GIDS

De complete gids voor email security as a service

Bescherming, kosten, selectiecriteria, NIS2/DORA-verplichtingen en het verschil tussen SEG, ICES en ingebouwde beveiliging. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

E-mail is de nummer 1 aanvalsvector voor cyberaanvallen. Hieronder de feiten die de urgentie onderbouwen.

27%

van alle datalekken begint via e-mail -- de grootste enkele aanvalsvector

Verizon DBIR 2025 [1]

EUR 750K--4M

typische schade per BEC-incident (Business Email Compromise) in Nederland

NCSC [2]

41,5%

van Nederlandse domeinen heeft geen DMARC-record -- geen bescherming tegen e-mail spoofing

PowerDMARC 2024 [3]

3,4 mld

phishing e-mails worden dagelijks wereldwijd verstuurd

Keepnet Labs 2025 [4]

+400%

toename QR-phishing (quishing) tussen 2023 en 2025

GBHackers / CaptainDNS [5]

48%

van phishing-aanvallen bevat MFA-bypass technieken

PowerDMARC 2026 [6]

237--278%

ROI van email security over 3 jaar volgens onafhankelijke studies

Forrester TEI Studies [7]

Q2 2026

Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- e-mail beveiligen wordt aantoonbare zorgplicht

Digitale Overheid [8]

1. Wat is email security as a service?

Email Security as a Service (ESaaS) is een cloud-gebaseerde beveiligingsoplossing die inkomende en uitgaande e-mail beschermt tegen phishing, malware, ransomware, BEC-fraude en spam. Het wordt aangeboden als managed dienst bovenop je bestaande e-mailplatform.

10 KERNCOMPONENTEN

COMPONENT	FUNCTIE
Anti-phishing	Detectie via AI, URL-analyse, sender reputation en behavioral analysis
Anti-malware	Scanning van bijlagen op bekende en onbekende malware
Sandboxing	Verdachte bijlagen worden geopend in een geisoleerde omgeving om gedrag te observeren voordat ze de inbox bereiken
URL rewriting & time-of-click	Links worden bij elke klik opnieuw gescand -- beschermt tegen delayed payload attacks
BEC/impersonatie-detectie	AI-gestuurde herkenning van CEO-fraude en leveranciersfraude zonder malicious links of bijlagen
DMARC/SPF/DKIM management	Monitoring en handhaving van e-mailauthenticatie met rapportages en policy enforcement
Email encryption	End-to-end of gateway-encryptie voor gevoelige uitgaande berichten
DLP (Data Loss Prevention)	Voorkomen dat gevoelige data (BSN, creditcardnummers) per e-mail wordt verstuurd
Post-delivery remediation	Automatisch verwijderen van mails die na aflevering alsnog als kwaadaardig worden geidentificeerd
Rapportage & compliance	Dashboards, audit trails en rapportages voor NIS2/AVG/ISO 27001 compliance [9]

> **Verschil met ingebouwde beveiliging:** Standaard e-mailplatformen bieden basisbeveiliging, maar missen geavanceerde BEC-detectie, sandboxing, DMARC lifecycle management en post-delivery remediation. Email security as a service voegt deze lagen toe als aanvulling of vervanging.

2. Waarom is het belangrijk?

E-mail is de meest gebruikte aanvalsvector ter wereld. De cijfers voor Nederland laten zien waarom ingebouwde beveiliging alleen niet volstaat.

E-MAIL ALS AANVALSVECTOR

Volgens het Verizon DBIR 2025 begint 27% van alle datalekken via e-mail [1]. Phishing is de initial access vector in 14--15% van alle breaches. Bij ransomware-aanvallen is e-mail in 35--42% van de gevallen het startpunt [10]. 57% van organisaties rapporteert wekelijkse of dagelijkse phishing-pogingen [4].

BEC-SCHADE IN NEDERLAND

Business Email Compromise (BEC) -- ook bekend als CEO-fraude of factuurfraude -- is een van de duurste vormen van cybercrime. In Nederland ligt de typische schade per incident tussen EUR 750.000 en EUR 4 miljoen [2]. In het eerste halfjaar van 2024 werden meer dan 50.000 BEC-incidenten gerapporteerd in Nederland, een stijging van 35% ten opzichte van 2023 [11].

