

Hoe houd je medewerkers alert?

Kennistoets als instrument

Kennisopbouw van informatiebeveiliging is voor steeds meer organisaties van belang. Veel opleidingen op dit gebied blijken echter te ver te gaan voor de meeste medewerkers. Het hoeven immers niet allemaal security-specialisten te worden. Wel wil je als organisatie bereiken dat een medewerker beschikt over een minimum aan basiskennis. Hoe pak je dit aan?

ANDRÉ VAN SOEST *

De meeste organisaties vinden het steeds belangrijker om medewerkers bewust te maken van de noodzaak om informatie te beveiligen. Daarom plaatst men zoveel mogelijk informatie op het intranet van de organisatie. Daarbij gaan zij er gewoon vanuit dat de medewerkers 'het wel vinden'. Maar hoe weet een organisatie dat medewerkers deze informatie ook daadwerkelijk vinden en raadplegen? En als dit al het geval is, nemen zij het dan voor kennisgeving aan of doen ze er wat mee en gaan zij dan ook bewuster om met informatie? Wat weten we als organisatie eigenlijk over de kennis die medewerkers hebben op het gebied van (informatie)beveiliging? Ervaring leert dat de meeste medewerkers geen vergaande kennis op dat gebied hebben. Iets wat voor de meeste functies ook niet vereist is. Laat staan diploma's of certificaten op dit gebied.

Kennistoets

Organisaties gebruiken een kennis- of een certificatioets voor het vaststellen van de vakbekwaamheid van de medewerker. Je toetst daarbij of een medewerker beschikt over de vereiste basiskennis. Alleen toetsen van deze kennis is slechts een van de zaken die je moet regelen. Het kennisniveau moet men

ook daadwerkelijk vastleggen. Dat kan door een bewijs van bekwaamheid in het personeelsdossier of op een andere wijze vast te leggen.

medewerkers in een organisatie beschikken over een computer met een internet- of intranettoegang en vaak ook over een privécomputer. Hierdoor

Wat weten organisaties eigenlijk over de kennis die medewerkers hebben van informatiebeveiliging?

Op de vraag wat onder basiskennis wordt verstaan, kan men vaak niet een eenduidig antwoord geven. Iedere organisatie zal aan moeten geven wat zijzelf minimaal noodzakelijk vindt dat een medewerker moet weten.

Kennis opnemen

Doordat niet iedereen evenveel tijd nodig heeft om kennis tot zich te nemen, is de klassikale manier niet voor iedereen geschikt. Ook de hoeveelheid tijd en het moment kunnen een rol spelen. Met een kennistoets kunnen medewerkers in het eigen tempo de kennis tot zich nemen. Ze kunnen tussentijds stoppen en op een later tijdstip weer doorgaan, 'just in time'. Op ieder willekeurig moment heeft een medewerker zicht op reeds doorlopen en nog te volgen trainingen en toetsen. De meeste

kan men de kennis ook eventueel thuis verkrijgen. Je hoeft er de deur (of het bedrijf) niet meer voor uit.

Een organisatie wil dat in korte tijd meerdere medewerkers een bepaald basisniveau op het gebied van informatiebeveiliging bereiken en vasthouden. Door gebruik te maken van een interactieve toetsvorm voldoet men aan deze voorwaarden.

Hoe te toetsen?

Over het algemeen wil je de competenties op het gebied van kennis, vaardigheden en houding beoordelen. Om deze competenties te toetsen, maken organisaties vaak gebruik van een combinatie van verschillende methodes. Te denken valt aan meerkeuzevragen, en juist- en onjuistvragen. Het grote voordeel is dat de medewerker aan de

ene kant getoetst wordt over zijn of haar kennis en aan de andere kant na gaat denken over de gestelde situatie. Wat wil je bij de medewerker toetsen? Er kunnen verschillende toetsen zijn voor diverse doelgroepen, bijvoorbeeld een algemene basistoets en een gevorderdentoets. Een toets bestaat veelal uit meerdere onderwerpen. Te denken valt aan vragen over veiligheid rond de werkplek, wachtwoorden, fysieke veiligheid, social engineering en technische beveiliging. Maar ook over onderwerpen als risicomanagement, integriteit, privacy, BHV, vakspecifieke toetsen, et cetera. Per toets worden (per onderwerp) een aantal relevante vragen

(meestal random) geselecteerd uit een vragendatabase.

Feedback

Na het beantwoorden van een vraag is het belangrijk dat een medewerker direct feedback krijgt. Om feedback te geven zijn er verschillende manieren mogelijk:

- » Aan het eind van de toets aangeven of men geslaagd of gezakt is, en welke vragen fout beantwoord zijn. Eventueel voorzien van uitleg.
- » Direct na iedere vraag aangeven of een gegeven antwoord correct is, eventueel voorzien van uitleg als een antwoord fout is.

