Understanding Cyber Security

Hellios Information Limited

August 2020

Understanding Cyber Security

Cyber security is an increasing threat across all industries. With advances in technology suppliers and buyers are having to adapt to new demands.

Threats which organisations may be faced with include:

Configuration management

The National Institute of Standards and Technology defines security configuration management as "The management and control of configurations for an information system with the goal of enabling security and managing risk."

Attackers are looking for systems that have default settings that are immediately vulnerable. Once an attacker exploits a system, they start making changes.

With a new zero-day threat revealed almost daily, signature-based defenses are not enough to detect advanced threats. To detect a breach early, organisations need to understand not just what is changing on critical devices but also be able to identify "bad" changes. SCM tools allow organizations to understand exactly what is changing on their key assets. By setting a gold standard configuration for your systems and continuously monitoring for indicators of compromise, organisations can quickly identify a breach. Early detection of a breach will help to mitigate the damage of an attack.

Network Security

Network security is a subset of cyber security which is concerned with protecting the IT infrastructure of an organisation and restricts access to it.

Both the terms are often used in conjunction with each other, network security is one aspect of information security which refers to the processes and techniques designed to protect any kind of sensitive data and information whether in print or electronic form from unauthorised access.

Misuse of assigned privileges

Privileged account abuse occurs when the privileges associated with a particular user account are used inappropriately or fraudulently, either maliciously, accidentally or through ignorance of company policies.

According to Verizon's 2017 Data Breach Investigation Report, abuse of privileged accounts is now the second most common cause of security incidents and the third most common cause of breaches.

In a typical scenario, privilege abuse is the direct result of poor access control: Users have more access rights than they need to do their jobs, and the organisation fails to properly monitor the activity of privileged accounts and establish appropriate controls.

How to improve your Cyber Security?

The Cyber Essentials accreditation is a Government backed scheme which enables suppliers to protect themselves from the most common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are now common-place, with both being recognised industry-standards which are used by buyers, for some contracts.

There are various ways to improve cyber security for companies of all sizes.

Control access

Make sure that individuals can only access data and services for which they are authorised. For example, you can:

- control physical access to premises and computers network
- restrict access to unauthorised users

- limit access to data or services through application controls
- restrict what can be copied from the system and saved to storage devices
- limit sending and receiving of certain types of email attachments

Use strong passwords.
Strong passwords are vital to good online security. Make your password difficult to guess by:

- using a combination of capital and lower-case letters, numbers and symbols
- making it between eight and 12 characters long
- avoiding the use of personal data
- changing it regularly
- never using it for multiple accounts
- using two factor authentication
-

Put up a firewall.

Firewalls are effectively gatekeepers between your computer and the internet, and one of the major barriers to prevent the spread of cyber threats such as viruses and malware. Make sure that you set up your firewall devices properly and check them regularly to ensure they have the latest software/firmware updates installed, or they may not be fully effective. Read more about firewalls in server security.

Use security software.

You should use security software, such as anti-spyware, anti-malware and anti-virus programs, to help detect and remove malicious code if it slips into your network. Discover how to detect spam, malware and virus attacks.

Update programs and systems regularly.

Updates contain vital security upgrades that help protect against known bugs and vulnerabilities. Make sure that you keep your software and devices up-to-date to avoid falling prey to criminals.

Monitor for intrusion

You can use intrusion detectors to monitor system and unusual network activity. If a detection system suspects a potential security breach, it can generate an alarm, such as an email alert, based upon the type of activity it has identified

Raise awareness.

Your employees have a responsibility to help keep your business secure. Make sure that they understand their role and any relevant policies and procedures and provide them with regular cyber security awareness and training.

Suppliers can register to become Cyber Essentials accredited through the government's official partner, IASME Consortium. For more information please follow https://iasme.co.uk/cyber-essentials/

There is also addition advice for organisations to maintain high standards of cyber security and increase their likelihood of obtaining Cyber Essentials via the National Cyber Security Centre website which can be found here: https://www.ncsc.gov.uk/cyberessentials/advice

If your company has not yet obtained Cyber Essentials, but wish to increase security, use the following guidance on how organisations can combat the threat posed by cyber-attacks: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary

Further information relating to Cyber Essentials can be found at:
https://www.ncsc.gov.uk/cyberessentials/resources

Hellios Information Limited