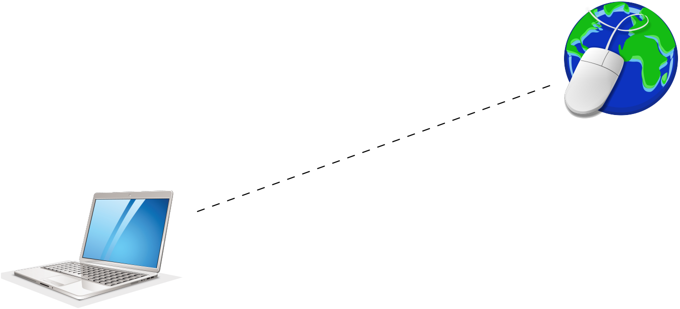
# Teleworking and cybersecurity in times of Covid-19: challenges and risks for SMEs

Ciprian Oprișa
ciprian.oprisa@cs.utcluj.ro

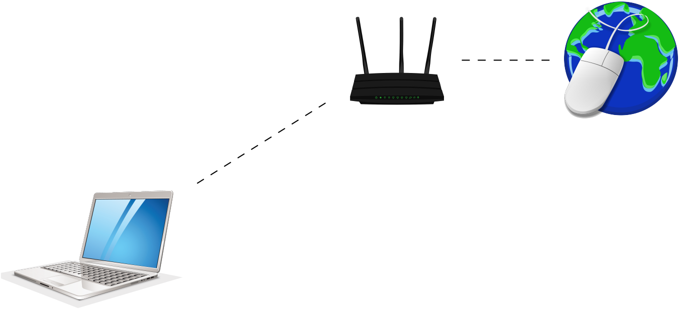
Cluj IT cluster
Technical University of Cluj-Napoca

