	- vsftpd (server FTP di default) - httpd (server Web di default) - dovecot (servizi IMAP e POP3) - smb (server Samba) - squid (Web Proxy Server) - snmpd (SOLO SE SNMP NON E' IN USO) - ypserv (server NIS) - rsh.socket (rsh) - rlogin.socket (rlogin) - rexec.socket (rexec) - ntalk (server Talk) - telnet.socket (server Telnet) - tftp.socket (server TFTP) - rsyncd (server rsync) - finger-server

Configurare il Mail Transfer Agent (MTA) in modalità locale	
Minaccia	- Abuso di risorse. - Negazione dei servizi.
Contromisure	Gli MTA (ad es. Sendmail e Postfix) sono usati per ricevere email in entrata e trasferire I messaggi all'utente o al mail server di destinazione. Se il sistema non è un mail server o un SMTP relay, l'MTA deve essere configurato per processare solo le mail generate localmente al sistema (ad es. da applicative che generano un errore e inviano un messaggio a root per scopi di diagnostica).

Controllo automatico di integrità dei sistemi	
Minaccia	Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Per sistemi particolarmente critici, installare e configurare un File Integrity Monitor tool, al fine di garantire l'integrità dei file di configurazione e di sistema. Tale strumento deve permettere l'invio di alert configurabili, qualora siano rilevate delle modifiche non autorizzate eseguite da utenti malevoli. Esempi di tali strumenti sono AIDE (Advanced Intrusion Detection Environment), TripWire File Integrity Manager e OSSEC[3].

5.2.13 Sicurezza di Windows

La versione di default di un server o una workstation Windows potrebbe non disporre di tutte le misure di sicurezza necessarie per essere impiegato direttamente in un contesto di produzione, anche se Microsoft negli ultimi anni ha notevolmente migliorato la configurazione predefinita in ciascuna versione del sistema operativo. Segue una sintesi in termini di raccomandazioni di carattere generale, alcune valide anche per altri sistemi e altre specifiche per Windows, utili a rafforzare la resilienza del sistema operativo alla maggior parte degli attacchi informatici:

- Tenere aggiornata l'installazione di Windows - Probabilmente il passo più importante da fare è controllare la presenza degli ultimi aggiornamenti di sicurezza e le patch disponibili per il sistema

[3] https://www.ossec.net

operativo Windows. E' possibile in Windows ottenere automaticamente gli aggiornamenti di sicurezza. Dopo aver verificato la disponibilità di aggiornamenti, tenere attivo l'aggiornamento automatico al fine di scaricare e installare gli aggiornamenti maggiormente importanti che possono essere di aiuto a proteggere la postazione di lavoro/server da possibili nuovi virus o malware. Ricordare sempre di mantenere aggiornato il sistema operativo applicando l'ultima patch di sicurezza disponibile. Il patching del software rimane una chiave essenziale per migliorare la sicurezza online.

