CYBER ESSENTIALS CLIENT VADEMECUM

Aprile 2017

Confidence, Assurance and Certainty

CYBER ESSENTIALS

CERTIFICATION EUROPE™

INTRODUZIONE

Questo documento rappresenta un vademecum per aiutare le organizzazioni a trovare risposte concise e puntuali a ciascuno dei quesiti e, di conseguenza, a fornire note e osservazioni su ciascuno dei controlli di sicurezza richiesti prima di poter procedere con il processo di certificazione Cyber Essentials e completare il questionario di valutazione.

Inoltre, questa guida vi aiuterà a comprendere cosa si aspetteranno i valutatori nel momento in cui leggeranno le vostre risposte al questionario Cyber Essentials, così da permettervi di sapere come poter rendere il processo di certificazione più semplice.

Ovviamente, è possibile ottenere la certificazione anche senza seguire i suggerimenti e le linee guida. Tuttavia, il rischio sarebbe, non sapendo come poter soddisfare le aspettative dei valutatori, di dover incorrere in un numero maggiore di richieste di follow-up e chiarienti da parte dell'organismo di certificazione, causando inutili ritardi o costi aggiuntivi.

Questo documento può anche essere utilizzato per aiutrarvi a rispondere a domande specifiche. Quando riterrete di aver risposto a tutte le domande e di aver raccolto evidenze sufficienti a supporto delle vostre risposte, dovrete effettuare il login dal portale web, procedere con il pagemento online e quindi inviare le risposte nel formato richiesto per la valutazione.

Si prega di notare che le evidenze a supporto delle vostre risposte dovranno essere raggruppate e inviate, laddove richiesto, per ciascuno dei controlli in valutazione. Le evidenze dovrebero essere aggiornate e pronte per essere inviate nel momento in cui deciderete di procedere con la compilazione del questionario di valutazione. Inoltre, il questionario di valutazione, una volta completato, dovrà essere controfirmato da parte della vostra Direzione.

CYBER ESSENTIALS, IN BREVE

Uno degli obiettivi principali dello schema Cyber Essentials, è quello di rendere la rete un posto più sicuro per poter condurre business. Tuttavia, saper riconoscere i benefici della sicurezza informativa e comprendere come cominiciare a lavorare su questo aspetto sono sfide decisive per aziende e organizzazioni di tutte le dimensioni.

Questo documento presenterà i requisiti necessari a mitigare le più comuni minacce alla sicurezza dei dati che possono provenire da internet. Sviluppare questi controlli può aiutare le organizzazioni a didendersi dalle forme più comuni di attacchi informatici che possono provenire dalla rete attraverso tool e strumenti ampiamente accessibili a cybercriminali con un livello di conoscenza e tecnica non elevato.Le organizzazione che applicheranno i controlli Cyber Essentials possono confidare nel fatto che le misure tecniche di base siano operative e che i primi importanti passi per proteggere i dati e le informazioni dei propri clienti siano state prese.

Lo schema Cyber Essentials elenca i requisiti di una protezione tecnica basilare dagli attacchi informatici attraverso cinque aree principali:

1. Firewall e Internet Gateways
2. Configurazioni sicure
3. Controllo degli accessi
4. Protezione dei Malware
5. Patch Management

Per implementare questi requisiti, le organizzazioni dovranno definire le propria tecnologia all'interno dello scopo, esaminare ciascuna delle cinque aree e applicare tutti I controlli specifici. Laddove un particolare controllo non possa essere implementato per una reale ragione, controlli alternativi dovrebbero essere identificati e implementati.

