	informazioni riservate, ma piuttosto di tentare di comprendere appieno ogni richiesta ricevuta prima di effettuare qualsiasi scelta; - non consegnare mai informazioni personali o riservate a individui o aziende sconosciuti; - eliminare messaggi e-mail che richiedono informazioni riservate o l'. Se la richiesta appare legittima, verificatene telefonicamente l'autenticità; - non disabilitare le protezioni aziendali antivirus, anti-phishing/pharming o altre misure di sicurezza (ad esempio quelle del browser); - contattare l'assistenza IT nel caso di comunicazioni ricevute per e-mail, telefono, fax o messaggistica immediata, che richiedono informazioni aziendali o personali.

Security awareness: prevenzione infezioni da malware	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger).
Contromisure	Verificare il contenuto della clipboard prima di incollarlo su un terminale o sulla barra degli indirizzi del browser web o all'interno di un messaggio di posta elettronica; Scaricare e installare software solo da siti web riconosciuti e certificati; Non aprire file o archivi sospetti; Su Windows non aprire file eseguibili (EXE) privi di firma digitale, né file CMD, BAT, REG. Su sistemi Windows o anche UNIX (dotati di interfaccia grafica tipo KDE o GNOME), non aprire mai i file con un doppio click in base all'icona visualizzata: visualizzare e controllare sempre l'estensione del file, perché un eseguibile contenente un malware può celarsi dietro l'icona falsificata di un file PDF o altro; Indipendentemente dalla piattaforma in uso, Linux o Windows, controllare i file di installazione software attraverso l'uso di programmi capaci di rilevare la presenza di malware.

5.2.11 Sicurezza di macOS

La sicurezza del sistema operativo macOS è importante, ma spesso trascurata. Mantenere la privacy e proteggere i dati è estremamente importante per ogni utente del sistema. Eppure, molte volte si dedica poca attenzione a tali aspetti e si fa poco più del minimo indispensabile, se non altro per garantire che gli hacker, e terze parti, siano in grado di accedere il meno possibile ai dati personali presenti nel sistema. Tuttavia, macOS rende la sicurezza dei dati molto semplice, grazie a una serie di strumenti disponibili nelle "Preferenze di sistema" e in Safari, nonchè in diverse applicazioni distribuite da terze parti. Apple solitamente reagisce in modo rapido quando emergono nuovi malware per il sistema, e dispone di diverse misure messe in atto al fine di proteggere il proprio software dalle minacce conosciute. Tuttavia, è possibile in taluni casi che compaiano dei malware non riconosciuti e pertanto potrebbe essere necessario apportare le opportune modifiche al modo in cui si utilizza il sistema, in attesa che si renda disponibile la necessaria protezione. Esistono tre fonti distinte da cui è possibile che provengano delle minacce: via Internet, via e-mail o da qualcuno che ha accesso diretto alla postazione di lavoro. In linea generale, adottando le opportune misure di protezione verranno ridotti al minimo i rischi.

Segue un elenco di best practices generali per la sicurezza di questo sistema:

- Impostazioni di sicurezza e privacy. Partendo dalle impostazioni di base del Mac che dovrebbero essere controllate al fine di garantire la adeguata sicurezza, verificare le impostazioni presenti nella finestra di "Sicurezza e privacy" disponibile nelle "Preferenze" di sistema. Ivi sono presenti quattro

schede (Generale, FileVault, Firewall e Privacy) che controllano i vari aspetti della sicurezza del sistema. In primo luogo abilitare il firewall, che blocca qualsiasi connessione di rete in entrata indesiderata. Si potrebbe pensare che il firewall sia abilitato per impostazione predefinita, ma spesso non lo è. È importante notare che il Firewall di macOS, sebbene utile, offre solo una protezione limitata dal malware. Questo perché protegge il sistema solo dal traffico in entrata. Il suo compito è quello di limitare le applicazioni e servizi nell'accettazione delle connessioni in entrata. Non fornisce alcun controllo sulle connessioni in uscita, vale a dire le applicazioni e i servizi che istaurano una connessione. Così, ad esempio, se si scarica del malware, il firewall di macOS non interromperà la connessione a Internet. A volte si sceglie di bloccare anche le connessioni di rete in uscita in modo che alcune applicazioni non possano "comunicare indebitamente con l'esterno". Ciò significa anche che un eventuale malware installato accidentalmente non è in grado di sottrarre impropriamente dati senza venirne a conoscenza.