- Aggiornare il software installato - Non è necessario aggiornare solo il sistema operativo, ma anche il software in esso installato. Pertanto, anche in questo caso è opportuno assicurarsi che vengano installati gli ultimi aggiornamenti e le patch di sicurezza per i programmi e le applicazioni principali presenti nel sistema. Inutile dire che i software più diffusi (come Java, Adobe Flash, Adobe Shockwave, Adobe Acrobat Reader), in particolare quelli obsoleti, sono sempre oggetto di minaccia da parte di attori malintenzionati che intendono sfruttarli per ottenere un accesso più facile ai dati sensibili. Poiché questi software sono sempre sotto attacco, è importante non limitarsi a fare affidamento sulla propria memoria per aggiornare manualmente ciascun programma o applicazione installata nel sistema.
- Creare un punto di ripristino - Se si sono già installati gli aggiornamenti di sicurezza per il sistema operativo, il passaggio successivo è creare un punto di ripristino di Windows. Dopo aver installato Windows, è possibile creare il punto di ripristino e denominarlo "Installazione pulita" e continuare con l'installazione dei driver e delle applicazioni necessarie alla destinazione d'uso della macchina. Se uno dei driver o applicazione causa problemi al sistema, è sempre possibile tornare al punto di ripristino ripartendo dall'installazione pulita.
- Installare un software antivirus - Nel prendere in considerazione l'installazione di un programma antivirus, assicurarsi di utilizzarne uno certificato da una azienda riconsciuta, in quanto si potrebbe incorrere in programmi antivirus falsi. È importante disporre sul sistema di una soluzione di sicurezza affidabile, che dovrebbe prevedere la scansione in tempo reale, l'aggiornamento automatico del software e delle ultime vulnerabilità/minacce nonché di un firewall. Se si sceglie di installare un software antivirus che non dispone di un firewall, assicurarsi quantomeno di aver attivato il firewall di Windows.
- Adottare una soluzione di sicurezza proattiva per una protezione a più livelli - L'utilizzo di un antivirus tradizionale non è più la soluzione ideale, semplicemente perché non riesce a tenere il passo con l'ascesa di nuove e avanzate minacce presenti online. In particolare, il malware di carattere finanziario viene prodotto per sottrarre illecitamente dati sensibili e informazioni riservate impiegando metodi sofisticati per farlo. Il malware di nuova generazione di solito ha la capacità di eludere il rilevamento e aggirare il software antivirus che gli utenti hanno installato sulle proprie postazioni di lavoro al fine di mantenere i propri dati al sicuro. Con l'aiuto di una soluzione di sicurezza informatica proattiva, è possibile ottenere una migliore protezione contro malware di carattere finanziario e di furto di dati, come Zeus o Cryptolocker. Ad esempio, per migliorare il controllo finanziario di un conto bancario online, è sempre possibile impostare degli avvisi inviati dalla banca per tenere traccia dell'attività svolta sul conto, applicando questo semplice ed efficace criterio come misura proattiva di sicurezza.
- Eseguire il backup del sistema - Le pratiche precedentemente descritte hanno lo scopo di proteggere il sistema da software dannoso e minacce online, ma si potrebbero comunque riscontrare problemi hardware che potrebbero mettere in pericolo le informazioni riservate presenti nel sistema stesso. Per garantire che i dati rimangano al sicuro, si dovrebbe utilizzare una duplice strategia, che dovrebbe includere la combinazione di un utilizzo di un disco rigido esterno con un servizio di backup online. E' opportuno sottolineare l'importanza di disporre di una soluzione di backup capace di fornire stabilità, facile da usare, che consenta di sincronizzare i file di sistema con un server di backup online e che disponga di capacità di sicurezza, come la crittografia. A prescindere, è sempre comunque possibile utilizzare il sistema di backup di Windows.
- Utilizzare account di utente standard - Windows fornisce un certo livello di diritti e privilegi a seconda del tipo di account utente in uso. È possibile utilizzare un account utente standard o un

account utente amministratore. Al fine di proteggere il sistema, è consigliabile l'utilizzo di account standard per impedire agli utenti di apportare modifiche che interesserebbero tutti coloro che utilizzano la macchina, come ad esempio la cancellazione di importanti file di Windows necessari per il sistema. Con un account utente standard, si hanno diritti limitati e non è possibile ad esempio, cambiare le impostazioni di sistema o installare nuove applicazioni software, cambiare il nome dell'utente e la relativa password. Questo il motivo per cui si dovrebbe usare un account di questo tipo. Se è necessario installare un'applicazione o apportare modifiche di sicurezza, ciò lo si dovrebbe fare solo con un account amministratore. E' inoltre una buona pratica di sicurezza impostare una password complessa per ciascun account di Windows.

