Student ID: 2136685

ISM CW1 – CISO MEMO

To: Executive team

From: John Doe, Chief Information Security Officer

Date: 7th December 2022

Re: Security audits issues

Summary

After analyzing the security audits from last year, I have found multiple issues with our infrastructure, such as software and hardware shortfalls however, my focus today will be on the critical security concerns, of which I have found many. I have taken the ten most crucial issues and I will discuss them in the following paragraphs. Moreover, I hope to highlight my responsibilities as a CISO, discuss the legislation, and propose a restructure of the cybersecurity team.

My Responsibilities as CISO

As a CISO, I am here to ensure that the risks we are willing to take are measured and in line with our risk appetite. My continuous task is to adapt our information management criteria based on new threats, regardless if they come from a new vulnerability in software or if it comes from a new technology we wish to adapt. In addition, I am here to make sure that any question from the executive team is answered and that they leave with a clear understanding of the information assets we protect and the security strategies we employ. (Bird, 2020)

Identified Issues

As I have mentioned in the summary, I have gathered ten critical issues that need to be solved as soon as possible. I will now outline them for you and give some ways to combat these issues:

1. Limited documentation on information security procedures

Being aware of the worst-case scenario is crucial. We must always prepare for the worst when it comes to information security. Having an extensive information security policy that covers all of the deep and sometimes even unlikely corners is incredibly important because even if a threat is unlikely to occur, it does not mean that it could not happen.

I propose that we follow the ISO's 27000 series of standards to compose robust information security procedures with a particular focus on the ISO 27000-27006 as they are the most relevant to the University of Cytroy. (International Organization for Standardization, 2013)

2. Limited effort to raise security awareness

It is important to ensure that everyone that uses the university resources has their data secure. Everyone has received a phishing email before, but some fall for them. I propose that we send out phishing email examples to our university staff and students and give mandatory training to the university staff about such attacks.

Every time there is a new vulnerability that affects the university's systems, everyone enrolled in the university must be notified, be it in person or through email, so they are aware if they must stop using a piece of software until the update that fixes the vulnerability is available.

3. No clear structure of responsibilities in an event of a cyberattack

Incident response is a major part of cybersecurity. We must plan for the worst-case scenario and outline mitigation tactics for every threat we might be exposed to. Given that we are a university, we must adjust our risk appetite keeping in mind the large number of data we process.

We must have a plan in case of a cyberattack as the financial and reputational penalties would be immense. We must start working on incident response as soon as possible.

4. Unlocked computer systems

Computers being unlocked can be used by threat actors to install malware that can compromise the security of all users. For example, a threat actor could install a keylogger on a machine, collecting users' information that they type into that machine.

I suggest that we lock all the machines on our campus using a login system that requires a user's unique university credentials to log in. This will not, however, prevent threat actors from using physical keyloggers such as the ones sold on keelog.com. (Keelog, 2022)

5. Unattended and unsecured portable devices

Unattended portable devices can be infected with malware and have their data stolen. In the worst-case scenario, an unattended portable device's data has been stolen and loaded with malware, awaiting a connection to a computer to infect it. Therefore, one must practice having their portable devices attached to objects they will not forget, for example, their keys.

Alternatively, portable devices laying around, such as the Hak5 Rubber Ducky, could have been planted by a threat actor with the intention of the device being picked up by an unassuming victim and being plugged into a computer, therefore infecting that computer. (Faife, 2022; Hak5, 2022)

The university must explain thoroughly the importance of keeping portable devices close to oneself and outlining the importance of not plugging in found portable devices. This can be done through an email, a meeting, or a training module.

6. Limited audit log policies

Audit logs, in case of a security breach, will tell us when and where the breach has occurred. They are invaluable to forensic investigation. We may even be dependent on audit logs in court, in case of a breach, so we need to make sure that all of our systems record logs. (ATIS, 2022)

After we started storing all of our system logs, we can start thinking about implementing the ISO 27000 series, which requires a scheduled audit every year.

7. Weak password enforcement

We must push people to have proper password etiquette. Passwords like "!dIL?zbM&(G8Vg{\m#5{" get forgotten quickly and changed to a weaker password, whereas strong passwords are passphrases such as "PlatinumRevealDrabThud". Passwords should be changed at least every season however, I understand that people would not think they need to. We must explain the importance of doing so, to keep their data safe.

We should consider implementing two-factor authentification in the university authentication system. This significantly decreases the risk of a threat actor accessing data with compromised credentials.

8. Out-of-date and expired antivirus software on internal servers

Antivirus software must always be kept up to date, as each update adds new virus definitions. This ensures that new viruses can be exterminated and old viruses get taken care of faster.

