bit
internet technology

Security *en* privacy

Hoe belangrijk vinden we het nu écht?

Eindverantwoordelijken en beslissers over databeheer, dataopslag en databeveiliging

Onderzoeksrapport 2022

Voorwoord

Al vanaf het prille begin – inmiddels ruim 25 jaar geleden – is BIT voorvechter van een vrij, open en veilig internet. Waar 'internet' destijds een doel op zich was, is het nu een onmisbaar medium geworden waarover zowel consumenten als bedrijven en organisaties verbinding maken met IT systemen.

Door het internet is het – vanuit technisch oogpunt – bijna volledig irrelevant geworden waar die systemen zich bevinden. Zolang ze via het (inter-) netwerk bereikbaar zijn, maakt het niet zo veel uit of je werkt op een systeem in je eigen kelder, ergens anders in Nederland of aan de andere kant van de oceaan. Vanuit technisch oogpunt. Maar hoe zit het met de veiligheid van je data als je het uit handen geeft aan een grote buitenlandse aanbieder van clouddiensten? In welk land staan je data? Welke bedrijven en overheden hebben toegang? Hoe afhankelijk ben je van zo'n aanbieder? En ben je als klant ook belangrijk voor zo'n aanbieder? Inmiddels is wel duidelijk dat de gemiddelde Nederlander – ondanks wetgeving – niet zo veel geeft om privacy. Of wel, maar denkt dat het toch al een verloren zaak is. Maar is dat wel zo? En spelen er niet meer belangen? Wat als bedrijfsgegevens bij de concurrent terechtkomen? En maken we ons niet veel te afhankelijk van andere landen?

Hoog tijd dus om een aantal vragen te formuleren en aan professionals voor te leggen, en dat hebben we gedaan.
De antwoorden op die vragen zijn op zijn minst opmerkelijk te noemen. Eigenlijk ben ik best een beetje geschrokken van de onverschilligheid en het gebrek aan kennis waarmee beslissingen lijken te worden genomen. Beslissingen die van invloed zijn op de eigen organisatie, maar ook op die van klanten, leveranciers of andere relaties. Maar dat is mijn gevoel.

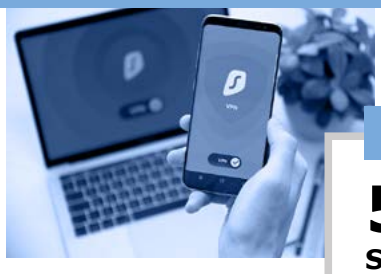
Ik ben benieuwd of u bij het lezen van dit rapport hetzelfde gevoel krijgt.

Alex Bik *CTO BIT*

INHOUD

Managementsamenvatting

Data onderbrengen bij een grote Amerikaanse of Aziatische public cloudprovider kan privacy- en securityrisico's met zich meebrengen. Zo maken deze hyperscalers lang niet altijd bekend waar ze de data van jouw bedrijf opslaan. Als je daar zelf geen afspraken over maakt, kan het zijn dat bedrijfsgevoelige en privacygevoelige data van klanten en/of medewerkers worden opgeslagen in een Amerikaanse cloud en zo buiten de Europese wet- en regelgeving vallen. Het is belangrijk dat organisaties zich hiervan bewust zijn en de juiste maatregelen nemen om te voorkomen dat dit gebeurt.

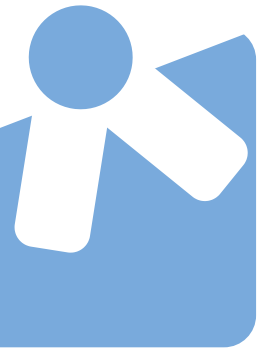


58%

Slechts 58% weet wat hun leverancier op het gebied van veiligheid en privacy doet

Om erachter te komen in hoeverre eindverantwoordelijken en beslissers over databeheer, dataopslag en databeveiliging zich bewust zijn van de securityrisico's die de public clouddiensten van grote Amerikaanse hyperscalers met zich meebrengen, heeft BIT een onderzoek gedaan onder 1089 Nederlandse werkenden. De respondenten zijn uitvoerend, adviserend, mede-beslissend, beslissend en/of eindverantwoordelijk op het gebied van IT binnen hun organisatie.

De uitkomsten zijn opvallend. Want waar veiligheid en privacy tot de top drie selectiecriteria horen bij de keus voor een hosting- of cloudprovider, weet slechts 58 procent wat hun leverancier doet op dit gebied. Maar liefst 17,5 procent van de mensen die betrokken zijn bij beslissingen op dit gebied, weet zelfs niet wat de eigen organisatie doet om data te beveiligen. Ze beslissen dus over zaken waar ze geen of onvoldoende kennis van hebben. Als iemand in de decision making unit zegt dat 'het wel goed zit met de security bij deze leverancier', wordt dit vaak voor waarheid aangenomen.



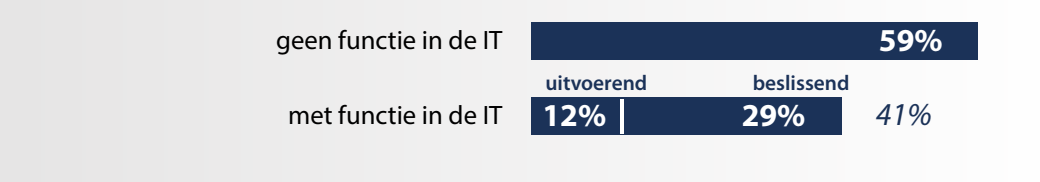
Nog geen vijftig procent van de organisaties controleert regelmatig op welke locatie data staan. Als een cloudprovider zou beslissen om data te verplaatsen naar een ander datacenter, zou dat in de helft van de organisaties dus heel lang onopgemerkt kunnen blijven. Toch is het vertrouwen in de maatregelen die de eigen organisatie neemt groot. Maar liefst 73,7 procent is niet bang dat de eigen organisatie te maken krijgt met een privacyschandaal. En dat terwijl ruim 36 procent van de organisaties al eens een datalek heeft meegemaakt en 18 procent überhaupt niet zeker weet of hun organisatie ooit slachtoffer is geweest van een hack of datalek. Opvallend is ook dat bijna de helft van de respondenten (ruim 46%) vindt dat de media privacyschandalen vaak uitvergroten. Toch zijn ze kennelijk niet bang voor reputatieschade van hun eigen bedrijf.

