Incident Response and the Law

Andrew Cormack, Chief Regulatory Adviser (@Janet_LegReg)
Logging

Essential for...

- **Detection**: Did anything happen?
- **Investigation**: What happened?
- **Mitigation**: How to repair it?
- **Learning**: How to stop it happening again?
Logging

Most logs contain (GDPR) personal data

- Network flows
- Application flows (e.g. who sent/received malware)
- Authentication (successes and failures)
- Web requests
- Database requests
- Application requests
- Etc.
Logging

OK (under GDPR Rec.49) to keep these so long as...

- They help us detect/respond
- No less intrusive way to do that
- Risk of keeping < risk of not keeping

So...

- Start from detection/response processes
- Keep (securely) the logs those may use
- Delete logs when no longer useful (e.g.)
  - External changes make investigation impossible
  - Lapse of time makes investigation pointless
Scanning: Proactive test for vulnerable machines
Is this (criminal) “unauthorised access?”

<table>
<thead>
<tr>
<th>Is it...</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access?</td>
<td></td>
</tr>
<tr>
<td>Unauthorised?</td>
<td></td>
</tr>
<tr>
<td>With good intention?</td>
<td></td>
</tr>
</tbody>
</table>
## Scanning

Is this (criminal) “unauthorised access?”

<table>
<thead>
<tr>
<th>Is it…</th>
<th>UK Computer Misuse Act 1990</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access?</td>
<td>Yes: Anything that prompts a response is “access”</td>
</tr>
<tr>
<td>Unauthorised?</td>
<td>Not defined, but UK law recognises both explicit (e.g. by contract/policy) and implicit (e.g. by action) authorisation.</td>
</tr>
<tr>
<td>With good intention?</td>
<td>Irrelevant</td>
</tr>
</tbody>
</table>

- Limited case law suggests
  - “in-protocol” scans (e.g. SYN/ACK or banner grabbing): should be OK
  - Active exploits: probably not OK
  - Scans that may crash target: probably not OK
Incident Response
Investigation

Again: “least intrusive that will achieve purpose”

- Focus on malicious/unknown activity
- Automate that selection where possible
- Avoid linking to humans if you can
  - Machine identifiers are preferable
- Identify *victims* when you know they need help

Keep identification of *attackers* (“attribution”) separate
  - Legal provisions are very different
Notification/Sharing

Again: “risk of sharing < risk of not sharing”

Informing victims (internal and external – to mitigate/remediate)
- Send only the information they need to help themselves
- Keep distribution small/effective (victim, org…)

Informing peers (mostly external – to prevent/detect)
- Send only the information they need to help themselves
- Use trusted communities if possible

Would this help attacker more than defender?