VGA
LAW & ADR

WHITE PAPER

GEGEVENS-BESCHERMING OP DE WERKVLOER

BELANGRIJKER DAN OOIT

A magazine is a periodical publication, which can either be printed or published electronically. It is issued regularly, usually every week or every month, and it contains a variety of content.

MENSELIJKE FOUTEN ZIJN DE ZWAKSTE SCHAKEL

Gegevenslekken ontstaan zelden door hackers alleen. In meer dan 5 op de 10 gevallen is het een menselijke fout die leidt tot het lekken van gevoelige informatie. Denk aan verkeerd geadresseerde e-mails, slordig wachtwoordgebruik of documenten die rondslingeren op kantoor. Data is waardevol, maar kwetsbaar. Daarom is het cruciaal om ook de werkvloer digitaal weerbaar te maken.

VEILIG GEDRAG BEGINT BIJ BEWUSTZIJN

Technologie kan veel beveiligen, maar zonder menselijk inzicht blijft elk systeem kwetsbaar. Een clean desk, een sterk wachtwoord of de juiste e-mailinstelling: het zijn simpele handelingen die grote incidenten kunnen voorkomen. In deze white paper reiken we heldere inzichten aan en bieden we een praktische checklist om organisaties te wapenen tegen datalekken van binnenuit.

Wat wij in de *praktijk* zien

Als advocaat en adviseur van ondernemers zie ik het dag na dag: veel bedrijven investeren in hun product, hun klanten, hun groei — maar vergeten dat ook data vandaag een kernonderdeel van hun werking zijn. Tot er iets misgaat. We krijgen dan vaak dezelfde reacties: "We hadden niet gedacht dat zoiets ons kon overkomen." Of: "We hadden wel ergens een policy, maar niemand gebruikte ze echt."



VGA
LAW & ADR

"Datalekken ontstaan meestal ten gevolge van kleine menselijke fouten: een medewerker die gevoelige informatie naar de verkeerde persoon mailt, een USB-stick die ergens blijft liggen, een wachtwoord dat te gemakkelijk te raden is, of toegang tot klantendata die te breed werd gedeeld binnen het bedrijf.

Vaak zijn de gevolgen ingrijpend: een melding bij de Gegevensbeschermings-autoriteit, paniek op de werkvloer, bezorgde klanten, juridische kosten, of reputatieschade.

Wat mij telkens opvalt: veel van deze risico's zijn perfect beheersbaar. Met de juiste afspraken, een goede basisopleiding, en een bedrijfscultuur die belang hecht aan dataveiligheid.

Daarom hebben we deze white paper opgesteld. We bundelden inzichten uit de praktijk, wetgeving, en concrete tools om bedrijven te helpen hun gegevens-bescherming op orde te krijgen.

In het tweede deel vindt u een lijst concrete do's en don'ts. Zie het als een praktische gids: wat kan u vandaag al aanpakken, waar liggen de quick wins, en hoe vermijdt u dat een klein incident uitgroeit tot een grote crisis? Veel leesplezier."

Laura Van Gompel, advocaat-partner

Datalekken in cijfers

KMO's

47% van de Belgische bedrijven die in 2023 een datalek rapporteerden, zijn kleine of middelgrote ondernemingen.

Kost

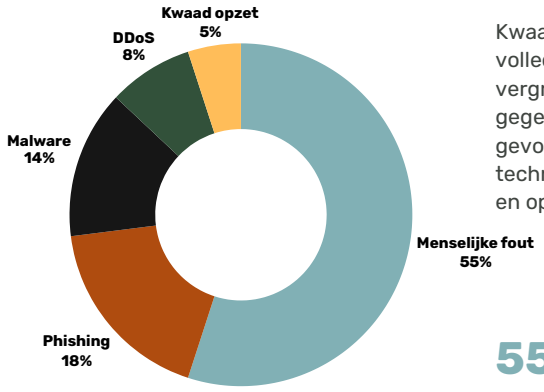
De gemiddelde kostprijs van een datalek voor een KMO in Europa is **147.000,00EUR** (incl. onderzoek, herstel en reputatieschade)

Incidentenplan

44% van de bedrijven betrokken bij een datalek had in 2024 geen incidentenplan bij hun eerste datalek.

18%

Incidenten zijn vaak ook het gevolg van misleiding, meestal via e-mail of sms. Medewerkers klikken op een valse link of geven hun inloggegevens door aan iemand die zich voordoet als een collega, klant of leverancier. Goede reflexen en alertheid maken het verschil.



5%

Een klein percentage van de datalekken wordt veroorzaakt door medewerkers die bewust gegevens misbruiken. Denk aan het downloaden van klantgegevens bij vertrek of het delen van gevoelige info met derden. Ook dit risico vereist een goed toegangsbeleid en heldere afspraken bij in- en uitdiensttreding.

14%

Kwaadaardige software kan volledige systemen vergrendelen of gevoelige gegevens buitmaken. De gevolgen zijn niet alleen technisch, maar ook financieel en operationeel zwaar.

55%

Meer dan de helft van de datalekken ontstaat door menselijke vergissingen. Dit soort fouten is vaak onbedoeld, maar wel perfect te voorkomen met een slim beleid en minimale training.

