

The background features a light gray network of interconnected lines and dots. A large teal rectangle is positioned in the upper left, containing the main title. The title text is white, bold, and sans-serif.

HET NATIONALE AVG EN SECURITY ONDERZOEK

**IS HET MKB VOORBEREID
OP DE AVG EN WAT
IS HET HUIDIGE
BEVEILIGINGSNIVEAU?**

Colofon

Onderzoek door D. Blokvoort
Uitwerking en vormgeving door
R. Dekker

© DataByte, 2018

Alle rechten voorbehouden.
Met dank aan alle respondenten.

HET NATIONALE AVG EN ICT-BEVEILIGINGSONDERZOEK

Is het MKB voorbereid op de AVG en wat is het huidige beveiligingsniveau?

Elke dag is er wel nieuws over de Europese privacyverordening of beveiliging van de ICT-omgeving. Bij DataByte vroegen we ons af hoe bedrijven zijn voorbereid op de Algemene Verordening Gegevensbescherming (AVG) die per 25 mei 2018 gehandhaafd gaat worden. En hoe is het überhaupt gesteld met het beveiligingsniveau in het MKB?

In maart en april zijn we met een online onderzoek gestart met twee hoofdonderwerpen: AVG en ICT-beveiliging. We hebben een online enquête uitgezet via direct mailing en onze social media kanalen. De vragen die gesteld werden, waren gericht op bewustwording, beleidsplannen en acties. De resultaten zijn verrassend en helaas soms risicovol.

In dit onderzoeksrapport nemen we u mee in de wereld van de AVG en ICT-beveiliging. U krijgt inzicht in hoe andere bedrijven zich beschermen. Vergelijk uw bedrijf met anderen en neem eventueel actie door uw beveiligingsbeleid (in samenwerking met uw ICT-leverancier) aan te passen.

Wij wensen u veel leesplezier en mocht u vragen hebben dan kunt u altijd contact met ons opnemen.

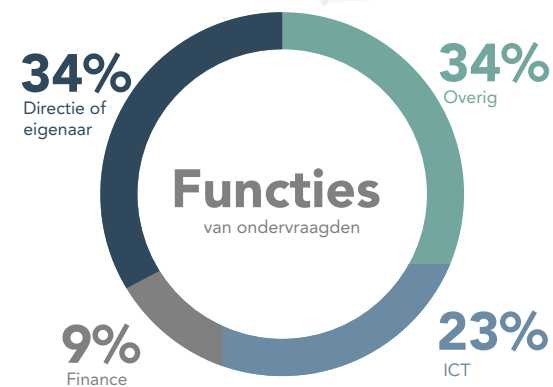
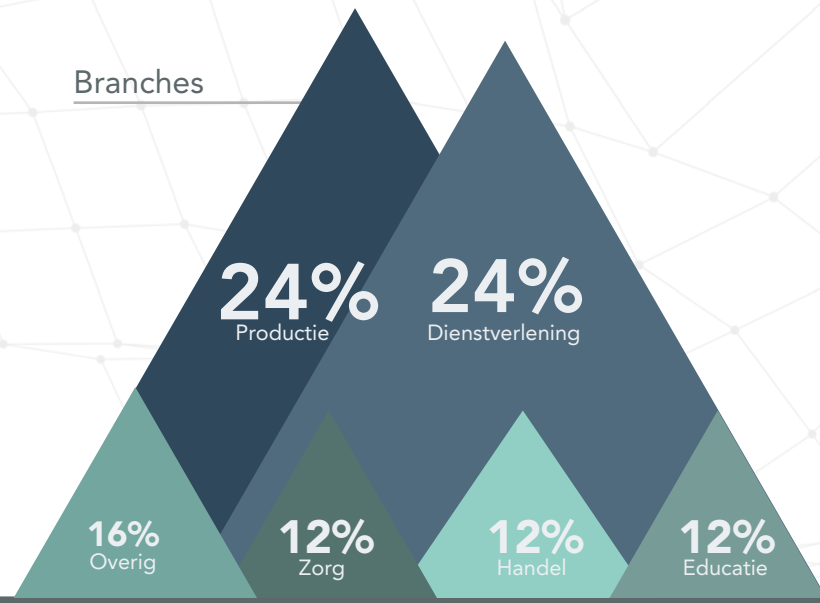
DataByte