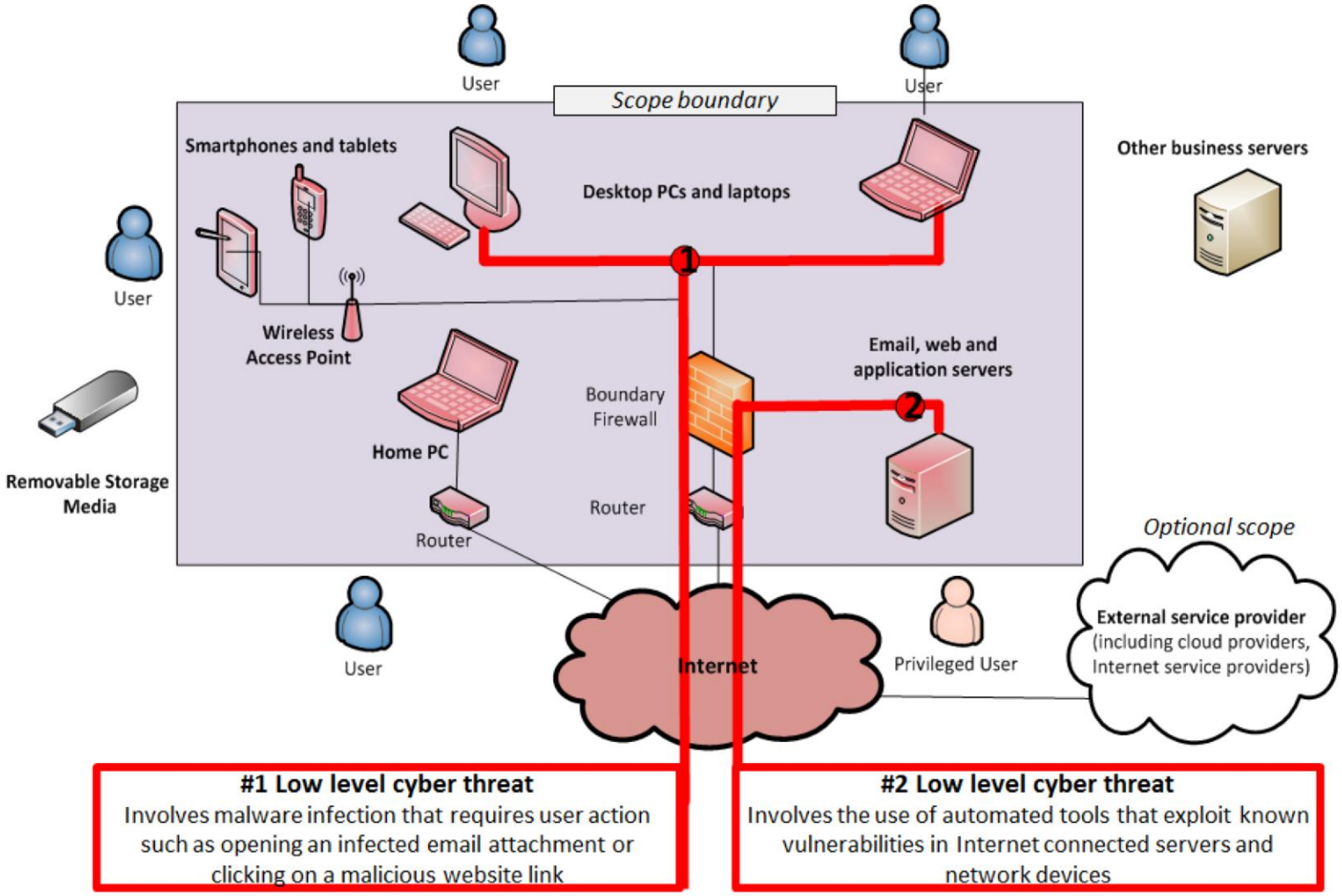

Figura 1: Campo di applicazione dei requisiti per una protezione tecnica di base

CAMPO DI APPLICAZIONE

Tenendo in considerazione quanto illustrato nella Figura 1, è necessario identificare l'ambito di applicazione del sistema (o dei sistemi) che devono essere verificati nel questionario, comprendendo: le sedi, i confini della rete, la gestione e la proprietà. Quando possibile, includere gli indirizzi IP e/o i loro intervalli.

A ciascun sistema sottoposto a valutazione dovrà essere assegnato un nome, il quale sarà utilizzato sui certificati rilasciati (NB: non è consentito assegnare il nome della società, a meno che tutti i sistemi all'interno dell'organizzazione siano verificati).

I dettagli che devono essere inclusi nel campo di applicazione sono:

- Numero di sedi nello scopo e loro localizzazione
- Numero di computer o server collegati e modalità di connessione
- Presenza di aree al di fuori del campo di appliciazione e loro segregazione (NAT/Firefall)
- Descrizione dei servizi cloud in uso (Dropbox, Office 365, Google Drive, ecc..)