- Utilizzo di una password. Nella sezione Generale della finestra "Sicurezza e Privacy", sono presenti tre impostazioni a cui si dovrebbe prestare particolare attenzione: La prima è quella che ci consente di impostare una password per l'account in uso, se non lo si abbia già fatto, o di cambiarla se lo si ritiene necessario. La seconda ci permette di specificare se è necessaria una password per sbloccare la postazione Mac, quando questa va in standby o quando parte uno screen saver. È possibile scegliere di richiederla immediatamente, o dopo un certo tempo prestabilito di inattività successivo all'avvio o un certo numero di screen saver. Se si lavora in un ufficio con altre persone, è opportuno considerare la possibilità di attivare tale impostazione. Esiste anche un'opzione per disattivare il login automatico, cosa che si dovrebbe fare. Si può anche scegliere di consentire ad un dispositivo "Apple Watch" di sbloccare la postazione Mac. Con questa opzione abilitata tutto ciò che è necessario fare è indossare l'Apple Watch. In tal caso la postazione Mac si sblocca automaticamente quando ci si trova nelle vicinanze. (Non è possibile utilizzare questa impostazione se la Condivisione Internet è attiva). Parlando di password, dobbiamo ricordare che una buona password dovrebbe essere difficile da ricordare. Inoltre, queste non devono essere assolutamente scritte. Fortunatamente, Apple fornisce "iCloud Keychain" come modo per ricordare le password e suggerirne di nuove da utilizzare tramite il generatore di password casuale incorporato. Con "iCloud Keychain" attivo è sufficiente effettuare il login con l'Apple ID per inserire automaticamente la password richiesta per accedere a qualsiasi servizio o sito web. L' "iCloud Keychain" può memorizzare tutti i dati dell'account, numeri di carta di credito e altre informazioni personali (comprese le impostazioni per le e-mail, contatti, calendari e servizi di social network) rendendoli automaticamente disponibili in caso di necessità di accesso attraverso una qualsiasi postazione Mac o dispositivo iOS.
- Impostazioni di download delle App. Nella parte inferiore della scheda "Generale" della finestra "Sicurezza e Privacy" sono presenti due opzioni che definiscono le modalità di download ed esecuzione delle applicazioni sulla postazione Mac. L'opzione più sicura, ma più limitativa, è quella di consentire l'esecuzione solo alle app scaricate dell'App Store. L'altra opzione è comunque un buon compromesso, in quanto consente di eseguire applicazioni scaricate dall'App Store e da fonti di sviluppo note ad Apple. Nelle vecchie versioni di MacOS esisteva un'opzione per consentire l'esecuzione di applicazioni provenienti da qualsiasi fonte. Se si dispone di tale opzione è fortemente sconsigliato usarla. Sarà comunque possibile eseguire un'applicazione che non provenga dall'App Store o da una fonte di sviluppo riconosciuta, ma sarà necessario fornire l'approvazione prima che questa possa essere eseguita.
- Abilitazione del FileVault. Con FileVault attivo, tutti i file dell'account utente verrano criptati. Per poterli decriptare, è necessario digitare la password dell'account o la chiave di recupero creata all'atto dell'attivazione di FileVault. Per la maggior parte degli utenti, l'inconveniente di dover digitare una password per aprire un file, insieme al tempo inizialmente necessario per crittografare tutti i file presenti sulla postazione Mac, supera i vantaggi della sicurezza. Nonostante ciò, se si intende mantenere il più possibile sicuri i dati memorizzati sulla postazione, è consigliabile attivare tale funzionalità.

