CYB 320 Project Two

Douglas Few

June 24th, 2022

Acceptable Use Policy

This incident, in my opinion, does violate the Ocwen Acceptable Use Policy. Policy number 4.1.4 states “Employees are responsible for exercising good judgment regarding the reasonableness of personal use…and if there is any uncertainty, employees should consult their supervisor or manager.” Using company issued devices to run a side business and post advertisements on a dating website does not constitute good judgment of personal use. Likewise, policy number 4.2.4 states “Postings by employees from an Ocwen-owned/leased computing device to personal social media accounts is strictly prohibited.” This scenario, based on the Acceptable Use Policy, clearly violates the guidelines of acceptable use.

Potential Evidence

Potential evidence can be found in a number of locations. The first place I would look is the server. By creating a forensic image of the server, we can create a direct copy of all of the information and data on the server at the time the image is created (Goldstein, 2019). This will allow us to examine and investigate the copy while the real server continues to run. This process will not only help in our investigation, but will also support business continuity by causing limited interruptions.

The second area that can be searched for evidence is the device that was used to conduct the alleged acts itself. Whether this incident occurred on a company-issued device or on a BYOD device otherwise owned by the user, it may be subject to confiscation. Once confiscated, we can search the device for evidence that the user was in fact uploading unauthorized posts to his personal social media pages. The device may still have evidence of its usage history stored within its hard drive and can be searched for when social media accounts were used and whether it was during working hours or on company property.

The final area that should be searched for evidence is the intrusion detection system. By checking the network intrusion detection system, we may be able to run a scan that verifies whether this incident occurred on the company network. The NIDS will scan the network for all incoming and outgoing traffic and the scan can be analyzed for suspicious outbound traffic that fits the description of the incident (Cole, 2013). If we are able to determine by this method that company computing assets were used for unauthorized personal use, we can more effectively build a case for disciplinary action toward the user.

Chain of Custody

The most important part of maintaining a chain of custody is ensuring that each instance of evidence being passed on to a new individual or organization is well documented. This needs to happen every time a new person inspects evidence so that there is a clear history of everyone that handled the evidence. This is important because it reduces suspicion of tampering. If each pass off is well documented, there will never be doubt about when and where the evidence was at all times. However, if no such documentation exists, there can be no confidence that the evidence was handled in a trustworthy manner. According to Badiye, Kapoor, and Menezes (2022), the ten pieces of information that should always be included in the chain of command are as follows:

1. Unique Identifier
2. Name and signature of the sample collector
3. Official address and contact number
4. Name of the recipient
5. Address of the Lab
6. Details of each sample
7. Signatures of everyone involved in the possession with date and time
8. Date and method of delivery
9. Authorization for the analysis of the evidence
10. Any other information about the evidence

Forensic Tools

One of the tools that should be used in the investigation is a forensic imaging tool. There are many options that range from freeware to paid software that can be used to digitally copy the data stored on a media device (Poston, 2021). This tool will assist in imaging the data on the suspected devices and on the network, allowing us to inspect the data stored on the hardware more easily. Another tool that will be critical in the investigation is a tool for unencrypting any software protections that may be placed on the device. By using a commercial product that enables a forensic investigator to bypass any potential passwords on the device, we need not worry about what protections the alleged actor placed on the suspected device. One popular tool used for such cases is Elcomsoft (2022).

Resources

Badiye, A., Kapoor, N., & Menezes, R. (2022, February 17). *National Center for Biotechnology Information*. Chain of Custody. Retrieved June 26, 2022, from https://www.ncbi.nlm.nih.gov/books/NBK551677/

Cole, E. (2013). Chapter 6 - Prevention is Ideal but Detection is a Must. In *Advanced persistent threat understanding the danger and how to protect your organization* (pp. 123–144). essay, Syngress.

Elcomsoft, E. (2022). *Elcomsoft mobile forensic bundle*. Elcomsoft Co.Ltd. Retrieved June 26, 2022, from https://www.elcomsoft.com/emfb.html

Goldstein, S. (2019, September 18). *Two key differences between digital forensic imaging and digital forensic clone and how they can affect your legal case.: News: Capsicum: Digital Forensics, investigations, cyber security*. CAPSICUM. Retrieved June 26, 2022, from https://capsicumgroup.com/2-key-differences-between-digital-forensic-imaging-and-digital-forensic-clone-and-how-they-can-affect-your-legal-case/

Poston, H. (2021, May 6). *7 best computer forensics tools*. Infosec Resources. Retrieved June 26, 2022, from https://resources.infosecinstitute.com/topic/7-best-computer-forensics-tools/