Premio FORUM PA 2017: 10x10 = cento progetti per cambiare la PA

Documentazione di progetto della soluzione:

Business Continuity, Disaster Recovery & Cyber Physical Security Center

INDICE

1. Descrizione progetto

Il sistema di sicurezza, all'interno di ciascuna azienda, deve garantire **l'integrità, la confidenzialità e la disponibilità delle informazioni** che costituiscono il patrimonio aziendale. Tale patrimonio deve essere protetto da eventi dannosi, da minacce di accessi non autorizzati, da intrusioni, come pure dal cattivo trattamento delle informazioni all'interno del sistema che le gestisce. L'obiettivo è consentire una operatività ottimale delle risorse e la continuità delle operazioni di business nel rispetto delle disposizioni vigenti.

Il raggiungimento delle esigenze di sicurezza e *compliance* richiede l'individuazione e la realizzazione di misure di tipo organizzativo, normativo e tecnologico, in un'ottica di prevenzione (*risk management*), piuttosto che in una logica di semplice vigilanza o gestione delle emergenze. La scelta delle strategie di sicurezza deve rispecchiare le linee guida e i principi formulati dalle norme di riferimento, coerentemente con gli obiettivi, le politiche, le strategie e, naturalmente, il livello di rischio accettabile per l'azienda.

In virtù della criticità dei servizi erogati per le Pubbliche Amministrazioni, IPZS ha adottato soluzioni tecnologiche, nonché specifiche metodologie tecnico-organizzative basate su standard internazionali di riferimento, in grado di consentire il graduale conseguimento di elevati livelli di sicurezza delle informazioni che si concretizzano nelle seguenti iniziative progettuali:

- **Business continuity e disaster recovery** – implementazione di un'infrastruttura tecnologica capace di garantire la continuità di tutti i servizi interni ed esterni, al fine di minimizzare gli effetti distruttivi, o comunque dannosi, determinati da gravi emergenze o eventi che ne inficino la regolare erogazione;
- **Cyber Physical Security Center (CyPSeC)** – realizzazione di una Centrale Operativa per il monitoraggio, il controllo e l'*incident detection/response* degli eventi di sicurezza logica e fisica, in grado di individuare le vulnerabilità e gestire le emergenze e le situazioni di pericolo, visualizzando allarmi e permettendo l'attuazione di specifiche procedure di intervento.

2. Descrizione del team e delle proprie risorse e competenze

- **Amministratore Delegato** (Dott. Paolo Aielli)
- **Sistemi Informativi e Soluzioni Integrate** (*Resp. ing. Maurizio Quattrociocchi)*
  - *L. Consiglio (U.O. Tecnologie Informatiche)*
    - *A. Gentile, M. Disummo, F. Ficetola (Ingegnerizzazione e Industrializzazione Progetti)*
    - *G. Valente, A. Sciusco, R. Buscemi, G. Conversano, A. Pistillo, G. Ciampi, C. Verde, D. Rinelli, S. Arceri, A. Cotellessa, S. Leoni, M. Crescenzo, W. Leonelli, D. Galfano, E. Giuzio, M. Garau, F. Fraioli, F. Cimmino (Sistemi, Tecnologie e Innovazione IT)*
- **Sicurezza e Tutela Aziendale** (*Resp. ing. Marco Ferraro)*
  - *F. Flammini (Sicurezza dei Processi e delle Procedure)*
- **Attività Immobiliari** (*Resp. ing. Francesco Bigi)*

- *A. Rossi (U.O. Gestione Tecnica Immobili)*
- *A. Iudici, F. Gabelli (Progetti)*

- **Acquisti e Servizi Generali** (*Resp. avv. Alessio Alfonso Chimenti)*
  - *F. Rusciano (Beni e Servizi ICT)*
  - *S. Colantoni (Lavori e Impianti a Serv. degli Immobili)*

3. Descrizione dei bisogni che si intende soddisfare

Business continuity e disaster recovery

Il progetto intende implementare, a regime, un modello di continuità operativa basata su una piattaforma tecnologica e su un'organizzazione a tre livelli:

- Sito primario (SP) presso la sede IPZS di via Salaria in Roma, per l'erogazione dei servizi;
- Sito di business continuity (BC) presso la sede IPZS di via Gino Capponi in Roma, per la replica sincrona dei servizi erogati;
- Sito di disaster recovery (DR) presso la sede IPZS di Foggia, per la replica asincrona dei servizi erogati.

