2311 Corporate Way
Kalamazoo, MI 49008

Incident Response Playbooks

[My IR playbooks are all in my head, but didn't want to leave you without anything to go on! Good luck, hope this helps! -Jacqui]

Yoyodyne's Kalamazoo office has 4 major categories of security incidents:

- Unauthorized access/Data breach
- Malware infections
- Phishing
- Other

No matter the incident, be sure to *document all investigation steps in the ticketing system!*

Important contact info

- Network Operations Center (616-555-4662), noc@kz.yoyodyne
- CISO (616-555-2476), ciso@kz.yoyodyne
- Help Desk (616-555-4357), help@kz.yoyodyne

Unauthorized access/Data breach

Once you have confirmed unauthorized access/data breach, contact the Network Operations Center (616-555-4662) and ask the on-call staff to disable network access to the wall jack (desktop) or network switch (data center).

Determine host/data criticality. The Configuration Management Database (CMDB) will be useful here, and will contain contact info for critical hosts or systems with sensitive data.

If the host/data is labeled critical or high in the CMDB:

- Contact the CISO (616-555-2476)
- Pull in additional resources if needed, e.g. assign someone to manage incident communication
- Capture RAM for possible forensic analysis. Help Desk (616-555-4357) has instructions and can help with this.
- Get a list of active processes on the host. Help Desk (616-555-4357) has instructions and can help with this.

Reset user credentials, including admin credentials and local credentials, on the host. Next, look for signs of lateral movement or data exfiltration. If there are signs of lateral movement, expand the scope of the investigation. If there are signs of data exfiltration, determine, if possible, the nature of the data. (This may not be possible until after the memory and disks have been analyzed forensically.)

Even if the unauthorized access appears to be focused on misuse of resources (e.g. cryptocurrency mining), keep in mind that could be a cover for a more hidden and persistent threat. The host should be rebuilt and restored from a known good image before being returned to the network.

Document all investigation steps in the ticketing system.

Malware infections

Once you have determined a host is infected:

- Contact the Network Operations Center (616-555-4662) and ask the on-call staff to disable network access to the wall jack (desktop) or network switch (data center).
- Reset the account passwords for any system users, including local and administrative accounts. Help Desk (616-555-4357) can assist with this.

Check network logs

- Document the path to infection, if known
- Check for other infected hosts (similar network traffic)
- Document any signs of lateral movement
- Document and signs of data exfiltration

Check the antimalware logs, if available. Was the threat detected and quarantined? Keep in mind that some malware packages download additional malware, and some may be detected while others are not. When in doubt, rebuild the system and restore data from a known good backup before restoring network access.

Document all investigation and follow-up steps in the ticketing system.

Phished Credentials

Phished credentials are typically observed in the following ways:

- User reported
- External notification or pastebin
- Suspicious account activity

Reset the user's account password and notify the user. Help Desk (616-555-4357) can help with user notification temporary password creation. Remind the user that if they use the same credentials for other 3rd-party accounts, those passwords should be changed as well. Encourage use of a password manager and unique credentials per account.

If user-reported, obtain a copy of the phishing email with full headers from the user. The help desk may be able to assist with this. Note the URL(s) in the phishing email.

- Check network activity for DNS lookups to the domain(s) in the message
    - If the domains do not have DNS lookups outside of known phishing activity, contact the Network Operations Center and request the domain be added to the internal DNS sinkhole
- Check network activity to IP addresses returned by any DNS lookups (above)
    - Note any traffic other than likely credential compromise

Check for unusual activity on the affected user accounts, including time-of-day, interesting locations, and multiple simultaneous logins. Note successful connections. If there are connections to any high security hosts, follow the data breach playbook.

Enroll the other in Yoyodyne's online training course, "Gone Phishin'" via the Training Portal.

Include details from the above steps in the ticketing system.

Other

There's always something that doesn't fit into a neat box!

In general:

- Remove network access via the on-call Network Operations Center (NOC) staff
- Reset account passwords
- Investigate unusual activity: lateral movement, data exfiltration
- Note any sensitive data that was compromised
- Document details of findings in the ticketing system