De conclusie van dit onderzoek is dan ook dat security en privacy voor de meeste organisaties op papier belangrijke waarden zijn en ook een grote rol spelen bij de selectie van een hosting- of cloudprovider, maar dat er daarna in de praktijk nauwelijks nog naar wordt omgekeken. Kennelijk is het bewustzijn van de risico’s op het lekken van bedrijfsgevoelige of privacygevoelige informatie nog niet erg groot.

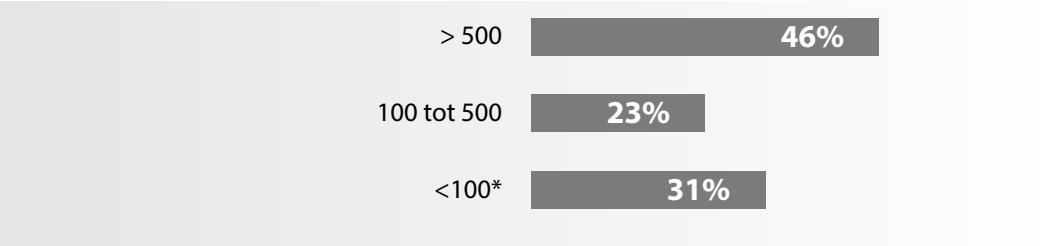
Deelnemende organisaties in beeld

In het voorjaar van 2021 voerde BIT een onderzoek uit onder 1089 professionals die zeer goed of redelijk goed op de hoogte zijn van het databeheer, de dataopslag en de databeveiliging in hun organisatie.

Beslissers op IT-gebied in 1089 ondervraagde bedrijven



Aantal medewerkers ondervraagde bedrijven



** In deze kleinere organisaties is in veel gevallen de directeur/eigenaar ondervraagd, omdat IT binnen zijn/haar takenpakket valt.*

Analyse deelnemers

Voor het onderzoek is bewust gezocht naar organisaties uit een grote diversiteit aan branches. De meeste deelnemers zijn werkzaam in zorg & welzijn, overheid, handel & industrie en financiële dienstverlening.

In 43 procent van de deelnemende organisaties maken alleen medewerkers gebruik van de IT-omgeving. In de overige 57 procent staat de IT-omgeving open voor zowel medewerkers als klanten. De manier waarop klanten in de IT-omgeving van het ondervraagde bedrijf werken, verschilt per branche. In de financiële dienstverlening zou het bijvoorbeeld kunnen gaan over een online boekhoudomgeving. In de zorg kun je denken aan patiënten en cliënten die online afspraken maken en hun dossier inzien, terwijl in handelsbedrijven en in de retail het vooral gaat om webshops.

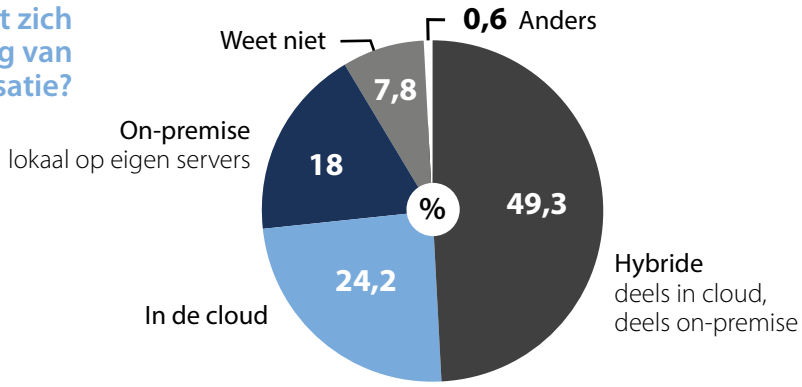
69 procent van de deelnemers heeft alleen vestigingen in Nederland, 31 procent van de bedrijven zijn multinationals met kantoren in het buitenland. Die buitenlandse kantoren bevinden zich het vaakst in Europa, gevolgd door de VS en Azië.

In bedrijven waar ook klanten gebruikmaken van de IT-omgeving, zijn de klantengroepen internationaler dan de vestigingslocaties; 49 procent focust zich op Nederlandse afnemers, hetzelfde percentage richt zich op zowel Nederlandse als buitenlandse klanten, en 2 procent heeft alleen maar klanten in het buitenland.

De status quo van IT-beheer, hosting en cloud

De eerste serie vragen in het onderzoek heeft betrekking op het IT-beheer. Van de ondervraagde organisaties beheert ruim vier op de tien de IT-omgeving zelf. Eenzelfde aantal heeft het beheer deels uitbesteed en deels in eigen hand, terwijl een kleine twintig procent het beheer volledig heeft ondergebracht bij een IT-leverancier.

Waar bevindt zich de IT-omgeving van uw organisatie?



