Quanto vale per voi un dato personale?

Si avvicina la fine dell'anno e per molti professionisti delle sicurezza informatica significa che è arrivato il momento di avviare il risk assessment, con tutto quello che comporta: audit, interviste, questionari, stime, bilanci, ecc.

Che l'obiettivo sia quello di governare in modo consapevole la sicurezza IT, soddisfare obblighi normativi (Privacy) o regole di certificazione (ISO27001), il lavoro da fare è più o meno il medesimo:

- Si recupera l'elenco dei beni da proteggere per procedere alla specifica classificazione con il relativo responsabile.
- Si individuano le minacce, le vulnerabilità, le contromisure esistenti, i potenziali impatti, ecc.
- Si stima il livello di rischio.
- Si pianificano e si mettono in atto le eventuali azioni correttive o preventive sulla base di un rapporto tra rischi, costi degli interventi e benefici attesi.

I processi e le metodologie variano, come pure il contesto operativo (risorse e strumenti disponibili, impegno ed interesse dell'azienda, complessità e dimensione del perimetro, competenze tecniche disponibili, ecc.) ma i passaggi fondamentali non sono poi così diversi.

Uno degli aspetti più delicati riguarda la modalità di classificazione dei beni. Generalmente classificare un bene consiste nell'assegnargli un valore di importanza rispetto ad aspetti di sicurezza. In pratica si assegna un voto utilizzando una scala di valori più o meno ampia (“1-Basso/2-Medio/3-Alto”, “1-Molto Basso/2-Basso/3-Medio/4-Alto/5-Molto Alto”, ...).

Si tratta di un processo apparentemente semplice che però nasconde alcune insidie: chi effettua la classificazione potrebbe infatti non essere in grado di produrre una valutazione oggettiva rispetto a quelli che sono gli interessi dell'azienda o dell'ente.

Se chiedessimo all'autista di un'utilitaria piuttosto costosa (15.000€ IVA inclusa) di assegnare un voto da 1 (Basso) a 3 (Alto) al suo unico mezzo di trasporto, probabilmente otterremmo il voto massimo. Se facessimo la stessa domanda all'autista di una berlina di lusso (100.000€ IVA inclusa), probabilmente riceveremmo lo stesso giudizio. Nulla di strano, a meno che le due votazioni non siano usate per decidere su quale auto installare un costosissimo sistema antifurto: due auto di valore molto diverso avrebbero lo stesso voto e, quindi, risulterebbero equivalenti per la scelta dell'antifurto.

Per risolvere l'inconveniente si potrebbero fornire ai due autisti alcune indicazioni su come effettuare la valutazione. Ad esempio si potrebbero suggerire le seguenti regole generali:

- Il punteggio 1 (Basso) deve essere assegnato a tutti quei veicoli del valore compreso tra 1€ e 10.000€;

- Il punteggio 2 (Medio) deve essere assegnato a tutti quei veicoli del valore compreso tra 10.001€ e 20.000€;

- Il punteggio 3 (Alto) deve essere assegnato a tutti quei veicoli del valore superiore a 20.001€.

Con queste regole i due autisti fornirebbero una differente valutazione: l'utilitaria riceverebbe il punteggio 2 (Medio) e la berlina di lusso riceverebbe il punteggio 3 (Alto). In questo modo sembrerebbe risolta elegantemente la questione dell'antifurto.

Probabilmente non saremmo altrettanto certi della bontà della soluzione trovata venendo a sapere che, in realtà, l'utilitaria è impiegata giornalmente per la consegna di costosi farmaci salvavita agli ospedali di Firenze e che la berlina è assegnata al Direttore Commerciale presso la filiale di Udine. Le precedenti regole di classificazione potrebbero non risultare più adeguate anche se, per fare un altro esempio, la flotta aziendale venisse ampliata con cinque nuove automobili del valore di 50.000€.

La questione non è di facile soluzione e per affrontarla in modo corretto è necessaria una buona conoscenza del “business”, quindi un forte coinvolgimento di tutto il management.

Lo scenario si complica notevolmente se si usano scale di valori per definire altri concetti come le probabilità di accadimento delle minacce (“la probabilità che si verifichi un tentativo di furto è 1-Bassa/2-Media/3-Alta”) e i livelli di vulnerabilità (“la vulnerabilità al furto è 1-Bassa/2-Media/3-Alta”). Se poi aggiungiamo anche operazioni aritmetiche tra questi concetti dicendo, ad esempio, che il livello di rischio si ottiene moltiplicando il valore del bene, la probabilità di accadimento di una minaccia ed il livello di vulnerabilità, la faccenda si fa veramente intricata. Si tratta in effetti di una criticità che riguarda tutte le metodologie qualitative basate su scale di valori (per approfondimenti suggerisco il recente “The Failure of Risk Management: Why It's Broken and How to Fix It” [1] di Douglas Hubbard).

Un approccio migliore potrebbe essere quello di impiegare metodologie quantitative, stimando il valore dei beni sulla base di costi reali o potenziali. In un'architettura ridondata, per fare un esempio, l'impatto derivante dalla distruzione fisica di un singolo server potrebbe essere calcolato in termini di:

- costi per l'acquisto di un nuovo server;

- costi delle risorse umane impegnate nelle attività di installazione, configurazione e ripristino dei backup;

- costi indiretti di varia natura.

Trattando beni immateriali però tutto diventa più difficile. Un caso emblematico potrebbe essere rappresentato dalla valutazione d'impatto del furto di un archivio informatico contenente i dati dei 500 pazienti di una clinica psichiatrica.

