

VADEMECUM D'URGENZA IN 10 PUNTI

Protocollo di reazione immediata per il personale della PA

Di fronte a un'attività sospetta, a un'anomalia comportamentale del sistema o a un potenziale attacco informatico, ogni funzionario deve applicare tassativamente la seguente procedura:

1. Riconosci l'Anomalia Comportamentale

Presta attenzione a rallentamenti improvvisi del PC, comparsa di file con estensioni strane, finestre pop-up insolite o richieste non autorizzate di codici OTP sul tuo smartphone.

2. NON Spegnerne il Computer

Se sospetti un attacco in corso, lascia il PC acceso. Spegnerlo cancellerebbe i dati temporanei della memoria RAM, fondamentali per l'analisi forense e per gli strumenti di *Threat Intelligence* dell'ente.

3. Stacca Immediatamente il Cavo di Rete

Sconnetti fisicamente il cavo Ethernet dal retro del computer o dalla presa a muro. Se sei connesso in Wi-Fi, disattiva immediatamente la connessione. Il distacco della rete blocca la diffusione del virus agli altri PC dell'ente in meno di un secondo.

4. Interrompi l'Inserimento di Password

Non inserire credenziali, password, codici SPID o PIN su nessun dispositivo della rete fino a quando l'incidente non sarà stato completamente isolato e risolto dai tecnici.

5. Fai una Foto allo Schermo

Se compare una schermata di riscatto (Ransomware), un messaggio d'errore strano o una minaccia, scatta subito una foto con il tuo smartphone. Sarà una prova preziosa per identificare il tipo di malware nei database della *Cyber Threat Intelligence*.

6. Attiva il "Double-Check" Telefonico

Se ricevi e-mail urgenti che richiedono dati sensibili (fascicoli giudiziari, dati ambientali, brevetti) o bonifici, non rispondere per iscritto. Chiama direttamente il mittente al telefono per verificare che non si tratti di un'identità rubata o di un inganno generato da IA.

7. Segnala l'Incidente Fuori Rete

Contatta immediatamente l'Ufficio IT o il Responsabile della Sicurezza (RSI) via telefono cellulare o di persona. Non usare mai la posta elettronica del computer sospetto per segnalare l'anomalia.

8. Segnala l'Errore Senza Timore

Se hai cliccato per sbaglio su un link sospetto o hai inserito la tua password in un sito insolito, comunicalo subito ai tecnici. La tempestività della segnalazione azzerà le sanzioni e previene il disastro sistemico dell'amministrazione.

9. Mantieni il Massimo riserbo

STUDIO LEGALE D'ANGELO
PATROCINANTE IN CASSAZIONE E MAGISTRATURE
SUPERIORI
SALERNO-ROMA

Non commentare l'accaduto con colleghi esterni, non scrivere sui social network e non diffondere dettagli dell'attacco per evitare fughe di notizie e garantire la conformità agli obblighi delle direttive NIS 2 e GDPR.

10. Attendi il "Via Libera" Formale

Non riconnettere il computer alla rete e non riprendere il lavoro fino a quando l'Ufficio IT o il Security Operations Center (SOC) non avranno rilasciato l'autorizzazione ufficiale di sicurezza.
