Cyberveiligheid: samen geven we cybercriminelen geen kans

1. Waarom een dossier rond cybersecurity en voor wie is het bestemd?

1.1. Waarom makelaars vandaag kwetsbaarder zijn dan ooit

België ziet een duidelijke toename van cyberincidenten. Volgens een artikel dat in februari 2026 in Computable verscheen, werd meer dan de helft van de Belgische bedrijven het afgelopen jaar geconfronteerd met een cyberaanval. Dat treft grote organisaties, maar net zo goed kmo's en kleinere dienstverleners zoals makelaarskantoren.

Recente gebeurtenissen tonen hoe ernstig de situatie is. Eind 2025 circuleerden er na verschillende datalekken meer dan anderhalf miljoen gegevens van Belgische burgers op internet. In januari 2026 moest het Antwerpse ziekenhuis AZ Monica bijna een maand zonder zijn IT-systeem werken na een cyberaanval. Dat illustreert hoe zwaar een organisatie geraakt kan worden.

Makelaars werken in het hart van een digitale keten waarin verzekeringsmaatschappijen, sectorplatformen, Portima, IT-partners en klanten met elkaar verbonden zijn. Eén zwakke schakel kan de hele keten verstoren en leiden tot operationele, financiële of reputatieschade.

Cyberveiligheid is daarom geen puur technisch onderwerp meer. Het is een essentieel onderdeel van de continuïteit van je kantoor en van het vertrouwen van je klanten.

1.2. Wat vind je in dit dossier?

Dit dossier geeft makelaars een helder en praktisch overzicht van de cyberrisico's waaraan ze vandaag blootstaan. Het helpt je om te begrijpen welke risico's relevant zijn voor je kantoor, ook als het om een kleine of middelgrote structuur gaat.

Je komt te weten wat Portima voor jou beveiligt in zijn rol van dienstverlener en welke verantwoordelijkheden bij jou liggen binnen je eigen digitale omgeving: werkstations, netwerk, e-mail, gebruikersbeheer en dagelijkse praktijken.

Daarnaast bevat dit dossier realistische aanbevelingen waarmee je prioriteiten kunt stellen en stapsgewijs de veiligheid van je kantoor kunt versterken. Een checklist helpt je daarbij om je situatie concreet te evalueren. Dit document wil je niet omvormen tot IT-expert, maar biedt een duidelijk, begrijpelijk en toepasbaar kader dat aansluit bij de realiteit van je sector.

1.3. Hoe gebruik je dit dossier?

Dit dossier kan dienen als leidraad om je cyberveiligheidsaanpak te structureren. Lees het eerst volledig door om een duidelijk beeld te krijgen van je sterke punten en kwetsbaarheden.

Bespreek daarna je prioriteiten met je IT-partner: sommige acties kun je meteen uitvoeren, andere vergen begeleiding of extra expertise.

Met de checklist in het volgende hoofdstuk kun je de situatie van je kantoor concreet evalueren en bepalen welke stappen je best eerst zet.

2. Zo garandeert Portima een robuuste beveiliging

2.1. Portima als versterkte digitale kluis voor de makelaar

Portima zorgt voor de beveiliging van alle gegevens die via Portima Connect worden uitgewisseld en voor de data die in de BRIO-databanken worden bewaard. De communicatiekanalen zijn beschermd en gemonitord. Ze draaien op een infrastructuur die voldoet aan de strengste eisen van de sector.
De gegevens blijven op elk moment beveiligd, van verzending tot ontvangst. Portima beschikt bovendien over de ISO 27001-certificering voor informatiebeveiliging.

2.2. Technische beveiliging van de infrastructuur

Portima werkt met een moderne en gelaagde beveiligingsarchitectuur. De hosting gebeurt bij betrouwbare partners zoals Microsoft Azure, waardoor gebruik gemaakt kan worden van stabiele en professioneel beheerde infrastructuren. Het netwerk is beschermd via meerdere verdedigingslagen die pogingen tot inbraak beperken en de continuïteit van de dienstverlening waarborgen.

Gegevens worden versleuteld tijdens het transport en in opslag. Software wordt ontwikkeld volgens een security-by-design-aanpak, waarbij beveiliging vanaf het begin in elke stap van het ontwikkelproces wordt ingebouwd. Deze aanpak zorgt voor een solide technische basis die voldoet aan de best practices van de sector.

2.3. Authenticatie en versterkte beveiliging

De toegang tot de toepassingen van Portima verloopt via een beveiligd authenticatiesysteem dat voortdurend wordt versterkt. Portima werkt permanent aan het verbeteren van deze mechanismen en laat ze regelmatig evalueren.

