SECURE PASSWORDS: YOUR FIRST LINE OF DEFENSE

ACS-RECOMMENDED BEST PRACTICES FOR PASSWORD SECURITY

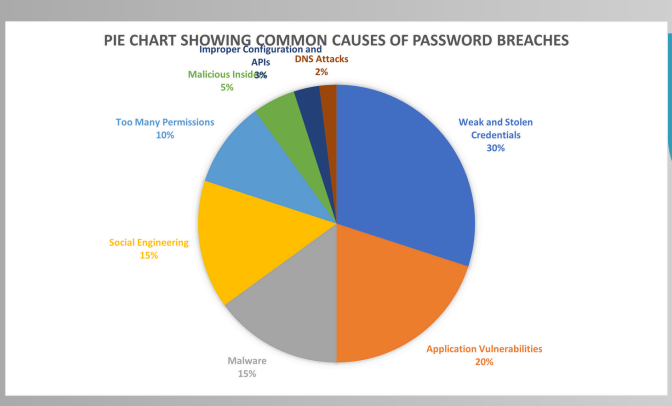
1 CREATING STRONG PASSWORDS

1. Length icon: Use at least 14 characters
2. Variety icon: Mix uppercase, lowercase, numbers, and symbols
3. Uniqueness icon: Create a unique password for each account
4. Unpredictability icon: Avoid personal information or common words

2 MANAGING PASSWORDS

Using a Password Manager Icon: A vault or safe

- Choose a reputable password manager
- Store all your passwords in the password manager
- Use the password generator feature for strong, unique passwords
- Ensure your master password is extremely strong and memorable
- Enable two-factor authentication for your password manager account



3 STATISTICS

4 PASSWORD DO'S AND DON'TS

For more information, visit the ACSC website:https://www.cyber.gov.au

ACSC Australian Cyber Security Centre

Stay safe online by keeping your passwords strong and secure

The Importance of an Up-to-Date Information Systems Security Baseline

Presenter: Damian Mutisya

Content

1. Vulnerability Assessment
2. Mitigation Planning
3. Vulnerability Scanning
4. Hardware and Systems Security
5. Information Systems Security Baseline
6. Relationship Between Terms

Section 1

Vulnerability Assessment

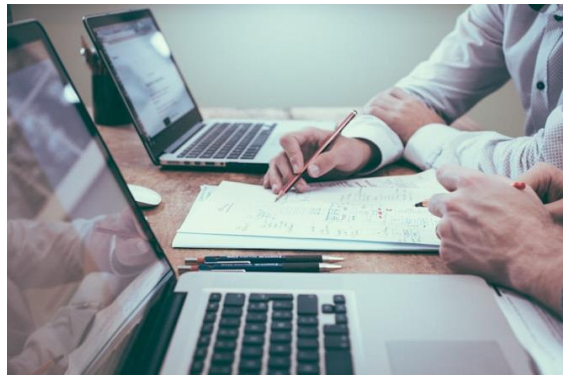
Understanding Vulnerability Assessment

Definition

The process of identifying, quantifying, and prioritizing vulnerabilities in a system. This involves a thorough examination of the system to uncover potential weaknesses that could be exploited by malicious actors.

Proactive Security

Regular assessments help in proactively securing systems. By continuously monitoring and evaluating the system, organizations can stay ahead of potential threats and mitigate risks before they become critical issues.



Comprehensive Strategy

Integral part of a comprehensive cybersecurity strategy. Vulnerability assessments are not standalone activities but are embedded within a broader security framework to ensure holistic protection.

Section 2

Mitigation Planning

Developing Mitigation Strategies

Strategic Development

Developing strategies and actions to reduce the impact of identified vulnerabilities. This involves creating detailed plans that outline specific steps to address and mitigate each identified risk.

Preparedness

Ensures the organization is prepared to respond to vulnerabilities. Effective mitigation planning means having the right resources and protocols in place to act swiftly when vulnerabilities are discovered.

Business Continuity

Minimizes potential impact on business operations. By addressing vulnerabilities promptly, organizations can avoid disruptions and maintain smooth operational flow.

Section 3

Vulnerability Scanning

Automated Vulnerability Detection

01

Automated Process

Automated process to scan systems for known vulnerabilities. This involves using specialized tools and software to continuously monitor the system for any signs of weaknesses.

02

Detection of Weaknesses

Detects potential weaknesses in the system. Automated scans can quickly identify vulnerabilities that might be missed during manual assessments.

03

Integrated Security Measures

Most effective when combined with other security measures. Vulnerability scanning should be part of a layered security approach, working in conjunction with other protective strategies.

Section 4

Hardware and Systems Security

Protecting Physical and Digital Assets

Threat Protection

Protection of hardware and systems from threats. This includes safeguarding physical devices as well as the software and data they contain.

Security Measures

Includes encryption, access controls, and regular updates. Implementing these measures helps to ensure that systems are secure from unauthorized access and potential breaches.

Cybersecurity Foundation

Foundational to any cybersecurity strategy. Robust hardware and systems security is essential for building a resilient and secure IT environment.

Section 5

Information Systems Security Baseline

Establishing Security Standards

Security Requirements

Set of security requirements to ensure a minimum level of security across all systems. These standards provide a baseline that all systems must meet to be considered secure.

Consistent Framework

Provides a consistent security framework. A standardized approach ensures that all systems are protected to the same level, reducing variability and potential weak points.

Threat Reduction

Crucial for reducing the threat surface and protecting against emerging threats. By maintaining a strong security baseline, organizations can better defend against new and evolving cyber threats.

Section 6

Relationship Between Terms

Integrating Security Concepts

01

Identifying Weaknesses

Vulnerability Assessment identifies weaknesses. This initial step is crucial for understanding where the system is vulnerable.

02

Addressing Vulnerabilities

Mitigation Planning addresses these vulnerabilities. Once weaknesses are identified, mitigation plans are developed to address and rectify them.

03

Detecting New Weaknesses

Vulnerability Scanning detects new weaknesses. Continuous scanning ensures that new vulnerabilities are quickly identified and addressed.

Thank You

Contact: damian@Bolding.com

What is phishing?

•Phishing is a type of cyber attack that uses deception to steal sensitive information
•Attackers pose as trusted entities to trick victims into revealing data or clicking malicious links
•Common targets: login credentials, financial information, company secrets
•Can occur via email, text messages, social media, or phone call

Familiarize yourself with phishing attacks

- Based on our recent phishing simulation:
1. HR: 75% phishing success rate
2. Marketing: 38% phishing success rate
- These teams are our primary focus for improved security awareness.

Learn to spot phishing emails

- Check the sender's email address carefully
- Be wary of urgent or threatening language
- Look for spelling and grammar errors
- Hover over links before clicking to see the true destination
- Be cautious of unexpected attachments
- If in doubt, verify requests through official channels

Common Phishing Tactics

- Impersonating known contacts or organizations
- Creating a sense of urgency or fear
- Offering deals that seem too good to be true
- Using generic greetings like "Dear Sir/Madam"
- Requesting sensitive information via email
- Directing you to fake websites that look legitimate

How do we stop getting phished?

- Stay informed about current phishing techniques
- Use strong, unique passwords for each account
- Enable two-factor authentication when possible
- Keep software and systems up-to-date
- Be cautious when sharing personal information online
- Report suspicious emails to IT security
- When in doubt, don't click or respond – verify independently