- Impostazioni relative alla privacy. La scheda "Privacy" presente nella finestra di "Sicurezza e Privacy", copre una serie di diversi controlli e impostazioni. Questi sono: "Servizi di localizzazione" che consente di controllare quali applicazioni hanno accesso ai dati di localizzazione. È possibile disattivare completamente i Servizi di localizzazione o impedire alle singole applicazioni di accedere a tali dati. Allo stesso modo, "Contatti", "Calendario" e "Promemoria" consentono di specificare quali app installate sulla postazione Mac possono accedere alle informazioni memorizzate dalle relative app di default dell'OS X. Inoltre è presente la sezione "Accessibilità". In questa sezione è possibile impostare quali applicazioni in qualche modo possono controllare la postazione Mac. Ad esempio, Deeper e Onyx consentono di modificare le impostazioni di sistema che normalmente richiederebbero gli opportuni comandi da terminale. Infine, l'opzione "Analytics" è stata aggiunta in macOS “High Sierra”, la quale consente agli sviluppatori di Apple e alle app in generale di migliorare i propri prodotti sulla base delle informazioni raccolte riguardo l'utilizzo delle app stesse. In tal senso, è possibile scegliere di non condividere tali informazioni.
- Verifica delle impostazioni di privacy in Safari. A differenza delle "Preferenze di Sistema", Safari dispone di diverse impostazioni che permettono di controllare gli aspetti di privacy. La prima è la finestra "Privacy", accessibile dal menu "File" (o Shift+comando+N), che consente di visitare siti web, senza che questi vengano registrati nel menu "Cronologia" o in qualsiasi altro punto del sistema. La seconda è "Clear History", accessibile dal menu "Safari", che cliccata periodicamente, cancella i cookie e altri dati memorizzati nella cache dei siti visitati rimuovendoli anche dal menu "Cronologia". Nelle "Preferenze di Safari", la sezione "Privacy" permette di evitare il tracciamento da parte dei siti web durante la navigazione in rete e di controllare quali siti possono memorizzare i cookie nel sistema. In passato era possibile specificare come i dati relativi alla posizione potevano essere resi disponibili tramite questa finestra, ma dalla versione “High Sierra”, tali impostazioni sono state trattate in una scheda separata, ovvero in "Siti web" > "Posizione". Qui è possibile scegliere di impostare Safari per negare come impostazione predefinita il rilascio di informazioni sulla posizione o consentire a siti web specifici di accedere alla posizione della postazione di lavoro. Relativamente alle impostazioni di archiviazione delle credenziali di accesso per un sito web, o dei dati personali, nelle sezioni "Riempimento automatico e Password" togliere la spunta sulle caselle che abilitano tali servizi.
- Verifica di ciò che viene condiviso. Il sistema operativo Mac è in grado di condividere file con altri sistemi Mac e può condividere dati in diversi altri modi, inclusa la condivisione dell'intero schermo per facilitare l'attività lavorativa da remoto. Ad esempio, per poter utilizzare la condivisione dello schermo, è necessaria una password, e questo potrebbe portare a considerare sicuro il servizio, ma esiste comunque la possibilità in cui la presenza di una difettosità nel servizio di condivisione potrebbe renderlo vulnerabile da un punto di vista della sicurezza. In generale, è buona pratica disattivare qualsiasi servizio di condivisione che non viene utilizzato. Nello specifico:
    - Condivisione dello schermo - Utilizzato principalmente in ambienti aziendali per consentire agli addetti all'assistenza tecnica di vedere o controllare lo schermo di una macchina remota, e di eseguire correzioni e/o aggiornamenti. Anche le macchine Windows e Linux, attraverso l’uso del servizio VNC, possono controllare lo schermo di un computer Mac. In tal caso assicurarsi che questo venga disattivato.
    - Condivisione di file – questo servizio consente ad altri computer in rete di accedere al file system del computer Mac. Tecnicamente parlando, abilita la condivisione del file system di Windows (SMB), Apple Filing Protocol (AFP) e Network File Service (NFS). Il sistema di file sharing del Mac veniva utilizzato nel passato dal servizio “Back To My Mac”, integrato in iCloud, ma Apple lo rimosse con l’uscita della versione di sistema “Mojave”. “Back To My Mac” consentiva di accedere da un sistema Mac, via Internet (anche se non ha assolutamente nulla a che fare con iCloud Drive, che svolge una funzione simile), ai file di un altro sistema Mac. Se non si ha la necessità di condividere file in rete e non si utilizza la feature “Back To My Mac”, allora questo servizio dovrebbe essere disattivato.

