GIDS

De complete gids voor security awareness e-learning platforms

Platformfuncties, kosten, LMS-integratie, NIS2-rapportage en selectiecriteria. Voor het Nederlandse MKB.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Een security awareness e-learning platform is de softwarelaag die training levert, meet en rapporteert. Het verschil met losse trainingen? Schaalbaarheid, automatisering en aantoonbare compliance.

60%
van alle datalekken heeft een menselijke factor als oorzaak
Verizon DBIR 2025 [1]

86%
reductie in phishing-klikken na 12 maanden doorlopende platformtraining
KnowBe4 Benchmark 2025 [2]

EUR 6--72
per medewerker per jaar -- de bandbreedte voor platformlicenties in 2026
Symbol Security / Gartner [3]

43%
hogere activatiegraad bij platforms met gamification
SoSafe Gamification Report [4]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet -- awareness training wordt verplicht
Digitale Overheid [5]

4:1
gemiddelde ROI -- elke EUR 1 geinvesteerd levert EUR 4 op aan vermeden schade
Arctic Wolf / diverse bronnen [6]

700%
stijging deepfake-fraude jaar-op-jaar -- platforms moeten meegroeien
FTC / Trend Micro [7]

50%
van bedrijven (10+ medewerkers) maakt geen risicoanalyse
CBS Cybersecuritymonitor 2024 [8]

1. Wat is een awareness e-learning platform?

Een security awareness e-learning platform is een SaaS-oplossing die trainingsmodules levert, gebruikersvoortgang bijhoudt, phishing-simulaties uitvoert en compliance-rapportages genereert. Het is het gereedschap -- niet de training zelf.

PLATFORM VS TRAINING

Het onderscheid is cruciaal. "Security awareness training" is de inhoud: de kennis die je overdraagt. Het "e-learning platform" is de software die je gebruikt om die training te leveren, te personaliseren, bij te houden en aantoonbaar te maken. [9]

Vergelijk het met een LMS (Learning Management System) voor cybersecurity. Sommige platforms focussen puur op content delivery, andere bieden een compleet ecosysteem met phishing-simulaties, rapportage, gamification en integraties met je bestaande IT-omgeving.

KERNCOMPONENTEN VAN EEN PLATFORM

> **Content library:** Vooraf gemaakte trainingsmodules -- video's, interactieve oefeningen, quizzen, infographics. Varieerend van 50 tot 1.300+ modules. [10]
>
> **Delivery engine:** Automatische toewijzing, herinneringen, planning en escalatie bij niet-voltooiing.
>
> **Simulatie-engine:** Phishing-simulaties, en bij geavanceerde platforms ook vishing (voice phishing) en deepfake-simulaties.
>
> **Analytics dashboard:** Voltooiingspercentages, scores, risiconiveaus per medewerker, afdeling en organisatie.
>
> **Compliance module:** Auditlogs, rapportage-exports, NIS2-compliance dashboards.

WIE HEEFT ER EEN NODIG?

Elke organisatie met meer dan 10 medewerkers die serieus is over cybersecurity. Specifiek:

- Organisaties die onder NIS2/Cyberbeveiligingswet vallen (essentieel of belangrijk)
- Bedrijven die een cyberverzekering willen afsluiten of behouden
- Organisaties die ISO 27001 gecertificeerd zijn of willen worden
- MKB-bedrijven die nu ad-hoc trainingen doen en willen professionaliseren

PRAKTIJKTIP

Een platform is niet hetzelfde als een eenmalige cursus. De waarde zit in de doorlopende levering, automatisering en meetbaarheid. Als je alleen een jaarlijkse presentatie wilt geven, heb je geen platform nodig -- maar mis je ook het NIS2-bewijs. [11]

2. Waarom is het belangrijk?

Ad-hoc trainingen zijn als een brandoefening die je een keer per jaar doet en dan hoopt dat iedereen het onthoudt. Een platform maakt van awareness een doorlopend proces -- met meetbare resultaten.

DE MENSELIJKE FACTOR

60% van alle datalekken heeft een menselijke factor als oorzaak. [1] Credential abuse veroorzaakt 32% van de breaches, gevolgd door social engineering (23%) en gebruikersfouten (14%). [1] Dit zijn geen technische problemen -- het zijn gedragsproblemen. En gedrag verander je niet met een PowerPoint per jaar.

