DINO
DOCUMENT SOLUTION

GDPR compliance

as a Service

Sharp IT Services

SHARP

GDPR: introduzione al nuovo **quadro normativo**

Ci sarà tempo fino a maggio del 2018 per adeguarsi al nuovo Regolamento europeo in materia di privacy.
Una disciplina complessa che richiederà molti cambiamenti nel modo di raccogliere e gestire i dati oltre a investimenti potenzialmente significativi da parte di tutte le aziende.

Noto come **Regolamento Generale sulla Protezione dei Dati** (**GDPR**), questa normativa impone nuove regole per le aziende, per le agenzie governative, per le no-profit e per tutte le organizzazioni che offrono prodotti e servizi diretti alle persone all'interno dell'**Unione Europea**, o che raccolgono e analizzano dati relativi a persone in essa residenti.

Ecco i principi cardine:

1. **NORMATIVA**
   General Data Protection Regulation (**GDPR**) – Regolamento Generale sulla Protezione dei Dati Personali): unico per tutti i Paesi europei, per il quale **la privacy e la gestione dei dati personali diventa prioritaria**.
2. **OBIETTIVI**
   Restituire ai cittadini **il controllo dei propri dati personali** e semplificare il contesto normativo comunitario.
3. **DIRITTI DEL CITTADINO**
   Chiedere la **rettifica**, la **cancellazione**, il **trasferimento** dei propri dati entro 30 giorni.
4. **DOVERI DELLE AZIENDE**
   - nominare un **Data Protection Officer** (DPO) quando richiesto;
   - segnalare all'autorità di vigilanza violazioni ai dati personali **entro 72 ore** dall'avvenimento.
5. **TEMPISTICHE**
   Adeguamento entro il **25 maggio 2018**.
6. **SANZIONI**
   Fino a 20 milioni di Euro o il 4% del fatturato.

Il **GDPR** vuole mettere al sicuro i dati personali dei cittadini dell'Unione Europea ovunque i dati stessi vengano inviati, elaborati o conservati.

Il **GDPR** rappresenta un passo importante per il diritto alla privacy dell'individuo: consente a coloro che risiedono all'interno dell'Unione Europea di avere il controllo sui propri dati personali.

GDPR: alcune **risposte** ai dubbi più comuni

In che modo il Regolamento Generale sulla Protezione dei Dati (GDPR) influenzerà la mia azienda?

Il Regolamento Generale sulla Protezione dei Dati (GDPR) contiene numerosi **adempimenti sulle modalità di raccolta, conservazione e utilizzo delle informazioni personali**.
Questo non include solo le modalità con cui identifichi e proteggi i dati personali nei tuoi sistemi, ma anche le modalità con cui rispetti i **nuovi obblighi di trasparenza**, rilevi e segnali le **violazioni** dei dati personali e sensibilizzi alla privacy il personale e i dipendenti.

Vista la moltitudine di adempimenti richiesti, le aziende non dovrebbero aspettare che il Regolamento entri in vigore a maggio del 2018 per prepararsi, ma dovrebbero iniziare sin da subito a rivedere le procedure di gestione dei dati e della privacy. Il mancato adeguamento alla predetta normativa potrebbe costare caro, dal momento che **se le aziende non soddisferanno i requisiti e gli obblighi previsti dal regolamento, andranno incontro a multe e a danni reputazionali**.

Che diritti devono essere garantiti dalle aziende ai sensi del GDPR?

Il GDPR permette ai **residenti nell'Unione Europea** di controllare i dati personali attraverso un set di "**diritti per gli interessati**". Tra questi, il diritto di:

- accedere a informazioni pronte e semplificate sulle modalità di utilizzo dei dati personali;
- accedere ai dati personali;
- far cancellare o correggere dati personali;
- far correggere dati personali e cancellarli in determinate circostanze ("diritto all'oblio");
- limitare o contestare l'elaborazione dei dati personali;
- ricevere una copia dei dati personali;
- rifiutarsi di elaborare dati per usi specifici, come ad esempio marketing o profiling.

Cosa sono i dati personali?