- Mantenere abilitato il controllo dell'account - Lo "User Account Control" anche detto UAC è una funzionalità di sicurezza essenziale di Windows che impedisce modifiche non autorizzate al sistema operativo. Spesso si ha la tendenza a disabilitarlo dopo aver installato/reinstallato il sistema operativo. Come si può ben comprendere, non è consigliabile disattivarlo. Invece di disabilitare l'UAC, è possibile ridurre il livello di notifica usando un cursore presente nelle impostazioni di controllo dell'account utente di Windows. L'UAC controlla quali modifiche potranno essere apportate al computer. Quando viene rilevata una modifica importante, come l'installazione di un programma o la rimozione di un'applicazione, viene visualizzato l'UAC che richiede un'autorizzazione a livello di amministratore. Nel caso in cui l'account utente sia infetto da malware, l'UAC aiuta a impedire che programmi e attività sospette apportino modifiche al sistema.
- Proteggere il browser web predefinito prima di connettersi a internet - Un'altra cosa da fare dopo l'installazione di Windows è quella di prestare particolare attenzione alla sicurezza del browser web. Poiché il browser Web è lo strumento principale utilizzato per accedere a Internet, è importante tenerlo al sicuro prima di connettersi online. Le vulnerabilità presenti nel browser web sono come una porta aperta verso il sistema per i criminali informatici che trovano sempre modi creativi per raccogliere dati significativamente importanti. Ad esempio, se si utilizza Adobe Flash, prestare attenzione alle difettosità di sicurezza di quest'ultimo e al modo in cui può esporre il sistema agli attacchi. Per rimanere al sicuro durante la navigazione sul Web, attenersi in generale alle seguenti regole:
    - Scegliere l'ultima versione del browser in uso.
    - Tenere il software del browser aggiornato.
    - Scegliere una sessione di navigazione privata quando si accede a un sito Web di cui non si è sicuri. La scelta di tale modalità impedirà che le credenziali (o i cookie) di autenticazione vengano archiviate e sottratte indebitamente dagli aggressori.
    - Poiché un eventuale malware capace di sottrarre dati potrebbe diffondersi anche nei siti Web legittimi attraverso del codice dannoso presente all'interno delle finestre popup, è buona norma assicurarsi che il browser web sia preimpostato per bloccare i popup.
- Utilizzare uno strumento software per crittografare il disco rigido - Anche se si imposta una password di account per l'accesso al sistema, soggetti malintenzionati possono comunque ottenere l'accesso non autorizzato ai file e documenti privati dell'account. Questi vi possono accedere semplicemente avviando la macchina con un proprio sistema operativo, ad esempio Linux, da un disco esterno o un'unità flash USB. In tal caso, una delle possibili soluzioni è quella di crittografare il disco rigido in modo tale da proteggere i file sensibili in esso memorizzati. Si consiglia di utilizzare tale livello di sicurezza se si dispone di un laptop, che può essere facilmente prelevato. La stessa cosa vale per un computer desktop. Uno strumento di crittografia gratuito che è possibile utilizzare è BitLocker, disponibile anche per le ultime versioni di Windows. Dopo aver abilitato la protezione BitLocker, non si noterà alcuna differenza e si potrà semplicemente accedere al sistema inserendo la normale password dell'account utente di Windows. I vantaggi apportati dall'utilizzo di questo strumento di crittografia sono:
    - la possibilità di cifrare l'intero disco, il che rende impossibile per i soggetti malintenzionati prelevare il laptop per rimuovere il disco rigido e leggere i file.

- la facilità d'uso e la totale integrazione con il sistema operativo Windows, quindi non è necessario aggiungere altro software crittografico.

Alle linee guida generali riportate nei paragrafi precedenti e valide per tutti i sistemi operativi, si aggiungono, per l'ambito specifico dei sistemi Windows (con un focus per Windows 7 Professional Edition), le indicazioni seguenti:

Controlli utente	
Minaccia	- Accesso non autorizzato al sistema. - Accesso non autorizzato alle informazioni. - Uso non autorizzato di privilegi.
Contromisure	È necessario assicurare che i seguenti controlli sulle utenze siano impostati: - L'utente Administrator deve essere disabilitato: questo avviene di default in fase di installazione e pertanto si raccomanda di non riattivarlo. - L'utente Administrator deve essere rinominato. - L'utente Guest deve essere disabilitato. - Il login automatico al desktop deve essere disabilitato. - La schermata di login deve essere configurata per richiedere l'inserimento manuale di nome utente e password (anziché visualizzare le immagini relative agli utenti presenti sul sistema). - La visualizzazione dei "suggerimenti" per la password deve essere disabilitata. - Bloccare lo schermo dopo 15 minuti di inattività e richiedere la password per sbloccarlo. - Richiedere la password quando il PC si riattiva da una sospensione. - L'utente che utilizza normalmente il PC non deve essere un amministratore, ma un utente comune (gruppo Users). - Il sistema Windows deve essere parte di un dominio di Active Directory dell'organizzazione. In conseguenza di ciò, la maggior parte dei controlli indicati nel seguente paragrafo, potranno e dovranno essere applicati ai sistemi sotto forma di Group Policy attuate automaticamente. - Sul sistema non devono essere presenti amministratori locali. Gli unici amministratori abilitati sul sistema devono essere quelli di dominio.

