Most essential of Eight

Anne Coull

UNSW

anne.objectiveinsight@gmail.com

October 2020

Anne Coull

Anne applies academic research in the corporate environment.

She is a strategic, hands on, influential leader with an entrepreneurial mindset and a passion for architecting modern technology that quickly delivers value to customers & stakeholders.

Anne has a track record for mentoring, developing and inspiring high performing teams within an inclusive culture. She applies her expertise and experience in Cyber Security, SDLC, ITSM, operational excellence, program management, and cultural change to implement business-culture-technology transformations.

Dedicated to continuous learning and research, Anne is the director of community for Women in Cyber Security (Wicys) Australia, a member of the NSW School of Engineering & Information Technology (SEIT) External Advisory Committee, an active contributor to the development of technical research papers and conference presenter for the International Academy, Research and Industry Association (IARIA). Topics include: Four testing types core to informed ICT governance for cyber-resilient systems; How much cyber security is enough; Most Essential of Eight; and Cyber security and service management.

Projects and Areas of Interest

1. Cyber Security in business
2. Integrating Cyber Security into everyday life
3. Integrating Cyber security into IT (service management)
4. Using intelligence to combat intelligence

AS ISO/IEC 27001
AS ISO/IEC 27002

ITIL4

Australian Signals Directorate

CPS 234

Australian Prudential Regulation Authority

National Institute of Standards and Technology
U.S. Department of Commerce

Essential Eight

Reduce cyber security risk and increase resilience:

1. Prevent malware delivery and execution.
2. Limit the extent of cyber security incidents and the damage they can cause; and
3. Recover data and Systems availability.

Mitigations to:

Prevent malware delivery and execution

- Patch applications
- Application whitelisting / control
- User application hardening
- Configure Microsoft Office macro settings

Limit extent of cybersecurity incidents

- Patch operating systems
- Restrict administrative privileges
- Multi-factor authentication

Recover data & systems availability

- Daily backups

Patching Operating Systems & Applications

Security vulnerabilities in systems and applications are used to execute malicious code, and create a gateway into an organisation's systems.

2016 to 2019:
Most commonly exploited vulnerabilities in Microsoft's Object Linking and Embedding (OLE) technology.
Second most commonly exploited vulnerability in Microsoft's Apache Struts Web framework, and Adobe Flash

2020:
Increase in exploits targeting Virtual Private Networks (VPN) vulnerabilities

Mitigation goal

1. Extreme risk security vulnerabilities in operating systems and firmware, applications and drivers are patched, updated or **mitigated within 48 hours** of the security vulnerabilities being identified
2. **Automated mechanism confirms and records** that deployed patches have been installed
3. Out of support systems replaced with **vendor-supported versions.**

Application Whitelisting / Control

Application whitelisting protects against the execution and spread of malicious code by ensuring only authorized applications can be executed or installed.

To implementing application whitelisting:

1. **Identify applications that are authorised to execute**
2. **Develop application whitelisting rules to ensure only those authorised applications can execute**
3. **Maintain the application whitelisting rules using change management**

Mitigation goal

1. **Application whitelisting/control implemented on all workstations and servers**
2. **Microsoft's block rules implemented to prevent application control bypasses.**

User Application Hardening

Application hardening reduces the attack surface by configuring business applications to disable functionality that is not needed.

Web browsers are configured to block and uninstall Flash, ads and Java from the internet.

Users are given access to functionality within an application on an as-needs basis.

Mitigation goal

1. **Web browsers** are configured to:
   - block or disable support for Flash content.
   - block web advertisements.
   - block Java from the internet.
2. **Microsoft Office** is configured to:
   - disable support for Flash content.
   - prevent activation of Object Linking and Embedding (OLE) packages.