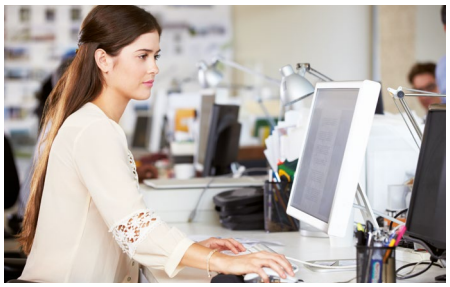
I dati personali sono qualsiasi informazione relativa a una persona identificata o identificabile.
Non c'è distinzione tra il ruolo pubblico, privato o lavorativo di una persona.

I dati personali includono:

- nome
- indirizzo e-mail
- post sui social media
- informazioni fisiche, fisiologiche o genetiche
- informazioni mediche
- posizione
- dettagli bancari
- indirizzo IP
- cookie
- identità culturale

A quanto può ammontare la multa per le aziende non conformi al nuovo Regolamento?

Le aziende possono essere multate **fino a 20 milioni di Euro o al 4% del fatturato annuo,** l'importo maggiore, per il mancato rispetto di alcuni requisiti del Regolamento Generale sulla Protezione dei Dati.



Il GDPR si applica sia ai responsabili che ai titolari del trattamento dei dati?

Sì, il Regolamento Generale sulla Protezione dei Dati (GDPR) **si applica sia ai titolari sia ai responsabili del trattamento**. Il titolare si occupa dei dati; il responsabile li elabora per il titolare.

I titolari devono soltanto usare responsabili che rispettino i requisiti del GDPR. Il titolare determina come e perché trattare i dati personali, mentre il responsabile tratta i dati personali per conto del titolare.

Ai sensi del GDPR, i responsabili hanno **ulteriori responsabilità e maggiori incombenze** in relazione alla non conformità o se agiscono al di fuori delle istruzioni fornite dal titolare.

Le responsabilità di conformità del processore includono:

- elaborare i dati solo secondo le istruzioni;
- utilizzare appropriate misure tecniche e organizzative per l'elaborazione dei dati personali;
- eliminare o restituire dati al titolare;
- ottenere il permesso per servirsi di altri responsabili.

La mia azienda ha bisogno di nominare un Data Protection Officer (DPO)?

Dipende da numerosi fattori previsti dal Regolamento. Se la tua azienda dovesse nominare un Data Protection Officer (DPO), questo avrà la responsabilità di:

- informare i dipendenti dei loro obblighi di conformità;
- condurre il **monitoraggio**, la **formazione** e i **controlli** richiesti dal GDPR.

In che modo il GDPR cambia la risposta di un'azienda alle violazioni dei dati personali?

Il GDPR cambierà la protezione dei dati e introdurrà **obblighi più rigidi** per i responsabili del trattamento dei dati e per i titolari **in relazione alle minacce ai dati personali che risultano essere un rischio per i diritti e le libertà individuali**.

Ai sensi della nuova normativa, il responsabile del trattamento dovrà immediatamente **notificare** al titolare del trattamento dei dati **qualsiasi violazione occorsa**. Il titolare del trattamento dovrà, di conseguenza, notificarla **entro le 72** ore all'autorità per la protezione dei dati competente.

Se la violazione risulta essere un grave rischio per i diritti e le libertà individuali, i titolari del trattamento avranno inoltre bisogno di notificare la violazione agli interessati senza ritardi.

Il GDPR ha a che fare con la crittografia?

La crittografia è identificata nel Regolamento Generale sulla Protezione dei Dati (GDPR) come una misura protettiva che rende inutilizzabili i dati personali quando vengono interessati da una violazione. Di conseguenza, **l'utilizzo o il mancato utilizzo della crittografia può avere effetti sulla notifica di una violazione dei dati personali**.

Il GDPR inoltre punta alla crittografia come un'appropriata misura tecnica e organizzativa. La crittografia è anche un requisito attraverso lo standard di sicurezza dei dati per le carte di pagamento e fa parte delle severe linee guida circa la conformità, specifiche per il settore dei servizi finanziari.

Quanto costa conformarsi al GDPR?

