Cyber Crisis: Trickbot

A company in the participant's supply chain has been infected by Trickbot. The participant must decide what action to take to protect themselves, their supply chain and minimise disruption to their business operations.

Initial Scenario

- Your company, Apiary, produces internet connected temperature control systems for commercial use. The internet connection, amongst other uses, allows you to update the software remotely from your network.
- One of your suppliers, with access to your network, has been infected by TrickBot and subsequently ransomware.
- The group behind the attack, RVile, are well known and have historically always provided a valid decryption key after the ransom is paid.
- You must decide the appropriate actions to take, considering business operations; customer ramifications; legal requirements and financial impact.

Subsequent Stages

1.

- You decided to search your network for compromise before proceeding.
- You detect compromise and either a) data exfiltration, b) lateral movement in your network onto customer facing areas of your network and/or c) lateral movement onto your customer networks.

2.

- You decided to isolate the customer connected areas of your network offline, while you search for compromise.
- RVile has seen this action and knows their time is limited. They deploy ransomware on the rest of your network but your customers are unaffected.
- Do you pay the ransom? (business disruption vs ethical considerations)

3.

- You decided to take your whole network offline to search for compromise.
- RVile send you an email stating that they have exfiltrated sensitive data from your network (PII & IP) and demand a ransom or they will sell it.
- Because you took your network offline, you can analyse network logs to identify what data was taken.

Considerations

- How long are operations disrupted for and what is the scale of disruption?
- How do you maintain customer trust throughout this crisis?
- What legal obligations do you have? e.g. reporting the incident.
- What moral obligations do you have? e.g. whether to pay a ransom, informing customers early.
- What are the financial impacts of possible decisions and outcomes?
- What mitigations can be taken and what are the possible unintended consequences of those decisions? Defensive actions such as patching EternalBlue to reduce lateral movement may alert attackers that you are aware of them, causing the attackers to expediate their plans or hide.