  - Condivisione delle stampanti – il servizio consente di condividere qualsiasi stampante collegata al sistema Mac, con altri computer presenti sulla rete. Se non si hanno stampanti collegate alla postazione Mac o non si ha la necessità di condividere alcuna stampante, questo servizio dovrebbe essere disattivato.
  - Condivisione della connessione Internet – il servizio consente a un sistema Mac di condividere una connessione di rete con altri Mac. Questo servizio fu concepito ai tempi delle connessione Internet in dial-up. È improbabile che al giorno d'oggi possa essere utilizzata una connessione di questo tipo, visto che oramai si dispone di banda larga e router Wi-Fi. Pertanto questo servizio dovrebbe essere disattivato.
  - Condivisione tramite Bluetooth – il servizio consente a un sistema Mac di inviare e ricevere file da e verso un altro dispositivo abilitato Bluetooth, come un telefono cellulare. L'iPhone e l'iPad non possono condividere file in questo modo, quindi è probabile che lo si possa utilizzare solo con un dispositivo Android. A meno di specifiche esigenze, questo servizio dovrebbe essere disattivato.
- Login remoto. Questo servizio abilita le connessioni al sistema Mac via SSH/SFTP, che per lo più viene utilizzato dai tecnici per operare tramite "command shell" da remoto. A meno di specifiche esigenze, questo servizio dovrebbe essere disattivato.
- Gestione remota. Questo servizio viene solitamente utilizzato in un ambiente aziendale per consentire agli amministratori di accedere al sistema Mac da remoto per poter eseguire le necessarie operazioni di manutenzione del sistema. Nei casi in cui non esiste tale necessità, questo servizio dovrebbe essere spento.
- Eventi remoti Apple. Questo servizio consente ad un sistema Mac di controllarne un altro per stampare, o fare qualsiasi altra cosa, difatti, grazie all'integrazione con AppleScript, è possibile utilizzare gli eventi remoti Apple per far eseguire comandi su un sistema Mac controllati da un altro sistema Mac attraverso sintesi vocale. Utilizzando questo servizio, un programma AppleScript in esecuzione su un sistema Mac può interagire con un altro Mac. Ad esempio, il programma potrebbe aprire e stampare un documento che si trova sul sistema remoto. Normalmente questo servizio dovrebbe essere spento a meno di particolari necessità.
- Applicare una password per l'accesso al firmware. Il sistema Mac è predisposto per utilizzare di default la crittografia di FileVault, il che significa che l'intero disco di avvio viene crittografato ed è impossibile accedervi a meno che non venga sbloccato al login utilizzando la password dell'utente. Tuttavia, ciò non impedisce a chiunque di poter utilizzare una chiavetta di memoria USB per avviare la postazione e potenzialmente cancellare tutti i dati presenti nel disco rigido, o semplicemente reinstallare il sistema operativo. La soluzione è quella di applicare una password per l'accesso al firmware. A differenza della cosiddetta password del BIOS di un PC, la richiesta della password del firmware del sistema Mac appare solo nel momento in cui si tenta di avviare il Mac in modo non standard, vale a dire, tramite una chiavetta USB, o se si tenta di avviare il Mac in Recovery Console. Per attivare la password del firmware è necessario farlo dalla Recovery Console. Da tener presente che, se si dimentica tale password, solo Apple è in grado di sbloccare la postazione.
- Abilitazione dell'utente "guest". L'account "Guest" è essenziale per l'utilizzo del servizio "Trova il Mio Mac", presente in iCloud e che permette di rintracciare un computer Mac smarrito o rubato. Pertanto, non disattivare l'account Guest se è abilitata l'opzione "Trova il Mio Mac" in iCloud.
- Disabilitare il "Security Hole" in FileVault. Quando il sistema Mac entra in modalità sleep (per esempio se si chiude il coperchio di un MacBook Pro), esiste un potenziale problema di sicurezza dovuto al fatto che la chiave necessaria per decriptare con FileVault viene mantenuta in memoria. Anche se molto difficile, in teoria qualcuno potrebbe riattivare il computer e in qualche modo recuperare questa chiave, e quindi avere accesso all'intero contenuto del disco senza la necessità di una password di login. Tuttavia, è possibile impedire che la chiave FileVault venga mantenuta in memoria, anche se questo comporterà a volte la richiesta di digitare due volte la password di accesso alla riattivazione della postazione Mac, e un rallentamento in fase di riattivazione dalla modalità sleep.

