DEPLOYMENT OF HONEYPOTS AS PROACTIVE DETECTION TOOLS FOR MONITORING CYBER RELATED INCIDENCES

Peter Odhiambo Ogada, George Raburu and S. Liyala
School of Informatics and Innovative Systems
Jaramogi Oginga Odinga University of Science and Technology
P.O. Box 210-40601, BONDO-Kenya

N. B. Okelo
School of Mathematics and Actuarial Science
Jaramogi Oginga Odinga University Science and Technology
P.O. Box 210-40601, BONDO-Kenya

ABSTRACT

The Kenya government is striving to roll out its Vision 2030 programme where ICT plays a major role in achieving the components of the Pillars associated with it. The purpose of this study was to find out the extent to which deployment of HoneyPots as early warning detection tools for monitoring cyber related incidents had been embraced within KENET member institutions in Western Kenya, how they are aiding the institutions in knowing and understanding their adversaries; and allowing them to implement solutions that work in defending the critical internet and network infrastructures they manage. The study was guided by a descriptive study design with a study population of 117 staff members working in various institutions in western Kenya. Using simple random sampling technique, a sample size of 80 respondents were picked and administered with questionnaires, 70 questionnaires were returned for data entry and analysis using Statistical Package for social Sciences version 20. This implies that 87.5% of the respondents turned up for the study. According to the major findings, the study established that most of the KENET member institutions in western Kenyan, despite experiencing cyber security related incidents, had not setup CIRT teams nor deployed Honeypots to help them study cyber security incidents and take appropriate action to defend their constituencies. As a recommendation, the Government, being one of the economic stakeholders, and KENET, should come up with intervention measures through the Ministry of ICT making it mandatory for setup CIRTs. All CIRTs should then be required to direct part of their traffic to the national CERT which ideally should be based at Communication Authority of Kenya to form a Honey Net, which can further be linked with other internationally recognized Honey Net projects.

1.1 INTRODUCTION

The Kenya government is striving to roll out its Vision 2030 programme where ICT plays a major role in achieving the components of the Pillars associated with it. The government has variously encouraged for the rapid deployment of the high speed fiber optic cables across the country to make it easier for its citizens to do business amongst themselves, with the government and the various industry players (Kenya Vision 2030, 2007). Unfortunately, as the deployment of high speed internet connections becomes more widespread and popular among citizens, complex cybercrimes are also on the raise thus creating a demand for improved cyber security to the users via use early warning systems with intrusion detection capabilities covering cybercrime incidents (Kenya cyber security report, 2014). It is for this reason that KENET, as a government supported entity embracing learning and research institutions, has been encouraging its member institutions to setup CIRT teams within their institutions. The teams are encouraged to deploy HoneyPots within their constituencies as one of the measures to help monitor cyber related incidents via generating incident reports which in turn would be used for identifying, understanding attackers and their communities modus operandi; cyber threats; prepare trend analysis on cyber threats; identify new tools or methods of cyber attacks; and act as early warning and prediction systems on cyber incidents (IATAC, 2009). The purpose of this study was to find out the extent to which deployment of HoneyPots as early warning detection tools for monitoring cyber related incidents had been embraced within KENET member institutions in Western Kenya, how they are aiding the institutions in knowing and understanding their adversaries; and allowing them to implement solutions that work in defending the critical internet and network infrastructures they manage.

1.2 Objectives

i. To examine the types of cyber security related incidents affecting KENET member institutions in western Kenya.

ii. To determine factors affecting the deployment of HoneyPots by CIRTs in KENET member institutions in western Kenya.

iii. To analyse the usability of HoneyPots in KENET member institutions in western Kenya as proactive detection tools for monitoring cyber related incidents.

1.3 Research Questions

i. What types of cyber related incidents are affecting KENET member institutions in western Kenya?

ii. What are the factors affecting the deployment of HoneyPots by CIRTs in KENET member institutions in western Kenya?

iii. How can KENET member institutions in western Kenya use HoneyPots as proactive detection tools for monitoring cyber related incidents?

