DATA MANAGER

diffusione:18000
tiratura:20000

Forcepoint, Human-Point Protection

Il settore della cybersecurity guarda troppo alle tecnologie e troppo poco al fattore umano. Per Forcepoint la compliance con le normative su privacy e segreto industriale sarà il driver della sicurezza "comportamentale"

di Andrea Lawendel

Che la sicurezza di dati e transazioni sia un presupposto fondamentale per un digital business di successo, è ormai un fatto acquisito. Tuttavia, l'atteggiamento nei confronti delle normative che a livello nazionale o internazionale prescrivono determinati livelli di adeguamento a specifiche contromisure tecnologiche a maggior salvaguardia delle informazioni digitali spesso inducono diffidenza e malumori in azienda. La cosiddetta "compliance", il rispetto della normativa in materia di sicurezza informatica - per esempio la tutela della privacy - viene spesso percepita come un carico di lavoro in più e come un onere economico: tanto più quando le normative vigenti, come periodicamente accade, subiscono una profonda revisione, o vengono introdotti requisiti e vincoli nuovi. Il 2018 è un anno di svolta, una normativa importante come la General Data Protection Regulation (GDPR) entra in vigore, fissando precise scadenze per l'adozione di nuove misure che riguardano il trattamento dei dati digitali e introducendo un elemento ulteriore di novità: il mancato adeguamento normativo può costare caro per le sanzioni previste dalla legge. Le aziende che non si adegueranno alla normativa entro i termini stabiliti saranno passibili di sanzioni fino a 20 milioni di euro o al 4 per cento del fatturato.

NUOVE REGOLE PER UN BUSINESS INNOVATIVO

Questa e altre normative all'orizzonte hanno di conseguenza sollevato non poche preoccupazioni da parte di imprenditori, manager e responsabili IT e proprio per riportare il discorso su un piano il più concreto possibile, **Forcepoint** (www.forcepoint.com/it) - già conosciuta come Websense prima e Raytheon/Websense

DATA MANAGER

diffusione:18000
tiratura:20000

poi - tra i leader riconosciuti sul mercato delle soluzioni per la sicurezza informatica - ha organizzato in collaborazione con *Data Manager* in veste di partner editoriale, un workshop dedicato a compliance e protezione del dato. Il titolo, "GDPR e Trade Secrets Directive: opportunità normative per implementare la compliance", mette in evidenza la filosofia positiva che anima Forcepoint e l'intero settore della tecnologia e dei servizi di cybersecurity. Lungi dall'essere considerate delle "costose manette", normative e compliance rappresentano una grande opportunità per un business innovativo, che nelle nuove regole e nelle strategie di adeguamento messe in atto dalle imprese, trova una valida certificazione di qualità e affidabilità. Al gruppo di lavoro hanno preso parte, accanto a **Luca Mairani** (senior sales engineer di Forcepoint ma selezionato tra i docenti del seminario in rappresentanza di Clusit) che ha delineato un quadro aggiornato del mondo delle "cyber minacce", anche due legali specializzati in diritto digitale: gli avvocati **Giuseppe Vaciago** e **Gianluca Morretta**, che hanno affrontato gli aspetti più tecnici delle nuove normative e dei relativi vincoli di compliance. **Emiliano Massa** e **Ferdinando Mancini** (rispettivamente area vice president sales Southern Europe e director sales engineering per Italia, Spagna e regione MEA di Forcepoint) hanno poi fornito una serie di spunti sia sulla generale strategia di prodotto sia sulle specifiche soluzioni che oggi caratterizzano l'offerta del provider tecnologico americano.

