APPENDICE AL CAPITOLATO TECNICO

Gara per l'acquisizione di beni e servizi di sicurezza per il Ministero dell'Economia e delle Finanze e la Corte dei conti

acronimi

CMA	Customer Management Add-on
ETSI	European Telecommunications Standards Institute
HA	High Availability
ICSA	International Computer Security Association
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion Prevention System
MDS	Multi-Domain Security Management
MEF	Ministero dell'Economia e delle Finanze
NAC	Network Access Control
NGF	Next-Generation Firewall
OPSEC	Open Platform for Security
PoE	Power over Ethernet
RTI	Raggruppamento Temporaneo d'Imprese
SIEM	Security Information and Event Management
SOAP	Simple Object Access Protocol
SPOF	Single Point of Failure
UTM	Unified Threat Management
VdC	Verifica della Conformità
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WAF	Web Application Firewall

1. PIATTAFORMA DI RISK MANAGEMENT

1.1 DESCRIZIONE

L'Amministrazione, sulla base dei propri obiettivi di governo della sicurezza, ha evidenziato l'esigenza di acquisire una soluzione di Risk Management. Tale soluzione dovrà consentire di realizzare un sistema di Security Governance per una gestione efficace ed efficiente dei processi aziendali in conformità ai principali standard internazionali e alle best practice di settore.
La gestione degli aspetti organizzativi e procedurali legati all'Information Technology risulta un elemento critico per le attività dell'Amministrazione, sia a causa dell'evoluzione dello scenario normativo, sempre più articolato (D.Lgs. 196/03, Amministratori di Sistema, etc.), sia a causa della rapida evoluzione delle tecnologie utilizzate, che inevitabilmente portano con sé numerose minacce per le informazioni trattate e per le risorse aziendali.
L'obiettivo dell'Amministrazione è la creazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di cui il Risk Management è una componente che potrà integrarsi in una più ampia soluzione di Governance, Risk e Compliance.

1.2 REQUISITI GENERALI

1.2.1 RISK MANAGEMENT

L'attività di gestione del rischio (Risk Management) è un processo che ha come obiettivo il governo della sicurezza delle informazioni attraverso la realizzazione e la gestione di interventi di tipo tecnologico, organizzativo e logistico in funzione del grado di sicurezza richiesto dagli obiettivi aziendali. Il fine principale di tale attività è quello di mitigare i rischi in modo da svolgere la mission aziendale, relativamente alla sicurezza, nelle migliori condizioni possibili.
La soluzione deve consentire di automatizzare le attività di Risk Management fornendo una metodologia consolidata e aderente a standard internazionali e a normative e vincoli legali; tale metodologia deve assicurare che le valutazioni del rischio forniscano risultati comparabili e riproducibili.

La soluzione deve fornire supporto per le decisioni in materia di sicurezza informatica nelle fasi di:

- Valutazione del Rischio
    - Analisi del rischio
        - Identificazione del perimetro d'intervento

- Identificazione e classificazione delle risorse aziendali (fisiche e logiche), delle informazioni trattate e dei flussi interni al perimetro di analisi del rischio
- Gestione della documentazione acquisita nella fase di rilevazione dello scenario (architetture IT, flussi dei dati scambiati, etc.) e nella fase di intervista con i responsabili (questionari)
- Individuazione delle minacce, degli attacchi e delle vulnerabilità relative agli aspetti di sicurezza (tecnologici, organizzativi, normativi e procedurali) del perimetro di analisi del rischio

o Valutazione del rischio
- Valutazione delle gravità delle minacce e della priorità di intervento per ogni vulnerabilità riscontrata. Deve essere possibile valutare vulnerabilità riscontrate da attività esterne alla soluzione quali, ad esempio, attività di vulnerability assessment (applicativi e di sistema), di audit interni, di incident management, etc.
- Possibilità di personalizzazione della gravità delle minacce e della priorità di intervento

• Trattamento del Rischio
  o Generazione di proposte di contromisure per abbattere il rischio (il database delle contromisure deve esser aggiornato a fronte dell'uscita di nuove minacce con una periodicità non superiore a sei mesi)
  o Scelta delle misure di protezione (comprensive di prescrizioni legali, regolamenti e vincoli contrattuali) congruenti con i risultati dell'analisi del rischio
  o Pianificazione delle attività (tempi e costi) da svolgere per implementare le contromisure individuate ed approvate dal management
  o Assegnazione e gestione degli owner delle attività scaturite dalle contromisure approvate
  o Storicizzazione delle contromisure individuate
  o Verifica dell'efficacia nel tempo delle contromisure adottate
  o Documentazione di tutte le contromisure (attuate, da attuare, non applicabili, etc.)
• Accettazione del rischio
  o Supporto nell'attività di presentazione dei risultati al management volti all'accettazione del rischio (accettato, modificato, trasferito, evitato) in considerazione dei criteri definiti dall'Amministrazione
• Comunicazione del rischio