Esempio di campo di applicazione

Il campo di applciazione è esteso all'intero ufficio localizzato a Novara in via Roma 5. Sono presenti sei computer operanti con Windows 8 e Windows 10, connessi direttamente a internet attraverso il firewall. La connessione internet è fornita da un noto servizio di banda larga. È presente un firewall, gestito da un fornitore. L'applicazione di backoffice maggiormente utilizzate sono Office 365 e Outlook per le email. Si utilizza dropbox per lo scambio di informazioni e documenti non sensibili. Un altro utente è presente due volte a settimana, il quale è escluso dal campo di applicazione e non ha accesso al nostro sistema IT, ma che utilizza la nostra rete wireless ospiti su di una connessione separata.

1 FIREWALL E INTERNET GATEWAYS

Firewall, internet gateways o dispositivi di rete equvalenti vengono utilizzati per proteggere da accessi non autorizzati e fuga di dati tramite internet. Se i dispositivi di rete non sono correttamente configurati, gli incursori possono riuscire ad accedere ai computer ed alle informazioni che essi contengono.

Un firewall di confine può proteggere contro le minacce dirette ai nostri sistemi reppresentate da malware, virus, trojans ed altre minacce basate su tecniche e competenze note e facilmente accessibili traminte internet limitando il traffico in ingresso e in uscita tra il sistema interno e l'esterno alle sole connessioni autorizzate. Queste restrizioni si ottenfono agendo sulle impostazioni di configurazione del firewall.

Devono essere presenti e politiche ed istruzioni per amministrare e gestire queste impostazioni. Laddove possibile, per dimostrare la conformità, devono essere fornite fotografie, log files, o screenshot

#	Domande	Risposta	Suggerimenti e linee guida
1.1	Give the details of any firewall or equivalent network devices Fornire i dettagli sui firewall o sui dispositivi di rete equivalenti		Riferimento o dettagli relative al fornitore ed al modello del dispositivo; specifiche tecniche e impostazioni di configurazionie.
1.2	Who is responsible for the administration of the devices? Chi è il responsabile per la gestione dei dispositivi?		Fornire dettagli su persone o fornitori che gestiscono il firewall o i dispositivi di sicurezza perimetrale (ad esempio, personale interno altamente qualificato o fornitore IT esterno)
1.3	Who is responsible for setting usernames and passwords the devices?		Come sopra

#	Domande	Risposta	Suggerimenti e linee guida
	Chi è il responsabile della configurazione di username e password dei dispositivi?		
1.4	Have the default passwords of the network firewall or alternative device been changed to use alternative and strong passwords or passphrases? Sono state modificate le password di default del dispositivo con nuove password sicure e complesse?		In genere, una password è complesse quando: • Comprende un numero minimo di caratteri • È differente dall'username di accesso associato • Non ripete più di due volte consecutive lo stesso carattere alfanumerico • È composta da un misto di caratteri testuali e numerici • Non è stata utilizzata in un periodo precedente (ad esempio negli ultimi 6 mesi) • Non è la stessa utilizzata per altri account
1.5	What approval process is in place for authorising network traffic to pass through the boundary devices? Quale procedura è in opera per autrizzare il traffico di rete attraverso il perimetro?		Ogni servizio o computer accessibile attraverso il firewall di confine deve essere soggetto all'approvazione da parte di personale autorizzato (necessaria documentazione con motivazione delle esigenze aziendali di approvazione)

#	Domande	Risposta	Suggerimenti e linee guida
1.6	Have unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), been disabled (blocked) at the boundary firewall or devices by default? Il firewall e i dispositivi assicurano di avere disabilitato come impostazione predefinita l'accesso a servizi non approvati o più tipicamente vulnerabili agli attacchi (quali Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh o rexec)?		I servizi che sono più facilmente vulnerabili afli attacchi come Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh o rexec devono essere disabilitati come impostazione di default al perimetro della vostra rete. Si prega di verificare e confermare.
1.7	Do you have a corporate policy covering all firewall rules? If some rules are no longer required are they removed or disabled in a timely manner? Is this policy adhered to (meaning that there are currently no open ports or services that are not essential for the business)? Disponete diistruzioni aziendali che tratti delle regole relative ai firewall? Se alcune regole non sono più necessarie, assicurate di averle tempestivamente rimosse o disabilitate? Le regole vengono rispettate (nel senso che si assicura che non ci siano porte aperte o servizi		Indicare il nome delle regole (se esistenti) o fornire dettagli necessari o descrivere processi alternativi in campo per poter garantire quanto richiesto.

