FOUNDATIONS IN IT SECURITY: SECURITY AUDIT

COMPUTER SYSTEMS SECURITY

GORDON | REYNOLDS (2019)

TODAY ….

Today we will overview conducting a basic and simple security audit., which includes:

- Scoping the Security Perimiter
- Defining the Threats
- Risk Scoring
- Assessing Security Posture
- Remediation

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: STARTING A SIMPLE SECURITY AUDIT

GORDON | REYNOLDS (2018)

SECURITY AUDITS

- What steps are necessary to defends an organisations assets in an optimal framework?
- Conducting automated and continuous security assessments of a network environment is important.
  - It provides both pro-active and preventative security measures.
- Still, it is advantageous to kick things off with a simple, yet crucial, security audit.
- When undertaking an initial security audit, it is important to use the most up-to-date compliance requirements to uphold security protocols.

GORDON | REYNOLDS (2018)

SECURITY AUDITS

- Security Audit in 5 Simple Steps:
  - **The Scope of the Security Perimeter**
  - **Defining the Threats**
  - **Prioritizing and Risk Scoring**
  - **Assessing the Current Security Posture**
  - **Formulating Automated Responses and Remediation Action**

GORDON | REYNOLDS (2018)

THE SCOPE OF THE SECURITY PERIMETER

- The first step in the auditing process is to clearly define the scope of the audit.
- For most companies and organisations, this will include both managed and unmanaged devices and machines.
  - Managed devices will encompass a list of computers, machines, devices and databases that belong to the company directly, which contain sensitive company and customer data.
  - Additionally, in a world that includes BYOD policies and IoT connected devices and machines, as well as contractors and visiting guests, the unmanaged segment of the audit should be positioned to continuously update visibility of all connected endpoints. Without clear visibility, it is impossible to create segmentation and remediation procedures.

GORDON | REYNOLDS (2018)

THE SCOPE OF THE SECURITY PERIMETER

- The security perimeter must include definitions relating to software that is allowed and not allowed so as to define a software perimeter as well.
- Finally, the scope should include all access layers:
  - wired, wireless and VPN connections.
- In this manner, the scope of the audit will ultimately include all software and devices, in all locations, so as to ultimately define the security perimeter for the company.

GORDON | REYNOLDS (2018)

DEFINING THE THREATS

- The next step is to list potential threats to the security perimeter.
- Common threats to include in this step would be:
  - **Malware** – worms, Trojan horses, spyware and ransomware – the most popular form of threats to any organisation in the last few years.
  - **Employee exposure** – making sure that employees in all locations change their passwords periodically and use a certain level of sophistication; (especially with sensitive company accounts) as well as protection against phishing attacks and scams.

GORDON | REYNOLDS (2018)

DEFINING THE THREATS

- **Malicious Insiders** – once onboarding has taken place, there is the risk of theft or misuse of sensitive information.
  - - employees, contractors and guests
- **DDoS Attacks** – Distributed Denial of Service attacks happen when multiple systems flood a targeted system such as a web server, overload it and destroy its functionality.
- **BYOD and IoT** – these devices tend to be somewhat easier to hack and therefore must be completely visible on the network.
- **Physical breaches and natural disasters** – less common but extremely harmful when they occur.

GORDON | REYNOLDS (2018)

PRIORITISING AND RISK SCORING

- There are many factors that go into creating the priorities and risk scoring.
  - **Cyber security trends** – working with a network access control system in place that factors in the most common and current threats along with the less frequent, could save you and your CISOs a lot of time and cut costs, while at the same time defending the organization in an optimal framework.
  - **Compliance** – includes the kind of data that is to be handled, whether the company stores/transmits sensitive financial or personal information, who specifically has access to which systems.
  - **Organisation history** – If the organisation has experienced a data breach or cyber-attack in the past.
  - **Industry trends** – understanding the types of breeches, hacks and attacks within your specific industry should be factored in when creating your scoring system.

