How To Respond When You've Been Breached

15 Critical Steps Your Organization Must Take

Cyberattacks come in many forms, but for the IT and cybersecurity professionals responsible for securing an environment, these reports are all alarming. Cybersecurity incidents are an unfortunate reality of operating a business today, and most cybersecurity experts agree that it's not a matter of if but when an organization will face a data breach. Global cybercrime costs are expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. So, is your organization prepared for an attack?

Here's a scenario that is all too familiar for many organizations. An employee calls the help desk saying that they can't access their files, and there's a note on the screen saying to email the attacker to send bitcoin to get the files decrypted. The CEO is receiving emails from their contacts asking whether they sent an email with a link to an "encrypted" message (hint: they didn't) asking recipients to log in to access it. Customers are calling saying that they can't access the company website. A journalist contacts the company's lawyer asking whether the company is aware that sensitive customer data is publicly exposed in a public file share.

As scary as this scenario might seem, at this moment, whether you're facing a data exposure incident, a business email compromise, or a dreaded ransomware attack, there are steps you can take to help your organization respond and, hopefully, recover from this incident.

The National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide publication (NIST SP800-61r2) provides a standardized approach for managing and responding to cybersecurity incidents. While this framework is best utilized in developing preventative policies and procedures, it is also very helpful in the midst of an incident. At a very high level, this framework provides the following lifecycle approach to responding to incidents:

While the lifecycle begins with the preparation phase, if you're in the midst of a breach, you're essentially already at least in the detection and analysis phase. As challenging as this experience may be, the good news is that the lessons learned from your current breach are not lost and can directly inform and improve your existing processes moving forward.

INGALLS
INFORMATION SECURITY

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

WWW.IINFOSEC.COM
(888) 860-0452

Detection and Analysis

For the purposes of this article, we'll assume that there's already some sort of breach reported. The Detection and Analysis phase and the Containment, Eradication, and Recovery phases will go hand in hand. As you investigate and analyze indicators of compromise, you will begin to work on containing and eradicating that threat, and as you work on containing and eradicating threats, newly discovered indicators of compromise may be detected and require additional analysis and investigation. At this early stage of an incident, time is of the essence, and while there are logical steps to follow, these steps can chronologically be pursued simultaneously. Where possible, the incident response lead needs to delegate and have multiple response efforts pursued in parallel. Further, it will be important to document the entire incident response process, and you may want to assign a scribe and designate a secure, out-of-band repository for investigation documentation.

Step 1. Triage Breach Detection and/or Notification

The initial step is to triage the reported breach to verify whether the report is valid. While false positives may seem like a waste of time, taking the time to understand why the report was generated can be useful for improving existing detection and reporting processes. If the report is not an actual incident, there's nothing to contain, eradicate, and recover from, so the breach can lead directly into the post-incident phase where the information learned should be documented and used to tune existing detection mechanisms, improve training for users, and to improve the security posture of the organization moving forward.

Step 2. Analyze Indicators of Compromise

Analysis should include researching whether the suspected malware, if known, has been sandboxed or included in open source intelligence sources such as threat data reports or public sandboxes. While analyzing the indicators of compromise, careful consideration should be made to preserving important sources of evidence. Depending on the specific breach type that you're facing, it may be necessary to preserve evidence for legal proceedings. For example,if there is reason to suspect an insider threat, you may want to preserve evidence on suspect and/or compromised systems for future legal proceedings. When making forensic images, it is generally advisable to start with most volatile evidence (live memory acquisition) and work to least volatile evidence (forensic image of hard drives).

Step 3. Scope the Investigation

While it can be challenging to do so early in an incident response, it is important to establish an initial scope for the investigation based on the current level of understanding and initial triage and analysis. It's generally better to over-scope the investigation rather than to under-scope the investigation. However, an overly-broad scope can result in expending time and resources containing and investigating unnecessary systems, and an overly-narrow scope can miss important evidence or result in the attacker maintaining or establishing persistence within the environment. As additional information and detections become available throughout the investigation, it may become necessary to increase the scope to additional systems or networks.

