	anti-phishing native, o in alternativa utilizzare un software anti-malware dotato di estensioni anti-phishing per i browser adottati dall'organizzazione.

5.7.9 Anti-Spam

Software anti-Spam	
Minaccia	Negazione dei servizi.
Contromisure	Installare sul Mail Server un software anti-spam che aggiorni il proprio database delle "firme" almeno una volta al giorno. Il software deve avere la funzione di auto-apprendimento in modo da incrementare l'accuratezza del filtraggio, e deve eseguire il filtraggio dei messaggi sospetti mediante analisi di tipo: - Semantico, ovvero la rilevazione in base a parole chiavi (ad es. Viagra, sesso, Prozac, etc.); - Euristico, ovvero individuare la posta ricevuta con comportamento anomalo (ad esempio con un numero insolitamente elevato di destinatari, con l'assenza dell'indirizzo del mittente o con l'indirizzo del mittente identico a quello del destinatario). Inoltre il software deve usare una specifica tecnica di blocco dei messaggi sospetti in base al mail server di provenienza come, ad esempio, la tecnica DNSBL (DNS-based Blackhole Lists) che si avvale dell'ausilio di una lista pubblicata su internet, che viene manutenuta costantemente da terze parti ed in cui sono elencati i servers che favoriscono lo spam (ad es. server SMTP Open Relay, server che emettono spam, ISP che supportano lo spam, etc.).

5.7.10 Procedure

A i principi generali già introdotti nel paragrafo [rif. 5.1.7] (i principi generali si applicano sia ai MailServer quanto che ai Mail Client), si aggiungono le seguenti indicazioni per il contesto specifico:

Uso corretto della posta elettronica	
Minaccia	- Abuso di risorse. - Attacchi all'integrità dei sistemi. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione.
Contromisure	- Evitare l'uso dell'e-mail a fini diversi da quelli strettamente aziendali (ad esempio, per iscriversi a mailing list, forum, chat, blog, etc.) che non siano attinenti alla funzione svolta. - Non cliccare mai direttamente su un link presente in una e-mail per accedere a un sito web contenente informazioni sensibili. Copiare e incollare il testo del collegamento in una nuova finestra del browser e verificare l'URL per assicurarsi che la sessione inizi dall'indirizzo autentico conosciuto del sito, senza che vengano aggiunti altri caratteri. - Controllare che la pagina web del sito dell'eventuale istituto creditizio a cui conduce un link presente in una e-mail, disponga di un certificato digitale attendibile, ovvero appartenente al legittimo proprietario, e che tale certificato sia ancora valido. Ad esempio, nelle versioni più recenti di diversi browser comunemente disponibili è sufficiente cliccare con il pulsante destro del mouse in un punto qualsiasi della finestra del browser e selezionare "Proprietà" dal menu a comparsa, dopo aver visualizzato la finestra "Proprietà", occorre cliccare su "Certificati" per controllarne la validità ed attendibilità.

Sensibilizzazione del personale sui rischi di infezione da malware	
Minaccia	- Attacchi all'integrità dei sistemi. - Furto di credenziali di autenticazione. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Sensibilizzare il personale sui rischi di infezione da malware. Ad esempio, informare sui rischi derivanti dal phishing/pharming (divulgazione a terze parti d'informazioni riservate o critiche quali, ad esempio, dati personali, password, numeri di conto o carta di credito) sui sintomi di infezione e sulla protezione di PC e dispositivi portatili. 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 informazioni riservate; - non consegnare mai informazioni personali o riservate a individui o aziende sconosciuti; eliminare messaggi e-mail che richiedono informazioni riservate. 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.

Procedura di monitoraggio sull'uso del mail server	
Minaccia	- Abuso di risorse. - Negazione dei servizi.
Contromisure	Definire procedure che specifichino le modalità con cui monitorare il mail server per garantirne la funzionalità e l'uso corretto. La procedura deve specificare cosa monitorare (ambito del monitoraggio) e quando eseguire l'audit rimanendo conformi ai requisiti di legge e alle politiche aziendali. Un monitoraggio di base dovrebbe considerare i carichi medi del traffico email e delle risorse del sistema: analizzando in tempo reale tali parametri e le loro deviazioni rispetto ai valori attesi, si possono trovare indizi di problemi e attacchi. La procedura deve specificare la frequenza con cui effettuare i controlli ogni qual volta sussista la necessità (non meno di una volta al giorno).

Accordi con i Service Provider	
Minaccia	Negazione dei servizi.
Contromisure	Considerare le seguenti linee guida per i contratti con i service provider di posta elettronica: - stabilire livelli di servizio garantiti, accettabili per l'organizzazione; - ottenere la garanzia di ottenere dal provider il massimo supporto in caso di attacco, per individuare gli indirizzi di rete (IP) degli aggressori mediante un percorso a ritroso, e per bloccare l'attacco.