WannaCry ransomware attack

The WannaCry ransomware attack occurred in May 2017 and was a significant global cyberattack. It targeted computers running the Microsoft Windows operating system, encrypting the data on those systems and demanding a ransom payment in Bitcoin to decrypt the files. The attack had a massive impact, affecting hundreds of thousands of computers in more than 150 countries. The WannaCry attack served as a wake-up call for the importance of cybersecurity on a global scale and underscored the potential consequences of failing to address vulnerabilities in widely used software systems.

Sony Pictures attack

The Sony Pictures attack refers to a high-profile cyberattack that occurred in late 2014, targeting Sony Pictures Entertainment, a subsidiary of Sony Corporation. The attack resulted in the theft of a significant amount of sensitive data, the leaking of unreleased movies, and the exposure of confidential corporate information. The attack was attributed to North Korean hackers and was allegedly motivated by the release of a comedy film called "The Interview," which portrayed a fictional assassination plot against North Korea's leader, Kim Jong-un.

Stuxnet attack

The Stuxnet attack is one of the most famous and complex cyberattacks in history. It was discovered in 2010 and is believed to have been in development and use for several years prior. Stuxnet is a sophisticated worm or computer virus that specifically targeted supervisory control and data acquisition (SCADA) systems, which are used to control and monitor industrial processes, particularly in critical infrastructure like nuclear power plants and water treatment facilities. The Stuxnet attack is a remarkable case study in state-sponsored cyberattacks and the use of cyberweapons for geopolitical purposes. It underscores the importance of cybersecurity for protecting critical infrastructure and the need for vigilance against advanced and persistent cyber threats.

SolarWinds cyberattack

The SolarWinds cyberattack, also known as the SolarWinds Orion compromise, was a highly sophisticated and widespread supply chain attack that was discovered in December 2020. This cyberattack targeted the software products of SolarWinds, a company that provides network monitoring and management tools to a wide range of organizations, including government agencies and businesses.

Petya and NotPetya attacks

Both the Petya and NotPetya attacks involved ransomware, but the 2016 Petya attack primarily focused on ransom payments, whereas the 2017 NotPetya attack had a more destructive and disruptive nature. The latter attack was also characterized by its use of a software update to propagate and its potential nation-state involvement. These attacks serve as reminders of the evolving and complex nature of cyber threats and the importance of robust cybersecurity measures. A NotPetya virus spreads on its own in a computer, but a Petya virus requires the user to open and download the malicious file. NotPetya is ransomware regardless of its author's abilities to decrypt computers because it prevents users from accessing their files or system and demands a ransom payment. Similarly, WannaCry is also a ransomware strain even though its authors may have the ability to decrypt computers.

Cosmos Bank cyberattack

The Cosmos Bank cyberattack is a notable banking-related cyberattack that occurred in August 2018. Cosmos Bank, based in India, is one of the country's oldest cooperative banks. The attack involved a sophisticated and coordinated effort by cybercriminals to steal millions of dollars from the bank's accounts. The attackers used a malware called "ATMitch" to compromise the bank's systems. This malware is known for targeting ATM systems and manipulating the bank's internal databases. The attackers used a malware called "ATMitch" to compromise the bank's systems. This malware is known for targeting ATM systems and manipulating the bank's internal databases.