1.4 Significance of the Study

This research study aims at aiding CIRTs know and understand their adversaries; hackers and the various malwares, hence allowing them to be in a position to implement solutions that work in defending the critical internet and network infrastructure they manage. Beneficiaries of this survey include Government departments currently rolling out e-services and the Academia especially KENET member institutions. Based on the study, the Government, through its various ministries and departments, will strive to offer quality e-services to their clients in the full knowledge of secure data centers setup, as they will be more proactive with their cyber security issues; while investing in quality equipment and technical staff with clear cyber security mandates, development cyber security policies, and how cyber security issues can be handled more proactively within the legal boundaries. On the other hand, the Academia will be more involved in researches that tackle cyber related incidents thus be in a position of sharing cyber related crime intelligence with cooperating partners; allowing them to understand cyber crime incidents and their perpetrators. It will also allow them to act much more swiftly and proactively, before they are affected for example consider the work done by the HoneyNet Project (Spitzner, 2014), an all volunteer, non-profit security research organization which is one of the most well known examples of using HoneyPots for research; the data they collect is distributed around the world even as threats are constantly changing, this information has proved to be more and more critical.

1.5 Scope of the study

This survey is intended to evaluate the level of deployment of HoneyPots as early warning detection tools for monitoring cyber related incidents. It was confined within the KENET member institutions in the western Kenya that are connected to the national fiber backbone. The survey was carried out within three months starting September to November 2014.

1.6 Assumptions of the study

i. All respondents will give honest responses.

ii. Where HoneyPots were set up, they were done so correctly to avoid them being hacked, thus compromising the whole research project's objectives.

4. RESULTS AND DISCUSSION

4.4 Types of cyber security incidents affecting institutions

4.4.2 Number of cyber security incidents

85.7% of the institutions had registered less than - 10 cyber security incidents. 10% reported 20 or more incidents, while 4.3% reported between 11-19 incidents. This numbers are very low thus further proof on the need to setup CIRT/CERT department or teams to fully dedicate their time and resources in collecting cyber related incidents. This would help institutions to plan for disasters associated with cyber security incidents. As it is, very few staff and resources were being dedicated to cyber related incident.

Table 15: Number of cyber security incidents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	<=10	60	85.7	85.7	85.7
	11- 19	3	4.3	4.3	90.0
	=> 20	7	10.0	10.0	100.0
	Total	70	100.0	100.0	

4.4.3 Most common cyber incidents cyber fraud

22.9% of institutions reported that cyber fraud was their most common cyber incident, while 77.1% reported never experiencing cyber fraud cases. This could be attributed to low adaptation of online payment methods or none deployment of mechanisms to detect such incidents even though they were occurring.

Table 16: Most common cyber incidents cyber fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	16	22.9	22.9	22.9
	No	54	77.1	77.1	100.0
	Total	70	100.0	100.0	

4.4.4 Most common cyber incidents Malware

75.7% of institutions reported that malwares were their most common cyber incidents, while 24.3% reported that they did not experience any malware cases. This report could be attributed to the reliance on Anti Virus engines that are the most commonly deployed tools against viruses.

Table 17: Most common cyber incidents Malware

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	53	75.7	75.7	75.7
	No	17	24.3	24.3	100.0
	Total	70	100.0	100.0	

4.4.5 Most common cyber incidents Botnets

Only 8.6% of the institutions reported that they had ever been victims of Botnets, while 91.4% indicated that they had never been affected by Botnets incidents. This could be due to non existence of data centres setup or incidents were occurring but no mechanisms to detect the same.

Table 18: Most common cyber incidents Botnets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	6	8.6	8.6	8.6
	No	64	91.4	91.4	100.0
	Total	70	100.0	100.0	

4.4.6 Most common cyber incidents Spam

57.1% of institutions reported that Spams were their most common cyber incidents, while 42.9% reported that they did not experience any Spam cases. This could again be attributed to the use of AV engines as the most widely deployed tool to control malicious software.