VAN AD-HOC NAAR DOORLOPEND

ASPECT	AD-HOC TRAINING	E-LEARNING PLATFORM
Frequentie	1-2x per jaar	Doorlopend, maandelijks
Personalisatie	Iedereen krijgt hetzelfde	AI-gestuurd per medewerker
Meetbaarheid	Handtekening op presentielijst	Scores, klikpercentages, trends
NIS2-bewijs	Moeilijk aantoonbaar	Automatisch gegenereerd
Schaalbaarheid	Max 20-30 per sessie	Onbeperkt
Kosten per medewerker	EUR 100--500/jaar	EUR 6--72/jaar
Vergeetcurve	80% vergeten in 4 weken	Spaced repetition bestrijdt dit

DE BUSINESS CASE

De gemiddelde ROI van een awareness-platform is 4:1 -- elke EUR 1 geinvesteerd levert EUR 4 aan vermeden schade op. [6] Organisaties met robuuste awareness-programma's besparen gemiddeld USD 1,5 miljoen aan breach-gerelateerde kosten. [12] Employee training vermindert de gemiddelde breach-kosten met USD 232.867. [12]

REKENVOORBEELD: 100 MEDEWERKERS

- Platformkosten: EUR 2.400--3.600 per jaar
- Implementatie eenmalig: EUR 2.000
- Verwachte incidentreductie: 40--60%
- Vermeden schade bij 1 voorkomen incident: EUR 270.000
- Break-even: na het voorkomen van 1 klein incident

INDIRECTE VOORDELEN

- Lagere cyberverzekeringspremie -- verzekeraars geven 10--25% korting bij aantoonbaar awareness-programma [13]
- NIS2-compliance -- vermijden van boetes tot EUR 10 miljoen [5]
- Snellere incidentmelding door medewerkers
- Betere audit-resultaten (ISO 27001, SOC 2)

3. Hoe werkt het?

Een awareness e-learning platform werkt in drie lagen: content delivery, tracking en rapportage. Hieronder leggen we elk onderdeel uit.

CONTENT DELIVERY

Het platform levert trainingsmodules aan je medewerkers. Dit kan op verschillende manieren:

MODEL	HOE HET WERKT	VOORDEEL	NADEEL
Standalone portaal	Medewerkers loggen in op het portaal van de leverancier	Snel operationeel, geen eigen LMS nodig	Nog een tool erbij voor medewerkers
SCORM-integratie	Content als SCORM-pakket in je bestaand LMS	Centraal leerportaal, bekende omgeving	Beperktere interactiviteit
API-first	Platform levert via API aan je eigen omgeving	Maximale flexibiliteit	Technische expertise nodig
Hybrid	Eigen portaal + SCORM export + API	Beste van beide werelden	Complexere setup

SCORM-standaarden

SCORM (Sharable Content Object Reference Model) is de standaard voor communicatie tussen e-learning content en een LMS. [14] De belangrijkste versies:

- **SCORM 1.2:** Meest breed ondersteund. Basistracking: voltooiing en score.
- **SCORM 2004:** Geavanceerder met sequencing en bookmarking. Minder breed ondersteund.
- **xAPI (Tin Can):** Modernste standaard. Rijke data, maar beperkte LMS-ondersteuning.
- **cmi5:** Combineert xAPI en LMS-functies. Opkomend.

TRACKING EN VOORTGANG

Een goed platform trackt minimaal:

- Voltooiingspercentage per module per medewerker
- Gemiddelde score op kennistoetsen
- Phishing-simulatie resultaten (geklikt, gerapporteerd, geen actie)
- Tijdbesteding per module
- Herhalingsfrequentie en trend over tijd
- Compliance-status per afdeling

RAPPORTAGE EN COMPLIANCE

De rapportagefunctie is wat een platform onderscheidt van losse trainingen. Je hebt exports nodig voor:

> **NIS2-audits:** Bewijs dat medewerkers periodiek getraind zijn, met scores en voltooiingsdata.
>
> **ISO 27001 (A.6.3):** Aantoonbaar awareness-programma met effectiviteitsmeting.
>
> **Cyberverzekeraars:** Dashboards die laten zien dat je actief aan awareness werkt.
>
> **Management:** Risicoscores en trends op organisatieniveau.