#	Domande	Risposta	Suggerimenti e linee guida
	autorizzati non essenziali per la vostra attività)		
1.8	In what circumstances is the administrative interface used to manage boundary firewall configuration accessible from the internet? In quali circostanze l'interfaccia di gestione per la configurazione dei firewall viene utilizzata tramite internet?		Ad esempio: i firewall sono configurati da remoto? In quali circostanze questo avviene? Chi se ne occupa?
1.9	Confirm that where there is no requirement for a system to have internet access, a default deny policy is in effect and that it has been applied correctly, preventing the system from making connections to the internet Confermare la presenza e la funzionalità di impostazioni predefinite che impediscano l'accesso a internet per i sistemi ogni volta che non ce ne sia necessità.		Descrivere le impostazioni attuali dei firewall (o dei dispositivi di confine), le regole e le motivazioni per i dispositivi che non necessitano di accesso a internet.

2 CONFIGURAZIONI SICURE

I computer e i dispositivi di rete devono essere configurati per ridurre il livello di vulenerabilità intrinseca e per fornire solo i servizi necessari alla propria funzione.

I computer e i dispositivi di rete (inclusi gli access point wireless) non possono essere automaticamente considerati sicuri al momento dell'installazione. La configurazione standard (out-of-the-box) include spesso un account amministrativo con una password predefinita (e pubblicamente nota), un o più account utente non necessari (talvolta con privilegi di accesso speciali) e applicazioni e servizi pre installate e non necessarie.

L'installazione di default di computer e di dispositivi di rete può permette agli incursori informatici diverse opportunità per riuscire ad accedere alle informazioni sensibili di un'organizzazione, spesso senza grosse difficioltà.

Adottando alcuni semplici controlli di sicurezza durante l'installazione di computer e dispositivi di rete (una tecnica conosciuta come *hardening* del sistema, a richiamare l'inspessimento dei confini), si possono ridurre alcune debolezze intrinseche, fornendo una maggiore protezione contro gli attacchi informatici.

#	DOMANDE	RISPOSTA	SUGGERIMENTI E LINEE GUIDA
2.1	Have all unnecessary or default user accounts been deleted or disabled in all computers and network devices? Tutti gli account utente non necessari predefiniti e non necessari sono stati disabilitati in tutti i computer e i dispositivi di rete?		Come lo sapete? Chi ha la responsabilità di controllare? Descrivere il processo ed assicurare che sia stato fatto
2.2	Do all accounts have passwords? Please confirm that any default passwords have been changed to strong passwords.		Si prega di descrivere come ci si assicura che il requisite sia rispettato e di speficifare eventuali controlli tecnici sulle password necessari per la modifica delle password o, in

#	Domande	Risposta	Suggerimenti e linee guida
	Tutti gli account sono protetti con password? Si prega di confemrare che ogni password predefinita sia stata modificata con una password complessa		alternativa le regole interne per richiedere l'utilizzo di password complesse.
2.3	Are all unnecessary software (including application, operating system utilities and network services) is removed or disabled? Vi siete assicurati che ogni software non necessario (incluse applicazioni, utilità di sistema e servizi di rete) siano stati rimossi o disabilitati?		Descrivere chi è l'incaricato per la gestione dei computer e dei dispositivi di rete e come ci si assicura che siano stati installati solo software e applicazioni approvate.
2.4	Has the auto-run feature been disabled? È stata disabilitata la funzione di esecuzione automatic?		La funzione di esecuzione automatica deve essere disabilitata per evitare che programme entrino automaticamente in esecuzione, ad esempio, nel momento in cui un dispositivo di archiviazione esterna (penna USB, hard disk esterno, SD...) è connesso al computer o quando si accede alle caselle di rete. Uno screenshot di come la funzione di esecuzione automatica sia stata disabilitata è richiesta come evidenza del controllo.
2.5	Has a personal/host based firewall (or equivalent) been enabled on desktop PCs and laptops, and configured to disable unapproved connections by default?		Fornire evidenza di come i personal firewall o altri sistemi equivalenti siano installati sui computer e come essi siano configurati per limitare le connessioni di rete in entrata ed in

