DEFENCE IN DEPTH

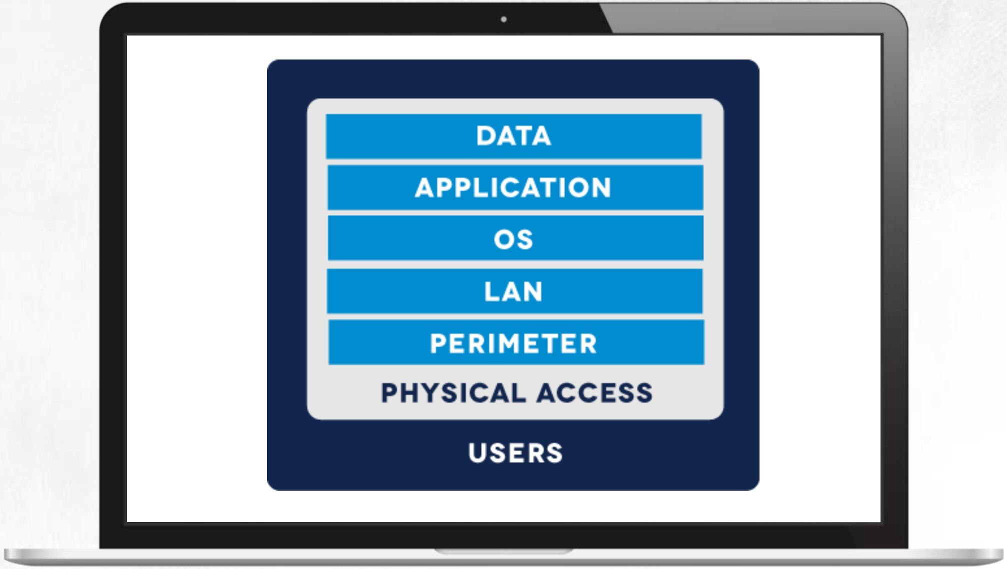
IT SECURITY ACADEMY

www.SecAcademy.com

DEFENCE IN DEPTH

THE DEFENCE IN DEPTH MODEL

originated as a military strategy. Rather than try to stop an enemy's offensive at a single, well-defended line, it might be better to make enemies bleed out by forcing them to fight for every resource or strategic entry point independently. Even if a first line of defence is broken, the attacker still has to break through the other lines, which gives you necessary time to regroup your forces and launch a counterattack