Hybride landschap is populairst

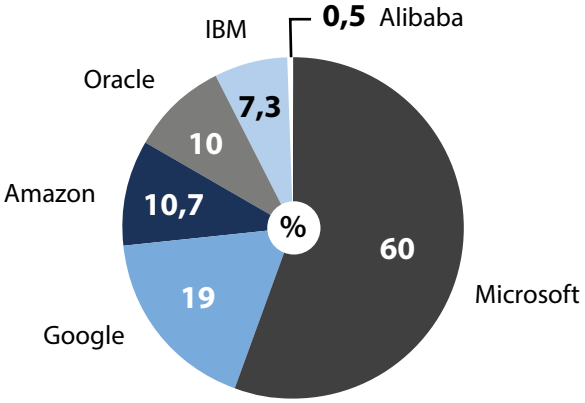
Ruim de helft van de organisaties heeft een hybride landschap. Dat wil zeggen dat de organisaties een deel van hun IT-omgeving in de cloud hebben staan en een ander deel on premise. Ruim een kwart van de bedrijven is al volledig over naar de cloud, terwijl een kleine twintig procent de volledige omgeving nog on-premise heeft staan. Facilitaire dienstverleners zijn het meest 'cloud minded': maar liefst 64 procent van die bedrijven zit volledig in de cloud, op ruime afstand gevolgd door onderwijs en onderzoek, waar ruim 41 procent zijn volledige omgeving in de cloud heeft ondergebracht. Branches die hun on-premise omgeving nog volledig omarmen zijn de overheid (29% van de overheidsorganisaties zegt nog geen gebruik te maken van clouddiensten), FMCG (26%) en handel en industrie (23%).
Opvallend is dat bedrijven in de ICT en telecom het vaakst gebruikmaken van een hybride landschap: respectievelijk 63 en 61 procent.

Datacenter in Nederland

De meeste organisaties (72 procent) maken gebruik van een datacenter in Nederland. Als ze hun data buiten onze landsgrenzen opslaan, gebeurt dat het vaakst in Europa (18 procent), gevolgd door de Verenigde Staten en Azië. Opvallend is dat 28 procent van de bedrijven dus geen datacenter in Nederland heeft. Bij de keuze voor de datacenterlocatie lijkt het geen rol te spelen waar bijvoorbeeld klanten gevestigd zijn. Het is namelijk niet zo dat bedrijven met veel klanten in de VS veel vaker dan andere organisaties kiezen voor een datacenter in de VS; of bedrijven met klanten in Azië voor een datacenter in Azië.

Welke cloudleveranciers?

Van welke clouddiensten maakt u gebruik?



Van de ondervraagde organisaties maakt ruim zes op de tien gebruik van de clouddiensten van Microsoft. Het kan hierbij gaan om IaaS en PaaS (Azure), maar ook om SaaS (bijvoorbeeld Office365).
Nummer 2 op de lijst is Google, waar 19 procent clouddiensten bij afneemt. Ook deze leverancier heeft een breed aanbod aan zowel IaaS-, PaaS- als SaaS-diensten. Amazon scoort een derde plaats met 10,7 procent. Deze leverancier levert met AWS primair IaaS- en PaaS-diensten. De lijst wordt gecompleteerd door Oracle (10%), IBM (7,3%) en Alibaba (0,5%).

Gebruikers van clouddiensten van bovengenoemde grote spelers zeggen opvallend vaak zeker te weten dat hun privacygevoelige data in Nederland staan. Nu hebben Microsoft, Google, IBM en Oracle ook daadwerkelijk datacenters in Nederland en kun je zelf aangeven of je wilt dat je data in Nederland staan. Maar ook bijna 73 procent van de Amazon-klanten denkt dat hun data in Nederland staan, terwijl Amazon geen Nederlandse datacenters heeft. Respondenten die gebruikmaken van de diensten van Alibaba maken dezelfde denkfout.

Het valt op dat er weinig verschil is tussen branches als het gaat om gebruik van clouddiensten. Waar je wellicht zou verwachten dat bedrijven uit sectoren die met zeer privacy- of concurrentiegevoelige data werken (zoals zorg, onderwijs, financiële dienstverlening) voorzichtiger zijn met het gebruik van SaaS-, PaaS- of IaaS-diensten, blijkt dat niet uit dit onderzoek.

Een ander opvallend gegeven is de score op de stelling ‘het maakt mij niet uit welke cloud mijn organisatie gebruikt’. Eigenlijk zijn alleen juridische dienstverleners, bedrijven in de communicatie en media en bedrijven die zich richten op de consumentenmarkt vrij kritisch en zeggen: jawel, dat maakt wel uit. In andere sectoren is men een stuk laconieker. Meer dan zestig procent van de respondenten in de facilitaire dienstverlening, in horeca & toerisme en in transport & logistiek zegt: nee.

Privacy en security

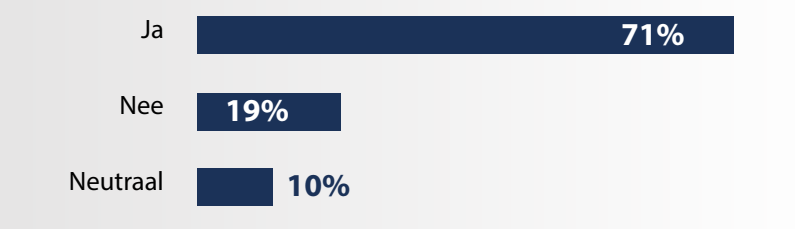
De belangrijkste reden om het onderzoek uit te voeren, is om inzicht te krijgen in het bewustzijn op het gebied van privacy en security. Realiseren organisaties zich dat ze extra maatregelen moeten nemen op het gebied van privacy en security als ze gebruikmaken van de public cloud van Amerikaanse of Aziatische aanbieders? Begrijpen ze dat cloudproviders die data opslaan buiten de EU minder zekerheden kunnen geven dat ze voldoen aan de EU-wetgeving, zoals de Algemene verordening gegevensbescherming (AVG)? Want Amerikaanse cloudproviders hebben zich te houden aan de Cloud Act. Dat betekent dat databases met klantgegevens door de Amerikaanse overheid opgevraagd kunnen worden.