Deze laatste manier zorgt ervoor dat niet alleen een toetsing van de kennis plaatsvindt, maar ook dat de medewerker direct na het beantwoorden van de vraag weet of het goed dan wel fout beantwoord is. Als het gegeven antwoord fout is, is het vanwege het lerend effect verstandig om te laten zien waarom het gegeven antwoord fout is en wat het juiste antwoord was met een uitleg 'waarom'. Verwijzingen (hyperlinks) naar informatie op het intranet van de organisatie, alsmede documenten zoals bijvoorbeeld een informatiebeveiligingsbeleid, instructies en formulieren, maken het geheel compleet. Door een nieuwe vraag over hetzelfde »



onderwerp te stellen worden kennis en inzicht in het onderwerp verhoogd. Het is prettig en stimulerend voor degene die de toets doet om een bevestiging te krijgen dat hij of zij goed bezig is. Daarnaast zullen mensen ook niet altijd zeker zijn van hun antwoord en dus gokken. Ook voor die gevallen is het goed aan te reiken waarom het gegeven antwoord het goede antwoord is. Als organisatie wil je graag feedback van medewerkers ontvangen over hoe

steeds bezit. Is dit het geval, dan kan de medewerker een nieuw persoonlijk certificaat afdrukken – met geldigheidskenmerken van de specifieke periode. Is dit niet het geval, dan krijgt de medewerker de foute antwoorden uitgelegd en nieuwe vragen ter beantwoording aangeboden. Omdat de bekwaamheid (en geldigheid van het certificaat) van de medewerker automatisch op een certificatielijst wordt geplaatst, kunnen rapportages

sen verschillende doelgroepen. Voor de ene organisatie kan dat handig zijn, omdat je dan zeker weet dat een ieder over hetzelfde kennisniveau beschikt. Soms wil je als organisatie toch een onderscheid maken tussen bepaalde doelgroepen. Op het gebied van informatiebeveiliging wil je in ieder geval de mogelijkheid hebben om te differentiëren. Specifieke doelgroepen zijn bijvoorbeeld: het management, standaardmedewerkers en ICT-beheerders c.q. -ontwikkelaars. De mogelijkheid om trainingen en toetsen af te stemmen op verschillende doelgroepen is voor een kennistoets zeer wenselijk.

Om effectief te borgen kan een periodiek awareness-programma behulpzaam zijn

zij de toets hebben ervaren, of zij suggesties hebben om de kwaliteit van de toets te vergroten, et cetera. Door medewerkers actief te betrekken bij het verbeteren van de informatiebeveiliging én de kennistoets zul je medewerkers willen aanmoedigen om via een vrij invoerveld terugkoppeling te geven.

Score en bewijs

Medewerkers vinden het niet alleen belangrijk om direct te weten wat gescoord is, maar willen ook weten hoe ver men nog verwijderd is om te slagen voor het betreffende onderdeel en uiteindelijk voor de gehele toets. Als resultaat voor het succesvol doorlopen van de basis- of de gevorderde toets wil je als organisatie de medewerker belonen met een tastbaar bewijs, bijvoorbeeld een certificaat. Medewerkers die met succes de voor hen bedoelde toetsen hebben doorlopen, kunnen vervolgens een eigen certificaat afdrukken als bewijs van bekwaamheid en komen automatisch op een certificatielijst. Als organisatie kun je ervoor kiezen om de geldigheid van een certificaat beperkt geldig te laten zijn, zoals we dat ook kennen voor een middelbare-schooldiploma. Je kunt er ook voor kiezen om de geldigheid van het certificaat te beperken (bijvoorbeeld een jaar), zoals dat bijvoorbeeld ook binnen de gezondheidszorg en (informatie)beveiligingsbranche gebruikelijk is. Is deze periode verstreken, dan kan de medewerker opnieuw een test doen om te toetsen of hij het gewenste niveau nog

inzichtelijk maken welke medewerkers de toets volbracht hebben. Een overzicht van de gecertificeerden kan richting het management, de in- of externe auditor, et cetera dienen als 'bewijsstuk'.

Borgen

Nadat medewerkers de kennistoets succesvol hebben doorlopen, wil je als organisatie er zeker van zijn dat de opgedane kennis ook daadwerkelijk de medewerkers bijblijft zodat ze die kennis kunnen toepassen op het moment dat ze nodig is: bij voorkeur minimaal ruim voorafgaande aan een aanstaand incident. Alleen het regelmatig gebruik van deze kennis tijdens de dagelijkse werkzaamheden zorgt voor kennisbehoud. Om effectief te borgen kan bijvoorbeeld een periodiek awareness-programma behulpzaam zijn.

Doelgroepen

Een organisatie kan ervoor kiezen om een algemene basistoets en een gevorderdetoets door alle medewerkers te laten maken, zonder onderscheid tus-

Analyse

Als informatiebeveiligingsverantwoordelijke wil je op een bepaald moment weten welke medewerkers de algemene en gevorderde toetsen hebben doorlopen (en gecertificeerd zijn). De 'kennistoets'-applicatie zal de mogelijkheid moeten hebben om op ieder willekeurig moment standaardrapportages zonder tussenkomst van de leverancier te genereren. Deze zullen bijvoorbeeld de volgende inzichten verschaffen:

- » probleemgebieden via analyse van foute beantwoording;
- » medewerkers gesorteerd naar organisatorische eenheid;
- » zijn alle toetsen doorlopen en wat zijn de resterende onderdelen;
- » feedback van deelnemers (verbetersuggesties, commentaar).

Je wilt ook wat kunnen doen met de feedback van de medewerkers. De coördinator zou vragen en toetsen moeten kunnen activeren en deactiveren en een vraag kunnen aanpassen aan bijvoorbeeld een actuele situatie. «

* André van Soest is adviseur bij LBVD Informatiebeveiligers, www.lbvd.nl

Samenvatting

- » De meeste organisaties vinden het steeds belangrijker om medewerkers bewust te maken van de **noodzaak** om **informatie te beveiligen**.
- » Maar wat weten organisaties eigenlijk over de **kennis** die hun medewerkers hebben op het gebied van (informatie)beveiliging?
- » Met een **kennis-** of een **certificatietoets** kunnen organisaties vaststellen wat de vakbekwaamheid van de medewerkers is. Daarbij wordt getoetst of een medewerker beschikt over de vereiste basiskennis.