COMUNE DI PALAZZOLO SULL’OGLIO

CONCORSO PUBBLICO ISTRUTTORE INFORMATICO PNRR

9 gennaio 2023

PROVA ORALE N. 2

- un collega va in pensione, quali sono le azioni da intraprendere da parte dei sistemi informativi aziendali?

- a seguito dello sviluppo del nuovo sito nell'ambito dei bandi finanziati dal PNRR, si vorrebbe far convogliare in esso anche 6/7 siti legati al comune, come per esempio quello della biblioteca, un sito di eventi teatrali, un e-commerce per favorire le attività locali. Illustri il candidato vantaggi e svantaggi di questo "porting" e che caratteristiche potrebbero in parte precluderlo considerando che il portale istituzionale è sviluppato su un CMS personalizzato del fornitore.

- Il Consiglio comunale

- Inglese – vd allegato

- Colloquio psicoattitudinale

Control 05. Account Management

Account management was Control 16 in CIS Controls version 7.

Securely managing user, administrator and service accounts is vital to preventing their exploitation by attackers. Control 5 includes six steps for avoiding security problems caused by vulnerable accounts:

- Create and maintain an inventory of all accounts.
- Use unique passwords.
- Disable accounts that haven't been used for 45 days.
- Restrict use of privileged accounts.
- Create and maintain an inventory of service accounts.
- Centralize all account management.

Why is this critical? Privileged and unused accounts provide an avenue for attackers to target your network. Minimizing and controlling these accounts will help protect your data and network from unauthorized access.

Control 06. Access Control Management

This safeguard merges controls 4 and 14 of version 7 of the CIS Controls.

Control 6 concerns controlling user privileges. Its best practices include establishing an access granting and revoking process, using multifactor authentication, and maintaining an inventory of systems for access control.

Why is this critical? Granting overly broad privileges for the sake of expediency opens an avenue of attack. By limiting each user's access rights to only what's required to do their job, you'll limit your attack surface.

Control 07. Continuous Vulnerability Management

In version 7 of the CIS Controls, continuous vulnerability management was covered by Control 3.

This control covers identifying, prioritizing, documenting and remediating each security vulnerability in your network. Examples include open services and network ports, and default accounts and passwords.

Why is this critical? Organizations that don't proactively identify infrastructure vulnerabilities and take remediation measures are likely to have their assets compromised or suffer business disruptions.