Unit 9 Reflection

This week, I read up concerning forensics of data. I found the content of this unit to interesting in that there is a tremendous amount of work that goes into ensuring the quality of data is kept as clean as possible when attempting to report on data breaches or attacks. Before launching into this module, I had very little idea that system forensics was an intricate job, taking as much care and attention to detail to preserve evidence of a crime scene; though the scene involves information security hardware and software, and the crime is committed against data and systems. I found the reading material quite enlightening regarding information security forensics, how similar the processes are between data forensics and civilian crime regarding evidence preservation.

To support information security, systems must implement some form of logging without which, it is not possible to know about security incidents. All events generated by an information system must be logged, though not all events may be relevant. Logging helps forensic analysis uncover steps that may have led to a malware infestation or other related security breach. Logging also helps identify compliance issues and enables organisations to become proactive in corrections. I think the one major usefulness of logging is to correlate related events, thus enabling easier auditing of process flows. Regarding logging, I appreciated the templates provided by Swift (2010) that highlight provided guidance on events of interest.

However, I think logging events of interest is only a single cog in the arsenal of information security management, others include having a Business Continuity Plan (BCP) to create processes and systems to act during extreme incidents such as earthquakes or terrorist attacks. In addition, a Disaster Recovery that enables how to continue operations when a system is attacked or fails. In addition to logging, I considered that malware scanning tools are often employed to for malware on copies of suspect data. Containment areas known as sandboxes are leveraged to isolate malware-infested data allows it to execute without impacting the surrounding network. One interesting tool I learned about was the idea of a write blocker used by forensic analysts to obtain data from a source disk without damaging the disk through accidental write commands.

Additionally, I learned that techniques such as static analysis and code analysis can be used in addition to information security forensics tools. Static analysis is useful to help identify malware or viruses. The reading material from this unit's eBook (Practical Information Security Management by Tony Campbell) referred to the IDA Linux-based tool to perform code analysis. I have some basic experience using this tool so found some connection to understanding of static analysis in computer forensics. Using tools and techniques to maintain security information management certainly does follow a pattern, as expressed by Vielberth and Pernul (2018). Lastly, briefly reading RFC 3227 was interesting as it provides a basic guideline on evidence collection and archiving was enlightening because it impacts

This week I contributed to the third collaborative discussion and engaged with students regarding their interesting case studies, posing questions to further understand the implementation of GDPR policy in their given cases.

References

Swift, D. (2010). Successful SIEM and Log Management Strategies for Audit and Compliance. Available from https://www.sans.org/white-papers/33528/ [Accessed 29 Jan. 2021]

Vielberth, M. & Pernul, G. (2018). A security information and event management pattern.