relativo bollettino di sicurezza è MS15-011 / KB 3000483.
Questo meccanismo richiede sia l'installazione di un aggiornamento di sicurezza, sia l'applicazione di specifiche impostazioni di Group Policy su TUTTI i computer del dominio che devono essere necessariamente basati su Windows Vista / Windows Server 2008 o versioni successive.
L'aggiornamento di sicurezza comprende anche un nuovo template di Group Policy (NetworkProvider.admx/adml) che indirizza i parametri da impostare.
Una volta applicato l'aggiornamento e il template di Group Policy, l'impostazione minima per mitigare il rischio in oggetto è la seguente:

"Hardened UNC Paths" → ENABLED, impostato come segue:

*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1

*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1

5.3 Sicurezza del Web Browser

Di seguito viene fornita una vista delle principali minacce e delle relative contromisure da adottare.

5.3.1 Architettura

Architettura	
Minaccia	- Accesso non autorizzato al sistema. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	- Utilizzare un sistema di protezione del perimetro (Firewall) in grado di effettuare Web Application Firewalling, posizionato tra la rete dei client e tutte le altre. - Installare un IDS (intrusion detection system) o IPS (intrusion prevention system) in grado di analizzare le richieste Web. - Impedire la manipolazione DNS: utilizzare DNS attendibile e protetto. - Bloccare i punti di accesso wireless e utilizzare un sistema di protezione come Wi-Fi Protected Access 2 e access point non vulnerabili (con firmware aggiornato) rispetto all'attacco KRACK precedentemente citato. **Nota Bene.** Si tenga presente che i dispositivi portatili personali possono eludere tali contromisure.

5.3.2 Hardening

Hardening del browser	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	- Utilizzare il browser con un account utente a bassi privilegi (ovvero senza privilegi di amministratore) in modo da limitare le possibilità di un attacco (security exploit) di compromettere l'intero sistema operativo. - Impostare il browser in modo da controllare la validità dei certificati presentati dai server, utilizzando le liste di revoca dei certificati (CRL), l'Online Certificate Status

	Protocol (OCSP), o altri meccanismi equivalenti. - Limitare/Disabilitare/Condizionare l'uso di: • Controlli ActiveX • Add-ons • Estensioni del browser (plug-ins) • JavaScript e Flash • Java Applets e applicazioni Silverlight. • "Mobile code" in generale. - Ad esempio, su Internet Explorer esiste la possibilità di esprimere delle white list e/o delle black list per controlli ActiveX, add-ons, ed estensioni del browser. - Abilitare (se disponibili) meccanismi di sandbox integrati nel browser. Ad esempio a partire da IE 7 è disponibile il "*protected mode*", una tecnologia che sfrutta i meccanismi di sandboxing chiamati "*Mandatory Integrity Control*". Anche Google Chrome fornisce una sandbox che limita l'accesso al sistema operativo da parte delle pagine web. - Valutare la possibilità di eseguire il browser all'interno di un software di una sandbox selezionata e approvata dall'organizzazione. - Valutare l'adozione di estensioni e plugin di terze parti create a scopo di hardening del browser. A titolo di esempio: - il software "NoScript" che consente l'esecuzione di contenuti web basati su JavaScript, Java, Flash, Silverlight e altri plug-in solo se il sito è considerato attendibile ossia è stato precedentemente aggiunto a una white list. - Valutare l'adozione del software "MyWOT/WOT" (Web of Trust) che fornisce un servizio di reputazione sul livello di trust dei siti web. - Considerare di utilizzare il browser all'interno di un LiveCD. I LiveCD, che forniscono un sistema operativo da una sorgente non scrivibile e sono tipicamente dotati di browser Internet. Se l'immagine originale LiveCD è priva di malware, tutto il software utilizzato, incluso il browser Internet, verrà caricato malware-free ogni volta che viene eseguito il boot dall'immagine LiveCD. Prestare però attenzione ad altro genere di pericoli: Qualsiasi traffico web non protetto (ad esempio, non utilizzando https) o verso siti web vulnerabili potrebbe ancora essere soggetto ad attacchi man-in-the-middle o altre manipolazioni basate sul traffico di rete.

