BOOK CHAPTER | Cloud Coverings

Information Security Incident Handling in the Cloud

Abraham Sackey
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: abram.sackey@gmail.com
Phone: +233244153371

ABSTRACT

Information security incident handling in the cloud is an integral part of security management, threats detection and analysis of security incidents. The strategies or models are important to ensure the security of an organization particularly in cloud and big data environment. Incident handling strategy is one key strategy to mitigate risks to the confidentiality, integrity and availability of organizational assets, as well as minimizing loss. This study concluded that cloud-based services has changed many organizational cyber threats. It recommended that, there is the need to integrate digital forensics with incident handling. This study suggested that, a collaborative model can be implemented, and this collaboration could be centrally managed by a trusted entity (e.g., Centre for Cloud Incident Management). Further studies are required in monitoring incidents both proactive and reactively.

Key words: Information Security, Incident Handling, Cloud, Cyber Security, Protection, Data

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Abraham Sackey (2022): Information Security Incident Handling in the Cloud
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics.
Pp 103-108 www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P17

1. INTRODUCTION

An incident is a violation (or imminent threat of violation) of computer security policies, acceptable use policies, or standard security practices. Therefore, denial of service, unauthorized sharing of sensitive information, a malicious attack on a computing system or network and the inadvertent deletion of an important document all qualify as incidents as stated by (Ahmad et al., 2015). (Hidayah et al., 2016) also said that, Information security incident handling strategies or models are important to ensure the security of organizations, particularly in cloud and big data environments. Incident handling is a general strategy that guides an organization in dealing with crises, and generally describes the types of incident, identifies the relevant person in-charge, and outlines the action strategy (Hidayah et al., 2016). According to (Mitropoulos et al., 2006) incident response has always been an important aspect of Information Security but it is often overlooked by security administrators.

Hidayah et al. (2015) confirmed from their study that, incident handling strategy is one key strategy to mitigate risks to the confidentiality, integrity and availability (CIA) of organization assets, as well as minimizing loss (e.g., financial, reputational and legal); particularly as organizations move to the cloud. As highlighted by Alberts et al. (2004), there is a need to integrate digital forensics practices in incident handling strategies. Forensic tools and techniques are not only useful for criminal prosecution in a court of law, but also for various other tasks within an organisation, such as event reconstruction (i.e., who, what, when, where, how, and why an incident took place), data or system recovery, and system operation troubleshooting. In other words, incorporating forensically sound practices in an incident handling strategy would support CSUs to be prepared, more proactive, and forensically ready when analysing an incident.

2. LITERATURE REVIEW

The internet is being the network that links the entire planet so responding to security incidents often requires the co-ordination of international efforts. With this, we see that a lot of international cyber security centers are been put up across the world to provide locations for reporting incidents as well as providing appropriate solutions. examples include the computer emergency response team/coordination center (cert/cc) at Carnegie melon university, Australian computer emergency response team, Australia, as stated by (Mitropoulos et al., 2006). Computer Security Incident Response Teams (CSIRTs) are becoming an essential part of modern Information Security Standards (like ISO/IEC 17799) (International Standards Organization, 2000). With their work fully described in RFC 2350 (Internet Engineering Task Force, 1998).

.

(Mitropoulos et al., 2006) proposed a detailed management framework for incident response handling which is mostly combined with the science of digital forensics. The incident response methodology model includes, starting with preparation, identification, containment, eradication, recovery and follow-up. (Grobauer & Schreck, 2010) also proposes similar framework for incident handling. Again, (Grobauer & Schreck, 2010) showed at cloud computing will have a significant impact on incident handling, one of the corner stones of sound security management. Hence stated that Cloud customers must establish clarity about their requirements on CSPs for successful handling of incidents and contract CSPs accordingly; CSPs must strive to support these requirements and mirror them in their SLAs; research into cloud incident handling must focus on the most pressing issues and most promising approaches.

(Hidayah et al., 2016) stated that incorporating forensically sound practices in an incident handling strategy would support CSUs to be prepared, more proactive, and forensically ready when analyzing an incident. Challenges in implementing both incident handling and digital forensics practices have been associated with issues from a CSU's perspective, such as limited access to systems that store data of forensic interest (e.g., data centers located overseas and in multiple jurisdictions), the correlation of activities across cloud stakeholders, and data segregation for CSUs who are not under investigation. Grobauer and Schreck (2010) further explain that response should incorporate containment, eradication and recovery phase, which is consistent with the proposed guidelines from CSIRT (Computer Security Incident Response Teams) (Alberts et al. 2004) and NIST (Cichonski & Scarfone 2012).

This is the definition adopted in this paper, namely: incident management is the 'big picture' (as presented in Figure 1) that comprises incident handling and incident response. Figure 1 represent the scope of this study.