CBS DATA EN NEDERLANDSE CONTEXT

- **18%** van alle datalekmeldingen betrof e-mail (verkeerde ontvanger, foutief verzonden persoonsgegevens) [12]
- **2,5 miljoen** Nederlanders (16% van de bevolking 15+) werden slachtoffer van online criminaliteit in 2024 [12]
- Minimaal **121 unieke ransomware-incidenten** in Nederland in 2024 (Project Melissa) [13]

DMARC ADOPTIE IN NEDERLAND IS LAAG

41,5% van Nederlandse domeinen heeft geen DMARC-record [3]. Van de domeinen die wel DMARC hebben, staat 21,6% op "none" -- dat rapporteert wel, maar blokkeert niets. MTA-STS adoptie is slechts 0,9%. Dit betekent dat de meeste Nederlandse organisaties geen bescherming hebben tegen e-mail spoofing.

REKENSOM

Email security kost EUR 1--15 per mailbox per maand. Een gemiddeld BEC-incident kost EUR 750.000--4.000.000. Bij 100 mailboxen betaal je EUR 1.200--18.000 per jaar -- een fractie van de potentiele schade van een enkel incident [2].

3. Hoe werkt het?

Email security werkt als een extra beveiligingslaag bovenop of in plaats van de ingebouwde beveiliging van je e-mailplatform. Er zijn twee fundamenteel verschillende architecturen.

SEG (SECURE EMAIL GATEWAY)

Een SEG zit als gateway tussen het internet en je e-mailserver. Alle inkomende e-mail passeert eerst de SEG, die filtert op spam, malware, phishing en verdachte bijlagen. Het MX-record van je domein wordt omgeleid naar de SEG. Voordeel: volledige controle over alle e-mail. Nadeel: vereist MX-record wijziging en kan conflicteren met ingebouwde beveiliging.

ICES (INTEGRATED CLOUD EMAIL SECURITY)

Een ICES-oplossing integreert via API direct met je e-mailplatform -- geen MX-record wijziging nodig. Het analyseert e-mail na aflevering en kan verdachte berichten automatisch uit inboxen verwijderen. Voordeel: snelle implementatie, werkt naast ingebouwde beveiliging. Sterk in BEC-detectie door behavioral analysis van interne communicatiepatronen.

DEFENSE-IN-DEPTH

De meest effectieve aanpak combineert meerdere lagen:

1. **E-mailauthenticatie** -- SPF, DKIM en DMARC correct geconfigureerd
2. **Gateway of API-beveiliging** -- SEG of ICES als extra laag
3. **Ingebouwde platformbeveiliging** -- features van je e-mailplatform correct ingeschakeld
4. **Post-delivery scanning** -- continue heranalyse van afgeleverde berichten
5. **Awareness training** -- medewerkers als laatste verdedigingslinie

VERSCHIL MET INGEBOUWDE BEVEILIGING

ASPECT	INGEBOUWD (STANDAARD)	DEDICATED EMAIL SECURITY
Anti-spam	Goed -- basisfiltering effectief	Vergelijkbaar of beter
Anti-phishing	Basis -- vooral signature-based	Veel beter -- AI, behavioral analysis
BEC/impersonatie	Beperkt -- handmatige configuratie nodig	Sterk -- AI-gestuurde payload-loze detectie
Sandboxing	Alleen in premium licenties	Standaard in mid/premium tiers

ASPECT	INGEBOUWD (STANDAARD)	DEDICATED EMAIL SECURITY
DMARC management	Geen actieve monitoring/rapportage	Volledige DMARC lifecycle management
Post-delivery remediation	Handmatig / beperkt automatisch	Automatisch
Prijs	Inbegrepen / EUR 2--6 add-on	EUR 1--15/mailbox/maand

VEELGEMAAKTE AANNAME

Organisaties nemen aan dat hun standaard e-mailplatform "genoeg" beveiliging biedt. In werkelijkheid staan veel krachtige beveiligingsfeatures standaard UIT en vereist goede beveiliging bewuste hardening van meerdere lagen [14].

4. Wat kost het?

Email security varieert van minder dan EUR 1 per mailbox per maand voor basisfiltering tot EUR 15 voor een volledige suite met sandboxing, DLP en managed SOC.