Il progetto prevede l'evoluzione espansiva dei Sistemi Centrali IT di IPZS e il contestuale allestimento dei sistemi informatici presso i nuovi Data Center da collocare nei citati siti, anche nel rispetto delle linee guida emanate dall'Agenzia dell'Italia Digitale per garantire la Continuità Operativa dei servizi IT delle PA (ex art. 50bis del CAD, in merito al quale IPZS ha ricevuto parere positivo sullo Studio di Fattibilità presentato).

Cyber Physical Security Center (CyPSeC)

Il progetto è dedicato alla sicurezza interna dell'azienda e si prefigge il compito principale di fornire la capacità di analizzare le informazioni e rilevare potenziali rischi e/o tentativi di intrusione, nonché rispondere in modo tempestivo ad eventuali incidenti di sicurezza. Il CYPSEC fornisce, inoltre, tutti quegli strumenti necessari a misurare le performance dei sistemi dedicati alla sicurezza e, quindi, a valutare correttamente il livello di rischio e di esposizione aziendale alle minacce. Permette inoltre di centralizzare il controllo da remoto dei sottosistemi di sicurezza fisica e di safety management.

Il CYPSEC monitora eventi di sicurezza. Tali eventi possono essere di diversa natura:

- Accidentali: che potrebbero verificarsi in maniera non predicibile (come guasti e malfunzionamenti, disastro ambientale, incendi, ecc.);
- Volontari: situazioni rilevate a fronte di eventi intenzionali (come tentativi di intrusione, attacchi ai sistemi informativi, ecc.).

Il rilevamento degli eventi viene effettuato attraverso l'integrazione di sorgenti eterogenee e distribuite, con l'ausilio di opportuni componenti (software e hardware), in grado di effettuare la data correlation delle informazioni acquisite, di rilevare l'accadimento di situazioni anomale e segnalarle agli operatori addetti all'interno della Sala Operativa.

4. Descrizione dei destinatari della misura

I destinatari delle iniziative in oggetto sono le Pubbliche Amministrazioni e gli utenti interni ed esterni per i quali IPZS eroga i propri servizi.

5. Descrizione della tecnologia adottata

Business continuity e disaster recovery

- Impiego di infrastrutture tecnologiche iperconvergenti, aperte e scalabili, abilitanti l'erogazione dei servizi in modalità cloud.

  In particolare, si è scelto di adottare soluzioni tecnologiche basate su **Architetture Iperconvergenti** costituite da elementi computazionali, di memorizzazione, di networking e di virtualizzazione gestite a livello **Software (Software Defined Data Center - SDDC)** indipendenti dalla tecnologia Hardware utilizzata.

  L'architettura si adatta dinamicamente alle specifiche esigenze dei servizi da offrire, adottando modelli di tipo PaaS, SaaS, IaaS e DaaS, garantendo la Continuità Operativa.