AVG-expert Martijn Brinkman: "Zie de AVG niet als een extra maatregel om hardwerkende ondernemers het nog lastiger te maken. De samenleving wordt steeds meer gestuurd op basis van digitale informatie, extra aandacht voor beveiliging en privacy is dus nodig, net als veiligheidsgordels op steeds drukker wordende autowegen."

DE ONDERZOEKSFEITEN

Branches



40

Gemiddeld aantal medewerkers per organisatie

ICT-BEVEILIGING

De hoeveelheid data en het belang van informatie voor uw bedrijf heeft de afgelopen jaren een enorme vlucht genomen. Tegenwoordig willen wij altijd en overal kunnen werken en over onze informatie kunnen beschikken. We gebruiken hiervoor onze eigen apparatuur en vaak zelfs onze persoonlijke, social ID's. Mooie technische ontwikkelingen die ons helpen eenvoudiger bij bedrijfsinformatie te komen en ons in staat stellen flexibeler en efficiënter te werken. Maar, volg het nieuws over cybercrime en het lekken van bedrijfsinformatie en u ziet dat beveiliging van uw ICT-omgeving noodzakelijk is. Organisatorische maatregelen, zoals beleid en procedures, en technische maatregelen beschermen uw organisatie en bedrijfsinformatie.

AVG

De bescherming van uw organisatie en bedrijfsinformatie is in deze tijd mogelijk niet voldoende. De Algemene Verordening Gegevensbescherming (AVG) is in mei 2016 in werking getreden, vanaf 25 mei 2018 wordt de wet ook gecontroleerd en gehandhaafd. Van bedrijven wordt verwacht dat zij de juiste maatregelen treffen om zo veilig mogelijk met persoonsgebonden gegevens van o.a. medewerkers, afnemers en leveranciers om te gaan. Tot 25 mei 2018 krijgen bedrijven de tijd hun bedrijfsvoering conform de AVG in te richten. Het gaat hierbij ook om organisatorische en technische maatregelen, waar niet alleen termen als rechten en plichten de boventoon voeren, maar ook bewustwording, transparantie en verantwoording.

AVG

Wij vroegen ons af in hoeverre het MKB weet wat de Algemene Verordening Gegevensbescherming (AVG) is, en hoe zij zich hierop hebben voorbereid.

Uit ons onderzoek is gebleken dat de meeste MKB-bedrijven wel weten wat de AVG is, maar er zijn minimale voorbereidingen getroffen.

Op grond van de Verordening moet elke verwerking van persoonsgegevens voldoen aan de volgende principes:

rechtmatigheid, behoorlijkheid en transparantie: de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn

doelbinding: de verwerking moet gebonden zijn aan specifieke verzameldoelen

minimale gegevensverwerking: de persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is

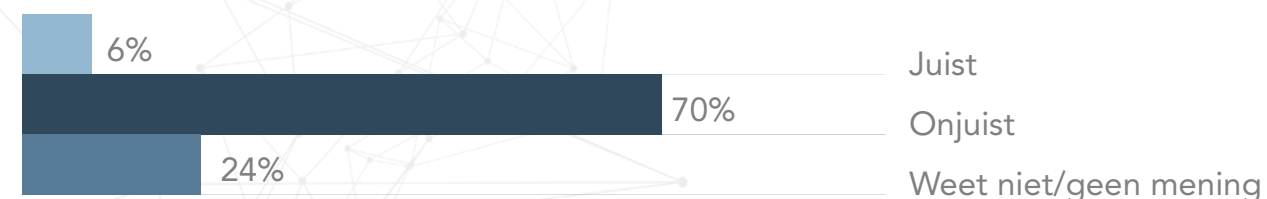
juistheid: de persoonsgegevens moeten juist zijn

opslagbeperking: de persoonsgegevens mogen niet langer bewaard worden dan nodig

integriteit en vertrouwelijkheid: de persoonsgegevens moeten goed beveiligd zijn en vertrouwelijk blijven