  - Definizione e generazione della documentazione di tutte le attività relative al governo della sicurezza delle informazioni (Dichiarazione di Applicabilità, elenco contromisure implementate, scartate, etc.)
- Monitoraggio
  - Definizione e generazione della documentazione a supporto della verifica periodica dello stato delle contromisure implementate
- Segnalazioni: generazione di alert personalizzabili per segnalare i punti di scopertura di sicurezza dell'ambito analizzato
- Dashboard: visione d'insieme attraverso dashboard e report di sicurezza e compliance realizzati per destinatari e ruoli differenti all'interno dell'organizzazione
- ENISA: recepimento delle indicazioni fornite dall'European Network and information Security Agency per la fase di Risk Management
- Supporto alle normative: supporto almeno per le seguenti normative:
  - Privacy (D.Lgs. 196/2003)
  - Provvedimento del Garante sugli Amministratori di sistema (27/11/2008)
  - Standard ISO/IEC 27001
  - Open Web Application Security Project (OWASP)
  - ITIL
- ulteriori standard e best practice di interesse per l'Amministrazione sono:
  - ISO/IEC 22301:2012 (Business Continuity)
  - ISO/IEC 24762:2008 (Disaster Recovery)
  - ISO/IEC 18044:2004 (Gestione degli incidenti)
  - PCI-DSS
- Mappatura delle politiche e dei vincoli contrattuali: Il sistema deve permettere di definire delle policy che descrivano le politiche aziendali interne e i vincoli contrattuali adottati. Tale policy devono consentire la gestione delle contromisure.

1.3 CARATTERISTICHE DELLA SOLUZIONE

1.3.1 REQUISITI DI SISTEMA

La soluzione deve offrire le seguenti funzionalità:

- Architettura web-based: console di gestione centralizzata in grado di definire opportuni indicatori che permettano di mantenere sotto controllo, in modo organico e completo, i risultati ottenuti dalle attività di analisi di sicurezza (siano esse di natura organizzativo-procedurale o di natura tecnica). Deve essere compatibile con i browser più recenti

- Profilatura: possibilità di configurare più ruoli di "amministratore di sistema"
- Scalabilità: possibilità di adattare le componenti hardware a nuove necessità in termini di storage e computazionali
- Storage: utilizzo di Storage Area Network per il database della soluzione

1.3.2 GESTIONE REPORTISTICA

- Report di alto livello (summary) e di dettaglio relativi alle contromisure tecniche e organizzative
- Report diversificati per unità organizzative, dipartimenti, gruppi e aree a cui sono destinati
- Report diversificati in base ai perimetri analizzati
- Report comparativi fra analisi storicizzate
- Possibilità di personalizzazione dei grafici da includere nei report.

1.3.3 MIGRAZIONE DATI DELLE ANALISI DEL RISCHIO EFFETTUATE

I dati presenti nel prodotto "Defender Manager" (attualmente in possesso dell'Amministrazione) dovranno essere migrati nella nuova soluzione di Risk Management.
I servizi necessari all'attività d'importazione devono essere previsti e compresi nella fornitura del prodotto.
Il corso di formazione sull'uso della soluzione saranno specificati nella componente di gara relativa ai servizi professionali.

Allo scopo di consentire una stima delle attività necessarie alla migrazione dei dati attualmente contenuti in Defender Manager, di seguito è descritta una panoramica delle analisi effettuate:

Perimetri analizzati (sistemi/applicazioni) attraverso lo strumento: 22

Tipi di Informazioni classificati e valutati (Riservatezza/Integrità/Disponibilità): 43

"Componenti", di seguito elencati, definiti per le applicazioni: 5

- Database
- Crittografia
- Aspetti organizzativi e procedurali
- Software
- Web Application (custom consip).

"Componenti", di seguito elencati, definiti per l'infrastruttura: 10

- Ambienti fisici
- Cavi elettrici/dati
- Dispositivi ICT
- Impianti elettrici
- Aspetti organizzativi (IO Locale)
- Personale
- Rete
- Supporti di memorizzazione
- Sistema Operativo
- WebServer.

1.3.4 INTEROPERABILITÀ CON SOLUZIONI ESTERNE

- Importazione: la soluzione deve essere in grado di importare ed interpretare i risultati prodotti dalle scansioni dei seguenti vulnerability scanner:

  - "HP WebInspect", per le web application e i web service
  - "IBM Enterprise Scanner" e "Nessus", per i sistemi operativi
- la soluzione deve essere in grado di importare le informazioni collezionate dal sistema SIEM "RSA enVision"
- la soluzione deve essere in grado di importare le informazioni collezionate dal sistema "SkyBox" utilizzato per la valutazione del rischio relativa ai componenti di sicurezza e di rete
- la soluzione deve essere in grado di integrarsi con i processi di change management secondo lo standard ITIL in particolare con:
  - la soluzione deve essere in grado di importare le informazioni presenti nella soluzione per il Change Management "BMC" (asset inventory con CMDB)
  - In particolare deve essere possibile l'importazione di informazioni e l'invio di segnalazioni (apertura ticket) da e verso la soluzione di Trouble Ticketing "Remedy" e USU Valuemation.

Nel caso in cui la soluzione offerta non sia nativamente compatibile con i prodotti precedentemente riportati, dovranno essere predisposti specifici connettori per l'integrazione. Tale attività farà parte della configurazione del prodotto e sarà quindi a totale carico dell'Impresa.

L'offerta dovrà essere comprensiva delle componenti hardware e software. E inoltre si precisa che dovranno essere comprese nell'offerta l'installazione, la configurazione, la migrazione e il supporto professionale per l'implementazione della soluzione.