AUTOMATISERING

Het platform neemt operationeel werk over:

- **Onboarding:** Nieuwe medewerkers krijgen automatisch een startprogramma
- **Herinneringen:** Automatische e-mails bij niet-voltooiing
- **Escalatie:** Melding aan manager als deadline verloopt
- **Hertoewijzing:** Periodieke trainingen worden automatisch opnieuw ingepland
- **Risico-triggers:** Extra training na een phishing-klik of ander risicogedrag

PRAKTIJKTIP

Vraag bij de demo altijd hoe de automatisering werkt. Een platform zonder goede automatisering geeft je evenveel werk als handmatig plannen -- je betaalt dan voor een dure content library.

4. Wat kost het?

Platformprijzen lopen uiteen van EUR 6 tot EUR 72 per medewerker per jaar. De variatie hangt af van platformtype, functionaliteit en contractvorm.

PRIJSMODELLEN

TYPE PLATFORM	PER USER/MAAND	PER USER/JAAR	DOELGROEP
Basis SaaS (MKB)	EUR 0,50--1,25	EUR 6--15	10--100 medewerkers
Mid-range SaaS	EUR 1,25--3,00	EUR 15--36	100--500 medewerkers
Enterprise	EUR 2,50--5,00	EUR 30--60	500+ medewerkers
Premium/specialist	EUR 4,00--6,00	EUR 48--72	Gereguleerde sectoren

Gemiddelde marktprijs in 2026: circa EUR 35 per user per jaar. [3] Volumekortingen van 10--25% bij 50+ gebruikers zijn standaard.

VERBORGEN KOSTEN

> **LET OP**
> De licentieprijs is niet alles. Reken ook met implementatie (EUR 500--5.000), SCORM-integratie (EUR 500--3.000), SSO-setup (EUR 1.000--5.000), vertaling naar Nederlands (EUR 2.000--8.000 als niet standaard beschikbaar), en custom content (EUR 1.000--10.000 per module).

REKENVOORBEELDEN

MKB -- 50 medewerkers

KOSTENPOST	JAAR 1	JAAR 2+
Platformlicentie	EUR 1.200	EUR 1.200
Implementatie	EUR 1.500	--
SSO-integratie	EUR 1.000	--
Totaal	EUR 3.700	EUR 1.200

KOSTENPOST	JAAR 1	JAAR 2+
Per medewerker	EUR 74	EUR 24

Middelgroot -- 200 medewerkers

KOSTENPOST	JAAR 1	JAAR 2+
Platformlicentie	EUR 6.000	EUR 6.000
Implementatie + integraties	EUR 4.000	--
Totaal	EUR 10.000	EUR 6.000
Per medewerker	EUR 50	EUR 30

BUDGETTIP

Vraag altijd een pilot aan voor 10--20 medewerkers. De meeste platforms bieden dit gratis of tegen gereduceerd tarief. Zo test je de kwaliteit voordat je commit aan een jaarcontract.

5. Waar moet je op letten?

De keuze voor een platform bepaalt of je awareness-programma slaagt of faalt. Hieronder de criteria die ertoe doen, gerangschikt op prioriteit.

MUST-HAVE CRITERIA

1. Nederlandse taalondersteuning

Native Nederlandse content is een harde eis. Machine-vertaalde modules worden herkend door medewerkers en ondermijnen de geloofwaardigheid. [15] Let op het verschil: "beschikbaar in 35 talen" betekent niet dat de Nederlandse versie goed is. Vraag altijd om een Nederlandstalige demo.

2. Geintegreerde phishing-simulaties

Een platform zonder simulaties is een halve oplossing. Kennis testen in de praktijk is wat gedrag verandert. Controleer of simulaties in de licentie zitten of apart kosten.

3. NIS2-rapportage

Met de Cyberbeveiligingswet op komst (Q2 2026) [5] heb je compliance-dashboards en auditlogs nodig. Een platform dat geen kant-en-klare NIS2-rapportages biedt, kost je extra werk bij audits.

