

Drotos Engineering: Security Considerations Diagram and Summary



Shane Ẽire Byrne

University of phoenix

NTC300

Abstract

The following material is a collection sought out to present as a security solution to Drotos Engineering. It will cover technologies utilized in the encryption of data, the various tools one can utilize to secure a cloud computing architecture, tools such as automated cloud monitoring, and other technologies and tools that would benefit the organizations cloud infrastructure overall.

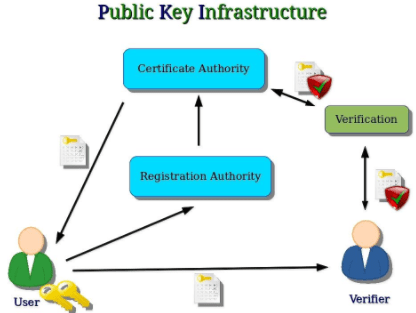
**Security Technologies**

As an engineering consulting company, it is understandable that this organization would keep data regarding where it has consulted on projects. This data itself could be of a sensitive nature and it would behoove this organization to take the initiative by protecting its data which in turn will help the organization to protect itself. In the prior instanciation of this presentation, it was noted it to be the best decision for this organization to develop its own cloud based infrastructure, while this is a prudent task to overtake for the organization as a whole it is also something that could leave the organization more vulnerable if not protected carefully.

Any plaintext(Wilson, 2018), this being unencrypted data, leaves the organization at large in jeopardy if it is to fall into the wrong hands. There are techniques that can be employed in order to assist in protecting the organizations data.

Asymmetric encryption (Wilson, 2018), for example uses a binary-key system in which a public key and private key are utilized. The keys themselves are stored in a PKI certificate; PKI certificates themselves being a part of a Public Key infrastructure, this being a collection of software, encryption technologies, and services that enables entities to protect the security of one’s communications and business transactions over networks (Venafi, 2020).

.



Source: Network Encyclopedia, 2020

Other security tools that can be utilized to protect a cloud system are firewalls, Intrusion Prevention Systems (IPS), and antivirus protection (Wójcik, 2018). By nature, firewalls are deployed to mitigate an attack by limiting or preventing access to a network from an intruder. IPS’s look for irregular patterns on a network and take preventative actions against a suspected intruder. Antivirus software can be configured to scan a physical or virtual machine in order to detect and deal with malicious software that may or may not be present on the machine in question; this is especially important as cloud systems are made up of nodes of virtual machines, if not protected properly, these machines can be just as vulnerable as physical machines. Another point Mr. Wójcik is the concept of data integrity.

As information is the world’s newest gold rush, data integrity plays a pivotal part in protecting an organizations data. The three dimensions of data integrity are: secure communication, safe storage, and the capacity of an organization to audit its data. Secure communication allows data to be safely transmitted between sources, from its origin to its receiver and visa-versa. Safe storage of data is important as it is beneficial to an organization to ensure its saved data has not been altered or modified and is still able to be used for its original purposes. Data should be audited as well, this ensures the fidelity of data, especially after any alterations are made, this also checks for bugs, and other unknown modifications.

**Automated Scanning/Monitoring**

Cloud monitoring is “the process of reviewing and managing the operational workflow and processes within a cloud infrastructure or asset” (ipswitch, 2019). Cloud monitoring intern is done by engaging in such activities as website monitoring (tracking of traffic and utilization of cloud-hosted websites), virtual machine monitoring (monitoring the virtual infrastructure and individual virtual machines (VM’s), database monitoring (monitoring of processes, queries, and the use/availability of database resources), virtual network (VN) monitoring (this being the monitoring of a VN’s resources, devices, connections as well as overall performance), and cloud storage monitoring (this being the monitoring of storage resources and their processed provisioned to virtual machines, services, databases, and applications) (ipswitch, 2019).

Regarding cloud monitoring there is a plethora of paid and shareware one can employ. For Amazon Web Services (AWS) users, there is Amazon Cloudwatch, for Microsoft Azure users there is Microsoft Cloud Monitoring which is a collection of built in tools for Azure (Dobran, 2020). Companies such as Solarwinds offer Software as a Solution (Saas)-based monitoring solutions for an organization’s applications and infrastructure (Solarwinds, 2020).; this in turn contains application and infrastructure monitoring, web performance monitoring, and cloud-based log management.

