Ilaria Garaffoni

Privacy compliance e cyber security: due facce della stessa medaglia

"La protezione dei dati è materia trasversale e multidisciplinare tra privacy e cybersecurity: due discipline che, partendo da esigenze e ragion d'essere differenti, si focalizzano però sullo stesso oggetto. La data protection è peraltro sempre più complessa, lato compliance (territorio di avvocati e DPO), per il ginepraio di normative UE ma anche nazionali post GDPR, e lato cybersecurity per la corsa ad un'innovazione tecnologica sempre più pervasiva ed impattante per i dati, oltre che utilizzabile per sferrare attacchi (feudo di CISO e Security Manager). Un contesto che fa sfumare gli stessi confini tra compliance e cybersecurity, richiedendo un approccio trasversale. Eppure il dialogo è ancora critico e può avere pesanti ripercussioni sulla protezione del dato. Se ne è parlato in uno dei talk show che si sono susseguiti al primo cyber&privacy forum 2023.

cyber & privacy 2023
secsolutionforum®

> **"Senza dimenticare che la sicurezza è una responsabilità corale, chi subisce un data breach è vittima fintanto che non si accerti che poteva fare di più per proteggere i dati personali affidati alla sua cura. In ogni caso, se sono da valutare le responsabilità di chi è vittima di un'aggressione, è certa invece la responsabilità degli attaccanti"**
> **(Guido Scorza)**

ILARIA GARAFFONI
RESPONSABILE DI REDAZIONE
SECSOLUTION MAGAZINE

GUIDO SCORZA
COMPONENTE DEL COLLEGIO DEL GARANTE
PER LA PROTEZIONE DEI DATI PERSONALI

ANDREA BILLET
DIRETTORE DEL CENTRO DI VALUTAZIONE
E CERTIFICAZIONE NAZIONALE,
PRESSO L'AGENZIA PER LA
CYBERSICUREZZA NAZIONALE

GIUSEPPE ALVERONE
DATA PROTECTION OFFICER
DELL'ARMA DEI CARABINIERI

MARCO MARIANI
CEO DI GFM - NET

GIANLUCA LOMBARDI
TITOLARE DI GL CONSULTING

Guido Scorza (Garante Privacy)

Nel mondo della complessità non può esistere uno scenario privacy senza interscambio tra discipline legacy e cyber. Come si muove il Garante? Sono previste competenze interne in ambito di cybersecurity? In quale misura? L'attività di produzione di provvedimenti prevede un occhio attento anche al tema tecnico?

Non c'è ormai settore della vita pubblica, privata e professionale che possa sottrarsi ad un approccio multidisciplinare. Questo vale a maggior ragione per le Autorità e in particolare per un'Autorità dedicata alla protezione dei dati personali, come il Garante. L'Autorità vanta competenze di varia natura, pur registrandosi tuttora uno sbilanciamento dei ruoli giuridici rispetto a quelli tecnici. Ritengo sia necessario invece un potenziamento delle competenze tecniche (che devono essere per forza interne in un'autorità indipendente), anche se queste ultime richiedono crescenti risorse per far fronte a sfide sempre più complesse che richiedono budget adeguati. Del resto è lo stesso GDPR che espressamente obbliga gli Stati a garantire alle Autorità le risorse necessarie per svolgere pienamente il loro ruolo.

Andrea Billet (ACN - Agenzia per la Cybersicurezza Nazionale)

Quanto influisce la sicurezza informatica delle imprese italiane private, quindi al di là della PA, sulla cybersicurezza e resilienza nazionale e che ruolo ha questo aspetto nell'agenda dell'Agenzia?

L'ACN ha scelto di partire dall'alto per costruire sicurezza e resilienza nel paese: siamo quindi partiti dalle infrastrutture critiche pubbliche e private. Nel privato le catene di valore sono molto frantumate: abbiamo quindi scelto che le policy di sicurezza imposte alle capomaglia scendano pian piano su tutta la catena inclusi le PMI, "portando" quindi la sicurezza anche nelle realtà meno dimensionate. Certo nessuno si aspetta che tutti abbiano tutte le competenze in casa, ma per costruire resilienza ciascuno deve porsi delle domande. Sono davvero padrone del mio castello? So come funziona la filiera? So dove sono i dati in tutte le fasi e come sono protetti? Quali rischi corrono i miei dati? Ebbene: se so che rischi corro, posso apprestare delle difese. E pormi altre domande: quali competenze servono? Dove devo attingerle? Come posso essere pronto ad affrontare un attacco e ad avere perdite di servizio tollerabili?