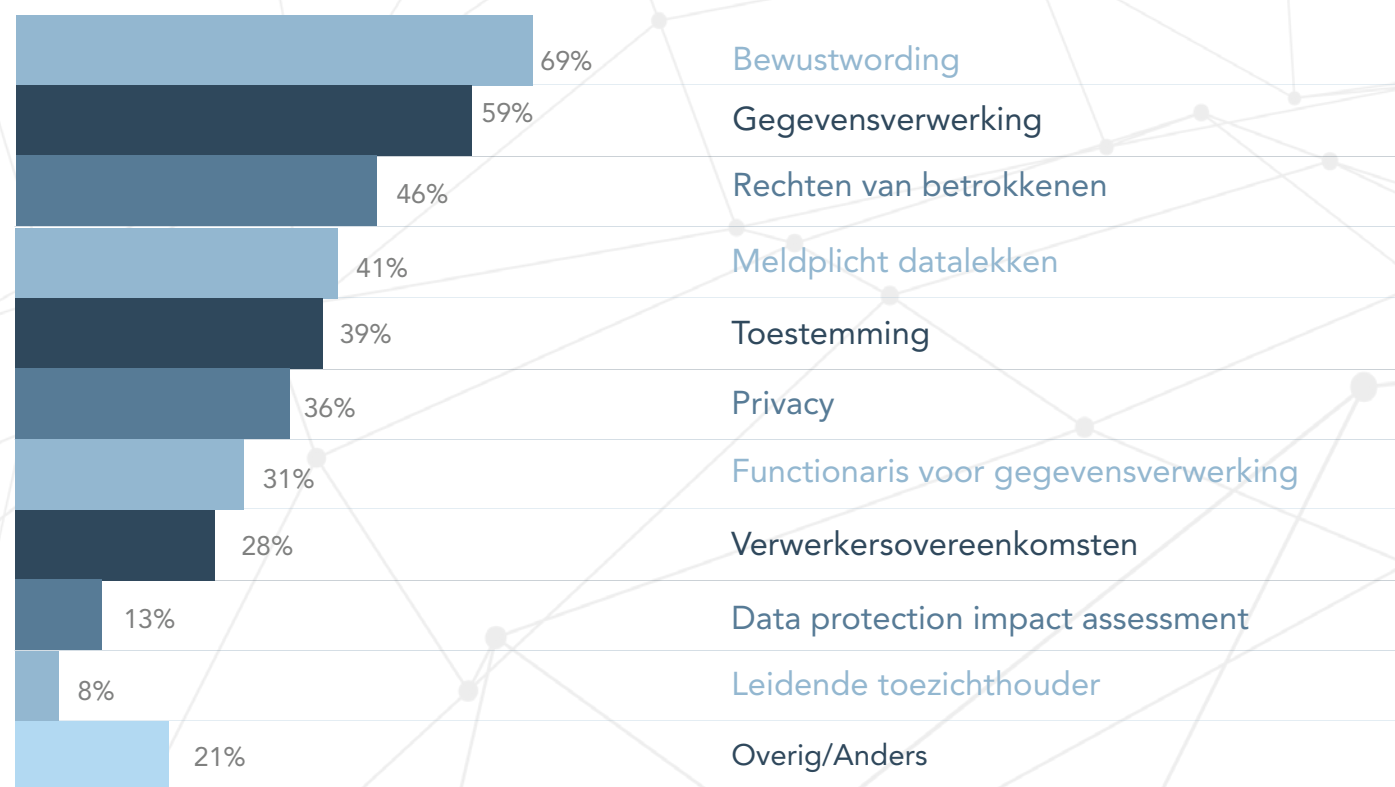
STELLING: DE AVG RICHT ZICH NIET OP DE BEVEILIGING VAN PERSOONSGEGEVENS EN DAT DIT VOLGENS BEDRIJFSVOERING OP DE JUISTE MANIER GEBEURT EN AANGETOOND WORDT.



