CAPITA

Assist Security: Capita Managed System Administration

Overview

A library's systems and customer-facing applications – and the business-critical data that underpins the quality of service – are a potential target for malicious attacks by hackers. Maintaining a secure online environment, along with the integrity of library services and customer account data, is a fundamental challenge for all concerned. It is important to clarify what possible vulnerabilities exist from the outset and ensure these are eradicated to avoid being the next easy target.

While point-in-time reviews and fixes are an important prerequisite to any security service, the true value is in the continuous monitoring and ongoing updates, providing day-to-day peace of mind.

Benefits for your customers:

- Maintain online services (avoiding disruption) in line with user expectations
- Confidence that online services and information are secure

Benefits for your library:

- Helps prevent hacking attempts
- Avoid potential compromise of services and library data
- Ensure your library is less vulnerable to security threats minimising potential downtime
- Reduce support overhead based upon tried and tested upgrades

Maintaining secure library services

Assist Services offers a managed complementary server and operating system security service, ensuring your core library management systems and data remain intact from external security threats.

This service includes an initial audit of all subscribed library management systems and OPAC servers, followed by the necessary upgrades to the operating system to resolve immediate security concerns. Once complete, a managed security vulnerability monitoring and updating service is rolled out across your servers to maintain a secure library services environment.

Security audit

First and foremost, a security audit is undertaken which identifies accessible ports and services, as well as operating system information. A comprehensive report is generated identifying the number of security threats found, and a summary of proposed or implemented fixes.

Resolve vulnerabilities

Security vulnerabilities identified during the initial scan are resolved by disabling or removing non-essential services and applying pre-tested patches to your server operating system. Any customised firewall rules are added as well as configuration changes applied to servers to support the standard security mechanisms.

Managed updates

Monitoring of newly discovered security vulnerabilities is carried out on a daily basis. The impact is assessed and necessary patches or other software upgrades applied. This service is fully maintained during the subscription period, providing ongoing access to a vendor-approved repository of security updates and patches – thereby maintaining the operational and secure status of your library services.

> "Assist Security provides us with the assurance that security vulnerabilities will be identified and dealt with appropriately."
>
> Gillian Hickman-Ashby, IT Manager, The City of London Libraries, Archives and Guildhall Art Gallery

Find out more about Assist services

To discover more about our suite of Assist services, please speak with your Capita account manager or:

call: 0121 717 3500
email: libraries-enquiries@capita.co.uk
visit: www.capita.co.uk/libraries