Sistema Socio Sanitario
Regione Lombardia

Capitolato Tecnico

Golden Copy – Progetto AREU Sicura

AREU Agenzia Regionale Emergenza Urgenza
Via Alfredo Campanini, 6 - 20124 Milano | C.F. e P. IVA 11513540960
Tel 02 67129001 | Fax 02 67129002 | Mail protocollo@pec.areu.lombardia.it
www.areu.lombardia.it

Emergenza 112 | 118 Soccorso Sanitario | 116117 Continuità Assistenziale | SRC Lombardia

Sommario

1 Soluzione di Cyber Recovery

1.1 Lo scenario: i Cyber Attacks

Il crimine informatico è stato definito il più grande 'trasferimento di ricchezza' della storia. Accenture stima che 5,2 trilioni di dollari di valore globale saranno a rischio di criminalità informatica nei prossimi 5 anni[1].

Indipendentemente dal settore o dalle dimensioni dell'organizzazione, gli attacchi informatici espongono continuamente aziende e governi a dati compromessi, perdite di entrate dovute a tempi di inattività, danni alla reputazione e costose sanzioni normative.

- Il costo medio annuo del crimine informatico per azienda ha raggiunto il valore di 13 milioni di dollari nel 2018, con un aumento del 72% solo negli ultimi 5 anni (1).

Implementare una soluzione che garantisca il recupero del dato, è diventato un mandato per i leader aziendali e governativi. Secondo uno studio Marsh & Microsoft del 2019, il 79% dei dirigenti globali classifica gli attacchi informatici come una delle massime priorità di gestione del rischio della propria organizzazione[2]

1.2 Come Proteggersi – Air Gapped/Offline Protection

Ci sono molte linee guida e BestPractices in merito:

- **FBI Cyber Defense Best Practices**

  Eseguire regolarmente il backup dei dati e verificarne l'integrità. Assicurarsi che i backup vengano adeguatamente isolati. Ad esempio, archiviali fisicamente offline. I backup sono fondamentali nel ransomware; se si è stati infettati, i backup possono essere il modo migliore per recuperare i tuoi dati critici, ma devi essere certo che non siano stati cancellati, criptati o che tu abbia eseguito un backup di un ransomware

- **FDIC Joint Statement on Heightened Cybersecurity Risk**

  Archiviare in modo sicuro i backup del sistema e dei dati fuori sede in ubicazioni

[1] Source: Accenture "The Cost of Cybercrime Study" 2019

[2] Source: Marsh & Microsoft "Global Cyber Risk Perception Study" 2019

geografiche separate e mantenere il backup offline o in un modo che preveda la separazione fisica o logica dai sistemi di produzione

- **Federal Financial Institutions Examination Council**

  Un'architettura di Backup Air-gaped limita l'esposizione ai Cyber Attack e garantisce il recupero del dato veloce e sicuro, al tempo T0 =momento prima dell'attacco

L'obiettivo degli attacchi informatici è distruggere, rubare o in qualche modo compromettere i dati più importanti, inclusi i backup. Proteggere e ripristinare i dati critici secondo un approccio sicuro orientato all'integrità è fondamentale per riprendere il normale svolgimento delle attività aziendali in seguito ad un attacco.

Al fine di ridurre i rischi per il business associati agli attacchi informatici e creare un approccio più cyber-resiliente alla protezione dei dati, è necessario modernizzare e automatizzare le strategie di ripristino e di continuità aziendale, oltre a implementare e attuare gli strumenti più avanzati per rilevare eventuali minacce informatiche e difendersi da queste ultime.

Di seguito vengono descritti gli elementi alla base di una soluzione di ripristino dagli attacchi informatici moderna e comprovata:

- **Isolamento e governance dei dati**: La soluzione deve essere in grado di creare un ambiente di data center isolato, offline e quindi scollegato sia dalle reti aziendali che di backup. Deve altresì garantire limitazioni di accesso per utenti diversi da quelli con autorizzazione adeguata
- **Immutabilità:** Si devono creare copie di dati non modificabili all'interno di un vault digitale protetto con processi che automatizzano un air gap operativo tra l'ambiente di produzione/backup e il vault
- **Intelligenza con Analisi e meccanismi di A.I.:** L'apprendimento automatico e l'indicizzazione completa dei contenuti sulla base di analisi efficaci, con tutta la sicurezza del vault, oltre a controlli automatizzati dell'integrità volti a individuare i dati interessati da malware e strumenti per un'eventuale correzione, devono essere alla base di una soluzione concreta di Vault.