4. SCORM-compatibiliteit

Als je al een LMS hebt (Moodle, Cornerstone, SAP SuccessFactors), moet het platform SCORM-pakketten kunnen exporteren. Controleer of het SCORM 1.2 of 2004 is, en of voortgangsdata teruggekoppeld wordt. [14]

5. Automatische toewijzing

Trainingen moeten automatisch toegewezen worden op basis van rol, afdeling en risicoprofiel. Handmatig toewijzen schaalt niet bij 50+ medewerkers.

6. SSO-integratie

Single Sign-On via Azure AD of Google Workspace verlaagt de drempel. Zonder SSO krijg je lage adoptie.

7. AVG-compliant dataverwerking

Data moet in de EU opgeslagen worden. Een verwerkersovereenkomst moet beschikbaar zijn. Check ook of het platform medewerkerdata deelt met derden.

NICE-TO-HAVE CRITERIA

FEATURE	WAAROM HET WAARDEVOL IS
Gamification	43% hogere activatiegraad [4]

FEATURE	WAAROM HET WAARDEVOL IS
Adaptive learning	30--40% minder trainingstijd, 20--35% betere retentie
Micro-learning	Modules van 3--5 min passen beter in de werkdag
Deepfake-simulaties	Bescherming tegen de snelstgroeiende dreiging [7]
Human Risk Score	Individuele risicoscore per medewerker voor gerichte interventie
API-koppelingen	Integratie met HR-systeem en security tools
Custom content builder	Eigen modules maken voor specifieke situaties

FEATURE-MATRIX PER PLATFORMNIVEAU

- **Budget (EUR 6--15/user/jaar):** 50--150 modules, 5--10 talen, basis phishing, basis rapportage
- **Mid-range (EUR 15--36/user/jaar):** 200--500 modules, 15--25 talen, aanpasbare simulaties, uitgebreide rapportage + export, gamification
- **Enterprise (EUR 36--72/user/jaar):** 800--1.300+ modules, 30--40+ talen, AI-gedreven simulaties, deepfakes, custom + API, dedicated support

6. Veelgemaakte fouten

De meeste mislukte awareness-programma's falen niet door het platform -- maar door de aanpak. Deze tien fouten zien we keer op keer.

1. Alleen op prijs selecteren

Het goedkoopste platform zonder goede Nederlandse content levert niets op. Je betaalt weinig, maar je medewerkers leren niets. De werkelijke kosten zijn de incidenten die je niet voorkomt.

2. Geen integratie met bestaand LMS

Twee losse portalen betekent dubbele administratie en lagere adoptie. Als je al een LMS hebt, controleer SCORM-compatibiliteit voor je tekent.

3. De content library niet evalueren

Demo-modules zijn vaak de beste die een platform heeft. Vraag om toegang tot de volledige library en bekijk minstens 10 willekeurige modules. Let op kwaliteit, relevantie en vertaling.

4. Geen pilot draaien

Een pilot met 10--20 medewerkers kost je twee weken en bespaart je een jaarcontract met het verkeerde platform. Test met een mix van tech-savvy en minder digitaal vaardige medewerkers.

5. Alleen e-learning, geen simulaties

Kennis zonder praktijktoets is onvoldoende voor NIS2-compliance. Phishing-simulaties zijn minstens zo belangrijk als de trainingsmodules zelf. [2]

6. Jaarlijks in plaats van doorlopend

80% van nieuwe kennis wordt vergeten binnen vier weken zonder herhaling. [16] Een jaarlijkse training is weggegooid geld. Kies een platform dat maandelijkse micro-learnings en spaced repetition ondersteunt.

7. Management niet meenemen

NIS2 vereist dat bestuursleden training volgen. [5] Als de directie niet meedoet, neemt niemand het serieus. Het platform moet een aparte management-track bieden.

8. Geen baseline meting

Zonder nulmeting kun je verbetering niet aantonen. Doe voor implementatie een baseline phishing-test en kennismeting. Vergelijk na 3, 6 en 12 maanden.

9. Rapportage niet testen

Veel platforms tonen mooie dashboards in de demo, maar de exports zijn beperkt. Test of de rapporten werkelijk aan NIS2- en audit-eisen voldoen voordat je tekent.

