Tahmid Hassan

CYBER SECURITY

19-90307-1

Q1. What security breach has occurred?

Ans: The CIO recived a ransom email from an unknown source stating they knew about the mergen plans and had a personal detail of 150,000 users. As a proof sample of 500 customers were included in the ransom email. After investication it was confirmed that 506 customer information is genuine. but no evidance about 150,000 customer detail that they were taken. Funther investigation found that client was compromised though a combination of human errors insufficient procedures and processes and technical vulnerabilites in their it system.

The CEO of the financial services organisation maintained a high public profile supporting various charities and speaking at industry-leading conferences. Her travels and eminences appearances were publicised on the clients website and without anyon's knowledge in even fan grafen detail in the social media account of her teenage daughter. So the hacker used social Engineering and also spam/malware Email. b. The information that the hacker gined from social Engineering and construct an email that were secived by her Executive assistant. The email appeared to be form the sponsor of a recent conference with an attachment that was described as an expense reporting form.

the EA opened the email and downloaded the expense form. The form contained malware that created an administractive level account. So the intruder had gone straight form the Costomen ~~service~~ database and extracted customer ~~database~~ detail. When it happedned it was the downtime of the fire wall, security measures. Any Alarm had triggered an alert but no one had acted on it because it had happend at the weekend.

Q2. What was the impact of the security breaches?

Ans: The impact of the security breach :-

① Reputational damage — Loss of customer and stakeholder trust can be the most harmful impact of cybercrime since the overwhelming majority of people would not do business with a company that had been breached.

② Theft: Intellectual property theft may be equaly damaging with companies losing years of effort and R&D investment in trade secret or copyrighted meterial — and their competitive advantage.

Financial losses: For a large corporation the financial impact of a breach may run into the millions. According to the latest data breach report by IBM and Ponemon institute the average cost of data breach in 2021 is $4.24M.

Fines: As it direct financial losses weren't punishment enough there is the prospect of monetary penalties for businesses that fail to comply with data protection legislation.

Below-the-surface costs: The economic costs of incident response, there are several intangible costs that can continue to blight a business long after the event itself.

Q3. How did the security get compromised?

Ans: They discovered that information about the CEO was used to construct an email that was received by her Executive Assistant. The email appeared to be from the sponsor of a recent conference with an attachment that was described as an expense reporting form. Without verifying the email EA opened the mail and downloaded the expense form. The form contained malware that created an' administrative level account.