Fullsoft Malware Attack and Security Breach

Fernando D. Parra

Metropolitan State University of Denver

CSS 2754-001 Host Security

Maranda Mulder

March 25, 2024

Fullsoft Malware Attack and Security Breach

The significance of security awareness, proper security controls, and effective incident response planning for Fullsoft is essential to address this issue and prevent similar events from occurring again, a comprehensive discussion of the incident and its impact on the company identifies measures to mitigate risks and exhibit substantial benefits that support the risk assessment and gap analysis plan along the way.

Circumstances

The incident highlights issues that may have contributed to the breach, employee security awareness training, plans, standard procedures, and security policies necessary to prevent such incidents weren't enforced. The absence of a policy and security controls for controlling the use of removable media played a vital role in the incident. In addition, a guide such as NIST's 800-61 for incident handling could have allowed Fullsoft to handle an incident using preparation, detection and analysis, containment, eradication, recovery, and finally post-incident activity. Furthermore, if the company's security systems were not properly configured, or there was a failure in the incident response plan, this could have made it easier for the malware to be installed and for proprietary information to be leaked. These gaps, along with potential weaknesses in endpoint security measures all allow similar incidents to occur again in the future.

Insights

Reports of similar malware attacks via USB drives can offer valuable insights for Fullsoft. In other organizations, similar events have commonly been caused by inadequate security controls, employee negligence, or malicious intent. For instance, Stuxnet: "a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant" (Kushner, 2024). The risks associated with using Stuxnet are

malware infection (evidently), spyware, and remote access. Threat actors will frequently exploit social engineering vulnerabilities to deploy USB flash drives within local area networks, this is a major attack vector that many organizations can overlook. In *The Real Story of Stuxnet* by David Kushner, it is stated that Stuxnet "could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant". Fullsoft can gain insight into the downstream impacts of data breaches, such as financial losses or reputational damage, allowing them to understand the true extent of the attack.

Outcomes & Countermeasures

Fullsoft should prepare for an attack on their business in multiple ways. The leaked intellectual property may be used by competitors, resulting in lost market share and revenue. Legal action may be necessary to protect trade secrets depending on the nature of the information. Moreover, the company may face regulatory fines for data breaches and a damaged reputation that impacts customer trust. It is imperative to implement an approach surrounding certain operations; incident response plans, disaster recovery plans, and business continuity plans. To achieve this, deploying hardening, a data loss prevention policy, and an acceptable use policy is essential. Although the previously mentioned policies and standard procedures are overlooked by numerous organizations or companies, these are severely crucial to know what to do, how, and when. Furthermore, executing application whitelisting, mean time to repair, mean time between failure, recovery time objective, recovery point objective, educating employees on phishing, and safe USB drive usage will significantly reduce the likelihood of malware infections.

References

Computer Security Incident Handling Guide. (n.d.-a). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

EDR security: Protecting the network from endpoint threats. Cynet. (2024, January 31). https://www.cynet.com/endpoint-protection-and-edr/

Harish.P, A. (2023, July 14). *USB flash drive malware: How it works & how to protect against it*. LinkedIn. https://www.linkedin.com/pulse/usb-flash-drive-malware-how-works-protect-against-ashwin-harish-p/

The hidden costs of an IP breach: Cyber theft and the loss of Intellectual Property. Deloitte Insights. (n.d.). https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html

Kushner, D. (2024, January 20). *The real story of stuxnet*. IEEE Spectrum. https://spectrum.ieee.org/the-real-story-of-stuxnet

Meyers, M., & Weissman, J. S. (2022). *Mike Meyers' comptia network+ certification passport, seventh edition (exam N10-008)*. McGraw-Hill Education.

Using caution with USB Drives: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2024, March 26). https://www.cisa.gov/news-events/news/using-caution-usb-drives