Zebware White Paper

Security in the Cloud

Challenges and solutions to secure your data in the cloud

CLOUD ADOPTION SECURITY RISKS

Cloud technology enables digital business transformation. Switching to the cloud for management, storage and analysis of data is the dominant component of digitalization strategies for both private companies and government agencies. Security issues are however counteracting cloud adoption, and therefore risk postponing the digital transformation needed to successfully future-proof business.

Apart from this, a new set of serious obstacles have surfaced. A series of legislation has been adopted with profound impact for the European public sector as well as many companies, adding regulatory risks to the list of issues. These are the EU's General Data Protection Regulation (GDPR), The Security of Networks and Information Systems Directive (NIS) and the US CLOUD Act. Parallel to this, Section 702 of the US Foreign Intelligence Surveillance Act (FISA) of 2008, presents another tangible issue for all users of US based Cloud Service Providers (CSPs). In summary, these legislations change both the way organizations need to perform their administrative processes, as well as the requisites for storing and working with certain data. The consequence for a large number of organizations, private and public, is a delayed or even stalled migration into cloud-based services.

This white paper aims to address the security and regulatory challenges facing organizations using the cloud and how to mitigate these challenges.

GENERAL SECURITY ISSUES IN THE CLOUD

Moving into the cloud presents a strategic shift for the efficiency of both storing and processing of data. The services available and the cost reduction for changing from on-prem hardware to the cloud, are very compelling. The shift to the cloud is continuing to excel both among private companies and government agencies alike. This shift exposes users to new and far more complex security concerns than before.

Although addressed by CSPs, the credibility of CSPs among users are often disputed. There is a number of security issues that need to be thoroughly assessed before migrating into the cloud or when expanding the use of cloud services.

According to a survey conducted by the Cloud Security Alliance (CSA)[1] the top concerns among respondents when migrating data to the cloud, involve misconfiguration of data, lack of visibility of the entire cloud estate, compliance, and difficulties with holistic management across hybrid and multi cloud solutions. The one aspect that overshadows all these issues, is related to security. The risks of unwanted access, data loss and leakage are the dominating concerns for cloud projects.

The risk for unwanted exposure of data increase when using cloud services for storing and computing, This risk includes competitors and/or foreign governments gaining access to confidential information or conducting surveillance. Exposure is increased by CSPs having inadequate security mechanisms in place or from interference by governments or mandatory extradition legislation in countries where either the data or the CSP has its legal residence,.

The spectrum of threats is evolving at the same pace as new services are being developed. The shared complexity of these threats requires a high level of competence and operational vigilance by the user. Cloud provider chains might have inadequate security mechanisms in place. Rogue employees of CSPs may grant themselves unauthorized access to data. Data thieves might break into service providers equipment. Other customers might get access to data if there is inadequate separation of customer data in resources shared in the cloud. Attackers may break into the networks of the CSP, to subcontractors or to co-hosted customers. Attackers may use de-anonymization techniques.

The damage that can be caused in all these cases is often greater than in non-cloud environments - primarily due to the scale of operation and the presence of certain roles in cloud architectures. In many cases these roles entrail potentially extensive access including CSP system administrators or managed security service providers.

SECURITY AT RISK IN THE CLOUD

There is a number of potential security related issues that need to be thoroughly analysed and assessed when migrating data to the cloud. Some are already known from traditional on-premise solutions. But some are new and worsened by cloud models. Researchers at Ryerson University in Toronto have categorized the most prevalent into the following groups[2]

Security Gaps
In the cloud, customers cede control to the cloud service provider. This produces a risk that the CSP will not adequately handle the responsibility of addressing security the way they are supposed to, or even that service level agreements (SLAs) do not include provision of necessary security services.

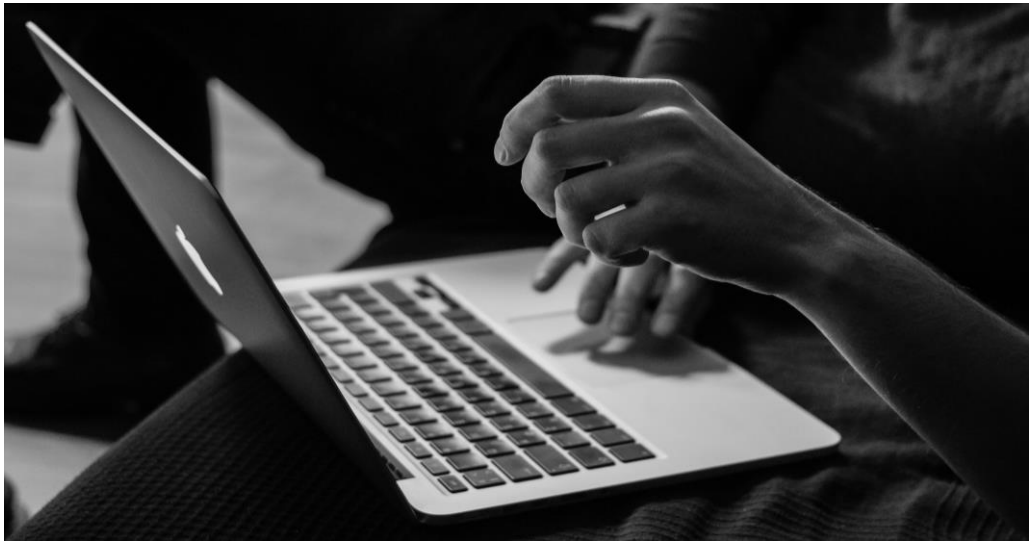
Inadequate Data Deletion
The problem here lies in ensuring that data that should be deleted is actually deleted and no longer possible to recover. This problem is accentuated in cloud environments since multiple copies of the data are available and it might be impossible to properly remove data since it is stored in shared resources.

