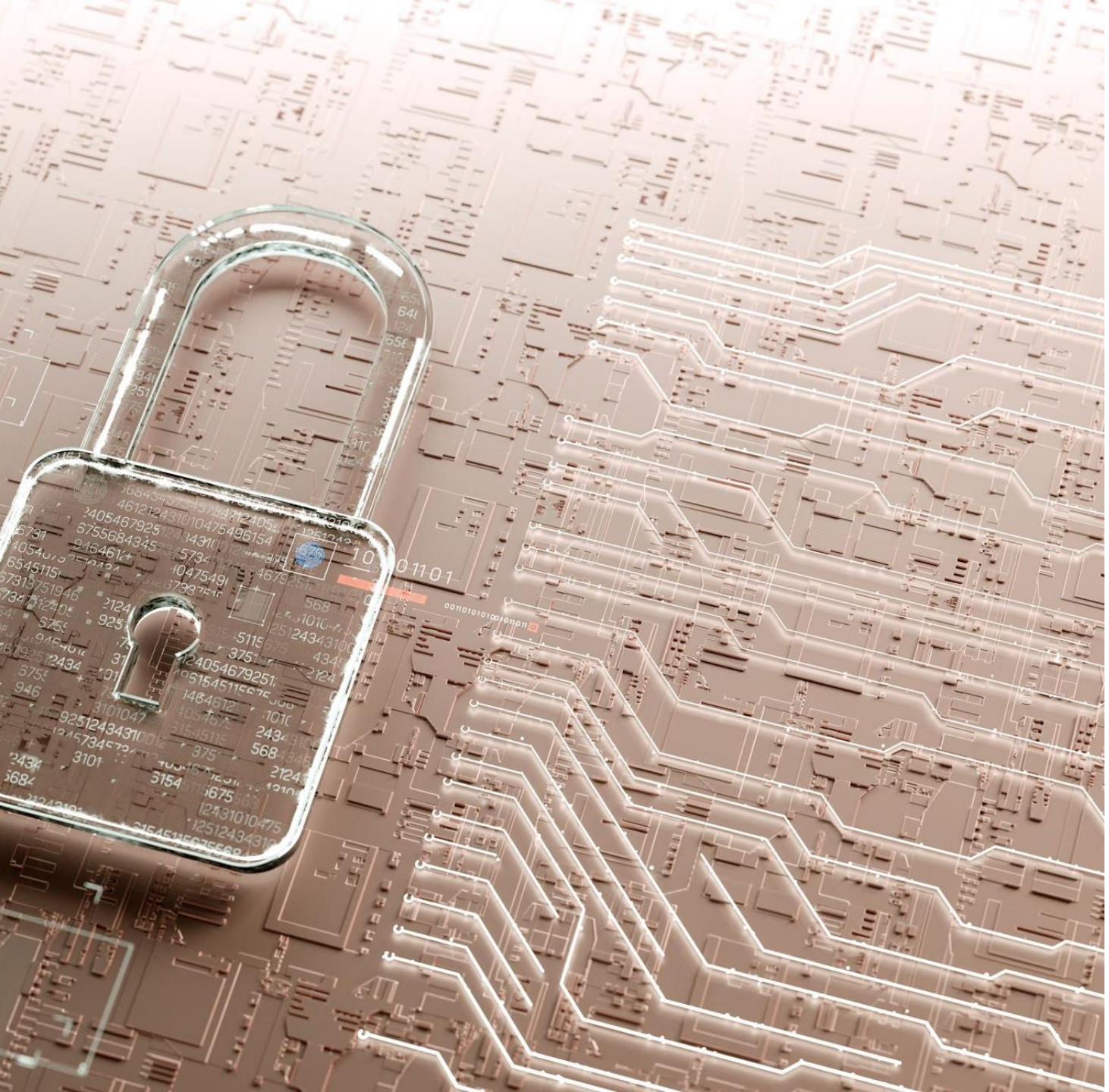

Endpoint Security

BY KAILEY OWENS AND LOGAN RILEY

What is Endpoint Security?

- An Endpoint is a hardware device that is connected to a network
  - Ex. Phone, Laptop, Printer
- Endpoint security is the defense of Endpoints
  - This includes protection against malicious entities, keeping systems up to date, and shielding against possible threats
- It is important to keep networks safe from their corruptible users: Endpoints

We need Endpoint Security

- Electrical devices are primary targets. Endpoint security prevents the loss of essential data, access, and control
- Protects individual systems
- Saves space and efficiency
  - System upkeep, updates
- It forces malicious activity to target a single device rather than a full system, forcing them to spend resources on a smaller catch

Prevent Malicious Actors

- One of the most important reasons for security; stop malware
- Firewalls, user permissions, and encryption
- Firewalls prevent suspicious activity from entering the system over a network
- Malicious or hacked users can only do so much with limited access to the system
- Important data, such as what could be found in files or disks, are heavily defended through encryption

Dealing with Vulnerabilities

- Devices are primarily attacked through active vulnerabilities. Endpoint security reduces vulnerabilities as much as possible
- Disable unused services or programs
  - This is why updating obsolete software reduces risk
- Replacing default passwords adds another layer of defense
- Open or unused ports are protected through closing them or installing firewalls

Activity Importance

- Our activity goes over a few ways to create Endpoint Security
- These examples show theoretical, real-world cases where Endpoint Security may be useful. Protecting our systems can be a remarkably simple process. Setting up these fundamental levels of security could be the difference between a healthy or broken machine

Sources

- learn.zybooks.com Chapter 9