Organizzare le risorse e rendere sicure le Informazioni per lo sviluppo nel tempo di Industria 4.0

Workshop

Andrea Foschi

Bologna, 6 settembre 2017

La sicurezza ad oggi

Le minacce dovute ad attacchi volontari stanno sempre più aumentando affiancando alle da logiche di attacchi massivi logiche mirate e personali (*Social Engineering*).

Ora come non mai il crimine informatico ha un ben preciso obiettivo : quello **economico**. Meno rumore per una pericolosità decisamente maggiore.

Non vengono coinvolti “solo” i dati, le minacce potrebbe riguardare aspetti infrastrutturali critici, quali rete elettriche, gasdotti, sistemi idrici, ecc.

In questo scenario si sfrutta l’opportunità : il più vulnerabile.

Sempre più si richiamano le aziende ad una responsabilità “sociale” condivisa : “…il problema non è più solo mio”

La sicurezza ad oggi

Se i grandi rischi sono “statisticamente” meno probabili (ma con maggiori impatti) , è la quotidianità a portarci un insieme di rischi (ad impatti meno rilevanti) ma invece assai probabili.

- Non rare le azioni dolose apportate da persone molto vicini alle organizzazioni, spesso avvantaggiate dalla conoscenza del contesto (asset e vulnerabilità) e dalle facili opportunità.
- Non sempre i pericoli sono legati ad azione dolose e volontarie; altrettanto pericolosa è la non corretta gestione dell’elevata complessità tecnologica (sempre più in ascesa).

L'importanza e l'aumento dell'informazione

L' informazione è oggi un elemento "cruciale" per poter svolgere qualsiasi tipo di attività; tutte le Organizzazioni trattano oramai un numero di informazioni che è aumentato in modo esponenziale nel tempo … forse fin troppe.

E' pertanto cresciuta la consapevolezza di quanto l'informazione (*parte degli Asset "intangibili" di ogni Organizzazione*) siano un **valore strategico**

La distruzione o la divulgazione non consentita di una informazione di business produce sempre e comunque un danno all'azienda.

Industry 4.0

I 3 paradigmi

- **Smart production**: nuove tecnologie produttive che creano collaborazione tra operatore, macchine e strumenti.
- **Smart services**: tutte le "infrastrutture informatiche" e tecniche che permettono di integrare fra sistemi e aziende (fornitore – cliente)
- **Smart energy**: sistemi più performanti riducendo gli sprechi di energia secondo i paradigmi tipici dell'Energia sostenibile.

Industry 4.0 si fonda sui sistemi ciberfisici (CPS) ovvero sistemi fisici **strettamente connessi con i sistemi informatici** e che possono interagire e collaborare con altri sistemi CPS (decentralizzazione e collaborazione tra i sistemi)

IOT (Internet of things)

Gli oggetti (le "cose") si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri.

Per "cosa" si può intendere : dispositivi, apparecchiature, impianti e sistemi, materiali e prodotti tangibili, opere e beni, macchine e attrezzature.

L'obiettivo dell'internet delle cose è far sì che il mondo elettronico tracci una mappa di quello reale, dando un'identità elettronica alle cose e ai luoghi dell'ambiente fisico. Gli oggetti e i luoghi muniti di sistemi di identificazione (etichette, Rfid, Codici QR, ecc.) comunicano informazioni in rete o a dispositivi mobili.

Industry 4.0 e IOT ... quale futuro ?

Industry 4.0 e IOT : due chiavi di lettura delle medesime opportunità... ma dei medesimi problemi

Maggiore volumi di dati trattati

Scambio ed elaborazione automatico di dati

Maggior numero di device (punti di ingresso) e complessità

Minor presidio e controllo umano

Maggiori vulnerabilità e Rischi

Garantire la sicurezza

Garantire la sicurezza delle proprie informazioni significa quindi garantire il proprio patrimonio da potenziali danni … anche se a riguardo le imprese maggiormente sensibili sono proprio quelle **che hanno subito rilevanti perdite di dati** e, di conseguenza, gravi perdite economiche.

Questo accade perché le imprese spesso tendono a sottovalutare i rischi connessi ad una non corretta gestione e tutela delle informazioni.

Il tema della "Security" non passa solo dal governare e tutelare il proprio Sistema Informativo bensì dal:

- *conoscere l'intera "mappa" delle informazioni aziendali (cartacee, informatiche, vocali, audio, video, ecc…)*
- *comprendere il valore delle diverse tipologie di dati gestiti*
- *prevedere opportune azioni a tutela degli stessi in base ad una corretta analisi dei rischi*

Devo esser contento se non ci succede nulla ?

La scarsa propensione al rischio fa si che le funzioni che si occupano di IT e Security in azienda abbiano spesso problemi a giustificare le spese inerenti la sicurezza delle informazioni

a peggiorare questa considerazione il fatto che la dimensione economica della sicurezza si fonda su un paradosso che affascina gli economisti e demoralizza i Manager IT:

più un investimento in sicurezza è adeguato meno visibili e misurabili sono i suoi risultati !

La misura dell'efficacia

Si può dare una metrica a quello che potenzialmente potrebbe accadere (analisi dei rischi)…

ma misurare ciò che "realmente" non è accaduto per via di una adozione di corrette contromisure di sicurezza … beh è estremamente difficile.

