**Understanding CIS Control Framework**

The challenge with Cyber Security is the complexity, the number of choices, and the number of options. There are a lot of defenses against the malpractices of cyber security. Critical Security Control, also known as CIS Control Framework refers to the guidelines that provide a list of measures to control the malpractices and attacks concerning the cyber security domain. This is a non-profitable organization. With the advent of technology, the rise of security measures has grown as well. But despite that, various attacks are happening every minute. In a recent security test, it was found that the CISCO umbrella received a nearly 96% rate of detection of threats.

CIS control is based on understanding the lifestyle of the attacker and modeling defense of actions for that. Experts from around the globe have collaborated and mentioned that twenty controls would be a defense mechanism against cyber attacks. In version 8, there is a decrease of control by two, resulting in the total number being eighteen. The effect of this ranges from people to firms.

**What are these controls about?**

There are nearly twenty controls that are used to prevent cyberattacks. These are as follows.

1. Firms should handle all the hardware devices so that authorized users can be identified and only given access and unauthorized users are eliminated before they can cause unwanted harm.

2. Applications that can detect the software which is authorized should be used and only that software must be installed, preventing the unauthorized ones from getting installed.

3. To prevent attackers from hampering the settings and configurations of the employee’s system, organizations should take charge of executing and maintaining the configurations concerning security issues of the devices.

4. To prevent attackers from invading the network and hampering the architecture, companies should check the information like new notices, updates, etc regularly.

5. Automatic tools should be used to determine whether any unauthorized user has control over the system. By using these tools, the actions of the user can be observed.

6. Upcoming and ongoing activities must be checked and observed so that any kind of malicious activity can be identified.

7. To minimize the attack surface and manage it, only web browsers and email clients which are fully trustable should be used.

8. All the systems of the organization must be regularly checked with anti-virus tools and in the case of malware code, it should be seen that installation and implementation of them are controlled from different points.

9. The protocols used, and the use of services must be checked by the firm to avoid the risk.

10. Important data must be backed up frequently and recovery of data should also be a matter of concern.

11. The security configuration of routers, switches, etc must be taken care of and managed by the organization itself.

12. Information flow in the midst of networks with varying trust levels should be detected and corrected by the firm.

13. Combined methods of encryption and techniques to prevent data breaching should be incorporated to maintain the well-being of confidential data.

14. As soon as an employee resigns, their user accounts should be deleted from the system as soon as possible to avoid any kind of discrepancy.

15. Critical assets are a valuable aspect of every organization whose well-being and control must be taken care of by the company.

16. The wireless devices which are used by the organization should be checked and their authentication must be checked as well.

17. Firms should gauge their skills concerning security purposes by making and executing plans to understand the loopholes.

18. Software lifecycle must be checked frequently and only the current versions of applications must be in use.

19. Security incidents must be managed by executing plans and actions.

20. The last control is about assessing the organization’s strong and weak parts by performing regular tests and improving the technologies from time to time.

**Why is it important?**

1. These controls protect the organization from unwanted malpractices.

2. Confidential data is kept secure and data breaching can be prevented.

3. They evaluate the already existing security actions and provide ways to improve.

4. Organization’s privacy is maintained.

**References**

1.<https://blog.netwrix.com/2018/02/01/top-20-critical-security-controls-for-effective-cyber-defense/>

2.<https://www.sans.org/blog/cis-controls-v8/>

3.<https://www.cisecurity.org/controls/cis-controls-list>

4.<https://www.cisecurity.org/controls>

5.<https://en.wikipedia.org/wiki/The_CIS_Critical_Security_Controls_for_Effective_Cyber_Defense>

6.<https://carbidesecure.com/resources/how-to-use-cis-security-framework/>

7.<https://www.upguard.com/blog/cis-controls>