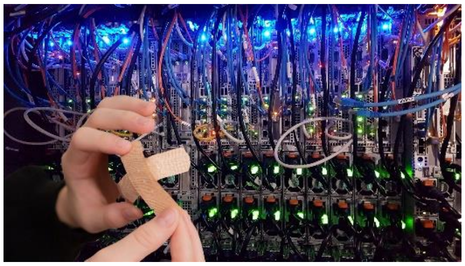
Patch Management for Security

Zero-day exploits and endless list of CVE vulnerabilities makes patching application systems, a top priority. Here are top tips for managing the patching process.

Step 1: Keep an updated inventory of all applications/ systems, this includes still-in-use end of product support, legacy applications/ systems & etc.



Step 2: Conduct risk assessments, rate all applications & systems according to level of criticality in terms of data sensitivity, connectivity spread and lateral movement. Should a hacker gain access to systems or applications, it is vitally important to know their access to other segments of the network, servers, platforms or other applications.

Step 3: Monitor vendor announcements and patch cycles; always verify or sanitise vendor patch configuration files before rolling out. Preferably test patches within a simulated environment or in smaller segments/ batches. This will prevent modified or fake patches being introduced into systems, such as the recent example of poisoned Microsoft O365 patches being deployed from 3rd party Solarwind supply chain. In Addition, a strong patch management framework will help prevent errors or issues with interoperability and dependencies.

Step 4: Mitigate applications and systems that can't be patched and act quickly to update using alternative solution or workarounds. Use automation but sanitise before rolling out to keep open-source vulnerabilities from becoming vulnerabilities in our own applications.

Step 5: Periodically review purpose and use of current technologies. Reduce the number of software versions or products. The more hardware or software versions i.e. Linux, WinOS, MacOS, Unix, the higher the Cybersecurity risk. Many large organisations complicate security further by procuring products that overlap or perform similar functions to existing hardware and software; succumbing to the pressure of upgrading without completing or fully understanding risk/ benefit analysis of meeting business objectives and cyber risk exposure.

PS: Time is critical when it comes to best practices in patch management, the more time between applications or systems being patched, the higher the risk of becoming another hacking statistic!