Cyber security

- Cyber awareness session on "cyber crime & safety" by police department.
- Cyber safe praetors
- Display of posters / roomers' on "cyber crime & best pri…" for awareness / possibility in campus & places
- Display reputation leaflet to all the students about cyber awareness & hygienic for institutions.

10 steps to an effective approach to cyber security

1. Risk management regime

- Assess the risks to your organisation's information and systems by embedding an appropriate risk management regime. This should be supported by the Board and senior managers. Ensure that all employees, contractors and suppliers are aware of the approach and any applicable risk boundaries.
- **2. Secure configuration**
- Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems.
- You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

3. Network security

- Connections from your networks to the Internet and other partner networks, expose your systems and technologies to a potential attack.
- Reduce the chances of your systems and technologies being attacked by creating and implementing simple policies and appropriate architectural and technical responses. Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

4. Managing user privileges

- If users are provided with unnecessary system privileges or data access rights, then the risk of misuse or compromise is increased. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role.

The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

5. User education and awareness

- Users have a critical role to play in their organisation's security. It is important to educate staff on the potential cyber risks, to ensure users can do their job as well as help keep the organisation secure.

6. Incident management

- All organisations will experience security incidents at some point.
- Investment in creating effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.

7. Malware prevention

- Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, this could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies.

8. Monitoring

- System monitoring aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

9. Removable media controls

- Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

10. Home and mobile working

- Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. Risk based policies and procedures that support mobile working or remote access to systems that are relevant to users, as well as service providers should be created. Train users on the secure use of their mobile devices in the environments they are likely to be working in.

PENIEL PAULDOSS

Digitally signed by PENIEL PAULDOSS
Date: 2024.03.10 22:15:28 +05'30'