In questo caso gli elementi da considerare sarebbero molti:

- le patologie trattate dalla clinica (potrebbe essere una clinica specializzata nella cura delle tossicodipendenze, oppure di patologie depressive o, ancora, di disturbi del comportamento sessuale);

- le tipologia di pazienti (potremmo avere a che fare con il database di una clinica esclusiva, frequentata abitualmente da personalità dello spettacolo o dell'imprenditoria);

- il tipo di dati archiviati (solo dati di fatturazione e riferimenti telefonici, cartelle cliniche complete e dettagliate, ecc.);

- le misure di sicurezza adottate (ad esempio se i dati sono cifrati).

Inoltre, anche conoscendo le diverse caratteristiche dell'archivio, ragionare in termini di costi può risultare comunque arduo. Entrano in gioco fattori quali il danno cagionato al singolo paziente dall'utilizzo improprio dei dati, il danno d'immagine per la clinica (i mancati ricavi dovuti alla fuga dei potenziali pazienti), eventuali sanzioni civili e penali per l'inadeguata protezione dell'archivio, i costi dovuti al ripristino ed alla messa in sicurezza dell'archivio, ecc.

Se provate a confrontarvi con un consulente legale sui possibili costi da sostenere per il risarcimento danni, probabilmente avreste difficoltà a far emergere una stima. Generalmente infatti le cause civili si basano elementi concreti e oggettivi, specifici per il singolo caso: giorni di invalidità temporanea o permanente causati, conseguenze patrimoniali calcolate sulla base di fattori quali il reddito medio del soggetto interessato, le spese mediche sostenute, ecc.

Per stimare il valore dell'archivio informatico dell'esempio precedente non è chiaramente possibile entrare nel merito di ogni singolo paziente censito. Si può però tentare di scoprire se il problema è stato già affrontato e, magari, risolto da qualcuno.

Si vengono così a sapere alcune notizie interessanti come, ad esempio, che:

- Negli Stati Uniti nel 2009 una violazione della sicurezza è costata mediamente 204$ per ogni record compromesso (si considerano sia i costi diretti che quelli indiretti), e che le violazioni nelle industrie che operano in ambito sanitario e

farmaceutico costano più care, cioè rispettivamente 294$ e 310$ [3].

- Il valore di ogni utente di Facebook è stimato fino a 100$ [7].
- Al mercato nero un'identità digitale completa viene valutata tra i 6$ e gli 80$ (30-40 identità possono essere acquistate per 20$) [5].
- Sempre al mercato nero, una cartella clinica vale tra 50$ e 60$ [6].

Si possono inoltre trovare alcuni interessanti “modelli”, gratuiti o a pagamento, per calcolare il costo di una violazione alla sicurezza.

Dal punto di vista metodologico si possono sollevare numerose ragionevoli obiezioni all'impiego delle informazioni riportate sopra. Uno degli aspetti più evidenti è la provenienza delle aziende: infatti i dati riguardano principalmente aziende statunitensi, operanti quindi in una realtà molto diversa da quella italiana, sia da un punto di vista legislativo, che economico, che culturale.

Del resto si può anche notare che i valori risultano piuttosto omogenei. Si tratta cioè di informazioni che ci potrebbero permettere di costruire un primo modello, magari molto approssimativo, per stimare l'impatto derivante dalla violazione di sicurezza e permetterci comunque di operare. Naturalmente si tratterebbe di un modello che deve essere costantemente verificato ed evoluto, secondo un processo iterativo di miglioramento continuo.

A questo punto dovremmo chiederci se è proprio necessario individuare in modo esatto il valore del singolo dato personale presente nell'archivio per avere benefici dall'impiego dei metodi quantitativi. Meglio ancora, se l'impiego di metodi quantitativi, con tutte le approssimazioni del caso, ci consente di prendere decisioni migliori rispetto a quelle che prenderemmo utilizzando metodi qualitativi.

Possiamo prendere decisioni migliori sulla sicurezza considerando che l'impatto per il furto dei dati dei 500 pazienti di una clinica psichiatrica è “Molto Alto”, oppure considerando che, con i dati disponibili, l'impatto è stimato tra 200$ e 300$ a paziente, cioè complessivamente tra i 100.000$ e i 150.000$?

Quanto vale per voi un dato personale?

Riferimenti

[1] Douglas W. Hubbard, The Failure of Risk Management, John Wiley & Sons, 2009.

[2] Gary Stoneburner, Alice Goguen, Alexis Feringa, Risk Management Guide for Information Technology Systems, NISP Special Publication 800-30, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2002. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

[3] Ponemon Institute, 2009 Annual Study: U.S. Cost of a Data Breach, PGP Corporation, 2010.
<http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf>

[4] Frank Costaneira, Quantified Risk Analysis for PCI, ISSA Journal, 2010.

[5] Antonio Forzieri, presentazione: Le minacce, le tecniche di attacco e i canali di vendita delle informazioni, Symantec, 2010.
<http://www.emea.symantec.com/info/pdf/it/Ppt_forzieri_am.pdf>

[6] James Koenig, Trends in Privacy, Security, Identity Theft and Information Risk Management, PricewaterhouseCoopers, 2009.
<http://www.phillyisaca.org/Documents/PwC%20Koenig%20ISACA%20Privacy%20Hot%20Topics%20v1.2.pdf>

[7] Stefania Rimini, Il prodotto sei tu, Report, Rai, puntata del 10 aprile 2011.