PRIJSOVERZICHT PER TIER

TIER	PRIJS/MAILBOX/MAAND	WAT JE KRIJGT
Basis	EUR 1--3	Anti-spam, anti-virus, basis phishing-detectie, quarantine management
Geavanceerd	EUR 3--7	+ URL rewriting, sandboxing, AI phishing-detectie, BEC-detectie, DMARC monitoring, post-delivery remediation
Premium	EUR 7--15	+ Volledige DMARC lifecycle, DLP, encryption, SIEM-integratie, managed SOC, NIS2-compliance rapportages

JAARKOSTEN PER ORGANISATIEGROOTTE

ORGANISATIEGROOTTE	BASIS	GEAVANCEERD	PREMIUM
10 mailboxen	EUR 120--360	EUR 360--840	EUR 840--1.800
50 mailboxen	EUR 600--1.800	EUR 1.800--4.200	EUR 4.200--9.000
100 mailboxen	EUR 1.200--3.600	EUR 3.600--8.400	EUR 8.400--18.000
250 mailboxen	EUR 3.000--9.000	EUR 9.000--21.000	EUR 21.000--45.000

Volumekortingen van 10--20% zijn gebruikelijk bij 100+ mailboxen. Meerjarige contracten (2--3 jaar) leveren 20--40% korting op. Onderhandelde enterprise-prijzen liggen doorgaans 22--55% onder de lijstprijs [15].

> **ROI:** Onafhankelijke Forrester TEI-studies meten 237--278% ROI over 3 jaar voor email security [7]. Bij een gemiddeld MKB-datalek van EUR 34.000 (directe + indirecte kosten) is de break-even bij het voorkomen van een enkel incident [16].

5. Waar moet je op letten?

De email security markt is breed. Hieronder de selectiecriteria die je helpen een onderbouwde keuze te maken.

SELECTIECRITERIA

CRITERIUM	WAAROM BELANGRIJK
AI-gestuurde detectie	Signature-based detectie mist AI-gegenereerde phishing. Behavioral analysis en NLP zijn essentieel voor moderne dreigingen.
Sandboxing	Verdachte bijlagen moeten in een geisoleerde omgeving getest worden -- niet alleen gescand op bekende signatures.
BEC/impersonatie-detectie	CEO-fraude bevat geen malicious links of bijlagen. Detectie vereist analyse van communicatiepatronen en taalgebruik.
DMARC lifecycle management	Niet alleen DMARC instellen, maar monitoren, tunen en doorgroeien naar p=reject.
Post-delivery remediation	Berichten die na aflevering alsnog kwaadaardig blijken automatisch uit inboxen verwijderen.
Integratie met je e-mailplatform	Naadloze koppeling met je huidige platform. Let op conflicten (dubbele URL-rewriting, ARC-support).
Uitgaande mailbeveiliging	DLP en encryption voor uitgaande berichten zijn net zo belangrijk als inkomende filtering.
Rapportage en compliance	NIS2 vereist aantoonbare maatregelen. Je hebt dashboards en audit trails nodig.
False positive rate	Agressieve filtering die legitieme berichten blokkeert is schadelijker dan milde filtering.
Support en implementatietijd	SEG vereist MX-record wijziging (complexer). ICES werkt via API (sneller). Kies wat past bij je team.

10 VRAGEN AAN EEN LEVERANCIER

1. Hoe detecteren jullie BEC/impersonatie-aanvallen zonder malicious payload?
2. Bieden jullie sandboxing voor bijlagen, en is dit standaard of een add-on?

3. Ondersteunen jullie DMARC lifecycle management (monitor, quarantine, reject)?
4. Hoe werkt post-delivery remediation -- automatisch of handmatig?
5. Welke integraties bieden jullie met ons e-mailplatform en SIEM?
6. Beveiligen jullie ook uitgaande e-mail (DLP, encryption)?
7. Wat is jullie aanpak bij conflicten met ingebouwde beveiliging (ARC, URL-rewriting)?
8. Welke NIS2-compliance rapportages leveren jullie?
9. Hoe hoog is de false positive rate en hoe wordt deze getuned?
10. Wat zijn de contractvoorwaarden, volumekortingen en implementatietijd?

6. Veelgemaakte fouten

De meeste e-mail security incidenten zijn vermijdbaar. Hieronder de fouten die je moet kennen.