Giuseppe Alverone (Arma dei Carabinieri)

Per essere "padroni del castello" e governare la filiera l'Arma si è data un modello organizzativo modello organizzativo per la protezione dei dati personali, che (oltre al DPO naturalmente) identifica anche il Privacy Manager. Ce lo racconta?

L'Arma si è data un modello che prevede la definizione di un perimetro, l'attribuzione di ruoli e responsabilità a tutte le entità che trattano dati personali e la definizione di procedure per l'esercizio di diritti privacy e per la gestione dei data breach. Sono stati previsti la mappatura e il rimodellamento di ogni processo in cui vengono trattati dati personali: informativa, notazione sul registro e un documento che dimostra la conformità del processo che viene validato dal DPO, dal CISO e dal Manager Privacy. E' stato attribuito quest'ultimo ruolo ad un Dirigente Generale che assiste il Comandante Generale nel coordinamento di tutti i soggetti che trattano dati all'interno dell'Arma. Non meno importante, la formazione: tutti gli ufficiali dirigenti sul piano nazionale hanno svolto un corso per valutatore privacy.

Marco Mariani (GFM - Net)

Per influenzare positivamente il decisore e quindi la macchina organizzativa, occorre presentarsi con una voce univoca ma pare già difficile parlarsi tra esperti. E allora partiamo da una questione semantica di fondo: cosa si intende per rischio, secondo la sua prospettiva?

Il rischio è la probabilità che accada un evento potenzialmente dannoso. Saper interpretare il rischio è fondamentale, ma è spesso fonte di equivoci anche perché si tratta di una probabilità per sua natura mutevole, dinamica ed in costante evoluzione. Fintanto che non capita l'evento dannoso, tipicamente l'azienda sottostima il rischio - e la conseguente perdita di denaro correlata - e non mette a disposizione risorse sufficienti per proteggersi e cercare di ridurre il perimetro di rischio. Nelle grandi realtà si impone un alto livello di sicurezza dei dati; nelle PMI se non traguarda un ROI la sicurezza cyber e la data protection sono considerate come mero costo. Ma il problema è che oggigiorno non è più una questione di *se*, ma di *quando* avverrà un data breach...meglio non farsi trovare deboli e impreparati.

Gianluca Lombardi (GL Consulting)

Cos'è il rischio, secondo la sua prospettiva?

Il vero rischio - che purtroppo riscontro quotidianamente, soprattutto nelle PMI - è l'assenza di comprensione delle motivazioni che sottostanno alle normative e alla richiesta di misure privacy. L'imprenditore non comprende le motivazioni per le quali deve pensare a una business impact analysis o a un piano di business continuity; non comprende perché non può installare le telecamere dove e come vuole, non capisce perché deve cancellare le mail di chi lascia l'azienda (le considera proprietà aziendale), non capisce il perché di una doppia autenticazione ai suoi sistemi (li considera spreco di tempo, complicazioni inutili). Il compito di noi consulenti privacy è far comprendere all'imprenditore, senza fare terrorismo, quello che rischia: una volta compreso questo, il budget non è mai un problema.

Una data governance accorta consente di raggiungere meglio e più rapidamente gli obiettivi aziendali; una data governance disattenta può fare grandi danni all'azienda e alla catena collegata

Guido Scorza (Garante Privacy)

Come si può trasformare la sicurezza del dato in uno strumento davvero competitivo e premiale per le imprese, come una "patente a punti" per intenderci?

L'obiettivo che ci siamo dati in passato è stato di portare la privacy ad essere considerata da costo a risorsa: non ci siamo ancora arrivati, ma ci stiamo avvicinando. Se la protezione del dato personale continua ad essere percepita come un mero adempimento amministrativo siamo, però, lontanissimi da questo obiettivo. E' essenziale abbandonare quella logica "antagonistica" tra il diritto a fare impresa e quello alla protezione dei dati personali, l'ancora consueta dicotomia tra autorità e soggetto vigilato. Libertà di impresa e tutela dei dati personali sono due diritti fondamentali che devono coesistere, non bisogna dover scegliere tra essi. Il fine ultimo del GDPR e del Data Act è anche quello di garantire la libera circolazione dei dati personali. Manca però ancora la cultura della privacy. Se scegliamo tutti la comodità e la semplicità (ad esempio acquistando il navigatore che fa risparmiare qualche minuto, ma che ignora i diritti) allora possiamo abbandonare la sfida. L'obiettivo è che il mercato scelga la privacy come driver competitivo, come è successo nel settore dell'automotive in tema di impatto ambientale, pur con l'auspicio che in questo avvenga in tempi più rapidi.

