5.8.9 Procedure

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.7].

5.8.10 Informazioni addizionali

Gli standard citati per mettere in sicurezza l'ESB (Security Assertion Markup Language (SAML), WS-Security, eXtensible Access Control Markup Language (XACML), ecc.) sono implementati e resi fruibili da soluzioni COTS (Commercial Of The Shelf), la cui adozione indirizza molte delle best practices descritte.

Riferimenti	
SAML, XACML, etc	Gli standard citati per mettere in sicurezza l'ESB (SAML - Security Assertion Markup Language, WS-Security, XACML - eXtensible Access Control Markup Language, ecc.) sono implementati e resi fruibili da soluzioni **COTS** (Commercial Of The Shelf), la cui adozione indirizza molte delle best practices descritte nei paragrafi precedenti.
Web Services	Per informazioni sulle problematiche di sicurezza relative alla tecnologia dei Web Services, visitare il sito: https://www.us-cert.gov/bsi/articles/best-practices/assembly-integration-and-evolution--security-concept-challenge-and-design-considerations-web-services-integration.

5.9 Sicurezza del pacchetto MS Office

5.9.1 Hardening

Hardening della suite Office	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Limitare/Disabilitare/Condizionare l'uso di contenuti attivi. Per contenuti attivi si intendono: - i controlli ActiveX, - i componenti aggiuntivi quali, ad esempio: • Componenti aggiuntivi COM (Component Object Model) • Componenti aggiuntivi Visual Studio Tools per Office (VSTO) • Componenti aggiuntivi di automazione • Server RTD (RealTimeData) • Componenti aggiuntivi di applicazioni, ad esempio file con estensioni wll, xll e xlam • Pacchetti di espansione XML • Fogli di stile XML • Macro VBA
Riferimenti	- Pianificare le impostazioni di sicurezza per i controlli ActiveX in Office 2013, https://technet.microsoft.com/it-it/library/cc179076.aspx - Pianificare le impostazioni di protezione per i componenti aggiuntivi per Office

	2013, https://technet.microsoft.com/it-it/library/ee857086.aspx - Pianificare le impostazioni di protezione per le macro VBA per Office 2013, https://technet.microsoft.com/it-it/library/ee857085.aspx

Hardening della suite Office	
Minaccia	Accesso non autorizzato alle informazioni. Attacchi all'integrità dei sistemi. Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Bloccare i contenuti esterni, come: Immagini, elementi multimediali, Hyperlinks, Connessioni dati, Templates, etc. I contenuti esterni possono nascondere Web beacons (che minano la privacy) o malware (con svariati esiti).
Riferimenti	- Blocco o sblocco di contenuti esterni in documenti di Office, https://support.office.com/en-us/article/Block-or-unblock-external-content-in-Office-documents-10204ae0-0621-411f-b0d6-575b0847a795?CorrelationId=2589076c-bc38-4c1e-bac5-317c19aed229&ui=en-US&rs=en-US&ad=US&ocmsassetID=HA010065176

Hardening della suite Office	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	I documenti possono contenere grandi quantità di informazioni nascoste: - Nome utente, organizzazione - Storia delle modifiche, aggiunte, cancellazioni - Note, Commenti - Testo nascosto - Un intero foglio di calcolo "dietro" a un semplice diagramma (con cifre confidenziali!) - A volte anche blocchi casuali di memoria - Proprietà del server di documenti (se il documento fosse stato salvato in un server di gestione dei documenti, che ad esempio si basa su Microsoft Windows SharePoint Services, il documento potrebbe contenere informazioni aggiuntive relative a quel server). Per rimuovere tali informazioni, utilizzare lo strumento di Office denominato "Document Inspector".
Riferimenti	- Remove hidden data and personal information by inspecting documents, https://support.office.com/en-us/article/Remove-hidden-data-and-personal-information-by-inspecting-documents-356b7b5d-77af-44fe-a07f-9aa4d085966f - Using the document inspector, https://msdn.microsoft.com/en-us/vba/office-shared-vba/articles/using-the-document-inspector

Hardening della suite Office	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - (Zero-day-exploits).
Contromisure	- Bloccare (in via temporanea) l'apertura e/o il salvataggio di certi di tipi di file. Ciò attenua il rischio di attacchi alla sicurezza di tipo zero-day, impedendo temporaneamente agli utenti di aprire tipi di file specifici, nell'attesa di

	aggiornamento software o un Service Pack. - Attivare la funzionalità "Convalida file di Office". Tale funzionalità consente di individuare e prevenire un tipo di exploit noto come "file format attack" o "file fuzzing attack" (la struttura del file viene modificata al fine di aggiungere malware). In pratica se "Convalida file di Office" determina che la struttura di un file (prima ancora di essere aperto) non è conforme a tutte le regole descritte nello schema, il file non supera la convalida.
Riferimenti	- Pianificare le impostazioni di blocco dei file per Office, https://technet.microsoft.com/it-it/library/cc179230.aspx

Hardening della suite Office	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	- Limitare/Disabilitare i servizi, basati su Internet, che contribuiscono a proteggere e migliorare le applicazioni di Office (ad esempio quelli che inviano le informazioni dei messaggi di errore a Microsoft), al fine di controllare la divulgazione di informazioni private (privacy). - Attivare la funzionalità di "Visualizzazione protetta". La "Visualizzazione protetta" protegge da diversi tipi di exploit poiché apre i documenti in una sandbox (un ambiente isolato da dove risulta difficile sferrare attacchi). In Visualizzazione protetta: • i contenuti attivi non sono abilitati • gli utenti possono visualizzare il contenuto di un file ma non possono eseguire operazioni di modifica, salvataggio o stampa, né visualizzare le eventuali firme digitali del file. - Limitare/Disabilitare l'uso dei meccanismi: • Trusted Documents • Trusted Locations • Trusted Publishers Tali meccanismi infatti by-passano molti controlli di sicurezza. In particolare tutti i contenuti di un "trusted document" o di un documento preso da una "trusted location", o firmati da un "Trusted Publisher" sono immediatamente attivi all'apertura del documento.
References	- Pianificare le impostazioni di Visualizzazione protetta per Office 2013, https://technet.microsoft.com/it-it/library/ee857087.aspx - Trusted documents, https://support.office.com/en-us/article/Trusted-documents-cf872bd8-47ec-4c02-baa5-1fdba1a11b53 - Pianificare e configurare le impostazioni di Percorsi attendibili per Office 2013, https://docs.microsoft.com/it-it/previous-versions/office/office-2013-resource-kit/cc179039(v=office.15)?redirectedfrom=MSDN

Hardening del sistema operativo che ospita la suite	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Eseguire l'hardening del sistema operativo che ospita la suite Office. L'hardening del sistema operativo è oggetto di un paragrafo specifico [rif. 5.2.2].