De stelling is onjuist. De AVG-wet richt zich WEL op de beveiliging van persoonsgegevens en dat dit volgens bedrijfsvoering op de juiste manier gebeurt en aangetoond wordt. Het is duidelijk dat het MKB in Nederland het antwoord op deze vraag weet, maar liefst 70% had het antwoord goed. Maar is het MKB ook voorbereid op deze wet?

10 MAATREGELEN OM AVG-READY TE WORDEN

We vroegen onze respondenten welke maatregelen zij hebben genomen om het bedrijf AVG-ready te maken. De antwoorden zijn gebaseerd op de handige checklist van de Autoriteit Persoonsgegevens (AP). Vaak wordt deze checklist doorlopen samen met uw ICT-leverancier.



Bewustwording

We kunnen concluderen dat het MKB grotendeels begrijpt dat **bewustwording** belangrijk is en wordt toegepast. Het MKB is zich bewust dat relevante medewerkers op de hoogte moeten zijn van de nieuwe privacyregels. Bewustwording is de eerste stap naar mogelijke, toepasbare acties.

Gegevensverwerking

We zien ook dat veel bedrijven de **gegevensverwerking** in kaart hebben gebracht. Dat is een goed vervolg van bewustwording. De gegevensverwerking en de processen die er doorheen lopen moeten zichtbaar zijn, zodat duidelijk is waar er ruimte is voor verbetering.

Rechten van betrokkenen

Wie heeft recht op wat? Mag iedereen bij alle bestanden of zijn er bepaalde rechten? Het is belangrijk om te weten wie waar recht op heeft, zodat gegevens altijd in de juiste handen blijven. De respondenten gaven maar in 39% van de gevallen aan toestemming te vragen voor **gegevensverwerking in de noodzakelijke gevallen**. Dit is belangrijk – de AVG vraagt namelijk van de bedrijven dat zij dit wel doen, en dat zij ook registreren hoe deze gegevens verwerkt worden.

Meldplicht datalekken

De meesten weten waar ze een **datalek moeten melden**. Hoewel het beschermen van de persoonsgegevens in vele gevallen nog niet voltooid is. Er zijn maar in 36% van de gevallen maatregelen getroffen bij het ontwerpen van producten of diensten om gegevens goed te beschermen.



AVG-expert Martijn Brinkman: "Start geen samenwerking met deskundigen die aangeven dat de AVG erg ingewikkeld is. Over het algemeen is de AVG duidelijk gestructureerd en zijn de kaders helder."



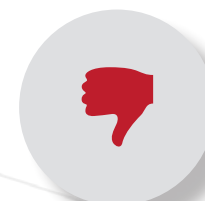
Functionaris

Opvallend is dat maar 30% aangeeft een Functionaris voor gegevensverwerking te hebben aangesteld. Is een Functionaris eigenlijk nodig? De Functionaris voor de gegevensbescherming (FG) houdt binnen een organisatie toezicht op de toepassing en naleving van de AVG. Een FG kan verplicht of vrijwillig worden aangesteld en is verplicht zich te melden bij de AP. **Een FG moet verplicht worden aangesteld bij bijvoorbeeld overheden, gemeenten en bedrijven die van aard personen volgen, zoals cameratoezichtsbedrijven.** Maar ook organisaties die in grote schaal persoonsgegevens opslaan en verwerken, zoals ICT-bedrijven met datacentra, moeten een verplichte FG aanstellen. Van een FG wordt verwacht dat hij of zij bovengemiddelde vakkennis heeft van privacywetgeving en van de praktijk van gegevensbescherming.

Twijfelt u of u een Functionaris moet aanstellen of dat u die nodig heeft? U kunt altijd contact met DataByte of uw eigen ICT-leverancier. Vaak kunnen zij u adviseren en met u bekijken hoe u het beste voorbereid kunt zijn op AVG.