- Verificare la presenza di applicazioni persistenti. Alcune applicazioni per il sistema Mac sono progettate per essere esguite in modo silente ad ogni avvio rimanendo invisibili durante l'utilizzo del computer. Queste vengono chiamate applicazioni persistenti, come ad esempio le app di controllo degli aggiornamenti che Google e Microsoft installano per garantire che Google Chrome e Microsoft Office siano sempre aggiornati. Anche Adobe installa alcune applicazioni persistenti come parte del pacchetto "Creative Cloud". Tuttavia, questa tipologia di applicazioni può contenere del malware, e a peggiorare le cose, esistono diverse posizioni all'interno del file system in cui il malware stesso può nascondersi con il fine di essere eseguito in modo del tutto invisibile ad ogni avvio. Riguardo tale problema, esistono due applicazioni gratuite che possono essere utilizzate come supporto per contrastare questo tipo di minaccia. La prima è KnockKnock la quale analizza queste posizioni sul file system, dando evidenza di cosa è presente. Non è uno scanner di malware, quindi non fornisce alcuna indicazione in merito alla pericolosità di ciò che viene rilevato. La seconda applicazione si chiama BlockBlock. Questa viene eseguita in background nel sistema Mac e verifica tutte le posizioni in cui vengono installate le applicazioni persistenti. Se un'applicazione tenta di installare qualsiasi cosa in modo persistente, viene mostrata una finestra di dialogo con una richiesta di conferma per poter procedere. Anche in questo caso, BlockBlock non è uno strumento anti-malware, quindi non è in grado di riconoscere cosa è legittimo è cosa non lo è. Queste applicazioni non risolvono definitivamente il problema, ma impiegate come mezzi di protezione dal malware risultano essere piuttosto efficaci.
- Eseguire le scansioni malware. Poiché OS X/macOS dispone già di un potente strumento anti-malware chiamato Xprotect, il quale è sempre in funzione, non è necessario eseguire alcuna azione in tal senso.
- Abilitare ovunque l'autenticazione a due fattori. L'autenticazione in due fasi è un sistema in cui l'accesso a servizi o siti web richiede più di un semplice nome utente e password. Questa richiede un codice numerico aggiuntivo. Tale codice viene inviato come messaggio di testo o viene generato da una particolare applicazione in esecuzione su un dispositivo mobile (esistono numerose applicazioni di questo tipo, ma per l'iPhone si consiglia Authy). La verifica in due fasi dell'identità viene a volte indicata con il suo nome più tecnico di autenticazione a due fattori, o TFA (two-factor authentication). Questa feature dovrebbe essere abilitata per tutti i siti e servizi a cui si accede. Ad esempio, se si utilizza un qualsiasi servizio di Google come ad esempio Gmail, è possibile abilitare il TFA per accedervi. E' possibile abilitare tale feature anche per i servizi e i siti Microsoft e Dropbox. Ovviamente, non tutti i siti o servizi supportano il TFA. Esistono alcuni siti come "https://twofactorauth.org" i quali forniscono un elenco continuamente aggiornato di quei siti/servizi che supportano tale feature. L'impostazione del TFA è piuttosto semplice. Alcuni siti e servizi inviano un codice all'atto della connessione, che poi deve essere fornito quando richiesto dal servizio stesso, a tal fine è necessario impostare in fase di configurazione del servizio, il numero del dispositivo mobile autorizzato. Per quei servizi o siti che utilizzano un'applicazione come sistema di verifica, come il suddetto Authy, quando si sceglie di configurare il TFA, è necessario utilizzare l'applicazione installata sul cellulare o tablet, quindi scegliere nel servizio di aggiungere un codice e puntare semplicemente la fotocamera del dispositivo mobile verso il codice a barre o QR mostrato nella schermata del sito. Se il dispositivo mobile non è provvisto di fotocamera, è possibile digitare manualmente il codice di autenticazione, che solitamente viene mostrato sotto il codice a barre o QR. Successivamente all'accesso al servizio, terminata la configurazione del TFA, l'applicazione installata nel dispositivo mobile viene avviata richiedendo a sua volta la digitazione del codice visualizzato (solitamente dopo aver inserito la password di accesso all'applicazione stessa), oppure rimanendo in attesa della ricezione di un messaggio di testo/chiamata vocale, prevedendo successivamente la digitazione del codice ricevuto quando richiesto.
- Crittografare le ricerche sulle pagine web. Il Domain Name System, o DNS, converte gli indirizzi basati su nomi di dominio che un essere umano può leggere e ricordare, come ad esempio "www.nomedominio.it", in indirizzi internet numerici IP, maggiormente comprensibili da un computer, come ad esempio "192.161.1.1". Tutti i computer collegati a Internet interagiscono con i

