Into Cyber Security

Brandon Chen, NubeSecure Partner Consultant

January 4, 2016

Cyber Security has never been more prominent as cloud computing and storage continues its momentum over the last 10 years. Globally, major brands have established. In cloud infrastructure provider category, Amazon is leading the way, followed by a Microsoft, RackSpace and Google, just to name a few. In software as a service (SaaS) category, Salesforce, Workday, ServiceNow, DropBox and Box are becoming the de factor industry standard. In US, business leaders has embraced the idea going to the cloud. GE is planning to move 90% of its data into the cloud. Riding the wave, cyber security is becoming a major concern and investment point.
Take a look at this beautiful presentation work about major data breach incidents at http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks, it's absolutely astonishing to almost anyone who didn't see it before.

In the enterprise world, cyber security are around 3Ps, namely People, Process and Products. The first two are the subjects of government and industry regulatory and business practices. In this blog, we will focus on the Products - the technology side of cyber security. In general, can be divided into four layers: network, system, application and data.

Network security detects viruses and malware and prevents them from spreading into connected systems or harming the normal network operation. It uses security appliances to inspect the traffic pattern and compares that with virus/malware signatures. The appliances typically are firewall, anti-virus, anti-malware and intrusion prevention systems. According to a recent Gartner report, traditional solutions are far from satisfactory as up to 90% alert are false alert. Using crow sourcing for virus/malware detection is highly desired. In this area, FireEye is doing an outstanding job.

System Security is about keeping the hardware and operating system up to date against virus, malware and security holes. In the cloud environment, this responsibility belongs to the service providers, not the infrastructure providers. Business need to vigilantly monitor and track the latest security alerts and plan the implementation into the cloud operation routines.

Traditionally, Application Security provides 4A services - account, authentication, authorization and auditing. Account service is about identity management and sometimes referred as user provisioning or user management. The challenges typically come from distributed and silo user data store that requires a lot of effort to consolidate or kept in sync. The trend for Authentication service is relatively clear: multi-factor authentication using soft token has a strong market demand, and biometric based authentication is rising, but still lack of definitive (100%) recognition. Out of the four services, Authorization is the most open and fluid area. There are quite a few choices in access control, i.e. role, attribute and policy bases access controls with an extra dimension “context”. It controls access for not only end user but also system (service account). Auditing is valued extremely high by business leaders. It’s the forensic aspect of security practice. Combined with big data analytics, it’s a very powerful deterrent weapon against security threats. As an extra point, Secure Assertion Markup Language (SAML), OAuth2, API Gateway and big data analytics are the prominent solutions in the cloud computing field.

Data Security is a red hot field with many competing solutions. The applicability of any solution is decided by the balance among complexity, performance and the level of security required. Essentially, we are dealing with structured and un-structured data in motion, at rest and/or in cloud. Data encryption is typically applied either at data structure level or at data file system level. The encryption key can be a system key or per-user key. Key management can be a practice of art.

In the next blog, we will talk about the challenges and the considerations going to the cloud.