10. Vertaald als "Nederlands" accepteren

Machine-vertaalde content met Belgische of Vlaamse taalconstructies ondermijnt de geloofwaardigheid. Vraag expliciet naar native Nederlandse content en controleer dit zelf.

> **WAARSCHUWING**
>
> De combinatie van fout 6 (jaarlijks) en fout 8 (geen baseline) maakt het onmogelijk om aan NIS2-auditvereisten te voldoen. Je hebt doorlopende training en meetbare verbetering nodig.

7. NIS2: wat wordt verplicht?

De Cyberbeveiligingswet (NIS2-implementatie) maakt doorlopende awareness-training verplicht. Hieronder wat dat concreet voor jouw platform-eisen betekent.

DE WETTELIJKE BASIS

De NIS2-richtlijn (EU 2022/2555) wordt in Nederland geimplementeerd via de Cyberbeveiligingswet, verwacht in werking Q2 2026. [5] Twee artikelen zijn direct relevant voor awareness-platforms:

> **Artikel 20 (lid 2) -- Bestuurstraining:** Bestuursorganen van essentiële en belangrijke entiteiten moeten training volgen. Organisaties worden aangemoedigd vergelijkbare training aan alle medewerkers aan te bieden.
>
> **Artikel 21 (lid 2, sub g) -- Cyberhygiëne:** "Basisuitoefeningen op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging" is een van de 10 verplichte risicobeheermaatregelen.

WAT JE PLATFORM MOET KUNNEN

NIS2-EIS	PLATFORMVEREISTE
Periodieke training	Automatische hertoewijzing op vaste intervallen
Risico-gebaseerd	Toewijzing op basis van rol en risicoprofiel
Bestuurstraining	Aparte track voor directie met governance-focus
Effectiviteitsmeting	Scores, trends en verbetering over tijd aantoonbaar
Incidentherkenning	Modules over herkennen en melden van incidenten
Auditlog	Onveranderbaar logboek van alle trainingsactiviteiten
Rapportage	Export naar CSV/PDF voor toezichthouder (RDI)
Functie-relevant	Training relevant voor de functie van de medewerker

SANCTIES

BOETES BIJ NIET-NALEVING

- **Essentiële entiteiten:** boetes tot EUR 10 miljoen of 2% wereldwijde omzet
- **Belangrijke entiteiten:** boetes tot EUR 7 miljoen of 1,4% wereldwijde omzet
- **Bestuurders:** persoonlijk aansprakelijk -- ook als ze zelf geen training hebben gevolgd

MELDPLICHT EN TRAINING

Bij significante incidenten gelden strikte meldtermijnen: 24 uur vroege waarschuwing, 72 uur gedetailleerd rapport, en maandelijks eindrapport. [5] Je platform moet modules bevatten die medewerkers leren wanneer en hoe ze een incident moeten melden.

PRAKTIJKTIP

Vraag de leverancier naar een NIS2-compliance mapping: een document dat per NIS2-artikel laat zien hoe het platform eraan bijdraagt. Geen mapping = niet voorbereid op de Nederlandse markt.

8. E-learning platform vs phishing simulatie vs classroom

Drie vormen van awareness, drie verschillende doelen. Het platform combineert idealiter alle drie, maar het is belangrijk om de verschillen te snappen.

ASPECT	E-LEARNING PLATFORM	PHISHING SIMULATIE TOOL	CLASSROOM TRAINING
Focus	Kennis + gedrag via digitale modules	Gedrag testen via gesimuleerde aanvallen	Kennis overdracht in groep
Format	Online, zelfgestuurd	E-mail simulaties	Live sessies
Frequentie	Doorlopend, maandelijks	Maandelijks/kwartaal	1--4x per jaar
Schaalbaarheid	Hoog (onbeperkt users)	Hoog	Laag (max 20--30 per sessie)
Personalisatie	AI-driven adaptive	Beperkt (per afdeling)	Trainer-afhankelijk
Meetbaarheid	Volledig (scores, voltooiing)	Klikpercentages	Beperkt (evaluatieformulier)
NIS2-bewijs	Automatisch	Deels	Handmatig
Kosten/user/jaar	EUR 6--72	EUR 3--25	EUR 100--500

WANNEER KIES JE WAT?

