Virtual Case Experience Cybersecurity

Model Work Task 4

1

Part 1

Network Segmentation I

The **network segmentation** not only logically groups cohesive systems into one zone but also creates secure passages between them. Every internal firewall works as check point, where a packet is challenged for its legitimacy which makes lateral movement much harder. The current trend is going more and more into a micro-segmentation of networks where the zones are broken down as far as it makes sense. It is also called a Zero Trust Architecture, because at every internal firewall the traffic is verified and not blindly trusted just because it's internal.

However, the firewalls allow for the configured protocols to pass through to the next zone. If for example the Domain Controller A was compromised, the attacker could use whitelisted, standard protocols to compromise more servers with very few indicators.

2

Part 2

Network Segmentation II