TECHNISCHE FOUTEN

FOUT	IMPACT
Alleen ingebouwde beveiliging vertrouwen	Geen bescherming tegen geavanceerde BEC, zero-day phishing en payload-loze aanvallen [17]
DMARC op "none" laten staan	Je ontvangt rapportages maar blokkeert niets. Spoofing van je domein blijft mogelijk [18]
SPF record met >10 DNS lookups	SPF faalt permanent. Alle e-mail die SPF controleert wordt als verdacht gezien [18]
Third-party senders niet in SPF	Legitieme e-mail van marketing-tools, CRM of ticketsystemen faalt authenticatie [18]
Uitgaande mail niet beveiligd	Geen DLP, geen encryption. Gevoelige data lekt via uitgaande berichten.
SEG + ingebouwde beveiliging zonder ARC	Dubbele URL-rewriting, broken links, anti-spoofing werkt niet meer correct [19]

ORGANISATORISCHE FOUTEN

FOUT	IMPACT
Geen awareness training	60% van breaches betreft menselijke actie. Techniek alleen is niet genoeg [1]
Geen incident response plan	Paniek, tijdverlies en grotere schade bij een aanval [20]
"We gebruiken M365" als compliance-bewijs	Onvoldoende voor NIS2 -- aantoonbare, gedocumenteerde maatregelen zijn vereist [8]
Focus op techniek, niet op mens	De meeste incidenten ontstaan door menselijke fouten, niet technische lekken [20]

DMARC: DE STAP DIE BIJNA IEDEREEN OVERSLAAT

21,6% van Nederlandse domeinen met DMARC heeft het op "none" staan [3]. Dat is alsof je een alarmsysteem installeert maar nooit inschakelt. De stap naar "quarantine" of "reject" wordt niet gezet uit angst voor false positives. Een managed DMARC-service begeleidt dit proces en voorkomt dat legitieme mail verloren gaat.

7. NIS2 en DORA

E-mail is de nummer 1 aanvalsvector. Zowel NIS2 als DORA stellen eisen die direct raken aan hoe je je e-mail beveiligt.

NIS2 / CYBERBEVEILIGINGSWET

VERPLICHTING	RELATIE MET EMAIL SECURITY
Zorgplicht	Beveiligingsrisico's analyseren en passende maatregelen nemen -- e-mail is de #1 aanvalsvector [1]
Meldplicht (24 uur)	Vereist detectiecapabiliteit voor e-mail-gerelateerde incidenten
Ketenverantwoordelijkheid	NIS2-plichtige organisaties stellen eisen aan leveranciers -- ook MKB in de keten wordt geraakt [21]
Aantoonbaarheid	Maatregelen moeten gedocumenteerd en aantoonbaar zijn -- "we gebruiken ons standaard platform" is onvoldoende [22]

DORA (DIGITAL OPERATIONAL RESILIENCE ACT)

DORA is van kracht sinds 17 januari 2025 voor de financiele sector. De relatie met email security:

- Financiele instellingen moeten aantoonbaar hun digitale communicatiekanalen beveiligen
- Email security valt onder ICT-risicobeheer en vereist testing
- DORA heeft voorrang bij overlap met NIS2 voor financiele organisaties
- Toeleveranciers van financiele instellingen worden indirect geraakt via supply chain-eisen [23]

> **LET OP: KETENVERANTWOORDELIJKHEID**
> Ook bedrijven die niet direct onder NIS2 of DORA vallen, krijgen vragen van klanten over hun e-mailbeveiliging. Een aantoonbare email security oplossing wordt een commercieel vereiste in de keten -- niet alleen een technische keuze [22].

8. SEG vs ICES vs ingebouwde beveiliging

Er zijn drie fundamenteel verschillende benaderingen van email security. Hieronder een heldere vergelijking.

ASPECT	SEG (SECURE EMAIL GATEWAY)	ICES (API-BASED)	INGEBOUWDE BEVEILIGING
Architectuur	MX-record omleiding, gateway	API-integratie, geen MX-wijziging	Native in e-mailplatform
Implementatie	MX-record wijziging, complexer	API-koppeling, sneller	Standaard aanwezig
Anti-spam	Sterk	Complementair	Goed
Anti-phishing	Sterk (pre-delivery)	Sterk (pre + post-delivery)	Basis--goed
BEC-detectie	Goed	Uitstekend (behavioral analysis)	Beperkt
Sandboxing	Standaard in premium tiers	Varieert	Alleen premium licenties
DMARC management	Vaak inbegrepen	Soms als add-on	Geen actieve monitoring
Post-delivery	Beperkt	Sterk (kern-functie)	Beperkt--handmatig
Conflicten	Mogelijk met ingebouwde features	Minimaal	Geen
Prijs	EUR 2--15/mailbox/maand	EUR 3--15/mailbox/maand	Inbegrepen / EUR 2--6 add-on

> **Wanneer welke aanpak?** Organisaties met veel extern e-mailverkeer en hoog risico kiezen vaak een SEG. Organisaties die snel willen implementeren zonder MX-wijziging kiezen ICES. Kleine organisaties met lage exposure kunnen starten met correct geconfigureerde ingebouwde beveiliging [14].

