Hoe beveilig je de cloud en blijf je compliant met security-eisen?

De meeste organisaties hebben inmiddels de stap naar de cloud gemaakt of maken plannen om (een deel van) hun IT-omgeving in de cloud te zetten. Niet onlogisch, want ten opzichte van on-premise biedt de cloud grote voordelen op het gebied van flexibiliteit en schaalbaarheid. Geautoriseerde gebruikers kunnen locatieonafhankelijk werken, terwijl je in de cloud ook snel, makkelijk en op basis van actuele behoeften capaciteit op- of afschaalt.

Tegelijkertijd worden cloudomgevingen in een rap tempo complexer. Het aantal gebruikte applicaties groeit, wat leidt tot meer afhankelijkheden tussen verschillende toepassingen en nieuwe uitdagingen op het gebied van IT-beheer, security en compliancy. Organisaties moeten zich aanpassen aan deze groeiende complexiteit om hun data en systemen veilig te houden en te voldoen aan alle wettelijke vereisten. Dit vraagt een diepgaand begrip van de unieke risico's en het nemen van effectieve security maatregelen.

In dit whitepaper lees je hoe je jouw cloudomgeving effectief beveiligt en te allen tijde compliant blijft met wet- en regelgeving op het gebied van cybersecurity, privacybescherming en databeveiliging.

Cloud security en compliancy met data- en privacywetgeving zijn belangrijker dan ooit. Lees hoe je op dit vlak succes boekt en problemen voorkomt.

uniserver

T +31(0) 72 - 57 25 646 | **E** info@uniserver.nl | www.uniserver.nl

Wat zijn cloud security en compliancy?

Cloud security heeft betrekking op het beschermen en beveiligen van gegevens, applicaties en infrastructurele componenten in de cloud. Door deze IT-onderdelen te beveiligen met de juiste tools en een goed, waterdicht systeem voor toegangs- en identiteitsmanagement op te zetten, verklein je de kans dat je ten prooi valt aan cyberdreigingen als malware, ransomware en phishing.

Compliancy verwijst naar het naleven van wetten en regels die van toepassing zijn op je cloudgebruik. Er is een breed scala aan normen en richtlijnen dat je verplicht om data veilig en correct te beheren. De plek waar je gegevens opslaat, het beveiligingsniveau van je cloudomgeving, de manier waarop je data uitwisselt met andere partijen en de bewaartermijn van gegevens zijn daarbij belangrijke aandachtspunten.

Waarom zijn cloud security en compliancy zo belangrijk?

Cloud security en compliancy zijn om meerdere redenen belangrijk in onze sterk gedigitaliseerde samenleving. Onveilige situaties en verstoringen binnen je cloudomgeving(en) kunnen bijvoorbeeld belangrijke processen hinderen of stilleggen, waardoor de winstgevendheid en continuïteit van je bedrijf onder druk komen te staan.

Niet voldoen aan (wettelijke) veiligheidsvereisten en regels zadelt je bovendien op met een financiële strop. Op het overtreden van de AVG staan bijvoorbeeld forse boetes die in het ergste geval kunnen oplopen tot twintig miljoen euro of vier procent van de jaaromzet. Als een cyberincident binnen jouw bedrijf breed uitgemeten wordt in de pers, loop je bovendien serieuze reputatieschade op. Niemand wil in het moderne tijdperk van ‘digital first’ bekendstaan als de organisatie die haar cybersecurity niet op orde heeft. Een solide beveiligings- en compliancestrategie helpt je om te voldoen aan wettelijke vereisten en vertrouwen te kweken bij klanten en partners.

Waarborging, standaarden en richtlijnen.