DATA

APPLICATION

OS

LAN

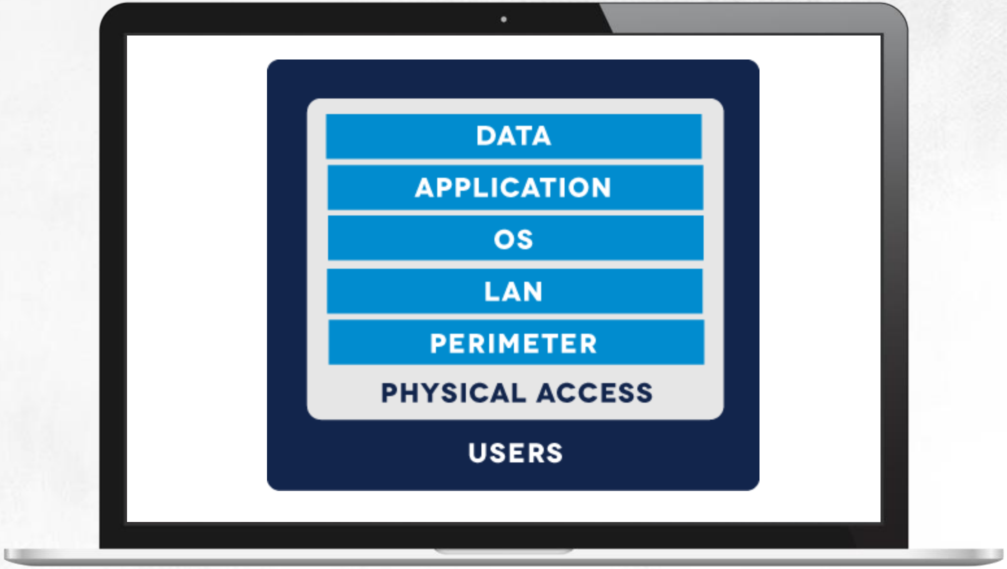
PERIMETER

PHYSICAL ACCESS

USERS

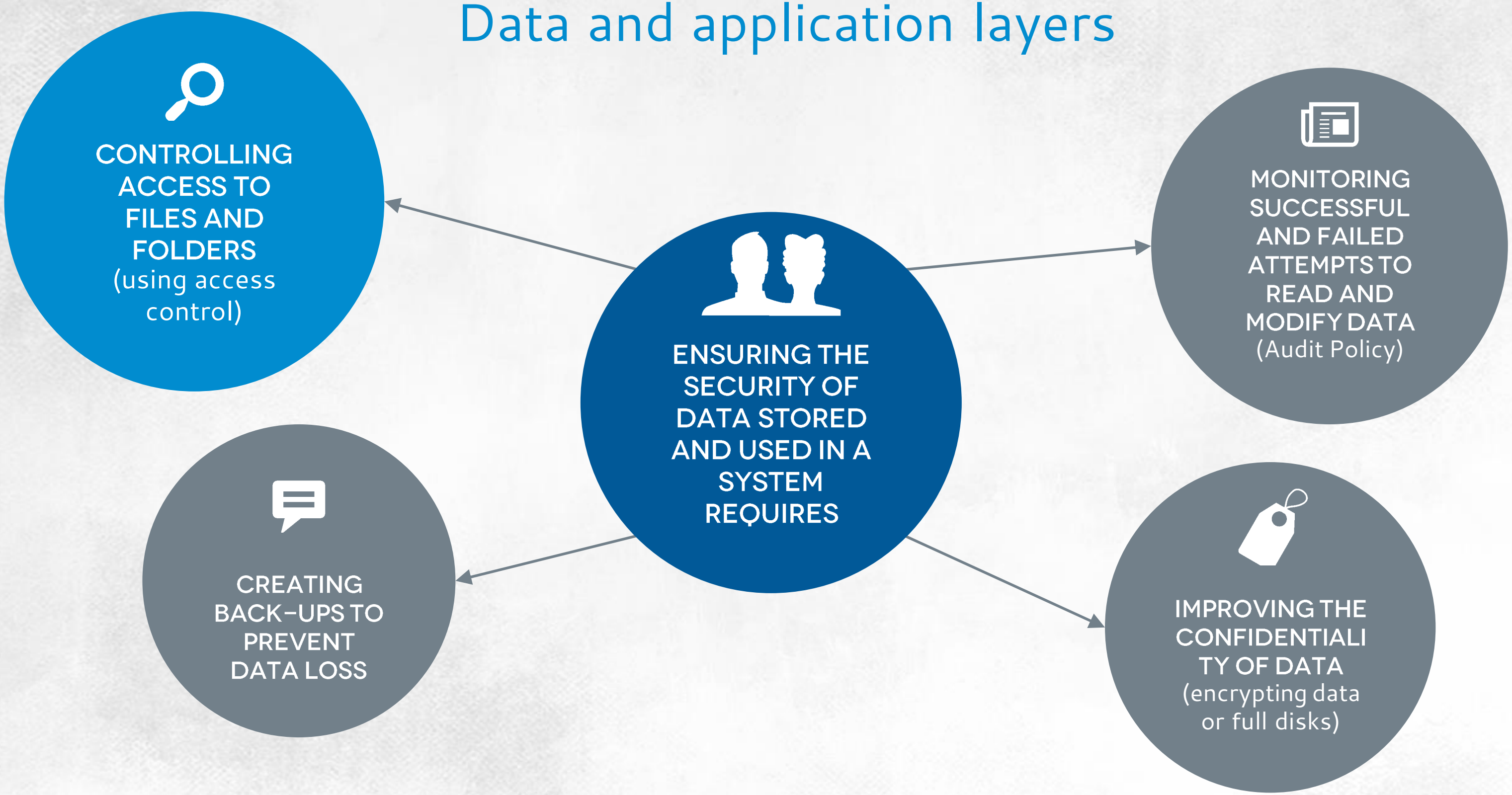
DEFENCE IN DEPTH

USING THE DEFENCE IN DEPTH TACTIC in IT is a way of looking at a computer system as a whole that is comprised of many layers that perform a variety of different functions. Even if total security of every layer is unattainable, you can apply protective measures to each of them independently and thus make the system effectively secure. This solution mitigates the risk of an attack attempt compromising the system and makes you more likely to discover an attack early and minimize the damage



DEFENCE IN DEPTH

Data and application layers



ENSURING THE SECURITY OF DATA STORED AND USED IN A SYSTEM REQUIRES

CONTROLLING ACCESS TO FILES AND FOLDERS (using access control)

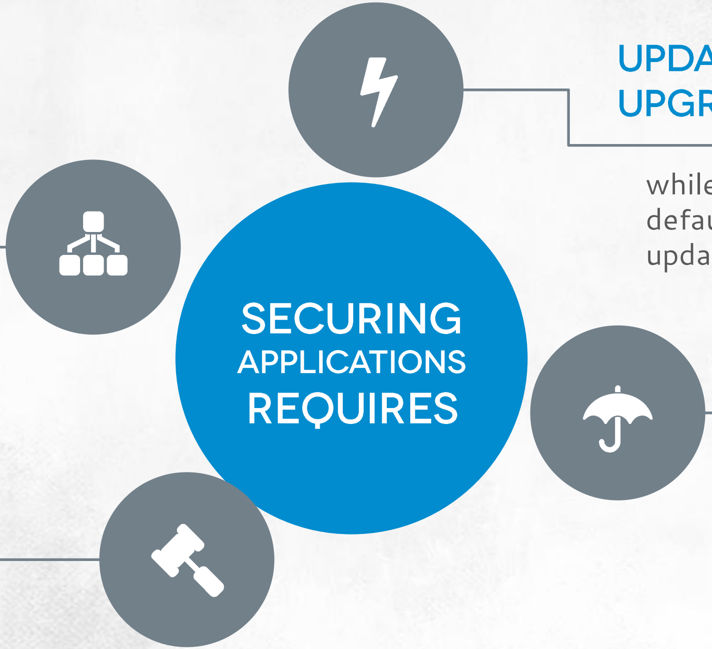
MONITORING SUCCESSFUL AND FAILED ATTEMPTS TO READ AND MODIFY DATA (Audit Policy)

