5.2.7 Documentazione

Valgono i principi generali introdotti nel paragrafo [rif. 5.1.5].

5.2.8 Logging

Valgono i principi generali introdotti nel paragrafo [rif.5.1.6].

5.2.9 Antivirus

Prevenzione e individuazione di codice malevolo sul sistema operativo	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, causata da Malware. - Negazione dei servizi causata da Malware. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Su sistemi sia client sia server è necessario installare un software antivirus e antimalware di riconosciuta efficacia, in grado di rilevare e rimuovere keylogger, spyware, trojans, worms, ransomware ed ogni altro tipo di malware conosciuto. I sistemi devono essere configurati in modo che l'antivirus/antimalware: - sia eseguito in modo automatico all'avvio della macchina senza possibilità di disattivazione da parte di utenti non autorizzati; - esegua in automatico l'aggiornamento della lista di definizione dei virus (DAT) anche più volte al giorno mediante un'infrastruttura di sistemi dedicati alla distribuzione del DAT; - esegua una scansione approfondita del disco fisso almeno una volta alla settimana, in orari che riducano l'impatto sulle attività lavorative (ad es. durante la pausa pranzo); - esegua una scansione anche dei file compressi fino a 3 livelli di nidificazione; - preveda una gestione remota per la segnalazione di infezioni virali; - abbia funzionalità di tipo euristico per la rilevazione dei virus che consenta di inserire in "quarantena" tutti i file ritenuti sospetti dal motore euristico; - si integri nel sistema operativo al livello di file system e nel software di gestione della posta; - notifichi, durante la fase di shutdown, se è presente un dispositivo removibile. L'amministratore di sistema deve verificare (e se necessario effettuare manualmente) l'effettivo aggiornamento dei sistemi anti-virus con cadenza almeno mensile.

5.2.10 Procedure

Alle linee guida 'Procedure generali' (Change management, Maintenance, Patching, Secure testing, Disposal) introdotti nel paragrafo [rif. 5.1.7], si aggiungono, per l'ambito specifico, le indicazioni di cui di seguito:

Controlli sulla regolamentazione dell'uso del codice mobile per Sistemi Operativi	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, causata da Malware. - Negazione dei servizi causata da Malware. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Nel caso in cui si utilizzi "mobile code" (ad es. JavaScript / VBScript scaricati da siti web, Java applets, controlli ActiveX, codice Adobe Flash o Shockwave, documenti PDF attivi

	o anche semplici macro VBA trasferite attraverso documenti Microsoft Office), è necessario controllare che il "mobile code" non effettui operazioni non autorizzate. In particolare è necessario predisporre il maggior numero possibile di controlli tra quelli di seguito elencati: - esecuzione del mobile code in un ambiente di test isolato logicamente (sistemi di malware analysis in grado di analizzare il mobile code); - blocco di ogni utilizzo di mobile code sulle postazioni di lavoro e sui server; - blocco della ricezione di mobile code da internet (operato dai firewall perimetrali); - attivazione delle misure tecniche disponibili sul browser in uso per bloccare o quanto meno mettere in sicurezza l'utilizzo del mobile code, ad es. impedendo che il mobile code possa eseguire qualsiasi operazione sul sistema operativo, o all'esterno di una "sandbox" predisposta dal browser; - limitazione delle risorse di sistema che possono essere utilizzate dal mobile code; - attivazione di controlli crittografici per autenticare il mobile code (firma digitale del codice).

Controlli dell'installazione di software sui sistemi in funzione	
Minaccia	- Negazione dei servizi. - Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Devono essere in vigore procedure per controllare l'installazione ed i cambiamenti del software sui sistemi di produzione. L'installazione deve essere effettuata seguendo scrupolosamente le indicazioni scritte fornite dal produttore e rispettando l'ordine delle operazioni da compiere. Nelle procedure devono essere indicate le istruzioni per i controlli che possono variare in relazione alla tipologia di ambiente/sistema operativo.

Autorizzazione per trasferimento di informazioni, strumenti elettronici e supporti all'esterno	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Uso non autorizzato di privilegi. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Il trasferimento all'esterno del sito aziendale o dell'organizzazione di informazioni contenute su strumenti o supporti elettronici, oppure in altre tipologie di supporti (es. atti e documenti cartacei) deve avvenire mediante preventiva autorizzazione dei soggetti responsabili. Per il trasferimento di archivi contenenti dati personali presso fornitori esterni operanti nell'Unione Europea, è necessaria l'autorizzazione del Titolare e può richiedere l'aggiornamento dell'informativa agli utenti laddove necessario. Il fornitore esterno deve essere formalmente nominato responsabile del trattamento. Il trasferimento di tali archivi all'esterno dell'Unione Europea deve essere impedito.

Security awareness: come combattere il phishing/pharming	
Minaccia	- Divulgazione di informazioni riservate. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Sensibilizzare il personale sui rischi del phishing/pharming (divulgazione non autorizzata a terzi di informazioni riservate o critiche, perdita delle informazioni ad es. da ransomware, ecc.). Istruire il personale sulle norme di comportamento cui attenersi per diminuire i rischi di phishing/pharming. Tali norme dovrebbero, almeno, indicare di: - non fare affidamento sull'intuito per distinguere tra richieste legittime e illegali di