ISC15D039

Title:	***Patch management of UEA systems***
Author:	Iain Husband (ISD)
Date:	3rd June 2016
Circulation:	ISSC - 14 June 2016
Agenda:	ISC15A003
Version:	Draft
Status:	Open

Issue

IT systems must be regularly patched to maintain security and remove vulnerabilities. Depending on how the system is configured, this will cause short periods of downtime. ISD will avoid critical periods in the University calendar to avoid disruption which may impact on business.

Recommendation

Recipients are invited:

- To note the report;
- To support the proposal for regular patching of systems;
- To agree on periods when routine patching of systems should be avoided.

Resource Implications

The proposed changes may require additional resources and costs which have not already been identified within the IT Security Project. Routine patching of systems will need to be included as part of day to day operational management within ITCS.

Risk Implications

There is a low risk that patching systems may disrupt service. On the other hand, by not patching systems there is a high risk of compromise and non-compliance with regulations to which the University is bound.

Equality and Diversity

The proposal is not expected to have any impact on individuals with protected characteristics.

Timing of decisions

Regular patching of systems will start immediately. All periods when patching is relaxed to avoid any potential impact on critical University periods are described in the paper.

Further Information

https://www.pcisecuritystandards.org/ the official website of the PCI Security Standards Council for further information on PCI DSS compliance requirements.

Contact for further information
Iain Reeman, ICT Director, email iain.reeman@uea.ac.uk ext 2926
Phillip Ayers, Information Security Manager, email p.ayres@uea.ac.uk ext 3994

Iain Husband, IT Project Manager, email i.husband@uea.ac.uk ext 1247

Background

Work in hand under the IT Security project to achieve PCI DSS compliance requires the University to undertake a more systematic and auditable approach to patching of systems. The IT Security project board wishes to gain ISSC support for this activity and to confirm those periods when patching should be avoided. Unpatched systems pose a risk to the whole institution, and therefore the intention is to ensure that all UEA-owned systems that connect to the data network are routinely patched.

Discussion

Patch Management of UEA Systems.

This document is for the review and support of the ISSC that the essential patching of systems and infrastructure is a requirement of ITCS. Also, that planned downtime for these processes is acceptable, given that ITCS will always try to keep this downtime to a minimum and away from business critical events, and if possible apply a change freeze for short periods over these events.

What is Patch Management?

Patch Management is the critical process by which ITCS update all information technology systems, network resources (such as switches, routers and firewalls) and applications to ensure that they are as secure as possible.

Why carry out this process?

Keeping systems as up to date as possible and secure is one of the most important tasks that should be under taken by ITCS. With the increasing use of malicious code to exploit known vulnerabilities on unpatched IT systems and hardware, those who wish to can now infiltrate systems, cause malicious damage and carry out financial and data theft. All of which can have major implications of cost, business continuity and reputational damage to the organisation.

Along with the ever increasing threat from those with malicious intent, requirements around governance and regulatory compliance (e.g. PCI DSS, DPA) now emphasise the securing of all systems and monitoring them on a very regular basis. Standards specifically include the need to monitor for vulnerabilities and patch systems.

The potential impact of breaching PCI compliance includes:

- fines for non-compliance
- removal of ability to take credit/debit card payments for the whole of UEA
- reputational damage to the University

In addition to fines that may be imposed if there were to be a data breach in relation to Data Protection Act, the Information Commissioner's Office may impose fines up to £500,000 (expected to rise to 4% of worldwide turnover under the General Data Protection Regulation [GDPR] replacing the Data Protection Act). Further losses will arise from compensation paid to each individual affected by the breach.

Proactively managing vulnerabilities of systems will help reduce the potential for exploitation and involve considerably less time and cost than responding after exploitation has occurred.

Types of patching carried out by ITCS:

- Firmware
  - Hardware including network core infrastructure, blade enclosures, SAN etc.
- Driver updates
  - Telephony, network devices, peripherals etc.
- Operating systems
  - Windows, Linux and IOS
- Applications
  - Both on servers and desktops
  - Including "plugin" updates

The patches need to be applied as soon as possible after release to be as effective as possible. Current ITCS policy states that critical patches should be installed within 1 month which is in line with current regulatory requirements: PCI DSS compliance requires critical patches to be applied within 30 days of their release.

However installing updated software even if tested by the manufacturer does pose a certain level of risk to any organisation. Rebooting systems may include planned downtime, or the patch may have unforeseen effects which can lead to un-planned downtime.

ITCS therefore employ several flexible strategies to avoid patching impacting on system availability and stability especially around critical periods within the University calendar.

Periods of change freeze:

A few periods throughout the year have been identified when system stability is viewed as essential and ITCS will make no planned changes to the systems or infrastructure during these periods unless there is an emergency that requires ITCS to intervene on specific systems or infrastructure. These periods are currently limited to 14 days as a maximum period and cover:

- Clearing: 14 days around the 2nd week in August:
  a. This year
     i. w/c 15th August Clearing
     ii. w/c 22nd August Clearing
- Start of year: 14 days around 3rd week of September. This allows a smooth start for new students and returning staff.
  a. This year
     i. w/c 19th September Start of Year
     ii. w/c 26th September Start of Year
- December Submission period: this normally covers a week to 10 days depending on the number of submissions and their frequency.
- Open days: ITCS avoid doing major upgrades on Open days to allow all systems to keep running as smoothly as possible.

Automated Patching:

ITCS use various applications to monitor patch management: Secunia highlights missing patches from Windows; Heatpatchlink can monitor those missing from Linux OS. All Windows desktops are patched automatically (via SCCM) following release of the latest patches by Microsoft (currently 2nd Tuesday of each month).

Windows Server Operating Systems and some applications, i.e. IIS, are also patched automatically using SCCM. Although Heatpatchlink can automate some Linux patching this is currently done manually.

Test systems:

A number of essential systems have duplicated test systems in place on which patches are tested and accessed before moving on to live systems.

Use of appropriate patch libraries:

Patches for Microsoft applications and operating systems will come solely from Microsoft.

Patches for non-Microsoft applications and operating systems can be sourced from various libraries across the internet. ITCS will source their Linux patches from the manufacturer or manufacturer recommended libraries which are validated.

Regular updating of desktop applications via the application catalogue:

This allows patches to be applied automatically where possible, or ITCS can contact customers who have installed the application and ensure all remedial action is required before the patch is applied.

Other considerations:

Apple Macintosh computers are only patched currently if they have specific “Casper Agents” installed as part of the build process. ITCS are currently able to patch 190 out of what is thought to be approximately 750-1000 Apple devices on the network.

Staff and student personal devices are not covered by UEA scanning or patching regimes, we advise users to ensure that their machines are fully up to date however we cannot control this.

Mobile devices: Phones and tablets are also not patched remotely by ITCS.

Servers not within the ITCS Managed service are not being scanned or patched regularly and are a high risk to University systems. A project entitled Faculty Housekeeping is tasked with identifying these systems and bringing them into the ITCS Managed Service.

When ITCS bring in a fully compliant patching regime across all systems, there may be a requirement for some additional resources to be put in place to ensure that business as usual is not impacted by this additional work load.