8%

Soms worden bedrijven getroffen door gerichte aanvallen op hun infrastructuur, zoals DDoS-aanvallen die websites of servers platleggen. Deze aanvallen leiden niet zozeer tot dataverlies. Ze zorgen wél voor chaos en onderbrekingen in de werking.

Intern beleid

Veel KMO's beschikken nog niet over een intern beleid of draaiboek om hier gepast mee om te gaan.

Bovendien groeit de externe druk. Steeds meer bedrijven worden door partners, leveranciers of klanten bevraagd over hun gegevensbeleid. Denk aan vragenlijsten, audits of contractuele verplichtingen rond gegevensverwerking.

Cultuur

Medewerkers weten vaak niet wat ze moeten doen bij een incident, en managers onderschatten de reikwijdte van hun verantwoordelijk-heid onder de GDPR.

Gegevensbescherming begint met bewustzijn, duidelijke afspraken en een veilige dagelijkse praktijk. Werknemers zijn daarbij zowel de grootste risicofactor, als de beste verdediging.

Preventie

Voorkomen is (echt) beter dan genezen.

Bedrijven die hun medewerkers opleiden , ontdekken datalekken gemiddeld 77 dagen sneller. Eenvoudige acties zoals clean desk policies, tweefactorauthenticatie en e-mailversleuteling kunnen het risico op een datalek met tot 80% verlagen.

Quick wins op de werkvloer? Yes, sir.

Credentials

- Zorg voor een sterk wachtwoord: gebruik minstens 13 tekens of uw vingerafdruk.
- Vermijd het gebruik van voor de hand liggende woorden of zinnen.
- Houd privé en werk gescheiden door verschillende wachtwoorden te gebruiken.
- Verander regelmatig uw wachtwoorden en maak gebruik van een (online) wachtwoordkluis.
- Controleer met regelmaat op gespecialiseerde sites of uw gegevens niet zijn gehackt.





- Voeg een extra beveiligingslaag toe door tweefactorauthenticatie in te stellen.
- Zorg voor een opgeruimde werkomgeving door de clean desk en clean screen methode toe te passen. Laat geen wachtwoorden rondslingeren.

Access

- Deel uw inloggegevens nooit met anderen.
- Gebruik voor andere gebruikers extra autorisatie.
- Beperk de toegang tot informatie tot wat strikt noodzakelijk is.
- Sla bestanden niet lokaal op, maar kies voor centrale opslag voor betere beveiliging en automatische back-ups om ongeorganiseerde opslag te voorkomen.
- Laat uw documenten of gegevensdragers nooit onbeheerd achter.
- Laat uw sleutels en toegangsbadges niet rondslingeren.

BYOD & MDM

- Vermijd verwijderbare media zoals USB-sticks, harde schijven.
- Gebruik een heldere mappenstructuur.
- Zorg voor een beveiligde verbinding met werkomgeving vanuit uw thuiscomputer.
- Verstuur geen informatie van uw werk naar uw privé e-mailadres.
- Verbind niet zomaar met openbare wifi zonder VPN.
- Gebruik geen onveilige apps of browsers.
- Bewaar werkdocumenten enkel in bedrijfsomgevingen zoals SharePoint of OneDrive.

Social Media

- Schakel locatievoorzieningen uit en pas tweefactorauthenticatie toe.
- Wees alert bij het downloaden van bestanden of klikken op links.
- Publiceer niet namens uw organisatie zonder toestemming. Deel geen meningen die u of uw organisatie kunnen schaden.
- Deel nooit interne informatie, vertrouwelijke documenten of namen van cliënten of collega's.
- Tag collega's enkel in posts waar zij inhoudelijk bij betrokken zijn én akkoord zijn met de inhoud.



E-mails

- Beperk het verzenden van gevoelige of vertrouwelijke persoonsgegevens.
- Klik niet op verdachte e-mails.
- Schakel het automatisch openen van gedownloade documenten uit.
- Gebruik geen algemene e-mailadressen (zoals info@...) voor persoonlijke opvolging.
- Stuur geen e-mails met een onpersoonlijke of generieke boodschap in BCC naar meerdere ontvangers, tenzij strikt noodzakelijk.
- Gebruik uw inbox niet als archief of takenlijst.
- Behandel binnenkomende e-mails volgens het 4D-principe: Do, Delegate, Defer, Delete.

"Kleine fouten, grote gevolgen? Kleine aanpassingen, grote win."



Gegevensbescherming is vandaag zonder twijfel een zaak voor IT-specialisten, maar eveneens een gedeelde verantwoordelijkheid van elke medewerker, leidinggevende en elk bedrijf.

Met heldere richtlijnen, een gezonde portie bewustzijn en een paar structurele keuzes kunt u als onderneming al heel wat risico's vermijden.

De kracht zit in eenvoud en continuïteit: weten wat u doet, waarom u het doet, en daar consistent naar handelen.

Heeft u vragen over hoe uw organisatie dit concreet kan aanpakken? Wilt u een interne check-up, een duidelijk beleid, of praktische ondersteuning voor uw team?

Wij denken graag met u mee.

TIP: Wist u dat u bij ons team terecht kan voor op maat opleidingen - zowel digitaal als fysiek - voor uw personeel, ICT-partner, management, consultants, etc.?

www.vga.law
info@vga.law
+ 32 11 281 280