Hardening del browser	
Minaccia	- Accesso non autorizzato alle informazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (phishing e malware). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	- Disabilitare la memorizzazione di password nel browser. Quasi tutti i browser e molti siti web in genere offrono la possibilità di ricordare le password per uso futuro. L'attivazione di questa funzionalità memorizza le password in un'unica posizione sul computer, rendendo più facile per un aggressore scoprirle se il sistema venisse compromesso. Se questa funzionalità risulta abilitata, è necessario disattivarla e cancellare le password memorizzate. - Attivare il blocco dei popup del browser. Le finestre di popup sono una notevole tecnica di "phishing". Il blocco dei popup è oggi una funzionalità standard dei browser e dovrebbe essere abilitato ogni volta che si naviga sul web. Può essere utilizzata anche su siti web specifici e non su altri, dove i popup potrebbero invece essere necessari.

Privacy durante la navigazione web	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	Adottare le seguenti misure a salvaguardia della privacy degli utenti, rispetto ai siti Web che monitorano le attività utente: - Impostare una routine specifica per eliminare i cookie regolarmente. Alcuni cookie possono costituire un rischio per la privacy in quanto tengono traccia dei siti visitati. Non sempre è possibile bloccare i cookie, ma è opportuno eliminarli (diversamente i cookie possono rimanere memorizzati nel sistema per settimane o più) - Attivare funzionalità "Do Not Track". "Do Not Track" è un header HTTP che comunica ai siti visitati e alle terze parti i cui contenuti sono ospitati in tali siti che le proprie attività non devono essere tracciate. **Nota Bene.** L'invio di una richiesta "Do Not Track" ai siti non garantisce la protezione della privacy. I siti possono scegliere di rispettare la richiesta o continuare a eseguire attività che potrebbero essere considerate di monitoraggio anche se è stata espressa questa preferenza. - Utilizzare la navigazione anonima. **Nota Bene**. Il livello di protezione è diverso a seconda dei browser. In certi casi si tratta fi una difesa da attacchi locali: alcune info, come le password, la cronologia di ricerca e la cronologia delle pagine, vengono eliminate alla chiusura della scheda. In altri casi si tratta della difesa dall'attaccante esterno ossia viene protetto l'**anonimato durante la navigazione**. - Disattivare la condivisione della posizione geografica.

Hardening del browser: configurazione di base per la sicurezza	
Minaccia	- Attacchi all'integrità dei sistemi. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	La configurazione di default per molti browser web non è sicura. Si raccomandano i passaggi a seguire per rendere maggiormente sicuro il browser web in uso. Tali impostazioni assumono particolare importanza nel caso in cui si utilizza il browser per accedere a sistemi aziendali o più in generale se si utilizza il browser per accedere, inviare o ricevere informazioni sensibili. - Impostare il browser di default: o Firefox: sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > scheda Generale. Selezionare la casella "Controlla sempre se Firefox è il browser predefinito". o Safari: andare nel menu Safari > Preferenze > scheda Generale e clicca sul pulsante "Imposta predefinito....". o Internet Eplorer: si raccomanda di non utilizzare IE come browser predefinito. o Google Chrome: andare sulle impostazioni nella sezione "Browser predefinito" e cliccare sul pulsante "Imposta come predefinito" in corrispondenza della voce "Imposta Google Chrome come browser predefinito". - Mantenere il software del browser aggiornato. - Abilitare nel browser gli aggiornamenti automatici e mantenerli in tale stato: o Firefox: sia per Mac che per Windows - vai al menu Firefox >