server DNS. Questi vengono resi disponibili dall'Internet Service Provider come parte del pacchetto complessivo dei servizi di rete. Il problema è che, come la maggior parte delle risorse disponibili online, anche i servizi DNS non sono in alcun modo sicuri. In altre parole, tutte le richieste che viaggiano da e verso siti web e che transitano per un DNS possono essere spiate. L'applicazione e il progetto DNSCrypt risolve tale problema semplicemente crittografando le richieste DNS sia da che verso il server DNS. È possibile scaricare questa applicazione dalla home page del progetto e la configurazione, una volta installata, è piuttosto semplice. Con DNSCrypt in esecuzione le ricerche eseguite dalle pagine web divengono immediatamente più sicure.

- Utilizzare una VPN. Non dare mai per scontato che un sistema Mac sia al sicuro quando si utilizza una rete condivisa. Sfortunatamente, è estremamente facile per un malintenzionato spiare i dati trasmessi da e verso i siti web. E' buona pratica utilizzare un servizio di rete privata virtuale (VPN). Questo ha la capacità di cifrare i dati di una comunicazione e di indirizzarli verso un end-point gestito dal servizio VPN. Azioni come la navigazione e il download non hanno alcun effetto sull'utente finale, ma chiunque si trovi sulla stessa rete fisica - come ad esempio un altro computer connesso sulla stessa rete Wi-Fi - viene completamente bloccato per contrastare qualsiasi forma di sniffing sui dati trasmessi o ricevuti dal sistema Mac. In genere, i servizi VPN sono dotati di un'applicazione che viene eseguita quando si desidera utilizzare la connessione VPN, anche se OS X/macOS è dotato di uno strumento VPN built-in che è possibile utilizzare.
- Utilizzare ovunque l'HTTPS. Per ragioni storiche, la maggior parte dei dati viene trasmessa sul web in forma semplice e ciò significa che chiunque li può intercettare durante il transito. Fanno eccezione le connessioni sicure come quelle adottate dalle banche, dai servizi di webmail e dai siti di shopping online. Questi normalmente utilizzano l'HTTP sicuro, e si riconoscono dal fatto che l'indirizzo del sito web inizia con "https://". Se si utilizza un browser che non è Safari - come Chrome o Firefox - installando l'estensione "HTTPS Everywhere" e possibile navigare utilizzando automaticamente l'HTTPS. Questo software è in grado di consultare un database di siti che sono opzionalmente disponibili in HTTPS cambiando automaticamente il protocollo di accesso da HTTP a HTTPS (se disponibile) in fase di accesso. Purtroppo, a causa della modalità di funzionamento di Safari, non è possibile implementare una vera estensione "HTTPS Everywhere" da utilizzare con tale browser e capace di garantirne la massima sicurezza. Tuttavia, l'estensione "SSL Everywhere" disponibile per il browser Apple, consente di ottenere risultati molto simili a "HTTPS Everywhere". L'unica differenza sta nel fatto che quando si accede a un sito web la trasmissione iniziale dei dati non viene crittografata, il che può fornire agli hacker o agli snoop interessati qualche informazione ad essi utile. Tuttavia, una volta che si è passati all'HTTP sicuro - cosa che in sostanza avviene immediatamente dal punto di vista dell'utente finale - tutti i dati vengono ovviamente criptati.
- Verificare i certificati digitali. Se viene mostrato un lucchetto accanto all'indirizzo web presente nella barra degli indirizzi di Safari, è possibile cliccare su di esso per visualizzare le informazioni sul Certificato digitale in uso. In Safari 11, introdotto nel 2017, Apple ha apportato dei miglioramenti nell'interfaccia utente relativamente alla visualizzazione di tali informazioni. Utilizzando l'ultima versione di Safari si dispone di un meccanismo potenziato di "Warnings" riguardo i certificati digitali in uso. Tali "Warnings" indicano chiaramente se una connessione non è privata. Si consiglia pertanto di usare l'ultima versione disponibile di Safari.