Policy di gruppo	
Minaccia	Accesso non autorizzato alle informazioni sensibili del sistema.
Contromisure	Adottare le seguenti impostazioni di Policy di gruppo, oltre a quelle specificamente menzionate in altre aree del presente documento, per attuare un insieme completo di politiche sui permessi degli utenti ed adeguato dal punto di vista della sicurezza. A tal fine procedere come segue: - Aprire lo strumento di sistema "Group Policy Management Editor". - Navigare fino al nodo "Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment" e selezionarlo. - Nel riquadro dei dettagli mostrato, modificare i permessi utente predefiniti impostando i valori delle opzioni come segue: o "Access Credential Manager as a trusted caller" con il valore "<blank>", o "Act as part of the operating system" con il valore "<blank>", o "Allow log on locally" con il valore "Administrators, Users", o "Create a pagefile" con il valore "Administrators", o "Create a token object" con il valore "<blank>",

	○ "Create global objects" con il valore "Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE", ○ "Create permanent shared objects" con il valore "<blank>", ○ "Create symbolic links" con il valore "Administrators", ○ "Debug programs" con il valore "Administrators", ○ "Enable computer and user accounts to be trusted for delegation" con il valore "<blank>", ○ "Force shutdown from a remote system" con il valore "Administrators", ○ "Impersonate a client after authentication" con il valore "Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE", ○ "Increase scheduling priority" con il valore "Administrators", ○ "Load and unload device drivers" con il valore "Administrators", ○ "Lock pages in memory" con il valore "<blank>", ○ "Modify an object label" con il valore "<blank>", ○ "Modify firmware environment values" con il valore "Administrators", ○ "Perform volume maintenance tasks" con il valore "Administrators", ○ "Profile single process" con il valore "Administrators", ○ "Take ownership of files or other objects" con il valore "Administrators".

Controlli di base	
Minaccia	- Attacchi all'integrità dei sistemi (software e configurazioni). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate (in assenza di un SIEM).
Contromisure	È necessario assicurare che i seguenti controlli di base siano attivati: - Abilitare Windows Update e configurare il sistema per l'aggiornamento automatico. - Disabilitare l'auto-play per supporti removibili quali CD/DVD, chiavette USB, schede di memoria, ecc. - Installare e configurare una soluzione per la raccolta, la gestione centralizzata e l'analisi dei log di sicurezza (SIEM – Security Information and Event Management). - Installare una soluzione anti-malware e aggiornarla regolarmente in automatico. Per la gestione centralizzata della sicurezza di una rete Windows complessa, si raccomanda l'uso di adeguati strumenti di gestione basati su template rilasciati da Microsoft, come ad es. Microsoft Security Compliance Manager.

Crittografia del disco di avvio	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni - Attacchi all'integrità dei sistemi (software e configurazioni). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Per i computer Windows portatili che contengono informazioni riservate, oppure dati personali sensibili, è necessario proteggere il disco di avvio con BitLocker. Si tratta di un meccanismo di crittografia del disco di boot che richiede all'avvio una password o una "recovery key" (o una smart card).

	In tal modo in caso di smarrimento o furto del portatile, i dati resteranno protetti. Ovviamente la password e la recovery key NON devono essere trascritte (ad es. su un foglio custodito nella valigetta del PC), né comunicate a terzi.

Crittografia dei dischi di ripristino e dei dischi esterni	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Quando si utilizza una unità removibile per creare dischi di ripristino, è necessario abilitare la crittografia BitLocker del disco. Questo controllo è particolarmente importante nel caso di backup su dischi rimovibili dato che essi possono essere smarriti o rubati. Più in generale, i dischi esterni removibili contenenti informazioni riservate devono essere inizializzati con un file system crittografato con BitLocker.

Partizionamento	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi.
Contromisure	In fase di installazione del sistema Windows, è necessario assicurarsi che la partizione di sistema sia di tipo NTFS e non FAT. Se il sistema precede la presenza di una partizione di ripristino del sistema operativo, si consiglia di rimuoverla e di recuperare il relativo spazio. Infatti l'eventuale reinstallazione del sistema operativo deve avvenire partendo da supporti originali non riscrivibili (DVD), o da altri supporti la cui integrità sia garantita.