De vereiste expertise en vaardigheden van een Functionaris omvatten in ieder geval:

- kennis van nationale en Europese privacywet- en regelgeving voor gegevensbescherming
- begrip van de gegevensverwerkingen die de organisatie uitvoert
- begrip van ICT- en informatiebeveiliging
- kennis van de organisatie en de sector waarin die actief is
- vaardigheden om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen



Verwerkersovereenkomsten

Uit ons onderzoek blijkt dat de hele zware kost van de AVG, zoals een leidende toezichthouder, verwerkersovereenkomsten en data protection impact assesment (DPIA) **niet worden toegepast**. Alle drie zijn belangrijk en kunnen mogelijke boetes voorkomen. Het is daarom altijd van belang, om bijvoorbeeld verwerkersovereenkomsten te hebben met partijen waarmee u persoonsgegevens uitwisselt. Dit kan al bijvoorbeeld bij een CRM-systeem zijn. U moet inzichtelijk hebben waarom u deze gegevens verwerkt, waar, hoe en wanneer.

■ *DataByte* PRO-TIP

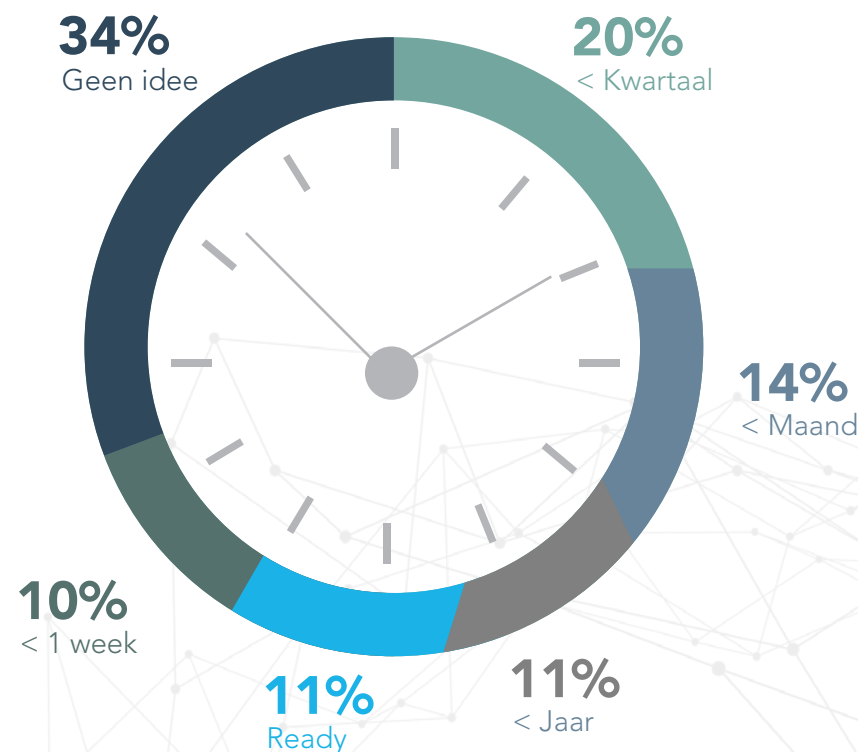
Een verwerkersovereenkomst heeft u nodig wanneer u toestemming geeft aan een andere organisatie voor verwerking van persoonsgegevens. Dit kan bijvoorbeeld een datacenter zijn waarbij gegevens gehost worden, maar ook een CRM-systeem waarin u persoonlijke gegevens host over een klant. Veel (grote) externe partijen hebben een standaard verwerkersovereenkomst waar u gebruik van kan maken. Op de website van Rijksoverheid vindt u twee voorbeelden van verwerkersovereenkomsten.

Bent u al AVG-ready? Bekijk zelf welke van de 10 maatregelen u al heeft genomen en waar u nog aan moet werken. Vaak voert u dit samen uit met uw ICT-leverancier. Mocht u advies zoeken, kunt u altijd vrijblijvend contact met ons opnemen.