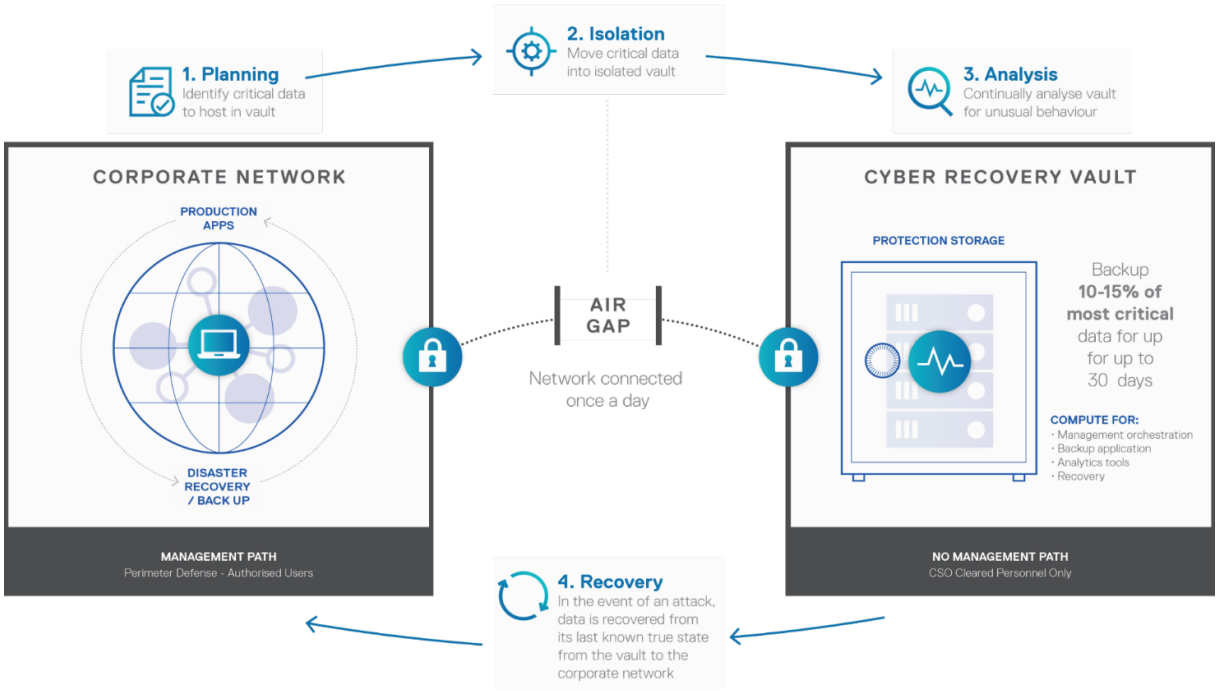

FIG.1

1.3 Requisiti per la soluzione di Cyber Recovery

L'attuale esigenza aziendale è quella di dotarsi di una soluzione di Cyber-Recovery che rispecchi le caratteristiche appena descritte e che sia in grado di proteggere dentro il sistema di vault i dati di backup che attualmente risiedono sui sistemi DataDomain di produzione (circa **30TB** effettivamente scritti a backend).

Considerando che la soluzione attuale di backup è da migliorare, si richiede pertanto la fornitura di una soluzione di cyber-recovery che comprenda un sistema di backup onsite per il sito di produzione ed un sistema di backup per l'ambiente di vault secondo lo schema riportato in fig.1, aventi ciascuno le caratteristiche minime obbligatorie descritte nei paragrafi successivi.

