FROM THE CLOUDS TO THE GROUND

CLOUD SECURITY ALLIANCE EMEA CONGRESS

MOSHE FERBER

Unsurprisingly, it was a very cloudy day on the end of September when about 200 cloud computing professionals gathered in Amsterdam Barbizon Palace Hotel for the annual cloud security alliance EMEA congress.

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing. It is the first time the CSA host this conference in Europe along with their partners, MIS Training Institute EMEA.

The diversity of the crowd indicated how complicated the challenges of cloud computing are. I don't recall many conferences where attorneys with tailored suites sat side by side with technical geeks and government officials. The variety of people present proved that cloud computing has expanded beyond a technical buzzword and became a concept that draws significant attention from all market & government sectors.

The fact that cloud computing is moving on to be a key factor in the world agenda is backed by the interesting case studies presented in that congress. We all know that early adopters of cloud computing were small and medium businesses, that were looking for cost reduction and flexibility and tended to ignore issues like security and governance. The question of cloud computing was always: when and how the big consumers of IT will join the celebration. The presentation of BBVA, the financial services giant, provided some answers to that question.

Jose Parada Gimeno, Security Innovation Manager for BBVA, spoke about the strategic decision BBVA management made by moving all back office applications such as e-mail and document management to a public cloud, in order to enjoy the advantages of flexibility and collaboration. As Mr. Gimeno put it nicely: "the world is changing, and companies must adapt and be as flexible as their consumers today."

Another interesting presentation regarding adoption of cloud computing came from Ron Roozendaal, Chief Information Officer at the Netherlands Ministry of Health, Welfare and Sport. According to Mr. Roozendaal, the Dutch government targeted a 0.8 Billion cost reduction on IT until 2015. In order to achieve it, Dutch government is implementing its own private cloud. This "government closed cloud" will provide infrastructure services for all government branches. As presented, the first stage of this ambitious project will begin 2013 with mail, digital work environment and collaboration services.

To conclude the interesting cloud projects chapter, Robert Jenkins, CTO for CloudSigma presented the "Helix Nebula" project. This unique cloud computing project is an initiative led by a partnership between leading IT providers and three of Europe's biggest research centers. Helix Nebula is eventually a "scientific cloud" that provides Cloud Computing Infrastructure to match the highly demanding requirements of research institutions and Area & space agencies.

But wherever there are clouds, there is also rain. Aside from presenting successful cloud adoption project, the two days conference addressed the current challenges and issues regarding cloud computing that pre-occupy Europe and the world. Those challenges can be divided into three major chapters:

- Legal & privacy issues
- Technology challenges
- Governance of the cloud

Legal & compliance challenges – or "Can I trust Microsoft not to give my EU data to the US government?"

Legal challenges with cloud computing existed since day one. Open questions about accountability, jurisdiction, ownership & privacy are probably the greatest obstacle for cloud adoption for enterprises and governnment institutes. So, in accordance to their importance, those issues took a significant share at the congress with variety of speakers and panels.

Dr. Siani Pearson, Principal Researcher at HP Labs, introduced the A4Cloud project (Accountability 4 cloud). A4Clouds is a new EU multidisciplinary research project aiming at simplifying & clarifying the boundaries of the accountability of cloud providers by suggesting a framework and tools such as Guidelines, Contract support, system of evidence collection, policy configuration and more. A4Cloud encompasses IT providers such as HP, SAP, and leading research institutes in Europe. Adaptation of it will result in greater trust between the cloud providers and their customers and in an improved reliability of cloud ecosystems.

But the most discussed topic in the congress was the recent developments in the EU regarding data protection directives and their effect on US based companies. EU data protection regulations are considered to be the most rigorous in the world, and forbid moving customer data outside *European Economic Area* (EEA) unless there is a guarantee that it will receive equivalent levels of protection.

In order to allow EU & US to still do business among them, a Safe Harbor agreement was made. Safe Harbor allows US companies to register certification of data protection in the EU once they declare they follow the 7 principles of data protection.

On July 1, 2012, Article 29 Working Party (WP29) issued an opinion 05/2012 - with new insights regarding the responsibilities of cloud clients and cloud providers. The WP29 declaration set a very high standard for both customers and cloud providers, and as a result, Safe Harbor principles may not be adequate for cloud computing.

According to Stewart Room, a partner at Field Fisher Waterhouse, the new WP29 sets the bar so high that it is probably unrealistic to match the requirements. Mr. Room recommends to EU companies who wish to share data with US based companies not to rely any longer on the Safe Harbor principles but rather to add contractual arrangements and additional data security safeguards.

This recent turnout of events places a big question mark for EU & US companies' ability to do business together in cloud environment and undoubtedly will force cloud providers to adopt more transparency, contractual flexibility and security measures. But this is only the tip of the iceberg on the challenges of EU and US cloud computing, according to Caspar Bowden, independent privacy adviser and previously Chief Privacy Adviser for Microsoft. Casper made a fascinating overview of the changes attempts in US to replace the patriot act and FISA (Foreign Intelligence Surveillance Act). Mr. Bowden claimed that the changes in legislation following 9.11 along with the US 4th Amendment, allow US government to perform mass surveillance on non US citizens using US cloud environments with no other excuse then purely political reasons. There is no need to prove any criminal actions or national security concerns, he added. "The difference between US and EU laws, concluded Mr. Bowden, is that while in the EU data privacy laws are mandatory for all, EU citizens or not, US laws do not address to privacy of non-US persons".

