SpySecure

Cybersecurity checklist

Voor het midden- en kleinbedrijf

Voor directie, CTO’s, IT-managers en externe IT-partners om te beoordelen hoe volledig en effectief de beveiliging van een organisatie is.

Checklist

Cybersecurity-checklist

Elk niveau bouwt voort op het vorige.

SpySecure

NIVEAU 1

De basis

Minimale beveiliging als je nauwelijks clouddiensten gebruikt.

- [ ] **Endpointbeveiliging**

NIVEAU 2

Standaard

Essentieel voor bedrijven die Microsoft 365, Google Workspace of andere SaaS-apps gebruiken.

- [ ] **E-mailbeveiliging**
- [ ] **Cloudbeveiliging**
- [ ] **Identiteitsbeveiliging**
- [ ] **Medewerkerbeveiliging**

NIVEAU 3

Geavanceerd

Als klanten bewijs van beveiliging vragen of je aan NIS2- of ISO-eisen moet voldoen.

- [ ] **Back-ups**
- [ ] **Compliancemanagement**
- [ ] **Zakelijk wachtwoordbeheer**
- [ ] **Domeinbeveiliging**

ALTIJD · IN ELKE BEVEILIGINGSLAAG

Volledig beheerde service

24/7 monitoring & respons

- [ ] **Tools installeren en beveiligingsinstellingen bijhouden**
- [ ] **Monitoring · beveiligingsmeldingen volgen**
- [ ] **Detectie · verdachte activiteiten onderzoeken**
- [ ] **Respons · dreigingen stoppen en incidenten oplossen**
- [ ] **Maandelijkse beveiligingsrapporten**

Tools bieden weinig bescherming zonder voortdurende monitoring en opvolging.

NIVEAU 1 · DE BASIS

Endpointbeveiliging

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- [ ] **Centraal apparaatbeheer**
  Alle zakelijke apparaten zijn geregistreerd, zichtbaar en gekoppeld aan een verantwoordelijke.

- [ ] **Updates van het besturingssysteem**
  Beveiligingsupdates worden tijdig geïnstalleerd. Mislukte updates worden opgevolgd.

- [ ] **Software-updates**
  Zakelijke applicaties worden centraal bijgewerkt; medewerkers hoeven dit niet zelf te doen.

- [ ] **Next-generation antivirus (NGAV)**
  Antivirus blokkeert schadelijke software op basis van verdacht gedrag, zoals ransomware die bestanden versleutelt.

- [ ] **Endpoint Detection & Response (EDR)**
  Alle actieve processen en apparaatactiviteiten worden op verdacht gedrag gecontroleerd, niet alleen bestanden.

WAAROM DIT NODIG IS

Elke laptop en desktop biedt toegang tot bedrijfsdata. Alleen antivirus kan moderne aanvallen niet herkennen en stoppen.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport endpointbeveiliging**
- ✓ **Apparaatoverzicht en updatestatus**
- ✓ **Gevonden dreigingen en genomen acties**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- [ ] **Monitoring**
  Beveiligingsmeldingen continu volgen
- [ ] **Detectie**
  Verdachte activiteiten onderzoeken
- [ ] **Respons**
  Dreigingen stoppen, incidenten oplossen

NIVEAU 2 · STANDAARD

E-mailbeveiliging

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- [ ] **Phishingfiltering**
  Misleidende berichten, afzendervervalsing en betaalfraude worden herkend en gefilterd.
- [ ] **Bijlagefiltering**
  Bijlagen worden gescand; schadelijke bestanden worden geblokkeerd of in quarantaine geplaatst.
- [ ] **Linkfiltering**
  Schadelijke links worden bij ontvangst en bij het aanklikken herkend en geblokkeerd.
- [ ] **Content Disarm & Reconstruction (CDR)**
  Documenten worden herschreven om riskante inhoud onschadelijk te maken en bruikbare inhoud te behouden.
- [ ] **Datalekpreventie voor uitgaande e-mail (DLP)**
  Controle van uitgaande e-mail voorkomt dat gevoelige informatie zonder toestemming wordt verstuurd.
- [ ] **Waarschuwingsbanners voor medewerkers**
  Waarschuwingen in e-mails leggen verdachte signalen uit en leren medewerkers veiliger te handelen.
- [ ] **Meldingen door medewerkers**
  Medewerkers kunnen verdachte e-mails eenvoudig melden. Elke melding wordt beoordeeld en opgevolgd.

