen.

Het is de bedoeling dat zowel de training informatiebeveiliging als de training privacybescherming eenmaal per jaar herhaald wordt en regelmatig voorzien wordt van nieuwe content. De trainingen kunnen naar keuze in samenhang gevolgd worden of apart van elkaar.

6. Monitoring

Om te bevestigen dat alle medewerkers de trainingen daadwerkelijk hebben gevolgd, worden de trainingen aangeboden via Casper, en wordt ook voortgang van de trainingen gemonitord via Casper. Medewerkers die de trainingen niet hebben voltooid, zullen worden herinnerd om dit

alsnog te doen. Als de medewerker de trainingen hardnekkig blijft weigeren, dan wordt hier melding van gemaakt bij HR. Bij herhaaldelijke, hardnekkige weigering behoort in uiterste gevallen beëindiging van het dienstverband tot de mogelijk te zetten stappen, binnen de daarvoor geldende wettelijke kaders.

Rapportages over het aantal medewerkers per hoofddirectie dat de training informatiebeveiliging heeft afgerond c.q. nog moet doen of afronden, worden daarnaast ten minste 1x per kwartaal door de CISO aan de CIO worden opgeleverd. Voor de training privacybescherming wordt dit in de Q-rapportage teruggekoppeld per divisie.

7. Advies

Een organisatie-brede bewustwordingstraining is een essentiële investering voor het CBS om zich te beschermen tegen cyberbedreigingen en privacybescherming in het digitale tijdperk. De voordelen van een dergelijke training zijn talrijk en wegen ruimschoots op tegen de kosten bij bijvoorbeeld een cyberaanval en de tijdsbesteding per medewerker.

Geadviseerd wordt daarom om een **verplichte organisatie-brede security en privacy training** te implementeren voor alle medewerkers. Dit betreft dus concreet: alle interne medewerkers, inhuurkrachten, stagiaires, enz, die toegang krijgen tot één of meerdere informatiesystemen van het CBS.

Deze training zal onze organisatie beter voorbereiden op toekomstige cyberbedreigingen, zal een continue zorgvuldige privacybescherming borging en zal helpen om het risico op datalekken, phishing-aanvallen en andere cyberincidenten te verminderen.