LECTURE 6

SECURITY POLICIES, STANDARDS AND COMPLIANCE

1. What are the types of policies?

* Acceptable Use Policy
* Privacy Policy
* Password Policy
* Wireless Policy
* Social Media Policy
* Rules of behavior for personnel.
* Should be specified on what to keep private and what is not .
* Define standards for password complexity and strength.
* Defines what device can connect to the wireless network.
* Defines how employees can use social media networks.

Acceptable Use policy:

* Sending sensitive files and passwords over email.
* Using weak passwords
* Leaving sensitive documents without any supervision
* Using workstation to play games which might download malware.
* Official policy of hoe employee should or should not use company property.

1. What are the Risk Response Techniques?

* Acceptance
* Avoidance
* Mitigation
* Deterrence
* Transference
* This involves acknowledging a risk and deciding to proceed without taking any action to mitigate it.
* This technique eliminates the risk entirely by changing plans or actions to prevent the risk from occurring.
* Mitigation aims to reduce the likelihood or impact of a risk.
* Involves creating policies or systems that discourage risky behavior or the exploitation of vulnerabilities.
* the risk is shifted to a third party, such as through insurance or outsourcing certain operations.

1. What are the passwords policies?

* Passwords length
* Passwords complexity
* Password history
* Password reuse

Access Control Issues:

* Authentication Issues
* Permissions Issues
* Access Violations
* Check for configuration changes to authentication mechanisms.
* Check for configuration changes to authorization mechanisms.
* Ensure users and groups don’t have access to resources they shouldn’t.

Personal Issues:

* Policy violation
* Social media and personal email use
* Social engineering
* Insider threat
* Determine the policy item that was violated
* Ensure that your personal info is protected on social media
* Educate employees about common social engineering attacks, such as phishing emails or fake phone calls.
* Manage personnel to avoid one person having too much power.

Software Issues:

* Unauthorized software
* Unlicensed software
* Outdated software
* Check installation logs, trace its source, analyze it in a sandbox, and run an anti-malware scan.
* Check if it breaks help ands, see what features are missing, look for other software that can help, and buy the right licenses from the vendor.
* Programs that no longer receive updates or support, making them vulnerable to security risks and compatibility issues.