#	Domande	Risposta	Suggerimenti e linee guida
	Sono stati abilitati gli host-based firewall (firewall personali) sui pc desktop, laptop ed altri dispositivi? Sono configurati per disabilitare automaticamente connessioni non approvate?		uscita da e verso le applicazioni autorizzate (ad esempio browser web e client email)
2.6	Is a standard build image used to configure new workstations? Does this image include the policies and controls and software required to protect the workstation? Is the image kept up to date with corporate policies? Si utilizza un'immagine di sistema standard per configurare le nuove workstations? Questa immagine di sistema include le regole, i controlli e i software necessari per proteggere la workstation? L'immagine di sistema viene costantemente aggiornata con le regole e le politiche dell'organizzazione?		Chi ha creato l'immagine di sistema? Fornire i dettagli sull'incaricato interno o il fornitore esteno che ce ne è occupato. Chi ha la resposnabilità di mantenere l'immagine di sistema aggionata? Se, invece, non vengono utilizzate immagini di sistema, ci sono istruzioni di configurazione e pratiche di installazione seguite? Se sì, quali?
2.7	Do you have a backup policy in place, and are backups conducted regularly? Avete regole di backup? Vengono eseguiti backup a intervalli regolari?		Un robusto processo di backup è fondamentale per poter garantire il recupero dei dati (e la continuità operativa del business) nel caso di attacchi di software malevoli quali malware o ransomware.

#	Domande	Risposta	Suggerimenti e linee guida
			Descrivere il proprio processo di backup (online, su disco, ecc con tempistiche e programmazione)

3 CONTROLLO DEGLI ACCESSI

Gli account utente, in particolare quelli con privilegi di accesso speciali (ad esempio gli account amministrativi), dovrebbero essere assegnato solo a persone autorizzate e gestiti in maniera efficace per fornire ul livello di accesso che non vada oltre al minimo necessario per reti, PC, applicazioni.

Gli account utenet con privilegi speciali di accesso come amministratori, hanno in genere il più alto livello di accesso alle informazioni, alle applicazioni ed ai computer. Quanto gli account amministrativi vengono compromessi, il loro livello di accesso privilegiato può essere utilizzato per irrompere ed accedere a un grande numero di informazioni, colpire i processi operativi dell'orgnizzazione e fornire accessi non autirizzati ad altri computer.

Per proteggersi contro l'abuso di poteri privilegiati di accesso, il principio del prviliegio minimo deve essere applicato agli account utente, limitando accessi e privilegi concessi laddove possibile

#	DOMANDE	RISPOSTA	SUGGERIMENTI E LINEE GUIDA
3.1	Are user account requests subject to proper justification, provisioning and an approvals process, and assigned to named individuals? Le richieste per la creazione di utenti sono soggette a adeguate giustificazioni? Si provvede acreare un processo di assegnazione ed approvazione degli utenti?		Descrivere il processo necessario all'attivazione di nuovi utenti o fare riferimento a procedure per l'apertura, la modifica o la chiusura di account, se presenti. Nel descrivere il processo, assicurarsi di fare riferimento specifico a come un nuovo account debba essere richiesto, approvato e quali sono le responsabilità ed i compiti assegnati.
3.2	Are users required to authenticate with a unique username and strong password		Le buone prassi richiedono che tutti gli utenti abbiano il proprio account protetto da

#	Domande	Risposta	Suggerimenti e linee guida
	before being granted access to computers and applications? Viene richiesto agli utenti di autenticarsi con username e con una password complessa prima di poter accedere ai PC ed alle applicazioni?		una password complessa che non deve essere condivisa. Descrivere il processo attraverso il quale si assicura che gli utenti non condividano le priprie informazioni di login e come password forti vengano richieste.
3.3	Are accounts removed or disabled when they are no longer required? Gli account non più necessary vengono disabilitati e rimossi?		Gli account utenti con privilege speciali di accesso dovrebbero essere rimossi o disabilitati ogniqualvolta essi non siano più necessari (ad esempio, ogni volta che una persona cambia ruolo o lascia l'organizzazione). Descrivere il processo per rimuovere o disabilitare gli account nel caso in cui qualcuno lasci l'organizzazione o fare riferimento a processi di rimozione adottati.
3.4	Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorised individuals? Si limitano i privilegi di accesso speciali (ad esempio gli account admin) a un numero limitato di persone autorizzate?		Quale ruolo hanno le persone autorizzate? Per quale motivo richiedono ed utilizzatno gli accessi priviliegiati o come amministratori?