WAAROM DIT NODIG IS

E-mail is een veelgebruikte ingang voor phishing, schadelijke links, onveilige bijlagen en factuurfraude.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport e-mailbeveiliging**
- ✓ **Geblokkeerde mails en DLP-meldingen**
- ✓ **Banners en opvolging van meldingen**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- [ ] **Monitoring**
  Beveiligingsmeldingen continu volgen
- [ ] **Detectie**
  Verdachte activiteiten onderzoeken
- [ ] **Respons**
  Dreigingen stoppen, incidenten oplossen

NIVEAU 2 · STANDAARD

Cloudbeveiliging

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- [ ] **Cloud Detection & Response**
  Activiteiten op belangrijke cloud- en SaaS-platforms worden centraal gemonitord.

- [ ] **Verdachte cloudactiviteiten**
  Ongebruikelijke downloads, gedeelde bestanden en wijzigingen in mailboxen of beheer worden herkend.

- [ ] **Riskante aanmeldingen**
  Onmogelijke reisbewegingen, onbekende apparaten en afwijkende inloglocaties worden onderzocht.

- [ ] **Monitoring van gekoppelde applicaties**
  Applicaties van derden en toegang via OAuth zijn inzichtelijk en worden beoordeeld.

- [ ] **Datalekpreventie (DLP)**
  Het verplaatsen en extern delen van gevoelige data wordt herkend en beheerst.

WAAROM DIT NODIG IS

Bedrijfsdata staat in Microsoft 365, Google Workspace en SaaS-apps. Zonder monitoring blijven ongewenste toegang en datadeling onopgemerkt.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport cloudactiviteiten**
- ✓ **Gekoppelde apps en deelinstellingen**
- ✓ **Verdachte activiteiten en genomen acties**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- [ ] **Monitoring**
  Beveiligingsmeldingen continu volgen
- [ ] **Detectie**
  Verdachte activiteiten onderzoeken
- [ ] **Respons**
  Dreigingen stoppen, incidenten oplossen

NIVEAU 2 · STANDAARD

Identiteitsbeveiliging

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- ☐ **MFA afgedwongen, niet alleen ingeschakeld**
  Meervoudige authenticatie is verplicht voor iedere gebruiker en beheerder. Instellen is niet optioneel.
- ☐ **Monitoring van accountbeveiliging**
  Aanmeldingen, resets, doorstuurregels en andere riskante wijzigingen worden gemonitord.
- ☐ **Beheer van beheerdersaccounts**
  Beheerdersrechten zijn beperkt, gescheiden en worden regelmatig beoordeeld.
- ☐ **Monitoring van gelekte inloggegevens**
  Bedrijfsdomeinen en accounts worden gecontroleerd. Bij gelekte gegevens wordt actie ondernomen.
- ☐ **Ongebruikte accounts en oud-medewerkers**
  Ongebruikte accounts en accounts van vertrokken medewerkers worden tijdig uitgeschakeld en gecontroleerd.

