Cybersecurity Recovery Checklist

Cybersecurity Recovery Checklist

- ❑ Disconnect the network from the internet
- ❑ Notify employees/customers of the breach
- ❑ Remove any additions to Servers/Computers
  - ❑ Active Directory
  - ❑ Firewall Users/VPN
  - ❑ Group Policies
  - ❑ Software
- ❑ Update passwords
  - ❑ Email
  - ❑ Domain
  - ❑ Accounts
    - ❑ Banking
    - ❑ Company-specific platforms
      - ❑ _____
      - ❑ _____
      - ❑ _____
      - ❑ _____
      - ❑ _____
      - ❑ _____
- ❑ Find the point of Entry
- ❑ Install patches to fix the entry point
- ❑ Wipe user computers
- ❑ Recover files from the last backup prior to the attack
- ❑ Connect the network back to the internet

Disconnecting Your Network

Disconnecting your network from the internet is **crucial** to your recovery. Without internet access, the attackers can't do any more damage to your network.

***How To*:** We want to start at the source to disconnect your network from the internet. The quickest way to disconnect is to simply unplug both your modem (ISP Device), and your firewall.

Notifying Employees/Customers

Notifying your employees and customers is another crucial step toward your recovery. You can't change what has already happened, but you can minimize your chances of it happening again by alerting everyone to look for suspicious activity around their accounts.

Removing Unwanted Items

Disclaimer: Do not take this step lightly! All your recovery efforts can quickly be undone if these checks are not thorough. Leaving any account or application on your network can easily allow the attackers access to your network again.

How To (Server): Start with your Active Directory accounts and security groups, and one by one, update the passwords for them and ensure there are no newly added accounts that the attackers used.

How To (Firewall): Log into your firewall, and first things first, update your password. Next, just like on the server accounts, go through all of the user accounts, and ensure no new accounts have been added. Once you have confirmed there are no additional user accounts, take some time to go through all of your routing policies, and look for any additional tunnels that may have been created.

Note: If no additional VPN accounts were created, checking the logs to see if any user connected to the VPN may indicate a compromised VPN account.

Updating Passwords

You should have already started to update some of the passwords that are used throughout your network. In this step, we want to update **ALL** of the passwords.

How To*:** To get started, start with any remaining domain accounts, and then move to every email account used within the company. ***Disclaimer: If 2FA is not already enabled, this would be an ideal time to enforce it throughout your organization. In addition, looking for any additional rules created in each inbox may indicate an entry point. Finally, take some time to go through all of the other accounts your organization uses. Just like your email, updating the passwords, and enabling 2FA is ideal.

Finding the Point of Entry

Finding the point of entry sounds like a daunting task. However, by this stage, you should have a pretty good idea as to how the attackers got in.

Disclaimer: If no point of entry has been found, moving forward in the recovery steps may result in a repeat attack.

Installing Patches

Hopefully, by this point, you have found the point of entry, and are ready to get it patched so the attacker's access is totally shut off after getting your company back online.

Ex. If you found an email was compromised, your patch is changing the password, and enabling 2FA for the account.

Ex. If you found that the firewall was compromised, removing any additions to the firewall will delete their access.

Disclaimer: There may be multiple forms of entry. If one entry point is found, each step to follow should be completed with the same level of thoroughness.

Wiping Computers

Wiping all of the computers may not be necessary. However, by wiping the machines and installing a fresh image of Windows can drastically decrease your chances of something slipping through unnoticed.

***How To*:** Create a Boot Disk with the latest version of Windows and on startup launch the installation wizard. During the setup, you can delete the old partitions, wiping any data that is on the drive(s).

Restoring Files

How you restore your files will be dependent on how your files are backed up. The length of time it takes to restore your files is also dependent on the style of backup, the number of files, and the overall effectiveness of your environment.

Getting Back Online

Finally, all your hard work is about to pay off. By now, we should have updated every password used within the company, enabled security measures, found their point of entry, refreshed everyone's workstation, and hopefully started taking measures to train employees on the newest cybersecurity threats.

At this stage, if all boxes are checked, you can plug your router and modem back in, and get everyone connected to the internet!

Disclaimer: Cyber threats become more and more advanced every single day. This checklist may not be totally conclusive for your business. If you would like additional assistance with your recovery process, contact Omnis Technologies at techsupport@omnistech.com or call us at 814-362-4359.