Preferenze (Mac), scheda Opzioni (Windows), scheda Generale > sezione Aggiornamenti di Firefox. Selezionare "Installare automaticamente gli aggiornamenti (consigliato)".
    - Safari: gli aggiornamenti in Safari sono gestiti nel menu Apple in Preferenze di sistema > Aggiornamento software. Impostare su Aggiornamenti giornalieri.
    - Google Chrome: a garanzia di protezione, Google Chrome si aggiorna automaticamente ogni volta che rileva che è disponibile una nuova versione del browser. Il processo di aggiornamento avviene in background e non richiede alcuna azione manuale.
- Bloccare l'accesso ai pop-up, plug-in e ai siti di phishing:
    - Firefox: per il blocco dei pop-up indesiderati, sia per Mac che per Windows – andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Permessi. Selezionare "Blocca le finestre pop-up".
    - Firefox: per il blocco delle estensioni del browser indesiderate, sia per Mac che per Windows – andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Permessi. Seleziona "Avvisa se un sito web tenta di installare un componente aggiuntivo".
    - Safari: per il blocco dei pop-up indesiderati, andare nel menu Safari > Preferenze > scheda Siti web, fare clic su "Finestre di pop-up" dal pannello di sinistra e impostare "Quando si visitano altri siti web:" su "Blocca e notifica".
    - Safari: per il blocco del phishing e delle estensioni del browser indesiderate, andare nel menu Safari > Preferenze > Scheda Siti Web e deselezionare i plug-in installati indesiderati presenti nel pannello di sinistra.
    - Edge: per il blocco dei pop-up indesiderati, andare su Impostazioni > Impostazioni avanzate > Blocca popup e impostarlo a Attivato.
    - Internet Explorer: per il blocco dei pop-up indesiderati, andare nel menu Strumenti > Opzioni Internet > scheda Privacy. Selezionare la casella di controllo "Attiva Blocco popup".
    - Internet Explorer: per il blocco delle estensioni del browser indesiderate, andare nel menu Strumenti > Opzioni Internet > scheda Avanzate e scorrere verso il basso fino a "Elementi multimediali". Deselezionare se selezionate, "Riproduci animazioni" e "Riproduci suoni" in pagine web.
    - Google Chrome: per il blocco dei pop-up indesiderati, andare su Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Pop-up e reindirizzamenti e impostare su "Bloccato".
    - Google Chrome: per il blocco delle estensioni del browser indesiderate, andare su Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Accesso al plugin senza sandbox e impostare su "Chiedi conferma quando un sito vuole utilizzare un plug-in per accedere al tuo computer (opzione consigliata)".
- Impostare il browser in modo tale da non salvare le password. Diversamente se strettamente necessario, utilizzare un meccanismo di master password conforme allo standard UCSC[4]:
    - Firefox: sia per Mac che per Windows - andare nel menu Firefox >

[4] https://its.ucsc.edu/security/passwords.html

Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Privacy del browser > Credenziali e password. Deselezionare la casella di controllo "Chiedi se salvare le credenziali di accesso ai siti Web".

- Firefox: per l'utilizzo di una master password, se è necessario salvare le password, impostare una password Master in modo che le password salvate non siano facilmente accessibili a chiunque abbia accesso al sistema. Sia per Mac che per Windows- andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Privacy del Browser > Credenziali e password. Selezionare "Utilizza una password principale".
- Safari: andare nel menu Safari > Preferenze > Scheda Riempimento automatico e deselezionare la casella "Nomi utente e password".
- Edge: andare nel menu Impostazioni > Impostazioni avanzate > Privacy e servizi > "Offri la possibilità di salvare le password" e impostare a Disattivato e "Salva i dati immessi nei moduli" a Disattivato.
- Internet Explorer: andare nel menu Strumenti > Opzioni Internet > Scheda Contenuto e fare clic sul pulsante Impostazioni di "completamento automatico" e deselezionare la casella "Nome utente e password sui moduli".
- Internet Explorer: IE non ha una funzione master password, ma sarebbe opportuno disabilitare la funzione di completamento automatico per le password. Vedere l'indicazione precedente.
- Google Chrome: andare nel menu Impostazioni > Compilazione automatica > Password e disattivare "Chiedi di salvare le password".