AVG-READY, HOE LANG DUURT DAT?

De meeste respondenten hebben geen idee hoe lang zij nodig hebben om AVG-ready te worden. Anderen zijn van mening enkele maanden nodig te hebben en enkele respondenten slechts één dag. Maar een klein deel was al klaar met hun voorbereidingen.



Gemiddeld genomen duurt **het minimaal zes maanden** om klaar te zijn voor de AVG. U dient eerst de processen te ontdekken, deze in kaart te brengen, te beoordelen, te herzien en toe te passen. De trajecten die wij begeleiden hebben een gemiddelde doorlooptijd van slechts 4,5 maand door de AVG-methode die wij hebben ontwikkeld.



HEEFT U AVG-BUDGET BESCHIKBAAR?

Voorbereiden op de AVG is niet gratis. Hoewel er niet direct geld beschikbaar moet worden gesteld, zal uw organisatie wel tijd moeten investeren. En nadat duidelijk is waar mogelijke beveiligingsrisico's in uw organisatie zitten, zult u mogelijk een externe ICT-partij moeten inhuren om deze risico's te verhelpen en verbeteringen te borgen. Daarom hebben we onderzocht of het MKB budget beschikbaar heeft gesteld voor hun bedrijf om 'AVG-ready' te worden.

27% van de respondenten geeft aan dat er een budget beschikbaar is om het bedrijf AVG-ready te maken, waarvan 33% respondenten aangeeft beschikbaar te maken wat er nodig is.

Het merendeel (39%) geeft aan dat er geen budget beschikbaar is, bijvoorbeeld omdat dit wordt meegenomen in standaard budgetten en bedrijfsvoering. Anderen geven aan geen idee te hebben of dat het budget nog uitgerekend moet worden. Een klein deel geeft aan in de veronderstelling te zijn alleen procedures te moeten schrijven.

■ DataByte PRO-TIP

Het grootste budget dat u nodig heeft is tijd. U moet collega's vrij maken van werkzaamheden om de processen in uw organisatie te ontdekken, te herzien en te verbeteren. Daarnaast moet u bewustwording creëren bij uzelf en uw collega's door bijvoorbeeld een bewustwordingstraining. Deze training, naast het feit dat uw collega's hier tijd in moeten investeren, kost geld.

Vaak schakelen organisaties ook hulp in van externe ICT-partijen om hun ICT-beveiliging op peil te brengen en te behouden. Ook daarvoor zult u budget vrij moeten maken.



IS HET MKB VOORBEREID OP EEN DATALEK?

73%

Weet waar een datalek
gemeld moet worden

71%

Heeft nog nooit een
datalek meegemaakt

Uit ons onderzoek blijkt dat de meeste bedrijven nog nooit een datalek hebben meegemaakt (71%). 73% van de respondenten weten waar datalekken gemeld moeten worden, namelijk bij de Autoriteit Persoonsgegevens (AP). 9% denkt dat dit bij hun ICT-leverancier is en 22% geeft aan dat zij niet weten waar ze datalekken moeten melden.

De juiste manier van het melden van een datalek is als volgt:

1. Meld het datalek bij de interne functionaris voor gegevensbescherming (FG) of Security Officer.
2. Als u die niet heeft, meld het lek dan bij uw leidinggevende en ICT-verantwoordelijke.
3. Bekijk waarom gegevens zijn gelekt (oorzaak), en welke gegevens zijn gelekt (gevolg).
4. Zijn er gegevens gelekt van derden, dan moet u altijd een melding doen bij de AP.
5. Zijn de gegevens versleuteld en kunt u dat aantonen? Dan hoeft u het lek niet te melden bij AP.
6. Interne registratie gemelde datalekken.



AVG-expert Martijn Brinkman: "Mijn advies? Start vandaag nog! De gevolgen van nalatigheid zijn groter dan de puntjes nog niet op de spreekwoordelijke i hebben."

