**Collaborative Discussion 1 – Peer Response 1 – Aldo Madrid**

Very good summary Aldo. With your example with Wannacry ransomware, you addressed one of the most widespread cyber attacks in history. Wannacry's story could be read like a crime thriller.

WannaCry is based on EternalBlue, an exploit of the MS17-010 vulnerability in Microsoft's NetBIOS (Heise, 2017). The United States National Security Agency (NSA) developed and used this vulnerability under the name EternalBlue for five years without informing Microsoft about the security vulnerability (Farand, 2017). Only after EternalBlue was stolen from the NSA did the agency inform Microsoft about the security breach. Microsoft then released updates to close the vulnerability in March 2017. However, these updates were only for the still supported operating systems Windows Vista and newer (Goodin, 2017).

Since the Windows XP operating system was not protected by the patch, the malware could cause such great damage. The WannaCry cyber attack in May 2017 affected over 230,000 computers in nearly 150 countries. Due to its scale, Europol has been described this cyber attack as an unprecedented event (BBC, 2017).

A large number of internationally operating companies were affected by the cyber attack. These include the Spanish telecommunications group Telefónica, the British National Health Service (NHS), the US logistics company FedEX and automotive groups such as Renault and Nissan, as well as the Chinese oil company PetroChina.

It is ironic that an agency like the NSA, which is responsible for the safety of its people, is responsible for causing such great national and global damage. On the other hand, such an incident shows the importance of cyber security in today's world and how important it is to keep the operating system up to date.

**References:**

Heise (2017) WannaCry: Microsoft liefert Sicherheits-Patches für veraltete Windows-Versionen. Available from: https://www.heise.de/newsticker/meldung/WannaCry-Microsoft-liefert-Sicherheits-Patches-fuer-veraltete-Windows-Versionen-3713417.html [Accessed: 17.08.2021]

Frarand, C. (2017) NHS cyber attack: Eward Snowden says NSA should have prevented cyber attack. Independent. Available from: https://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-edward-snowden-accuses-nsa-not-preventing-ransomware-a7733941.html [Accessed: 17.08.2021]

Goodin, D. (2017) NSA-leaking Shadow Brokers just dumped its most damaging release yet. ARS Technica. Available from: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/ [Accessed: 17.08.2021]

BBC (2017) Ransomware cyber-attack threat escalating – Europol. Available from: https://www.bbc.com/news/technology-39913630 [Accessed:17.08.2021]