Alle linee guida generali, riportate nei paragrafi precedenti e valide per tutti i sistemi operativi, si aggiungono, per l'ambito specifico dei sistemi Mac OS X (con un focus per la versione 10.12), 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 siano impostati i seguenti controlli sulle utenze:

	- L'utente root deve essere disabilitato (default). - L'accesso all'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. - L'accesso dell'utente Guest alle cartelle condivise degli altri utenti deve essere disabilitata. - Bloccare lo schermo dopo 15 minuti di inattività e richiedere la password per sbloccarlo. - Richiedere la password quando il Mac si riattiva da una sospensione.

Servizi di condivisione file obsoleti	
Minaccia	- Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione.
Contromisure	È necessario disabilitare, sui computer Mac, i servizi legacy FTP e NFS che consentono di accedere ai file e alle cartelle del Mac da remoto con protocolli obsoleti e altamente insicuri. In particolare si ricorda che il protocollo FTP richiede l'invio delle credenziali di autenticazione in chiaro sulla rete.

Funzionalità di condivisione	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Negazione dei servizi. - Furto di credenziali di autenticazione.
Contromisure	Mac OS X dispone di numerose funzionalità di condivisione che devono essere disattivate se non effettivamente necessarie. In particolare è necessario disattivare: - "Apple Events" Remoti, per impedire a programmi in esecuzione su Mac remoti di eseguire programmi sul sistema locale. - Condivisione Internet (Internet Sharing), per ridurre la superficie d'attacco del sistema. - Condivisione dello schermo (Screen Sharing), per prevenire il rischio di connessioni remote in grado di visualizzare le operazioni svolte dall'operatore sul sistema locale, a sua insaputa. - Login remoto (Remote Login), per impedire l'accesso remoto al sistema attraverso una sessione terminale all'insaputa dell'utente del sistema locale. In questo caso si disabilita il server SSH, ovviamente solo per i sistemi client dato che sui server, probabilmente, tale servizio risulterà necessario. - Condivisione Bluetooth (Bluetooth Sharing), per ridurre la superficie d'attacco del sistema. - Condivisione File (File Sharing), per disabilitare i servizi SMB (Samba) e AFP, in modo da impedire ogni tentativo di accesso remoto a cartelle e file del Mac. - Gestione Remota (Remote Management), per impedire ogni tentativo di accesso remoto al sistema attraverso il protocollo Apple Remote Desktop (ARD). Tale protocollo dovrebbe essere attivato solo se effettivamente in uso, in abbinamento con controlli di autenticazione basati su un Directory Server, e solo su una rete assolutamente "trusted".