CREATING BACK-UPS TO PREVENT DATA LOSS

IMPROVING THE CONFIDENTIALITY OF DATA (encrypting data or full disks)

DEFENCE IN DEPTH

Data and application layers



SECURING APPLICATIONS REQUIRES

PREVENTING USERS

from installing new programs. Every new program in a system makes it more vulnerable. Also, if an admin doesn't know an application has been installed, he will not be able to make it secure

UPDATING AND UPGRADING APPLICATIONS:

while system updates are on by default, many admins forget to update programs in the systems

MAKING USERS

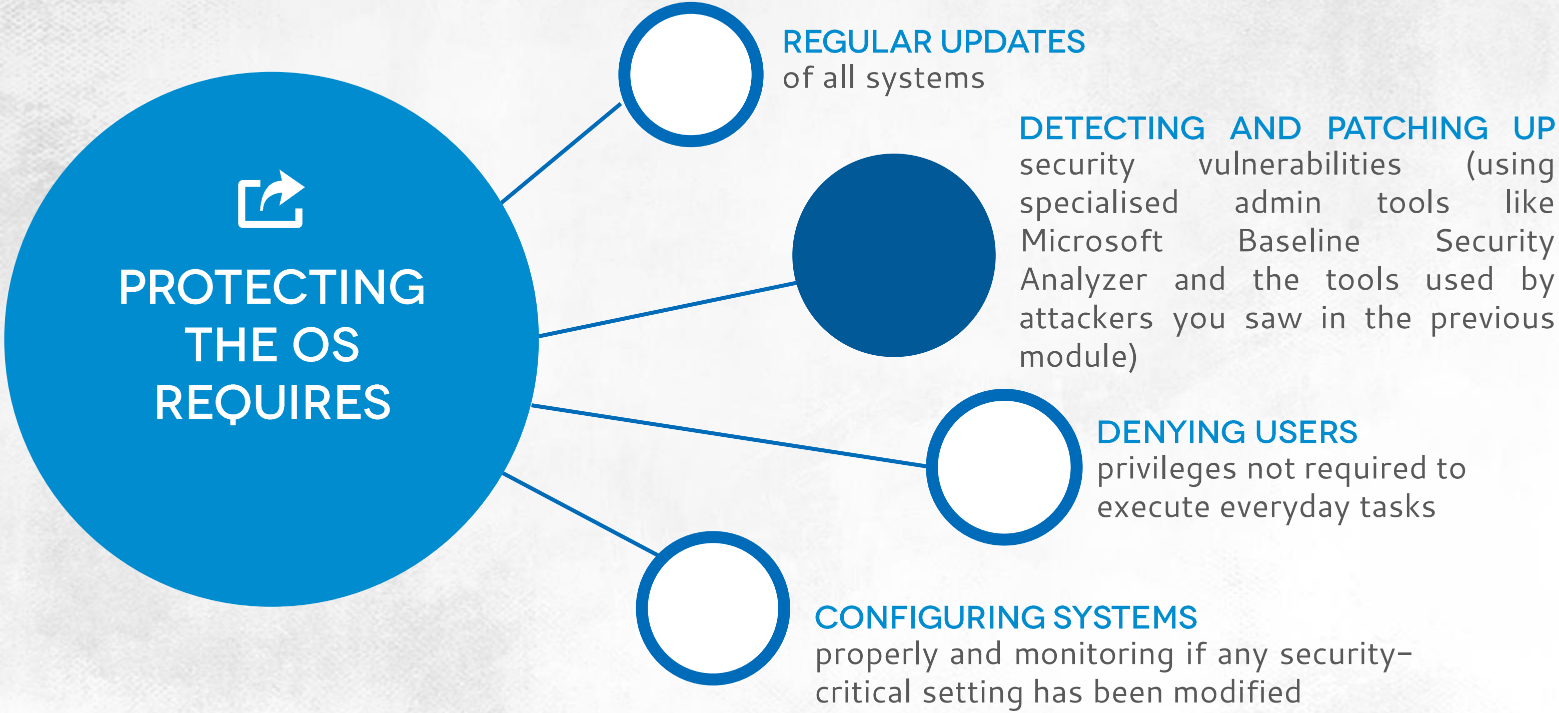
able to start only allowed applications (using Software Restriction Policies)

PROTECTION

from malware (antiviruses)