Accesso al PC dalla rete	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Attacchi all'integrità delle informazioni.
Contromisure	La policy di sicurezza 'Access this computer from the network' deve essere ristretta al solo gruppo Administrators, a meno che l'utente (gruppo Users) non debba davvero accedere a questa postazione anche da altri sistemi.

Blocchi per il gruppo Guests	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni.
Contromisure	Le seguenti policy di sicurezza che impediscono determinate funzionalità sul sistema a certi utenti e gruppi, devono includere esplicitamente il gruppo Guests: - Deny log on as a batch job - Deny log on as a service - Deny log on locally - Deny log on through Remote Desktop Services

Logon Interattivo	
Minaccia	Accesso non autorizzato ai sistemi.
Contromisure	Quando un sistema, facente parte di un dominio, non riesce a raggiungere il server

	Active Directory in fase di accesso, consente comunque di effettuare il login all'utente ma solo per un certo numero di volte (default 10). Tale numero deve essere ridotto a 4 per sistemi particolarmente critici. La relativa policy è denominata: Interactive logon: "Number of previous logons to cache". Inoltre, è necessario disattivare la visualizzazione del nome utente che ha effettuato l'ultimo login, attraverso la policy "Interactive logon: Do not display last user name".

Enumerazione di utenze e condivisioni	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.
Contromisure	Per impedire agli utenti anonimi di enumerare le utenze di dominio, le utenze locali e le condivisioni presenti sul sistema, abilitare la policy "Network access: Do not allow anonymous enumeration of SAM accounts and shares".

Null Session	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.
Contromisure	Quando alcuni servizi che "girano" come Local System si connettono a sistemi legacy (Windows Vista / Windows Server 2008), utilizzano una Null Session priva dei più elementari controlli di sicurezza. Per impedire questo comportamento ed utilizzare un meccanismo più robusto basato sulla "computer identity", abilitare la policy "Network security: Allow Local System to use computer identity for NTLM".

Sicurezza del protocollo NTLM	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.
Contromisure	Se tutti i sistemi Windows in rete supportano NTLMv2, è necessario abilitare questo protocollo come mandatario. Ciò è sicuramente possibile in modo del tutto affidabile solo se in rete vi sono unicamente sistemi Windows 7 / Windows Server 2008 e successivi. A tale scopo devono essere abilitate le seguenti policy: - "Network security: LAN Manager authentication level" → "Send NTLMv2 response only. Refuse LM & NTLM" - "Network security: Minimum session security for NTLM SSP based (including secure RPC) clients" → "Require NTLMv2 session security, Require 128-bit encryption" - "Network security: Minimum session security for NTLM SSP based (including secure RPC) servers" → "Require NTLMv2 session security, Require 128-bit encryption"

Sicurezza del protocollo SMB	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.

	- Negazione dei servizi
Contromisure	Per prevenire lo spoofing dell'identità del client, su tutti i sistemi Windows deve essere abilitata la seguente policy per SMB: - "Microsoft network server: Server SPN target name validation level" → "Accept if provided by client" (o più stringente). Quando risulti possibile, è però consigliabile di impostare questa funzionalità come obbligatoria ("Required from client"). Tale impostazione è supportata da tutte le versioni di Windows ma deve essere comunque verificata attentamente prima di essere introdotta. Inoltre, il protocollo SMB nella configurazione di default (che consente la compatibilità con sistemi Windows legacy), è vulnerabile ad attacchi di session hijacking, che consentono ad un utente malevolo, della rete, di interrompere una sessione SMB o di carpire i dati della sessione per introdursi in essa in maniera non autorizzata. Per impedire questa evenienza, è necessario configurare una serie di policy di sicurezza che richiedono la firma digitale e l'encryption del protocollo SMB. Tuttavia tali policy possono bloccare il funzionamento della rete in presenza di sistemi legacy, e quando i sistemi Windows non sono TUTTI configurati nello stesso modo. Se i sistemi presenti sono tutti basati su Windows 7 / Windows Server 2012 (oppure Windows Server 2008 con una hotfix, cfr. Microsoft Knowledge Base KB 950876) e successive versioni, e se è possibile configurare TUTTI questi sistemi allo stesso modo ad es. attraverso una Group Policy, è necessario abilitare le seguenti policy di sicurezza: - "Microsoft network client: Digitally sign communications (always)" → ENABLED - "Microsoft network server: Digitally sign communications (always)" → ENABLED - "Microsoft network server: Digitally sign communications (if client agrees)" → ENABLED Per completezza si nota che sistemi server con ruoli multipli (es. Domain Controller e File Server) fortemente utilizzati e dotati di processori obsoleti, risentiranno necessariamente di un calo delle performance dato che la firma digitale apposta ai pacchetti pone un carico non trascurabile sulla CPU.