CHI NON SI ADEGUA PAGA

Il livello della partecipazione e l'interesse dimostrato dal pubblico sono stati particolarmente elevati e la cosa non sorprende più di tanto. Con l'introduzione della GDPR, della Trade Secrets Directive e, in prospettiva, della Network Infrastructure Security, l'intero spazio normativo europeo in materia di protezione di dati e infrastrutture fisiche e virtuali compie un netto balzo in avanti rispetto al passato, con nuovi obblighi e precise - e salate - sanzioni. Le nuove regole sulla protezione dei dati - che entreranno in vigore nel 2018 e non necessitano di recepimento da parte del nostro Parlamento - sposta l'attenzione finora focalizzata soprattutto sulla tutela dei dati personali e della privacy del consumatore, verso una dimensione più estesa del dato come asset fondamentale dell'impresa. Quest'ultimo è esattamente l'ambito della direttiva europea del 2016 sulla "protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti". Trattandosi di direttiva, questa norma invece dovrà essere recepita dalla legislazione italiana, entro il maggio del 2018. Entrambe le tematiche sono tuttavia in un certo senso già presenti, "in pectore" nell'azione del Parlamento e del Governo. Per esempio, nei decreti attuativi del cosiddetto Job Act, che prevedendo il diritto del lavoratore alla riservatezza e alla dignità, concede alle imprese un certo spazio di manovra tecnologico proprio con la finalità di tutelare le informazioni sensibili pertinenti al business. All'orizzonte, infine, si delinea l'entrata in vigore di una terza normativa europea, la numero 1148 del 2016 (NIS) che dovrà essere anch'essa recepita entro il 25 maggio 2018. Lo scorso mese di marzo, il governo Gentiloni aveva già acquisito le necessarie deleghe per il progetto di legge di recepimento dell'insieme di regole questa volta centrate sulla sicurezza e la protezione di reti e sistemi informativi. Il seminario promosso da Forcepoint inizia fornendo una descrizione dello scenario su cui insistono i meccanismi previsti dalle nuove norme. «Il 2016 è stato l'anno peggiore di sempre in termini di cybersecurity» – ha esordito Luca Mairani. «Non serve più mettere insieme la banda del buco. Si possono guadagnare molti più soldi con il cybercrime, specie andando a colpire obiettivi specifici». L'ultimo Rapporto Clusit cita dati ENISA, l'agenzia UE per la sicurezza informatica, in cui vengono segnalati in forte crescita fenomeni come malware, attacchi via web, anche usando dispositivi IoT, reti "bot", phishing e ransomware. All'interno della top ten delle minacce, troviamo l'insieme dei cosiddetti "insider", dipendenti delle aziende che agiscono scientemente per carpire e rivendere informazioni riservate delle aziende per cui lavorano.

Luca Mairani senior sales engineer di Forcepoint e membro di Clusit **Emiliano Massa** area vice president sales Southern Europe di Forcepoint
Ferdinando Mancini director sales engineering per Italia, Spagna e regione MEA di Forcepoint

DATA MANAGER

diffusione:18000
tiratura:20000

Data protection, privacy e security: le nuove regole come fattori di complessità e driver verso una dimensione più estesa del dato in ottica strategica e di accountability

L'ANNUS HORRIBILIS DEI CYBERATTACCHI

«Il data leakage, cioè la fuga dolosa di informazione, è triplicata in termini di eventi, valore e record perduti – sottolinea Mairani – e il fenomeno è più difficile da gestire perché i furti avvengono non più attraverso dispositivi fisici come le chiavette, ma con i dischi virtuali del cloud. In un caso su due, il data theft viene fatto risalire al furto di credenziali, altro fenomeno in crescita. Una credenziale d'accesso costa solo sette dollari sul mercato nero e uno studio europeo ripreso da Forcepoint valuta in una percentuale del 17 per cento la quota di dipendenti che sarebbero disposti a vendere la propria identità». Mairani cita il caso della compromissione di mezzo miliardo di utenze Yahoo! nel 2014. «In realtà, si stima una perdita compresa tra uno e tre miliardi di account. E quel che è peggio è che l'AD di allora, Marissa Mayer, mise a tacere l'entità del disastro». Non a caso le nuove normative indirizzano proprio il problema dell'omissione, obbligando le vittime di un attacco a denunciarne l'entità. Le strategie di difesa devono però partire dalla consapevolezza della "minaccia interna". Oggi, l'utente autorizzato è diventato un elemento critico nella catena informativa aziendale, conclude Mairani: «Il problema in questo caso si trova tra la tastiera e la sedia».