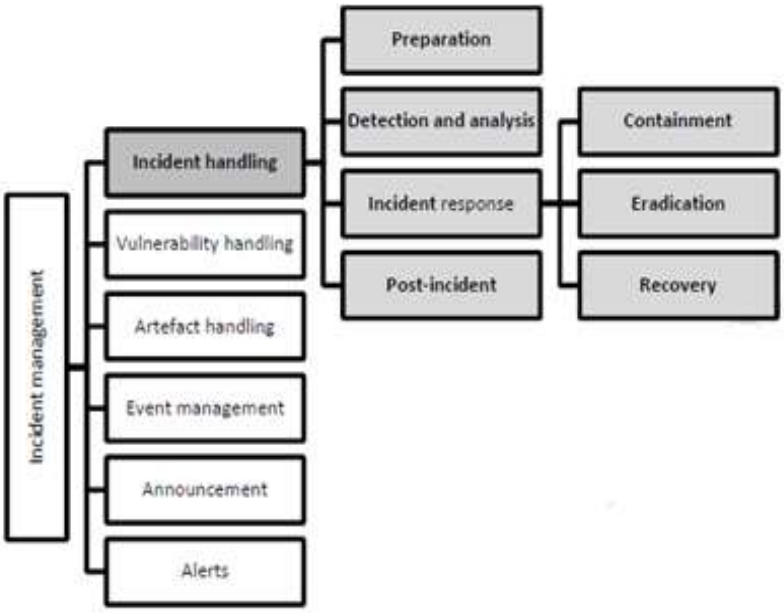

Figure 1: What is incident management? (Adapted from: Alberts et al. 2004; British Standards Institution 2007; Cichonski & Scarfone 2012

Alberts et al. 2004; Cichonski & Scarfone 2012; Grobauer & Schreck 2010). Despite the use of different terminologies to describe the various phases in the standards and guidelines and academic models Incident handling generally starts with incident preparation, followed by detection and analysing of the (detected) incidents, executing response activities, discussing the incident issues in the post incident phase and finally implementing improvements for future actions. Therefore, we conclude that the four main phases in incident handling are: (1) preparation, (2) Detection and Analysis, (3) Incident Response

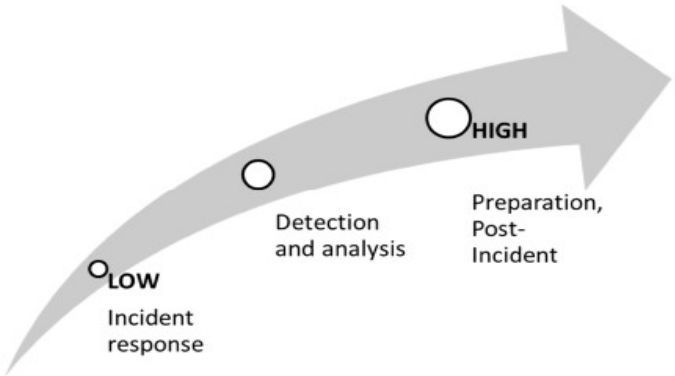

Figure 2: Degree of Proactiveness

We argue that both Preparation and Post-Incident phases require high degrees of proactiveness as both phases actively incorporate mechanisms to prepare, protect and secure an organisation's assets. Incident response is mainly reactive, and the proactive degree for Detection and Analysis ranges between low and high.

2.1 Research Gaps

Base on the research performed, the following findings or area of improvement were noted in respect to incident handling and management in the cloud:

Digital forensics are not integrated incident handling in the cloud environment.

Cloud service providers and users are in the fundamental stages of integration of forensic reviews in their incident handling approach. New and creative technique of monitoring are yet to be deployed to check user activities in cloud environments utilizing a secure cloud forensic framework.

Governmental organizations do not handle incidents cases with the right laws and directives.

Most governmental organizations across the globe but with specific reference to the Africa Region do not have right laws or directives that govern their activities, these directives should be integrated in policies and standards that will service as guidelines for cloud service providers to ensure that consumer's data remains confidential and secure. Furthermore, there is lack of collaboration among multiple national organizations in the handling of incidents handling. This includes criminal investigative bodies, cloud software service providers, hosting service providers and users.

There is limited security incident visibility for cloud system users, owners, manager and administrator

While migrating critical services to the cloud, most enterprises focus their attention on handing of local and wide network security incidents overlooking the need to oversee the security incidents happening on the cloud platforms which house their data.

Limited Availability of Affordable Tools and Technology

Currently there are limited availability of affordable tools and technology to support a holistic enterprise security incident monitoring including cloud security incidents. This is a disincentive to the medium and small enterprises across the Africa Region and globally who form the significant proportion of enterprises.

3. PERSPECTIVES AND IMPLICATION FOR AFRICAN ONLINE SAFETY

The introduction of cloud computing in the part of the world the African sub region has transformed information and communication technologies capabilities through new forms of hosting and delivering ICT services over the Internet. This has allowed African countries to bypass infrastructural and provisioning limitations by removing the costs of expensive technology and allowing them to use hardware, software, data, and platform services provided by service providers who possess the technological infrastructure. Cloud computing advancements provide cost-effective data handling opportunities that benefit crucial areas like economic productivity, employment, natural catastrophe and resource management, and public service delivery.