- Disabilitare i third-party cookie.
  - Firefox: sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > Blocco contenuti. Seleziona "Personalizzato" e imposta i cookie per bloccare "Traccianti di terze parti". Abilitare anche i controlli per bloccare i criptominer e le Fingerprinter.
  - Edge: andare nel menu Impostazioni > Impostazioni avanzate > "Privacy e servizi" quindi attivare "Invia richieste Do Not Track", disattivare "Mostra suggerimenti per la ricerca e i siti durante la digitazione", impostare i Cookie su "Blocca solo i cookie di terze parti", disattivare "Usa la previsione della pagina per velocizzare l'esplorazione, migliorare la lettura e migliorare l'esperienza nel complesso" e abilitare "Proteggi il PC da siti e download dannosi con il filtro SmartScreen".
  - Internet Explorer: andare nel menu Strumenti > Opzioni Internet > scheda Privacy e fare clic sul pulsante "Avanzate". Selezionare la casella "Accetta" per i cookie dei siti Web visualizzati e il pulsante "Chiedi conferma" per i cookie di terze parti. Il pulsante "Accetta sempre i cookie della sessione" non dovrebbe essere selezionato. Fare clic su OK. Al termine, fare clic sul pulsante Applica.
  - Google Chrome: andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Cookie > e attivare "Consenti ai siti di salvare e leggere i dati dei cookie (opzione consigliata)" e "Blocca cookie di terze parti".
- Impostazioni specifiche per tipologia di browser:
  - Firefox: installare l'estensione del browser "uBlock Origin" per il blocco degli annunci.
  - Firefox: contenuto ingannevole e protezione da software pericoloso -

sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Sicurezza. Spuntare "Blocca contenuti a rischio e ingannevoli", "Blocca download a rischio" e "Avvisa in caso di software indesiderato e non scaricato abitualmente".

- Firefox: raccolta e utilizzo dei dati Firefox – sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > Raccolta e utilizzo dati di Firefox. Deselezionare "Consenti a Firefox di inviare a Mozilla dati tecnici e relativi all'interazione con il browser", "Consenti a Firefox di installare e condurre studi" e "Consentire a Firefox di inviare segnalazioni di arresto anomalo in sospeso".
- Safari: disabilitare Java. Andare nel menu Safari > Preferenze > Scheda Sicurezza e impostare il segno di spunta per abilitare "Avvisa quando visiti un sito web fraudolento" e un segno di spunta per "Abilita JavaScript".
- Safari: privacy - andare nel menu Safari > Preferenze > scheda Privacy e selezionare "Prevent cross-site tracking".
- Safari: apertura in modo sicuro dei file scaricati - andare nel menu Safari > Preferenze > scheda Generale. Deselezionare la casella di controllo che indica "Open 'safe' files after downloading".
- Edge: disattivare Flash – andare nel menu Impostazioni > Impostazioni avanzate > "Usa Adobe Flash Player" e impostare su Disattivato.
- Internet Explorer: impostare le security zones, ovvero i livelli di sicurezza per le aree "Internet", "Intranet locale", "Siti attendibili" e "Siti con restrizioni".
- Internet Explorer: disattivare il filtro ActiveX - aprire IE, premere il tasto Alt, aprire il menu Strumenti, e cliccare su "ActiveX Filtering", se non è già spuntato.
- Internet Explorer: suggerimenti aggiuntivi – IE dispone di zone di sicurezza che possono essere impostate per diversi livelli di protezione. Aprire IE, premere il tasto Alt, aprire il menu Strumenti, e cliccare su "Opzioni Internet", selezionare la scheda "Sicurezza". Si consiglia di impostare il livello di sicurezza per l'area "Internet" su ALTA. È inoltre possibile identificare i "Siti attendibili" e impostarli su MEDIO-ALTA.
- Google Chrome: andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > JavaScript e attivare "Consentita (opzione consigliata)".
- Google Chrome: fare in modo che per l'esecuzione di contenuti Flash venga chiesto il consenso - andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Flash > e impostare su "Chiedi prima".
- Google Chrome: download automatici - andare in Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Download automatici e impostare su "Chiedi conferma quando un sito tenta di scaricare automaticamente file dopo il primo file (opzione consigliata)".
- Google Chrome: accesso alla videocamera - andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Videocamera e impostare su "Chiedi prima di accedere (opzione consigliata)".
- Google Chrome: accesso al microfono: andare nel menu Impostazioni