Moreover, expired antivirus software is a problem as they require a valid license for important features like real-time protection, which constantly scans for malware on a computer and quarantines them immediately.

To ensure that our antivirus software is never expired or out-of-date, I propose that we purchase licenses for an antivirus solution and enable automatic updates for it. I recommend Malwarebytes, which offers enterprise solutions. (Malwarebytes, 2022)

9. Elevated security privileges to computer systems of some members of staff

Elevated security privileges for staff that do not require them is a security risk. Elevated privileges must only be given to system administrators who have to keep the machines up-to-date. System administrators are more careful with credentials than staff and their cohort is smaller, making the attack surface less. We must update staff privileges to only contain as much as they need to carry out daily activities.

10. Unauthorised software installed on university-owned systems

Unauthorised software can be installed by people that should not have access to do so, due to the privilege policy being poor. Giving user accounts the ability to install applications is a bad idea, as they could install malware and gather sensitive data.

The privilege policy must be reviewed to ensure that only system administrators can install applications.

Importance of the Data Protection Act and UK-GDPR

The Data Protection Act and UK-GDPR are the key data protection laws in the UK. They set out the rights, obligations, and key principles of handling and processing personal data.

We keep strongly regulated data, like race. This data must be kept safe at all times, especially in case of a breach. Whenever we use data, it must be used with a specific purpose and limited to only the necessary data. Moreover, whenever a student or staff leaves, we must not keep their data for longer than necessary and then destroy it. Breaking the data laws can result in fines of up to £17.5 million or 4% of annual turnover, devastating our finances and our reputation. (GOV.UK, 2018; Information Commissioner's Office, 2019; Information Commissioner's Office, 2021b)

As we take in EU students, we must also fully comply with EU-GDPR. Currently, the UK has adequacy through UK-GDPR. Should it change drastically, adequacy might be taken away, so we must comply with EU-GDPR as well. (Information Commissioner's Office, 2021a)

Restructure of the Cybersecurity Team

To keep our data safe, we must implement a Security Operations Centre. Having a SOC will help with activities such as coordinating incident responses, managing audit logs and systems, and implementing security policies. We must hire a SOC manager and work with them to build a team while re-assigning our current cybersecurity team to positions in the SOC. Assigning people their preferred roles laser-focuses them on their strengths, increasing efficiency. As a result, we will recognise incidents faster, apply mitigation tactics faster and decrease the incident fallout. (Checkpoint, 2022)

Thank you,

John Doe

Chief Information Security Officer

References

ATIS (2022). Audit trail – Glossary. [online] atis.org. Available at: https://glossary.atis.org/glossary/audit-trail/ [Accessed 28 Nov. 2022].

Bird, B. (2020). What is a Chief Information Security Officer? [online] Office of The CISO. Available at: https://www.officeoftheciso.com/2020/04/21/what-is-a-chief-information-security-officer/ [Accessed 23 Nov. 2022].

Checkpoint (2022). Security Operations Center (SOC) Roles and Responsibilities. [online] Check Point Software. Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/security-operations-center-soc-roles-and-responsibilities/ [Accessed 28 Nov. 2022].

Faife, C. (2022). The new USB Rubber Ducky is more dangerous than ever. [online] The Verge. Available at: https://www.theverge.com/23308394/usb-rubber-ducky-review-hack5-defcon-duckyscript [Accessed 23 Nov. 2022].

GOV.UK (2018). Data Protection Act. [online] gov.uk. Available at: https://www.gov.uk/data-protection [Accessed 28 Nov. 2022].

Hak5 (2022). USB Rubber Ducky. [online] Hak5. Available at: https://shop.hak5.org/products/usb-rubber-ducky [Accessed 23 Nov. 2022].

Information Commissioner's Office (2019). The Principles. [online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ [Accessed 28 Nov. 2022].

Information Commissioner's Office (2021a). Data Protection and the EU. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/ [Accessed 28 Nov. 2022].

Information Commissioner's Office (2021b). Penalties. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/penalties/ [Accessed 28 Nov. 2022].

International Organization for Standardization (2013). ISO/IEC 27001 Information security management. [online] ISO. Available at: https://www.iso.org/isoiec-27001-information-security.html [Accessed 23 Nov. 2022].

Keelog (2022). Hardware Keylogger - AirDrive & KeyGrabber Keylogger - C64 PSU Power Supply. [online] www.keelog.com. Available at: https://www.keelog.com/ [Accessed 23 Nov. 2022].

Malwarebytes (2022). Malwarebytes Enterprise Security Solutions. [online] Malwarebytes. Available at: https://www.malwarebytes.com/business [Accessed 28 Nov. 2022].