Compromising of the Management Interface
There is an increased risk of compromise of management interfaces in the cloud compared to traditional hosting providers due to remote access and web browser vulnerabilities.

Isolation Failure
There is a risk that Storage-as-a-Service mechanisms separating storage, memory or routing between different tenants might fail, and, as a result, tenants could access sensitive information belonging to other customers.

Missing Assurance and Transparency
Cloud users need to obtain assurance from CSPs that their data will be protected properly. They may also require notifications about security and privacy incidents. However, this approach can be difficult, particularly in cases of multiple transfers of data. Heterogeneous cloud infrastructures make it difficult to effectively check privacy compliance in an automated way and the end user has no means to verify that the privacy requirements are being fulfilled. It is challenging to find a balance between data provenance and related privacy in the cloud, where physical perimeters are not always clearly defined.

Inadequate Monitoring, Compliance and Audit
When migrating to the cloud, previous investment in security certifications may be put at risk if the CSP cannot provide evidence of compliance with relevant requirements and does not enable users to audit CSP processing of customer data. Furthermore, it may be difficult to evaluate how cloud computing affects compliance with internal security policies. Provisioning of a full audit trail within the cloud is a challenge.



REGULATORY RISKS IN THE CLOUD

Implementing cloud services is an obvious strategy for many organizations. There are simply no alternatives that can compete with the advantages of storing and processing data in the cloud. For government agencies and the public sector in general, this however causes a dilemma. On one hand, all government agencies are responsible for maintaining both cost and service efficiency for their constituents. For this purpose, a cloud based infrastructure often presents an unbeatable alternative. However, there are security challenges that need to be addressed. There are also regulatory constraints for government agencies and the public sector within the European Union.

According to EU official legal interpretations regarding the public sector, using cloud services presents legal obstacles. The Swedish public administration legal advisory organization, eSam, concludes that from amendments in the US CLOUD Act of 2018, US CSPs are required to provide customer propriety information to competent US authorities[3]. This is in direct breach of both GDPR and Sweden´s Public Access to Information and Secrecy Act (SFS2009:400).

The Council of Bars and Law Societies of Europe (CCBE)[4], also concludes that the CLOUD Act grants US law enforcement agencies unlimited jurisdiction over any data controlled by a service provider with sufficient connecting factors to the US. In short, The US CLOUD Act is in direct conflict with applicable EU privacy legislation and mutual legal assisting procedures between the US and the EU. Another aggravating factor is that FISA strictly prohibits US based CSPs to inform users if extraditing of to US authorities, making the use of US based CSPs legally impossible.

In summary, private companies, government agencies, public sector organizations and their subcontractors are facing both security obstacles and legal issues when migrating to cloud services. There is a need for a solution that would address all issues, security related as well as regulatory. This solution also needs to be intuitive and fully agile to the infrastructure and strategy of its users, no matter the level of cloud maturity or accessible resources. It is time to introduce Orchesto®.

SECURING CLOUD DATA WITH AN ABSTRACTION LAYER

In order to successfully implement a cloud first strategy there are a number of potential risks that need to be addressed, to grant data owners the benefits of a secure, portable and compliant use of the cloud. Orchesto® is the solution. An Orchesto® deployment addresses the inherent security challenges of migrating to the cloud.

Orchesto® is an easily deployed software-based data management solution which is mapped 1-to-1 to every application to be connected to a single or to multiple cloud backends. Orchesto® uses virtual buckets as an abstraction layer between application and cloud. This gives the owner of the data full control of both data and application, no matter where the data is stored or how it is used.

The migration of data objects to cloud environments entails a need for the security perimeter to be extended from on premise to cloud or from single cloud to multi or hybrid cloud solutions. Securing data end-to-end with the *Orchesto® Identity and Access Management (IAM)* allows the control of identity and user access to critical information when stored or used off-site. *The Orchesto® Gateway Side Encryption (GSE),* encrypts data all the way from customer premises to its destination using customer-controlled keys. *The Zebware Information Dispersion Algorithm (zIDA*) finally adds an additional and unrivaled level of security to data objects, creating unreadable fragments of objects which can be dispersed across multiple backends and hybrid cloud designs according to the policies set by the data owner.

ZEBWARE

TAKE OWNERSHIP OF YOUR DATA IN THE CLOUD

We are Zebware

We are a software company providing the tools for organizations to seize the full benefit of being truly cloud native while securing complete data sovereignty. We do this with Orchesto® – our solution for hybrid cloud security and orchestration, focused on portability, performance and protection of data.

Our vision is to be the world's leading provider of hybrid-cloud enablement software, securing our customers absolute sovereignty of their data in cloud environments.

With our globally available, market-disrupting software, we apply a close-to-application abstraction layer to the cloud, allowing our customers full security and all benefits from being truly cloud native.

To learn more about how Orchesto® could secure your cloud data, please visit our site zebware.com and contact us!

contact@zebware.com
+46 (0) 8 525 282 32

Sources:
1. https://cloudsecurityalliance.org/articles/cloud-security-alliance-study-identifies-new-and-unique-security-challenges-in-native-cloud-hybrid-and-multi-cloud-environments/
2. https://www.researchgate.net/publication/301348543_White_Paper_Cloud_Security_Basic_Principles
3. http://www.esamverka.se
4. https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf

ZEBWARE

Take ownership of your data in the cloud