La conformità al Regolamento Generale sulla Protezione dei Dati (GDPR) costerà tempo e denaro per la maggior parte delle aziende, ma **sarà più semplice per le organizzazioni che dispongono di un modello di servizi cloud ben architettato e per coloro che hanno un programma di data governance efficace**.

Dove posso ottenere maggiori informazioni sul GDPR?

Per ottenere maggiori informazioni sul Regolamento Generale sulla Protezione dei Dati (GDPR), visita la pagina della Comissione Europea, organo esecutivo dell'Unione Europea che ne promuove l'interesse generale: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

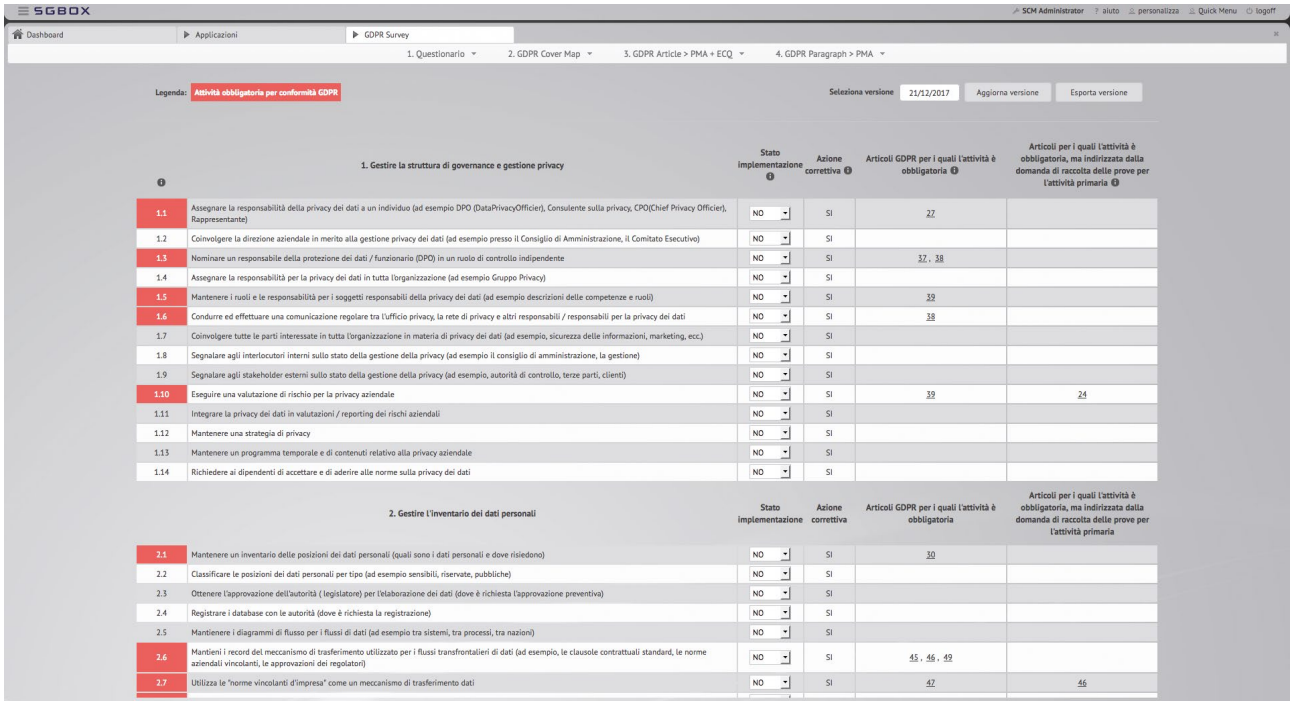
La soluzione proposta da Sharp per essere **conformi al GDPR**

