COMUNE DI PALAZZOLO SULL’OGLIO

CONCORSO PUBBLICO ISTRUTTORE INFORMATICO PNRR
9 gennaio 2023

PROVA ORALE N. 1

- il comune ospita un data center on premise che è stato classificato dall'AgID con la classe B.
  Cosa significa praticamente e quali sono i passi da intraprendere nel medio/lungo termine? Considerare che con il passaggio di tutti gli applicativi sul cloud, in esso sono contenuti unicamente il file server, il sistema di disaster recovery, il firewall e l'active directory.

- il provider internet informa che un sito del comune, adibito unicamente alle segnalazioni dei cittadini, ha subito un attacco Distributed Denial of Service.
  In cosa consiste questo tipo di attacco?
  Da cosa può essere stato causato e quali sarebbero le azioni per prevenirlo?

- Il Sindaco

- Inglese – vd allegato

- Colloquio psicoattitudinale

With the cost of a data breach at an all-time high of $4.35 million and regulations worldwide imposing steeper penalties for compliance failures, organizations must ensure that they have all necessary security controls in place to keep their data safe. Implementing the CIS Controls provides a sound foundation for effective defense against cyber threats.

First developed in 2008, the CIS Controls are updated periodically in response to the evolution of both technologies and the threat landscape. The controls are based on the latest information about common attacks and reflect the combined knowledge of commercial forensics experts, individual penetration testers and contributors from U.S. government agencies.

This article details the 18 controls in CIS version 8. These guidelines take into account the rise of remote work and the resulting increase in access points and need for perimeter-less security.

Control 01. Inventory and Control of Enterprise Assets

The first step in developing and implementing a comprehensive cybersecurity strategy is to understand your company's assets, who controls them and the roles they play. This includes establishing and maintaining an accurate, updated and detailed list of all hardware connected to your infrastructure, including assets that aren't under your control, such as employees' personal cell phones. Portable user devices will periodically join a network and then disappear, making the inventory of currently available assets very dynamic.

Why is this critical? Without this information, you can't be sure you've secured all possible attack surfaces. Keeping an inventory of all assets connecting to your network and removing unauthorized devices can dramatically reduce your risk.

Control 02. Inventory and Control of Software Assets

Control 2 addresses threats from the dizzying array of software that modern companies use for business operations. It includes the following key practices:

- Identify and document all software assets, and remove any that are outdated or vulnerable.
- Prevent the installation and use of unauthorized software by creating an authorized software allowlist.
- Use automated software tracking tools to monitor and manage software application