Post by: Edward van Biljon

The SolarWinds hack that happened in March 2021 was a sophisticated attack. The attack not only left SolarWinds vulnerable but also the thousands of other companies that were also part of the attack and one of them being Microsoft as they make use of SolarWinds. Marcus Willet. (2021) Lessons of the SolarWinds Hack. Available from: https://www.tandfonline.com/doi/full/10.1080/00396338.2021.1906001 [Accessed 14 August 2021].

The attack was used to gain intelligence into big companies and Governments but it resulted in Microsoft Exchange being exploited. Many companies that make use of Microsoft Exchange were now vulnerable and from experience, the attacks brought down email systems in these organizations resulting in downtime but also loss of data and potentially having these attackers implement back doors for future attacks.

In the case of this cyber breach, multiple vulnerabilities were identified since March 2021 in Microsoft Exchange, each month new patches coming out to address the vulnerabilities. The supply chain was affected and this caused massive damage not only to SolarWinds and Microsoft's reputation but to all their clients as well.

It can be concluded that patch management is essential and should not be ignored when they are released. Clients rely on the vendor to ensure their systems are up-to-date and data is kept intact and not exposed to the internet for attackers to exploit.