Chichester District Council

Corporate Governance and Audit Committee

19 July 2021

Update Following Global Microsoft Exchange Hack

1. Contacts

Report Author:
Andrew Forward, ICT Manager
Tel: 01243 534770 E-mail: aforward@chichester.gov.uk

2. Recommendation

2.1. **That the Committee are fully briefed on the circumstances, actions and outcomes following the Global Microsoft Exchange Hack in March 2021.**

3. Background

3.1. At the beginning of March we became aware of a weakness in Microsoft Exchange Servers (used to provide the Council's email capabilities), and joined the worldwide scramble to 'close the door' on hackers and cybercriminals attempting to exploit this vulnerability (weakness).

3.2. We were targeted. The below chronology describes the circumstances surrounding the incident, our immediate response and subsequent clean-up activities.

3.3. Throughout we adhered to the 'Incident Management' approach. A 5 stage model (Identify, Protect, Detect, Respond and Recover), as recommended by the National Cyber Security Centre (NCSC) part of Government Communications Headquarters, commonly known as GCHQ.

4. Outcomes to be achieved

Identify

4.1. 02 March 2021: Microsoft announced the detection of multiple zero (0) – day exploits being used to attack on-premises versions of Exchange Servers.

4.2. A zero (0) day vulnerability is about as scary as it gets.

4.3. 03 March 2021: Microsoft issued an emergency security patch to block Exchange Server systems becoming compromised and seeded with powerful backdoor Trojan horse programmes.

4.4. The attack, which Microsoft has said started with a Chinese government-backed hacking group, had moved from targeting high value intelligence targets to mass indiscriminate exploitation attacks.

Protect

4.5. 03 March 2021: We attempted to apply patch to server. Patch failed.

4.6. Server taken off line immediately. Providing instant security from hacking attempt, but caused service interruptions.

4.7. 04 March 2021: Working with (our) Microsoft partner we applied patch at 17:15 and brought server back on line.

Detect

4.8. Having secured our servers we began a forensic examination of our systems, looking for any indicators of compromise (IOC).

4.9. We discovered that our exchange server had been targeted between 01 and 03 March. The last attempt approximately 30 minutes *before* we received official Microsoft notification of the threat.

Respond

4.10. Having confirmed that our systems had been targeted, we undertook detailed line by line script searches looking for evidence of

(a) Any data losses, and

(b) Presence of any (backdoor) 'Trojan horse' webshells.

4.11. Our searches returned negative results;

(a) No data was extracted from our systems. Although data exfiltration was attempted, the request was denied and the 'hack' failed. This was repeated three times between 01 and 03 March. Each attempt returning a '500' internal server error code – 'unable to complete the request' for extraction of data.

(b) Full system diagnostics (as advised by NCSC) found no trace of Trojan horse webshell scripts. Additionally, line by line script analysis (in accordance with Microsoft guidance), also found no trace of inserted backdoors.

4.12. We also took additional measures to restrict access to our Exchange Server. Blocking all but recognised traffic to/from the Microsoft 365 (cloud) exchange.

Recover

4.13. Having proved conclusively that we had not suffered data loss or Trojan horse infection, we referred our findings to Microsoft. On 31 March 2021 we formally signed off on our investigation and recovery activities.

4.14. We are now seeing other cybercriminals seeking to exploit this weakness. Subsequently, Microsoft has issued additional urgent patching action requests, which have been applied immediately.

4.15. Continuously monitoring the situation as new information and advice is coming to light.

Conclusion

4.16. We have shut the door on the known server weakness (patched). Restricted access to the server (stopped any exfiltration of data) and searched our systems for evidence of compromise.

4.17. As more details emerge surrounding this incident, coming just weeks after the suspected Russian hackers compromise of the leading global provider SolarWinds, further fall out can be expected.

4.18. Within days this hack had claimed at least 60,000 known victims globally, including notably the European Banking Authority. Whilst exposure is limited, due to our current use of Microsoft 365, this incident is a stark reminder of the constant and ever changing threats we face.

4.19. Before this incident, work had already started on an ICT security strategic review. Already identified as a priority action in our 2021/22 Service Plan, this work was fast tracked and, taking into account the lessons learned, a framework plan developed. Full details are contained in a follow on report to the Committee.

5. Alternatives that have been considered

5.1. None.

6. Resource and legal implications

6.1. Data breaches carry reporting responsibilities. In this instance although no breach occurred, data protection protocols were followed and NCSC and ICO were advised.

6.2. ICT Security Management is an integral business as usual function. Recent intelligence indicates increasing cyber-criminal activity in both volume and sophistication. As a service we need to respond appropriately to this changing threat environment. Our ICT Security Plan framework has been developed to ensure our security posture reflects the changing threats we face.

7. Consultation

7.1. None.

8. Community impact and corporate risks

8.1. Corporately, the potential impacts of cybercrime on the Council are well understood, being reflected under Corporate Risk CRR 97 – Cyber risk across the ICT estate. Where, despite existing mitigations, we see an increase in the likelihood of that risk materialising, it is important that we reflect on any learnings and take appropriate actions.

8.2. This report provides an explanation as to the actions taken, and provides an actual account of the processes we followed when dealing with a clear and present danger.

9. Other Implications

	Yes	No
Crime & Disorder		✓
Climate Change		✓
Human Rights and Equality Impact		✓
Safeguarding and Early Help		✓

General Data Protection Regulations (GDPR)		✓
Health and Wellbeing		✓
Other (Please specify):		✓

10. Appendices

10.1. None.

11. Background Papers

11.1. None.