GORDON | REYNOLDS (2018)

ASSESSING THE CURRENT SECURITY POSTURE

- A ***Security Posture*** refers to the overall security status of an organisations assets.
  - These assets include software, hardware, networks, services and information.
  - A security posture may also include the controls and measures in place to protect the organisation from cyber-attack.

GORDON | REYNOLDS (2018)

ASSESSING THE CURRENT SECURITY POSTURE

- At this stage, an initial security posture should be available for each item included in the initial scope definition.
- Ideally, with the right access control systems in place, no internal biases affect your initial audit or any continuous risk assessments performed automatically later on.
- Additionally, making sure that all connected devices have the latest security patches, firewall and malware protection will assure more accuracy in your ongoing assessments.

GORDON | REYNOLDS (2018)

RESPONSES AND REMEDIATION ACTIONS

- Based on the discovers of the previous steps, a number of key solutions to include are:
- **Network monitoring**
  - Establishing continuous automated monitoring and creating automated risk assessments will lead to improved risk management.
  - Cyber offenders are typically working to gain access to networks. Activating software that automatically takes notice of new devices, software updates/changes, security patches, firewall instalments and malware protection is the best way for any organisation to protect itself.
  - Ideally your CISOs should be alerted to any questionable device, software, activity, unknown access attempts, and more, so as to be a step ahead of any harmful activity whether it is maliciously done or not.

GORDON | REYNOLDS (2018)

RESPONSES AND REMEDIATION ACTIONS

- **Software Updates**
  - Making sure that everyone on the network has the latest software updates and patches, firewalls etc.
- **Data Backups/Restores and Data Segmentation**
  - Data Backups and Restore Testing is crucial and can be relatively simple to establish.
  - Frequent data back-ups along with segmentation will ensure minimal damage should an organisation ever fall to malware or physical cyber-attacks.

GORDON | REYNOLDS (2018)

RESPONSES AND REMEDIATION ACTIONS

- **Employee education and awareness**
  - Training for new employees and continuous security updates for all employees to make sure best practices are implemented company-wide.
  - Training should include,
    - How to spot phishing campaigns,
    - Passwords and password complexity,
    - Two-factor (or multi-factor) authentication.

GORDON | REYNOLDS (2018)

TO CONCLUDE

- Completing these simple but crucial steps will bring your first security audit to a close.
- Next, it is common to proceed to establishing an ongoing automated risk assessment, management and controls to secure the company's assets for the short, medium and long terms.
- The first security audit, when done properly will serve as a touchstone for future risk assessments and self-audits.
- Monitoring all devices and machines as well as software over time is the best way to control the risks associated with a device and software security perimeter.
- The continuous fine-tuning of controls and processes will maintain ongoing visibility as well as the ability to properly assess your overall preparedness for cyber-threats along with the ability to manage risks and remediate attacks.

GORDON | REYNOLDS (2018)

TO CONCLUDE

- Due to the proliferation of wireless networks and mobile devices, through BYOD and IoT, the workplace has become, on the one hand, a more agile and flexible environment, increasing productivity and employee satisfaction, and on the other, a breeding ground for vulnerabilities and cyber risk.
- A Network Access Control (NAC) solution address the needed steps to audit your organisation's security while also providing intelligence into network behaviour.
- For some organisations, NAC is a must-have part of a robust self-auditing security mechanism. By controlling access to the network with a NAC solution, organizations control their exposure to a wide array of emerging digital business risks, keeping their organisational network healthy and secure.
- Now that you have completed your initial network security audit, you can focus your attention on keeping your network safe.
- A core factor in achieving that is to have full visibility and control of all devices connecting to the network in real time.

GORDON | REYNOLDS (2018)

SUMMARY ….

Today we looked at conducting a basic and simple security audit., which includes:

- Scoping the Security Perimiter
- Defining the Threats
- Risk Scoring
- Assessing Security Posture
- Remediation

GORDON | REYNOLDS (2019)