ICT-BEVEILIGING

U weet nu hoe u een datalek kunt melden. Bij DataByte hanteren wij het gezegde: 'Voorkomen is beter dan genezen'. Liever een goed beveiligingsbeleid dat wordt nageleefd om datalekken en beveiligingsrisico's tegen te gaan, dan ze te moeten oplossen of lekken te moeten melden.

Om te bekijken hoe het gesteld is met de ICT-beveiliging bij bedrijven in het MKB hebben we enkele vragen opgesteld. De resultaten leest u op de volgende pagina's.

In de resultaten op de volgende pagina's staat een quiz waarmee u kunt testen hoe goed u de beveiliging in uw organisatie beheert. Doe onze Security Quiz, tel de punten op en zie hoe uw beveiliging scoort.

HOE VAAK HEEFT HET MKB HET OVER ICT-BEVEILIGING IN DE ORGANISATIE?

Is ICT-beveiliging belangrijk?

98% 

 **2%**

Maar liefst 60% gaf aan dat ICT-beveiliging zeer belangrijk is, 38% vindt het belangrijk en 2% vindt het niet belangrijk.

Maar toen we vroegen hoe vaak ICT-beveiliging op de agenda staat, gaf 46% aan dat het vaak op de agenda staat, en 47% gaf aan van niet. De oorzaak hiervan was een gebrek aan kennis en inzicht, omdat het onvoldoende leeft of omdat de ICT wordt beheerd door een externe partij.

46%  

  **47%**

QUIZVRAAG 1

Hoe belangrijk is ICT-beveiliging voor u?

- A) zeer belangrijk
- B) niet belangrijk

QUIZVRAAG 2

Hoe vaak staat ICT-beveiliging op de agenda?

- A) Elke week
- B) Elke maand
- C) Elk half jaar of langer
- D) Nooit



BEVEILIGINGSBELEID

Een beveiligingsbeleid helpt in kaart te brengen hoe om gegaan wordt met veiligheid, hoe de situatie nu is en waar naar toe wordt gewerkt. Het kan dienen als een planning voor korte en lange termijn doelen.

Ook wordt daarin vastgelegd wat er gedaan wordt bij bijvoorbeeld een virusuitbraak of datalek.

We vroegen ons af in hoeverre het MKB over een ICT-beveiligingsbeleid beschikt.

Ongeveer de helft van het MKB heeft geen beveiligingsbeleid. De andere helft beschikt wel over een beveiligingsbeleid binnen de organisatie.* Wij gaan uit van drie verschillende beveiligingsbeleidsstukken:

37%

Operationeel beleid
met bijvoorbeeld acties, taken,
tijdspad en mankracht.

25%

Tactisch beleid
met bijvoorbeeld korte termijn doelen,
plannen en technieken.

14%

Strategisch beleid
met de stip aan de horizon, visie,
structuur en lange termijn doelen.

46%

Weet niet/ geen mening

*Respondenten hadden meerdere keuzemogelijkheden, hierdoor is het totaalpercentage groter dan 100%.



AVG-expert Martijn Brinkman: "Het meest spannende? De aantoonplicht, het moet aantoonbaar zijn dat de informatiebeveiliging op een kwalitatief niveau is geborgd. Borgen kan eenvoudig in speciaal ontwikkelde applicaties, maar kan ook in een informatiebeveiligingsmatrix."

QUIZVRAAG 3

Het schrijven van een beveiligingsbeleid is een vak apart. Weet u welke items daarin naar voren moeten komen? Een beveiligingsbeleid wordt vaak geschreven door Business Consultants van een ICT-partij. Over welk beleid beschikt uw organisatie?

- A) Operationeel
- B) Tactisch
- C) Strategisch
- D) Wij hebben geen beleid



ICT-BEVEILIGINGSPROCEDURES

We vroegen onze respondenten of ze een beveiligingsprocedure hebben en waar deze uit bestaat. Bijna de helft van de ondervraagden beschikken hier niet over (42%). De andere helft heeft wel een procedure of heeft er één in ontwikkeling. Voorbeelden van de procedures zijn regelmatige backups, updates en antivirusprogramma's. Maar wat het meest wordt ingezet, ziet u in de diagram hiernaast.