DEFENCE IN DEPTH

OS and LAN layers



PROTECTING THE OS REQUIRES

REGULAR UPDATES of all systems

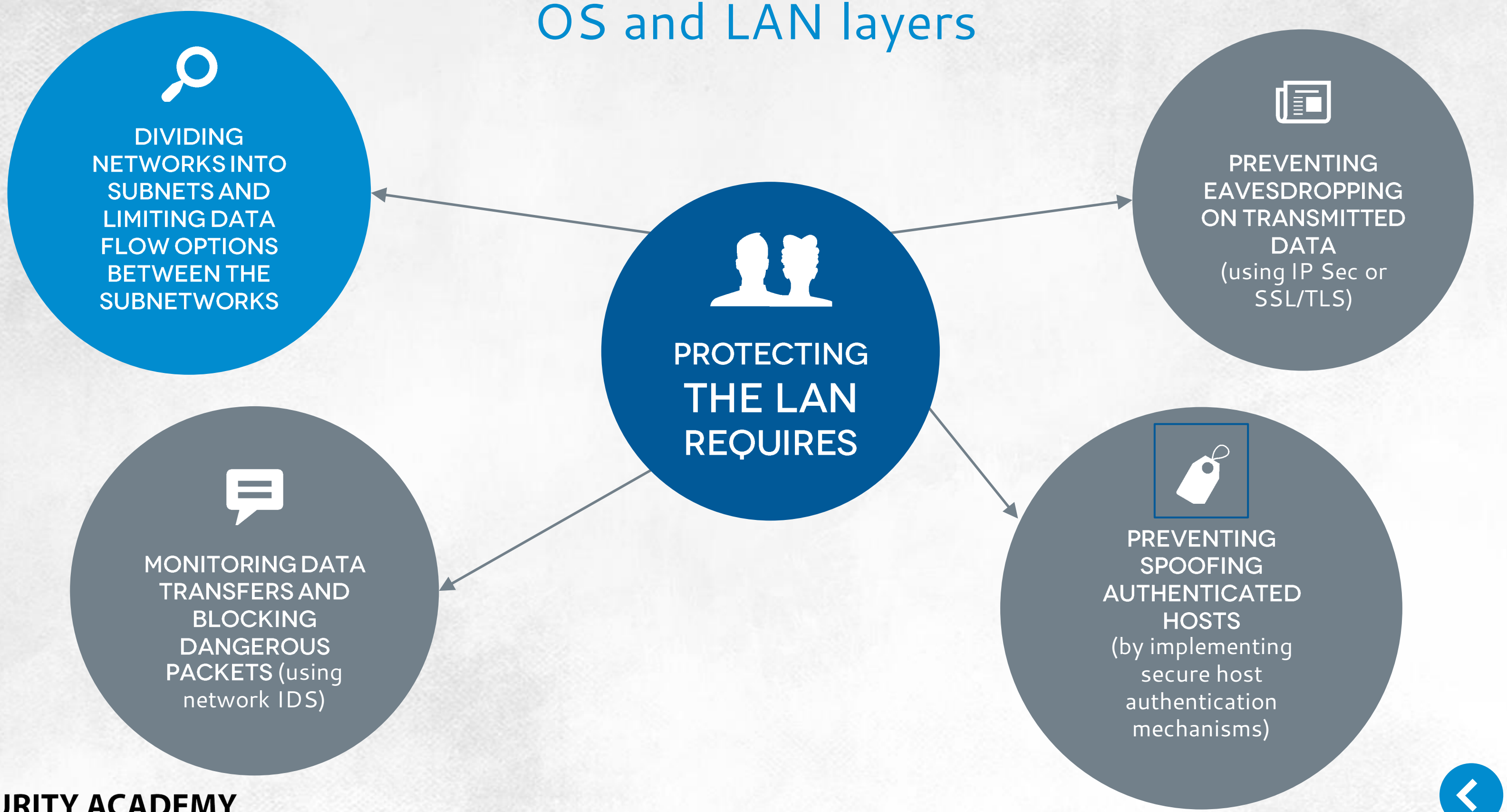
DETECTING AND PATCHING UP security vulnerabilities (using specialised admin tools like Microsoft Baseline Security Analyzer and the tools used by attackers you saw in the previous module)

DENYING USERS privileges not required to execute everyday tasks

CONFIGURING SYSTEMS properly and monitoring if any security-critical setting has been modified