Configure MS Office Macro settings

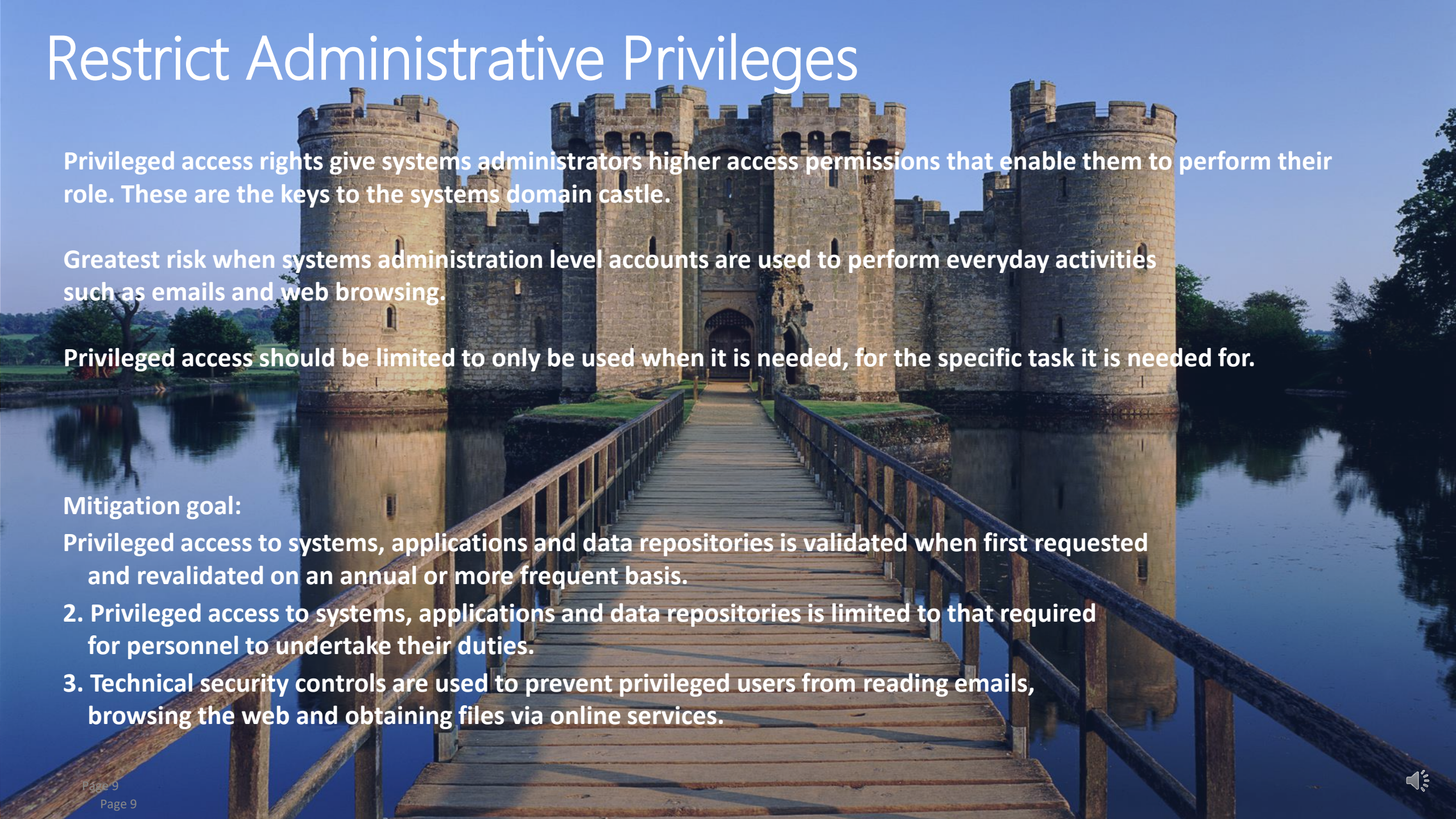
Microsoft Office macro settings configured to block macros from the internet.

Only allow vetted macros from trusted locations or those that have been digitally signed with a trusted certificate to execute, and only with limited write access.

Mitigation goal

1. Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.
2. Microsoft Office macros in documents originating from the internet are blocked.
3. Microsoft Office macro security settings cannot be changed by users.

Restrict Administrative Privileges



Privileged access rights give systems administrators higher access permissions that enable them to perform their role. These are the keys to the systems domain castle.

Greatest risk when systems administration level accounts are used to perform everyday activities such as emails and web browsing.

Privileged access should be limited to only be used when it is needed, for the specific task it is needed for.

Mitigation goal:

Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.

2. Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.
3. Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Page 9

Multi factor authentication

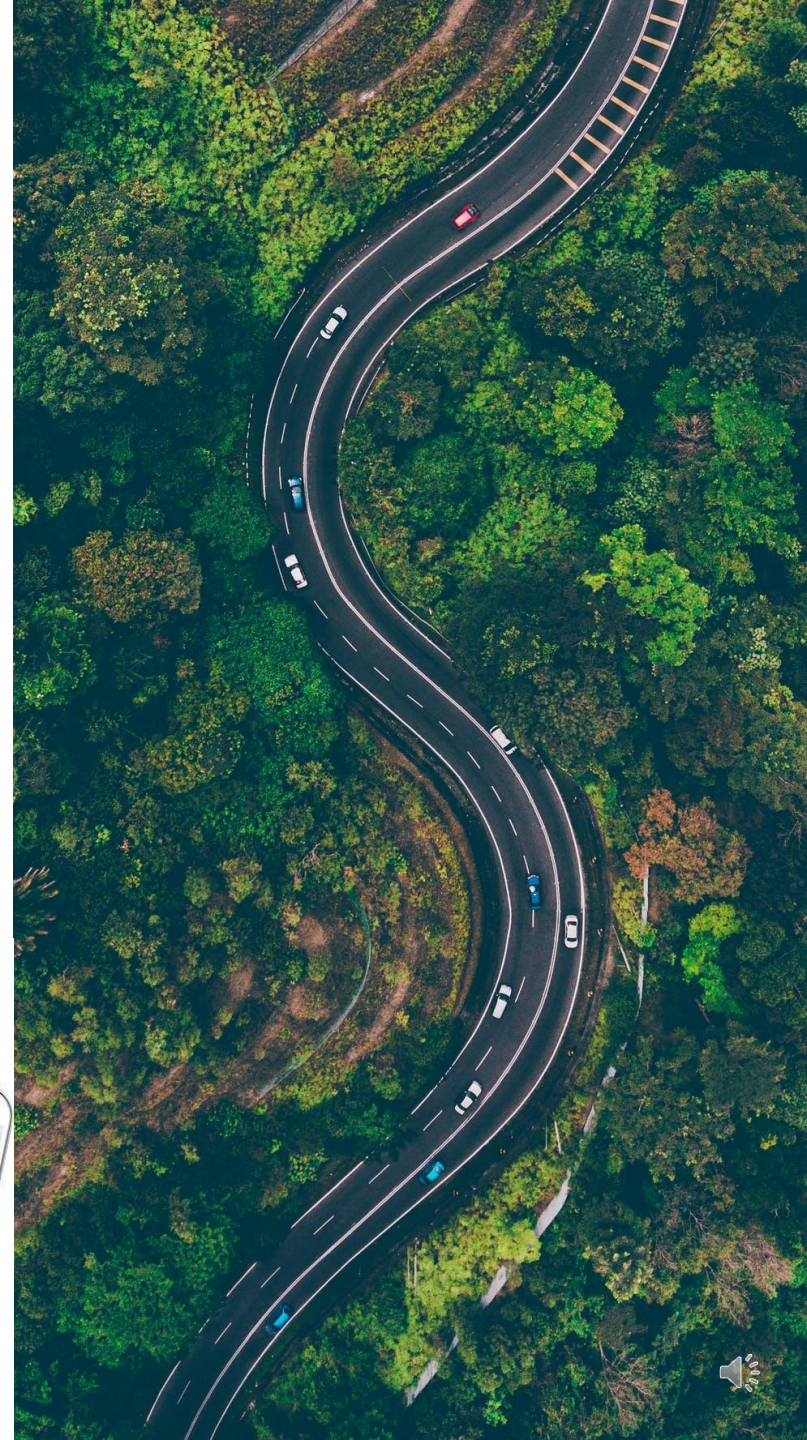
MFA uses a combination of verifications from different sources, including:

1. Something the user knows: a pin, a password or passphrase, or security questions; and
2. Something the user physically possesses, a code or token automatically generated by an authenticator app and / or SMSed to their mobile phone; and
3. Something the user inherently possesses, biometrics, a finger print, or retina.

Mitigation goal

MFA to authenticate:

1. all users of remote access solutions.
2. all privileged users and any other positions of trust.
3. all users when accessing important data repositories.