1.4 Oggetto della Fornitura

APPLIANCE DI BACKUP PER IL BACKUP PROPEDEUTICO ALLA GOLDEN COPY:

- 2x appliance di primo e secondo livello con spazio utile complessivo 80 TB
- porte di connessione: 4 * 1/10Gb rame BaseT + 4*10Gb SFP+ + 2 * 16Gb FC
- Installazione e configurazione chiavi in mano

- Manutenzione 60 mesi Next Business Day
- Software per sistema operativo, deduplica, encryption e replica compresi

SOFTWARE DI BACKUP PER IL SITO DI PRODUZIONE/VAULT:

- Il software di backup a copertura del dato sorgente che operi sia come Backup primario che di gestione della soluzione di cyber recovery deve essere incluso nella fornitura
- Installazione e configurazione chiavi in mano
- L'ente metterà a disposizione una VM su cui installare il software di Backup con le seguenti caratteristiche. Qualora il sw fornito ne richiedesse maggiori, il fornitore sarà obbligato a fornire un server fisico completo di, installazione, manutenzione 3 anni, licenze VmWare vCenter/ESXi 6.7, 7.0, 7.0u1, 7.0u2, 7.0u3

Requisiti minimi per il sw di backup in ambiente VMware (ESXi server).

- CPU—10 CPU cores
- Memoria—18 GB RAM for PowerProtect Data Manager
- Sette dischi con le seguenti capacità:
  - Disco 1—100 GB
  - Disco 2—500 GB
  - Dischi 3 and 4— 10 GB ciascuno
  - Dischi 5, 6 e 7— 5 GB ciascuno
- 1 GB network interface card (NIC)

APPLIANCE DI BACKUP PER IL SERVIZIO DI VAULT:

- spazio utile 44 TB
- porte di connessione: 4 * 1/10Gb rame BaseT + 4*10Gb SPFPP
- Installazione e configurazione chiavi in mano
- Manutenzione 60 mesi mission critical 4 ore
- Software per sistema operativo, deduplica, encryption e replica compresi

- Software la gestione dell'ambiente di vault compreso
- Software per l'analisi del dato all'interno del vault compreso

INFRASTRUTTURA DI VAULT (requisiti minimi):

- La connessione, privata e dedicata, tra il DC Primario di AREU e il servizio di Vault dovrà essere pari almeno a 10Gb SFPP.
- Il Vault dovrà offrire una infrastruttura fisicamente isolata tramite VPN e/o FW. Tale infrastruttura dedicata al cliente dovrà comprendere almeno n.1 Rack 42Unità dedicato all'erogazione del servizio di VAULT e che conterrà i seguenti elementi:
    - N.1* Infrastructure Server (vSphere pre-installed su BOSS o nel modulo Internal Dual SD con relativa licenza):

CPU Cores	32 x 2.8GHz
Memory	384GB
Network	4* 10GbE SFP+
Boss/MicroSD Card	2x480GB
Storage Internal RAW	24TB
Storage Internal Usable	21.6TB
RAID Config	RAID 5

    - N.1 Management Workstation interno al Vault

CPU Cores	8 x 2.6GHz
Memory	32GB
Network	4* 10GbE SFP+
Storage Internal RAW	1.92TB
Storage Internal Usable	960TB
RAID Config	RAID 1

    - N.1 KVM/KMM Switch interno al Vault

KVM console	18.5"

Monitor, Keyboard, Mouse	Included
Server Interface Module	Yes
KVM Mounting Bracket	1U

- N.1 Diodo per Reporting dal Vault verso il cliente

Connection	Base-T port

- N.1 Network Switch interno al Vault

Ru	1
Dimension	Full-width
Networks	12*10GbE SFP+ 6*10GbE base-T ONIE per zero-touch installation
VLAN TAG	Yes

- N.1 CyberSense Server interno al Vault

CPU Cores	32 x 2.8GHz
Memory	384GB
Network	4* 10GbE SFP+
Boss/MicroSD Card	2x 480GB
Storage Internal RAW	11.52TB
Storage Internal Usable	9.6
RAID Config	RAID 5
OperativeSystem	RedHat

- Installazione, cabling della soluzione di backup e configurazione della solution completa (vault e backup) in modalità chiavi in mano
- VmWare non sarà oggetto della fornitura ma per tutti gli elementi per cui non è richiesto il sistema di virtualizzazione si chiede di fornire il server con il relativo sistema operativo.