#	Domande	Risposta	Suggerimenti e linee guida
3.5	Have special access privileges been documented and reviewed regularly (e.g. quarterly)? I privilege di accesso speciali sono documentati? Vengono rivisti con cadenza periodica (ad esempio trimetsrale)?		Mostrare come i privilegi di accesso sono documentati (foglio di calcolo, database, documento di testo, ecc...) e quando è stata fatta l'ultima verifica dei privilege di accesso
3.6	Are all administrative accounts only permitted to perform administrator tasks, with no internet or external email permissions? Tutti gli account amministrativi vengono utilizzati esclusivamente per le operazioni amministrative, escludendo quindi accessi a internet o a servizi email?		Quali controlli sono adottati per prevenire l'accesso ad internet ed ai servizi email tramite account admin con privilegi di accesso? Descrivere le configurazioni di account, se possibile.
3.7	Do you have a password policy or process which requires or enforces changing administrator passwords (e.g. at least every 60 days) to a complex password? Disponete di regole per le password o processi che richiedono o impongono di		Come vi assicurate che gli account amministrativi siano configurati per richiedere la modifica della password con cadenza regolare?

#	Domande	Risposta	Suggerimenti e linee guida
	modificare le password di accesso degli amministratori con password complesse (ad esempio ogni 60 giorni)?		

4 PROTEZIONE DA MALWARE

Ogni computer connesso ad internet deve essere protetto da infezioni da malware attraverso l'uso di software specifici anti-malware

I computer, in particolare quelli esposti e connessi a internet, sono spesso vulnerabili di fronte all'attacco di software specificatamente progettati per danneggiarli (i cosiddetti malware). Esistono software specifici necessari per monitorare, riconoscere e disattivare i malware.
I malware possono infettare i computer in diversi modi. Spesso, comunque, sono coinvolti utenti che aprono mail infette, navigano su siti compreomessi oppure aprono file sconosciuti da unità di archiviazioni rimovibili (penne USB).
I PC desktop, i laptop e i server che hanno accesso o sono accessibili da internet devono, secondo lo scopo di questo documento, essere protetti da malware. Sebbene fuori dal campo di applicazione specifico, anche gli altri computer e dispositivi portatitli come smartphone e tablet dovrebbero essere protetti.

#	DOMANDE	RISPOSTA	SUGGERIMENTI E LINEE GUIDA
4.1	Has malware protection software been installed on all computers within scope? I computer all'interno del campo di applicazione definite sono stati protetti da software anti-malware?		Si riporti il nome del software e la tipologia di protezione (es: antivirus, endpoint…) utilizzata
4.2	How often does malware protection software have all of its updates applied, and is this applied rigorously? Con quale frequenza il software di protezione da malware viene completamente aggiornato? Gli		I software di protezione da malware devono essere configurati per aggiornarsi automaticamente a seguito del rilascio degli aggiornamenti software da parte dei loro programmatori. Descrivere come è configurato il proprio sistema di

#	Domande	Risposta	Suggerimenti e linee guida
	aggiornamenti sono rigorosamente applicati?		aggiornamento della protezione anti malware.
4.3	Have all anti malware signature files been kept up to date (through automatic updates or through centrally managed deployment)? La lista delle firme dei malware (signature) è mantenuta aggiornata (tramite aggiornamenti automatici o distribuzione degli aggiornamenti gestita centralmente)?		Descrivere il processo in grado di assicurare che tutti i files delle signature siano aggiornati
4.4	Has malware protection software been configured for on-access scanning, and does this include downloading or opening files, opening folders on removable or remote storage, and web page scanning? Il software di protezione da malware è stato configurato per la scanione all'accesso, comprensiva delle attività di downloading, aperture files, aperture cartelle su unità di archiviazione esterne (USB) o remote e scansione di pagine web?		In che modo vi assicurate che il software di protezione da malware sia configurato per scansionare automaticamente i files al momento del loro accesso (ad esempio prima del loro download, della loro apertura, del loro accesso da unità esterna o remota) e che scansioni le pagine web attraverso il browser al momento del loro accesso?

