LINEE GUIDA PER LA CORRETTA GESTIONE DEI PC E DEI SERVER AUTOGESTITI

adottate con determina n. 04/2024 del Responsabile del Servizio Soluzioni Digitali e Infrastrutture IT di data 28 febbraio 2024

Premesse ed obiettivi

Nell'ambito del Progetto Sicurezza FBK realizzato dal Servizio Soluzioni Digitali e Infrastrutture IT in collaborazione con il Centro per la Cybersecurity ed in seguito ai colloqui effettuati con un campione di ricercatori per rafforzare la sicurezza delle reti e dei sistemi FBK, sono state elaborate le presenti "Linee guida per la corretta gestione dei PC e dei Server autogestiti", ispirate ai maggiori standard nazionali e internazionali (ad esempio AGID e IEC 62443) ed allo stesso tempo concepite per essere pratiche e poco impattanti in termini di overhead.

Queste Linee Guida, oggetto di specifici e obbligatori momenti formativi, al fine di spiegare in dettaglio le tecniche per gestire al meglio i sistemi diminuendo al massimo i rischi, **entreranno in vigore a partire dal 28 febbraio 2024** e dovranno essere **seguite da tutti gli Amministratori di Sistema della Fondazione**, così come definiti all'art. 12 del Regolamento Privacy, siano essi Amministratori di PC e/o di Server.

L'Amministratore di Sistema accetta la presa in carico delle conseguenti responsabilità civili e penali e garantisce la messa in atto di misure tecniche ed organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato e dei dati di cui FBK è Titolare. L'obiettivo delle presenti Linee Guida è infatti quello di supportare l'Amministratore di Sistema nell'assicurare che venga mantenuto e mai diminuito l'attuale livello di sicurezza sui dati trattati.

Le presenti Linee Guida si compongono di:

- Procedura per conseguire l'abilitazione alla gestione autonoma di strumenti e servizi informatici forniti da FBK ed assumere il ruolo di Amministratore di Sistema;
- Linee Guida per i PC autogestiti;
- Linee Guida per i sistemi Server autogestiti.

Procedura per conseguire l'abilitazione alla gestione autonoma di strumenti e servizi informatici forniti da FBK ed assumere il ruolo di Amministratore di Sistema FBK

Per assumere il ruolo di Amministratore di Sistema è imprescindibile afferire al Servizio Soluzioni Digitali e Infrastrutture IT (per i sistemi gestiti centralmente) o alle articolazioni organizzative di ricerca (per i sistemi gestiti dalla ricerca e/o per esclusivi scopi di ricerca scientifica). È inoltre **obbligatorio concludere l'attività propedeutica e periodica di formazione** resa disponibile dalla Fondazione sulla piattaforma FBK Academy, in italiano con sottotitoli e materiale in inglese. Si tratta di **corsi online, disponibili dal primo aprile 2024,** che sarà possibile seguire a partire da pochi giorni dopo averne richiesto l'iscrizione.

Nello specifico, per diventare Amministratore di Sistema di un PC è obbligatoria la frequenza al corso "Autogestione sicura dei PC", mentre per diventare Amministratore di Sistema di un Server è obbligatoria la frequenza al corso "Autogestione sicura dei Server". Per gestire uno o più PC e uno o più Server è obbligatoria la frequenza di entrambi. Inoltre, **tutti coloro che attualmente agiscono quali Amministratori di Sistema di Server sono tenuti ad iscriversi al nuovo corso e superare il test di apprendimento entro la fine di giugno 2024**.

Il/la diretto/a Responsabile del/la richiedente e l'Amministratore di Sistema FBK (Responsabile del Servizio Soluzioni Digitali e Infrastrutture IT) autorizzano l'autogestione dello strumento attraverso l'approvazione della partecipazione ai corsi obbligatori.

LINEE GUIDA PER I PC AUTOGESTITI

1. VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
    a. Installare automaticamente e rapidamente le patch e gli aggiornamenti di sicurezza del software sia per il sistema operativo sia per le applicazioni.
        i. Configurare i dispositivi in modo che eseguono automaticamente e costantemente gli aggiornamenti di sicurezza del sistema operativo e delle applicazioni.
        ii. Controllare comunque regolarmente, sui canali ufficiali, la disponibilità di nuovi aggiornamenti di sicurezza.
        iii. Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure.
        iv. In caso di nuove vulnerabilità, prevedere misure sostitutive, ad esempio usare tool alternativi rispetto a quelli attualmente vulnerabili, se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con i rischi.

2. USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
    a. Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
    b. Impedire che per le utenze, soprattutto quelle amministrative, vengano utilizzate credenziali deboli.
    c. Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
    d. Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza, e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
    e. Conservare le credenziali in modo da garantirne disponibilità e riservatezza usando, ad esempio, un password manager.
    f. Se per l'autenticazione si utilizzano chiavi pubbliche e private o passkey, si raccomanda che la chiave privata sia adeguatamente protetta (con gli appropriati permessi e con richiesta di password ad ogni uso della chiave privata) e non sia mai condivisa o comunicata ad altri.