In dat kader wordt binnenkort een vorm van multifactorauthenticatie geïntroduceerd. Die toevoeging zorgt voor een extra validatie boven op de identificatie van de gebruiker en verhoogt de bescherming tegen ongeoorloofde toegang, vooral wanneer een wachtwoord zou worden onderschept of misbruikt. Portima voert deze veranderingen geleidelijk in, zodat de beveiliging verbetert zonder de gebruikerservaring te verstoren.

2.4. Administratieve procedures en identificatie van gebruikers

Wanneer een nieuw kantoor wordt aangesloten, verifieert Portima altijd de identiteit van de verantwoordelijke, via een bezoek of een videogesprek. Ook bij de overname van een portefeuille wordt deze controle uitgevoerd. Hierdoor wordt gegarandeerd dat gevoelige toegang enkel aan de bevoegde personen wordt toegekend.

Binnen het kantoor bepaalt de verantwoordelijke zelf de gebruikersrechten van zijn medewerkers. Portima voorziet de nodige tools om deze rechten veilig en gestructureerd te beheren. Op die manier is duidelijk wie welke toegang heeft en blijft er steeds een correcte en controleerbare historiek beschikbaar.

2.5. Opvolging en voortdurende verbetering

Cyberveiligheid is geen statisch gegeven. Portima voert regelmatig interne audits uit en laat, wanneer dat nodig is, penetratietests uitvoeren om de weerbaarheid van zijn systemen te controleren. In het kader van de ISO 27001-certificering is een jaarlijkse test voor alle kritieke onderdelen verplicht.

De infrastructuur wordt 24/7 gemonitord zodat verdachte activiteiten snel worden gedetecteerd en aangepakt. Daarnaast volgen de interne teams regelmatig opleidingen in cyberveiligheid om een hoog niveau van waakzaamheid te behouden en goede praktijken in het dagelijkse werk toe te passen.

2.6. Conclusie

Portima zet een volledige en gestructureerde beveiliging op, die de infrastructuur, de toegangen, de gegevensuitwisseling en de interne procedures omvat. Die bescherming vormt een stevige basis voor de hele sector. Ze vervangt echter niet de rol van de makelaar, die verantwoordelijk blijft voor zijn eigen IT-omgeving en de manier waarop er in het kantoor wordt gewerkt. Ook al zijn de BRIO-platformen en Portima Connect op hoog niveau beveiligd, het is uiteindelijk de makelaar die bepaalt wie toegang krijgt tot deze platformen en die de gegevens die daar zijn opgeslagen uitwisselt met zijn cliënten en partners in de verzekeringswereld. De makelaar moet dus waakzaam zijn over welke toegangen hij aan zijn partners geeft, welke gegevens precies worden gedeeld en op welke manier die uitwisseling gebeurt.

3. Inzicht in risico's en zwakke punten om cyberincidenten te voorkomen

3.1. Welke risico's loopt een makelaarskantoor?

Een cyberincident kan verschillende vormen aannemen en elk onderdeel van jouw kantoor treffen. De gevolgen gaan veel verder dan een tijdelijk technisch probleem. Een inbreuk kan leiden tot herstelkosten, omzetverlies, meldingsplicht en mogelijke sancties onder de GDPR. Vertrouwen speelt een centrale rol in de relatie tussen jou en je klanten. Een veiligheidsincident tast dat vertrouwen onmiddellijk aan en kan langdurige schade veroorzaken.

Diefstal of verlies van klantengegevens	Makelaars beheren gevoelige gegevens die bijzonder waardevol zijn voor cybercriminelen. Het verlies of lekken van die informatie kan ernstige gevolgen hebben, zowel voor je klanten als voor je kantoor.
Identiteitsdiefstal van de makelaar of medewerkers	Bij identiteitsfraude kunnen criminelen zich voordoen als jou of je medewerkers, waardoor zij valse berichten kunnen versturen, betalingen kunnen uitlokken of informatie kunnen opvragen bij verzekeraars of klanten.
Compromittering van de professionele mailbox	Een gehackte mailbox kan worden misbruikt om kwaadaardige e-mails te verzenden naar klanten, maatschappijen of partners, waardoor het vertrouwen ernstig wordt geschaad.
Overname van de IT-omgeving	Sommige aanvallen versleutelen gegevens op jouw computer of bij jouw IT-partner, blokkeren jouw

	systemen en eisen losgeld. Zo'n aanval kan jouw activiteiten van de ene dag op de andere stilleggen.
Tijdelijke onderbreking van de werkzaamheden	Zelfs een beperkte storing kan dossiers vertragen, klantvragen onbeantwoord laten en de communicatie met verzekeraars verstoren.

