How To Respond When You've Been Breached:

15 Critical Steps Your Organization Must Take

Cyberattacks are varied, but for the professionals responsible for securing an organization's environment, any reported breach can be alarming. **Breaches are an unfortunate reality of business operations today, and most cybersecurity experts agree that it's not a matter of if, but when, an organization will face a breach.** As scary as this might seem, whether you're facing a data leak, a business email compromise (BEC), or a dreaded ransomware attack, there are steps that you should take to respond to and recover from an incident.

The National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (NIST SP800-61r2) provides a standardized approach for responding to cybersecurity incidents. While best utilized before a breach occurs, this framework also provides a helpful structure in active incidents. While the Incident Response lifecycle begins with the Preparation phase, if you're in an active breach, you're already at least in the Detection and Analysis phase.

Detection and Analysis

For the purposes of discussion, we'll assume that there's already a breach reported. **At this early stage of a breach, time is of the essence**, and while there are logical steps to follow, the incident response lead should delegate to have multiple response efforts pursued simultaneously. Documenting the entire incident response process is critical, and you may want to assign a scribe and designate a secure, out-of-band repository for documentation.

INGALLS INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452

Step 1. Triage Reported Breach

Triage begins with verifying whether the reported breach is valid. **While investigating false positives may seem like a waste of time, understanding why the report was generated can be useful for improving existing processes.** A false positive report can lead directly into the post-incident phase where the information learned should be documented and used to tune existing detection mechanisms, improve training, and to improve the organization's security posture.

Step 2. Analyze IoCs

Analysis should include researching whether IoCs have been sandboxed or reported in open source intelligence. While analyzing the IoCs, make efforts to preserve evidence. Depending on the breach type that you're facing, it may be necessary to preserve evidence for legal proceedings. For example, if there's reason to suspect an insider threat, you may want to preserve evidence on the suspect user and compromised systems for legal proceedings. **When making forensic images, it's advisable to start with most volatile evidence** (live memory) and working to least volatile evidence (hard drives).

Step 3. Scope the Investigation

It's important to establish an initial scope for the investigation based on the current level of understanding. It's better to over-scope the investigation rather than to under-scope the investigation. However, an overly-broad scope can result in expending resources containing and investigating unnecessary systems, and an overly-narrow scope can miss important evidence or result in the attacker maintaining or establishing persistence. The scope can be expanded as additional information becomes available throughout the investigation.

Step 4. Preserve Evidence

While evidence preservation is important, restoration of data and services is often a higher priority. In these cases, you may forego forensic images, but it's still important to preserve logs and sources of evidentiary value. In a breach, **logs are key to understanding how the breach occurred and whether remediation is complete**. Key log sources include event logs, VPN and remote access logs, database access and transaction logs, and antivirus logs.

Step 5. Internal Notifications

Once a breach has been verified, it's necessary to inform the appropriate internal parties. Key members of IT, management, legal, and public relations should be notified. A specific notification interval to provide updates to relevant parties should also be established. Some incidents require special considerations for communication channels. While email and ticketing systems may be a quick and obvious choice, some incidents require alternate solutions for internal communications. For example, **if there's reason to suspect an insider threat or a compromise of standard communication channels, out-of-band communications should be used.**

Step 6. Coordinate a Communication Plans

Once initial notifications have been made, legal counsel and public relations teams should begin to coordinate with executive leadership regarding how breach details will be communicated to stakeholders, as well as the process required to make any external notification requirements. The communication plans should include whether, when, and who will communicate details about the breach to those who may need to be notified. Within the United States, most states have individual reporting and notification requirements for any breaches involving Personally Identifiable Information (PII), and other nations may also have reporting and notification requirements, such as the General Data Protection Regulation (GDPR). It's important that the **individuals tasked with making communications decisions be fully informed of legal obligations**. Once Detection and Analysis has been completed, you may proceed to the Containment, Eradication, and Recovery phase.