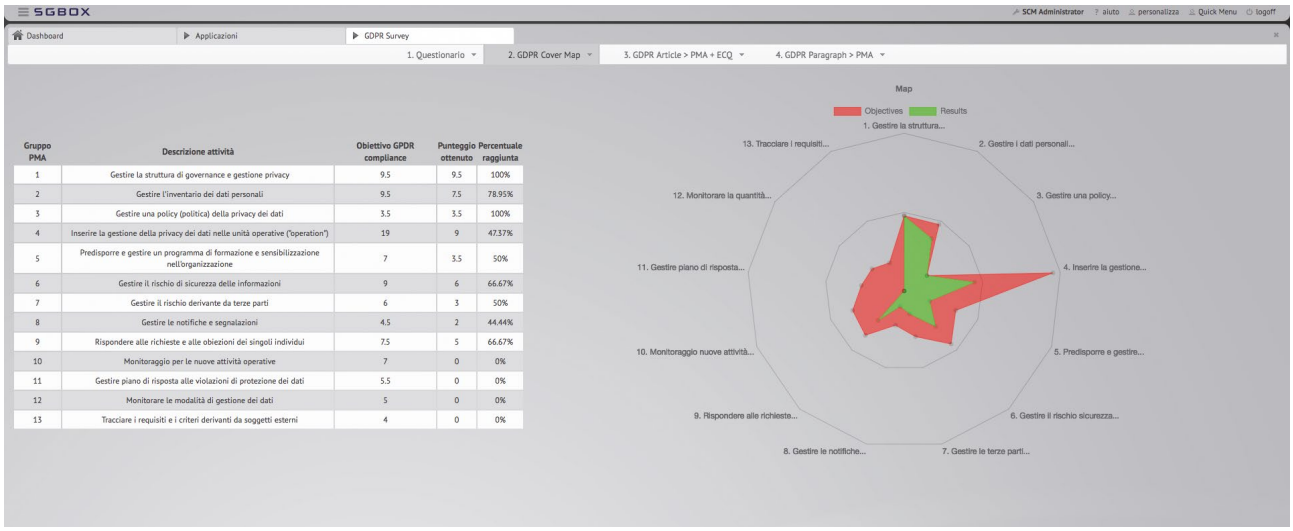
AUDIT & DESIGN

Il primo passo nel percorso verso la compliance al GDPR è acquisire **la consapevolezza delle vulnerabilità dei propri sistemi informativi e dei rischi a cui si è esposti**. A questo proposito, proponiamo un'attività professionale specifica che, attraverso strumenti già predisposti, permette di ottenere in poco tempo:

1. la mappatura di tutti gli asset di rete, network e server di elaborazione dati. Risultato:

- elenco asset in forma excel, schemi di rete;
- elenco repository dati personali (GDPR) e relazioni funzionali.





Gruppo PMA	Descrizione attività	Obiettivo GPDR compliance	Punteggio ottenuto	Percentuale raggiunta
1	Gestire la struttura di governance e gestione privacy	9.5	9.5	100%
2	Gestire l'inventario dei dati personali	9.5	7.5	78.95%
3	Gestire una policy (politica) della privacy dei dati	3.5	3.5	100%
4	Inserire la gestione della privacy dei dati nelle unità operative ("operation")	19	9	47.37%
5	Predisporre e gestire un programma di formazione e sensibilizzazione nell'organizzazione	7	3.5	50%
6	Gestire il rischio di sicurezza delle informazioni	9	6	66.67%
7	Gestire il rischio derivante da terze parti	6	3	50%
8	Gestire le notifiche e segnalazioni	4.5	2	44.44%
9	Rispondere alle richieste e alle obiezioni dei singoli individui	7.5	5	66.67%
10	Monitoraggio per le nuove attività operative	7	0	0%
11	Gestire piano di risposta alle violazioni di protezione dei dati	5.5	0	0%
12	Monitorare le modalità di gestione dei dati	5	0	0%
13	Tracciare i requisiti e i criteri derivanti da soggetti esterni	4	0	0%

2. l'analisi dei gap esistenti e proposta di soluzioni per l'adeguamento.

Risultato:

- documenti di presentazione dei risultati con elenco GAP suddivisi per priorità, requisiti obbligatori GDPR e suggerimenti per l'adeguamento dei requisiti e di quelli opzionali.

