SOPHOS

Ransomware Tabletop

What is a Tabletop?

- Ensure Open discussion about ways in which we can manage a given scenario
- Consider our processes and potential responses (both technical and non-technical)
  - Much easier (and less stressful) to have these discussions now rather than in an actual incident
- The tabletop scenario:
  - Not real (thankfully) but please treat it as if it were
  - As with any incident, communication is key, please engage and use this as a forum to throw ideas about
    - There aren't necessarily right/wrong answers
  - This is NOT a finger pointing exercise
    - The aim is to collaborate and find ways we can improve together
    - Find gaps and improvements that can be made so in a real event you will be better prepared

Ransomware Tabletop Exercise

Report of ransomware on employee laptop 4
Another system infected 5
Ransom Demand 6
External Queries 7
Phishing Email 8
Infection spreading 9
Important systems/data compromised 10
Source Code 11
Communication 12
Further escalation of events 13
Employees 14
Active Directory 15
Malware Analysis 16
Clean-up and next steps 17
Recap & food for thought 18
What else? 19

Report of ransomware on employee laptop

- IT have received a report of issues with employee laptop – appears to have been hit with ransomware
  - Employee is working remotely
- We don't know the capabilities of malware at this stage – how can we prevent spread from this laptop?
- What can we do to prevent potential data exfiltration?
  - What Active Directory groups is the user a member of?
  - Disable laptop/account?
- What might be the source of infection?
  - Check recent emails received by user?
  - What URLs were visited prior to infection?
  - Have devices been plugged into laptop recently?

Another system infected

- Multiple reports of users unable to access internal file share/server X. Appears to be same ransomware.
- How can we lockdown access to/from server X immediately to prevent further spread?
- What access does X have to other systems?
  - Shared service accounts in use?
- Source of infection?
  - Which systems have accessed/written to X in the last few hours?
- What alternative can we offer employees in the interim to avoid impact to work/business?

Ransom Demand

- Public ransom request received - $10 million via cryptocurrency. Public declaration of intent to publish data unless ransom is paid.
  - What is the company policy on ransom demands?
  - Are there any legalities to consider?
  - Need to involve legal and PR/Marketing team
  - Do we have cyber insurance?

External Queries

- Legal team and news outlets asking questions
  - Has data been lost/stolen? We don't know for sure at this point
    - Have we seen increase in outbound traffic?
    - Exfiltration likely to be by HTTP(S), FTP, SMTP, DNS
  - Has PII data been lost? If so, how much?
    - Type and quantity of data could have significant implications
    - What type of data is held on affected systems?
      - PII?
      - Source code?
  - Public ransom request has created questions from news outlets
  - What is our response currently?

Phishing Email

- Suspected phishing email reported by employee, appears to be related to the ransomware
  - Can we identify other recipients of email?
    - Can we delete the mail from other recipient's inbox?
    - Should we consider blocking all recipients of the email from the network to be sure?
      - What if the recipients include SMT members?
  - Email contains an IP address which is presumed malicious
    - Can we check for connections to/from this URL/IP?
    - Can we block this IP across the business?
    - Implement alerts for any systems attempting to access the IP?

Infection spreading

- Further systems affected – 1 domain controller and email archive now infected
  - We must prevent further spread – how?
  - This is hitting critical systems now. If further systems are hit it could prove difficult to communicate with the teams as many are remote
  - What is our out of band communication policy in case we are separated?

Important systems/data compromised

- Now that a domain controller and email-archive has been infected we have almost certainly lost PII data of employees
  - What notifications need to take place as a result of this?
  - Do we need to consider potential effects to employees?
  - GDPR? Other national / regional requirements?

Source Code

- Company source code repository has now been hit
  - Have we lost source code?
    - What volume of data was exfiltrated?
    - Which products and repositories were lost?
  - We still don't know the full capabilities of the malware. How can we check/prove that source code has not been altered?
  - How can we prevent further builds/releases until we can verify?

Communication

- Internal and external communication
  - We need to give an update on incident
  - Where should this be published?
  - What should it say?
  - What do we tell employees?
  - What should employees such as support say if asked?

Further escalation of event

- Incident has worsened – Single sign on, 0365, Azure no longer accessible
  - Next steps?
  - How long will it take to restore from backup?
    - What is the process?
    - How can we ringfence restored/re-built systems?

Employees

- Most employees are now without access to company resources – and most are remote
  - How can we communicate with employees?
  - Do we have a list of mobile numbers for employees?
    - How could we message them en-masse?
  - What actions do we need them to take?
    - Rebuild laptops?
    - Switch off/disconnect laptops until we have a better handle on the issue?

Active Directory

- Active Directory Recovery
  - Should we consider a full AD rebuild?
    - What is the process for this?
    - How long would a full recovery take?
  - What is the risk to other parts of the business?
    - Other networks that may be linked to corporate network?

Malware Analysis

- Analysis of malware by Sophos Labs via the phishing email shows malware is spreading via a vulnerability that had a patch released last Tuesday
  - Capabilities are now confirmed:
    - Encryption
    - Exfiltration via ports 80 or 443
    - Remote shell
  - How can we utilise this information?

Clean-up and next steps

- Need a full list of everything yet to receive a patch. How?
- Can we restrict access to anything that is not yet patched in order to prevent further infections?
  - Only allow network access to systems that have been patched?
- How can we ensure no persistence remains?
- Legal/Privacy
  - State/federal notifications?
  - Report crime – what info will legal team need
  - GDPR, CCPA, et al.
- PR/Marketing
  - Status update, cause and resolution
  - What information will the team need?

Recap & food for thought

- Initial infection via phishing email
  - Should we increase phishing training and awareness across the business?
- Infection spread via known vulnerability
  - What is the average time across the business for patches to be applied?
  - Are we confident all systems are receiving patches?
- Damage might have been limited if infected systems/offices were isolated quickly
  - What playbooks/readiness preparation could be implemented to help make significant decisions in a real world event?
    - For example – at what point do we disconnect a whole office from the business to prevent spread/infection?

What else?

- What else haven't we covered in the previous slides?
- Other suggestions or concerns?

For more information on the Ransomware Tabletop Exercise click here.

2023-10-23 (PC)

SOPHOS