Data Security Breach

Putting a Response Plan in Place

The instant your organization suspects its data security might be compromised, it needs to swing into action—not just to ensure regulatory compliance, but to limit the scope of the damage a breach might cause. The faster you can act, the less dire the consequences. A recent report from the Ponemon Institute[1] shows that while the average per-record cost of a data breach increased by 12 percent over the past year, an organization's speed in identifying and containing a breach was directly correlated to its ability to minimize the financial impact. And the fastest way to respond to a data security breach is to have a response plan already in place.

XANTRION
CYBERSECURITY • IT SUPPORT

The response plan should be well-defined and concise, with standard operating procedures to follow in the crucial first 24 hours after a breach is suspected or detected.

Response Planning

What should an effective data security breach response plan look like?

The plan should be well-defined and concise, with standard operating procedures to follow in the crucial first 24 hours after a breach is suspected or detected. It should also be rehearsed, like a fire drill, until all your employees not only know the procedures, but respond almost instinctively to an alert.

Creating a Plan

The following general guidelines can be modified based on the severity and scale of a given incident.

Assign roles and responsibilities.

1. Report the suspected breach to the designated security breach response manager.
2. Security breach response manager assigns a lead incident response investigator and works with other managers to designate additional members of the incident response team, which may include any or all of the following:
    - Technical experts
    - Legal counsel
    - Members of the management team
    - Insurance agencies
    - Law enforcement agencies
    - Communications/public relations

Determine the scope of the incident.

1. What information was lost or suspected compromised?
2. Was the lost information encrypted?
3. Who had access to this data?
4. Are there backups for any damaged and/or missing information?

Secure systems to limit further impact.

1. Inspect servers for:
    - Unusual processes
    - Unusual network connections
    - Large files or folders on servers
    - Systems broadcasting to or scanning the network
    - Events: Failed logon
    - Unusual services running
    - Unusual programs in startup or scheduled
    - Active guest accounts, unusual local accounts, local admin accounts
2. Change all user passwords and all service account passwords.
3. Change passwords on all hardware (firewalls, routers).
4. Audit all accounts
    - Are all accounts real?
    - Have any been created recently?

5. Audit all group memberships to ensure users are only in groups they belong to.
6. Change the local admin password on all computers with a login script if possible or by hand if necessary.
7. Ensure antivirus software is installed and running on all computers.
8. Audit for spyware on all servers and schedule a re-install for any server that cannot be easily cleaned. Perform basic firewall penetration testing.
9. Review the firewall configuration and ensure that all passthroughs are required and secure.
10. Validate basic Active Directory policies including patch deployment, password complexity, and auditing.
11. Review installed software report for all machines.
12. Monitor network for unusual traffic patterns.

Preserve evidence.

1. Consider creating server images if a forensic investigation will ensue.
2. Collect server and firewall logs.
3. Prepare a list of possible disgruntled current/former employees or other suspects.
4. Create a written record of observations.

Send appropriate notifications.

1. As needed, engage legal counsel to review obligations for breach notification to:
   - Regulatory agencies
   - Individuals whose information may have been compromised
2. If needed, develop a notification and remediation plan. Consider working with a Breach Response firm if a significant effort is required.
3. Include insurance representatives in planning to ensure best possible cost coverage.

Review the incident.

1. Incident response team leader prepares an incident response report containing:
   - Incident summary
   - Date of incident
   - Duration and impact of incident
   - Systems and information lost or compromised
   - Root causes, to the extent they can be determined
   - Actions taken
   - Recommendations for changes in security practices
2. Review response report with incident response team for agreement on follow-up action items.
   - Changes to security practices
   - Need for public relations efforts

Rehearse your plan, like a fire drill, until all your employees not only know the procedures, but respond almost instinctively to an alert.

Putting Best Practices into Action

Although it's impossible to guarantee immunity from data security breaches, implementing proven policies and best practices can ensure that your business is able to respond quickly and appropriately if and when one happens. Xantrion relies on these tested approaches to develop and implement data security breach response plans, not just for our clients, but for ourselves. Our IT experts will draw on their successful experiences to help you create a response plan that takes your organization's individual risks and needs into account. Call us at (510) 272-4701 to get started.

References

[1] http://www.prnewswire.com/news-releases/ponemon-institutes-2015-global-cost-of-data-breach-study-reveals-average-cost-of-data-breach-reaches-record-levels-300089057.html

XANTRION
CYBERSECURITY • IT SUPPORT

Xantrion
651 20th Street
Oakland, CA 94612

xantrion.com

(510) 272-4701