Veel vertrouwen in securitymaatregelen van cloudproviders

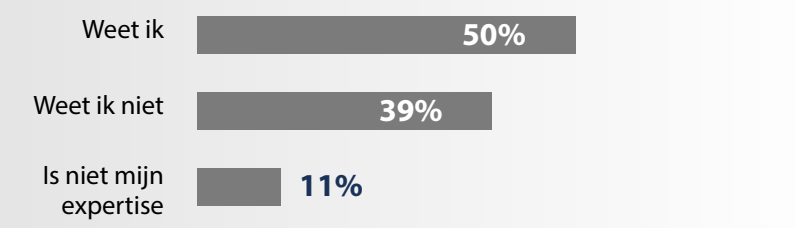
We vroegen respondenten naar de perceptie van de cloud. De cloud heeft in de beginjaren te kampen gehad met een wat negatief imago als het gaat om security en privacy, mede doordat de wetgeving toen nog vrij onduidelijk was. Nu de wetgeving is verbeterd, heeft het vertrouwen zich hersteld, zo laat dit onderzoek zien. Want hoewel er nog altijd beslissers zijn die weinig vertrouwen hebben in de cloud als het gaat om databescherming en privacy (ruim 19% van de respondenten), geeft 71 procent aan dat vertrouwen wel te hebben. Een kleine 10 procent antwoordt neutraal. Niet geheel verwonderlijk zijn het vooral de organisaties met een volledige on-premise omgeving die weinig vertrouwen hebben in de cloud als het gaat om databescherming en privacy.

Van de organisaties die gebruikmaken van de cloud – in totaal 731 respondenten – weet de helft goed wat de cloudprovider doet op het gebied van data-

Vertrouwt u uw data toe aan de cloud?



Wat doet uw cloudprovider op gebied van databeveiliging?



beveiliging. 39 procent weet het niet en vertrouwt volledig op de leverancier en 11 procent staat hier te ver van af om een zinnig antwoord te geven. Logischerwijs zijn IT'ers veel beter op de hoogte van de securitymaatregelen van hun cloudprovider dan de beslissers die niet in IT werken.

Opvallend is het verschil tussen sectoren. Juist de zorg (37,8% is op de hoogte) en de overheid (48,6%) scoren laag op 'ik weet goed wat mijn cloudprovider doet op het gebied van databescherming'. Terwijl de organisaties in deze sectoren uit de aard van hun werk te maken hebben met zeer privacygevoelige data en aan strenge wetgeving moeten voldoen. Communicatie en media (bijna 77%) en juridische dienstverleners (71,43%) scoren een stuk beter.

72,3%
van de organisaties heeft privacy op directieniveau op de agenda staan

Belang van privacy

Een onderwerp dat nauw samenhangt met security is privacy. Om privacy te garanderen is het naast goede security ook belangrijk dat data van personen (in de regel klanten en medewerkers) in Europa blijven en uitsluitend onder Europese jurisdictie blijven vallen. Daarnaast moet de toegang tot deze privacygevoelige data met rollen en rechten goed worden afgeschermd. Dat organisaties dat belangrijk vinden, blijkt wel uit het feit dat privacy in 72,3 procent van de organisaties op directieniveau op de agenda staat. Dat is niet zo vreemd, want 44 procent krijgt regelmatig vragen van klanten over hoe de privacy van hun data is gewaarborgd.

Maar liefst tweederde van de organisaties (65,6%) zegt goed te weten waar klant- en andere privacygevoelige data staan en wie daar toegang toe heeft. Toch controleert nog niet de helft van de organisaties (48,3%) regelmatig waar de data staan. Ze vertrouwen dus volledig op ooit gemaakte afspraken met een leverancier.

>50%
van de organisaties controleert regelmatig waar klant- en andere privacygevoelige data staat

Externe expertise gewenst bij inregelen van privacy

Privacy is een onderwerp waar organisaties graag externe expertise bij inschakelen. Bijna een derde (32,7%) heeft het inregelen van privacy geheel of grotendeels extern belegd, terwijl 48,4 procent weliswaar een consultant in de hand nam, maar zelf in de lead bleef.

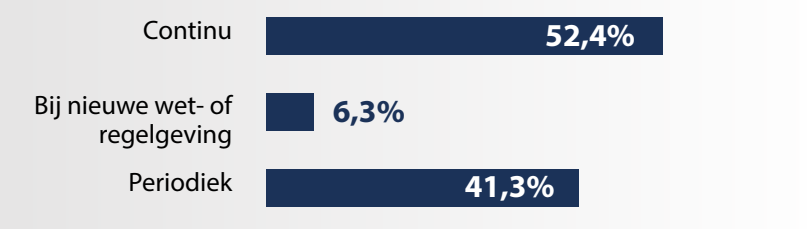
58 procent van de organisaties wil ook heel nauwgezet van partnerorganisaties uit het ecosysteem weten wat zij doen om de privacy van klantgegevens te waarborgen. Ze nemen geen genoegen met simpelweg een vinkje bij de verwerkersovereenkomst.

Voldoen aan privacywetgeving

In ruim de helft van de organisaties (52,4%) wordt continu gemonitord of de organisatie nog voldoet aan privacywetten en -regels. 6,3 procent controleert dit op het moment dat er nieuwe wet- of regelgeving wordt geïntroduceerd. De overige organisaties voeren periodieke controles uit (eens per kwartaal of eens per jaar). Overigens wordt ook op dit gebied externe expertise op prijs gesteld. Want hoewel 78,8 procent van de ondervraagden aangeeft goed op de hoogte te zijn van de privacywetgeving, waardeert 58,3 procent de voorlichting van hun IT-leverancier op dit gebied.

