How do cyber security products work and what do I need?

In the past we traditionally just installed Antivirus and trusted that it protected us. Now attack technology has advanced and we need multiple services to protect us. Andy Morrison explains the various modules and how they help.

Endpoint Security

This is the software you install directly on your devices .

- **Next-Gen Antivirus & Firewall**
  This is the traditional anti-virus module that scans files as you open them, and also scans servers etc over night
- **DNS Security - Endpoint**
  91% (Heimdal info) of online threats use a DNS attack to redirect you to a dangerous site.
  DNS security constantly monitors your DNS requsts and block access to sites that have malicious code or are operated by attackers.
- **Next-Gen Antivirus & Firewall**
  The traditional anti-virus module that scans files as you open them, and also scans servers etc over night.
- **Ransomware Encryption Protection**
  This module constantly monitors disk activity and stops any processes that are attempting to encrypt data.. Unlike Antivirus, it isn't based on a dictionary of known viruses! It can spot unknown and new attacks.

Vulnerability Management

Often when you are attacked, the virus is accessing a known vulnerability on a PC that hasn't had updates applied. The update would have fixed a bug a bug in the operating system that is allowing malicious code to affect operation. The way to prevent this is to keep all computers up to date, however that means relying on users to constantly reboot and install updates. What happens if a faulty update is released? How do you monitor to check that updates are installed? This module keeps you safe by automating updates, centrally selecting which ones should install and automatically scheduling the process.

Priviledged Access Mangement (PAM) & Application Control (AC)

PAM works by preventing users from having admin priviledges unless manually requested and allowed.

Without admin priviledges a the configurations and files that can be accessed are limited. A user should never operate as an admistrator normally! If a user needs to install software or change a setting they first request admin access by clicking a button near the clock.

AC allows the IT team build a list of allowed software and prevent any processes from running that are not related to the list. It prevents viruses from running and keeps ylour licenses under control.

In combination, AC and APM Implement "Zero Trust" by only allowing known processes to run, and managing when something runs as an admin.

Suite 1, 1 Cardale Park, Harrogate, North Yorkshire, HG3 1RY

supportdesk@andisa.net | 01423 290029 | www.andisa.net

Cont.

Agent

All of these modules need controlling and displaying in one place to make them manageable. The agent listens for instructions and sends status updates to the central console to make life easy for the IT team.

Email Security

Full cloudbased email security works by confioguring the world to send your emails to the security system before it is delivered to you. It means that it is compared against a list of known spam senders, spam internet addresses and also scanned for viruses and spam alogrythms to prevent emails from being delivered if they look malicious.

The emails are also checked to make sure that they were sent from the address of the responsible mail server, and not from a different server impersonating them. This process is called SPF and DKIM.

Any email that fails a test is sent to quarantine.

Threat Action Centre (TAC)

The TAC is a portal accessed by the IT team to detect and respond to threats and alerts. It means they can fix problems quickly without having to visit a device.

The TAC can also be linked to a remote helpdesk or AI system to provide immediate response even out of hours. - true 24 * 7 protection for your users.

How to choose what to install

Each module provides a very different level of protection and so your own circumstances need to be taken into account.
If you have any form of complaince need then you probably need every module. Not only will you be most safe, you will have a traceable route to full compliance.

If you are still confused then why not arrange a discovery call with one of our senior members of staff.

Scan the barcode to arrange your free call.

Suite 1, 1 Cardale Park, Harrogate, North Yorkshire, HG3 1RY

supportdesk@andisa.net | 01423 290029 | www.andisa.net