**WHAT IS LAYERED SECURITY?**

Using several different cyber security solutions that work together to reduce the attack surface of a networked system.

**WHAT DO YOU NEED?**

- **Awareness solutions**
  - Am I using tech that helps enforce these policies?
  - Are my cyber security policies documented?
  - Are they reasonable?
  - Are my employees actually following the policies?

- **Tech solutions**
  - Falling for phishing attacks and other social engineering tactics
  - Bypassing security measures and installing malware directly on the system
  - Giving away credentials in phishing attacks
  - Posting secure information over social media

**WHERE ARE THE HOLES IN YOUR DEFENSES?**

A majority of IT admins and security practitioners believe there's a significant increase in endpoint risk because of:

- **Tech solutions**
  - Firewalls
  - Anti-attack software
  - Internet-facing applications
  - Traditional AV guards
- **Network Castle**
  - Fully updated and patched OS software helps keep the network secure.
- **Anti-malware Knights**
  - Targets new threats and cleans infections. Can also detect undesired software like PUPs, keeping them from spamming users or draining system resources.
- **Discovery times too long, known flaws not being patched, security policies not enforced or well-known, missing or poorly implemented encryption, lack of malware protection, weak wireless configurations, physical security flaws, unstructured information, legacy applications that are no longer supported, vendors and business partners that may not be fully secure.**

**WHAT ARE THE LATEST CHALLENGES?**

- **User Education (User Awareness)**
  - The user is the most important yet often the most neglected layer of security.
  - The user is the only layer of security that we can’t automate or bypass.
  - The user is the only layer of security that we have full control over.
  - The user is the only layer of security that we can actually work with.
  - The user is the only layer of security that we can start with.

**WHERE ARE THE HOLES IN YOUR DEFENSES?**

- **Policies not enforced or well-known**
- **Missing or poorly implemented encryption**
- **Lack of malware protection**
- **Weak wireless configurations**
- **Physical security flaws**
- **Unstructured information**
- **Legacy applications that are no longer supported**
- **Vendors and business partners that may not be fully secure.**

**WHAT LAYERS DO YOU NEED?**

- **Awareness solutions**
  - Am I using tech that helps enforce these policies?
  - Are my cyber security policies documented?
  - Are they reasonable?
  - Are my employees actually following the policies?

**Learn more at malwarebytes.com/articles**

Sources: