PATCH APPLICATIONS

Mitigation Strategies to Prevent Malware Delivery & Execution

What does 'patching' applications mean?

Patching refers to applying fixes or updates to close 'holes' or vulnerabilities. *Applications* are programs that are run on Operating Systems. For example, Microsoft Office is the application that runs on the operating system, Windows 10. Patching Applications refers to ensuring you are running the latest version of the applications you use. For example, if you use Adobe Reader to read PDF documents, you need to ensure you are running the latest version of that product.

To reduce your risk of vulnerability, you should run the latest version in all your applications.

TO ENSURE CONFORMANCE TO THE ESSENTIAL EIGHT

- Security vulnerabilities in applications and drivers assessed as extreme risk must be patched and updated or mitigated within 48 hours.
- An automated mechanism needs to be used to confirm and record that deployed applications and driver patches or updates have been installed, applied successfully, and remain in place.
- Applications that are no longer supported by vendors need to be updated or replaced with supported versions.

Shortcut to the government's webpage: https://loyalit.com.au/e8

PATCH APPLICATIONS

Mitigation Strategies to Prevent Malware Delivery & Execution

SUMMARY SNAPSHOTS

WHAT IS AN APPLICATION?

The definition from Wikipedia:

- Application software is computing software designed to carry out a specific task other than one relating to the operation of the computer itself, typically to be used by end-users.
- Applications are installed on top of the operating system. The operating system controls the computer, the application performs a specific task on the computer.

EXAMPLES OF APPLICATIONS.

- Microsoft suite of products, e.g., Excel, Word, PowerPoint, Outlook, etc.
- Internet browsers e.g., Firefox, Safari, Edge, Chrome.
- Video games, e.g., Fortnite, Candy Crush, Doom.
- Accounting software, e.g., MYOB and Reckon Software.
- The list goes on…

SOME GOLDEN POINTS

- There is no silver bullet that will cover all applications as to the update mechanism, some are manual, some automated; it varies from vendor to vendor.
- This mitigation strategy applies to all applications you have running on your device(s) and network(s).
- If you do not need a particular application, or if there is no updated version; then remove it.

HOW TO MONITOR APPLICATIONS AND MANAGE PATCHING

- The best way is to have a vulnerability scanner running on your network. If your older software has a vulnerability, the vulnerability scanner will find it.
- If your older software does not have a vulnerability, then there is nothing to worry about… right now.
- Speak to your I.T. provider as it is likely they have a managed services product to help manage patching.

LEARN MORE

Go to the Cyber Security Business Connect and Protect portal www.loyalit.com.au/cybersecurity

and see our videos, Q&A sessions and podcasts on this and other topics.

LOYAL I.T. SOLUTIONS

PROFESSIONAL. RELIABLE. LOYAL.