> **E-learning platform als basis:** Voor doorlopende kennisoverdracht en compliance-bewijs. Dit is je fundament.
>
> **Phishing simulatie als aanvulling:** Om kennis te testen in de praktijk. De meeste e-learning platforms bieden dit geintegreerd.
>
> **Classroom als verdieping:** Voor kick-offs, teamspecifieke scenario's en menselijke interactie. Gebruik het voor de start en voor jaarlijkse verdieping, niet als vervanging.

DE IDEALE COMBINATIE

De effectiefste aanpak combineert alle drie: een e-learning platform als doorlopende basis (maandelijks), phishing-simulaties om gedrag te testen (maandelijks/kwartaal), en periodieke classroom-sessies voor verdieping en teambuilding (1--2x per jaar). Veel moderne platforms bieden de eerste twee geintegreerd.

PRAKTIJKTIP

Als je budget beperkt is, start met een platform dat e-learning en phishing-simulatie combineert. Voeg classroom-sessies toe als het budget het toelaat. Begin niet andersom -- classroom zonder platform is niet aantoonbaar voor NIS2.

9. Trends 2025--2026

De markt voor awareness e-learning platforms beweegt snel. Hieronder de acht trends die je selectie en verwachtingen moeten kleuren.

1. AI-gedreven personalisatie

Platforms gebruiken AI om individuele leertrajecten samen te stellen. OSINT-driven personalisatie gaat verder: simulaties worden gebaseerd op de digitale footprint van de medewerker -- welke informatie is online vindbaar en hoe kan een aanvaller die gebruiken? [7]

2. Deepfake en voice phishing simulaties

Deepfake-fraude steeg 700% jaar-op-jaar. [7] Vooruitstrevende platforms voegen voice phishing (vishing) en video deepfake-simulaties toe. "Deepfake-as-a-Service" maakt deze dreiging ook voor het MKB relevant.

3. Convergentie met security tools

Platforms integreren steeds vaker met SIEM, SOAR en email security gateways. Risicogedrag in de inbox triggert automatisch extra training. "Human Risk Management" wordt het overkoepelende concept. [10]

4. Compliance-driven adoptie

NIS2, ISO 27001:2022 (control A.6.3), DORA (financiele sector), en eisen van cyberverzekeraars maken awareness-platforms vrijwel verplicht. De vraag verschuift van "moeten we dit doen?" naar "welk platform kiezen we?"

5. Behavioral science integratie

Nudging in de dagelijkse workflow: browser-extensies die waarschuwen bij verdachte links, e-mail banners bij externe afzenders, en real-time coaching bij risicogedrag. De focus verschuift van "weten" naar "doen".

6. Multi-channel delivery

Niet alleen via desktop: mobiele apps, Slack/Teams-integratie, SMS en push notificaties. "Training in the flow of work" vervangt het aparte leerportaal. Micro-interventies op het juiste moment.

7. Human Risk Scoring

Van "wie heeft de training afgemaakt" naar "wie vormt een risico". Predictive analytics identificeren welke medewerkers kwetsbaar zijn voor specifieke aanvalstypes. Benchmarking tegen branchegemiddelden geeft context.

8. Nederlandse content en context

Groeiende vraag naar native Nederlandse content -- niet vertaald, maar geschreven voor de Nederlandse markt. Sector-specifieke modules (zorg, overheid, financieel), AVG-specifieke trainingen, en integratie van NCSC-waarschuwingen in content.

WAAR HET NAARTOE GAAT

Het awareness e-learning platform van 2026 is geen los leersysteem meer. Het is een geintegreerd onderdeel van je security stack dat risico meet, gedrag beinvloedt en compliance aantoonbaar maakt -- geautomatiseerd en gepersonaliseerd.

10. Aan de slag

Je weet nu wat een awareness e-learning platform is, wat het kost en waar je op moet letten. Hieronder het stappenplan om van selectie naar operationeel te komen.

1 Meet je baseline

WEEK 1--2

Doe een baseline phishing-test voordat je een platform kiest. Stuur een simulatie-phishing naar alle medewerkers en meet het klikpercentage. Dit is je nulmeting waartegen je verbetering afzet. Veel platforms bieden dit als gratis trial aan.