Table 19: Most common cyber incidents Spam

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	40	57.1	57.1	57.1
	No	30	42.9	42.9	100.0
	Total	70	100.0	100.0	

4.4.7 Most common cyber incidents Phishing

Only 17.1% of institutions reported that Phishing was their most common cyber incident, while 82.9% reported that they did not experience any Phishing cases. This low figures are a further proof cyber security features very low in the Institutions priority areas. No mechanisms deployed to report on such incidents.

Table 20: Most common cyber incidents Phishing

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	12	17.1	17.1	17.1
	No	58	82.9	82.9	100.0
	Total	70	100.0	100.0	

4.4.8 Most common cyber incidents VoIP PBX fraud

Among institutions in western Kenya, only 2.9% had reported that they had experienced **VoIP PBX fraud,** while 97.1% reported that they did not experience any **VoIP PBX fraud** cases. This could be attributed to low or non deployment of VoIP facilities within these institutions, or none deployment of sensor mechanisms to monitor VoIP facilities.

Table 21: Most common cyber incidents VoIP PBX fraud

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	2	2.9	2.9	2.9
	No	68	97.1	97.1	100.0
	Total	70	100.0	100.0	

4.4.9 Most common cyber incidents Insider Threats

Only 22.9% of the institutions had reported that they had experienced **Insider Threats,** while 77.1% reported that they did not experience any **Insider Threats** cases. Despite the large number of staff deployed in these institutions ICT units, this is a unique observation. Again, the monitoring and reporting mechanisms could be missing, staff are very highly disciplined or none existence of ICT policies to guide in ways of handling such cases.

Table 22: Most common cyber incidents Insider Threats

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	16	22.9	22.9	22.9
	No	54	77.1	77.1	100.0
	Total	70	100.0	100.0	

4.4.10 Most common cyber incidents Social media

62.9% of the institutions had reported that they had experienced **Social media** incidents, while 37.1% reported that they did not experience any **Social media** incidents. Since most of the institutions surveyed were academic oriented, this is no surprise at all as most students use such media a lot. Institutions seem not to be filtering such traffic via their firewalls. Those with low numbers could be having strict policies on use of social media, or their firewalls are actively controlling such traffic.

Table 23: Most common cyber incidents Social media

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	44	62.9	62.9	62.9
	No	26	37.1	37.1	100.0
	Total	70	100.0	100.0	

4.4.11 Most common cyber incidents DOS attacks

24.3% of the institutions had reported that they had experienced **DOS attacks** incidents, while 75.7% reported that they did not experience any **DOS attacks** incidents. This is an indication of low presence of the institutions in the World Wide Web, or none existence of mechanisms to monitor and report on DOS oriented attacks on services or facilities available online to their staff and clients.

Table 24: Most common cyber incidents DOS attacks

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	17	24.3	24.3	24.3
	No	53	75.7	75.7	100.0
	Total	70	100.0	100.0	

4.4.12 Most common cyber incidents Cyber Espionage

7.1% of the institutions had reported that they had experienced **Cyber Espionage** incidents, while 92.9% reported that they did not experience any **Cyber Espionage** incidents. This being a more complicated concept of cyber crime, its rarity is not surprising at all. But again a lack of cyber monitoring and reporting tool could also come into play in such a scenario.

Table 25: Most common cyber incidents Cyber Espionage

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	5	7.1	7.1	7.1
	No	65	92.9	92.9	100.0
	Total	70	100.0	100.0	

CONCLUSION

There is need to conduct a research survey across all institutions that are affiliated to KENET as well as all government ministries and agencies to determine their preparedness in terms of detecting and monitoring cyber related incidents. This will help in facilitating a deeper understanding of cyber network traffic within KENET infrastructure and the country, and thereby be able to pinpoint ways of improving our networks security.

REFERENCES

Babbie, E. (2007). *The Practice of Social Research*. Twelfth Edition. USA: Chapman University.

