The Cyber-attacks that occurred in 2011 and 2014 on Sony that would have ruined their reputation

Gerkeil Owens

Old Dominion University

CYSE 300

1/14/2022

The Sony breaches of 2011 and 2014 are excellent examples of the potential consequences of cybersecurity vulnerabilities and the threat of their exploitation. According to (Warren, 2011) The breach of 2011 exploited a well-known weakness in Sony's systems such as the use of plain-text passwords, whereas in the 2014 breach, the lack of encryption in Sony's data revealed itself as the major vulnerability. This exploit in 2011 was shown by a hacking group called "LulzSec" who exposed Names, passwords, emails, and other user information for 77M people because of the breach. Sony's PSN platform was down for 23 days because of Sony's inability to stop the breach from spreading. The 2011 breach cost Sony dearly in terms of reputation and finances with their Sony online entertainment and streaming service being shut down for a month, Sony also had to deal with a twenty day plus public outrage that embarrassed the company and damaged its reputation, leading to a subsequent fine of $400,000 by the British government and compensation to the affected players (De Groot, 2022).

The 2014 breach three years after the 2011 breach, on the other hand, was hacked by another group called "Guardians of Peace" which resulted in 100TB of data being taken , the delay of several movie releases, a massive data leakage, and the company having to pay

compensation to its employees (De Groot, 2022).To mitigate the consequences and prevent similar incidents in the future, Sony needed to implement a more robust security strategy to protect its networks, data and customers. For the 2011 attack, they should have been using stronger encryption for their passwords and user data and better authentication systems. To protect their networks, firewalls, intrusion prevention systems, encryption software and other cyber security measures should have been put in place. For the 2014 attack, strong encryption with strong passwords should have been used and a system should have been put in place to detect attempts by unauthorized users to access the system.

Additionally, employees should have been thoroughly trained in the best cyber security practices and security training courses in order to educate and keep them informed of the risks and threats, because with Sony being such a big company and having two cyber security attacks in three and a half years apart is bad for how big the company is in the film industry releasing various movies in 2011 that grossed a good amount of money but the highest grossing movie being The "The Smurf's" movie and grossing $142,614,158 according to (*Box Office Performance for Sony Pictures Movies in 2011*, n.d.). As well as, in 2014 Sony produced another year of various movies with the highest grossing movie being "The Amazing Spider-Man 2" which grossed up to $202,853,933 according to (*Box Office Performance for Sony Pictures Movies in 2014*, n.d.).

So, with Sony having not only two years of producing various movies that did well in the years of 2011 and 2014 at that time. Not to mention the release of the PlayStation four released in the previous year of 2013, which was big for the gaming world because of the long wait for the next generation consoles to be released. Sony had so many customers who would buy their gaming consoles and PlayStation exclusive games, while just the PlayStation four gaming

consoles alone according to (Owens, 2022) sold ten million in sales units in the year of 2014. Sony, having such lucrative movies in the film industry, gaming consoles no matter which console you had, and video games, you would think Sony would have a great security system to keep their information and projects more discreet and very hard to access to prevent things like this from happening. Finally, the risk of threats should have been monitored and audited regularly to prevent this from happening or slow the process of getting hacked down until a solution was found. As well as, using they're funds to pay for a better security system or to bring in more employees that does cybersecurity to work for them and pay them to secure their information and projects.

The Sony breaches of 2011 and 2014 should be a reminder to everyone and to all companies of the importance of investing in a comprehensive cybersecurity strategy to protect their networks, data, and customers. The proper security measures are essential to protect confidential information and maintain a secure online environment. Companies and people in general should always be reviewing their security strategies and procedures regularly to stay ahead of potential cyber threats and mitigate the consequences of their exploitation.

References

Box Office Performance for Sony Pictures Movies in 2011. (n.d.). The Numbers. Retrieved January 15, 2023, from https://www.the-numbers.com/market/2011/distributor/Sony-Pictures

Box Office Performance for Sony Pictures Movies in 2014. (n.d.). The Numbers. Retrieved January 15, 2023, from https://www.the-numbers.com/market/2014/distributor/Sony-Pictures

De Groot, J. (2022, August 22). *The Biggest Moments in Cybersecurity History (in the Past 10 Years)*. Digital Guardian. Retrieved January 15, 2023, from https://digitalguardian.com/blog/biggest-moments-cybersecurity-history-past-10-years

Gara, T., & Warzel, C. (2014, December 3). *A Look Through The Sony Pictures Data Hack: This Is As Bad As It Gets*. BuzzFeed News. Retrieved January 15, 2023, from https://www.buzzfeednews.com/article/tomgara/sony-hack

Owens, T. (2022, August 11). *Global PS4 console unit sales 2021*. Statista. Retrieved January 15, 2023, from https://www.statista.com/statistics/651576/global-ps4-console-unit-sales/

Warren, C. (2011, June 11). *Sony Pictures Website Hacked, 1 Million Accounts Exposed*. Sony Pictures hacked. Retrieved January 15, 2023, from https://mashable.com/archive/sony-pictures-hacked