Data Protection and Security

Student's Name

Institutional Affiliation

Data Protection and Security

Education and training

One of the most frequent cases of data breaches is employee error, and not only those in the IT department. Almost half of the instances of data breaches are due to human errors (Lewis, 2017). The types of information that is breached are not only the credit card numbers, medical information of the patients and the social security numbers. The breaches also include the valuable trade information about trade secrets, proprietary information, financial or privileged data which belongs to employees and customers, and the internal communications about the company. Every misstep can lead to serious consequences such as not locking a door, losing a company device, not knowing the authorized persons to access data and sending the wrong attachment among others.

Although there are safeguards which can minimize the errors by employees, training of the staff is still crucial to prevent a data breach. In some industries, it is required by the law to offer training. Even in the conditions that it is not a statutory requirement to offer training, it is a reasonable safeguard for protecting certain data. In other industries, the contracts they make have conditions which require an organization to conduct data security training. With the vast amounts data that is readily accessible, it is an important business practice to train all staff members about the policies of the company and the best practices that are used for enforcing data privacy, confidentiality, and integrity. With sufficient training, some of the common attacks such as phishing can be prevented. Employees must know how to spot an attack; therefore a proactive leadership can reduce the cyber-risks.

Implementing VPNs

A Virtual Private Network uses encryption technologies such as IPSec, Layer 2 Tunneling Protocol, Transport Layer Security and Secure Sockets layer among others (Duffield et al., 2005). The VPN creates a virtual encrypted tunnel between one device on the network and VPN server. While traffic is in the tunnel no one can see the traffic, or know what the user is doing. The encryption that VPNs employed is strong enough so that even if traffic is intercepted, an attacker would not be able to read the contents.

VPNs can also mask the location that traffic is coming from. Since the remote access servers that ISPs deploy, using one's IP address, an attacker or any other party can be able to trace their location. However, when using a VPN, the traffic always appears to be coming from the VPN servers. Also, some VPN services have the ability to terminate applications from connecting o the internet if the link goes down. This way, the chances of data leaks from sensitive applications is reduced.

An organization using VPNs enable all the enterprise traffic that is widely spread to be unified within a single tunnel. This allows workers within and outside the enterprise to access their corporate network. Although a VPN company can shield one from any malpractice by ISPs, the company that offers the service needs to be trustworthy. They must not, for instance, keep logs about their traffic (Finhanmobile. 2018). With this, they make it clear that even in the case of lawsuits and warrants to access their servers, they will not be able to produce any records.

References

Lewis, J. (2017). Employee Privacy and Data Security Training. A legal Requirement and Prudent Business Practice. Retrieved from https://www.workplaceprivacyreport.com/wp-content/uploads/sites/162/2016/03/Privacy-Training-White-Paper-March20162.pdf

Finhanmobile. (2018). What Does a VPN Do? For One, It Keeps Your Data Secure. Retrieved form https://www.finjanmobile.com/vpn-data-security/

Duffield, N. G., Greenberg, A. G., Goyal, P., Mishra, P. P., Ramakrishnan, K. K., & Van der Merwe, J. E. (2005). *U.S. Patent No. 6,912,232*. Washington, DC: U.S. Patent and Trademark Office.