#	Domande	Risposta	Suggerimenti e linee guida
4.5	Has the malware protection software been configured to run regular (at least daily) scans? Il software di protezione da malware è stato configurator per eseguire scansioni regolari (ad esempio quotidianamente)?		Descrivere il programma di scansioni dettagliato (scansioni complete, scansioni veloci, scansioni di sistema, ecc...)
4.6	Apart from Anti-Virus Software, how are your commonly accessed executables protected from being attacked by malicious files? Oltre che attraverso i software antivirus, come è organizzata la protezione dall'esecuzione di file eseguibili malevoli?		Quali meccanismi sono adottati per assicurare che, nel caso in cui un utente clicchi su un link malevolo (ed esempio all'interno di un'email), il file eseguibile non venga lanciato? Ad esempio, il software vi notifica il rischio attraverso un pop up?
4.7	Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function? L'accesso ai siti web riconosciuti dannosi viene impedito agli utenti da parte del software di protezione malware attraverso la creazione di una blacklist?		Il vostro software di protezione da malware previene l'accesso ai siti conosciuti come dannosi? Oppure è prevista una soluzione alternativa per proteggersi da siti potenzialmente dannosi o poco raccomandabili, ad esempio tramite il settaggio di firewall personalti oppure tramite software di web filtering?

5 PATCH MANAGEMENT

Per il proprio funzionamento, ciascun computer o dispositivo di rete è basato su software, il quale può contenere debolezze o difetti o altre vulnerabilità tecniche.
Anche in molti tra i software più polpolari emergono vulnerabilità con frequenza elevata e quasi quotidiana. Una volta individuata la vunerabilità del software, individui o organizzazioni con finii malevoli possono rapidamente sfruttarla per attaccare i computer o le reti ad essi collegate.
I fornitori di software, in genere, provano a risolvere le vulnerabilità note non appena possibile, tramite aggiornamenti di software (chiamati patch) che rilasciano ai propri clienti (talvolta utilizzando un programma ufficiale di aggiornamento con cadenze predefinite).

Per evitare di essere vittime di cyber attacchi che sfruttano le vulnerabilità note dei software installati, le organizzazioni devono gestire le patch e gli aggiornamenti di software in maniera efficace.

#	Domande	Risposta	Suggerimenti e linee guida
5.1	Is all software installed on computers and network devices in the scope licensed and supported? Il software installato sui computer e sui dispositive di rete inclusi all'interno del campo di applicazione definite è autorizzato e supportato da aggiornamenti?		Come garantite che il software in escuzione su computer e dispositivi connessi alla rete sia autorizzato e supportato da parte del fornitore o dai programmatori al fine di garantire che siano rese disponibili patch di sicurezza per ogni vulnerabilità scoperta?
5.2	Are all operating system security patches applied within at least 14 days of release?		Descrivere il processo che assicura che le patch rese disponibili per il proprio sistema operativo (es: Microsoft Windows) siano installate entro il termine concordato

#	Domande	Risposta	Suggerimenti e linee guida
	Le patch si sicurezza del sistema operativo sono applicate almeno entro 14 giorni dal loro rilascio?		
5.3	Are all application security patches applied within at least 14 days of release? Le patch si sicurezza delle applicazioni sono applicate almeno entro 14 giorni dal loro rilascio?		Descrivere il processo che assicura che le patch rese disponibili per le applicazioni utilizzate (es: Microsoft Office o Adobe Photoshop) siano installate entro il termine concordato
5.4	Is out-of-date software (i.e. software that is no longer supported) removed from a computer or network device? Il software obsolete e non più supportato viene rimosso dai computer e dai dispositivi di rete?		Descrivere il processo che identifica e rimuove il software obsoleto
5.5	Is there a mobile working policy in force that requires mobile devices ((including BYOD (Bring Your Own Device)) to be kept up to date with vendor updates and application patches? Esistono delle istruzioni (quali le BYOD - Bring Your Own Device) in vigore per coloro che lavorano in mobilità che richieda che dispositivi portatili (smartphone, tablet) siano mantenuti aggiornati con aggiornamenti e patch rilasciate?		Descrivere la presenza e l'utilizzo di strumenti non aziendali, se applicabile, e la loro eventuale connessione alle reti aziendali. È presente una rete "ospiti/guest" alla quale essi si possono connettere? Si prega inoltre di riferire quale tipo di lavoro viene svolto da tali dispositivi. Nel caso in cui non esista una politica BYOD, come vi assicurate che software dannosi possano entrare all'interno della vostra rete interna tramite dispositivi non protetti?

NOTE

NOTE