DEFENCE IN DEPTH

OS and LAN layers



PROTECTING THE LAN REQUIRES

DIVIDING NETWORKS INTO SUBNETS AND LIMITING DATA FLOW OPTIONS BETWEEN THE SUBNETWORKS

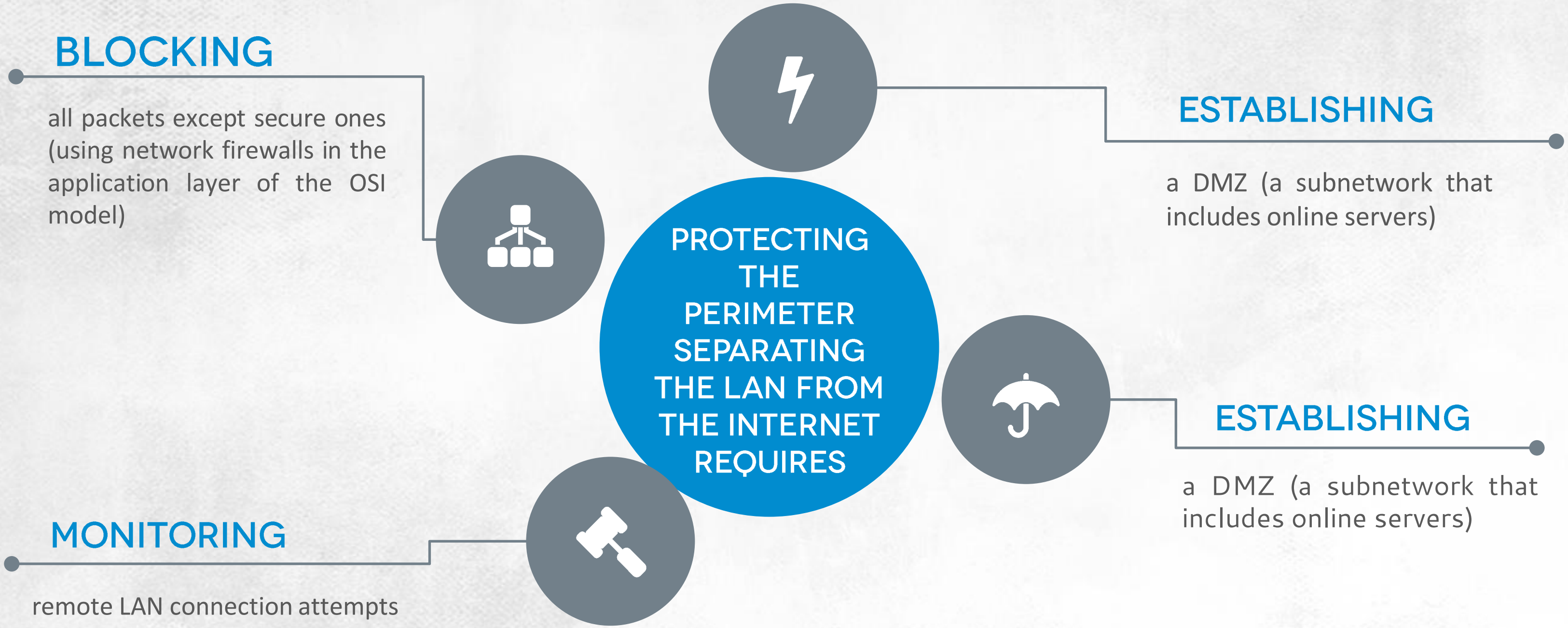
PREVENTING EAVESDROPPING ON TRANSMITTED DATA (using IP Sec or SSL/TLS)

MONITORING DATA TRANSFERS AND BLOCKING DANGEROUS PACKETS (using network IDS)

PREVENTING SPOOFING AUTHENTICATED HOSTS (by implementing secure host authentication mechanisms)

DEFENCE IN DEPTH

Perimeter and Physical Access layers



PROTECTING THE PERIMETER SEPARATING THE LAN FROM THE INTERNET REQUIRES

BLOCKING

all packets except secure ones (using network firewalls in the application layer of the OSI model)

ESTABLISHING

a DMZ (a subnetwork that includes online servers)

ESTABLISHING

a DMZ (a subnetwork that includes online servers)

MONITORING

remote LAN connection attempts

DEFENCE IN DEPTH

Perimeter and Physical Access layers

No technical solution, however, regardless of its price and sophistication, will protect you from physical local attacks. That's why you should:

- **RESTRICT ACCESS** to premises with computers, especially servers (security doors, smart card door locks)
- **CONTROL THE PEOPLE** who enter your company's premises (security personnel)
- **MONITOR EMPLOYEES** (cameras on premises)

The defence in depth strategy, unlike the classic computer security model that focuses primarily on remote attacks, covers all sorts of threats, including the human factor attacks, internal attacks and social engineering: these threats constitute the entry point of more than 85% of all intrusions

EXERCISE

Local Attacks Targeting Admin Password

DELETING ADMIN PASSWORD:
Offline NT Password and Registry Editor, Microsoft Diagnostics and Recovery Toolset

