AI IN CYBERSECURITY

Byunghee Jeon - *Geumcheon-Gu High School*

Ransomware is a type of malicious software that locks the victim's data and demands payment in exchange for unlocking it. Over the past few years, ransomware attacks have been increasing, with major targets being corporations, healthcare systems, and public organizations The fallout from cyberattacks has worsened the borough's "challenging financial environment," with government aid falling by nearly 40% since 2010, in particular.

Phishing is a type of social engineering attack where hackers pretend to be trustworthy companies to trick individuals into revealing sensitive information, like passwords. Recently, spear phishing, a more targeted and personalized form of phishing, has become more common. These attacks are becoming more sophisticated, making it easier for people to fall for them.In the second half of 2024, phishing attacks with a 202% increase in total phishing messages surged, and the situation became so serious that there were cases where commonly used platforms and services were exploited for phishing campaigns. A supply chain attack occurs when hackers compromise a trusted third-party vendor's system and use it to access the target organization. These attacks are particularly dangerous because they take advantage of trusted relationships, making them harder to detect and stop.

Experts warned that modern "smart" agricultural machinery could be vulnerable to malicious hacker attacks, exposing global supply chains to risks. Concerns have been raised that hackers could exploit flaws in agricultural hardware used to plant and harvest crops, and global food supplies are under threat. Data is one of the main targets in cyberattacks, so encrypting sensitive information is crucial. For example, data in transit can be secured using SSL/TLS encryption, and data at rest should be protected with strong algorithms like AES (Advanced Encryption Standard). User education is essential in defending against phishing and other social engineering attacks. Employees need to be trained to recognize suspicious emails and avoid clicking on questionable links or attachments. Adding multi-factor authentication (MFA) can also provide an extra layer of security for user accounts.

Installing intrusion detection and prevention systems (IDS/IPS) is important for identifying and stopping cyberattacks early. IDS systems monitor network traffic in real-time for suspicious activity, while IPS systems actively block malicious actions. These systems play a key role in minimizing the damage caused by attacks. To prevent supply chain attacks, companies must carefully vet their third-party vendors and implement security measures that limit access to sensitive systems. Regular security audits and enforcing security standards for partners can help identify and reduce potential vulnerabilities.

In conclusion, cybersecurity threats like ransomware, phishing, and supply chain attacks are becoming increasingly sophisticated, making it essential for individuals and organizations to stay vigilant. These threats not only cause significant financial damage but also impact critical services and personal information. While recent incidents, such as the WannaCry attack and the SolarWinds hack, show how widespread these dangers can be, they also highlight the importance of strong cybersecurity measures. By adopting encryption technologies, training employees, and securing third-party relationships, we can reduce the risks and ensure that systems and data remain safe from cybercriminals. As technology continues to evolve, it is crucial for everyone, from large corporations to individual users, to prioritize cybersecurity and take proactive steps to protect themselves from emerging threats.

Bibliography

Marshall, Claire, and Malcolm Prior. "Cyber Security: Global Food Supply Chain at Risk from Malicious Hackers." *BBC News*, 20 May 2022, www.bbc.com/news/science-environment-61336659.

Mascellino, Alessandro. "Phishing Attacks Double in 2024." *Infosecurity Magazine*, 18 Dec. 2024, *Infosecurity Magazine*.

Steen, Josef. "Cyber Attack Costing Six-Figure Sum, Council Says." *BBC News*, 21 Dec. 2024, *Hackney Council: Cyber-attack Cost 'Hundreds of Thousands'*.