Guide

AVERTIUM®

8 STEPS TO TAKE IF YOU'VE BEEN BREACHED

Table of Contents

INTRODUCTION

Eventually becoming the victim of a cyberattack may be inevitable, and climbing your way out of the hole that a breach creates can be treacherous. Advance preparation must include being ready to respond. These eight steps help guide a rigorous response that can limit the losses your business could suffer to intellectual property, finances, and reputation after a cyberattack.

With the prevalence, severity, and sophistication of cybersecurity attacks growing by the day, businesses of all types and sizes are scrambling to protect themselves. Losses can be devastating; the average cost of a data breach now approaches $10 million.

This makes detection, mitigation, and response critical to reducing its impact. When it comes to cybersecurity, cooler heads prevail, which means that a formal, methodical approach to handling security breaches is vital. The steps outlined here provide a guide to get you started on thinking about what's needed in the event your network is hacked for a more rigorous and relevant response.

Step 1

DETERMINE THE SCOPE OF THE ATTACK

Organizations often rapidly respond to attacks by means of immediate—and often unplanned—responses. This type of action typically leads to more damage occurring than with a slower, better-planned response. For instance, powering off a machine infected with ransomware or malware can often be more detrimental than leaving it running, but disconnected from the internet.

When a breach is detected, security responders must take methodical steps to understand its extent. They must identify the...

1. Specific machines, applications, and data impacted by the incident
2. Effects on each
3. And remaining threat outlook as part of the basis for tailoring a response

In particular, teams need to establish whether the incident has impacted critical business processes and data. That investigation helps illuminate the true severity of the breach, which can help guide specialized measures such as disaster recovery procedures or mandated reporting to regulatory entities.

Step 2

CONTAIN THE THREAT

Armed with an understanding of the extent of the compromise and damage, teams should isolate the systems, applications, or services that have been impacted by the attack from the internet as well as from the rest of the network. These measures help prevent exfiltration of data or communication with the attacker's command and control apparatus, as well as lateral spread of the breach inside the network.

Additional measures may also be needed, based on the specific nature of the attack. For example, if the attack was borne into the network via email, response teams may search for additional copies of the same message or notify other users of the threat.

Step 3

NEUTRALIZE THE BREACH

Response teams should use digital forensics to systematically identify all effects on IT resources that were caused by the incident. Detailed threat analysis based on that information should generate a tailored response plan to halt additional damage to affected resources as quickly as possible. This should include elements such as disabling or removing malware, user accounts, and services related to the attack, as well as backing out unauthorized configuration changes.

This work also includes identifying all sensitive data that may have been improperly accessed, transferred, or destroyed as a result of the breach. Clearly assessing impact and damage is an important means of risk mitigation in its own right, as well as being a prerequisite for reporting to regulatory agencies, data owners, and others.

Step 4

REMEDIATE THE DAMAGE

Once a breach has been quarantined, its effects on systems, applications, and data must be remediated while reducing risk of further attacks. This includes repairing resources left in a degraded or non-operational state, as well as restoring systems to a known, trusted status.

Measures may include:

- Returning systems to factory-reset condition before rebuilding them to operational status
- Utilizing security hardened images/configurations
- Restoring them using certified backups and datasets

After remediation, affected parts of the environment must be scanned and validated to ensure they are ready to be put back into service.

Step 5

DOCUMENT THE INCIDENT

Reporting on security incidents is a critical part of the response. Comprehensive documentation should be produced that includes the entire process of detecting and responding to the attack, including the...

1. Outcomes of forensic analysis
2. Measures taken to mitigate the breach
3. Recommendations for the future

The documentation produced as part of this step should be operationalized to improve security posture and resiliency. It will also need to be submitted to interested parties that include...

- Senior management
- Partners and affiliates
- Customers
- Regulators as required by any applicable laws, regulations or compliance requirements

Step 6

CLOSE THE HOLES

Cyber attackers continue to become more advanced and persistent, but businesses often fail to take even simple precautions. For example, 60% of breaches are linked to vulnerabilities for which a patch was available but hadn't been applied. That's why it's important to start with the basics: ***Close the holes and apply the updates that create vulnerabilities, then bring all hardware and software up to date with the latest patches.***

Organizations should identify the requirements for patch timeliness in a matrix based on the severity of the vulnerability the patch is designed to fix. High or critical severity vulnerabilities must be patched quickly. For highly risk-averse organizations, we recommend the following:

- Critical Severity – 72 hours
- High Severity – 7 days
- Medium Severity – 30 days
- Low Severity – 60 days

With basic hygiene out of the way, it's critical to carry out a full threat assessment and gap analysis of the security measures already in place, as well as determine the full scope of changes needed to protect cyber health going forward.

Step 7

BE VIGILANT

Moving forward, detecting security incidents as early as possible is a dramatic advantage. Starting countermeasures earlier helps limit the extent of a breach before it can move laterally within the organization, reducing the resources that are exposed and the effort needed to remediate them. Earlier interventions also help mitigate the risk of data being exfiltrated from the network.

To bulk up your program, tools and processes must be put in place and maintained to detect indicators of compromise. These may be as concrete as malware or unauthorized access to resources, but in a world of blended, persistent, and insider threats, the scope of what to watch for also includes subtleties such as anomalous user behavior, unusual data movements, and log irregularities.

Step 8

CALL IN THE EXPERTS

It’s no secret that security and technology teams are stretched thin, with the demands of the job growing constantly and the majority of organizations reporting a problematic shortage of cybersecurity skills. Bringing in subject matter expertise in the form of external resources can overcome such shortages, as well as set up a relationship you can lean on in the future, so you know where to turn in a crisis.

Avertium provides a comprehensive range of consulting, prevention, mitigation, and response services to midsize and enterprise customers. We can help you plan security posture improvement, harden your network, watch over it to help keep it safe, and respond rapidly to any issues that do arise to minimize impact and protect business continuity.

CONCLUSION

Protecting your business is a process, not a destination or check box. It involves constantly assessing threats and vulnerabilities, putting measures in place to protect against them. It also requires responding to incidents in a way that minimizes damage, reveals root cause, and improves security knowledge to make the company safer in the future.

Adapt. Attack. Evolve.

Looking for your next read? We think you might also be interested in:

"2023 Cybersecurity Landscape: 8 Lessons for Cybersecurity Professionals"

ABOUT AVERTIUM

Avertium is the security partner that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom. That's why over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. **Show no weakness.®**

CONNECT WITH US

Cyber Fusion Centers of Excellence
Arizona • Colorado • Tennessee

Contact Us | www.Avertium.com

This publication contains general information only and Avertium is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. A**vertium shall not be responsible for any loss sustained by any person who relies on this publication.**