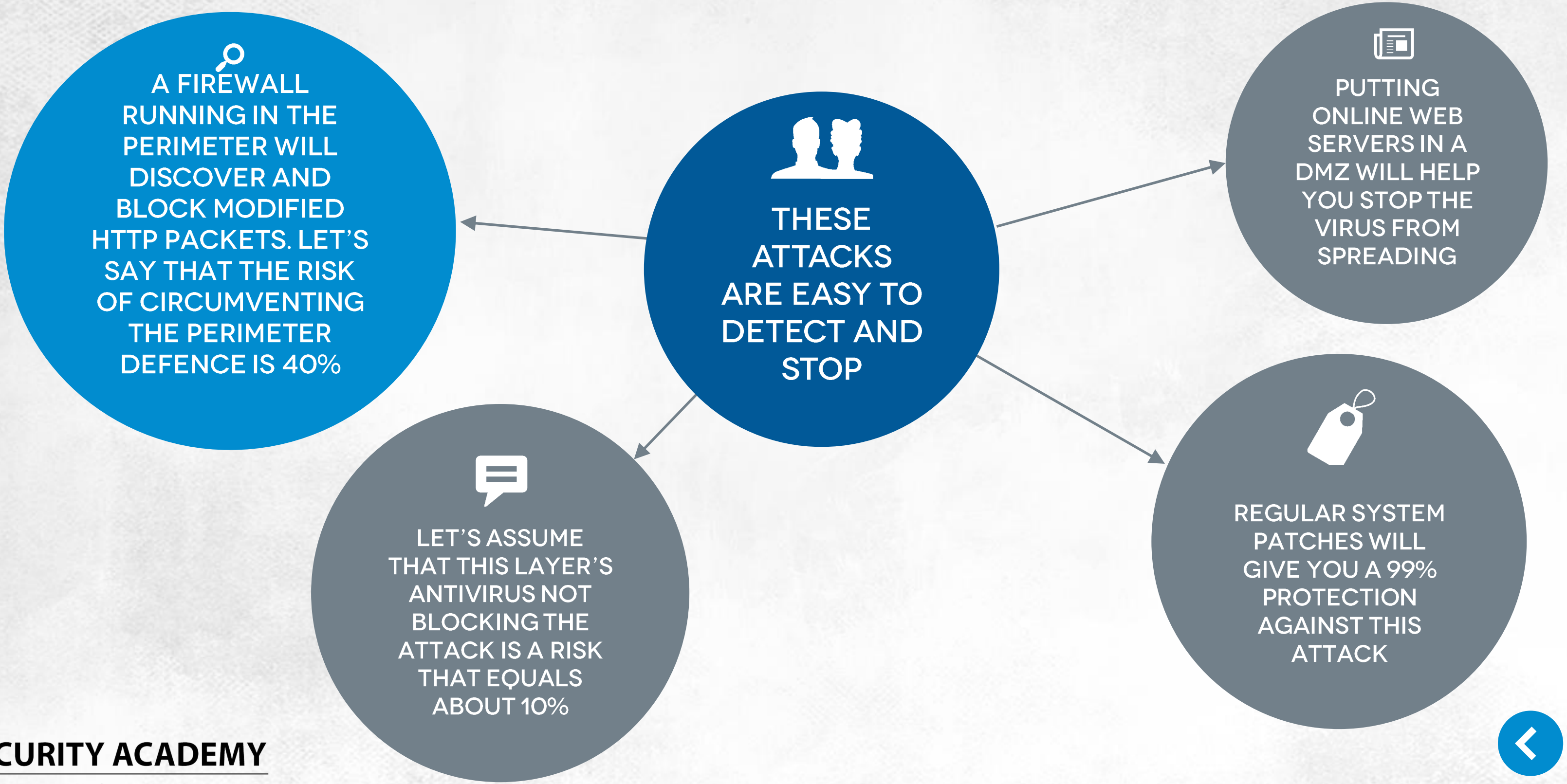
DEFENCE IN DEPTH

Possible scenario: Automated attack taregeting a service

IN 2001 CODE RED exploited a flaw in the indexing service in Microsoft IIS 4.0 and 5.0. The attack used crafted HTTP packets. A buffer overflow vulnerability of Idq.dll enabled the worm to disable the Windows File Protection system and to modify the registry, install a Trojan horse and start scanning for other vulnerable computers. The worm's payload was to run intermittent DDoS attacks against selected web servers

DEFENCE IN DEPTH

Possible scenario: Automated attack taregeting a service



THESE ATTACKS ARE EASY TO DETECT AND STOP

A FIREWALL RUNNING IN THE PERIMETER WILL DISCOVER AND BLOCK MODIFIED HTTP PACKETS. LET'S SAY THAT THE RISK OF CIRCUMVENTING THE PERIMETER DEFENCE IS 40%

LET'S ASSUME THAT THIS LAYER'S ANTIVIRUS NOT BLOCKING THE ATTACK IS A RISK THAT EQUALS ABOUT 10%

PUTTING ONLINE WEB SERVERS IN A DMZ WILL HELP YOU STOP THE VIRUS FROM SPREADING

REGULAR SYSTEM PATCHES WILL GIVE YOU A 99% PROTECTION AGAINST THIS ATTACK

DEFENCE IN DEPTH

Possible scenario: Automated attack taregeting a service

WHEN YOU MAKE YOUR DEFENCE mechanisms independent from each other (meaning if an attacker gets through one line, there are still others to break through), the risk of a successful attack may be assessed by multiplying the individual probability scores : 40%*1%*10%=0.04%

EVEN IF A SYSTEM IS COMPROMISED, the multi-layer strategy will keep it from spreading onto other web servers

DEFENCE IN DEPTH

Possible scenario: A virus with multiple propagation paths

An example is Nimda, a virus that infected computers by:

- **MASS-MAILING** attachments
- **SAVING INFECTED** files in shared folders
- **AN IIS VULNERABILITY** that could be exploited to run a TFTP server in a targeted host and send infected files to it

After compromising a computer, the worm added a guest account to the admin group and shared all the computer's drives in a network

DEFENCE IN DEPTH

Possible scenario: A virus with multiple propagation paths

Stopping a virus that uses multiple propagation methods is more complicated:

A UTM'S SMPT FILTER

will detect and block an email containing an infected attachment, except for messages sent over an encrypted connection (like a VPN) or from a local computer. Let's say that the risk of circumventing the perimeter defence mechanisms is about 70% for both cases

FIREWALLS

that protect computers by blocking incoming packets will prevent a virus from saving infected files to shared folders: the chance that this propagation method will be blocked is 75%

REGULAR SYSTEM

patches give you a 99% protection from exploiting IIS vulnerabilities

DEFENCE IN DEPTH

Possible scenario: A virus with multiple propagation paths

Stopping a virus that uses multiple propagation methods is more complicated:

LET'S SAY

that the risk that an application-layer antivirus will fail to block this attack is 10%

LET'S SAY

that being aware of the risks connected to opening email attachments means 75% of users will not fall victim to a mass-mailing virus

DEFENCE IN DEPTH

Possible scenario: An automated user-targeting attack

ONE OF THE VIRUSES THAT WAS DESIGNED to exploit users' security-ignorance was Mydoom. It infected a host as soon as a user clicked and opened a malicious file, and spread via emails and P2P networks. Once it compromised a system, the worm copied itself to the taskmon.exe file, modified the registry to make itself launched upon system start and installed a Trojan horse in the system.

