Oh #@$%! I've Been Breached:

WHAT TO DO NEXT

The importance of data security is no secret. So you've thought ahead and taken steps to safeguard sensitive information. But then it happens—you discover a breach. It's no time to panic.

Sit down, take a deep breath and follow the steps outlined in your incident response plan (IRP). Because you thought ahead, you drew up the plan with the guidance of experienced experts and now's the time to put it to use. Start by notifying both operations professionals and business stakeholders at your company. Then, follow the IRP guidelines to preserve artifacts of the breach, stop the "bleeding" or exfiltration of data, discontinue applications as necessary and, finally, return to normal operations.

Table of Contents

Get out your IRP

Your IRP is a complete roadmap that includes standard measures that are adapted with the help of your security provider to the unique needs of your company. Since a breach involves a number of legal issues, your IRP should include specific steps that must be followed so that your organization will be in a position to withstand any legal actions that might be taken with regard to lost or stolen data. Because every company is different, the legal issues relating to your organization and your industry will also be different. For example, companies that are in the financial services or e-commerce fields must meet the requirements for PCI compliance; healthcare organizations, meanwhile, must comply with HIPAA guidelines.

Assemble your team

The members of your incident response team are spelled out in your IRP, so there's no need to scramble to recruit people. The team members may come from either inside or outside your organization. And because you've lined up the team ahead of time, each member understands his or her responsibilities and the importance of collaboration with other team members. The team should include:

- Security experts, including the director of your Security Operations Center
- IT managers who understand the data and applications
- Marketing officers, to assure your brand does not suffer
- Lawyers who are knowledgeable in matters relating to breaches
- Business stakeholders
- Contractors or third-party providers
- Compliance officers

Preserve artifacts

Since there will be a post-breach audit, it is essential to preserve artifacts relating to the event for evidence and attribution. Because much of the data that must be collected is time-sensitive and cannot be reproduced, it is essential to collect and preserve it promptly. Key artifacts include:

- Time stamps for critical files
- Network connections
- Current logins
- Process lists
- Memory dumps
- Packet captures

Artifacts such as these help to tell the story of the breach. For example, time stamps indicate when files are accessed and by whom. The activity of a systems administrator who regularly works during daylight hours but is accessing files in the middle of the night should be investigated. Similarly, comparing the firewall policies that were in place at the time of a breach to what they should have been can uncover an administrative failure or a suspicious action.

A close look at user accounts can be telling as well. Duplicate or old accounts that have been reactivated can point to the source of a breach. Weak passwords or elevated privileges can also be strong indicators of poor practice or dubious activity. Examining network traffic flows and CPU utilization is also worthwhile. A CPU at 90% utilization or a mail server processing unusually large inbound traffic may indicate a brute-force attack.

Since procedures must be followed carefully at this stage, experienced incident response professionals should take part. Each incident requires specific actions relating to each company and each industry. PCI and HIPAA requirements are very specific and quite different. For example, PCI requires that consumers be notified quickly, since a criminal might begin using a stolen credit card right away. Under HIPAA, the theft usually involves personally identifiable information (PII) such as a Social Security number that could be used at some point in the future for identity theft.

Seasoned experts can help address the needs of each company so that time is not wasted preserving artifacts that are not relevant. Experts are also knowledgeable with regard to the artifacts that must be preserved for a criminal prosecution. This phase is complete when your team has saved sufficient evidence to prove that a breach occurred, or when there is no more evidence to gather.

Protected by Armor

Armor's secure cloud can help you protect highly sensitive and regulated data from data breaches, ransomware and DDoS attacks. Armor technologies are specifically geared to enable HIPAA and PCI compliance.

Armor Complete provides secure managed hosting. By placing your sensitive data in the Armor Complete virtual private cloud, you gain advanced threat intelligence, compliance that exceeds HIPAA and PCI requirements, dwell times that are 100 times shorter than the industry average and 24/7 support.

Armor Anywhere provides secure infrastructure on Amazon Web Services or Microsoft Azure public clouds. Armor Anywhere

Stop the bleeding

In order to stop the exfiltration of data, it may be necessary to shut down one or more applications. Whether or not you take this action depends on how the breach occurred and the extent of remedial action required. When you believe you have stopped the exfiltration of data, continue monitoring to assure that your efforts were completely successful before returning to normal operations. If exfiltration continues, you will need to repeat your remedial measures. You must also close the door that the threat actors used to gain access. Once you have shut down this vulnerability, once again, monitor for continued exfiltration and repeat this step if necessary.

Return to normal operations

Only when all exfiltration has ceased and there is no evidence of continued activity should you return to normal operations. Several processes are important as normal operations are resumed. These include patching, following best practices, re-imaging and manual cleanup.

Because out-of-date code often contains old yet dangerous vulnerabilities, administrators should install all updates so applications are running at the latest version. Re-imaging endpoints will also get rid of old code and residual weaknesses. Manual steps include cleaning up accounts by matching account identities with permissions, and enforcing password change and reuse policies.

Lessons learned

When the audit is complete, the team should convene to recap the lessons learned from the breach and add to your IRP a list of tasks and processes designed to prevent a similar breach in the future. Statistics on repeat successful attacks (if available) can provide information that is useful in this process. Your security provider should be an active participant.

To apply lessons learned, you should continue to foster a culture of collaboration between members of your IRP team and the company as a whole. On an ongoing basis, it is critical for IT to communicate the

Protected by Armor
cont.

managed security as a service includes malware protection, patch monitoring, log and event management, external vulnerability scans, file integrity monitoring and 24/7 security. It also includes Armor Management Portal, a mobile-friendly window into your security environment.

SEE WHICH SOLUTION IS RIGHT FOR YOU?

armor.com/armor-advisor

value of security measures to business leaders, not in technical terms but in terms of dollars-and-cents risk to the organization.

Conclusion

There is nothing good about a data breach. But should a breach occur, there is a best way to handle it. Putting a comprehensive IRP in place with the aid of trained experts is the first step. Then, it's important to follow the plan closely to minimize damage, respond to legal demands and put your company in a position to return to normal operations quickly.

Working with trusted incident response professionals can speed your reaction and help you to apply lessons learned so that your company can avoid a similar breach in the future.