Sinds de inwerkingtreding van de AVG zijn sommige organisaties verplicht een functionaris gegevensbescherming aan te stellen. Dit geldt voor alle overheidsorganisaties, voor organisaties die bijzondere persoonsgegevens verwerken (over bijvoorbeeld gezondheid, ras, politieke opvatting of geloofsovertuiging) en organisaties die regelmatig en stelselmatig vanuit hun kernactiviteiten individuen observeren (zoals banken). Het is logisch dat sectoren als juridische dienstverlening (89%), energiebedrijven (89%) en b2c-bedrijven (83%) hoog scoren. Dit zijn immers bedrijven die ofwel op grote

Hoe vaak controleert u of u voldoet aan privacywetgeving?



schaal of heel gevoelige persoonlijke gegevens verwerken. Wat opvalt is dat slechts 82% van de overheidsorganisaties zegt een functionaris gegevensbescherming te hebben en slechts 73% van de organisaties in zorg en welzijn. Sectoren die onverwacht hoog scoren zijn technische dienstverlening (59%) en facilitaire dienstverlening (75%).

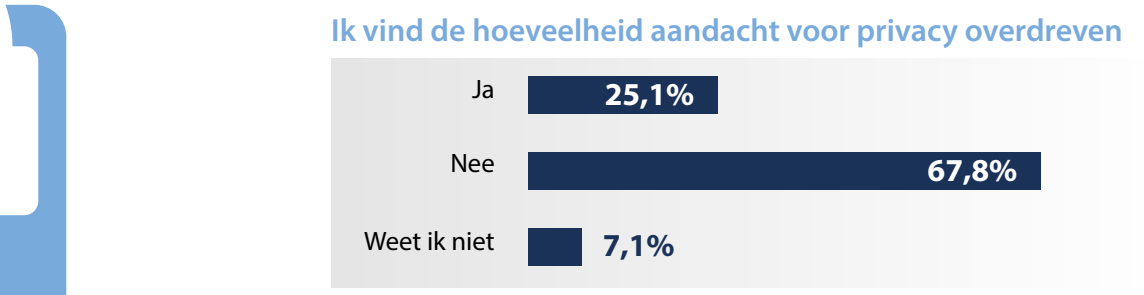
Datalekken worden niet altijd gemeld

Ondanks de aandacht voor security en privacy en zorgvuldigheid van organisaties op dit gebied, heeft ruim 36 procent van de organisaties wel eens een datalek meegemaakt. Bijna 46 procent van de respondenten steekt zijn hand ervoor in het vuur dat dat nooit is gebeurd. Terwijl 18 procent aangeeft niet zeker te weten of hun organisatie ooit slachtoffer is geweest van een hack of datalek. Met name dit laatste percentage is opvallend, want de AVG schrijft voor dat er melding moet worden gemaakt bij de Autoriteit Persoonsgegevens van een datalek. Het is op zijn minst vreemd dat bijna een vijfde van de mensen die betrokken zijn bij beslissingen op het gebied van dataopslag en databeheer niet weet of er ooit een datalek is geweest en dus ook niet controleert of die melding wel is gedaan. Hoewel er bij de introductie van de Wet meldplicht datalekken en de latere AVG veel ophef ontstond over de in de wet genoemde boetes, blijkt dus in de praktijk dat bedrijven het allemaal niet zo nauw nemen. Kennelijk is de angst om een boete te krijgen vervaagd en lijkt het erop dat de ernst van de mogelijke impact van een datalek door veel beslissers op het gebied van dataopslag wordt onderschat.

Privacy- en security-bewustzijn van de organisatie

Een keten is zo sterk als de zwakste schakel. Daarom is het verhogen van het privacy- en securitybewustzijn van het personeel minstens zo belangrijk als alle technische maatregelen die je neemt om data te beschermen. 18 procent van de respondenten vindt dat de eigen organisatie te weinig doet om dit thema bij de medewerkers op de agenda te krijgen. Dat blijkt ook wel, want maar liefst 14,5 procent zegt nog nooit door de eigen organisatie te zijn voorgelicht over privacy. Bijna een op de zeven organisaties heeft de introductie van de AVG dus niet aangegrepen voor een interne voorlichtingscampagne. Medewerkers weten daardoor niet welke maatregelen zij in hun eigen werk zouden moeten nemen om ervoor te zorgen dat persoonsgegevens optimaal beschermd zijn.

Gelukkig geldt dit voor de minderheid en geeft bijna 73 procent aan dat de organisatie veel moeite doet om het privacybeleid bekend te maken bij medewerkers, partners en klanten. Toch twijfelen nogal wat respondenten of al die aandacht voor dit onderwerp terecht is. Een kwart vindt de aandacht voor privacy in zijn of haar organisatie overdreven, 68 procent vindt dat niet.



Het vertrouwen in de maatregelen die de eigen organisatie neemt is groot. Maar liefst 73,7 procent is niet bang dat de eigen organisatie te maken krijgt met een privacyschandaal. Ruim 38 procent vindt dat het eigen bedrijf niet voorop hoeft te lopen op dit terrein;

52 procent vindt het juist wel belangrijk dat de eigen organisatie voorop loopt als het gaat om privacy. Opvallend is ook dat bijna de helft van de respondenten (ruim 46%) vindt dat de media privacy-schandalen vaak uitvergroten.

74%
is niet bang dat de eigen organisatie te maken krijgt met een privacyschandaal

Aan de respondenten is gevraagd om in te schatten in hoeverre hun organisatie zich vijf jaar geleden, bij de inwerking-treding van de Wet meldplicht datalekken in 2016, focuste op privacy en in hoe-verre dat vandaag de dag het geval is. Niet geheel verrassend is een duidelijke verschuiving te zien. Waar vijf jaar gele-den de meerderheid van de respondenten op een schaal van 1 tot 10 koos voor 6 of 7, scoren momenteel 8 en 9 verreweg het hoogst.