3.2. Welke zwakke punten leiden tot deze risico's?

De meeste incidenten zijn niet het gevolg van bijzonder geavanceerde aanvallen, maar van eenvoudige kwetsbaarheden binnen het kantoor. De meest voorkomende zijn:

Wachtwoorden die worden hergebruikt, gedeeld of te eenvoudig zijn	Wanneer meerdere medewerkers hetzelfde wachtwoord gebruiken of hetzelfde wachtwoord op verschillende plaatsen wordt ingezet, wordt het voor aanvallers veel makkelijker om binnen te raken. Als iemand hetzelfde wachtwoord gebruikt voor privé en werk, brengt een lek op een onschadelijke website ook de meest gevoelige accounts in gevaar.
Onvoldoende beveiligde toestellen	Computers, laptops of smartphones zonder degelijke beveiliging vormen een gemakkelijke ingang voor aanvallers.
Niet-geüpdatete software en systemen	Uitgestelde updates laten gekende kwetsbaarheden openstaan die actief worden misbruikt.
Onbeveiligd of slecht gescheiden wifi-netwerk	Een zwak of gedeeld wifi-netwerk kan toegang geven tot het interne netwerk van jouw kantoor.

Slechte onboarding en offboarding van medewerkers	Een oud account dat niet wordt gedeactiveerd vormt een direct risico. Nieuwe medewerkers die de oude logingegevens van iemand anders overnemen maken correcte opvolging onmogelijk.
Gebrek aan bewustzijn bij medewerkers	Veel bedreigingen komen via Outlook, bijlagen, links of gedeelde mappen binnen. Zonder regelmatige training worden basisregels geen reflexen, waardoor fouten en incidenten vaker voorkomen.

3.3. Hoe leiden deze zwakke punten tot risico's?

Elke zwakke plek verhoogt de kans op een incident. Deze twee voorbeelden tonen hoe snel het kan gaan.

• Voorbeeld 1: een gecompromitteerde mailbox

Een medewerker klikt op een phishinglink, zijn Outlook-wachtwoord wordt buitgemaakt en de aanvaller neemt de mailbox over.
Mogelijke gevolgen: frauduleuze e-mails naar klanten, vervalste betalingsverzoeken, vertrouwensverlies, datalekken.

• Voorbeeld 2: een niet-geüpdatete computer

Een pc zonder recent beveiligingspatch kan besmet raken met malware.

Mogelijke gevolgen: versleutelde bestanden, geblokkeerde systemen, werkonderbreking, dure herstelling.

Deze scenario's tonen hoe kleine fouten of nalatigheden grote gevolgen kunnen hebben. De positieve boodschap is dat de meeste zwakke punten met eenvoudige maatregelen kunnen worden verholpen.

4. De goede praktijken om jouw activiteit beter te beveiligen

Dit hoofdstuk beschrijft een reeks eenvoudige en realistische acties om de veiligheid van een makelaarskantoor te versterken. Daarnaast is er een gedetailleerde checklist beschikbaar die je kantoor helpt om het eigen beveiligingsniveau te evalueren en de belangrijkste prioriteiten te bepalen.

4.1. Een cybersecuritybeleid op maat van je kantoor

Elk kantoor, ook een klein of middelgroot, vaart wel bij een aantal interne afspraken die de aanpak van cyberveiligheid structureren. Dat begint met het helder vastleggen van de rollen: wie doet wat, wie beheert de toegangen, wie moet verwittigd worden bij een incident? Het beheer van rechten is daarbij cruciaal: alleen medewerkers die het echt nodig hebben, mogen toegang krijgen tot bepaalde gegevens of toepassingen.

Een eenvoudig beleid moet het gebruik van systemen, wachtwoorden en telewerk kaderen. Het moet ook minimaal voorzien in procedures voor het onthaal van nieuwe medewerkers en voor het snel intrekken van toegangen wanneer iemand het kantoor verlaat. Zulke basismaatregelen voorkomen al heel wat kwetsbaarheden.

Dat beleid mag geen papieren oefening blijven, maar moet openlijk met het team besproken worden. Het is belangrijk om een klimaat van vertrouwen en transparantie te creëren: bij een menselijke fout – en de meeste cyberaanvallen spelen precies daarop in – is het beter dat een medewerker het probleem niet verbergt. Hoe sneller een incident wordt opgemerkt en gemeld, hoe groter de kans dat de schade beperkt kan blijven.

