Current UK Incident Response Program

Process Phases Updated 101118

Identification

Incident is reported in Service Now ticket

Security team receives incident from email/phone/other

Assign Sec-Incident Coordinator

Security team Identifies the type of incident

- Denial of Service
- Malicious code
- Unauthorized access
- Inappropriate usage
- Multiple component
- reech/Reportabl Incident
- Ransomeware

Yes

No

Assign ticket to appropriate party

Security Incident Coordinator will assign priority Level to incident

- Critical 15 minute from notification
- High 1 hour from notifaction
- Medium 8 hours from notifaction
- Low 8 hours from notification

Analysis

Was there PII on the system? Or, is it impacting services.

Yes

Assemble Response Team fro evaluation (appendix b)

Evidence Collection:
Was the information encrypted?
Was the encryption key compromised?
When was the incident detected?
How was the incident detected?
When did the incident occur/end?
Is the incident still occurring?
Is the incident contained?
What systems were involved?
Who is the attacker (IP, hostname, country)?
How was the vulnerability exploited?
What type of information was compromised?
Was information deleted, modified, and/or accessed?
What level of access was compromised?
What tools/techniques were used?
Are utilities or malware installed on systems?

If needed expand response team

Was there PCI data?

No

Log to Service Now or respond to user.

Yes

Notify Kevin Sisler

Notify CISO

CISO Notifies : CIO, Corporate Compliance, Legal , Public Affairs, Law Enforcement, Human Resources, Public Relations

Notify HB-5

Containment

If Possible, Disabling/disconnecting network connections; Increased monitoring (physical or logical); Powering down systems; Halting or reducing business services.

Incident Coordinator will ensure all actions are recorded

Is a forensic back up need?

No

Yes

Contact James Welch (DTS)

Eradication

Ad-Hoc but can include the following

- Law Enforcement (follow SOP, appendix A)
- Wipe & rebuild
- Patching OS/APP/Protcol
- Security Vendor Support
- Application vendor support

Recovery

The Response Team will implement strategy for recovery including

- Restore form back up
- Rebuild Machine
- Install patches
- Change password & reset questions
- Monitor System for activity
- Follow up with the user to educate

Lessons Learned

- Automate
- Communication to UK : CoP SECSWAT Dean's IT
- OSINT
- Develop strategies for future incidents
- After Actions report

Continuous Education

- PCI Table Top Exercise
- Yearly Education