2 Stel je eisen vast

WEEK 2--3

Bepaal je must-haves: NIS2-rapportage, Nederlandse taal, SCORM-integratie, SSO. Gebruik de selectiechecklist op ibgids.nl/awareness-elearning om niets te vergeten. Betrek IT, HR en management bij de eisenlijst.

3 Maak een shortlist

WEEK 3--4

Selecteer 3--5 platforms die aan je must-haves voldoen. Vraag demo's aan en controleer specifiek de Nederlandse content kwaliteit, de rapportage-exports en de SCORM-compatibiliteit.

4 Draai een pilot

WEEK 4--6

Test met 10--20 medewerkers -- een mix van digitaal vaardige en minder vaardige collega's. Meet voltooiingspercentage, gebruikerstevredenheid en kwaliteit van de Nederlandse modules.

5 Implementeer en communiceer

WEEK 6--8

Configureer het platform (branding, afdelingen, rollen), richt SSO in, en stel de eerste trainingsreeks in. Communiceer naar alle medewerkers waarom dit gebeurt -- en dat de directie ook meedoet.

6 Meet, rapporteer, verbeter

DOORLOPEND

Na 3 maanden: vergelijk met je baseline. Na 6 maanden: eerste managementrapportage. Na 12 maanden: evaluatie en contractbeslissing. Gebruik de data om je programma bij te sturen.

Hulp nodig bij het kiezen? Op **ibgids.nl/word-gematcht** koppelen we je gratis en vrijblijvend aan aanbieders die passen bij jouw organisatiegrootte, sector en eisen. Je ontvangt binnen 48 uur vergelijkbare offertes.

Bronnenlijst

[1] **Verizon Data Breach Investigations Report 2025.** https://www.verizon.com/business/resources/reports/dbir/

[2] **KnowBe4 Phishing Industry Benchmarks 2025.** https://www.knowbe4.com/phishing-benchmarks

[3] **Symbol Security -- Security Awareness Training Pricing Guide 2026.** https://symbolsecurity.com/blog/security-awareness-training-cost-2026-complete-pricing-guide/

[4] **SoSafe Gamification Report.** https://sosafe-awareness.com/resources/reports/gamification/

[5] **Digitale Overheid / Rijksdienst voor Identiteitsgegevens (RDI) -- Cyberbeveiligingswet update.** https://business.gov.nl/amendments/nis2-directive-protects-network-information-systems/

[6] **Arctic Wolf -- Value of Security Awareness Training.** https://arcticwolf.com/resources/blog/calculating-roi-for-security-awareness-training/

[7] **FTC / Trend Micro Security Predictions 2026.** https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/

[8] **CBS Cybersecuritymonitor 2024.** https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[9] **Gartner Peer Insights -- Security Awareness CBT Reviews 2026.** https://www.gartner.com/reviews/market/security-awareness-computer-based-training

[10] **Expert Insights -- Top Security Awareness Training Solutions 2026.** https://expertinsights.com/security-awareness-training/the-top-security-awareness-training-platforms-for-businesses

[11] **NIS2 Directive Article 20 & 21.** https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html

[12] **IBM Cost of a Data Breach Report 2025.** https://www.ibm.com/reports/data-breach/action-guide

[13] **Keepnet Labs -- Security Awareness Training Statistics 2026.** https://keepnetlabs.com/blog/security-awareness-training-statistics

[14] **Keepnet Labs -- SCORM Proxy for LMS Integration.** https://keepnetlabs.com/blog/keepnet-s-scorm-proxy-revolutionizing-security-awareness-training-with-lms-integration

[15] **Guardey -- Security Awareness Training Software Tools 2026.** https://www.guardey.com/security-awareness-training-software/

[16] **Ebbinghaus-vergeetcurve (academisch concept, geen directe URL).**

[17] **NCSC Cybersecuritybeeld Nederland 2025.** https://www.ncsc.nl/producten-en-diensten/cybersecuritybeeld-nederland-csbn

[18] **ENISA NIS2 Risk Management Guidance.** https://www.enisa.europa.eu/publications/implementation-guidance-on-nis-2-security-measures