Uitdagingen bij het waarborgen van veiligheid en compliance in de cloud

Het waarborgen van veiligheid en compliance in de cloud is een klus die gepaard gaat met de nodige uitdagingen. Denk bijvoorbeeld aan:

- De gedeelde verantwoordelijkheid die cloudproviders hebben bij het beheren en beveiligen van IT-omgevingen. Cloudproviders zijn (zeker bij SaaS-constructies) meestal verantwoordelijk voor updates en het beveiligen van soft- en hardware, terwijl de gebruikers zelf moeten zorgen voor het veilig opslaan, beheren en uitwisselen van hun data. Goede afspraken over elkaars taken en verantwoordelijkheden zijn daarom nodig.
- Het beveiligen van gevirtualiseerde omgevingen. Die zijn in de regel namelijk complexer en abstracter dan de traditionele IT-ecosystemen die bij de gebruiker op locatie staan. Het gebrek aan zichtbaarheid en controle over je cloudresources is in zo'n situatie soms een hindernis voor een optimaal security- en compliancebeleid.
- Het naleven van diverse regionale en branchespecifieke voorschriften. Die komen nog eens bovenop de regels en wetten die op mondiaal, Europees of nationaal niveau gelden en stellen vaak weer extra (strenge) eisen aan de inrichting van je cloudlandschap.

Actuele standaarden en richtlijnen voor veilig cloudgebruik

Er zijn verschillende regels en richtlijnen die van toepassing zijn op veilig cloudgebruik en cybersecurity. De belangrijkste zijn:

- De AVG (GDPR). Dit is een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.
- De Health Insurance Portability and Accountability Act (HIPAA), een Amerikaanse wet die toeziet op de privacybescherming en informatiebeveiliging binnen de zorgsector.
- De ISO/IEC 27001 voor informatiebeveiliging. Deze wereldwijd erkende norm beschrijft hoe je procesmatig omgaat met het beveiligen van data om zo de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen jouw organisatie veilig te stellen.

Cloud security en compliance verbeteren: de mogelijkheden.

Gelukkig zijn er diverse mogelijkheden om je cloud security en compliance naar een hoger niveau te tillen. We zetten de belangrijkste op een rij.

Tools en oplossingen

Er is tegenwoordig een divers spectrum aan tools en oplossingen voor het verhogen van je security-niveau en waarborgen van compliance voorhanden. Denk bijvoorbeeld aan:

- **Cloud security posture management (CSPM):** Hiermee identificeer je op een geautomatiseerde manier zwakke plekken binnen je cloudomgeving en in je cloudconfiguratie. Daarnaast biedt de dienst concrete richtlijnen om je beveiliging te verbeteren.
- **Cloud access security brokers (CASB):** Deze beveiligingsoplossingen fungeren feitelijk als een tussenstation tussen de hardware- of computing-infrastructuur van een bedrijf en de cloudserviceproviders. Een CASB stelt beveiligingsprotocollen en beveiligingsstandaarden in en dwingt die af tussen netwerken, cloudserviceproviders en eindgebruikers.
- **Identiteits- en toegangsmanagement (IAM):** Creëert gebruikersrollen en toegangsrechten. Hierdoor weet je zeker dat alle gebruikers het juiste toegangsniveau (geen toegang, alleen lezen, bewerkingsrechten) hebben tot gegevens, documenten en systemen.
- **Security and event management (SIEM):** Een security-oplossing die organisaties helpt om bedreigingen te detecteren, te analyseren en erop te reageren voordat ze bedrijfsactiviteiten schade berokkenen. SIEM doet dat door informatie te verzamelen uit log- en gebeurtenisgegevens.

Verschillende cloudbeveiligingsdiensten en -platforms analyseren

Bij het kiezen van cloudbeveiligingsdiensten en -platforms is het belangrijk om verschillende opties te evalueren op basis van hun functionaliteit, integratiemogelijkheden en compliance- ondersteuning. De meeste grote en populaire clouddiensten (Azure, AWS, Google Cloud) bieden uitgebreide beveiligingsdiensten, maar het is wel cruciaal om na te gaan welk platform het beste aansluit bij de specifieke behoeften van je organisatie.

Kijk bij deze Amerikaanse diensten ook goed en kritisch naar hun verhouding met wetten als de CLOUD ACT en Patriot Act. Die geven Amerikaanse opsporings- en veiligheidsdiensten (FBI, CIA) namelijk het recht om gegevens van Amerikaanse providers op te vragen als ze denken dat de nationale veiligheid in het gedrang is.

De 5 best practice voor cloud security & compliance.

Je kunt jouw cloud security en compliance verbeteren en professionaliseren met het juiste beleid. De volgende 5 best practices vormen een stevige basis voor een coherente security- en compliancestrategie:

1. **Sterke authenticatie- en toegangscontrole:** ontwikkel en gebruik een MFA-systeem en strikte toegangscontroles om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot gevoelige gegevens en resources.