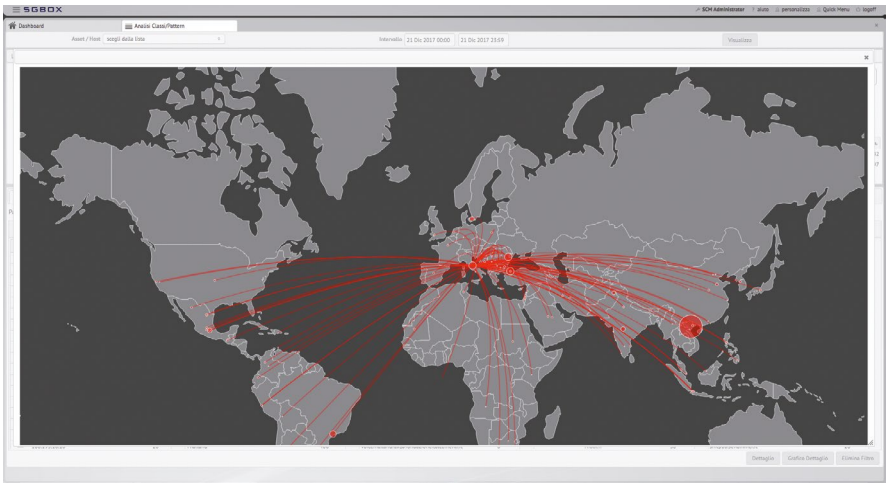
I risultati della GAP Analysis sono utili per identificare i rimedi di processo e tecnologici da implementare al fine di raggiungere la compliance al GDPR.

LA SOLUZIONE SIEM AS A SERVICE

PER LA GESTIONE DEI DATI E DEGLI EVENTI

È stata predisposta in Data Center una piattaforma di SIEM (Security Information and Event Management) che permette di accedere in modalità ”as a service” a strumenti specifici che facilitano la tracciabilità dei dati, la raccolta dei log dei sistemi, la correlazione degli eventi e la scansione della vulnerabilità.

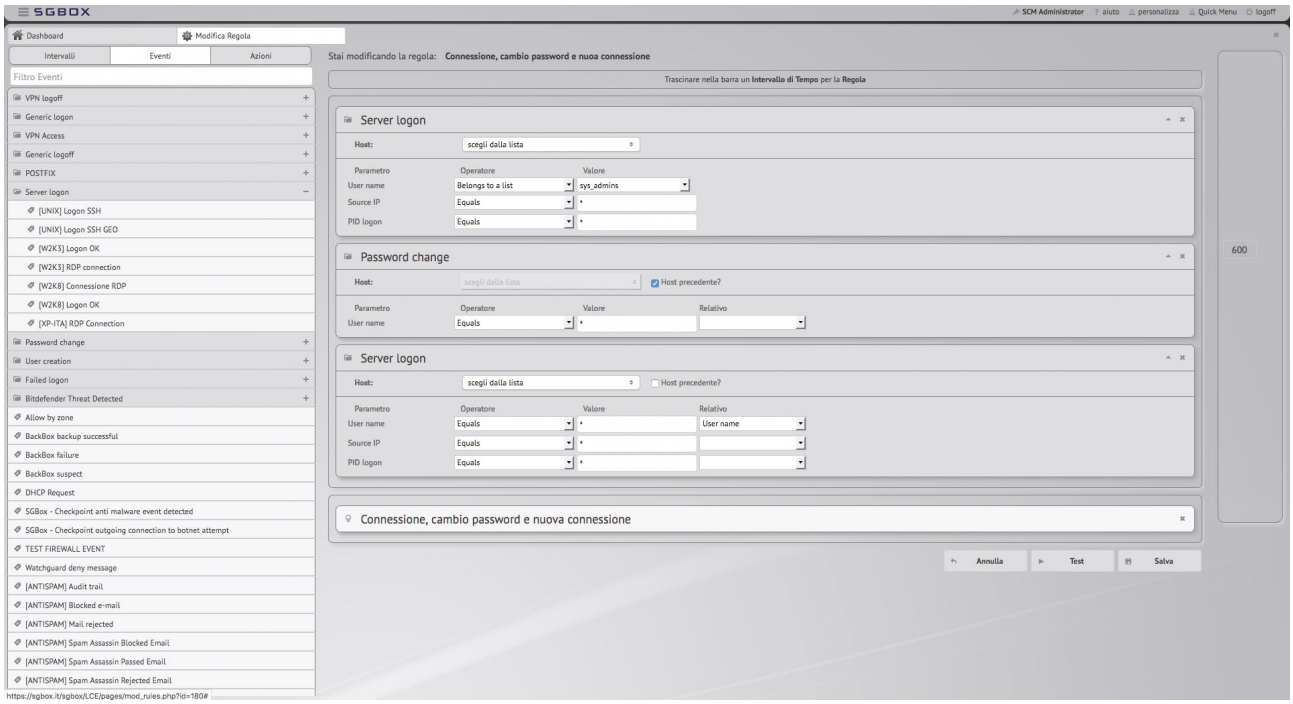
In questo modo sarà più semplice adempiere a molte delle incombenze richieste dal GDPR, avendo pieno controllo e monitoraggio di tutto quello che avviene nei propri sistemi informatici.