Protocollo Bonjour	
Minaccia	- Accesso non autorizzato al sistema. - Negazione dei servizi.
Contromisure	Se non strettamente necessario (ad es. per un Mac che espone servizi di rete legittimamente), è necessario disabilitare il meccanismo di "advertising" del protocollo Bonjour. Il Bonjour è un protocollo di auto-discovery che consente di enumerare dispositivi e servizi TCP/IP in una rete locale. Un attaccante potrebbe utilizzare le funzionalità di multicast DNS di Bonjour per individuare la presenza di un servizio vulnerabile o non correttamente configurato, o per collezionare informazioni sui servizi esposti da un sistema target. Si noti che alcune applicazioni (come ad es. Final Cut Studio e AirPort Base Station management) potrebbero non funzionare se si disabilita Bonjour.

Estensioni dei nomi file	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	Il Mac OS X non mostra di default l'estensione associata ai nomi dei file. In tal modo l'utente è portato a credere che il tipo file sia quello associato all'icona visualizzata sulla scrivania per quel file. Per evitare che un programma malevolo possa mascherare la sua vera natura attraverso l'icona contenuta nel file stesso, e per evitare errori, è necessario istruire Mac OS (nelle preferenze del Finder) affinché visualizzi sempre l'estensione associata al nome file (es. ".pdf", o ".doc").

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 Mac portatili che contengono informazioni riservate, oppure dati personali sensibili, è necessario proteggere il disco di avvio con il FileVault (impostazioni di Sicurezza & Privacy di sistema). Si tratta di un meccanismo di crittografia del disco di boot (analogo al bitlocker di Windows) che richiede all'avvio una password o una "recovery key". 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 Mac), né comunicate a terzi.

Crittografia dei volumi di backup 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 Time Machine (o altri strumenti di terze parti) per creare volumi di back-up, è necessario abilitare sempre l'opzione che richiede la crittografia di tali

	volumi. Questo controllo va sempre applicato, ma è particolarmente importante nel caso di backup su dischi rimovibili dato che essi possono essere smarriti o rubati. Si pensi ad es. ad un Mac portatile con disco di avvio crittografato con FileVault. Se nella stessa borsa è presente un disco esterno con un volume di back-up Time Machine in chiaro, le informazioni riservate presenti nel Mac sono fortemente a rischio. Più in generale, i dischi esterni rimovibili contenenti informazioni riservate devono essere inizializzati con un file system HFS crittografato (usando lo strumento Disk Utility di Apple).

Controllo sull'origine degli applicativi	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.) - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Per prevenire la possibile introduzione di malware sui Mac è necessario abilitare la funzionalità denominata Gatekeeper. Il Gatekeeper è un meccanismo di controllo di tipo white-listing che impedisce l'esecuzione di applicazioni scaricate, quando sono state rilasciate da fonti sconosciute o non autorizzate.

Host Firewall	
Minaccia	- Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	È necessario abilitare l'host firewall integrato nel Mac OS X (preferenze di sistema, sicurezza e privacy). Nelle opzioni del firewall, abilitare inoltre la modalità stealth, in modo da rendere il sistema meno riconoscibile e più difficilmente individuabile da parte di software di scansione di rete.

Sicurezza del terminale	
Minaccia	- Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione.
Contromisure	Quando si utilizza l'utility di sistema "Terminale" del Mac, è necessario utilizzare sempre la modalità "Input da tastiera sicuro" (Secure Keyboard Entry), visibile nel menù "Terminale" dell'utility. Questo impedisce ad altre applicazioni sul sistema e in rete di leggere o registrare i caratteri digitati sul terminale.

"Safe Files" in Safari	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.) - Attacchi all'integrità dei sistemi (software e configurazioni). - Accesso non autorizzato ai sistemi - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
Contromisure	Un file, la cui tipologia è considerata sicura (Safe Files), viene automaticamente eseguito da SAFARI al termine del download.