L'obiettivo dell'intervento di **Giuseppe Vaciago di** R&P Legal (www.replegal.it) non è quello di illustrare punto per punto il contenuto di una norma, la GDPR, intorno alla quale si è creata da tempo una ampia offerta formativa. «La cosa interessante è il modo in cui la GDPR trasforma il paradigma della sicurezza». La differenza tra privacy intesa come riservatezza e il trattamento, la protezione del dato è rimasta troppo a lungo latente, osserva Vaciago, facendo sì che per una quindicina d'anni, le aziende interpretassero la precedente normativa come una "rottura di scatole" fatta solo di moduli e firme per il consenso al trattamento. «La GDPR mette le cose a posto introducendo il principio di accountability, affermando cioè che le aziende sono responsabili dell'implementazione delle misure di protezione e devono dimostrare a terzi la loro validità». Un cambiamento che stimola un approccio pragmatico, attraverso concetti come i codici di condotta e il Registro di Trattamento (reso obbligatorio per aziende con più di 250 dipendenti). «Per quest'ultimo esistono specifici applicativi in grado di assistere nella compilazione» – ha ricordato Vaciago consigliandone l'impiego. «Questi due concetti sono il cardine del regolamento le cui novità sostanziali sono la Privacy by Design, il principio dell'accountability, l'obbligo di notifica al Garante esteso a tutte le società in caso di data breach, i nuovi diritti all'oblio e alla portabilità, oltre all'istituzione del ruolo del Data Protection Officer».

VECCHI RISCHI NUOVE RESPONSABILITÀ

Nel suo intervento, l'esperto di diritto penale societario e delle nuove tecnologie ha messo in risalto anche alcuni spazi di incertezza sul piano della execution di una normativa complessa e ancora da interpretare, riconoscendo tuttavia l'effetto positivo che un regolamento correttamente implementato può avere sull'intera filiera dell'IT aziendale e sulla cultura del dato come valore.

La violazione dei dati (data breach) diventa il problema centrale delle aziende sia per il rischio di subirla sia per le procedure obbligatorie di notifica. «Nel momento in cui un soggetto subisce un data breach, lo deve notificare a tutti gli interessati alla violazione, a meno di non poter dimostrare, tramite codice di condotta o certificazioni come la 27001, di essersi dotato di adeguati strumenti di protezione».

La creazione di figure responsabili di questa tutela, conclude Vaciago, potrà avere un effetto positivo analogo a quello del responsabile della prevenzione e protezione, previsto dalle leggi sulla sicurezza del lavoro. «Una figura che ha portato a una diminuzione degli incidenti mortali».

La discussione sulla direttiva "Trade Secrets" di **Gianluca** Morretta **di** R&P Legal parte col rilevare la qualità della normativa italiana che tutela la proprietà intellettuale. «In Italia, il segreto aziendale è ben protetto, facciamo a mio parere un'ottima figura in sede internazionale. Tant'è vero che la direttiva europea riprende molte delle tematiche affrontate dalle nostre normative e il lavoro di integrazione sarà modesto». Anche l'armonizzazione a livello europeo sarà positiva e secondo l'esperto nella tutela della proprietà intellettuale e industriale, faciliterà lo sforzo necessario per colmare gli attuali gap di implementazione. «Proteggere i segreti aziendali richiederà molti investimenti, ma una buona disciplina aiuta». I fenomeni di violazione sono sicuramente in aumento, riconosce Morretta, ma il know-how «resta il più intangibile dei beni intangibili». Uno dei punti da far risaltare, anche perché legato agli aspetti sanzionatori della direttiva, è l'equiparazione della violazione del segreto industriale al concetto di illecito vantaggio competitivo: «Una informazione riservata può consentire a un concorrente di arrivare prima sul mercato. E carpirla equivale a un furto».

TRA SEGRETI INDUSTRIALI E CONCORRENZA SLEALE

Come spiega Morretta, l'accesso all'informazione deve essere selettivo e sotto il pieno controllo da parte del proprietario del dato riservato, tenendo presente le due grandi "famiglie" di sottrazione: «Quella interna, di dati non accessibili, e quella che invece consegue a una divulgazione formalmente autorizzata». Alla fine del suo intervento, il legale si è occupato anche degli aspetti relativi a nuove forme di

DATA MANAGER

diffusione:18000
tiratura:20000

tutela giuridica, inclusa quella cautelare, che prevedono per esempio la possibilità di ricorrere a perquisizioni utili a reperire le prove di una violazione. Anche chi è sospettato di un illecito può accedere a forme di salvaguardia - inclusa l'autorizzazione allo sfruttamento dell'informazione, dietro adeguate garanzie a sostegno di un eventuale futuro risarcimento. Così come per «i terzi in buona fede che hanno acquistato il prodotto figlio della violazione, che potranno versare un indennizzo per continuare a utilizzare quel prodotto».