Brenner S. W., L. L. (2005). Distributed Security: A New Model of Law Enforcement. *John Marshall Journal of Computer & Information Law, Forthcoming.*

CAK. (2014). *KE-CIRT*. Retrieved from www.cck.go.ke: https://www.cck.go.ke/

Canada, L. C. (2004). *What Is a Crime? Defining Criminal Conduct.* Vancouver/Toronto: UBCPress.

Carter, L. W. (2004). *SANS Institute.* Retrieved from http://www.sans.org: http://www.sans.org/reading-room/whitepapers/casestudies/setting-honeypot-bait-switch-router-1465

Cunningham, C. C. (2013). *Honeypot-Aware Advanced Botnet Construction and Maintenance.* University of Central Florida, School of Electrical Engineering and Computer Science. Orlando, FL: University of Central Florida.

Denzin, N.K., & Lincoln, Y.S. (1994). *Handbook on Qualitative Research*. Thousand Oaks, CA: Sage

Economic Times. (2009, August 19). *Cybercrime india and brazil major hub*. Retrieved from www.articles.economictimes.indiatimes.com:

ENISA. (2012). *Proactive Detection of Security Incidents.* Polska: ENISA.

European Cybercrime Survey. (2011). EECTF. Rome: EECTF.

Goodman Marc D. (1997). Why the Police don’t care about computer crime. *Harvard journal of law and Technology*, 1-30.

IATAC. (2009). Measuring Cyber Security and Information Assurance. In (Information Assurance Technology Analysis Centr) IATAC, *Measuring Cyber Security and Information Assurance.* Fort Belvoir, Virginia: Defense Technical Information Center.

KENET. (2014). *Our History*. Retrieved from www.kenet.or.ke: https://www.kenet.or.ke/

KENET, CERT report. (2014). *Welcome to the KENET CERT*. Retrieved from www.kenet.or.ke: https://www.kenet.or.ke/

Kenya Cyber Security Report (2014). *Serianu Limited.* Nairobi: Serianu Ltd,.

Kombo, D. K., & Delno, L. A. T. (2006). *Proposal and Thesis Writing: An Introduction*. Nairobi: Pauline’s publications Africa.

London Daily News. (2009). *www.cyberlawtimes.com*. Retrieved from CyberLawTimes.com: http://www.cyberlawtimes.com/cyberlaw/3-million-online-crimes-a-year-new-cyber-crime-squad-to-be-established/

Newswise. (2009). *China linked to 70 percent of worlds spam says computer forensics expert.* Retrieved from www.newswise.com: http://www.newswise.com/articles/china-linked-to-70-percent-of-worlds-spam-says-computer-forensics-expert

Pariyani, R. (2014). *www.manupatra.co.in.* Retrieved from manupatra.co.in: http://www.manupatra.co.in/newsline/articles/Upload/779E337A-DDF8-41AE-ACA4-89F3CB746F2D.pdf

Pathan, A.-S. K. (1990/91). *The State of the Art in Intrusion Prevention and Detection.* Natick, Massachusetts: CRC Press, Taylor & Francis Group.

Ping Wang, L. W. (2010). Honeypot detection in advanced botnet attacks. *Int. J. Information and Computer Security*, 30-32.

Punch, F.K. (2010). *Introduction to Social Research: Quantitative and Qualitative Approaches*. Second Edition. New Delhi: Sage Publications Ltd.

Sabine, L., & Everitt, B.S. (2004). *A Handbook of Statistical Analysis Using SPSS*. USA: Chapman & Hall /CRC Press on 30/08/2012.

Saini H., Rao Y. S., Panda T.C.(2012) International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209.

Schuttler, K. (2014). *Eastern Michigan University College of Technology*. Retrieved from www.emich.edu: www.emich.edu/ia/pdf/research/Honeypotresearch.pdf

Spitzner, L. (2002). *Honeypots: Tracking Hackers*. Boston, Massachusetts: Addison Wesley.

Spitzner, L. (2002, December 10). *Windowsecurity*. Retrieved from www.windowsecurity.com: www.windowsecurity.com/whitepapers/honeypots/Honeypots_Definitions_and_Value_of_Honeypots.html