Vertrouwen in de techreuzen

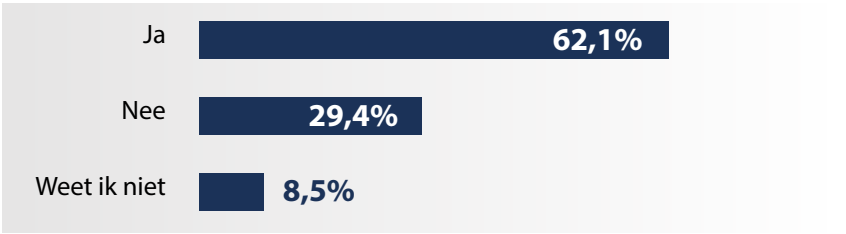
Wie het heeft over de cloud, denkt al snel aan de toenemende macht van Amerikaanse en Chinese techreuzen. Daarom hebben we de respondenten gevraagd naar hun perceptie van de Europese cloud ten opzichte van Amerikaanse of Aziatische cloudproviders.

Daaruit blijkt dat angst dat data in een cloud van een Amerikaanse of Aziatische provider minder veilig zijn, geen hele grote rol speelt. Hoewel 40,8 procent aangeeft een Europees cloudplatform betrouwbaarder te vinden dan een platform van een aanbieder buiten Europa, vindt slechts een op de tien ondervraagden het zorgelijk dat de eigen organisatie gebruikmaakt van een Amerikaanse provider.

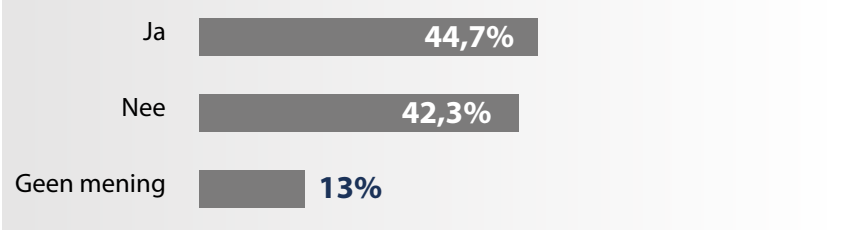
Wel houden respondenten een stevige slag om de arm als het gaat om techreuzen. 62 procent is bang voor de groeiende macht van grote public cloudproviders als Amazon, Google en Microsoft.

64,8 procent denkt dat deze bedrijven wegkomen met fouten omdat ze zo machtig zijn. Tegelijkertijd vindt bijna 56 procent dat de techreuzen de grondleggers zijn van innovaties. Opvallend is dat het voor de beantwoording van deze vraag niet zo gek veel uitmaakt of het eigen bedrijf gebruikmaakt van de clouddiensten van Microsoft, Google of Amazon. Gebruikers van Google- en Amazondiensten zijn iets minder bang dan gemiddeld voor de macht van techreuzen (59%), gebruikers van Microsoft (66%) en Oracle (bijna 72%) juist iets meer.

Ik ben bang voor de almaar groeiende macht van techreuzen



Ik heb vertrouwen in de techreuzen



Dit beeld zien we ook terug als we vragen naar het vertrouwen dat respondenten hebben in techreuzen. Voor de beantwoording van de vraag maakt het nauwelijks uit of de organisatie gebruikmaakt van de diensten van een van die partijen. Als er al iets uitspringt, dan is het dat de gebruikers van Google clouddiensten het best van vertrouwen zijn (slechts 33% van hen vertrouwt techreuzen niet). Met andere woorden: mensen die vertrouwen hebben in techreuzen gaan eerder met Google in zee, mensen die toch wat wantrouwen koesteren, kiezen liever voor de cloud van IBM of Oracle.

Europese federatieve cloud

De Europese Commissie nam in 2020 het initiatief om de gezamenlijke Europese cloudinfrastructuur te versterken middels een Europese federatieve cloud. Het doel is om de innovatie die organisaties nu bij techreuzen halen binnen de EU te bieden, zonder de nadelen van deze machtige spelers te ervaren. Het vervolg daarop was de oprichting van The European Alliance for Industrial Data, Edge and Cloud in juli 2021. Alle partijen – van bedrijven, universiteiten en andere onderzoeksinstituten tot grote gebruikers – kunnen zich aansluiten om samen na te denken over de technologische roadmap.

Hoewel de behoefte groot is, zo blijkt uit de antwoorden, is dit initiatief nog erg onbekend. Nog geen 7 procent was kort voor de oprichting van de European Alliance for Industrial Data, Edge and Europese cloudinfrastructuur te versterken. 19 procent is redelijk op de hoogte, terwijl 45 procent er nog nooit van heeft gehoord. De rest heeft er wel van gehoord, maar weet niet wat het precies inhoudt. De mensen die de term Europese federatieve cloud kennen, menen dat het door deze federatie makkelijker wordt om veilig en via Europese richtlijnen te werken.

Er ligt voor de partijen die onderdeel kunnen uitmaken van de European Alliance for Industrial Data, Edge and Cloud dus nog een behoorlijk grote taak om de bekendheid te vergroten. Het onderzoek laat immers duidelijk zien dat organisaties dringend behoefte hebben en op zoek zijn naar de innovatie die grote cloudproviders bieden, maar dat ze de macht van met name de Amerikaanse spelers vervelend vinden.

SELECTIECRITERIA

Selectiecriteria voor een hosting- of cloudprovider

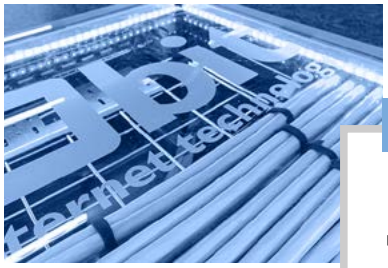
In het onderzoek is gevraagd welke selectiecriteria organisaties hanteren als ze een hosting- of cloudprovider zoeken. Ze konden daarbij kiezen uit een lijst van achttien argumenten. Met stip op 1 staat het criterium veiligheid. Gevolgd door prijs-kwaliteitsverhouding en privacy. Daarnaast scoren thema's die te maken hebben met de persoonlijke dienstverlening van de cloudprovider relatief hoog. Opvallend genoeg wordt relatief minder waarde gehecht aan toezeggingen in de SLA, uptime en certificeringen. Ook de locatie van dataopslag wordt minder vaak als top-3 argument genoemd dan je op voorhand wellicht zou verwachten. Al letten financiële dienstverleners en overheden wel wat meer dan gemiddeld op waar hun data staan (respectievelijk 19 en 18%).