**High-Level Steps Implementation**

Other things to consider in order to improve the security of Drotos Engineering’s cloud systems would be an investment in physical security. Policies should be enacted that only allow authorized personnel access to the servers. The server room itself should be secured by whatever means budgeting permits; either lock and key, keypad, biometric identification (ocular scanners, finger print scanner, voice recognition, or palm scanners), there should also be the establishment of a demilitarized zone (DMZ) established between the public internet connection and the organizations network.

A DMZ or perimeter network would establish a buffer between public internet connections and the organizations network by establishing permitted connections between the public internet to the organizations network through the DMZ, whereas the DMZ itself is only accessible through the organizations private network (CISA, 2020).

The set-up and configuration of an Intrusion Detection and Prevention System (IDPS) would be beneficial in additionally protecting the organizations infrastructure. The configuration of an IDPS on Drotos network allows it to monitor and look for any breaches or attempts at a breach in the organizations network. An IDPS essentially looks for irregular patterns within the organizations network and takes measures to mitigate the threat to the network up to disconnecting the attacker from the network; some IDPS systems can even capture the attackers IP address. Enterprise solutions can be purchased through McAfee (McAfee NSP), Trend Micro (Trend Micro TippingPoint), Darktrace (Darktrace Enterprise Immune System) (Robb, 2019); it is important to note, Darktrace employs an AI based system, this could be beneficial in that it limits the need for personnel to monitor the traffic the IDPS digs through (Darktrace, 2020). Something else of importance, IDPS’s can be used to detect compromised user accounts such as attacks by disgruntled personnel (Robb 2019).

In summation, we have explored the possibility of the utilization of various technologies by addressing encryption possibilities. We have also explored tools such as Firewalls, IPS’s IDPS’s, and the concept of data integrity. We have also explored cloud monitoring and various applications that can assist the organization in its cloud operations. And finally, we have addressed the implementation of better physical security practices for the organization, the implementation of a DMZ and IDPS in order to better protect Drotos Engineering’s systems from possible internal and external threats.

**References**

Carter, D. (2017). Certified Cloud Security Professional Exam Guide [PDF edition]. New York, NY: McGraw-Hill Education.

CISA. (2020). Control System Security DMZ. Retrieved from <https://www.us-cert.gov/ics/Control_System_Security_DMZ-Definition.html>

Content Security. (2019). INTRUSION DETECTION & PREVENTION SYSTEMS. Retrieved from <https://www.contentsecurity.com.au/intrusion-detection-prevention>

Cucu, P. (2017). 11 Point Checklist to Data Integrity. Retrieved from <https://heimdalsecurity.com/blog/data-integrity/>

Darktrace. (2020). Cyber AI Platform. Retrieved from <https://www.darktrace.com/en/technology/>

Dobran, B. (2020). 23 Cloud Monitoring Tools: The Definitive Guide For 2020. Retrieved from <https://phoenixnap.com/blog/cloud-monitoring-tools>

Eletriby, Sherif & Meslhy, Eman & Abd elkader, Hatem. (2012). Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing. Retrieved from <https://www.researchgate.net/publication/264235540_Modern_Encryption_Techniques_for_Cloud_Computing_Randomness_and_Performance_Testing>

ipswitch. (2019). Cloud Monitoring and the 9 Best Practices You Need to Adopt. Retrieved from <https://www.ipswitch.com/Ipswitch/media/Ipswitch/Documents/Resources/Whitepapers%20and%20eBooks/eGuide-NM-9-Best-Practices-Cloud-Monitoring.pdf>

Kumar, Vimal., Chaisiri, S., & Ko, R. (2017). Data Security in Cloud Computing [PDF edition] . Stevenage, United Kingdom: The Institute of Engineering and Technology.

Network Encyclopedia. (2020). Public Key Infrastructure (pki) . Retrieved from <https://networkencyclopedia.com/public-key-infrastructure-pki/>

Robb, D. (2018). 9 Top Intrusion Detection and Prevention Systems: Guide to IDPS. Retrieved from <https://www.esecurityplanet.com/products/top-intrusion-detection-prevention-systems.html>

Solarwinds. (2020). Full-Stack Cloud Performance Monitoring. Retrieved from <https://www.solarwinds.com/topics/cloud-monitoring-tools>

Venafi. (2020). How Does Pki Work. Retrieved from <https://www.venafi.com/education-center/pki/how-does-pki-work>

Wilson, S. (2018). CompTIA Cloud+ Certification Study Guide, 2nd Edition [VitalSource Bookshelf version]. Retrieved from vbk://1260143503

Wójcik,  D. (2018). Analyzing security solutions in cloud computing technology. Retrieved from <https://www.cloudcomputing-news.net/news/2018/jan/30/analysing-security-solutions-cloud-computing-technology/>