Step 4. Preserve Evidence

While evidence preservation is important, the priority in many breaches is restoration of data and/or services. In this case, there may be less of a need for forensic acquisition and images, but it is still very important to preserve logs and sources of evidentiary value such as logs. In an incident response, logs are often the key to understanding how the breach occurred and whether containment and eradication has been achieved. Key log sources to consider include domain controller logs, workstation logs, VPN and remote access logs, Remote Monitoring and Management logs, database access and transaction logs, and antivirus logs.

Step 5. Internal Notifications

Once your IT or cybersecurity staff have verified that a breach has occurred, it's necessary to inform the appropriate internal parties that a breach has occurred. Key members of IT (especially those with incident response duties), management, legal, and public relations should be notified. A specific notification interval for each of the relevant parties should be established. Some incidents require special considerations for communication channels. While email and ticketing systems may seem like a quick, obvious communication channel, some incidents require special consideration for how notifications, updates, and internal communications take place. For example, if there's reason to suspect an inside actor or that established communication channels have been compromised, an out-of-band communication channel should be used.

Step 6. Coordinate a Communication Plans

Once initial notifications have been made, your legal counsel and public relations teams should begin to coordinate with executive leadership concerning how to communicate details about the breach as well as any external notification requirements. The communication plans should include who, whether, and when to communicate details about the breach to, including employees, customers/clients, law enforcement, and the media. Within the United States, most states have individual reporting and notification requirements, such as the California Consumer Privacy Act (CCPA), for any breaches involving Personally Identifiable Information (PII), and other nations may also have reporting and notification, such as the European Union's General Data Protection Regulation (GDPR). It is important that the individuals tasked with making decisions about communications be fully informed of legal obligations as well as the expectations of organizational leadership and stakeholders.

Once Detection and Analysis has been completed, you may proceed to the Containment, Eradication, and Recovery phase. Keep in mind that as you progress through the Incident Response Lifecycle, new information, detections, or reports may require you to return to the Detection and Analysis phase.

Containment, Eradication, and Recovery

Step 7. Deploy Endpoint Protection (EPP)

During containment and eradication, the incident response team will work to neutralize the source of the breach. This may require disconnecting compromised hosts or subnets to stop the spread of malware or to prevent the attacker from maintaining access to compromised hosts, 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 antivirus solutions to choose from, including free versions, most of these will not provide protection from many modern types of malware and do not offer centralized control, reporting, or Endpoint Detection and Response (EDR) capabilities.

Key features to consider when choosing an EPP platform are whether the platform provides protection against malicious files (including novel, metamorphic, or polymorphic malware), file-less malware residing entirely in memory (also known as "living off the land"), malicious scripts (Active Scripts, Macros, and PowerShell Scripts). Traditional EPP solutions rely on signatures for known malware, but these notoriously miss new, metamorphic, or polymorphic malware. Metamorphic and polymorphic malware includes malware that is constantly evolving how it functions or how it is compiled to evade signature-based detection. Next-generation EPP relies on advanced heuristics such as machine-learning and dynamic analysis in addition to signature-based detections. Another important feature to consider is a centralized reporting and whitelisting capability and Endpoint Detection and Response (EDR) capabilities. Centralized reporting and whitelisting allow investigators to address quarantines and whitelisting from a single console rather than having to do so at each individual host, a frustrating and often futile task in the midst of a breach.

Step 8. Deploy Investigation Tools

While the initial purpose of advanced EPP is to contain and eradicate malware within the breached environment, it's also important to deploy tools that provide investigation capabilities. A robust Endpoint Detection and Response (EDR) solution, often included with Next-Generation EPP platforms, allows for the incident response team to detect, investigate, and respond to suspicious activities within the investigative scope. In addition to an advanced EPP and EDR solution, there are other investigative tools that may prove to be invaluable to your incident response efforts. Some additional tools to consider deploying are Log Forwarding Agents and Intrusion Detection Systems.