- *Replica sincrona* in area metropolitana dei dati, delle configurazioni e dei sistemi IT dal nuovo Sito Primario verso il Sito di Business Continuity, attraverso funzionalità miste basate sia su storage, sia sulla virtualizzazione introducendo tecnologie di networking integrative in grado di assicurare l'erogazione dei servizi in modalità "Active/Active" attraverso un bilanciamento di carico geografico;
- *Replica asincrona/semisincrona* in area geografica dei dati, delle configurazioni e dei sistemi IT sul Sito di Disaster Recovery, attraverso funzionalità miste basate sia su storage sia sulla virtualizzazione e, laddove possibile, l'erogazione dei servizi in modalità "Active/Active" attraverso un bilanciamento di carico geografico;
- Infrastrutture di rete e sicurezza, finalizzata all'erogazione di servizi datacenter ad alta affidabilità e alte prestazioni, con caratteristiche d'interconnessione tali da assicurare capacità di virtualizzazione avanzate, repliche sincrone e, in definitiva, indicatori *RPO* ed *RTO* prossimi allo zero, rafforzando i seguenti principi base:
  - **Difesa Multilivello** (*approccio di difesa in profondità (almeno 3 livelli), al fine di garantire la riservatezza, l'integrità e la disponibilità dei dati, delle applicazioni, degli endpoint e della rete stessa*)
  - **Modularità e Flessibilità** (*attraverso la suddivisione in moduli funzionali omogenei a più livelli, backbone, core, distribuzione, accesso, ognuno dei quali serve un ruolo specifico nella rete, introducendo la flessibilità dei livelli funzionali, consentendo un'implementazione graduale dei moduli e adattandosi al meglio alle esigenze di business di IPZS*)
  - **Affidabilità e Resilienza** (*diversi livelli di ridondanza per eliminare i Single Point of Failure "SPOF" e per massimizzare la disponibilità delle infrastrutture di rete attraverso l'impiego di interfacce ridondanti, moduli di backup, dispositivi standby, percorsi topologicamente ridondanti al fine di rendere la rete più resistente agli attacchi e ai guasti*)

- **Compliance** (*rispetto delle norme nazionali UNI, dalle norme internazionali EN-ISO/IEC, dalle norme RFC emanate dall'IETF, dalle Common Validated Design dei vendor di riferimento, e dalle principali best practices esistenti nel mercato dei datacenter*)
- **Efficienza Operativa** (*facilità di gestione e delle operations durante l'intero ciclo di vita delle soluzioni, fornendo una visione unificata dello stato complessivo della rete*)
- **Centralizzazione** (*consentirà di poter realizzare un punto centrale di controllo e gestione attraverso strumenti e procedure necessarie per verificare il funzionamento e l'efficacia delle infrastrutture IT così che, ogni evento generato dai dispositivi di rete venga istantaneamente raccolto e correlato centralmente permettendo la massima visibilità e rapidità sulle azioni di risposta e mitigazione degli eventuali eventi indesiderati*).

- *Modello composito*, in parte legato a tecnologie già in esercizio, per garantire l'interoperabilità dei protocolli e le policy di sicurezza già configurati in rete, e in parte a tecnologie di tipo *open (storage, server, bilanciatori di carico, ecc.).*

Cyber Physical Security Center (CyPSeC)

- SIEM: sistema di Security Information and Event Management per il collezionamento dei log da sorgenti eterogenee, la correlazione e l'analisi degli eventi e delle segnalazioni di sicurezza e il monitoraggio in tempo reale finalizzato alla prevenzione e alla protezione degli IT asset di IPZS;
- Vulnerability Manager: modulo che permette il discovery e la scansione automatica degli IT asset presenti nella rete aziendale (*vulnerability assessment*) per l'analisi e il rilevamento di potenziali minacce e vulnerabilità;
- Risk Manager: modulo che permette il monitoraggio della topologia, degli apparati e del traffico di rete, la simulazione degli attacchi di rete (*offense*) e che fornisce suggerimenti su policy e configurazioni da apportare sugli apparati di rete per minimizzare i rischi (*compliance assessment*);
- Application Scanner: modulo che consente l'analisi statica e dinamica degli applicativi software;
- PSIM-BMS: piattaforma di gestione integrata di Sistemi di Videosorveglianza, Antintrusione, Controllo Accessi, Videocitofonia, Rivelazione Incendi, Diffusione Sonora, Comunicazioni, Building Management (BMS), Monitoraggio Ambientale, Processi Aziendali, in grado di interconnettere i componenti dell'infrastruttura IT, collezionare e correlare eventi dai più disparati ed eterogenei apparati di sicurezza e sistemi informativi (video, controllo degli accessi, sensori, analytics, sistemi di rilevamento, ecc.).