WAAROM DIT NODIG IS

Een gestolen, vergeten of te ruim gemachtigd account kan apparaatbeveiliging omzeilen en direct toegang geven tot bedrijfsdata.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport identiteitsbeveiliging**
- ✓ **MFA-afdwinging en accountstatus**
- ✓ **Gelekte inloggegevens en genomen acties**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- ☐ **Monitoring**
  Beveiligingsmeldingen continu volgen
- ☐ **Detectie**
  Verdachte activiteiten onderzoeken
- ☐ **Respons**
  Dreigingen stoppen, incidenten oplossen

NIVEAU 2 · STANDAARD

Medewerkerbeveiliging

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- ☐ **Cybersecuritytraining**
  Minimaal maandelijks interactieve e-learnings, afgestemd op de rol en het gedrag van elke medewerker.
- ☐ **Phishingsimulaties**
  Wekelijkse realistische phishingtests laten medewerkers oefenen met het herkennen van verdachte berichten.
- ☐ **Gerichte vervolgtraining**
  Medewerkers die klikken of gegevens delen, krijgen relevante aanvullende training.
- ☐ **Nieuwe medewerkers direct toevoegen**
  Nieuwe medewerkers worden direct toegevoegd aan het doorlopende leerprogramma en de phishingsimulaties.
- ☐ **Managementrapportage**
  Deelname, risico's en voortgang zijn inzichtelijk voor het management.

WAAROM DIT NODIG IS

Medewerkers nemen dagelijks beslissingen over beveiliging. Training moet daarom doorlopend, relevant en meetbaar zijn.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport medewerkerbeveiliging**
- ✓ **Trainingsdeelname en phishingresultaten**
- ✓ **Persoonlijke opvolging en voortgang**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- ☐ **Monitoring**
  Beveiligingsmeldingen continu volgen
- ☐ **Detectie**
  Verdachte activiteiten onderzoeken
- ☐ **Respons**
  Dreigingen stoppen, incidenten oplossen

NIVEAU 3 · GEAVANCEERD

Back-ups

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- [ ] **Versleutelde apparaatback-ups**
  Belangrijke lokale data wordt automatisch en veilig geback-upt.
- [ ] **Versleutelde cloudback-ups**
  Van Microsoft 365, Google Workspace en SaaS-data worden back-ups gemaakt buiten de bestaande omgeving.
- [ ] **Back-upmonitoring**
  Mislukte back-ups en ontbrekende apparaten of accounts worden actief opgevolgd.
- [ ] **Bewaartermijnen en onveranderbaarheid**
  Versies blijven bewaard en zijn beschermd tegen verwijdering of manipulatie.
- [ ] **Hersteltests**
  Herstel wordt getest. Doelen voor de hersteltijd en het maximaal toegestane dataverlies zijn vastgelegd.

WAAROM DIT NODIG IS

Ransomware, verwijdering of een gehackt beheerdersaccount kan actuele data én slecht beschermde back-ups vernietigen.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport back-ups**
- ✓ **Dekking, fouten en bewaartermijnen**
- ✓ **Resultaat van de laatste hersteltest**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- [ ] **Monitoring**
  Beveiligingsmeldingen continu volgen
- [ ] **Detectie**
  Verdachte activiteiten onderzoeken
- [ ] **Respons**
  Dreigingen stoppen, incidenten oplossen

NIVEAU 3 · GEAVANCEERD

Compliancemanagement

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- [ ] **Scope en gapanalyse**
  Relevante NIS2-, ISO- en klanteisen zijn in kaart gebracht en beoordeeld.
- [ ] **Beheer van beveiligingsbeleid**
  Beleidsdocumenten hebben een eigenaar, goedkeuringsdatum en vaste beoordelingscyclus.
- [ ] **Maatregelen en bewijs**
  Elke relevante eis is gekoppeld aan een ingevoerde maatregel en actueel bewijs.
- [ ] **Compliancerapportage**
  Het management heeft inzicht in tekortkomingen, prioriteiten, acties, verantwoordelijken en status.
- [ ] **Kwetsbaarhedenbeheer**
  Kwetsbaarheden worden gevonden, geprioriteerd en verholpen. De opvolging wordt vastgelegd.

