COMUNE DI PALAZZOLO SULL'OGLIO

CONCORSO PUBBLICO ISTRUTTORE INFORMATICO PNRR

9 gennaio 2023

PROVA ORALE N. 3

- descrivere le caratteristiche dei diversi sistemi di filtraggio web.

- in un sistema basato su server Microsoft Windows 2019, quali sono le soluzioni adottabili per la software distribution al fine di mantenere aggiornate le postazioni di lavoro presenti sul dominio?
  Quali sono i vantaggi e gli svantaggi rispetto ai normali aggiornamenti di sistema configurati di default su postazioni con sistema operativo Windows?

- La Giunta comunale

- Inglese – vd allegato

- Colloquio psicoattitudinale

Control 08. Audit Log Management

This topic was covered under Control 6 in CIS Controls version 7.

Audit log management involves controls related to collecting, storing, retaining, time synchronizing and reviewing audit logs.

Why is this critical? Security logging and analysis helps prevent attackers from hiding their location and activities. Even if you know which systems were compromised in a security incident, if you don't have complete logs, you'll have a hard time understanding what an attacker has done so far and responding effectively. Logs will also be needed for follow-up investigations and determining the origin of attacks that remained undetected for a long time.

Control 09. Email and Web Browser Protections

This safeguard was Control 7 in CIS Controls version 7.

Email and web browsers are common vectors of attack. The primary technical controls for securing email servers and web browsers include blocking malicious URLs and file types. For more comprehensive protection against such attacks, you must also provide organization-wide training on best security practices.

Why is this critical? Using techniques like spoofing and social engineering, attackers can trick users into taking actions that can spread malware or provide access to confidential data.

Control 10. Malware Defenses

This topic was covered under Control 8 in CIS Controls version 7.

Organizations wielding ransomware and other malware have become as professional as mainstream businesses. This control describes safeguards to prevent or control the installation, execution and spread of malicious software. Centrally managing both behavior-based anti-malware and signature-based tools with automatic updates provides the most robust protection against malware.

Why is this critical? Malware can come in the form of trojan horses, viruses and worms that steal, encrypt or destroy your data. Ransomware is big business, with a global price tag expected to reach $265 billion by 2031. Following the practices outlined in Control 9 will help protect your organization against an expensive and damaging malware infection.