paper_3.edited.docx

by

Submission date: 26-Sep-2021 03:56PM (UTC-0600)
Submission ID: 1657972047
File name: paper_3.edited.docx (13.99K)
Word count: 309
Character count: 2148

Executive Summary on Current Cybersecurity Position

Student's Name

University

Course

Professor

Date

Executive Summary on Current Cybersecurity Position

CVS Health has collected patients' data in several ways, such as through websites and mobile applications. The data is then transferred to the cloud database and can be retrieved easily through the electronic health records by the physicians or by the patients in their dashboard. Therefore, effective cybersecurity strategies are critical in CVS Health in safeguarding against cyber-attack. The elements that need protection in CVS Health are network, endpoint devices such as phones, computers, routers, and finally, the cloud. Some of the cybersecurity strategies implemented comprise risk assessment procedures such as penetration testing every year, patch management programs, use of antivirus. Other cybersecurity strategies are network monitoring, file system integrity monitoring and prevention, and employee training.

CVS Health has recently faced a challenge because more than one billion health records were exposed to a misconfigured cloud database (Brewster, 2021). The records could help the attackers recognize and target CVS customers because they contain device information, configuration, and medication data. Although CVS Health stated that they rapidly took the database down, which they claim was unintentionally unveiled, the organization did not acclaim the email addresses revealed in the database. Several technologies are used to support the cybersecurity infrastructure; however, based on the current CVS cybersecurity strategies, the technologies used are antivirus software, malware protection, and firewalls (Ct gov, n.d). Improving cybersecurity in the organization is always a challenging task to many companies; however, it is recommended that supporting the cybersecurity team in the organization prioritize risk evaluation, frequently review policies and procedures, and evaluate and performing yearly staff awareness training would help CVS Health protect their database and network.

References

Brewster, T. (2021). CVS Accidentally Leaks 1 billion Website Records-Including Covid-19 Vaccine. https://www.forbes.com/sites/thomasbrewster/2021/06/16/cvs-accidentally-leaks-1-billion-website-records-including-covid-19-vaccine-searches/?sh=10546b962c4f

Ct gov. (n.d). CVS Health: Information Security Controls. https://www.cidverifylicense.ct.gov/portalApps/viewFile.aspx

paper_3.edited.docx

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		