2. **Regelmatige audits en monitoring:** voer regelmatig audits uit om de beveiligingsstatus van je cloudomgeving te beoordelen. Maak ook gebruik van geautomatiseerde bewakingssystemen om verdachte activiteiten te detecteren en snel te reageren op beveiligingsincidenten.

3. **Data residency en compliance:** verzeker je ervan dat je cloudprovider voldoet aan de wet- en regelgeving met betrekking tot het opslaan van gegevens en het naleven van de AVG. Kies indien mogelijk voor cloudproviders die datacenters in Nederland hebben en die garanties bieden voor het naleven van lokale wetgeving.

4. **Beveiligingspatches en updates:** houd jouw cloudinfrastructuur, inclusief besturingssystemen, applicaties en middleware, up-to-date met de nieuwste beveiligingspatches en updates om bekende kwetsbaarheden te verhelpen.

5. **Beveiligde ontwikkeling:** integreer beveiliging vanaf het begin in je ontwikkelingsproces door middel van methodologieën als DevSecOps. Dit omvat het automatiseren van beveiligingstests en het gebruik van veilige praktijken bij het coderen.

Hoe helpt Uniserver?

Uniserver helpt je op verschillende manieren bij het waarborgen van cloud security en compliance.

Vulnerability Management

Vulnerability management is een waardevolle extra dienst voor het creëren en behouden van optimale veiligheid. Wij detecteren, inventariseren en prioriteren kwetsbaarheden in jouw systemen om deze snel en effectief aan te pakken. Zo is jouw organisatie in staat om zich proactief te beschermen tegen bedreigingen en blijft de veiligheid gewaarborgd.

Managed XDR

Managed XDR is een combinatie van XDR (extended detection and response) met SIEM en SOC binnen één dienst. Daarmee heeft Uniserver 24/7 zicht op de cloudomgeving en reageren we, in het geval van een calamiteit, altijd adequaat. Op die manier geniet je van het hoogst mogelijke niveau van veiligheid.

Incident response en forensisch onderzoek

Uniserver biedt gestructureerde respons op incidenten en voert forensisch onderzoek uit om de oorsprong en impact van (security) incidenten vast te stellen. Door deze effectieve probleemoplossing en bewijsvoering voor juridische stappen, blijft jouw organisatie veerkrachtig en prima bestand tegen cyberdreigingen. Daarnaast kijken we bij de onboarding ook altijd uitgebreid mee waar mogelijke risico's zitten en timmeren we zwakke plekken in je IT-omgeving stevig dicht.

Security Baseline

Wanneer je onze core-dienstverlening afneemt, zoals VDC, ben je standaard verzekerd van onze security baseline. Hieronder vallen platformbeveiliging, netwerkbeveiliging en anti-DDOS.

Over ons.

Uniserver, opgericht in 2000, is een vooraanstaande aanbieder van soevereine private cloud-oplossingen in Nederland. Wij maken de kracht van cloud toegankelijk voor alle sectoren – van zorg en finance tot overheid en retail. Onze private cloud-oplossingen zijn speciaal ontworpen om te voldoen aan de hoogste eisen, waarbij veiligheid en betrouwbaarheid voorop staan. Gehost in Nederlandse datacenters, waarborgen onze oplossingen volledige data-soevereiniteit.

Als onderdeel van de Atomic Group, werken we nauw samen met CloudNation en RevoData om naadloze integraties en superieure cloudoplossingen in private, publieke en hybride omgevingen te bieden. Onze aanpak is gericht op het vereenvoudigen van complexe cloud-uitdagingen, waardoor onze klanten kunnen focussen op wat echt belangrijk is: groei en innovatie. Uniserver staat voor geavanceerde technologie, operationele excellentie en onvoorwaardelijke klanttevredenheid.

Meer weten?
Neem vandaag nog contact met ons op.

Wil je jouw cloud security en compliance naar een hoger niveau tillen? En ben je benieuwd hoe wij je daarbij kunnen helpen? Neem dan gerust contact met ons op via +31 072 572 56 46 of info@uniserver.nl.