Technology challenges - or "Identity is the new Perimeter"

Technology sessions at the CSA congress 2012 focused on the challenges of identity in cloud computing. Or as Hans Zandbelt, Technical Architect for Ping Identity put it: "Identity is the new perimeter." In his presentation Mr Zandbelt called cloud consumers to leverage their own existing identities into the cloud instead of creating new ones. He mentioned that Ping Identity allows organizations to better integrate their current identities into the cloud by utilizing the identity standards for authentication, authorization and provisioning. Mr. Zandbelt reviewed the current status and expected road map of SAML, OAUTH and OPENID, mentioned that more and more cloud providers add support for web SSO and reviewed the new standard of SCIM (Simple Cloud Identity Management) that will help to replace the old provisioning protocol of SPML.

Another aspect of identity is the access and authorization of services and API between machines, and not necessarily between people. Security issues of access keys and authentication mechanisms between software services were always neglected in the security world, and never received proper attention. Mark O'Neill, CTO for Vordel presented case studies from his customers using Vordel products for securely storing access and API keys for programmers, REST services and mobile devices in cloud environment. My belief is that this neglected area of security will take a significant step forward in the next couple of years with the growth of cloud chaining and the increasing number of internet based automated services.

To conclude the technical chapter, Phil Dunkelberger, CEO for Nok Nok Labs and previously CEO for PGP Corporation reviewed the future of cloud authentication. Mr. Dunkelberger surveyed the current failures in common authentication methods and claimed they simply do not work. He called the industry to develop a more simple, secure and scalable authentications methods.

Governance in the cloud - or "Can I convince myself (and my auditors) that my data is safe?"

The cloud computing technology raises many questions about the nature of relationships between a cloud provider and a consumer. Consumers and providers are struggling on the same questions of responsibilities and transparency.

In the CSA congress the discussion on these issues evolved around: how to evaluate you cloud provider security, negotiate the right controls for your data and continually monitor and improve data security while passing regulation audits.

Among the speakers were cloud providers such as Microsoft, Amazon Verizon-TerreMark and Orange describing the efforts they take to increase their customer competence by using tools and standards such as CSA STAR & ISO 27001.

On the opposite side, speakers such as David Cripps, Chief Information Security Officer for Investec and Nikita Reva, Global Security Specialist for MARS Inc. described the difficulties that customers face in evaluating cloud services and the obstacles they encountered when running through compliance process.

From the presentations it is clear that customers evaluating and operating in the cloud still face requirements gaps when it comes to mature security policy, transparency and clear contractual and SLA language. It is also clear that there is a lack of cloud knowledge among auditors and that the current standards for security audits are still not adapted to cloud computing environments.

One effort to bridge the gaps between cloud provider and consumers was introduced by Becky Swain, Founding Member of the CSA, who presented version 2 of the Cloud Control Matrix (CCM) project from CSA. CCM is part of the GRC stack research and specifically designed to provide fundamental security principles to guide cloud vendors. CCM maps all controls in the different regulations (PCI, COBIT, HIPAA, ISO, NIST) into a scheme and makes the necessary adoption to cloud technology. CCM and other projects from the Cloud Security Alliance such as CloudTrust protocol and CAIQ (Consensus Assessments Initiative Questionnaire) will ultimately produce more trust between the provider and the consumer by helping to evaluate, score and audit ongoing operations.

Conclusions

It is now clear that cloud computing passed the early adoption stage and is now making his way to be an important global phenomena that will result in changes for the way we consume IT and do business. Enterprises & government bodies who wish to be more effective, efficient and competitive must adopt some kind of cloud strategy. But it is also clear that challenges facing cloud computing are wider and complicated than the regular technology challenges we are used to.

Governments, standards institutes and cloud provider must join hands in order to invent the "game rules" that will allow organization to move their business into the cloud with minimum risk and maximum transparency.

And how this can be done? Some of it is already taking place. US FEDRAMP initiative to secure cloud computing for government is a giant step in the right direction and the EU commission is also planning to issue its own cloud computing strategy as presented by Thomas Haeberlen from ENISA at the congress. But a key driver to move it all together is to integrate the industry into the process in order to reduce some of the uncertainty that the market feels toward cloud computing. This is why conferences and panels like the Cloud Security Alliance congress are important for the industry, government and regulations bodies to meet, share ideas and try to clear the current situation.

MR. FERBER

is a Cloud Security Professional considered to be one of the highly regarded managers in the security professional community in Israel.
In the past 20 years, Mr. Ferber has been serving in different roles in the IT security industry, always in the front lines of technology and performing the most advance projects at the most demanding customers from all sectors. Prior to his current position, Mr. Ferber served as Security Department Manager for the Global IT services company Ness technologies (NASDAQ: NSTC) where he developed the technical and marketing portfolio for all security products and services.
At 2010 Mr. Ferber founded Cloud7, an Israeli based MSSP that provide unique cyber and web security SAAS and since then he has been attracted to cloud computing solutions and challenges. Today Mr. Ferber is a member of the CSA Israel chapter and spends his time on different cloud projects and educates students on cloud security challenges and risks as a certified CCSK instructor.
Mr. Ferber can be contacted at: Moshe.Ferber (at) gmail.com
http://www.linkedin.com/pub/moshe-ferber/0/58a/828