THE ATTACKERS WERE ABLE TO REMOTELY control the infected systems and used them to run a distributed denial of service attack once in a month, targeting a selected web server

DEFENCE IN DEPTH

Possible scenario: An automated user-targeting attack

This type of attack should fail with well-protected systems:

- **A UTM'S SMTP FILTER AT THE PERIMETER WILL DETECT AND BLOCK** all messages containing an infected attachment. The perimeter will also block connections with P2P networks, even if established on port 80 or 443. Let's assume that the risk of circumventing the defence mechanisms at this layer is about 30%

- **LET'S ASSUME THE RISK** that an application-layer antivirus will fail to block this attack is 10%

- **LET'S SAY THAT A** well-configured email client that blocks executables will protect 85% of users (15% will save and run malicious files regardless of warnings)

- **LET'S SAY THAT** knowing about the risks connected to running untrusted files (like email attachments or P2P files) will mean 75% of users will not run a worm that is propagated in this way

DEFENCE IN DEPTH

Possible scenario: An automated user-targeting attack

AN CASE IN POINT: the Conficker pandemic. The versions of this virus propagated over LANs (using a Windows vulnerability described in KB 08-067) and removable media. According to Microsoft's stats, at the time of the pandemic 30 to 40% Windows systems were not updated, which means that more than half of compromised machines were infected using removable media.

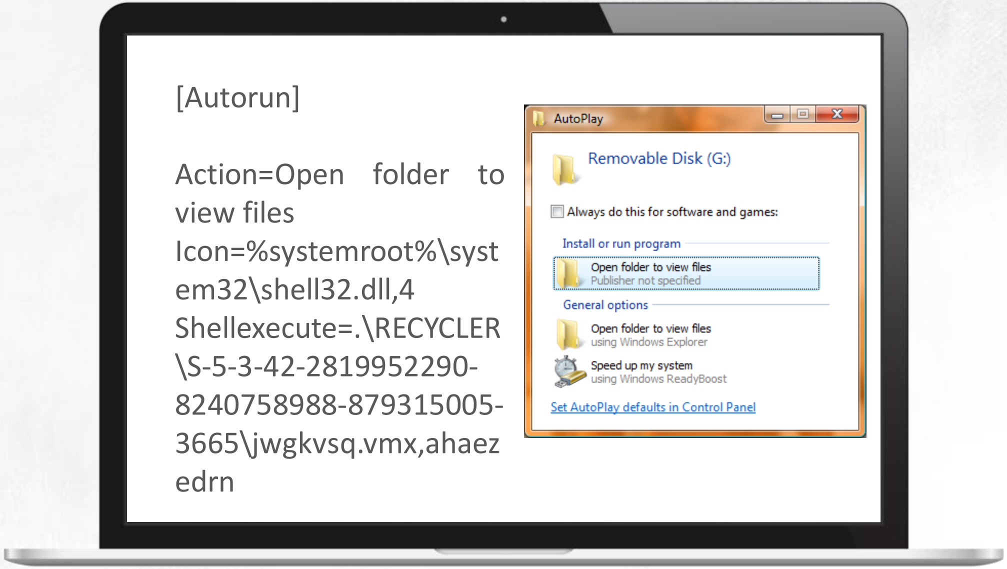
THE SCALE OF THIS ATTACK was immense: Conficker infected over 6 million computers with public IP addresses (each of these addresses could have been used for LANs comprising of multiple computers), while the damage caused was estimated at almost 10 billion dollars

DEFENCE IN DEPTH

Possible scenario: An automated user-targeting attack

MOST COMPUTER SECURITY measures prove fallible with this type of attack:

SINCE THE ATTACK is launched over the LAN, perimeter defence mechanisms are bypassed



