Napoli, 11/11/2026
Prot. n. 194/2026

Agli *Enti Soci*
c.a. Sig. Sindaco/Presidente
Segretario/Direttore Generale
Resp.le Transizione Digitale
LORO SEDI

OGGETTO: CYBERSECURITY – Nasce il primo Centro Operativo di Sicurezza Informatica dei Comuni

L'ondata di attacchi informatici di questi giorni ha reso necessari piani di emergenza a livello globale. Recentemente, il Ministro dell'Interno Piantedosi ha convocato una riunione per definire le contromisure contro un'offensiva su larga scala mirata alle pubbliche amministrazioni, alle infrastrutture critiche e ai funzionari di Stato.

Anche i Comuni sono oggi tenuti ad adottare rigorose misure di gestione e controllo della sicurezza informatica, in linea con le disposizioni del «Sistema di prevenzione e difesa cybernazionale». Garantire la protezione dei sistemi non rappresenta soltanto un obbligo normativo, ma una necessità imprescindibile per evitare gravi responsabilità penali e amministrative. Tuttavia, sul fronte della cybersecurity, i piccoli Comuni affrontano importanti criticità, frenati dalla limitata disponibilità di risorse economiche, competenze specialistiche e infrastrutture adeguate.

Per consentire ai Comuni associati di accedere, a costo zero, a strumenti avanzati e competenze specialistiche senza personale informatico dedicato, Asmenet ha strutturato una strategia integrata di **cyber-resilienza**, fondata sulla prevenzione delle minacce e sulla capacità di difesa attiva. L'approccio è pratico e concreto, orientato a creare una solida barriera a protezione dei dati e dei sistemi attraverso la combinazione di tecnologie avanzate, procedure codificate e formazione continua:

1. **SOC (Centro Operativo di Sicurezza Informatica)**: dedicato alla difesa locale dei dati e dei servizi comunali. Un team di professionisti IT assicura la protezione XDR dei terminali, gestita tramite un'unica console centralizzata per garantire il rispetto dei livelli minimi di sicurezza.
2. **Monitoraggio continuo**: supervisione costante dei dispositivi degli Enti associati per rilevare in tempo reale gli eventi di sicurezza e intervenire con la massima rapidità. Il sistema individua le vulnerabilità di ciascuna risorsa e monitora la vetustà di hardware e software.
3. **Pianificazione e conformità**: redazione di procedure e misure tecniche e organizzative essenziali, volte a consentire all'Ente di assorbire eventuali attacchi informatici senza compromettere l'operatività quotidiana.
4. **Addestramento e formazione del personale**: i dipendenti costituiscono la prima linea di difesa. Programmi di formazione regolare insegnano a riconoscere minacce come il phishing, a evitare le trappole online e a trattare in modo sicuro i dati e le informazioni sensibili.

Per aderire inviare il modulo compilato sottostante. Info su *soc.asmenet.it*, per maggiori dettagli contattare lo 0817504545 oppure scrivi a supporto@asmenet.it.

Cordiali saluti e buon Lavoro

Il Presidente del CDA
Gen. Antonio Felice Caputo

L'Amministratore delegato
arch. Gennaro Tarallo

MODULO DI ADESIONE
inviare via mail a supporto@asmenet.it

il/la_____

in qualità di_____ del Comune di_____

tel_____ mail_____

☑ **Chiede di aderire al SOC - Centro Operativo di Sicurezza Informatica dei Comuni**

timbro e firma