Segue un elenco di requisiti minimi obbligatori che dovranno essere rispettati pena esclusione.

1.5 Requisiti minimi obbligatori

	REQUISITO
1	**Appliance di Backup e di VAULT** La soluzione deve essere basata su "appliance di backup" di tipo rack-mountable in cui l'hardware (server/controller più espansioni a disco per la conservazione dei dati) ed il software (gestione e verifica dei dati, emulazione delle librerie fisiche, processi di deduplica, encryption, ecc.) siano integrati nativamente.
2	**Software di backup e di cyber recovery** La soluzione proposta deve comprendere: • Il software che deve eseguire le operazioni di backup e ripristino in maniera veloce ed efficiente sul sito di produzione, applicando il concetto di deduplica lato sorgente prima di trasferirli in rete e archiviarli. Il software deve consentire di ripristinare rapidamente i backup in un unico passaggio. Il sofware deve poter effettuare il backup di qualsiasi tipo di workload non solo quelli indicati • Il software di gestione della soluzione di cyber recovery deve essere in grado di gestire tutte le operazioni necessarie a proteggere il dato all'interno dell'ambiente di vault. Tali operazioni comprendono la replica del dato dal sito di produzione al vault, l'applicazione del meccanismo di immutabilità del dato e la verifica del dato attraverso opportuni algoritmi di analisi e Machine Learning
3	**Appliance di backup e dischi** È richiesta la fornitura e la messa in produzione di n.1 appliance di backup su disco con funzionalità di deduplica e compressione di dimensione pari almeno a 80TB utili per il sito di produzione e 44TB utili per il sito di vault.
4	**Connettività** Le appliance di backup devono essere equipaggiate almeno con le seguenti porte di connessione: sito di produzione • porte 1/10Gb baseT • 4 porte 10Gb SFP+ con relative ottiche sito di vault • porte 10Gb baseT • 4 porte 10Gb SFP+ con relative ottiche
5	**Resilienza e disponibilità** Il sistema deve prevedere l'alta affidabilità a livello locale almeno per alimentatori e ventole. Il ripristino dei componenti disco, alimentatore e ventola non deve comportare alcun disservizio.

	REQUISITO
6	**Prestazioni** Il sistema di backup principale e il sistema di Vault devono supportare almeno 10TB/Hr. Ambedue i sistemi devono supportare compressione e deduplica "inline" dichiarate su datasheet pubblici. Non sono accettati sistemi che eseguono compressione e/o deduplica in modalità "post-processing".
7	**Protocolli e performance** Il sistema deve supportare almeno i protocolli NAS (CIFS/NFS v.3 e 4), OST/DDBoost o equivalente, anche contemporaneamente. Il sistema deve avere un Throughput di targa non inferiore 20TB/Hr (vault e backup produzione) quando utilizza il protocollo BOOST o equivalente per features e performance.
8	**Compatibilità** La soluzione proposta come storage di Backup e Vault deve essere compatibile con almeno due tra i seguenti software di backup: Dell Networker, Dell Avamar, Dell PowerProtect Data Manager, Veritas Netbackup, Commvault,IBM Spectrum , IBM TSM, Veeam
9	**Connessione air gapped verso il vault** La soluzione deve prevedere il collegamento dal sito primario al sito di vault mediante una connessione di replica di tipo air-gapped, ovvero che rimanga attiva solo per il tempo strettamente necessario ad eseguire la copia dei dati tra i due ambienti (produzione e vault). Al termine di questa operazione la connessione deve essere chiusa per garantire l'isolamento dell'ambiente di vault. La gestione dell'apertura e chiusura della connessione deve essere completamente automatizzata e controllata dal software di gestione della soluzione di cyber recovery. La soluzione deve consentire agli utenti con privilegi di admin/root e security officer di bloccare manualmente la connessione tra l'ambiente di produzione ed il vault, inibendo così qualsiasi attività automatizzata di copia dei dati tra i due ambienti
10	**Immutabilità de dato** La soluzione deve consentire di rendere il dato incancellabile e immutabile
11	**Analisi del dato** La soluzione deve prevedere uno specifico software basato su algoritmi di analisi e machine learning che sia in grado di verificare il dato copiato nel vault e di fornire specifica segnalazione di allarme nel caso fosse riscontrata una corruzione/compromissione del dato stesso causato da un cyber-attack Il dato che presenta anomalie deve essere marcato come dato "corrotto" ed il sistema deve essere in grado di segnalare qual'è l'utima copia valida
12	**Analisi del dato** La soluzione deve implementare una metodologia di verifica del dato
13	**Analisi del dato all'interno dell'ambiente di vault** Tutte le fasi di analisi e verifica del dato devono iniziare ed essere completate