9. Trends 2025--2026

De dreigingslandschap voor e-mail verandert snel. Hieronder de vier trends die email security in 2026 vormgeven.

AI-GEGENEREERDE PHISHING

86% van organisaties heeft al minimaal 1 AI-gerelateerd phishing-incident meegemaakt [24]. AI genereert hyperpersoonlijke phishing in minuten, nauwelijks te onderscheiden van legitieme interne communicatie. Verwachting mid-2026: volledig autonome aanvalssystemen die automatisch scrapen, personaliseren, versturen en follow-ups plannen.

QR-PHISHING (QUISHING) +400%

QR-phishing is met 400% toegenomen tussen 2023 en 2025 [5]. 26% van alle malicious links wordt nu via QR-code geleverd. QR-codes verschijnen in e-mails, PDF-facturen, fysieke borden en bezorgnotificaties. Traditionele URL-scanning mist QR-codes -- specifieke detectie is nodig.

DEEPFAKE VOICE PHISHING

Deepfake-fraude is met meer dan 700% jaar-op-jaar gestegen [25]. Voice cloning is niet meer voorbehouden aan labs -- stemmen zijn kloonbaar vanuit publieke presentaties en calls. "BEC 3.0" combineert AI-gegenereerde e-mails, deepfake voices en nep-videovergaderingen.

MFA-BYPASS EN PHISHING-AS-A-SERVICE

48% van phishing-aanvallen bevat MFA-bypass technieken zoals EvilProxy en Adversary-in-the-Middle [6]. Het aantal bekende phishing-kits is in 2025 verdubbeld -- Phishing-as-a-Service maakt geavanceerde aanvallen toegankelijk voor niet-technische aanvallers [26].

MARKTOMVANG

De wereldwijde email security markt groeit van USD 5,2--7,3 miljard (2025) naar USD 12,2--23,4 miljard in 2030--2035, met een jaarlijkse groei van 9,9--13,1% [27]. De Europese markt bedraagt circa USD 1,8 miljard (2025), gedreven door NIS2, DORA en de migratie naar cloud-gebaseerde e-mail.

10. Aan de slag

Je weet nu hoe email security werkt, wat het kost en waarom het noodzakelijk is. De volgende stap: een oplossing kiezen die past bij jouw organisatie.

IN VIJF STAPPEN NAAR VEILIGE E-MAIL

1 DMARC check

Controleer of je domein SPF, DKIM en DMARC correct heeft geconfigureerd. 41,5% van Nederlandse domeinen heeft geen DMARC -- begin hier [3].

2 Huidige beveiliging beoordelen

Inventariseer welke e-mailbeveiliging je nu hebt. Staan alle features van je platform aan? Heb je sandboxing, BEC-detectie en DMARC monitoring?

3 Behoeften bepalen

Klein bedrijf met weinig externe mail? Ingebouwde beveiliging kan volstaan. Veel extern verkeer, financiele transacties of NIS2-plichtig? Dan heb je een extra laag nodig.

4 Selectie en implementatie

Vergelijk oplossingen op de criteria in hoofdstuk 5. Kies tussen SEG (gateway) en ICES (API) op basis van je situatie. ICES is sneller te implementeren.

5 DMARC naar reject

Plan de DMARC-uitrol: none, quarantine, reject. Gebruik een managed DMARC-service om false positives te voorkomen. Documenteer alles voor NIS2-compliance.

Bronnenlijst

[1] **Verizon -- Data Breach Investigations Report 2025.** 27% breaches via e-mail, ~60% menselijke actie. https://www.verizon.com/business/resources/reports/dbir/

[2] **NCSC -- Business Email Compromise: een snelgroeiende vorm van digitale fraude.** EUR 750K--4M per incident NL. https://www.ncsc.nl/blog/business-email-compromise-een-snelgroeiende-vorm-van-digitale-fraude-met-grote-impact

[3] **PowerDMARC -- Netherlands DMARC Adoption 2024.** 41,5% zonder DMARC, 21,6% op none. https://powerdmarc.com/netherlands-dmarc-adoption/

[4] **Keepnet Labs -- Top Phishing Statistics and Trends 2025.** 3,4 miljard phishing mails/dag. https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

