Paper B - Report from Head of Computing 2021-10-29

Email forwarding

IS announced on Oct 15th that they would be emailing, on Oct 20th, all those who currently forward their email out of Office365 giving them notice that this forwarding will cease from 12th November. Alastair requested and was provided with a copy of this email so that managers could be pre-warned - he circulated this to the DoIs. Some other Schools objected to the late notice, so the notice email date was pushed back to Oct 25th.

SSH servers

Acting on JISC and NCSC advice, the University is pushing the majority of University 'ssh' services behind the VPN. Only those 'ssh' services for which a business case has been submitted and accepted will be permitted to be accessible without VPN, with restrictions likely to be applied. All managers of Informatics 'ssh' services were given a deadline of 26th October to indicate whether they intended to submit a business case, with a deadline of 1st November to submit a case. Those 'ssh' services for which no intent was declared were blocked on 26th October.

A business case to create a new VPN-free access 'remote.ssh.inf.ed.ac.uk' was submitted to IS and accepted, though it's not clear whether further conditions may be applied in the future. This service will be opt-in for only those staff, research postgrads and collaborators who need VPN-free access. A separate 'ssh' service, behind the VPN, will be introduced for general use. 'student.ssh.inf.ed.ac.uk' will only be available behind the VPN. Intent to submit a business case was declared for three self-managed 'ssh' services.

EdLAN replacement project

We have been unable to progress with our testing of how our office desktops, etc, will work with the new EdLAN network at the edge. This is because IS have yet to furnish us with the technical details that we require to progress this work, despite repeated requests. Alastair has raised this issue at the Project Board.

Recent incidents

- 20th August: IS reported that a self-managed web server was vulnerable to the SSL POODLE attack. Further investigations revealed that it was running Ubuntu 14.04 which was long unsupported. Firewall access was restricted and the owner was required to upgrade the machine. There was no detected compromise of the system.
- 23rd August: A self-managed wordpress instance was compromised and used to attack other sites. For full details see the report (https://dice.inf.ed.ac.uk/publications/2021/wordpress_exploit_report.pdf). University CISO was made aware.
- 13th September: A request to remove some personal data from a web page revealed a page from 2008 with student names and matric numbers on it. The page was immediately restricted and subsequently removed, and the incident reported to the University DPO.

IS developments

- Teams Webinar - introduces webinar features to Teams including attendee registration, 1000 interactive and live-streaming to 10,000 view-only attendees. Clearer definition of roles for organiser, presenters and attendee.