Selectiecriteria	%
Veiligheid	45,1
Prijs-kwaliteitsverhouding	31,2
Privacy	27,5
Persoonlijke dienstverlening - support	23
- technische dienstverlening	18
- flexibiliteit	11
Toezeggingen in de SLA	11
Uptime	11,7
Certificering	12,7
Locatie van dataopslag	13
Laagste prijs	7,7

Waar respondenten bij de voorgaande vraag hun drie topcriteria kozen uit een lijst van achttien selectiecriteria, is ook gevraagd in hoeverre prijsoverwegingen een belangrijke rol speelden bij de keuze voor een hosting- of cloudprovider. Dit blijkt in slechts 22 procent van de gevallen zo te zijn. Ruim 41 procent geeft aan dat prijs hooguit in de marge een rol heeft gespeeld, maar dat op kwaliteit gerichte argumenten belangrijker waren. In de overige 37 procent van de organisaties speelde prijs een ongeveer even grote rol als argumenten die betrekking hebben op kwaliteit.

Van de organisaties die primair kozen op basis van prijs kwam een behoorlijk deel van een koude kermis thuis. Want van hen geeft ruim 48 procent aan dat hun leverancier weliswaar een lage instapprijs hanteert, maar dat vervolgens voor iedere extra dienst of uitbreiding van de omgeving veel geld wordt gevraagd. Daardoor vallen de kosten veel hoger uit dan initieel gedacht.

Het lijkt er dus op dat ook hostingproviders vaak intransparante prijsmodellen hanteren. Dat is niet enkel voorbehouden aan grote buitenlandse public cloudproviders, waarvan algemeen bekend is dat de kosten uiteindelijk vaak tegenvallen omdat het gebruik van resources in de praktijk veel hoger is dan vooraf ingeschat. Als bijna de helft van de gebruikers van externe resources – of het nu in de vorm is van colocatie, private of public cloud – aangeeft dat de werkelijke kosten hoger zijn dan vooraf gedacht, dan ligt er een gezamenlijke opgave om transparanter over de kosten te communiceren.



50%

van de respondenten is zo tevreden met hun huidige hosting- of cloudprovider dat ze met de huidige kennis precies dezelfde keuze zouden hebben gemaakt

Tevredenheid met huidige leverancier

Precies de helft van de respondenten geeft aan zo tevreden te zijn met hun huidige hosting- of cloudprovider dat ze met de huidige kennis precies dezelfde keuze zouden hebben gemaakt. Je zou verwachten dat de snelheid waarmee ze iemand aan de telefoon krijgen die verstand heeft van zaken een belangrijke 'satisfier' is, maar dat komt niet uit het onderzoek naar voren. Het is niet

zo dat organisaties die blij zijn met hun provider sneller of gemakkelijker iemand aan de lijn krijgen als ze bellen. Dat is opvallend. Je zou verwachten dat wanneer er een serieus probleem is, je zo snel mogelijk iemand wilt spreken die daadwerkelijk kan helpen.

8,5 procent van de organisaties is zo ontevreden over de cloudleverancier dat ze het liefst zouden willen overstappen naar een andere provider. Ze doen dit nu nog niet uit oogpunt van kosten, contractuele afspraken of omdat ze niet meer uit het ecosysteem van hun cloudprovider kunnen ontsnappen zonder de bedrijfscontinuïteit in gevaar te brengen.

IT'ers
hechten meer waarde aan een grote naam dan beslissers die vanuit de business betrokken zijn

Continuïteit versus bekendheid

Net iets minder dan de helft van de ondervraagden geeft aan gevoelig te zijn voor de naamsbekendheid van een cloudleverancier. Deze mensen denken ook relatief vaak dat wereldwijd opererende cloudleveranciers een betere continuïteit bieden dan lokale partijen. Opmerkelijk genoeg hechten IT'ers meer waarde aan een grote naam dan beslissers die vanuit de business betrokken zijn (bijna 60% van de IT'ers versus 40% van de niet IT'ers).

Veel belangrijker dan de naam van een provider is echter de ervaring van andere organisaties in het netwerk. Maar liefst 66,8 procent van de respondenten geeft aan dit heel belangrijk te vinden. 16,2 procent neemt het mee, maar niet als belangrijkste argument. En voor slechts 16,9 procent speelt de ervaring van anderen helemaal geen rol in de keuze van een cloudleverancier.

Waar uit het antwoord op de vraag naar top drie selectiecriteria blijkt dat locatie voor de meeste organisaties geen doorslaggevend criterium is, geeft toch ruim 54 procent van de organisaties aan dat ze het liefst hebben dat de data op Nederlandse bodem staan. Dit is vooral belangrijk voor juridische dienstverleners (89%)en overheden (70%). Financiële

dienstverleners en zorgorganisaties, die toch ook zeer privacygevoelige informatie verwerken, scoren hier gemiddeld. Dit is opvallend omdat veel van deze organisaties tegelijkertijd ook gebruikmaken van de clouddiensten van Microsoft, Google en Amazon Web Services (AWS). AWS heeft niet eens een datacenter in Nederland, bij de andere twee leveranciers ben je er niet bij alle diensten zeker van dat je data in Nederland of Europa blijven.

In de helft van de gevallen wordt op strategisch niveau in de organisatie beslist of de data al dan niet in Nederland moeten blijven. In de andere helft van de gevallen zijn het de IT-medewerkers die hier leidend in zijn.