Sicurezza del protocollo WS-Management	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - Negazione dei servizi
Contromisure	Windows Remote Management (WinRM) è l'implementazione Microsoft del protocollo WS-Management che è stato sviluppato come standard pubblico per lo scambio remoto di dati di gestione tra i dispositivi che lo implementano. Se per tale protocollo non viene attuata un'adeguata autenticazione e crittografia, il traffico può essere soggetto ad attacchi da parte di un avversario. Per ridurre questo rischio, Windows Remote Management dovrebbe essere configurato in modo sicuro adottando le adeguate impostazioni dei criteri di gruppo. A tal fine procedere come segue: - Aprire lo strumento di sistema "Group Policy Management Editor". - Navigare fino al nodo "Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client" e selezionarlo. - Nel riquadro dei dettagli mostrato, modificare i permessi utente predefiniti impostando i valori delle opzioni come segue:

	○ "Allow Basic authentication" con il valore "Disabled", ○ "Allow unencrypted traffic" con il valore "Disabled", ○ "Disallow digest authentication" con il valore "Enabled". - Navigare poi fino al nodo "Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service" e selezionarlo. - Nel riquadro dei dettagli mostrato, modificare i permessi utente predefiniti impostando i valori delle opzioni come segue: ○ "Allow Basic authentication" con il valore "Disabled", ○ "Allow unencrypted traffic" con il valore "Disabled", ○ "Disallow WinRM from storing RunAs credentials" con il valore "Enabled".

Disattivazione degli accessi tramite Windows Remote Shell	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - Negazione dei servizi
Contromisure	Quando Windows Remote Shell è abilitato, può consentire ad un avversario di eseguire a distanza script e comandi sulle workstation. Per ridurre questo rischio, Windows Remote Shell dovrebbe essere disabilitato. Per disabilitare l'accesso a Windows Remote Shell, è possibile attuare una specifica impostazione di policy di gruppo procedendo come segue: - Aprire lo strumento di sistema "Group Policy Management Editor". - Navigare fino al nodo "Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell" e selezionarlo. - Nel riquadro dei dettagli mostrato, modificare i permessi utente predefiniti impostando i valori delle opzioni come segue: ○ "Allow Remote Shell Access" con il valore "Disabled".

POSIX Subsystem	
Minaccia	Attacchi all'integrità dei sistemi.
Contromisure	Per ridurre la superficie d'attacco del sistema, è necessario disabilitare il sotto-sistema POSIX a meno che non sia effettivamente utilizzato. A tale scopo impostare la policy di sicurezza: - "System settings: Optional subsystems" → "Defined: (blank)"

User Account Control	
Minaccia	- Attacchi all'integrità dei sistemi. - Uso non autorizzato di privilegi. - Errori di amministrazione dei sistemi. - Furto di credenziali di autenticazione (es. da keylogger).
Contromisure	È necessario abilitare il meccanismo "User Account Control" per l'utente Administrator, built-in utilizzando la policy di sicurezza: - "User Account Control: Admin Approval Mode for the Built-in Administrator account" → ENABLED Si raccomanda, inoltre, di impedire agli utenti standard la possibilità di inserire credenziali amministrative per ottenere un token di amministratore, lasciando le operazioni privilegiate ai soli amministratori del dominio. In tal modo gli utenti non potranno, ad es., installare autonomamente software o driver di periferiche né

	eseguire software che richiede l'accesso amministrativo al sistema. Il comportamento normale di Windows quando un utente non amministratore lancia un'applicazione che tenta di ottenere privilegi amministrativi è di richiedere l'immissione delle credenziali amministrative. Se si abilita la seguente policy invece, non apparirà alcuna richiesta di credenziali dato che l'operazione amministrativa sarà automaticamente negata: - "User Account Control: Behavior of the elevation prompt for standard users" → "Automatically deny elevation requests"

