Alex Smetana

11/11/2021

CIS226

CSC Control 10: Data Recovery

CSC Control 10: Data Recovery, involves the processes and tools used to properly backup critical information in a timely fashion. It is composed of four main points. Firstly, it ensures that each system is automatically backed up on a weekly basis. The more frequent the data is backed up, the more accurate information that you will maintain in the event of an attack. Secondly, it involves testing the data by performing a data restoration process to ensure that the data is working. It is very important to make sure that the system is up to date and functional. Also, it makes sure that the data is protected by encryption or physical security when it is stored. It is important to make sure that this backup is secure so that no one can get access to it. If it wasn't secure, then it would pose more of a liability than an asset. Finally, it ensures that key systems have at least on backup destination that is not continuously addressable through operating system calls.

It is important for cybersecurity because involves the protection of data. It concerns the Availability leg in the CIA triangle. This is most useful for attacks that compromise availability, such as in a denial-of-service attack. For an individual or a small-scale business, it may not be as significant, however the larger a business gets, the more critical this control is. In a large-scale business, for example a hospital, with thousands of personal records and PII has information that must be kept secure. If a business were to lose record of that data, the results could be catastrophic. It is very important to make sure that this data is backed frequently and kept secure. If not followed correctly, an attack could set a company back years, lead many fines, and most likely put them out of business.

Implements CSC 11 is very easy. Firstly, an organization must start with backing up important data. The backup of critical data is very crucial and the more frequent the data gets backed up, the more accurate the data will be. It is especially important to backup any sort of PII records. Secondly, once the data is backed up, it must be protected both digitally and physically. Physically, the access controls must be set. Only people that needs access to the information must have

access to that information. As for digital, the information should follow standards and use some sort of encryption. This can be done in numerous ways. For example, an organization may make use of Multi Factor Authentication to ensure that the right user is attempting to access the data Finally, an organization should perform some sort of tests to make sure that a system is protected and up to date. They must work find flaws in the security to ensure that it is up to date.

In conclusion CSC Control 10: Data Recovery, involves the processes and tools used to properly backup critical information in a timely fashion. It acts as a fail safe in the loss of crucial attacks. It is very crucial in for a business to follow this control.

Resources

Nielsen, Anna. “CIS Critical Control 10 Explained: Data Recovery Capability: Rapid7 Blog.” *Rapid7*, Rapid7 Blog, 24 Aug. 2018, https://www.rapid7.com/blog/post/2018/03/12/cis-critical-control-10-data-recovery-capability/.