WAAROM DIT NODIG IS

NIS2, ISO en klanteisen vragen om vastgelegde maatregelen, duidelijke verantwoordelijkheden en controleerbaar bewijs.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport compliancestatus**
- ✓ **Gapanalyse en maatregelenregister**
- ✓ **Bewijs en voortgang van verbeteringen**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- [ ] **Monitoring**
  Beveiligingsmeldingen continu volgen
- [ ] **Detectie**
  Verdachte activiteiten onderzoeken
- [ ] **Respons**
  Dreigingen stoppen, incidenten oplossen

NIVEAU 3 · GEAVANCEERD

Zakelijk wachtwoordbeheer

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- [ ] **Zakelijke wachtwoordmanager**
  Zakelijke inloggegevens staan in een zakelijke wachtwoordmanager, niet in browsers, spreadsheets of chats.
- [ ] **Gecontroleerd wachtwoorden delen**
  Toegang wordt waar mogelijk verleend zonder inloggegevens te kopiëren of zichtbaar te maken.
- [ ] **Toegang tot teamkluizen**
  Medewerkers krijgen toegang tot de teamkluizen en inloggegevens die bij hun rol horen.
- [ ] **Auditlogboek**
  Gebruik, delen en wijzigen van inloggegevens zijn traceerbaar.
- [ ] **Uitdiensttreding en herstel**
  Toegang kan centraal worden ingetrokken. Noodtoegang is gecontroleerd geregeld.

WAAROM DIT NODIG IS

Gedeelde en hergebruikte wachtwoorden maken toegang ondoorzichtig en blijven vaak bruikbaar na vertrek van medewerkers of leveranciers.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport wachtwoordbeheer**
- ✓ **Gebruik van en toegang tot teamkluizen**
- ✓ **Toegangswijzigingen en uitdiensttreding**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- [ ] **Monitoring**
  Beveiligingsmeldingen continu volgen
- [ ] **Detectie**
  Verdachte activiteiten onderzoeken
- [ ] **Respons**
  Dreigingen stoppen, incidenten oplossen

NIVEAU 3 · GEAVANCEERD

Domeinbeveiliging

SpySecure

Wat moet je controleren?

Vraag om bewijs, niet alleen om een ja of nee.

- [ ] **SPF, DKIM en DMARC instellen**
  E-mailauthenticatie is correct ingesteld voor elke dienst die namens je organisatie e-mail mag versturen.
- [ ] **DMARC afdwingen**
  Het beleid wordt opgebouwd naar ‘reject’, in plaats van alleen te blijven monitoren.
- [ ] **Doorlopende afzendermonitoring**
  Nieuwe afzenders en mislukte authenticatie worden onderzocht.
- [ ] **Bescherming tegen domeinvervalsing**
  Misbruik van je domein en pogingen met gelijkende domeinen worden herkend en aangepakt.
- [ ] **Brand Indicators for Message Identification (BIMI)**
  Waar ondersteund verschijnt een geverifieerd bedrijfslogo bij geauthenticeerde e-mails.

WAAROM DIT NODIG IS

Criminelen kunnen je bedrijfsdomein nabootsen om klanten, leveranciers en medewerkers te misleiden, zonder je systemen te hacken.

VRAAG DEZE BEWIJSSTUKKEN OP

- ✓ **Maandrapport domeinbeveiliging**
- ✓ **Authenticatie en DMARC-afdwinging**
- ✓ **Toegestane afzenders en domeinmisbruik**

VOLLEDIG BEHEERDE SERVICE

24/7 beveiligingsbeheer

- [ ] **Monitoring**
  Beveiligingsmeldingen continu volgen
- [ ] **Detectie**
  Verdachte activiteiten onderzoeken
- [ ] **Respons**
  Dreigingen stoppen, incidenten oplossen

SpySecure

Alles-in-één cybersecurity.

Volledig beheerd.

Voor een MKB-prijs.

Vanaf €9,99 per licentie per maand

Hulp nodig?

Spreek met ons Security Operations Center.

Plan een gesprek →

Meer informatie over het verbeteren van je beveiliging

Midden- en kleinbedrijf — Bekijk onze pakketten

Professionele IT-partners — Bekijk ons partnerprogramma