Despite massive ICT spending and investment in many African countries, money and cost remain a hurdle to fully utilizing cloud computing. These hurdles are computed by further challenges with ensuring adequate security of data and environments hosted on the cloud. With the challenges of limited visibility of security events on the cloud, African users are further disadvantaged by having majority of the service providers not in Africa. Cloud computing can become the most viable information technology solution by focusing more on information security awareness, cloud privacy, and ensuring proper rules and processes are first put in place. The major themes in analyzing the strategic information security of Cloud computing, which should be explored in the coming years for African are cloud security policies, cloud transparency and cloud incident handling.

The drive for a more secure African cloud can be piloted through entities such as the African Union and National Regulators to provide education and guidelines that ensure that Africa service users ask the right questions and consider all the relevant terms before signing up for cloud hosting services or deploying cloud environments. The region also need to build the capacity to cope with the cloud computing services by investment in improves employees' existing skills, digital skills or completely reskill those whose job descriptions will change because of the introduction of cloud computing services.

4. RECOMMENDATION

Base on the reseach above I noted the following areas of inprovments for informantion secuity cloud incident handing and management.

- Cloud operator or service providers should allow the visibility for cloud service users so they can know and see what security incidents are occurring on their platform. This could be in the form of periodic reports or dashboard.
- Governments and cloud Incident Management Bodies should desiged a conceptual cloud incident handling model which will integrate with digital and cyber forensics knowledge base to support the mitigation of incidents. As reiterated by: (Hidayah et al., 2016) a conceptual cloud incident handling model can be designed by integrating digital forensics principles, Capability Maturity Model for Service (CMMI-SVC), to better support incident handling in the cloud environment.
- Governmental organizations and industry regulators should design and institute policies and standards to govern cloud incident management. This framework will emphasizes on the significance of evaluating cloud computing policies, standards, and guidelines, as well as exposing significant corporate risks. (Mitropoulos et al., 2006) recommended that governmental institutions should to treat all incidents with respect to privacy and issue appropriate laws and directives.
- As digital forensics are not integrated in incident handling in the cloud, a new and creative technique, affordable tools and technology to monitor, need to be deployed to check user activities in the cloud environments, Compared with classic digital forensic, the field of cloud forensic poses a lot of difficulties since data is not stored on a single storage unit and furthermore it involves the use of virtualization technologies.

5. CONCLUSION

The growing use of cloud-based services has altered the cyber threat landscape for businesses and presented new obstacles during incident response. *Cloud* Service Users (CSUs) would be able to draw out an effective and efficient plan if they had a clear awareness of security responsibilities and incident handling skills. Cooperate bodies, State National Authority should form legal framework for cloud incident management and also consider implementing tools that will help in monitoring and mitigate cyber threats and attacks in any form.
Integrate digital forensics in incident handling strategy is also a critical tool for reducing threats to the confidentiality, integrity, and availability of corporate assets as also identified by Nikkel, 2014). However, it has a disadvantage of the cloud's organizational data being attacked as organizations and business move to the cloud.

6. DIRECTIONS FOR FUTURE WORKS

(Mitropoulos et al., 2006) stated that incidents should be both proactive and reactively addressed to counter against a lunched attacked. The responses such as automated trace-back mechanisms are all in the early stages which still needs more research. (Hidayah et al., 2015) mentioned that, a collaborative and international cloud incident management platform with the aims of sharing information between geographically dispersed multiple stakeholders and facilitating real-time incident handling and responses to malicious cyber activities in real-time. Collaborative information sharing among Computer Security Incident Response Teams (CSIRT) members is an area worth further studies particularly in a cloud environment context.

REFERENCE

1. Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 1–7. https://doi.org/10.1016/j.ijinfomgt.2015.08.001
2. Alberts, C, Dorofee, A, Killcrece, G, Ruefle, R & Zajicek, M 2004, Defining Incident Management Processes for CSIRTs: A Work in Progress, Pittsburgh.
3. Alecsandru Patra¸scu and Victor-Valeriu Patriciu Beyond Digital Forensics. A Cloud Computing Perspective Over Incident Response and Reporting
4. Military Technical Academy, Computer Science Department, Bucharest, Romania DOI: 10.1109/SACI.2013.6609018
5. Grobauer, B., & Schreck, T. (2010). Towards Incident Handling in the Cloud : 77–85.
6. Hidayah, N., Rahman, A., & Choo, K. R. (2015). AC SC. Computers & Security. https://doi.org/10.1016/j.cose.2014.11.006
7. Hidayah, N., Rahman, A., Dwi, N., Cahyani, W., & Choo, K. R. (2016). Cloud incident handling and forensic-by-design : cloud storage as a case study. https://doi.org/10.1002/cpe
8. Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response : A state-of-the-art approach. https://doi.org/10.1016/j.cose.2005.09.006
9. Nikkel, BJ 2014, 'Fostering Incident Response and Digital Forensics Research', Digital Investigation, inpress, DOI: http://dx.doi.org/10.1016/j.diin.2014.09.004.