INGALLS INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452

Containment, Eradication, and Recovery

Step 7. Deploy Endpoint Protection (EPP)

The goal of containment and eradication is to neutralize the source of the breach. This may require disconnecting compromised hosts to stop the spread of malware or to prevent the attacker from maintaining access, but **for any malware-related breach this should include deploying a next-generation EPP** to all systems scoped into the investigation.

While there are many solutions to choose from, including free versions, many of these will not adequately protect against modern malware and don't offer centralized control, reporting, or Endpoint Detection and Response (EDR) capabilities. Key features to consider when choosing EPP are whether the solution protects against malware, file-less malware residing in memory, and malicious scripts. Traditional EPP solutions rely on signatures for known malware, but these can miss novel or metamorphic/polymorphic malware which constantly evolve how they function or are compiled to evade signature-based detection. Next-generation EPP relies on machine-learning or dynamic analysis heuristics in addition to signatures. Another important feature to consider is a centralized reporting and whitelisting capability and EDR capabilities. These features allow responders to work from a console rather than investigating from each individual host, a frustrating and often futile task during a breach.

Step 8. Deploy Investigation Tools

While EPP helps to contain and eradicate malware, it's also important to deploy tools that provide investigation capabilities. A robust EDR solution, often included with Next-Generation EPP platforms, allows for the incident response team to detect, investigate, and respond to suspicious behavior. In addition to an advanced EPP and EDR solution, there are other investigative tools, such as Log Forwarders and Intrusion Detection Systems, that may help incident response efforts.

Step 9. Investigate the Breach

Following investigative tool deployment, **begin to establish an attack timeline and, if possible, determine the initial source of the breach**. This is a necessary and often overlooked portion of an incident response. Neglecting this step leaves open the possibility of persistence mechanisms and reinfection. Using the collected logs and investigative tools, work outwards from the initial breach detection, establish a timeline, and verify that no ongoing threats exist.

Step 10. Recovery

The goal of recovery is to restore your organization to normal operations. **Take necessary steps to protect from re-infection throughout the investigation.** This should include steps such as securing accounts, performing global password resets, implementing Multi-Factor Authentication (MFA) for email and remote access, and eliminating persistence mechanisms.

Post-Incident Activity

Step 11. Review the Incident and Lessons Learned

Once you've contained and eradicated the source and symptoms of the breach, **review the details of the breach and the lessons learned from the experience**.

Step 12. Make Process and Procedure Improvements

Based on the incident review, there should be definitive improvements to help prevent similar incidents. **Evaluate existing safeguards,** update policies and procedures to address gaps, and share final reports with stakeholders.

INGALLS INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111
WWW.IINFOSEC.COM
(888) 860-0452

Preparation

Step 13. Review, Update, Rehearse, and Socialize Documentation and Plans

During the preparation phase, your team should review, update, and rehearse policies and procedures. This includes preparatory actions such as tabletop exercises, penetration tests, and vulnerability assessments. This should be an ongoing process for the organization.

Step 14. Review Recent Breaches and Threat Intelligence

Use internal and external breaches to continually improve policies and procedures. In addition to lessons learned from breaches, **cybersecurity teams should stay informed of cybersecurity news and events**. Consider sources like Cybersecurity blogs, threat reports, Information Sharing and Analysis Center (ISAC) reports, and podcasts to remain informed.

Step 15. Employee Training

The final step in the preparation phase is to ensure all employees receive training. At a minimum, this should include **onboarding training, annual security awareness training, and regular security reminders**. Finally, employees should be trained and capable of performing their duties and know how to report suspected cybersecurity incidents.

Ingalls Information Security

Ingalls understands cybersecurity attacks and how to respond effectively. Since 2010, we've been in war rooms and boardrooms, investigating computer networks targeted and attacked by criminals and nation-state sponsored hackers. This experience gives us a powerful edge in preventing and responding to cyberattacks.

Ingalls helps businesses manage security risks and defend against cyberattacks. Contact us today to learn more. Our cybersecurity experts will be happy to assist you and answer any questions you may have.

INGALLS
INFORMATION SECURITY

Cyber Innovation Center (CIC)
6300 Texas Street, Ste. 240, Bossier City, LA 71111

WWW.IINFOSEC.COM
(888) 860-0452