A **Emiliano Massa** è spettato il compito di orientare la bussola del convegno da una dimensione di legalità all'ambito tecnologico. Ma è davvero di natura tecnologica la risposta alla domanda di protezione generata dai nuovi regolamenti? La domanda nasce spontanea, parlando della svolta strategica che il nuovo CEO di Forcepoint, Matthew Moynahan, insediatosi poco più di un anno fa, ha impresso all'azienda. «La compliance è un driver, ma anche un fattore di complessità. In molti casi, noi provider di sicurezza abbiamo fatto parte più del problema che della soluzione» – ha riconosciuto Massa. «Forcepoint ha saputo guardarsi dentro e cambiare la propria focalizzazione in direzione delle persone». Parlando degli aspetti giuridici delle normative, gli esperti hanno fatto riferimento a codici di condotta e policy. «Ma non possiamo pensare a una policy unica – ha detto Massa – perché le decisioni, i comportamenti di ciascuno, in azienda, hanno una componente emotiva e mutevole. Per questo abbiamo cambiato paradigma». Finora il mondo della security si è concentrato sulle minacce esterne e interne, cercando di impedire l'accesso ai "bad guys". «Ma forse – ha continuato Massa – bisogna guardare alle intenzioni che animano ciascuno di noi quando interagiamo con i dati». Partendo da un presupposto quasi "pirandelliano", ciascuno di noi, ha centomila maschere, a seconda delle emozioni del momento. La nuova filosofia alla base dello sviluppo tecnologico di Forcepoint non ha solo la protezione degli "endpoint" come obiettivo, ma soprattutto la gestione corretta dello Human Point, il delicato punto di interfaccia tra essere umano e informazione digitale. «La nostra missione – conclude Massa – non deve essere quella di bloccare indiscriminatamente, ma di fornire in ogni istante le informazioni necessarie a prendere le decisioni giuste, nella massima sicurezza possibile».

Giuseppe Vaciago avvocato associato di R&P Legal - Rossotto, Colombatto & Partners
Gianluca Morretta avvocato associato di R&P Legal - Rossotto, Colombatto & Partners

SICUREZZA ISTRUZIONI PER L'USO

Prima della sessione di casi di studio e domande del pubblico che ha concluso il workshop sulla protezione dei dati, **Ferdinando Mancini** ha raccontato alcune delle novità che riguardano l'uso degli strumenti di cybersecurity targati Forcepoint a presidio di questa mutevole interfaccia uomo-dato. In una realtà fatta di cloud computing, mobilità, dispositivi e applicazioni a cavallo tra impieghi professionali e sfera personale, i nostri comportamenti cambiano da un momento all'altro. «Come gestire allora il rischio sicurezza con sistemi che non parlano l'uno con l'altro, di log di eventi che non riusciamo a correlare?» – si chiede Mancini, mostrando a video le soluzioni mirate contro il data leakage e il nuovo "dashboard" della soluzione, di origine militare, che Forcepoint ha mutuato da Raytheon per combattere le "insider threat", le minacce interne. «L'approccio alla base della reportistica fornita da queste soluzioni consiste nel valutare di volta in volta l'importanza delle deviazioni rispetto ai comportamenti medi». Se a un certo punto l'addetta al telemarketing lancia processi basati su script molto complessi, il sistema illustra i possibili scenari - leciti o illeciti, autorizzati o fraudolenti - che spiegano la natura di questo comportamento. Gli "actionable reports" di Forcepoint non forniscono solo i valori delle soglie di rischio, ma suggeriscono le azioni che un'azienda, anche non dotata di specifiche competenze né tantomeno di un Security Operation Center, può implementare, nella pratica quotidiana, per realizzare concretamente una sicurezza «human-centered» e rispettosa delle future normative.