July, 23rd 2020

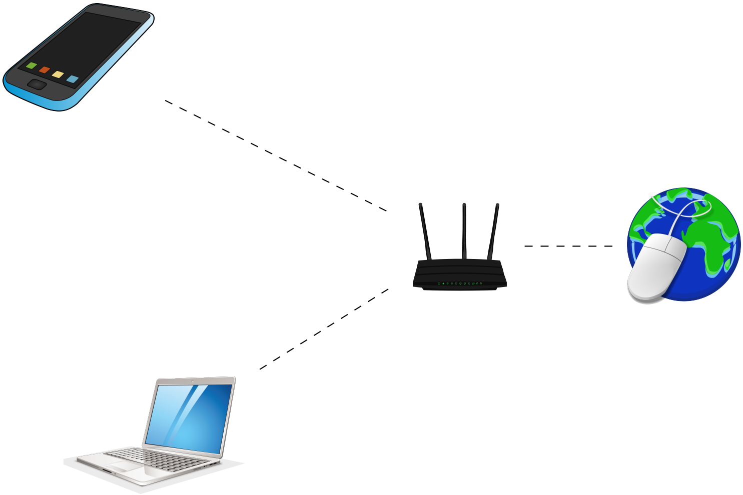
# Threats from the home network



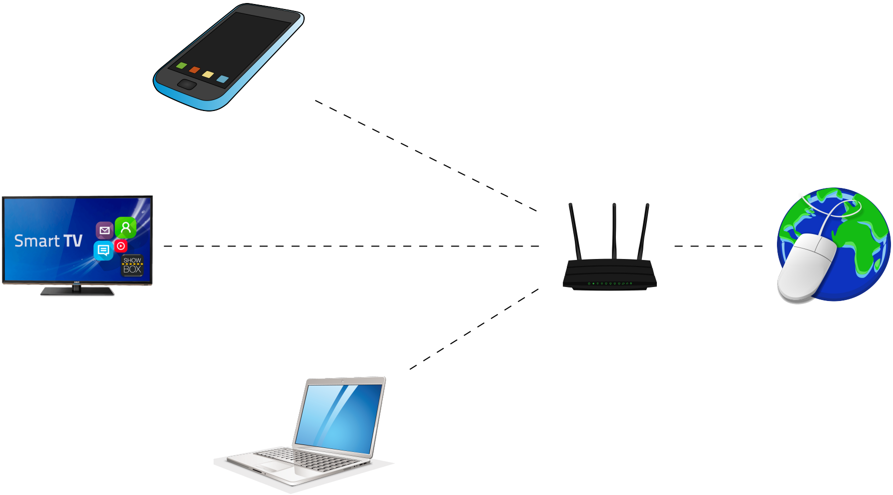
# Threats from the home network



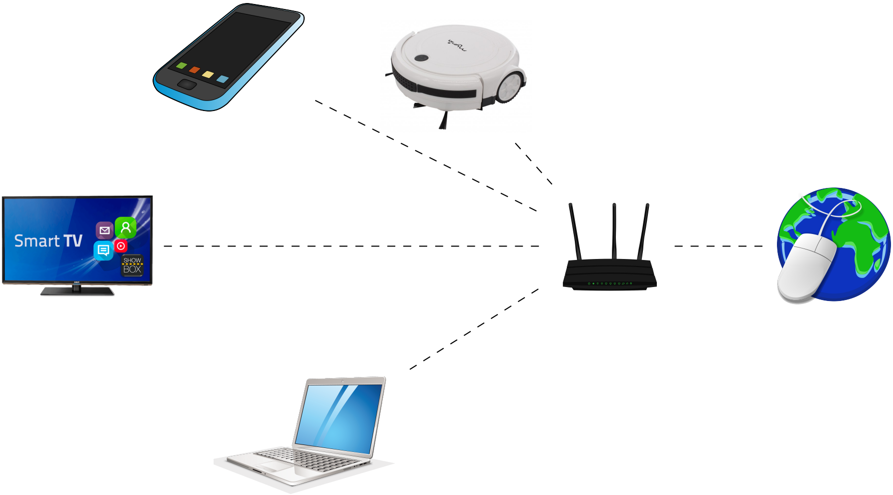
# Threats from the home network



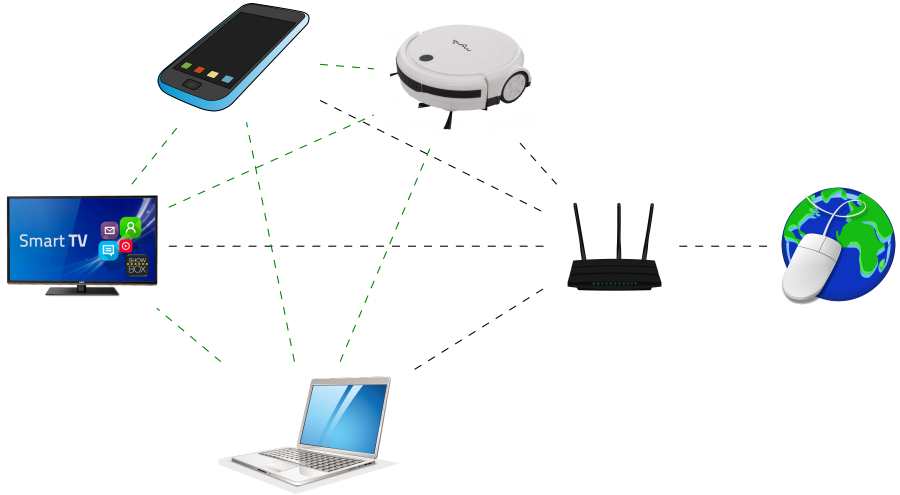
# Threats from the home network



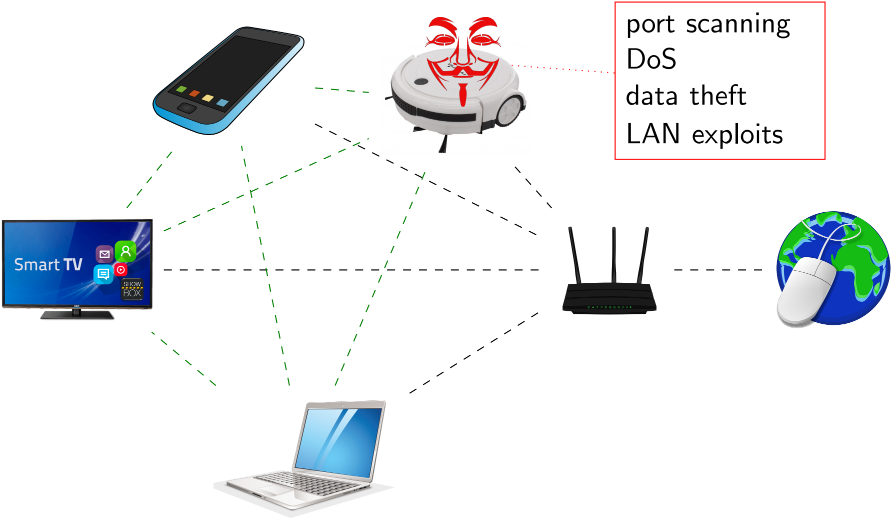
