BUSINESS SOFTWARE

= exact

Exact Online

VEILIG DE CLOUD IN

De 7 vragen die experts stellen bij het kiezen van software in de cloud

www.exactonline.be

Inhoud

INLEIDING

U doet de ramen en deuren toch ook op slot als u het huis verlaat? Daarom bent u net zo voorzichtig als het aankomt op het beveiligen van uw bedrijfsgegevens. Maar hoe weet u of uw data veilig blijft, vooral als u cloudsoftware voor uw bedrijf aan het uitkiezen bent?

Weet u niet precies waar u moet beginnen? Lees dan deze korte whitepaper. Hier leest u de 7 belangrijkste vragen die u een aanbieder van cloudsoftware moet stellen over de beveiliging van uw gegevens en de betrouwbaarheid van hun service.

> "Hou u niet in. Het draait om uw bedrijfsgegevens die online staan."

1

HET DRAAIT ALLEMAAL OM BEVEILIGING

Hoe veilig zijn mijn gegevens in de cloud? Dat is een belangrijke vraag als u in de cloud gaat werken. Het korte antwoord is ‘erg veilig’. Streng beveiligde datacenters en voortdurende monitoring zorgen daarvoor. Maar dan moet u wel voor een betrouwbare hostingprovider kiezen. Stel daarom de volgende vragen over de beveiliging.

Vraag 1. Wie is de hostingprovider?

Waar worden de gegevens opgeslagen? Op een bekend en streng beveiligd datacenter? Het is essentieel dat u nagaat wie de hosting-provider is, omdat er veel verschillende soorten zijn en de kwaliteit enorm kan variëren.

Het overgrote deel van hostingpartners komt bijvoorbeeld niet in aanmerking voor de ISAE 3402 certificering. Zonder deze certificering kan een hostingprovider niet garanderen dat het volledige controle heeft over bijvoorbeeld beveiliging en gegevensbescherming.

Tel daarbij op dat veel hostingproviders hun ondersteuning en administratie uitbesteden aan lage loonlanden. Dit betekent dat uw bedrijfsgegevens overgedragen zouden kunnen worden naar een land buiten de EU en zo onder lokale wetgeving vallen. En laten we die wetgeving in de meeste gevallen maar voorzichtig omschrijven als ‘niet zo streng’ als u graag zou zien.

Tot slot is van belang te weten dat datacenters gewaardeerd worden door het Uptime Institute. Overweeg alleen Tier 3+/Tier 4 datacenters voor de opslag van uw kritieke gegevens.

Een professionele aanbieder van cloud-software geeft duidelijk aan met welke hosting provider ze samenwerken. De erkende standaarden waaraan de laatste zich moet houden zijn ISO 270001, ISO 27002 (voorheen ook bekend als ISO 17799) en ISAE 3402 Type I.

> “Hoe veilig zijn mijn gegevens in de cloud? Het korte antwoord is ‘erg veilig’. Streng beveiligde datacenters en voortdurende monitoring zorgen hiervoor, mits u natuurlijk voor de juiste provider heeft gekozen.”

Vraag 2. Wordt de verbinding beveiligd?

Logt u in op uw online bedrijfssoftware met een beveiligde verbinding? Zo ja, dan zit u goed. Want als de verbinding niet beveiligd is dan worden de gegevens onversleuteld over het internet verzonden. Let dus goed op!

De standaard op het gebied van beveiligde online verbindingen is HTTPS. Dit wordt ook gebruikt door banken, overheden en veiligheidsdiensten. Bij HTTPS is de verbinding versleuteld met een 1024 bit algoritme (SHA1) met behulp van een SSL-certificaat.

Let er ook op dat het bijbehorende SSL-certificaat uitgegeven is door een een betrouwbare en internationaal erkende Certificate Authority (CA), een zogenaamde poortwachter voor de uitgifte van dit soort certificaten. VeriSign (Symantec) is hier een voorbeeld van. (Symantec heeft de uitgifte van certificaten van VeriSign overgenomen. De naam VeriSign wordt echter nog steeds gebruikt.)

Vraag 3. Wordt de software voortdurend gecontroleerd en getest?

Laat niets aan het toeval over: vraag na of de online bedrijfssoftware ook voortdurend wordt gecontroleerd en getest door onafhankelijke experts. Breng penetratie- en white-box tests ter sprake. Daar herkent u de professionele aanbieders aan.

Vertrouw nooit een provider die veilig zegt te werken zonder daarvoor het bewijs te leveren. Vertrouw in plaats daarvan op een ISAE 3402 certificaat. Dan weet u zeker dat alle risico's zijn geïdentificeerd en er aan strenge eisen wordt voldaan, die weer net zo streng worden gecontroleerd.

Vraag 4. Worden er dagelijkse back-ups gemaakt?

Uw bedrijfsgegevens zijn pas echt veilig als er dagelijkse noodback-ups worden gemaakt door de hostingprovider. Deze zijn niet voor persoonlijk gebruik, maar om uw data extra goed te beschermen tegen brand, diefstal en falende hardware.

> "Vraag providers welke monitoringsystemen ze gebruiken, wat hun capaciteit en managementproces inhoudt en hoeveel systeembeheerders ze gebruiken om de infrastructuur van het datacentrum te onderhouden."

2

BETROUWBAARHEID VOOROP

Het grote gemak van bedrijfssoftware in de cloud is dat u 24/7 wereldwijd uw gegevens bij de hand heeft. Daarom is - naast veiligheid - stabiliteit en dus betrouwbaarheid erg belangrijk.

Vraag 5. Wat voor soort monitoring systeem gebruikt de provider?

Meten = weten! Daarom meten betrouwbare aanbieders van cloudsoftware dagelijks de capaciteit, prestaties en stabiliteit van hun systeem - vanaf verschillende locaties. Loopt er iets niet vlot? Dan kunnen ze preventief ingrijpen. Vraag er dus naar!

Ga na welke monitoringsystemen de hostingprovider gebruikt, hoe hun capaciteitsmanagementprocessen opgebouwd zijn en hoeveel systeembeheerders ze gebruiken om de infrastructuur van het datacenter te onderhouden.

Vraag 6. Is er een back-upsysteem?

Een failover is in feite een veiligheidsnet. Het is een operationele modus voor een back-up die in werking hoort te treden als er iets misgaat met 1 van de onderdelen in het hoofdsysteem. Bijvoorbeeld met de processor, de server, het netwerk of de database.

Hoe u weet of de hostingprovider zijn werk serieus neemt? Als ze de back-upserver - ook wel failoverserver genoemd - goed op orde hebben. Pro-tip: vraag wanneer de laatste volledige failover- of recoverytest is uitgevoerd.

Vraag 7. Wanneer wordt er onderhoud uitgevoerd?

Aanbieders van cloudsoftware werken voortdurend aan het uitbreiden en updaten van hun product. In 99% van de gevallen wordt het onderhoud 's nachts uitgevoerd. Dan merkt u er niets van. Kortom, ga na hoe de aanbieder dit aanpakt.

> "De standaard op het gebied van beveiligde verbindingen is HTTPS. Dit wordt ook gebruikt door banken, overheden en veiligheidsdiensten."

3

CONCLUSIE

U kunt met een gerust hart veilig werken in de cloud. Maar dat hangt wel van de aanbieder af. Stel dus veel vragen - waaronder deze 7 - om ervoor te zorgen dat u met professionelen te maken heeft.

Maar vergeet niet dat het veilig houden van uw bedrijfsgegevens ook van u afhangt. Uw computers, tablets en smartphones hebben allemaal toegang tot uw bedrijfsgegevens. Naast het gebruiken van uw gezonde verstand hier nog 4 tips om u daarmee te helpen.

Tips om uw gegevens veilig te houden

1. Gebruik verschillende wachtwoorden voor zowel uw apparaten als programma's.
2. Zet de automatische vergrendeling aan op uw pc's, smartphones en tablets.
3. Installeer software of apps die uw apparaten bij diefstal of verlies kunnen vinden.
4. Installeer goede antivirussoftware en hou deze up-to-date.

Daadkrachtige business software, dat is wat Exact maakt. Voor meer dan 200.000 organisaties wereldwijd. Voor ondernemende doeners die hun dromen nog dezelfde dag in daden willen vertalen.

Exact heeft diezelfde mentaliteit. Dertig jaar geleden startten we als zes studenten een bedrijf, nu zijn we een internationale onderneming met 1550 collega's in 15 landen. Daarom zijn we gek op snelgroeiende bedrijven. En weten we als geen ander hoe innovatie voelt.

Onze business software zorgt ervoor dat je je voluit kunt richten op het volgende doel, de volgende uitdaging. Zodat je niet hoeft te wachten op wat de toekomst je brengt, maar je 'm zelf kunt bepalen.

Analyseer, test en verbeter je product, je organisatie en je business model. Continu. Met de daadkrachtige business software van Exact.

Exact. Focus on what's next.
www.exact.com

Exact Software België N.V.

Koningin Astridlaan 166
1780 Wemmel

Tel: 0800 - 97 631
Email: info@exactonline.be
Website: www.exactonline.be

© Exact Group B.V., 2014. Alle rechten voorbehouden. Alle hierin vermelde merk- en handelsnamen behoren toe aan de respectievelijke eigenaren. MCL640101BN004

BUSINESS SOFTWARE

= exact