Andrea Billet (ACN - Agenzia per la Cybersicurezza Nazionale)

Come si può rendere la cyber security un elemento di competitività ed uno strumento premiale per le imprese meritevoli? Si parla di sgravi fiscali, di assicurazioni informatiche, di incidenza sul rating del cyber rischio, di corsie preferenziali nell'aggiudicazione di gare d'appalto...

Prima di premiare i migliori, sgombriamo il campo da chi compete in modo sleale, ossia chi vince la gara del prezzo perché non rispetta le regole o non mette in campo i necessari adempimenti. Per fare questo, l'agenzia sta qualificando diverse centinaia di servizi e operatori in ambito cloud; impone delle clausole nei bandi per imporre sensibilità al tema cyber; lavora col Garante per l'impiego della crittografia nelle password; siede ai tavoli per studiare i vari schemi di certificazione. Agevolazioni sul ranking? Ci arriveremo, ma non è ancora tempo. Il perimetro ad oggi è composto da gruppi enormi e realtà molto piccole ma non di rado eccellenti: non è possibile usare lo stesso metro. Per diversificare occorre adottare un modello di maturità*, ma serve ancora tempo per conoscere appieno il mercato e il suo livello di maturità. A regime, ai soggetti più qualificati verrà fornito un accreditamento tramite autocertificazione, ai soggetti che devono crescere verranno imposte delle regole e ai soggetti più arretrati verrà *portata la sicurezza* sotto forma di servizio gestito da soggetti specializzati con regole minime da seguire.

***modello di maturità =** strumento di valutazione che permette alle aziende, indipendentemente dal settore di appartenenza, di identificare quali siano le più grandi debolezze che riducono il giro d'affari del business

Giuseppe Alverone (Arma dei Carabinieri)

A Marzo il sito della Benemerita (e non solo quello) è stato oggetto di attacchi di hacker filorussi. Dovremmo aspettarci sempre più attacchi cyber anche di natura cosiddetta "etica"? I Carabinieri come possono condurre attività ispettive in un mondo così tecnologicamente dinamico?

A marzo scorso ci sono stati dei tentativi di attacco al sito dell'Arma che però non si sono tradotti in un vero data breach. Risultato: io l'ho appreso dalla rete e non dal CISO. Quanto alla natura "etica" degli attacchi, ricordo in primis che ogni attacco malevolo è da considerarsi reato. Chi peraltro pretende attenzione offrendo protezione rispetto a danni potenzialmente generabili da lui stesso, ricorda assai da vicino l'atteggiamento intimidatorio di stampo mafioso...quanto alla difesa, è vero che la tecnologia consente all'attaccante di nascondersi nell'anonimato, gli permette di giocare sull'effetto sorpresa e soprattutto di giocare fuori dalle regole. Per converso il difensore è costretto a giocare nel perimetro delle regole, ma posso affermare che l'Arma è oggi dotata di strumenti tecnologici e legali di difesa di tutto rispetto.

Marco Mariani (GFM - Net)

Il Comandante Alverone ha appreso dalla rete e non dal CISO dei tentativi di accesso al sito dell'Arma. Che succede quando un attacco informatico non comporta un data breach (almeno visibile), quindi non viene allertato il team privacy?

I danni possono essere inimmaginabili. Basta pensare all'esempio di log4jL (cfr. *secsolution magazine* 23/2023 pag. 60). Lì la vulnerabilità si chiuse a livello di CISO, quindi non venne data notizia al team privacy per valutare l'impatto sulla data protection. Ma il tam tam mediatico generatosi portò i legali a chiedere conto al CISO del danno arrecato. Ma il danno non c'era... oppure sì? Non ne possiamo essere certi, ma è assai probabile che qualcuno abbia approfittato della falla. In presenza di un team multidisciplinare, questo non sarebbe accaduto.

Gianluca Lombardi (GL Consulting)

Sembra che la comunicazione sia l'anello debole per un'efficace governance dei dati. Quali sono i rischi?

Se parliamo di comunicazione, ci possiamo riferire sia a quella interna alle aziende sia alla sfera della divulgazione. Lato divulgazione, manca la percezione del valore del dato e del rischio che si corre: sta a consulenti, DPO e informatici sensibilizzare le masse. Lato azienda, IT e Direzione faticano spesso a dialogare: gli informatici cercano di segnalare problematiche, anche importanti, legate alla protezione dei dati, ma la Direzione non comprende il pericolo e rimanda. L'IT chiede un budget per investire sulla sicurezza della rete ma il Board ritiene la richiesta esagerata perché sottostima il problema. In uno scenario di questo tipo, le aziende sono bersagli facili. Serve un linguaggio comune che renda comprensibile il messaggio tecnico e riesca a trasmettere la necessità di considerare il tema cybersecurity come prioritario.

cyber & privacy 2023
secsolutionforum®