+44 345 094 0945
www.waterstons.com
Article

Managed patching

Breadcrumb

1. Home /
2. Print /
3. Pdf /
4. Node /
5. Entity Print

Insight navigation

- Latest insights
- Latest news
- Articles
- Case studies

Download PDF

Jun 2023

Managed patching

Old shirts, roads, and walls where paint has flaked off. What do these things have in common with your server, network and infrastructure?

Categories Managed IT Monitoring and Management, Managed Services, Managed IT Service, Managed IT Support

Jun 2023

Daniel Wrend

Head of Support Services

Email

daniel.wrend@waterstons.com

They all need patching from time to time.

Technology and digital services are constantly evolving, and regularly need attention to ensure there is no space for vulnerabilities to infiltrate. Programmes often release ‘patches’ for services to ensure they are combatting security and compliance issues, as well as offering the best possible operation.

Despite these patches being regularly available, many businesses don’t implement them, which can lead to issues around security, compliance and vendor support.

Security

Ultimately, not updating your system could lead to a major security breach.

Data could be stolen, systems infiltrated, malware installed, phishing attacks launched; the list is endless - and this doesn't only impact your business.

A breach of any kind can have a knock-on effect on others within your supply chain, starting a web of security issues and possible, costly down time.

Compliance

Maintaining Cyber Essentials accreditation requires a business to successfully install patches to remediate any 'critical' or 'high' risk within 14 days.

If not, a business risks losing its accredited status, potentially impacting other areas of the business such as health and safety, and finance – and could make it ineligible for certain tenders or frameworks.

All of which could lead to a loss of revenue.

Vendor support

Ultimately, the end must come some time, and vendors, while generous with their support, will choose to end it after a given period.

Approved patches should be installed as soon as they become available to ensure the vendor continues to support you.

If a business misses several patches for any reason, over time this could leave them far behind the current service, and a vendor can refuse support until a system is up to date. Costly, time consuming, and ultimately fraught with danger.

Managed patching

Managed patching is designed to offer a comprehensive and tailored approach to ensuring business systems are on the latest secure and stable version, firmware or update.

The service provides a tailored approach for businesses with patching policies developed, schedules agreed, testing metrics applied, and governance and reporting requirements understood and implemented.

Ultimately, this ensures that not only do critical updates get installed annually (or whenever agreed), the smaller patches that can make a huge difference to a firm's security posture and vulnerability management, are also implemented.

To find out more about managed patching, contact Daniel Wrend in our Managed Services team, or email info@waterstons.com.