Daily backups

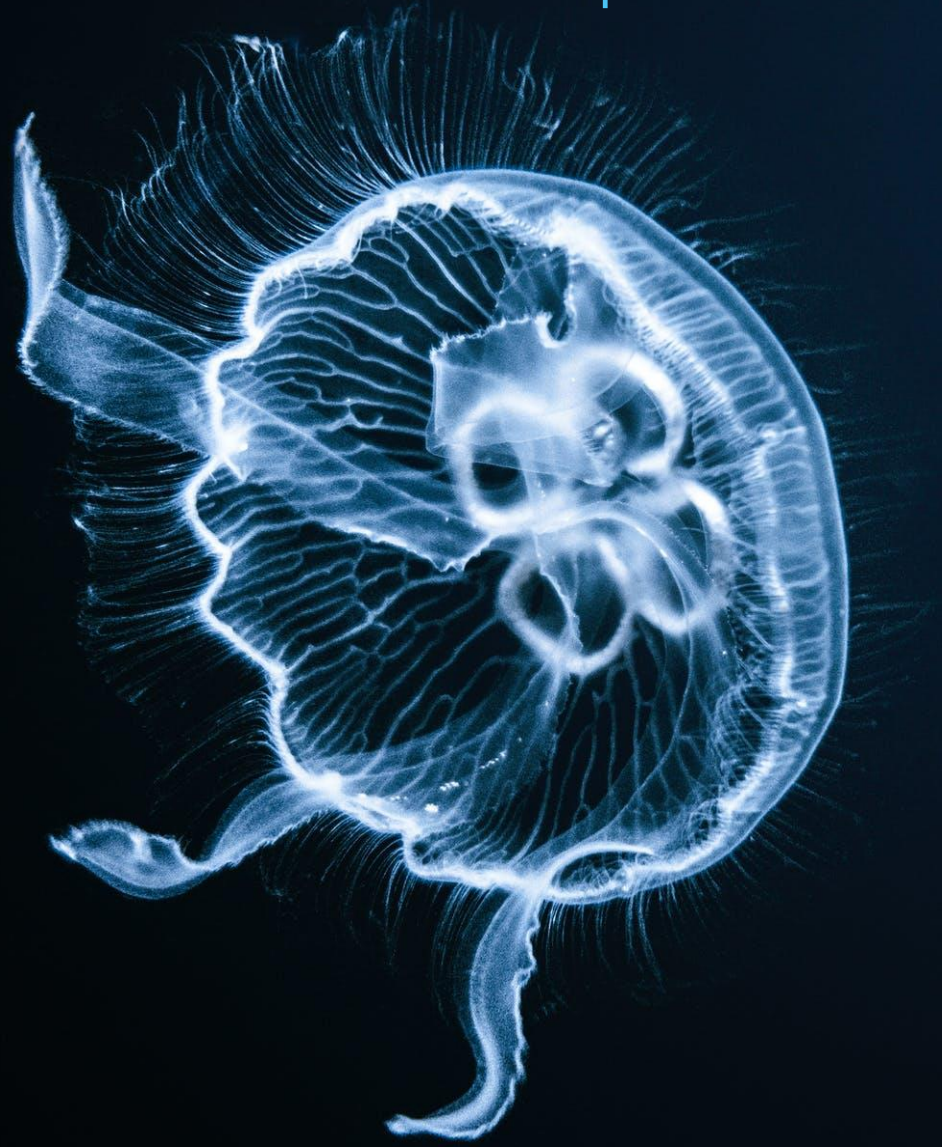
Without backups:

- Lost, destroyed, or altered data cannot be restored;
- Data integrity cannot be validated;
- A ransomware attack, can bring a business to its knees.

Mitigation goals

1. **Backups** of important information, software and configuration settings **performed at least daily.**
2. **Backups stored offline**, or online in a non-rewritable and non-erasable manner.
3. **Backups are stored for three months** or greater.
4. **Full restoration of backups tested** initially and each time fundamental information technology infrastructure changes occur.
5. **Partial restoration of backups tested** quarterly.

2020 Threat Landscape



Three top malware incidents in 2020:

1. Password dumping to obtain access credentials,
2. Phishing to directly install malware, and
3. Ransomware

4. Droppers and Trojans in the form of downloaders and keylogger in 20% and 12% malware samples, but fewer incidents

5. Decrease in incidents caused by malware that exploits vulnerabilities.

2020 Data breach investigations report

Address highest risk first

For the most essential mitigations:

First

Implement mitigation for high-risk users and computers:

- access to sensitive or confidential information
- exposed to untrustworthy internet content
- high-availability systems

Then

Implement for all other users and computers.

Test

Perform hands-on testing to verify the effectiveness of implemented mitigation strategies.

Discussion & Questions

What are your experiences in implementing these mitigations?

Where did you start? Why?

How did you progress?

What challenges did you face?

What did you learn?