Ambiente di Management

Per ogni modulo è possibile:

- Autenticare su directory esterna (autenticazione unica);
- Assegnare permessi per gruppi utente: Readonly/RW/Exec;
- Modificare la visibilità degli oggetti per gruppi utenti (profili);
- Condividere le configurazioni (host/network/asset…).



Modulo di Log Management

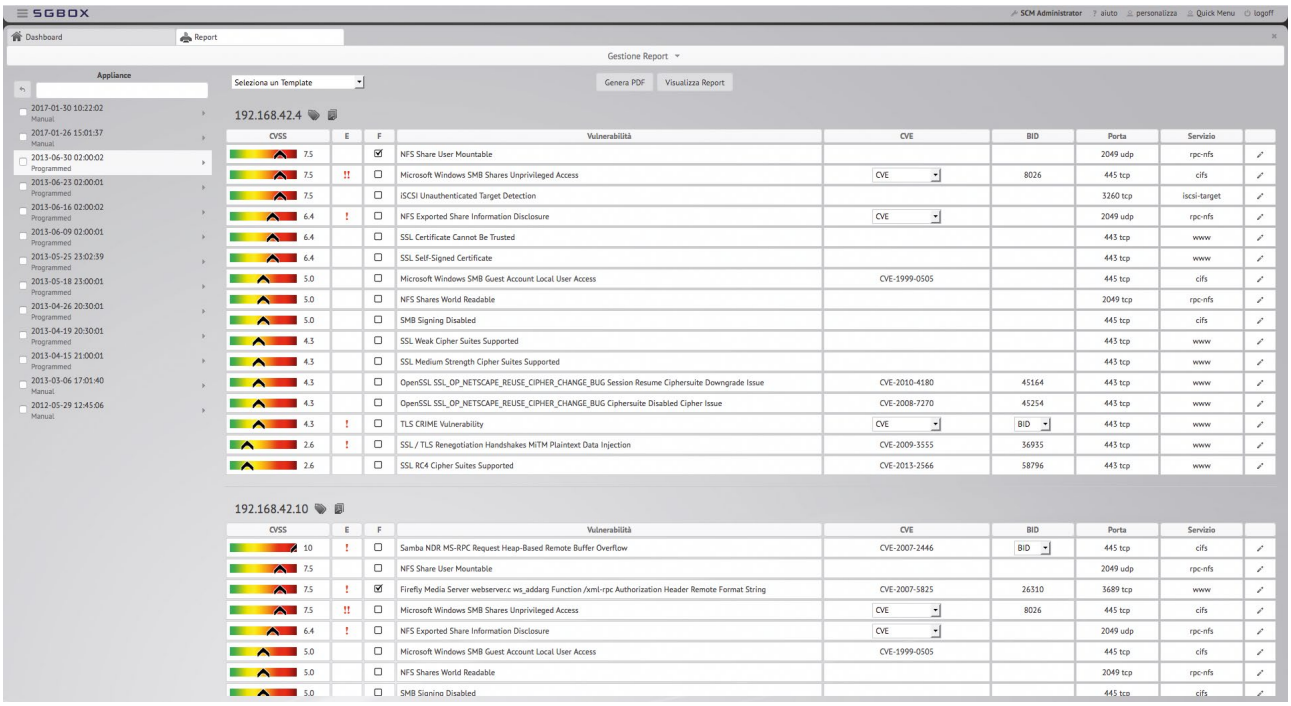
- Raccoglie e gestisce elevate quantità di informazioni;
- Categorizza le informazioni raccolte in base ai parametri scelti;
- Estrae eventi dalle informazioni raccolte in modo da rendere i log significativi;
- Mette a disposizione strumenti base per l'analisi degli eventi
- Genera report personalizzati su quanto analizzato;
- Consente un primo livello di correlazione degli eventi.