# Threats from the home network



# Threats from the home network

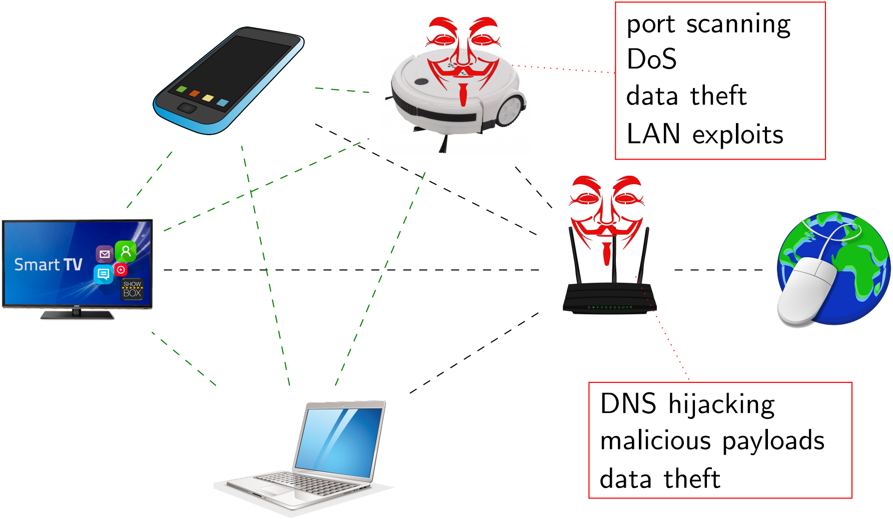


# Threats from the home network



port scanning
DoS
data theft
LAN exploits

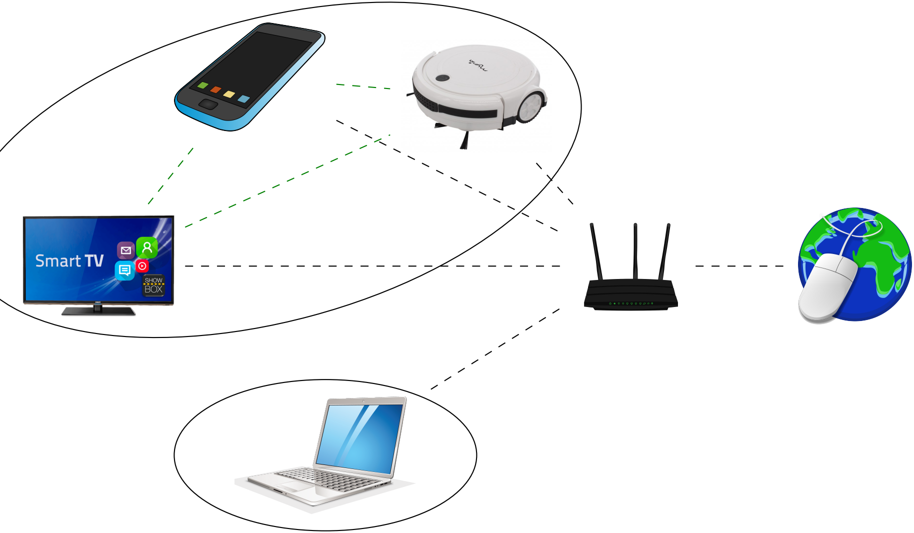
# Threats from the home network



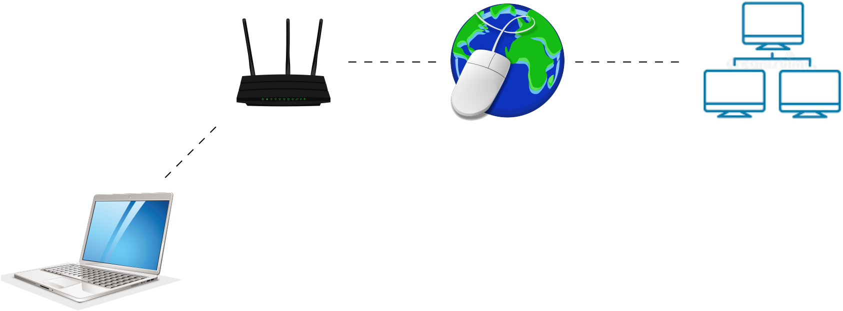
port scanning
DoS
data theft
LAN exploits

