TECNICAI · SCHEDA DI AUTOVERIFICA

Il PC dove fai girare l'AI è sotto controllo?

Dieci domande da fare alla propria macchina prima di affidarle documenti di lavoro. Nessuna richiede un informatico: le prime nove si verificano in pochi minuti, la decima dice chi chiamare. Stampala, compilala, conservala: è documentazione anche questa.

	DOMANDA	RISPOSTA CHE TRANQUILLIZZA	RISPOSTA CHE APRE UN CANTIERE
1	**Esiste un registro di ciò che il PC invia in rete?**	Sì, con data, programma e destinazione, conservato almeno 30 giorni.	Non esiste o lo cancella il sistema stesso: nessun controllo possibile.
2	**Il server del modello gira con un account limitato?**	Sì, un utente di servizio senza accesso alle cartelle di lavoro.	Gira come l'utente amministratore: può leggere tutto ciò che leggi tu.
3	**L'indirizzo dei metadati cloud (169.254.169.254) è bloccato in uscita?**	Sì, bloccato a livello di sistema, non solo consigliato.	No: è la prima porta che un PC sotto attacco prova.
4	**Chi ha scritto le istruzioni che l'agente legge, e quando sono state verificate?**	Una persona definita, con data dell'ultima verifica e file scansionati.	Non si sa: quelle istruzioni valgono quanto un programma eseguito alla cieca.
5	**Sai da dove arrivano i pesi del modello e quale versione gira?**	Sì, fonte ufficiale, versione e firma verificati.	Copie di provenienza incerta: la filiera del software vale anche per l'AI.
6	**Gli aggiornamenti sono decisi da qualcuno?**	Sì, con una persona responsabile e una cadenza.	Tutto si aggiorna da solo, o nulla si aggiorna mai.
7	**Quali cartelle può leggere l'agente?**	Solo quelle necessarie, indicate esplicitamente.	Tutto il disco: ogni pratica riservata è a portata di strumento.
8	**Ci sono chiavi di accesso o file di configurazione con credenziali a portata di agente?**	No, sono fuori dalla sua portata.	Sì: sono esattamente ciò che un'esfiltrazione cerca per prima.
9	**Di notte cosa succede su quella macchina?**	Attività pianificate note e tracciate.	Nessuno lo sa: le attività notturne sono il turno di chi non guarda nessuno.
10	**Se domani il registro segnala un'anomalia, chi chiami?**	Una persona e un numero, scritti da qualche parte.	Nessuno: la procedura migliore senza un nominativo resta carta.

Una sola risposta nella colonna di destra merita attenzione: non perché il danno sia certo, ma perché senza quel controllo non si può escludere. Dubbi sul PC dove fai girare l'AI ogni giorno? Scrivici: **info@tecnicai.it** · Altri documenti gratuiti su tecnicai.it/news

A cura di TecnicAI · Iscritto all'Ordine dei Periti Industriali di Padova · RSPP · Professionista antincendio n° PD01774P00344. Contenuto informativo, non consulenza legale.