Modulo di Correlazione di Eventi

- Analizza gli eventi ricevuti dai moduli e dall'infrastruttura;
- Ricerca sequenze di eventi che corrispondano a scenari definiti dall'utente;
- Genera allarmi in base alle sequenze di eventi individuate;
- Esegue script esterni in risposta agli scenari definiti;
- Genera nuovi eventi.

Modulo di System Monitoring

- Verifica – sfruttando diversi protocolli – la disponibilità di sistemi e servizi;
- Indica i tempi di risposta dei servizi;
- Fornisce report interattivi su SLA e uptime dei sistemi/servizi;
- Genera eventi/allarmi in base allo stato dei servizi.



Modulo di Vulnerability Scanner

- Report differenziali su più livelli;
- Attribuzione di priorità per la fase di "remediation";
- Indice di vulnerabilità secondo lo standard internazionale CV; (Common Vulnerability Scoring System);
- Auditing PCI (Payment Card Industry);
- Report personalizzati;
- Report programmati a fronte di scansioni ed indirizzati ai responsabili degli asset

I RIMEDI TECNOLOGICI

In base ai risultati della GAP Analysis, potrebbe essere necessario incrementare i livelli di sicurezza e, di conseguenza, utilizzare specifiche soluzioni per la protezione dei dati:

- **Soluzioni di Cifratura dei Documenti e dei Dischi**
  Con le soluzioni di cifratura è possibile impostare policy che consentono solo alle persone autorizzate di accedere a file o directory. Anche in caso di furto del PC non sarà possibile accedere alle informazioni sui dischi.

- **Soluzioni Unified Threat Management**
  Le tecnologie per la protezione contro le minacce avanzate permettono di proteggere i dati anche verso gli attacchi più evoluti.

Le tecnologie di Data Loss Prevention permettono di evitare la trafugazione di dati anche all'interno della rete aziendale.

- **Backup as a Service (BaaS) e Disaster Recovery as a Service (DRaaS)**
  Con la soluzione BaaS i dati vengono copiati su data center esterni in modalità cifrata, così da poter essere recuperati anche in caso di disastri gravi.

La soluzione di DRaaS aumenta ulteriormente il livello di protezione dei dati consentendo RTO e RPO (tempo di replica e tempo di ripartenza) tendenti allo zero.

IL RISCHIO RESIDUO

Se attraverso il percorso proposto (Audit, GAP Analysis, Sistema di Gestione dei Dati e degli Eventi, Rimedi Tecnologici) si dimostra di aver messo la propria azienda nelle condizioni di essere conforme al GDPR, è possibile accedere a prodotti assicurativi messi a punto da compagnie di assicurazione leader a condizioni particolarmente favorevoli.

Le coperture previste per il rischio residuo sono:

- **Spese per servizi di Incident Response e costi investigativi**
  Con il supporto di una linea diretta e multilingue, attiva 24/7, per il supporto in situazioni di crisi
- **Costi derivanti da ritardi o interruzione in caso di ''business interruption''**
- **Spese legali, ivi comprese quelle per far valere le penali contrattuali**
- **Spese sostenute per la comunicazione in situazioni di crisi e la mitigazione del danno alla reputazione**
- **Responsabilità derivante dalla mancata tutela dei dati riservati**
- **Responsabilità derivante dall'uso non autorizzato delle telecomunicazioni**
- **Estorsione/riscatto legato alla rete o ai dati (ove assicurabile)**
- **Responsabilità relativa alla gestione di media online**

DINO
DOCUMENT SOLUTION

DINO S.r.l.
Via E. Gianturco, 23
80146 Napoli (NA)
Tel./Fax 081 191 75 228
info@centrosharpnapoli.it

SHARP

www.centrosharp.it