**Tesla Data Breach - Insider Attack**

Tesla is a member of the automotive industry specializing in the innovation of electric cars and clean energy products. Based in Palo Alto, California, Tesla now has 45,000 plus employees and is the only vertically integrated energy company that continues to scale and reduce the cost of systems to eventually reach energy grids that are a 100% renewable (“About Tesla | Tesla”, 2019). On June 17, 2018, Tesla was known to be exposed to an inside attack when Elon Musk, CEO of Tesla announced to the employees’ that a disgruntled employee of Tesla had greatly damaged and sabotaged the company’s operations by using his trusted access to the company’s network to download gigabytes of sensitive corporate data and export it to third parties. According to Musk, the employee was also able to alter Tesla’s manufacturing operating system by making direct code changes using false credentials (Vijayan, 2018). The stolen and exported information included trade secrets, financial information of the company, dozens of confidential photos, and a video of Tesla’s manufacturing systems. According to the company, the loss of any other data is still being investigated. From what is known about the breach today, the forensics investigation launched by Tesla indicated that the source code written by the identified employee was found to be designed to send the company’s data to third parties even after the employee left the company. Additionally, the code was found to be installed on three other computers as an attempt to implicate employees other than the disgruntled employee himself. Tesla also filed a lawsuit against the former employee for $167 million in damages (Kolodny, 2018), and the employee had admitted to writing the code that altered the manufacturing operating systems. However, the employee stressed that “he didn’t hack anything and was being singled out for being a whistleblower” for warning investors and the public about the company’s lithium batteries from his experience as a technician in Tesla (Tung, 2018).

Tesla’s breach indicates the importance of insider monitoring in any organization. Whether an inside threat occurs for malicious purposes, through an honest mistake or carless employee behavior, monitoring limits the risk exposure by allowing the security team to quickly detect the unusual employee activity on systems. Furthermore, it is important to note that disgruntled employees have intimate knowledge of the organization and its systems and can easily cause significant amounts of damage. However, even though predicting human’s nature is hard, encouraging a periodic discussion between employees and their managers can diffuse insider threats.

References

About Tesla | Tesla. (2019). Retrieved from https://www.tesla.com/about

Kolodny, L. (2018). Tesla is seeking $167 million in damages from the former employee Elon Musk accused of sabotage. Retrieved from: https://www.cnbc.com/2018/12/11/tesla-seeks-167-million-in-damages-from-ex-employee-martin-tripp.html

Tung, L. (2018). *Tesla: We’re now suing ex-employee for alleged theft of gigabytes of trade secrets.* Retrieved from https://www.zdnet.com/article/tesla-were-now-suing-ex-employee-for-alleged-theft-of-gigabytes-of-trade-secrets/

Vijayan, J. (2018). Tesla Employee Steals, Sabotages Company Data. DarkReading. Retrieved from https://www.darkreading.com/informationweek-home/tesla-employee-steals-sabotages-company-data/d/d-id/1332098