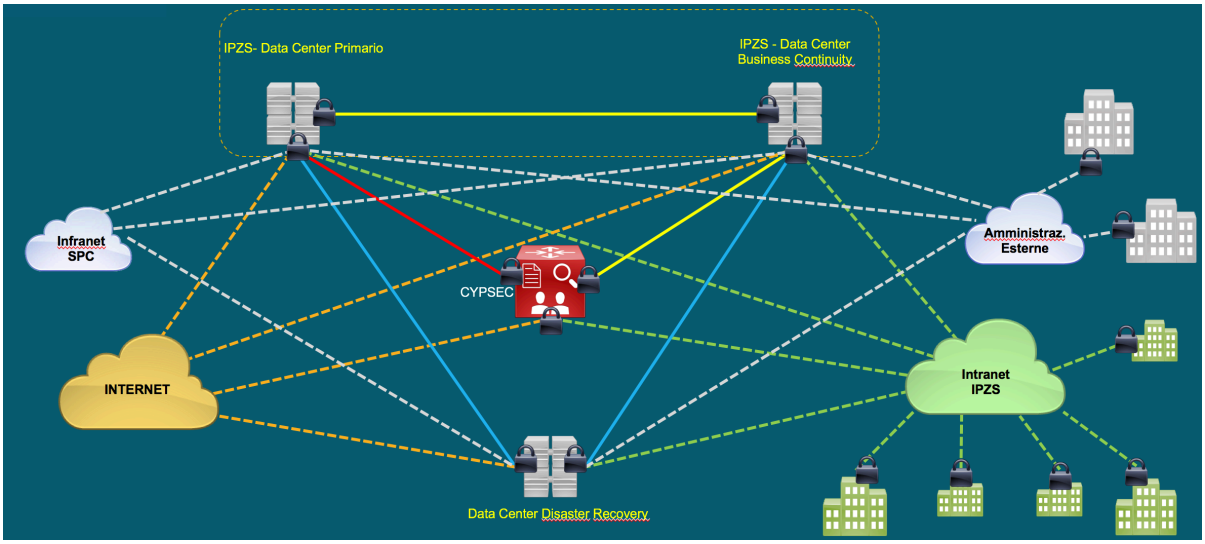

Figura 1 - Architettura di rete Data Center e Security

6. Indicazione dei valori economici in gioco (costi, risparmi ipotizzati, investimenti necessari)

Gli investimenti riguardano principalmente gli ambiti riguardanti i:

- Sistemi IT per i Data Center Primario, Business Continuity e Disaster Recovery
- Connettività di rete e Cifratura dei collegamenti
- Infrastrutture e impianti a supporto dei Data Center (TIER3/4)
- Centro Comando e controllo della Sicurezza Fisica e Logica (CypSec)

Spesa Stimata in 5 anni di: circa € 80.000.000

Le soluzioni e le tecnologia adottate consentiranno un risparmio stimato di circa il **20%** rispetto all'impiego di tecnologie tradizionali garantendo livelli di affidabilità e sicurezza molto più elevati.

7. Tempi di progetto

Business continuity e disaster recovery

- Attivazione dei Siti Primario e Business continuity per i servizi mission critical erogati da IPZS: entro la prima metà del 2017
- Attivazione dei Siti Primario, Business continuity e Disaster recovery per tutti i servizi erogati da IPZS: entro la fine del 2018

Cyber Physical Security Center (CyPSeC)

- Allestimento della Sala Operativa: entro la fine del 2017
- Attivazione dei servizi di sicurezza fisica: entro la prima metà del 2018
- Attivazione dei servizi di sicurezza logica: entro la prima metà del 2018