Incident Analysis Brief  
CYB 200 Cybersecurity Foundations

Sergio Mateos

Southern New Hampshire University

Last week, while the payroll administrator was taking a coffee break, a suspicious individual broke into her office damaging property and stealing a document in the drawer, including the USB headset. Also, the payroll administrator noticed that the suspicious user was carrying a backpack filled up with a lot of equipment or documents, and a “weird-looking” electronic device. The situation is very sensitive since the information was stolen and the identity of the individual is unrecognizable.

While the payroll administrator was reporting the incident, the information security noticed several foreign connections were made to the corporate network using the payroll administrator account. The next day, the payroll of the employees was calculated incorrectly, and this scale to the human resource office.

As a member of the information security, my job is to create a scenario analysis of the situation and conclude with a solution. Based on the information provided, the exposure of the information, and the result of the attack, the company had an integrity issue. Based on the tenets of cybersecurity, CIA (Confidentiality, Integrity, and Availability), refer to Integrity as only authorized user can modify information. The legitimation of information is crucial in any industry, from employee to customer since it could involve financial or personal information that could be necessary in their situation.

In our scenario, the suspicious user broke into the payroll administrator and was able to access the information of the employees in the company. The investigation indicates that the user had remote access log several times using the payroll administrator, and since the payroll administrator has most of the information of the employees, the suspicious individual was able to alternate the information in the payroll. The impact of the suspicious user was so great in the company that the human resource office had to look into it, unfortunately, we do not have a lot of information on the type of alteration in the documents, but how the situation scaled the damage was unmeasurable. Also, the knowledge of the documents stolen is unknown, and it could be impossible to identify the content of the stolen documents since the workstation was turned sideways. But that information plus the payroll administrator could end up in a huge modification on the database, affecting many employees.

Threat to the integrity of the data is a serious problem for the company, employees, and customers since the attacker now has a lot of information that could help attack different areas. The payroll system was inaccurate is a significant problem for the company, since an attack was available to modify the payroll plus it provide information about the income of members of the industry which is a violation of the laws of the employees, and it could end up in legal issues. Since most of the companies have direct deposit implemented, the malicious user is available to have access to the bank information of the users which could end up in major issues. The malicious user could find a vulnerability in the system after logging in with the payroll administrator credential, and if so, the malicious user could install a backdoor for easier access to the system or deploy a virus or worm to damage the database.

The data has been breached and now it is time to mitigate the problem via different techniques which will help us to get to the information or patch any vulnerability in the system. To define a better solution, I will use the Fundamentals Security Design Principles, which will improve security. In our scenario, I will work with two important design principles which are layering and isolation.

Layering is a security strategy in which multiple tools, mechanisms, and policies are deployed to back one after the other, in other words, if one of the tools fails by a malicious user, there would be another strategy that will hold. Layering could be in the form of hardware or software. “Layered security seeks to implement multiple mitigating layers of protection so that intruders have to break through many security measures at the same time” (Imi, 2021). Every part would be secure in different layers starting from access to the offices, and strict requirements to access the building would be implemented. The use of cameras, key cards, and constant monitoring of every person who accesses the building. At the entrance, before the employee is allowed to access the building, there will be a biometric reader (fingerprint reader), which will identify the authenticity of the employee. The biometric reader will minimize the number of unauthorized users if they try to sneak into the building. Since most of the employees would not have a set office, the drawers will require a lock to prevent any vulnerability in the physical access of information. Even if the malicious user gets to access the office and the payroll administrator room, the network would be secured by implementing firewalls to monitor what comes in and out of the network, unique identification to access important information (username and password), and two-factor authentication would be implemented if the information is the high level of secure.

Isolation is the process in which a part of the system is running in its own space which helps to not interfere with other processes running. If we secure the payroll and other important information in certain workstations the compromised network will decrease significantly. Since the payroll administrator has access to a lot of important information, the network will need to be more secure, to preserve the security of the data it will need to implement a two-factor authenticator, which only the right user will have the answer for the question or special key to access to the data. Monitoring the network would provide a better view of what is connecting from the external network and what is coming in.

The solutions balance impacts on people, processes, and technology because it focuses on physical and network aspects. The physical security of the offices prevents any suspicious individuals from having access to the building. There would be different processes for new hires or vendors which also prevent access to malicious users trying to personify any staff members. Outside the building cameras should be of high quality to be available to identify any suspicious move or induvial. The system should be updated frequently to prevent unpatched vulnerability. The use and follow of preventive action would preserve the integrity of the information within the company. The actions may take time to implement but they need to be implemented since the security of the data and employees is a high priority.

Overall, every aspect is important to prevent a physical or network attack, but focusing on the security awareness and education of the employees will prevent most of the access to our data. Most of the threats to a company are successfully achieved via social engineering, from emails to phone calls. “Most digital attacks today involve some form of social engineering.” (Bisson, 2023))

.

Reference

Rundle, J. (2021, December 17). *Cyberattack on payroll provider sets off scramble ahead of Holidays*. The Wall Street Journal. https://www.wsj.com/articles/cyberattack-on-payroll-provider-sets-off-scramble-ahead-of-holidays-11639778286

Imi. (2021, April 24). *Importance of layered security in Cyber Defense*. Identity Management Institute®. https://identitymanagementinstitute.org/importance-of-layered-security-in-cyber-defense/

Plankers, B., Bob Plankers                  Staff Cloud Infrastructure Security & Compliance Architect & CISSP at VMware working to bridge people, & Petrov, A. (2020, July 7). *The importance of isolation for security*. VMware vSphere Blog. https://blogs.vmware.com/vsphere/2020/07/importance-of-isolation-for-security.html

Bisson, D. (2023, July 19). *Most digital attacks today involve social engineering*. Security Intelligence. https://securityintelligence.com/articles/most-digital-attacks-today-involve-social-engineering/