What would you like to share?

email anne.objectiveinsight@gmail.com

References

1. J. Andress & S. Winterfeld, “Cyber Warfare: Techniques, tactics and tools for security practitioners, second edition”, Elsevier, Inc, United States of America. 2014. [1a] page 11, [1b] p.187.
2. Australian Cyber Security Centre (ACSC), ”Strategies to mitigate cyber security incidents”, Australian Government, Australian Signals Directorate, 2017, Available from: https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents, accessed October 2020
3. ACSC, ”Essential eight explained, Australian Government”, Australian Signals Directorate, 2019, Available from: https://www.cyber.gov.au/sites/default/files/2020-01/PROTECT%20-%20Essential%20Eight%20Explained%20%28April%202019%29.pdf, accessed October 2020
4. ACSC, ”Implementing application whitelisting”, Australian Government, Australian Signals Directorate, 2019,Available from: https://www.cyber.gov.au/sites/default/files/2019-04/PROTECT%20-%20Implementing%20Application%20Whitelisting.pdf, accessed October 2020
5. ACSC, ”Essential eight maturity model”, Australian Government, Australian Signals Directorate, 2020, Available from: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model, accessed October 2020
6. ACSC, ”Multi factor authentication”, Australian Government, Australian Signals Directorate, 2020, Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/multi-factor-authentication, accessed October 2020
7. ACSC, ”Application Hardening”, Australian Government, Australian Signals Directorate, 2020, Available from: https://www.cyber.gov.au/acsc/view-all-content/guidance/application-hardening, accessed October 2020
8. ACSC, ”Guidelines for system hardening”, Australian Government, Australian Signals Directorate, 2020, Available from: https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening accessed October 2020
9. ASCS, “Australian Government Information Security Manual”, Australian Government, Australian Signals Directorate, 2020, Available from: https://www.cyber.gov.au/sites/default/files/2020-06/Australian%20Government%20Information%20Security%20Manual%20%28June%202020%29.pdf, accessed October 2020
10. Australian Prudential Regulation Authority (APRA), ”Prudential Practice Guide CPG 234 Information Technology”, 2019, Available from: https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019.pdf, accessed October 2020
11. APRA, Prudential Standard CPS234 Information Security”, 2019, Available from : https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf, accessed October 2020
12. AntiPhishing Working Group APWG, “Phishing activity trends reports”, 2020 , Available from: https://apwg.org/trendsreports/, accessed October 2020
13. CISA, ”Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities”, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, May 2020, 2020, Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-133a, accessed October 2020
14. D. Gibson, “Managing risk in information systems”, Jones Bartlett Learning, Burlington MA 01803, 2015. [14a) p. 233.
15. J. Leopando, ”World backup day: The 3-2-1 rule, 2 April 2013”, Trend Micro 2013, Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/world-backup-day-the-3-2-1-rule/, accessed 25 October 2020
16. Malwarebytes, “Ransomware”, 2020, Available from: https://www.malwarebytes.com/ransomware/, accessed October 2020
17. T. McIlroy, ”Protections against porting scams to be forced on all telcos by April”, Australian Financial Review October 16 2019, Available from: https://www.afr.com/politics/federal/telcos-pushed-to-toughen-mobile-scam-protections-20191016-p5313i, accessed 20 October 2020
18. Microsoft, “Security Update Guide”, 2020, Available from: https://msrc.microsoft.com/update-guide, accessed October 2020
19. NAB, “Fraud warnings for all NAB customers”, Security Alert March 2020, Available from: https://www.nab.com.au/about-us/security/fraud-warnings-for-all-nab-customers, accessed October 2020,
20. A. Rousseau 2017, ”WCry/WanaCry ransomware technical analysis”, End Game, 14 May 2017, Available from: https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis, accessed 25 October 2020
21. C. Schou and S. Hernandez, “Information Assurance handbook: Effective computer security and risk management strategies”, McGraw Hill Education. United States of America, 2015.
22. Verizon, ”2020 Data breach investigations report”, 2020, Available from: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf, accessed October 2020
23. S. Winterfeld & J. Andress, ”The basics of cyber warfare: understanding the fundamentals of cyber warfare in theory and practice”, Elsevier, Inc, United States of America.” 2013 [21a] p.11
24. M. Woodcock, ”APRA Regulation CPS 234: What is it and how does it apply to your organisation? ”, BDO August 2020, Available from: https://www.bdo.com.au/en-au/insights/cyber-security/articles/apra-regulation-cps-234-what-is-it-and-how-does-it-apply-to-your-organisation, accessed October 2020

Most essential of Eight