	REQUISITO
	all'interno dell'ambiente isolato di vault. Non sono ammesse soluzioni che richiedano l'invio dei dati al di fuori del vault per il completamento delle operazioni di analisi degli stessi.
14	**Report post attacco** In caso di rilevamento di corruzione /compromissione del dato, il sistema deve essere in grado di fornire un report dettagliato con tutte le indicazioni relative all'attacco volte a velocizzare la fase di ripristino, ovvero: • Chi è stato colpito dall'attacco • Cosa è stato colpito • Da dove è partito l'attacco, ovvero quale utente è stato usato per sferrare l'attacco e quale specifico attack vector è stato utilizzato • Quale è l'ultimo backup valido Il Service Provider, che erogherà il servizio di Vault, dovrà fornire il report al cliente con il risultato dell'analisi del software con cadenza pari ad almeno 3 volte a settimana.
15	**Protezione- dual sign-on e autenticazione multifactor (MFA)** Il sistema deve permettere l'abilitazione di un utente di sicurezza denominato "security officer" che controlli e in caso inibisca modifiche distruttive come data sanitization effettuate attraverso le credenziali e i privilegi dell'amministratore dell'appliance (dual-party authentication) Deve essere possibile anche l'abilitazione della funzionalità di autenticazione multifactor (MFA) attraverso la quale viene richiesto un passcode aggiuntivo oltre alle credenziali di amministartore p security-officer per l'esecuzione di determinati comandi distruttivi.
16	**Encryption** La soluzione deve permettere l'abilitazione della funzionalità di encryption dei dati in modalità INLINE, criptando i dati prima che vengano scritti sui dischi e anche durante la replica remota tra il sito di produzione e quello di vault.La funzionalità deve usare librerie validate e certificate dalla FIPS 140-2 con algoritmi Advanced Encryption Standard (AES) a 256-bit.
17	**Assistenza e supporto** Il servizio deve essere assicurato direttamente dal Vendor a partire dalla data di accettazione della fornitura per un periodo di 60 (sessanta) mesi con intervento onsite entro 4 ore. Il supporto deve rispondere alle chiamate 24 ore su 24, 7 giorni su 7. Per malfunzionamento dell'apparecchiatura si intende ogni difformità del prodotto hardware (sia per la configurazione base sia per i singoli dispositivi opzionali) dalle specifiche indicate nella relativa documentazione tecnica e manualistica d'uso. Il sistema oggetto della fornitura deve includere un meccanismo proattivo di segnalazione dei guasti hardware. Tale meccanismo deve inoltre attivare il Supporto Tecnico del vendor e aprire automaticamente un Ticket di supporto. Il supporto dovrà essere erogato dal vendor secondo le seguenti modalità:

	REQUISITO
	• Unico punto di supporto per hardware e software • Apertura automatica delle chiamate • Supporto per 36 mesi con assistenza telefonica 24 x 7 e invio delle componenti e manodopera entro il giorno lavorativo successivo Monitoraggio proattivo, rilevamento dei problemi, servizio di notifica, creazione automatica di casi e upgrade software operato da remoto direttamente dal supporto del Vendor. Non sono accettate soluzioni che forniscano questo tipo di supporto tramite un system integrator, un partner o un'azienda di terze parti. Se il Target di backup appartiene all'azienda X, il supporto sopra descritto deve essere fornito ed erogato dall'azienda X e non da alcuna affiliata.
18	L'appliance di backup primario deve poter supportare le funzionalità di Tiering del dato verso PublicCloud o ObjectStorage S3.
19	Le soluzioni di appliance di backup e di Vault devono supportare la replica dei dati 1-1, 1 a molti, molti a molti verso potenziali modelli hardware differenti.