CYBR 320

M5 Simulation

Abby Gopal

10-9-2023

A person looking at something

Description automatically generated

A company is planning to launch a new app, but the IT team discovers evidence that they are under a targeted attack. The attackers are using social engineering to trick employees into revealing their credentials. As a CIO, I decided to postpone the app launch until they could be sure it was secure. I believed this was a wise decision, as a successful attack could damage the company's reputation and cause financial losses. This was a difficult decision for me as it meant delaying the launch of the app and potentially losing revenue. However, it is also the safest option, allowing the team to thoroughly investigate the security breach and fix any vulnerabilities before launching the app.

A person in a suit

Description automatically generatedA person in a suit

Description automatically generatedAs a CIO, I outsource the security assessment to a third party. It was a good decision, allowing the company to access expert help without hiring additional staff. I chose this option because the team does not have the expertise or resources to investigate the security breach internally. However, selecting a reputable third-party provider and carefully reviewing the contract before signing it is essential. This is a risky option, as there is no guarantee that the freelancers can identify and fix all the security vulnerabilities—ITFr33X, recommended by one of the IT team members.

A person in a car

Description automatically generated

A person sitting in a car

Description automatically generatedAs a CIO, I implemented stricter access policies using the company's internal Active Directory. I felt it was a good decision, as it would make it more difficult for attackers to gain unauthorized access to the company's systems. This would help to improve the security of the company's systems. Still, it is important to ensure that the access policies are implemented correctly and do not disrupt the company's operations. On an added note, it can save companies revenue without buying additional security software. At this point, I felt that encrypting all intellectual property could be a valuable way to protect it from unauthorized access. But then, I thought it was not always necessary. If the company has a strong risk management program and has taken steps to protect its intellectual property in other ways, such as through access control, then encrypting all intellectual property may not be necessary to waste the company's investment. Ensuring compliance with all the regulatory requirements is important for a number of reasons. First, it helps to protect the company from fines and penalties. Second, it helps to protect the company's reputation. Third, it helps to protect the company's customers and employees. Ensure that we are fully compliant with all the regulatory requirements the company can help to protect itself from these risks. The company can also demonstrate to its customers that it is committed to protecting their data.

A person looking at something

Description automatically generatedA person in a suit

Description automatically generatedThe decision to make the journalist wait for the launch of the app is important to fix any known vulnerabilities before launching a new app, as a successful attack could damage the company's reputation and cause financial losses. In the cybersecurity decision scenario context, the company faces several security risks. The attackers are using social engineering to trick employees into revealing their credentials, and they have also attempted to compromise the company's code repository. Until the company can be sure that all these security risks have been mitigated, it is prudent to delay the launch of the app. This will give the company time to fix known vulnerabilities and implement additional security measures. By making the journalist wait for the launch of the app, the company is protecting the journalist from potential harm. The journalist may be able to access the app before it is officially launched, but they would be doing so at their own risk.

A person looking at the camera

Description automatically generated

As a CIO, I decided to purchase breach detection technology. By purchasing breach detection technology, the company can improve its ability to detect and respond to these security threats. The technology will monitor the company's systems for suspicious activity and alert the security team if anything is detected. This will allow the security team to investigate and take appropriate action to mitigate the risk quickly. Breach detection technology can detect malware that has bypassed traditional security measures. It can also detect unauthorized access to systems and data and can detect any data exfiltration attempts. This is a good option for improving the company's ability to detect and respond to security breaches. However, choosing the right breach detection technology for the company's needs and budget is important. This scenario suited very well without breaking the company's budget.

A person holding a cell phone

Description automatically generated

As a CIO, I had the security team check the breach detection system logs. This is a good decision, as it will help the company to identify any suspicious activity that may have occurred. By checking the breach detection system logs, the security team can identify any suspicious activity that may have occurred due to these attacks. For example, the logs may show that the attackers could gain unauthorized access to specific systems or data or that they attempted to exfiltrate data from the company's network. Quite honestly, at this point, I felt I had enough of a threat to deal with for one day…. I was also hoping the end was near …the smile on the CIO's face assured me that.

THE END

A person shaking hands with another person

Description automatically generated

References:  
<http://targetedattacks.trendmicro.com/index.html>

What I learned from playing the game

I learned a lot from playing the Targeted Attack. I learned about the different types of targeted attacks, how to identify them, and how to defend against them. I also learned the importance of having a strong security posture and being prepared for a security incident. I felt more confident in this game than in the first one. I think this is because I better understood the different types of targeted attacks and how to defend against them. I also better understood the game's mechanics and how to use the available resources.

Targeted attacks are becoming more sophisticated and dangerous. The game showed me how attackers use social engineering and other techniques to target specific individuals and organizations. It is important to have a strong security posture. The game showed me how important it is to invest in purchasing a breach detection system to help detect security incidents more quickly so that companies can mitigate the damage. It is important to be prepared for a security incident. The game showed me how important it is to have a plan, like strict access policies and breach detection technology, that can help improve a company's overall security posture for responding to a security incident.

Overall, I found The Game to be a valuable learning experience. It helped me better understand the threats of targeted attacks and how to defend against them. I also learned that thinking critically and making quick decisions in high-pressure situations is essential. The game often put me in problems where I had to make quick choices about allocating my resources and responding to threats. This helped me to develop my decision-making skills. Overall, I felt that the game was a good representation of the challenges that cybersecurity professionals face daily. It was a challenging game, but it was also gratifying. I felt accomplished when I successfully defended my organization from a targeted attack.