Assignment 3: Classifying Security and Privacy Issues

CYBR3080

IT Service and Delivery Security

Gregory Stephens

Incident 1: Compromised Supplier Software Update (Security Issue)

The company depends on an outside vendor for its enterprise resource planning (ERP) software needs. The company remained unaware that cybercriminals had infiltrated the vendor's systems and inserted malicious code into a regular software update. The malicious software propagated throughout the company's network after they applied the update which allowed attackers to gain unauthorized access to essential systems. The incident resulted in severe operational disruptions including production stoppages and shipment delays which resulted in millions of dollars in lost revenue. Avetta identifies these attacks as major supply chain risks due to their exploitation of trust between organizations and their vendors. [1] The main concern of this event is security because attackers gained the ability to manipulate systems and data which allows them to interrupt operations. The cyber breach that did not involve the theft of personal information underscores the necessity of thoroughly examining suppliers' cybersecurity protocols. To mitigate this risk organizations need to conduct thorough testing and validation of third-party updates before they are deployed.

Incident 2: A data breach occurred through a logistics company leading to both privacy and security problems.

A third-party logistics company managing confidential customer data for a major online retailer fell victim to a phishing attack directed at its workforce. Unencrypted databases provided attackers access to customers' personal details including their names, addresses, and payment information. According to Terranova Security supply chain vulnerabilities like insufficient workforce training and encryption flaws frequently lead to confidential information leaks. [2] This security breach poses dual threats by infringing on personal data access rights while revealing system defense weaknesses. The incident resulted in customer lawsuits and damaged the e-commerce company's reputation. Businesses can stop similar breaches by applying strict data protection measures throughout supply chains while requiring constant cybersecurity education for employees and applying end-to-end encryption to protect sensitive data.

References

[1] https://www.avetta.com/blog/top-5-supply-chain-cyber-risks
[2] https://www.terranovasecurity.com/blog/supply-chain-attacks