The Hitchhiker's Guide to Data Breaches

DON'T PANIC!

Josh M. Bryant
Cybersecurity Architect
Microsoft
Incident Response Lifecycle

Preparation → Detection & Analysis → Containment Eradication & Recovery → Post-Incident Activity

Source: NIST
Incident Response Lifecycle

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity

Source: NIST
WHO YOU GONNA CALL?

1. GHOSTBUSTERS
2. Lawyers
3. Insurance
4. Law Enforcement
5. Trusted Partner

DON’T PANIC!
Does it worry you that you don’t talk any kind of sense?

- Douglas Adams, Agda to Arthur Dent, The Restaurant at the End of the Universe

Protect me from knowing what I don’t need to know.
Protect me from even knowing that there are things to know that I don’t know.
Protect me from knowing that I decided not to know about the things that I decided not to know about.

Amen

- Douglas Adams, Arthur Dent’s personal prayer, Mostly Harmless
We always ask ourselves "why" because we always do something with intention.

Douglas Adams

IT DOESN'T MATTER!
IT DOESN'T MATTER!
IT DOESN'T MATTER! WHO?
What?

(This actually matters, a lot.)
Incident Response Lifecycle

- Preparation
- Detection & Analysis
- Containment Eradication & Recovery
- Post-Incident Activity

Source: NIST
What should we do?

Plan

Scope Compromise

Stage

Critical Hardening

Execute

Tactical Monitoring

Rapid Eviction
### Scope Compromise

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Investigation</td>
<td>The investigation results determine “what” needs to be mitigated during recovery. It’s important to prescribe the correct medication to a patient by first understanding the symptoms.</td>
</tr>
<tr>
<td>Document Indicators</td>
<td>Defining Scope helps reduce the tendency to introduce sweeping network changes. Focus on addressing the current attacker. Remember your ABCs: Accounts, Backdoors, Command and Control</td>
</tr>
<tr>
<td>Identify Business Critical</td>
<td>What systems can the organization not live without? What support systems do those business critical systems depend on?</td>
</tr>
<tr>
<td>Review Active Directory</td>
<td>Active Directory is the authentication and authorization provider for most organizations. Active Directory must be reviewed for highly exposed security settings that can be easily leveraged by an attacker.</td>
</tr>
</tbody>
</table>
## Critical Hardening

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory</strong></td>
<td>RemEDIATE Critical Security Issues identified during the review. If there is a business justification for not remediating, it must be identified as a risk.</td>
</tr>
<tr>
<td><strong>Workstation Traffic</strong></td>
<td>Prevent or limit the ability of an attacker to easily move between systems.</td>
</tr>
<tr>
<td><strong>C2 Lockdown</strong></td>
<td>Prepare to block the attacker’s Command and Control communication channels.</td>
</tr>
<tr>
<td><strong>Administrative Practices</strong></td>
<td>Put controls in place to prevent exposing high value accounts to high risk systems.</td>
</tr>
</tbody>
</table>
## Tactical Monitoring

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Account Logon</strong></td>
<td>Monitor Local Account activity for signs of attacker use.</td>
</tr>
<tr>
<td><strong>Advanced Threat Analytics</strong></td>
<td>Detect advance credential theft techniques through analysis of authentication traffic as it moves across the network, as well as user and entity behavior analytics.</td>
</tr>
<tr>
<td><strong>Business Operations</strong></td>
<td>Business Critical Systems must be monitored for signs of attacker activity based on available Threat Intelligence.</td>
</tr>
<tr>
<td><strong>Authentication System</strong></td>
<td>The heart of any network or system services is the authentication store. It contains the keys to all systems and is often the first target for attackers. These systems must be monitored in order to protect the entire enterprise.</td>
</tr>
</tbody>
</table>
## Rapid Eviction

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staged Rebuild</strong></td>
<td>Systems that require attention are prebuilt for transition into production during the eviction event. The goal of eviction is to catch the adversary off guard and eliminate their access holistically.</td>
</tr>
<tr>
<td><strong>Password Resets</strong></td>
<td>Password resets of compromised assets – whether users, service accounts or the AD krbtgt – are performed during the eviction event. Some accounts, such as excessive admin accounts or stale accounts, may be removed during this event.</td>
</tr>
<tr>
<td><strong>C2 Blocking</strong></td>
<td>An attacker can't prosecute your network if they can't communicate with it. During execution, all known C2 channels are blocked in a coordinated effort so an attacker cannot reconstitute their network foothold.</td>
</tr>
<tr>
<td><strong>Implant Cleanup</strong></td>
<td>Overly complex systems, systems with limited bandwidth, or widespread infections can make rebuilding impractical. In these cases, implant persistence and artifacts are removed from the infected system.</td>
</tr>
</tbody>
</table>
For a moment, nothing happened. Then, after a second or so, nothing continued to happen.

-Douglas Adams, The Hitchhiker’s Guide to the Galaxy
Incident Response Lifecycle

Preparation → Detection & Analysis → Containment Eradication & Recovery → Post-Incident Activity

Source: NIST
Human beings, who are almost unique in having the ability to learn from the experience of others, are also remarkable for their apparent disinclination to do so.

-Douglas Adams, Last Chance to See