DNS hijacking
malicious payloads
data theft

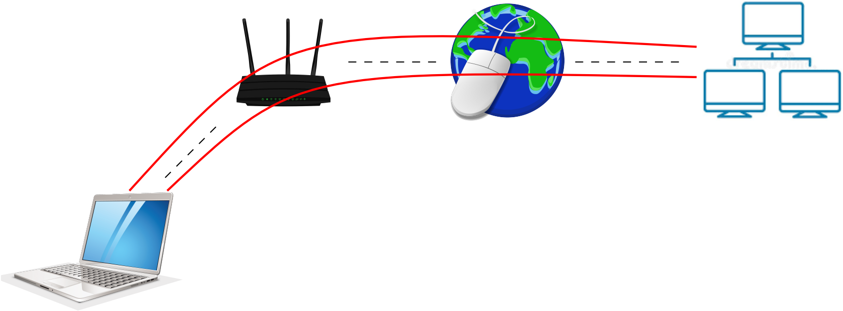
# Partial solution: VLAN / Guest network



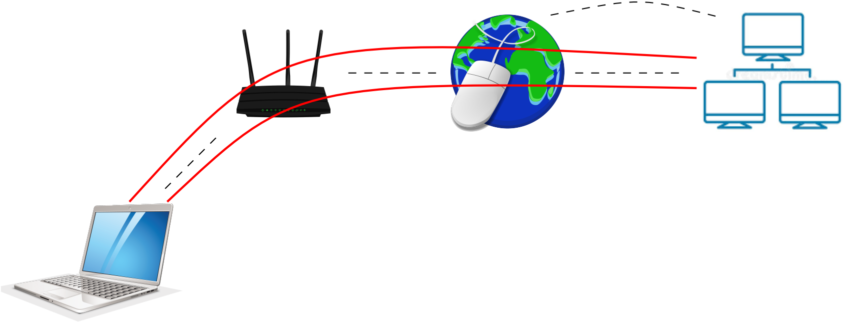
# Partial solution: full VPN



# Partial solution: full VPN



# Partial solution: full VPN



# Tighten security policy - Access Control Matrix

| | financial statements | web server | e-mail |
|---|---|---|---|
| developer | | R+W | X |
| accountant | R+W | | X |
| marketing | | | X |
| CEO | R | | X |

- an employee should only have access to the components required to do his job
- extra access can be granted upon justified requests

# Tighten security policy - Software Updates

To defend against exploits, we need to use the latest version for all programs.

# Tighten security policy - Software Updates

To defend against exploits, we need to use the latest version for all programs.

## Example - browser

The user navigates to a compromised website

- updated browser → infection only if downloads & executes malware
- unpatched browser → exploit, stealth infection

# Tighten security policy - Software Updates

To defend against exploits, we need to use the latest version for all programs.

## Example - browser

The user navigates to a compromised website

- updated browser → infection only if downloads & executes malware
- unpatched browser → exploit, stealth infection

## Example - Windows

Unpatched Windows, vulnerable to EternalBlue (2017 exploit).

- anyone from the LAN can execute code on our system

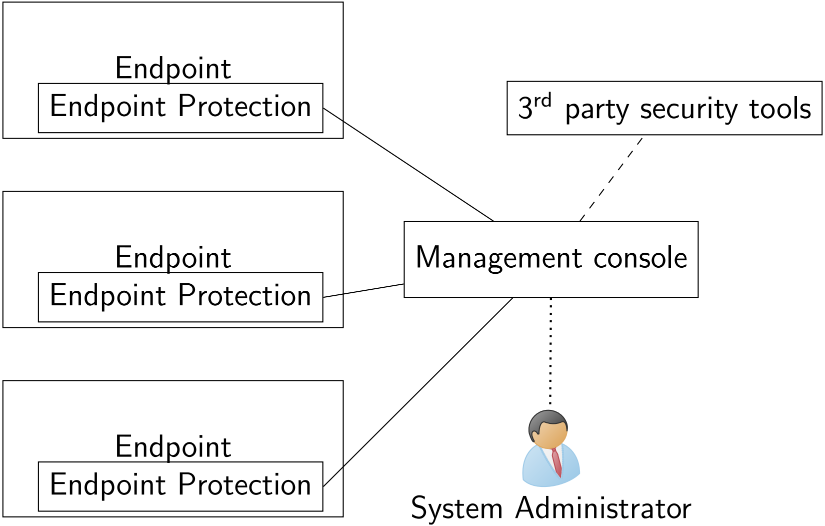
# Tighten security policy - Passwords

- good password

$$\left.\begin{array}{l}\text{hard to guess}\\ \text{lowercase, uppercase, digits \& symbols}\\ \text{changed frequently}\\ \text{different for every system}\end{array}\right\} \rightarrow \text{password manager}$$

- use 2FA
- only reset the password when 100% sure the request came from the user

# Use proper security solutions



# Security training

- know what to expect
- know how to recognize a security threat
- detect impersonation
- know what **not** to do