GLOBAL CYBER ALLIANCE

globalcyberalliance.org
New York City | London | Brussels

GCA Cybersecurity Toolkit Backgrounder: Update Your Defenses Toolbox

GCA Cybersecurity Toolkit™ For Small Business

Cyber criminals are constantly looking for ways to gain access to systems and data. One way to achieve this is to find a weakness in a configuration or in a developer's code which could be replicated across the entire user base and exploited to the cyber criminal's advantage.

Manufacturers and software developers regularly release updates for their operating systems and applications to address newly discovered weaknesses or vulnerabilities.

- These fixes are usually referred to as patches, and the process is known as patching.

It is really important that patches are applied quickly, and wherever possible automatically, to avoid them being used in a cyberattack.

- The WannaCry ransomware attack in May 2017 took advantage of a flaw identified in the Windows Operating System and had devastating global consequences.
    - It did not target specific sectors but rather the type of devices in use.
        - It impacted individuals.
        - It impacted small, medium, and large organizations.
        - It impacted police, health, transport, telecoms, banking services, etc.
    - It is estimated that within 24 hours over 230,000 computer systems were affected across 150 countries, with billions of dollars in losses.
- Patches had been released by Microsoft in March 2017 for all supported devices.
    - Those that had not applied the patch before the attack started were at risk.
    - Those that had applied the patch (manually or automatically) were not at risk.
    - Those using Windows XP were at risk because Windows XP was no longer being updated ("End of Life" - although a patch was quickly developed because of the severity of WannaCry).

End of Life

All devices and operating systems have an "End of Life" date after which they are no longer maintained; support ceases, no further patches are released, and they become an immediate and ongoing risk for newly discovered vulnerabilities. This can also happen if a manufacturer ceases trading and no one takes on the development of its product set.

- Windows 7 went End of Life in January 2020.
- Windows XP went End of Life in April 2014.
- *Unsupported systems should be removed from the network, upgraded, or replaced.*

IoT Devices

The growth of Internet of Things (IoT) devices, particularly in the consumer product marketplace where purchasing decisions are often based on price, ease of use, functionality, and less on security, can create potential access points for attackers. Many have limited security features and no patching capability, so if a flaw did exist, it would leave your network open to attack until the device is physically removed or proper mitigation methods are implemented. There would be minimal preventative action, if any, that could be taken to remove this risk.

Old applications that are no longer in use and legacy equipment (older equipment that has been "adapted" for use on a network or over the Internet) are best removed. These should ideally have been identified and removed/updated while completing the Know What You Have toolbox, ensuring that minimum levels of access for "business as usual" functionality are adopted.

In summary:

- Patches/updates include important security fixes to protect against newly discovered vulnerabilities and should be implemented immediately, ideally via an auto-update option if this exists.
  - *Failure to patch in a timely manner will put your computer systems – and, therefore, your organization - at risk.*
- Remove devices that cannot be patched (i.e., many consumer IoT devices) and any devices or applications that are no longer supported – these may otherwise be putting your organization at risk.
  - *If the device is necessary for business, then isolate the device as best as possible and prevent any level of Internet access and access to other devices.*
- Ensure minimum levels of access for business as usual functionality and remove access immediately for employees who have left the organization or third-party companies who no longer provide services (or customers).
- Ensure all software and systems are up to date – patched to the latest revision and reviewed regularly.

Use the tools in the Update Your Defenses Toolbox to help you. Have a policy in place that ensures regular reviews of your inventory, supply chain, and updates.

https://gcatoolkit.org/smallbusiness/update-your-defenses/