ENPM 686

Samridha Murali

04/02/2022

Current Event #9

Brenntag SE is a German-based chemical distributor company [1]. It is the second-largest chemical distributor in North America[2]. On April 28, 2021, DarkSide a Russian hacker group that provided Ramsonware as a service launched a Ransomware attack on Brenntag. Darkside targeted the North American division. Darkside initially demanded $7.5 million[3]. Brenntag after negotiating paid $4.4 million (133.65 bitcoins) as ransom in bitcoins on May 11 for the decryptor and to prevent stolen data [3][4]. DarkSide used stolen credentials for the Remote Desktop server from a third party. They did not know how credentials were obtained [5].

DarkSide encrypted devices on Brenntag's North American division and stole encrypted files of about 150 GB[3] and uploaded screenshots and details of information stolen on a private page [6]. Brenntag has more than 17,000 employees worldwide and about 6700 of them are affected by this data leak[7]. According to Brenntag Data of birth, driver's license number, medical records, and SSN of employees were leaked.[5]. According to Bleeping Computer, "stolen data includes financial and account information, Financial and accounting information, Sensitive Accounting & HR information, Contracts, NDAs, Marketing, Legal Projects, Chemical Formulas "[2]. An investigation by forensic experts has shown that leaked data has not been misused.

Following best practices could have prevented this attack. As the attack started using a leaked password if multifactor authentication was enabled it would have been difficult for the hacker to penetrate the network. If passwords were changed frequently it would have reduced the chances of attack. A lot of sensitive data has been leaked due to this attack as it was unencrypted. Encryption would have prevented it.

References :

[1]. "Brenntag." Wikipedia, Wikimedia Foundation, 9 Mar. 2022, https://en.wikipedia.org/wiki/Brenntag.

[2]. Trusty, Joe. "Brenntag Hacked by Darkside, Pays $4.4m Ransomware Attack." PoolMagazine.com - Get The Latest Pool News, 13 June 2021, https://www.poolmagazine.com/pool-news/brenntag-hacked-by-darkside-pays-4-4m-ransomware-attack/.

[3]. Abrams, Lawrence. "Chemical Distributor Pays $4.4 Million to Darkside Ransomware." BleepingComputer, BleepingComputer, 13 May 2021, https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/.

[4]. Abrams, Lawrence. "Chemical Distributor Pays $4.4 Million to Darkside Ransomware." BleepingComputer, BleepingComputer, 13 May 2021, https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/.

[5]. Din, Antonia. "Brenntag Disclosed What Data Was Stolen during the Darkside Ransomware Attack." Heimdal Security Blog, Heimdal Security, 5 July 2021,

https://heimdalsecurity.com/blog/chemical-distributor-brenntag-says-what-data-was-stolen-during-the-ransomware-attack/.

[6]. Aurand, Jake. “Chemical Supplier Pays $4.4 Million to Darkside Ransomware.” Binary Defense, 14 May 2021, https://binarydefense.com/threat_watch/chemical-supplier-pays-4-4-million-to-darkside-ransomware/.

[7]. Staff, SC. “Brenntag Sheds Light on Darkside Ransomware Attack.” SC Media, 9 Oct. 2021, https://www.scmagazine.com/brief/ransomware/brenntag-sheds-light-on-darkside-ransomware-attack.