Old Dominion University

IT 417 Management of Information Security

UScellular Data Breach

Professor: Vijay Kalburgi

Brian Delos Santos

UIN: 01180618

September 1, 2022

Cyber-attacks are carried out across the world every day. Threats are becoming more manipulative and discrete as technology advances. Without proper funding, technology, knowledge, and motivated individuals to uphold information security within an organization, that organization will be at the mercy of cyber criminals across the world. This is the case with UScellular, a wireless service provider in the United States. This service provider was the victim of a cyber-attack which targeted one of their many employees. This attack allowed threat actors to obtain (PII) personal identifiable information from their (CRM) customer relation management tool. UScellular is only one example of many data breaches that demonstrate the importance of implementing enterprise-wide information security awareness and it will not be the last (Abrams).

Details of the initial attack are very briefly described in UScellular's notice of data breach. An employee was scammed into downloading a remote access trojan which provided the attackers control of the employee's computer. The notice of data breach did not specify if the employee was scammed via a phishing email, call, or if it was just a hoax found on the internet that was intentionally downloaded. Regardless of the attack vector, while the employee was still authenticated to the CRM tool, the attackers were able to exfiltrate PII from the CRM tool and out of their network. The PII exfiltrated by the attackers included client names, addresses, PINs, cell phone numbers, service and billing information. On the bright side, the CRM tool utilized data masking which prevented client social security and credit card numbers from being compromised. This added bit of security saved UScellular from an extreme loss of PII and a potential lawsuit (UScellular).

According to UScellular's "Notice of Data Breach" the incident occurred on January 4, 2021. The notice was sent on January 21 and claimed to have detected the incident two days after

it occurred. Upon detection, UScellular said to have prevented the affected party's information from being accessed any further by employing containment strategies on the infected computer. They also took measures to prevent further access to the accounts compromised by the initial breach by resetting the involved employee credentials and customer CRM authentication information (UScellular).

One of the major tangible impacts of this breach is the customer data that was exfiltrated from the CRM tool. Even though the attackers could not obtain the more sensitive PII like credit card and social security numbers, the affected parties will still have to be very mindful of their compromised accounts. The affected clients could even start to receive an influx of spam or phishing attacks from their phone or emails. The most important intangible consequence is the damage to UScellular's reputation. This consequence cannot be accurately measured, but something all organizations should consider when thinking about the risks associated with a data breach. If you have to disclose a data breach to the public, then potential customers may think twice before buying services because they do not want their data mishandled (UScellular).

In my opinion, UScellular has several options to move forward past this data breach. The first could be to refine the company's user training and awareness program. The second is to address the lack of complimentary controls to prevent the exfiltration of data from the company network to the internet. A data loss prevention tool could have been configured to stop the exchange of certain types of data from the internal network to the internet. Even an application whitelisting policy could have prevented the employee from downloading a malicious application in the first place (UScellular).

In conclusion, UScellular is a wireless service provider who was the victim of a social engineering attack on January 4, 2021. The hackers were able to manipulate a store employee to

download malicious software that allowed remote access to the employee's computer. The hackers were able export data from a CRM application while the employee was authenticated to it and sent it out of their internal network. Because of the intrusion, UScellular's has taken a hit in public reputation for poor data handling. The effected clients will have to monitor their accounts and even reset authentication information to proactively prevent identity fraud. Even though UScellular has suffered a data breach, they can use this as the catalyst to implement better cybersecurity posture and improve the security of their operations (Abrams).

Works Cited

Abrams, L. (2021, January 29). USCELLULAR hit by a data breach after hackers access CRM Software. BleepingComputer. Retrieved September 1, 2022, from https://www.bleepingcomputer.com/news/security/uscellular-hit-by-a-data-breach-after-hackers-access-crm-software/

UScellular notice of data breach to consumers. Office of the Vermont Attorney General. (2021, January 28). Retrieved September 1, 2022, from https://ago.vermont.gov/blog/2021/01/22/uscellular-notice-of-data-breach-to-consumers/