Duurzaamheid wordt belangrijker

Duurzaamheid is voor slechts 6,8 procent van de organisaties een top drie argument bij de keuze voor een datacenter of cloudprovider. Maar dit op het oog lage percentage verbloemt dat duurzaamheid voor meer dan de helft van de organisaties (53%) toch wel degelijk een rol speelt. In volgorde van belangrijkheid is het vaak het vierde of vijfde criterium. Nu steeds meer organisaties van maatschappelijk verantwoord ondernemen (MVO) een strategisch doel maken, wordt steeds meer gelet op aspecten als het energiegebruik van het datacenter. De verwachting is dan ook dat dit onderwerp de komende jaren aan belang zal toenemen.

Over het selectieproces dat de eigen organisatie doorliep voor een hosting- of cloudprovider is ruim tweederde van de respondenten zeer te spreken. Dat vond zorgvuldig plaats, waarbij meerdere aanbieders tot in detail zijn bekeken en met meerdere partijen is gesproken. Slechts 12 procent vindt dat de selectiecommissie te kort door de bocht ging.

Conclusies en aanbevelingen

Hoe belangrijk vinden bedrijven aspecten als security en privacy nu écht als het gaat om keuzes die ze maken ten aanzien van hoe ze hun data beheren en waar ze die opslaan? Dit onderzoek laat zien dat het aan de voorkant van het traject, bij de selectie van een hosting- of cloudprovider, belangrijke waarden zijn. Maar dat veel professionals die betrokken zijn bij de keuze niet goed weten waar ze op moeten letten.

Het kan uiteraard zo zijn dat sommige respondenten gebruikmaken van een Amerikaanse public cloudprovider voor data die niet erg gevoelig zijn, terwijl ze tegelijkertijd de zeer privacygevoelige of bedrijfsgevoelige data in een private omgeving hosten. Toch laat het hoge percentage 'weet niet'-antwoorden op sommige vragen wel zien dat hier kennelijk intern weinig over wordt gesproken. Niet iedereen die betrokken is bij de beslissing welke data waar worden opgeslagen weet namelijk hoe het eigen bedrijf ermee omgaat. Dat is op zijn minst merkwaardig.

Ons advies is dan ook om dit gesprek veel intensiever te voeren, met een grotere groep mensen. Nu lijkt het erop als of de beslissing welke data waar worden opgeslagen teveel aan de IT-afdeling wordt overgelaten en soms op ondoordachte wijze plaatsvindt. Als iemand in het team die beslist over de opslaglocatie roept dat 'het met de security bij deze provider wel goed zit', dan neigen de andere beslissers om daar in mee te gaan zonderzelf te onderzoeken waar de risico's zich bevinden en wat de organisatie moet doen om die te mitigeren.

Het gesprek over de IT-risico's die organisaties lopen moet niet alleen breder in de organisatie gevoerd worden, maar ook op het allerhoogste bestuursniveau. In veel bestuurderskamers is nog niet doorgedrongen dat IT-kwetsbaarheden gevolgen kunnen hebben voor het imago van en het vertrouwen in de organisatie. Een voorbeeld van zo'n kwetsbaarheid is een datalek. Dat het risico daarop reëel is, blijkt duidelijk uit de cijfers die de Autoriteit Persoonsgegevens publiceert over de aantallen datalekken in Nederland.

Het gesprek over de IT-risico's die organisaties lopen moet niet alleen breder in de organisatie gevoerd worden, maar ook op het allerhoogste bestuursniveau

Maar er zijn ook risico's die de continuiteit en zelfs het voortbestaan van de organisatie ernstig in gevaar kunnen brengen. Het bekendste voorbeeld daarvan is het risico op een infectie met ransomware. Waar tot een paar jaar geleden criminelen zich met hun ransomware richtten op particulieren, maken zij tegenwoordig bij voorkeur slachtoffers bij overheden, organisaties en bedrijven. Bestuurders lijken zich niet bewust van het risico op besmetting dat zij lopen en de gevolgen die zo'n besmetting heeft. Bij veel organisaties staan alle (productie)processen stil als zij het slachtoffer zijn van een geslaagde ransomware-aanval.

Er is dus ook gewoon een goede businesscase voor maatregelen om de security en privacy te verbeteren en zo de risico's op een datalek of hack te verkleinen. Het is daarmee een onderwerp dat thuishoort in de boardroom en dat ook op de niveaus daaronder aandacht moet krijgen. Het feit dat we in dit onderzoek regelmatig tegenstrijdige antwoorden tegenkomen en relatief veel mensen eenvoudige vragen beantwoorden met 'weet niet', geeft aan dat het gesprek op dit moment nog niet breed genoeg wordt gevoerd en dat strategische beslissingen eigenlijk teveel worden overgelaten aan de IT-afdeling.

bit
internet technology

BIT beheert een drietal datacenters in Ede en is gespecialiseerd in groene colocatie en managed hosting. BIT levert met de BIT NL Cloud een privacyvriendelijk, 100% Nederlands, alternatief voor clouds van hyperscalers zoals Microsoft Azure, Amazon Web Services, of Google Cloud.
BIT levert aan kwaliteitsbewuste organisaties de ruggengraat voor hun IT- en internet-infrastructuur. Betrouwbaarheid is het uitgangspunt van de dienst-verlening, zodat klanten zich zorgeloos met hun kernactiviteiten bezig kunnen houden.

BIT onderscheidt zich door een hoog kennisniveau, jarenlange ervaring en een pragmatische aanpak. BIT is ISO 27001 en NEN 7510 gecertificeerd.

Contact opnemen met BIT mag altijd:
Galileïlaan 19, 6716 BP Ede
T +31 (0)318 648 688
E info@bit.nl **I** https://www.bit.nl