Tohono O'odham Nation

Department of Information & Technology

CYBERSECURITY AWARENESS MONTH 2022

Patch Management

Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

Patch Management

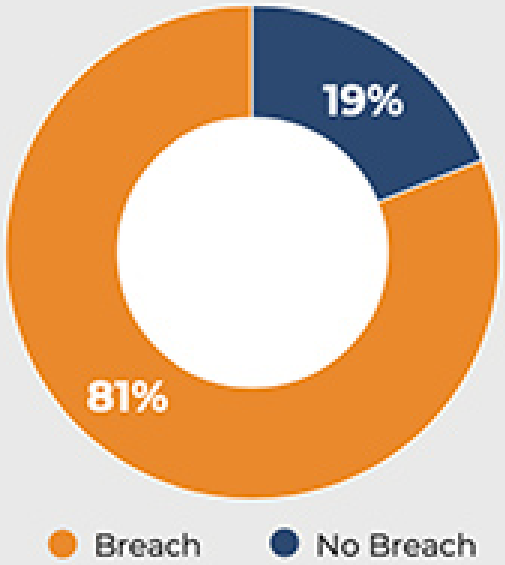
Introduction

This week's content will go over patching and what it is. Along with last week's content, unpatched machines lead to vulnerabilities in systems. If not addressed, unpatched machines allow threats to enter & access information via a "back door" into the systems.

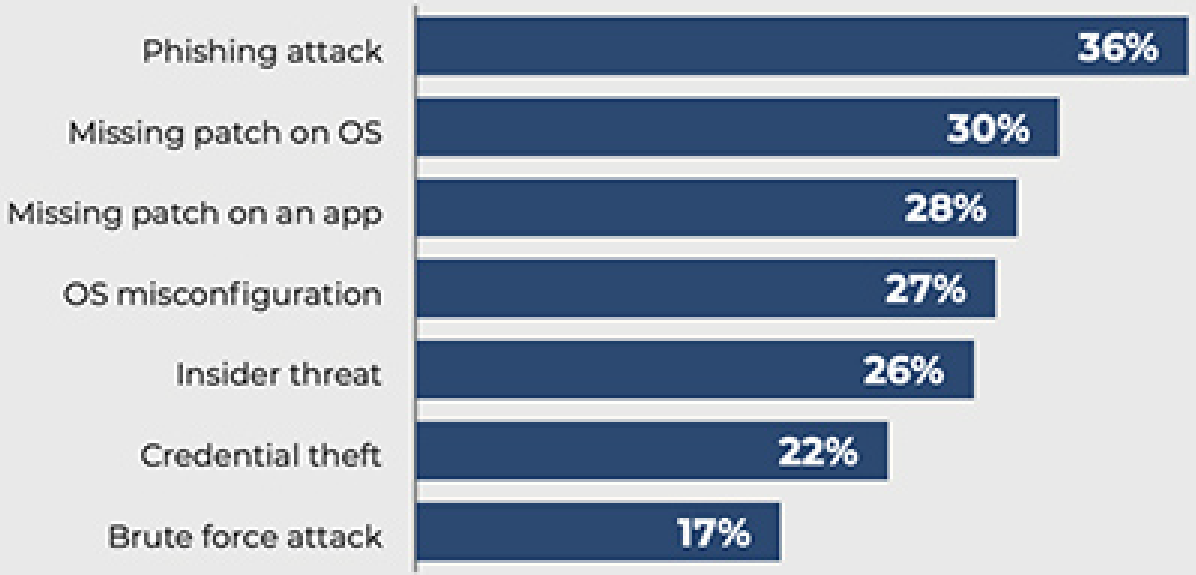
Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

Patch Management

Organizations with breaches in the past two years (n=522)



For any breaches your organization experienced in the past two years, select the root causes that were identified (n=482)



Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

Patch Management

What is Patch Management?

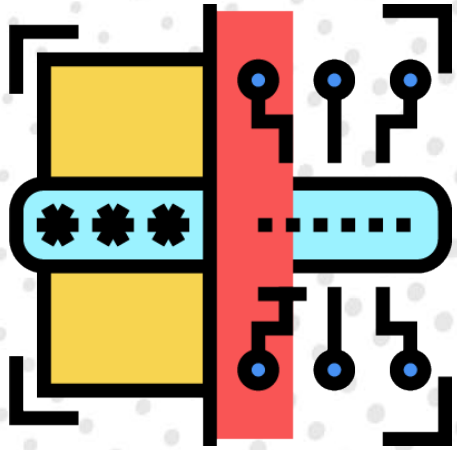
- Patch management is the process that helps acquire, test, and install, multiple patches (code changes) on existing applications and software tools on a computer; enabling systems to stay updated on existing patches
- Applying patches ensures you are able to access the newest features and have the latest security vulnerabilities patched
- Is your home computer receiving the latest updates?
- What about your phones?

Why is Patch Management important?

- Threats are always looking for ways to gain access to sensitive information for their benefit.
- They do this by looking for vulnerabilities in systems and applications.
- As most users have Windows machines, attackers used to focus on Windows vulnerabilities. This has changed as attackers are also focusing on Apple and Android devices.
- Newer protocols are always being put into effect to combat vulnerabilities of older technologies.
- As computers get smarter, it is tougher to protect against threats.
- A new topic, the Internet of Things (IoT), is important to consider.

Patch Management

What needs to be patched?



- Smart devices rely on network access and are points of vulnerabilities
  - Ensure these types of devices are patched and kept up to date on their firmware and updates
  - Alexa, thermostats, home camera systems, anything with a network connection
  - These can be back door vulnerabilities to get into your computer systems as they have access to the same network.
- Windows machines
- Phones
- Applications on your phone and programs on your computers
- Access points and Routers- how your home connects to the internet

Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

Patch Management

How do I patch?

- Please refer to the links to ensure your phone and Windows machine is patched
- Remember to make sure any device you are connecting to your home internet is also being patched
  - Router and Access Points
  - Thermostats and lights
  - Camera systems
  - Even toys
- Please refer to the manufacturer's website - ensure that devices automatically update

- Window Home Patch
  - http://www.tonation-nsn.gov/wp-content/uploads/2022/10/WindowsHome_Patch.pdf
- Android
  - http://www.tonation-nsn.gov/wp-content/uploads/2022/10/Android_Patch.pdf
- iOS
  - http://www.tonation-nsn.gov/wp-content/uploads/2022/10/iOS_Patch.pdf