4.2. Gebruikers en wachtwoorden: strengheid voorop

De meeste incidenten vinden hun oorsprong in slechte gewoontes rond toegangen. Het gebruik van één en hetzelfde wachtwoord door meerdere personen, of hetzelfde wachtwoord op verschillende plaatsen inzetten, brengt een groot risico met zich mee. Elke gebruiker moet over eigen, unieke

inloggegevens beschikken, die sterk genoeg zijn om niet eenvoudig te kunnen worden geraden en die nooit worden hergebruikt.

Om dat haalbaar te maken, is het gebruik van een wachtwoordmanager sterk aan te raden. Waar de toepassingen het toelaten, zorgt multifactorauthenticatie (MFA) voor een extra beveiligingslaag bovenop het wachtwoord.

4.3. Digitale basishygiëne

De bescherming van het kantoor hangt in grote mate af van de manier waarop systemen en toestellen worden onderhouden. Automatische updates moeten worden ingeschakeld en niet eindeloos worden uitgesteld, omdat ze vaak bekende kwetsbaarheden dichten die door cybercriminelen actief worden misbruikt.

Toestellen die professioneel worden gebruikt, moeten beschermd zijn met een betrouwbaar antivirus en bij voorkeur met schijfversleuteling. Een regelmatige back-upstrategie is onmisbaar: één lokale kopie is niet genoeg, er moet minstens één back-up bestaan die offline of op een andere locatie wordt bewaard.

4.4. Opleiden en sensibiliseren van medewerkers

Zelfs met goede tools blijft de beveiliging zwak als medewerkers zich niet bewust zijn van de risico's. Er bestaan tal van opleidingen voor makelaars, aangeboden door federaties, gespecialiseerde organisaties en andere partners in de sector.

Het is belangrijk dat de boodschappen rond cyberveiligheid vanuit het management komen en door de leidinggevenden zelf worden gedragen. Wanneer de verantwoordelijke van het kantoor de juiste reflexen toepast en regelmatig herhaalt, neemt het team die houding sneller over.

Korte sensibilisatiemomenten kunnen eenvoudig in teamvergaderingen worden geïntegreerd om basisregels te herhalen. Bestaande opleidingen vormen een uitstekend vertrekpunt, zeker voor kleinere structuren. Iedereen draagt bij aan de veiligheid van het kantoor, ongeacht de functie, door alert te blijven voor verdachte e-mails, ongebruikelijke verzoeken en risicovol gedrag.

4.5. Focus op wat echt telt

Geavanceerde hulpmiddelen zoals phishing-simulaties, complexe audits of crisisoefeningen kunnen nuttig zijn voor grotere organisaties.

Voor kleinere kantoren volstaat het om zich te concentreren op de basis en gebruik te maken van bestaande, gestructureerde opleidingen en hulpmiddelen. Een eenvoudige aanpak, consequent toegepast, kan de veiligheid al aanzienlijk versterken zonder onnodige complexiteit.

5. Wat Portima doet bij een hacking en wat jij zelf moet doen

Dit hoofdstuk legt uit hoe Portima optreedt wanneer er zich een incident voordoet in een kantoor, en welke stappen jij tegelijk moet nemen om zo snel mogelijk opnieuw veilig te kunnen werken.

5.1. Wat Portima doet als jouw kantoor getroffen wordt door een hacking

Zodra je een incident vermoedt, is het belangrijk Portima meteen op de hoogte te brengen. Dat activeert een standaardprocedure die erop gericht is om je omgeving zo snel mogelijk te beveiligen.

Vanaf het moment dat je het incident meldt, koppelt Portima je tijdelijk los van het Portima-netwerk om verdere verspreiding te vermijden. De lokale certificaten die op de toestellen staan en de wachtwoorden die gelinkt zijn aan de Portima-toegangen, worden ingetrokken. Daarna worden nieuwe certificaten en nieuwe toegangen aangemaakt, zodat alleen een schone, gecontroleerde configuratie opnieuw verbinding kan maken.

Indien nodig worden bepaalde onderdelen opnieuw geïnstalleerd of geconfigureerd, zodat je in veilige omstandigheden kunt heropstarten. Op die

manier zorgt Portima ervoor dat je toegang op een correcte en veilige manier wordt hersteld.

Het doel van deze procedure is tweeledig: de impact van het incident zoveel mogelijk beperken en je zo snel mogelijk opnieuw in een veilige werkomgeving brengen. Door de snelle interventie van Portima te combineren met de juiste stappen binnen jouw kantoor, kun je de activiteiten gecontroleerd hervatten.