QUIZVRAAG 4

Van welke beveiligingsoplossingen maakt u gebruik? Bekijk de diagram op de pagina hiernaast. U verdient één punt bij elke oplossing waar uw organisatie over beschikt.

92%

Individuele werkplekken hebben wachtwoorden

85%

E-mailserver heeft spamfilter en een antivirusfilter

81%

Er worden back-ups van de servers gemaakt en deze worden buiten het bedrijf of in de cloud bewaard.

79%

Netwerkkapparaten hebben een wachtwoord

71%

Mobile devices hebben een wachtwoord

69%

Het besturingssysteem (OS) wordt regelmatig ge-update

54%

Er is een gescheiden draadloos gastennetwerk

50%

Het netwerk beschikt over een next-generation firewall

37%

Het netwerk beschikt over een SSL/VPN toegang

37%

Thuiswerkers maken gebruik van een tweestapsverificatie (tokens)

UITSLAG QUIZ

Hoe is het gesteld met uw ICT-beveiliging?

1

A: 2
B: 0

2

A: 4
B: 3
C: 2
D: 0

3

A: 2
B: 3
C: 4
D: 0

4

Per oplossing
1 punt

UW UITSLAG:

 0-7 punten

U kunt wel wat hulp gebruiken bij het beter beveiligen van uw ICT. De kans op datalekken en virussen is groot. We adviseren u om uw ICT-beveiliging beter op orde te krijgen in samenwerking met een ICT-leverancier.

  8-15 punten

Uw ICT-beveiliging is redelijk up and running. U voldoet hoogstwaarschijnlijk aan de standaard eisen die uw organisatie heeft. Maar of uw ICT-beveiliging up-to-date is en of u volledig beschermd bent tegen bijvoorbeeld uitbraken, dat betwijfelen we.

 16-20 punten

U bent goed op weg! Uw ICT-beveiliging komt als goed uit de quiz. Maar bent u ook al voorbereid op AVG en heeft u alle 10 stappen doorlopen? En hoe gaat u uw beveiligingsbeleid onderhouden?

TEN SLOTTE

Wij zijn dit onderzoek gestart om te bekijken hoe het gesteld is met ICT-beveiliging in het MKB. Daarbij wilden wij ook onderzoeken hoe het MKB voorbereid is op AVG.

MKB onderschat AVG en ICT-beveiliging

Hoewel we hebben gezien dat het MKB een aantal voorbereidingen heeft getroffen voor AVG, zien we ook nog veel verbeterpunten en mogelijke risico's. Van de 10 stappen geadviseerd door de Autoriteit Persoonsgegevens, werden maar 4 veel uitgevoerd. Dat zijn er 6 te weinig.



Uitgevoerd

1. Bewustwording
2. Gegevensverwerking
3. Rechten van betrokkenen
4. Meldplicht datalekken



Niet uitgevoerd

1. Toestemming
2. Privacy
3. Functionaris voor gegevensverwerking
4. Verwerkersovereenkomsten
5. Data protection impact assessment
6. Leidend toezichthouder

Vorbereiden op AVG is niet ingewikkeld, maar alleen voorbereid zijn op AVG is niet de oplossing. Als u hieraan begint wordt ook uw ICT-beveiliging onder de loep genomen. Door dit te doen komt u vaak achter mogelijke risico's, processen die verbeterd kunnen worden en beleidsstukken die u kunt opstellen voor de lange termijn. Vaak weten ondernemingen niet waar ze moeten beginnen om hun beveiligingsprocedures in kaart te brengen om o.a. voorbereid te zijn op AVG.

De conclusie van ons onderzoek: het MKB onderschat AVG en ICT-beveiliging, er is dus nog werk aan de winkel!



Drukkerij 3, 4651 SL Steenbergse
t: 0167 544 544
e: info@databyte.nl