[5] **GBHackers -- AI-Driven Phishing and QR Code Quishing Surge.** +400% quishing. https://gbhackers.com/spam-and-phishing-report/

[6] **PowerDMARC -- Email Phishing & DMARC Statistics 2026.** 48% MFA-bypass. https://powerdmarc.com/email-phishing-dmarc-statistics/

[7] **Proofpoint / Guardian Digital -- Forrester TEI Studies.** 237--278% ROI. https://www.proofpoint.com/us/blog/email-and-cloud-threats/analysis-reveals-roi-proofpoint-prime

[8] **Digitale Overheid -- Cyberbeveiligingswet (NIS2).** https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[9] **Barracuda -- Email Protection Features.** 10 kerncomponenten. https://www.barracuda.com/products/email-protection/features

[10] **AppSecure -- Ransomware Statistics 2025.** 35--42% ransomware via e-mail. https://www.appsecure.security/blog/ransomware-statistics-2025-trends-costs-defense

[11] **CustomerFirst -- Toename cyberfraude treft Nederlandse bedrijven.** 50.000+ BEC H1 2024. https://customerfirst.nl/nieuws/2025/05/toename-cyberfraude-treft-nederlandse-bedrijven/index.xml

[12] **CBS -- Cybersecuritymonitor 2024.** 18% datalekken via e-mail. https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[13] **NCSC -- Jaarbeeld Ransomware 2025.** 121 unieke incidenten NL (Project Melissa). https://www.ncsc.nl/ransomware/jaarbeeld-ransomware-2025

[14] **Trustifi -- Google Workspace Email Security in 2025.** Beveiligingsfeatures standaard UIT. https://trustifi.com/blog/google-workspace-email-security/

[15] **CostBench -- Proofpoint Pricing 2026.** Volumekortingen 22--55%. https://costbench.com/software/email-security/proofpoint/

[16] **Vanoers.nl -- Gemiddelde kosten datalek stijgen.** EUR 34.000 MKB. https://www.vanoers.nl/nieuws/it-advies/gemiddelde-kosten-datalek-stijgen/

[17] **Abnormal AI -- Microsoft 365 Email Security Solutions.** https://abnormal.ai/blog/microsoft-office-365-security-solutions

[18] **DMARCSaaS -- 10 meest gemaakte DMARC-fouten.** https://www.dmarcsaas.com/de-10-meest-gemaakte-fouten-bij-het-uitrollen-van-dmarc/

[19] **Microsoft Learn -- Integrate non-Microsoft security services.** ARC-support en URL-rewriting conflicten. https://learn.microsoft.com/en-us/defender-office-365/mdo-integrate-security-service

[20] **Felloo -- 5 veelgemaakte fouten in MKB-bedrijven die hackers wel kennen.** https://www.felloo.nl/blog/5-veelgemaakte-fouten-in-mkb-bedrijven-die-hackers-wel-kennen/

[21] **CertificeringsAdvies -- NIS2 voor MKB.** Ketenverantwoordelijkheid. https://certificeringsadvies.nl/de-nis2-richtlijn-wat-is-nis2-en-wat-betekent-het-voor-mkb-bedrijven/

[22] **ABN AMRO -- NIS2 vereist aantoonbare cybersecurity.** https://www.abnamro.nl/nl/zakelijk/insights/cybersecurity/beveiliging/nis2-vereist-aantoonbare-cybersecurity.html

[23] **1Key -- DORA & NIS2 nieuwe cyberverplichtingen 2025.** https://www.1key.nl/dora-nis2-nieuwe-cyberverplichtingen-in-2025/

[24] **Kymatio -- Phishing Trends 2026.** 86% heeft AI-phishing incident meegemaakt. https://kymatio.com/blog/phishing-trends-ai-phishing-qrishing-and-voice-attacks

[25] **ZeroThreat -- Deepfake & AI Phishing Statistics.** 700%+ stijging deepfake-fraude. https://zerothreat.ai/blog/deepfake-and-ai-phishing-statistics

[26] **Infosecurity Magazine NL -- Phishing-kits verdubbeld in 2025.** https://infosecuritymagazine.nl/nieuws/het-aantal-phishing-kits-is-in-2025-verdubbeld-slimmer-innovatiever-maar-ook-voorspelbaar

[27] **Fortune Business Insights / Mordor Intelligence -- Email Security Market.** USD 5,2--7,3 mld (2025), CAGR 9,9--13,1%. https://www.fortunebusinessinsights.com/email-security-market-106607