Step 9. Investigate the Breach

Now that you've got your breached environment contained, known malware and attacker access eradicated, and your investigation tools in place, it's time to establish the attack timeline and to determine the initial source of the breach if at all possible. This is a necessary and, unfortunately, often overlooked portion of an incident response. Neglecting this step of your incident response efforts leaves open the possibility of persistence mechanisms and sources of re-infection. Using the collected logs and investigative tools deployed throughout the investigation, begin to work outwards from the initial breach detection or notification, establish a known timeline, and verify that no ongoing threats exist. As additional information, indicators of compromise, and findings become available it may be necessary to move back to the detection and analysis phase, to adjust your scope, or to deploy additional investigation tools. Following the NIST Incident Response Lifecycle allows you to systematically begin working towards recovery.

Step 10. Recovery

The goal of recovery is to remediate your environment and to restore your organization to normal operations (hopefully with an improved security posture!). As you detect, analyze, contain, and eradicate throughout your investigation, take necessary steps to protect your organization from re-infection. Generally speaking, this should include steps such as securing compromised accounts, performing global password resets, implementing Multi-Factor Authentication (MFA) for email and remote access, and eliminating persistence mechanisms (or re-imaging potentially compromised hosts).

Post-Incident Activity

Step 11. Review the Incident and Lessons Learned

Once you've established containment and eradicated the source and symptoms of the breach, you have survived the most stressful and challenging portion of your incident response efforts, but this isn't the end of the road. Now is the time to review the details of the breach and the lessons learned from the entire experience.

Step 12. Make Process and Procedure Improvements

If you've reached this point in the incident response process, there should be some definitive improvements to help prevent the organization from experiencing similar incidents moving forward. Based on your insight from your review of the incident, evaluate your existing safeguards, and begin to update or to develop and implement policies and procedures to address any gaps in your existing preparations, detection and analysis, and/or containment, eradication, and recovery efforts. Once this has been accomplished, create, file, and communicate any final reports to stakeholders.

Congratulations! You've reached the end of the incident. Once the breach has ended (and you've had a moment to catch your breath), it's time to continue with the improvements this experience has afforded your organization.

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, internal/external penetration tests, and internal/external vulnerability assessments. This shouldn't be a one-time event. Rather, it should be a regular, ongoing process for the organization. Once documentation has been updated, and on a regular basis, ensure all stakeholders can access and understand their roles in those documents.

Step 14. Review Recent Breaches and Threat Intelligence

As part of your organization's continual process improvements, it's important to use both internal and external breaches to inform the organization's policies and procedures. In addition to lessons learned from any breach the organization has experienced, cybersecurity and IT teams should stay informed of cybersecurity news and events. These teams should consider sources such as Cybersecurity newsletters, blogs, threat data reports, Information Sharing and Analysis Center (ISAC) reports, and podcasts to keep informed of threats that the organization faces.

Step 15. Employee Training

The final step in the preparation phase of the Incident Response Lifecycle is to ensure all employees receive appropriate training. At a minimum, this should include onboarding training for new hires, annual security awareness training for the organization's entire workforce, and regular security reminders and updates. Further, employees should be trained and capable of performing their duties and roles regarding security roles and how to report any suspected cybersecurity incidents.

Ingalls Information Security

Ingalls Information Security 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 large and small manage security risks and defend against cyberattacks. If you'd like to learn more please contact us here. One of our cybersecurity experts will be more than happy to assist you and answer any questions you may have.

About the Author

Cyrus Robinson, CISSP, MCSE, MCITP, CEH, CHFI, Sec+

Mr. Robinson is a skilled Information Security professional with experience working with diversified technologies and environments. Mr. Robinson's professional IT career began as an electronic forensics engineer as an active duty Airman with primary responsibilities with testing and evaluating digital forensic software, policies, and procedures. In this capacity, he worked alongside federal investigators and various DoD, CIA, FBI, NSA, and NIST employees. Following his active duty role with the USAF, Mr. Robinson went on to work in change management and system administration as a DoD Contractor. Mr. Robinson also has extensive experience in the roles of Information Security Officer and IT Director for a large medical group which contribute to his knowledge with security risk assessments, HIPAA compliance, and drafting and implementing corporate IT security and business continuity policies. Mr. Robinson holds various industry standard certifications and a Masters of Science in Information Security and Assurance.

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

WWW.IINFOSEC.COM
(888) 860-0452