5.2. Wat jij zelf moet doen

Terwijl Portima de technische beveiliging van de Portima-toepassingen opnieuw opzet, moet jij zelf een aantal aanvullende stappen nemen. Volg in de eerste plaats de aanbevelingen die Portima je bezorgt voor het gebruik van de toepassingen, zodat nieuwe pogingen tot misbruik worden vermeden.

Een duidelijke interne communicatie is essentieel. Je medewerkers moeten begrijpen wat er aan de hand is en weten wat ze tijdelijk niet mogen doen tot de situatie gestabiliseerd is. In bepaalde gevallen kan het aangewezen zijn om transparant te communiceren met specifieke klanten, zodat hun vertrouwen behouden blijft.

6. Beschikbare bronnen en opleidingen

6.1. Officiële instanties en informatiesites

Verschillende Belgische organisaties publiceren duidelijke en up-to-date aanbevelingen rond cyberveiligheid. Ze vormen een goede eerste bron om risico's te begrijpen en basismaatregelen te leren toepassen.

- Centrum voor Cybersecurity Belgium (CCB)
- Safeonweb

- FOD Economie

Deze websites bieden praktische tips, waarschuwingen bij actieve bedreigingen en toegankelijk informatiemateriaal.

6.2. Financiële sector en federaties

De financiële sector communiceert geregeld over de meest voorkomende bedreigingen en over passend gedrag. De federaties bieden bovendien opleidingen aan die geschikt zijn voor kleine kantoren.

- Febelfin – dossier fraude et sécurité
- FvF
- Feprabel Magazine Risk

Deze organisaties helpen je beter inzicht te krijgen in de risico's van je dagelijkse activiteiten en ondersteunen je bij het opleiden van je medewerkers.

7. Checklist: beoordeel het veiligheidsniveau van je kantoor

7.1. Wat je vindt in de checklist

De checklist bestaat uit een reeks punten die je eenvoudig kunt evalueren met antwoorden zoals Ja, Gedeeltelijk of Nee.

Je kunt ze afdrukken en gebruiken als praktisch hulpmiddel, alleen of samen met je IT-partner. De checklist helpt je om je acties te structureren en je vooruitgang op te volgen.

7.2. Belangrijkste thema's in de checklist

De punten in de checklist zijn gegroepeerd rond een aantal essentiële thema's:

Toegangsbeheer en wachtwoorden	Nagaan hoe toegangen worden toegekend, hoe wachtwoorden worden beheerd en of de juiste praktijken worden toegepast.
Updates en back-ups	Controleren of toestellen, software en systemen regelmatig worden bijgewerkt en of de gegevens van het kantoor correct worden geback-upt.
Interne procedures	Zeker zijn dat de komst en het vertrek van medewerkers goed geregeld zijn, en dat toegangsrechten op tijd worden aangepast.
Sensibilisering van het team	Evalueren hoe vaak en op welke manier er wordt ingezet op cyberbewustzijn binnen het kantoor.
Reactie bij een incident	Controleren of je weet welke stappen je moet nemen bij een hacking en of de rollen duidelijk zijn gedefinieerd.

Je vindt de checklist op de startpagina van www.portima.com en MyPortima.

8. Conclusie: cyberveiligheid is een gedeelde verantwoordelijkheid

Cyberveiligheid steunt op de inspanningen van iedereen. Portima vervult zijn rol door de gegevens die via zijn oplossingen worden uitgewisseld te beveiligen en ze te beschermen als een echte digitale kluis. De voortdurende investeringen in infrastructuur, processen en opleiding zorgen voor een hoog beveiligingsniveau in de hele sector.

Jouw kantoor blijft echter verantwoordelijk voor de eigen IT-omgeving en de dagelijkse praktijk. Toegangen, toestellen, e-mail, wachtwoorden en bewustmaking van je team zijn allemaal elementen die rechtstreeks door jullie organisatie worden beheerd.

Door de krachten te bundelen met Portima, makelaars, federaties en gespecialiseerde organisaties, wordt de volledige sector veerkrachtiger

tegenover cyberdreigingen. Iedereen speelt een eigen, onmisbare rol in deze beveiligingsketen.

We nodigen je uit om dit dossier geregeld te raadplegen via www.portima.com en MyPortima. Het wordt geactualiseerd met nieuwe tips, hulpmiddelen en goede praktijken die je helpen om het beveiligingsniveau van je kantoor verder te versterken.