A traditional network is hard on the outside by focusing on protection against the threats from outside whereas soft on the inside, many companies using firewalls and tools such as Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) to monitor incoming traffic to protect their network, all of that focusing on external actors, however, let us assume that the network is already breached then, the intruder can access all network and data (Metivier, 2017).

Network segmentation is a technique to divide the network into smaller sections such as subnet for printers and data storage, with an independence every subnet has its access and security controls such as stop traffic between specific subnets consequently, the isolation in subnets network can limit the ability of threat to spread through the network if an intruder gets access to any part of the network, the other parts will not be compromised (Velimirovic, 2020).

According to (Onunkwo et al, 2019) segmentation in networks removes the visibility of packets, the outside attacker could not read or modify packets, by using this technique company preserving the integrity and confidentiality of their data.

References

Metivier, B. (2021) The Security Benefits of Network Segmentation. Available from: https://www.tylercybersecurity.com/blog/the-security-benefits-of-network-segmentation [Accessed 25 September 2021].

Onunkwo et al., I. (2019) *Cybersecurity Assessments on Emulated DER Communication Networks*. Sandia National Laboratories. Available from: https://www.researchgate.net/publication/332057688 [Accessed 25 September 2021]

Velimirovic, A. (2021) 7 Key Security Benefits of Network Segmentation. Available from: https://phoenixnap.com/blog/network-segmentation-security [Accessed 25 September 2021]