Forensic Evidence Collection and Handling Policy

7/21/2022

Daniel Moreno

Evidence Collection

Investigation

Before gathering evidence, the CSIRT members assigned to the incident must investigate the situation. These individuals should have authorization to collect the evidence from the proper members of management and the legal department (Wex Definitions Team; Solomon 301). They should determine the extent of the incident and the affected devices. They need to contact the appropriate individuals, as listed by the communication policy. They should acquire the necessary tools and resources to collect the evidence. The individuals that use or oversee the affected devices need to be interviewed regarding the incident to determine the duration and their part in the incident, especially when dealing with viruses. In addition, they should take pictures of the area, the office, and the desktop (CWU Information Security Services 6; Department of Information Technology 26, 30). These interviews and pictures should be logged and stored in a secure location, like a safety deposit box.

Collection

Only individuals who have undergone the proper training regarding evidentiary procedures and have signed the InfoSec NDA should be permitted to collect evidence (CWU Information Security Services 6). Once authorized personnel have been located, they should be deployed to acquire available evidence. Based on the results of their investigation, the CSIRT should be able to determine whether it would be better to simply observe the attacker or to quarantine the system. If the attack poses too great of a danger to the company's network or proprietary data, all cables connecting the device to the network should be removed. Avoid turning the device off unless absolutely necessary (Department of Information Technology 22).

Volatile evidence should be targeted first to prevent its erasure when the device is restarted and can be captured through a complete memory dump. On a PC, this should capture the operating system kernel modules, active network connections, open processes and registry handles, ARP cache, temporary files, unallocated space, and more. On a router, the memory dump will collect the routing table, configuration, and network topology (Department of Information Technology 25, 34; Pekker). If relevant to the investigation, save emails and other files sent from the affected devices that the system did not store locally (CWU Information Security Services 7). Immediately after placing the data on a removable storage media, insert it into a tamper-proof bag with an attached item tag and chain of custody form (“Alert Antistatic Tamper Evident Evidence Bag”). The cryptographic hash of the data on the removable media needs to be stored on either the item tag or a separate, tamper-proof device (Department of Information Technology 26). Later, they should create a cryptographic hash of all data on the hard drives before turning the device off and physically removing the hard drives. These hard drives should be stored within tamper-proof bags that have an item tag and a chain of custody form (“Alert Antistatic Tamper Evident Evidence Bag”).

Evidence Handling and Analysis

Preserving Evidence Integrity

Throughout the process of gathering the evidence, everything should have been stored in tamper-proof, electrostatic-safe bags to prevent any alterations of their contents (“Alert Antistatic Tamper Evident Evidence Bag”; Department of Information Technology 31). The stored cryptographic hashes of data will indicate that the data on the devices has not been changed (Department of Information Technology 26). The chain of custody forms with proper signatures will reveal who gathered the evidence, who has accessed it, and who has overseen its storage (Solomon 300). By tracing the evidence from its collection through its usage to its presentation in court, the company can guarantee the data’s admissibility (*Digital Evidence: Policies and Procedures Manual* 1). If the evidence will be stored off-site, the team should photograph the transportation vehicle as it leaves the original scene and arrives at the storage site (Department of Information Technology 30). The evidence should be stored in a secure location like a bank’s safety deposit box (Department of Information Technology 46).

Evidence Analysis

Evidence must be analyzed for it to contribute to the company’s case in court. A copy of the evidence should be made to prevent any changes to the original data on the storage devices. The individual responsible for performing the examination must sign the chain of custody form and replace the tamper-proof seal on the bag after making the copy. These copies can be analyzed using the company’s standard programs to perform activities like file carving (Department of Information Technology 39-40; Pekker). To ensure admissibility in court, the original copy of the evidence must be presented without any alterations, including ones accidently induced during the analysis process (*Digital Evidence: Policies and Procedures Manual* 1; Bommisetty et al.).

Works Cited

"Alert Antistatic Tamper Evident Evidence Bag." *Alert Security Bag*, alertsecurityproducts.com/antistaticsecuritybag/index.shtml. Accessed 21 Jul. 2022.

Bommisetty, Satish, et al. *Practical Mobile Forensics*. E-book, Packt Publishing, 2014.

CWU Information Security Services. *Digital Forensics Policy and Procedure*. Central Washington University, 2020. www.cwu.edu/security-services/sites/cts.cwu.edu.security-services/files/documents/Digital Forensics Policy and Procedure -Public.pdf, PDF file.

Department of Information Technology. *Digital Notes on Computer Forensics*. Malla Reddy College of Engineering & Technology, 2019-2020. mrcet.com/pdf/Lab Manuals/IT/R15A0533 CF.pdf, PDF file.

Digital Evidence: Policies and Procedures Manual. National Institute of Justice, 1 May 2020. Report no. NCJ 254661. www.ojp.gov/pdffiles1/nij/254661.pdf, PDF file.

Pekker, Michael. "PlainSight: Open Source Computer Forensics Software." *Data Recovery*, Apr. 2013, files-recovery.blogspot.com/2013/04/plainsight-open-source-computer.html. Accessed 21 Jul. 2022.

Solomon, Michael G. *Security Strategies in Windows Platforms and Applications*. 3rd ed., E-book, Jones & Bartlett Learning, 2021.

Wex Definitions Team. "Admissible Evidence." *Cornell Law School*, Nov. 2021, www.law.cornell.edu/wex/admissible_evidence. Accessed 21 Jul. 2022.