Windows Firewall	
Minaccia	- Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	Il firewall di Windows è attivo di default. Si raccomanda di non disattivarlo e di non modificare in senso più permissivo le impostazioni di default. Pertanto, a meno che il firewall di Windows non sia stato sostituito da un altro prodotto commerciale (ad es. come parte di una soluzione anti-malware adottata dall'ente/organizzazione), si raccomanda di assicurare tramite Group Policy le seguenti politiche di sicurezza, in modo da impedirne la disattivazione: - "Windows Firewall: Domain: Firewall state" → "ON" - "Windows Firewall: Domain: Inbound connections" → "Block (default)" - "Windows Firewall: Domain: Outbound connections" → "Allow (default)" - "Windows Firewall: Domain: Settings: Apply local firewall rules" → "Yes (default)" - "Windows Firewall: Domain: Settings: Apply local connection security rules" → "Yes (default)" - "Windows Firewall: Domain: Logging: Log dropped packets" → "'Yes" (default: NO) - "Windows Firewall: Domain: Logging: Size limit (KB)" → "16,384 KB" (default 4.096 KB). Identiche impostazioni devono essere applicate alle stesse policy di sicurezza per i profili di rete PRIVATE e PUBLIC del Firewall.

Audit degli accessi	
Minaccia	- Accesso non autorizzato ai sistemi. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
Contromisure	Per abilitare l'auditing (logging) degli accessi sia riusciti che falliti, impostare la seguente policy di sicurezza: - "Audit Credential Validation" → "Success and Failure" In tal modo saranno generate più informazioni di auditing sull'account logon, tra cui: - 4774: An account was mapped for logon. - 4775: An account could not be mapped for logon. - 4776: The domain controller attempted to validate the credentials for an account. - 4777: The domain controller failed to validate the credentials for an account Inoltre, impostare anche le seguenti policy di audit per l'accounting: - "Audit Logon" → "Success and Failure" - "Audit Logoff" → "Success" - "Audit Other Logon/Logoff Events" → "Success and Failure" - "Audit Special Logon" → "Success" - "Audit Account Lockout" → "Success"

Audit degli eventi di sicurezza	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Uso non autorizzato di privilegi.
Contromisure	È necessario impostare le seguenti policy di audit, in modo da tracciare nei log di sistema i principali eventi di sicurezza: - "Audit Application Group Management" → "Success and Failure" - "Audit Computer Account Management" → "Success and Failure" - "Audit Other Account Management Events" → "Success and Failure" - "Audit Security Group Management" → "Success and Failure" - "Audit User Account Management" → "Success and Failure" - "Audit Policy Change" → "Success and Failure" - "Audit Authentication Policy Change" → "Success" - "Audit Security State Change" → "Success" - "Audit Security System Extension" → "Success and Failure" - "Audit System Integrity" → "Success and Failure"

Pass the Hash	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Falsificazione di identità.
Contromisure	Per mitigare la vulnerabilità "pass-the-hash" è necessario adottare, come minimo, le impostazioni di sicurezza fornite dall'apposito template di Microsoft Security Compliance Manager. Da ciò consegue l'impostazione delle seguenti policy: - "Apply UAC restrictions to local accounts on network logons" → "Enabled" - "WDigest Authentication" → "Disabled"

Visualizzazione delle password immesse	
Minaccia	Furto di credenziali di autenticazione.
Contromisure	Generalmente le applicazioni e i servizi di Windows utilizzano le librerie di sistema per visualizzare le finestre di dialogo per l'immissione di username e password. In questo tipo di finestre è presente un "check-box" che consente di visualizzare la password in chiaro. Tale check-box deve essere disattivato a livello globale sul sistema, per impedire che la password possa essere vista da persone diverse dall'utente legittimo. A tale scopo, impostare la seguente policy di sicurezza: - "Do not display the password reveal button" → "Enabled"

Path UNC di NETLOGON e SYSVOL	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Attacchi all'integrità delle informazioni.
Contromisure	Nel febbraio 2015, Microsoft ha rilasciato un nuovo meccanismo di controllo ("Hardened UNC Paths") per mitigare un rischio di sicurezza nelle Group Policy. Il