3. DIFESE CONTRO I MALWARE
    a. Installare strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware. Tali strumenti devono essere aggiornati in modo automatico.
    b. Attivare i sistemi di firewall presenti.
        i. Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga il PC.
        ii. Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.

4. COPIE DI SICUREZZA
    a. Si raccomanda di usare strumenti che permettano di non conservare dati di lavoro sul PC, soprattutto dati sensibili, ad esempio drive Google o Microsoft di FBK per i dati, browser per la lettura della posta, ecc.
    b. Se questo non è possibile e sul PC sono presenti dati di lavoro, è obbligatorio:
        i. effettuare periodicamente una copia di sicurezza delle informazioni strettamente necessarie per evitare la perdita di dati;
        ii. crittografare il disco del PC.

LINEE GUIDA PER I SISTEMI SERVER AUTOGESTITI

1. INVENTARIO DEI DISPOSITIVI E DEL SOFTWARE
    a. Implementare un inventario delle risorse attive, aggiornandolo quando nuovi dispositivi vengono collegati in rete.
        i. Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando l'indirizzo IP, i nomi delle macchine, la funzione del sistema, l'amministratore responsabile della risorsa.
        ii. Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.
    b. Mantenere un inventario del software installato sui Server, ad esempio registrando il nome del software, la versione, il produttore, le licenze disponibili, la data di installazione, la data di scadenza delle licenza, lo stato delle licenze, ecc.
        i. Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

2. PROTEGGERE LE CONFIGURAZIONI HARDWARE E SOFTWARE SUI SERVER
    a. Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
        i. Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.
    b. Definire ed impiegare una configurazione standard per Server.
        i. Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.
        ii. Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
        iii. Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.
        iv. Assicurare con regolarità la validazione e l'aggiornamento delle immagini di installazione nella loro configurazione di sicurezza, anche in considerazione delle più recenti vulnerabilità e vettori di attacco.
        v. Le immagini di installazione devono provenire da siti ufficiali ed essere validate con le procedure messe a disposizione dal fornitore.
    c. Eseguire tutte le operazioni di amministrazione remota di Server, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette allineate agli standard di sicurezza piu' recenti (e.g: AES, SHA256, TLS >=1.2, chiavi RSA di almeno 2048 bit).
    d. Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.
    e. Implementare il "logging" delle operazioni dei Server.
        i. Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.
    f. Utilizzare, quando possibile, soluzioni di "Infrastructure as code" per il deploying di infrastruttura e applicativi.

3. VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
    a. Ad ogni modifica significativa della configurazione, eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano report con indicazioni delle vulnerabilità più critiche a ciascun Amministratore di Sistema.
    b. Eseguire periodicamente la ricerca delle vulnerabilità con frequenza commisurata alla complessità dell'infrastruttura.
    c. Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità

d. Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.
e. Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
f. Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità, utilizzandole per aggiornare le attività di scansione.
g. Dopo essersi assicurati che le patch non causino problemi o interruzioni nei sistemi in produzione, ad esempio utilizzando un ambiente di test, installare automaticamente e rapidamente le patch e gli aggiornamenti di sicurezza del software sia per il sistema operativo sia per le applicazioni.
h. Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure.
i. Prevedere, in caso di nuove vulnerabilità, misure alternative, ad esempio bloccare l'accesso dall'esterno, se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con i rischi.

4. <u>USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE</u>
    a. Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.
    b. Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
    c. Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.
    d. Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.
    e. Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata, controllandone periodicamente la reale necessità.
    f. Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
    g. Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.
    h. Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria, chiavi con password ed altri analoghi sistemi.
        i. Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
    i. Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
    j. Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza dove non è supportata l'autenticazione a più fattori.
    k. Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
    l. Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
    m. Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona, tranne per utenze tecniche collegate alle applicazioni o ai servizi.
    n. Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
    o. Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza usando, ad esempio, un password manager propriamente configurato e periodicamente revisionato.
    p. Se per l'autenticazione si utilizzano chiavi, si raccomanda che la chiave privata sia adeguatamente protetta (con gli appropriati permessi e con richiesta di password ad

ogni uso della chiave privata).

5. DIFESE CONTRO I MALWARE
    a. Installare su tutti i sistemi strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware. Tali strumenti devono essere aggiornati in modo automatico.
    b. Attivare i sistemi di firewall presenti sui Server.
        i. Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.
        ii. Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.

6. COPIE DI SICUREZZA
    a. Effettuare almeno giornalmente una copia di sicurezza delle informazioni strettamente necessarie per il completo ripristino del sistema.
        i. Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.
        ii. Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi sullo stesso possano coinvolgere anche tutte le sue copie di sicurezza.