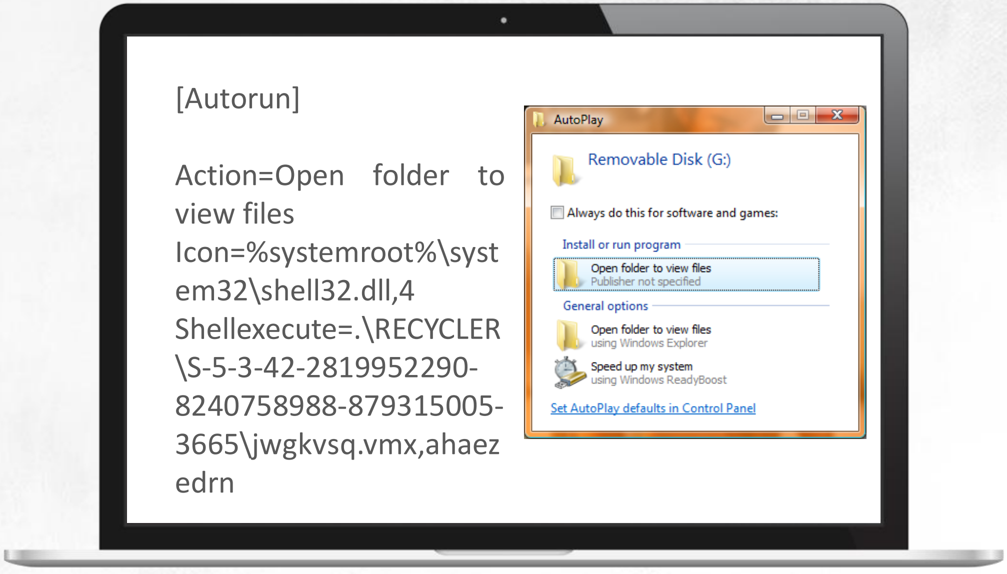
```
[Autorun]

Action=Open folder to view files
Icon=%systemroot%\system32\shell32.dll,4
Shellexecute=.\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx,ahaezedrn
```

DEFENCE IN DEPTH

Possible scenario: An automated user-targeting attack

BECAUSE IT IS A user-targeting attack, the countermeasures used for protecting other layers in the system will also fail, provided you don't disable connection for removable media on enterprise machines using Group Policy

THE ONLY WORKING solution against this attack is making users aware of the risks related to connecting untrusted drives to computers



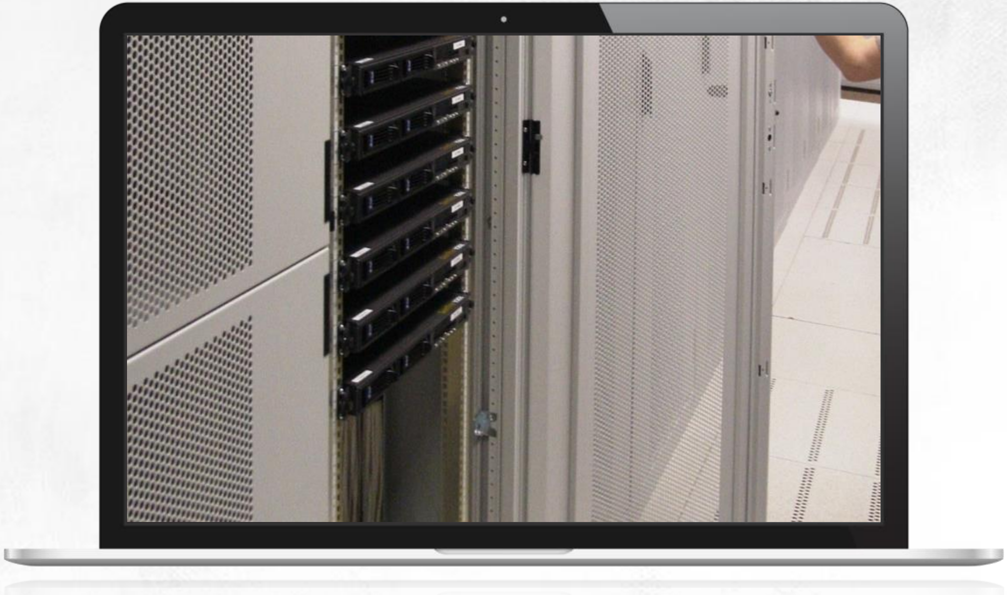
```
[Autorun]

Action=Open folder to view files
Icon=%systemroot%\system32\shell32.dll,4
Shellexecute=.\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx,ahaezedrn
```

DEFENCE IN DEPTH

Possible scenario: An attack targeting a service

LET'S NOW GO OVER a scenario in which an attack is targeted at an enterprise FTP server. Since it is an online server, the attackers will be able to identify its name and version easily. Let's say that this server had been found to contain some buffer overflow-type flaws.

EVEN IF THE FTP SERVER is updated, the attackers may try to see if they can find another vulnerability of this kind. Let's assume they have succeeded and launched a mass attack on your FTP server



DEFENCE IN DEPTH

Possible scenario: An attack targeting a service

A perimeter firewall will only prove effective if the packets used for the attack will share some atypical features. Let's say the risk of accepting malicious packets is 80%

Putting your FTP sever in a DMZ will not save you from this attack but can go a long way to restrict the damage. Let's say the risk of detecting this attack by your network IDS is 35%

A proper configuration of the FTP server will not protect you from an attack targeting a software vulnerability, but will make it harder for the attacker to gain control over the whole computer. Let's say the chance this attack will be discovered soon enough is 10%

DEFENCE IN DEPTH

Possible scenario: An attack targeting a service

Since the attack exploits a zero-day vulnerability, updating FTP servers regularly will not help you in any way

Since this attack is not mass-scale, antivirus vendors probably did not have enough time and chance to add the attack to their virus signature base. Let's say that a heuristic analysis run by an FTP server's antivirus gives you a 15% chance of detecting the attack

THANKS