TS-GDPR care

Soluzioni per il General Data Protection Regulation (GDPR) assessment

Il regolamento generale sulla protezione dei dati (GDPR) protegge i dati personali dei cittadini dell'Unione Europea indipendentemente dalla posizione geografica o dalla tipologia di informazione. Le organizzazioni di tutto il mondo devono essere conformi al GDPR entro il 25 maggio 2018. Si tratta di un adeguamento che ha impatto sul personale, sui processi e sulle tecnologie dell'organizzazione. L'obiettivo è garantire che i dati personali siano correttamente controllati, elaborati, mantenuti, conservati e protetti. Le penali per violazione del GDPR possono arrivare fino a 20 milioni di euro.

L'articolo 5 del GDPR impone una serie di principi relativi al trattamento dei dati personali, che devono essere:

- Elaborati in modo lecito, equo e trasparente
- Raccolti per scopi specifici, espliciti e legittimi
- Adeguati, pertinenti e limitati a ciò che è necessario
- Accurati e aggiornati
- Mantenuti solo per il tempo necessario
- Elaborati in modo appropriato per mantenere la sicurezza

Ma soprattutto i dati vanno protetti e i requisiti relativi alla segnalazione delle violazioni dei dati personali impongono modalità e tempistiche estremamente vincolanti.

Probabilmente hai già adeguato la tua organizzazione ai requisiti del GDPR e hai compreso che è solo l'inizio di un lungo percorso. Alcuni aspetti evidenziati nel Regolamento, infatti, impegnano l'organizzazione in un vero e proprio cambiamento culturale, di visione, soprattutto per quanto riguarda accountability e sicurezza.

LE IMPLICAZIONI DEL GDPR

Gli articoli 33 e 34 del GDPR impongono ai responsabili del trattamento di segnalare violazioni dei dati personali a un'autorità di vigilanza senza ritardi e entro 72 ore dalla loro scoperta. Devono anche comunicare ai loro utenti se esiste il rischio che la violazione inciderà in qualche modo sui loro diritti e la loro libertà.
Per evitare che tutto ciò avvenga, dovendo agire quando il danno è fatto, è necessario disporre delle persone, dei processi e delle tecnologie giuste per essere in grado di rilevare, investigare e rispondere preventivamente ad un attacco. La migliore risposta è una buona difesa.

LE SOLUZIONI TS-WAY

Un'esperienza decennale nella sicurezza e un pool di professionisti di altissimo profilo sono le basi dell'offerta di TS-WAY a supporto delle organizzazioni alle prese con il GDPR. Processi, metodo, tecnologie specifiche si uniscono a grandi capacità di comprensione dello scenario geopolitico e della mentalità degli attaccanti.
TS-WAY propone un "pacchetto GDPR" a base di vulnerability assessment, penetration test, APT detection, per riconoscere rapidamente i punti di debolezza della propria organizzazione, stimandone l'impatto, pianificando azioni correttive, ma soprattutto contribuendo alla costruzione di una cultura aziendale orientata alla prevenzione ed alla comprensione delle minacce.

VULNERABILITY ASSESSMENT

“La capacità di assicurare la persistenza continua, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione” sono richieste specifiche contenute nel GDPR (art. 32 sec. 1b). Gli attacchi malevoli possono riguardare tutte queste aree, quindi identificare con precisione le vulnerabilità presenti nei sistemi è fondamentale per il tuo programma di sicurezza. Il vulnerability assessment di TS-WAY individua le problematiche presenti focalizzando le proprie attività esclusivamente su un primo livello di frontiera. Verifica i processi in profondità con strumenti commerciali ed open source amplificati da tool proprietari. I vulnerability assessment svolti da TS-WAY sono privi di falsi positivi perché tutti i risultati ottenuti dalla componente tecnologica sono vagliati da personale specializzato. Vanno effettuati a cadenza regolare.

TARGET	METODOLOGIA
NETWORK WEB APP	VULNERABILITY SCAN FUZZING

RESPONSIBLE DISCLOSURE REFERENCES

Microsoft Google

PENETRATION TEST BLACK BOX

I dati personali sono un obiettivo professionale per gli hacker. In TS-WAY abbiamo una profonda conoscenza delle loro tecniche, degli strumenti che usano, di come pensano e agiscono. Il nostro team di professionisti certificati OSCP (Offensive Security Certified Professional) individua e verifica le vulnerabilità dei sistemi, procede al loro sfruttamento e ne testa la profondità. I *pentester* sono in grado di simulare azioni malevole senza disporre di informazioni sul target (black box), avendone una conoscenza limitata (grey box) oppure piena (white box). Per garantire la massima efficacia e l’ideale livello di monitoraggio, i penetration test vanno effettuati in funzione dell’evoluzione dell’infrastruttura, e comunque con cadenza annuale.
I test sono certificati.

TARGET	METODOLOGIA
NETWORK WEB APP	MANUAL ACTIVITY VULNERABILITY SCAN FUZZING

RESPONSIBLE DISCLOSURE REFERENCES

Microsoft Google

DETECTION

TS-Threat Detector è la soluzione sviluppata da TS-WAY che analizza e scansiona su più livelli i sistemi informatici e consente una detection profonda ed efficace delle minacce, scandagliando l’intero sistema operativo del pc Windows. **TS-Threat Detector** rileva le infezioni APT (Advanced Persistent Threat), individua gli attori responsabili e ne fornisce la descrizione di base. La sinergia fra strumenti tecnologici e personale altamente specializzato consente inoltre di registrare ogni anomalia e di verificarne l’eventuale natura criminale, anche in caso di riscontro non immediato con le minacce già note. Per un’ottimale attività di detection, le scansioni vanno effettuate trimestralmente.

TS-DETECTOR	DETECTION LEVELS
ANOMALOUS BINARY DETECTION ENGINE	PROCESSES FILESYSTEM REGISTRY MEMORY NETWORK MUTEXES PIPES

Al termine di ognuno dei tre servizi proposti, TS-WAY rilascia una **documentazione specifica** che certifica l’avvenuta attività.

TS-WAY sviluppa sistemi, tecnologie e metodi di collaborazione per organizzazioni di medie e grandi dimensioni. Le sue soluzioni tecnologiche trasformano i dati delle minacce globali in informazioni di tipo strategico, tattico, operativo e tecnico, consentendo alle organizzazioni di risparmiare tempo e risorse, anticipare le minacce, comprenderne la portata e la natura, potendo contare su un partner affidabile in caso di incidente informatico. Un approccio alla sicurezza preventivo ed estremamente completo a garanzia e tutela dei beni e della continuità del business. TS-WAY schiera un dream team di professionisti, istruttori OSCP (Offensive Security Certified Professional), cofondatori del progetto “The Exploit Database” e con un passato da responsabili e sviluppatori core della distribuzione professionale per penetration test BackTrack Linux (Kali LInux). L’esperienza di TS-WAY è riconosciuta in consessi internazionali e avvalorata da grandi organizzazioni private nei comparti finanza, energia, telecomunicazioni, e da organizzazioni governative e militari che nel tempo hanno utilizzato i servizi di questa società indipendente, interamente italiana.

TS-WAY srl, Piazza Monte Rosa, 33, int. 6, Orvieto (TR) 05018, Italy

0763.340498
www.ts-way.com