E quindi non rimane che affidarsi a **metodi** ed adeguati strumenti (di analisi e tecnici)…e misurare la loro efficacia.

Analisi dei rischi nel GDPR

Art. 32 - Sicurezza del trattamento

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del **contesto e delle finalità del trattamento**, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure** tecniche e organizzative **adeguate** per garantire un livello di sicurezza **adeguato** al **rischio**, che comprendono, tra le altre, se del caso:

a) la capacità di assicurare su base permanente la **riservatezza**, **l'integrità**, **la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento;
b) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
c) una procedura per **testare, verificare e valutare** regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2.Nel valutare **l'adeguato livello di sicurezza**, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ...

Regolamento UE 2016/679

Solo Compliance ?

- Un azienda che ha la necessità di implementare soluzioni di conformità legislative sul fronte della sicurezza delle informazioni (es. GDPR) avrà, quasi sicuramente, anche problematiche di sicurezza di Business.
- Nell'ambito della compliance non esiste solo l'aspetto del GDPR collegato alla sicurezza delle informazioni ... non ultimo il D.Lgs 231 (ma anche altro).
- I costi di adeguamento ad aspetti di conformità (es. PIA e AR per GDPR; Protocolli 231, ecc) spesso non hanno ordini di grandezza differenti rispetto ad affrontare il tema della sicurezza delle informazioni in modo più esteso.
- Include valenze anche di Business nella gestione della sicurezza delle informazioni rende più efficace anche la parte di compliance.

Approccio alla sicurezza

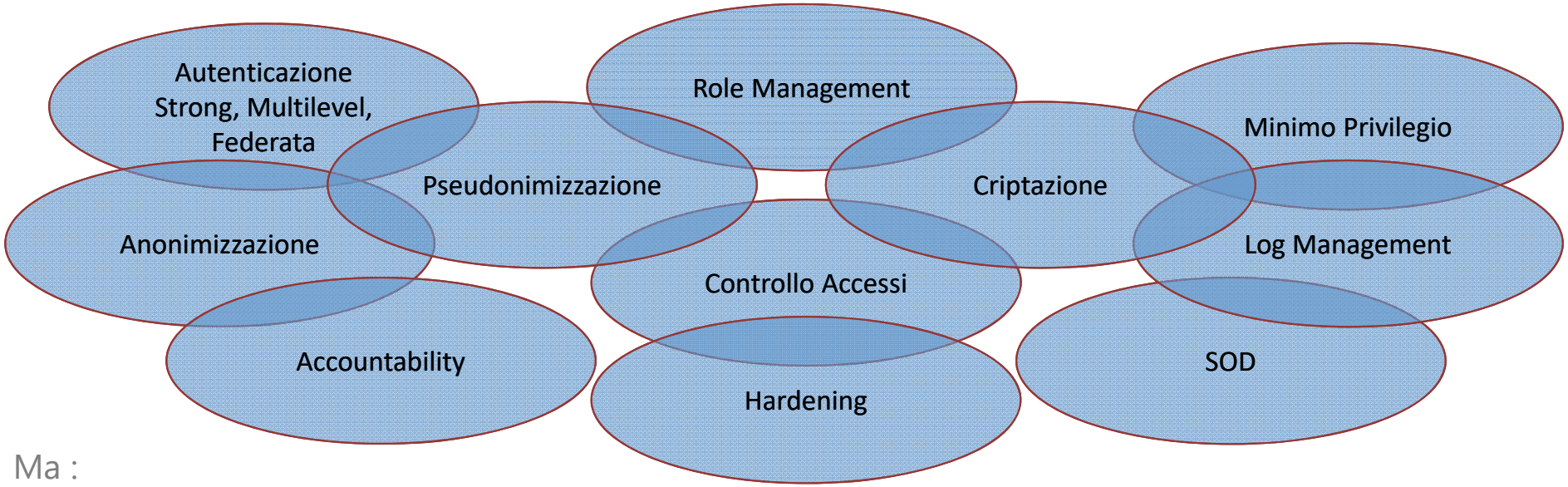
"Governare" la sicurezza significa prima di tutto avere la conoscenza di quello che può accadere e degli impatti che questo può provocare sulla nostra organizzazione sotto ogni punto di vista (business e compliance).

Questo significa che la metodologia, l'organizzazione e l'esperienza giocano un ruolo fondamentale.

Meglio quindi partire da metodologie e strumenti acquisiti e consolidati, adattandoli e contestualizzandoli alla nostra realtà (es. ISO27001).

È anche vero però che …

LE SOLUZIONI DI IDENTITY GOVERNANCE



Ma :
-Le misure identificate potrebbero essere non idonee
-Non riesco a dimostrare una correlazione fra rischio e controlli
-Potrei implementare contromisure eccessive

…sono tutte best practice alla base di un buon

Attenzione all'effetto "misure minime di sicurezza" del Dlgs 196/03

Sistema per la Gestione della Sicurezza delle informazioni

Riferimenti

Andrea Foschi
afoschi@soluzioniaziendali.net

Soluzioni srl

Via Andrea Ercolani, 9 40026 Imola
info@soluzioniaziendali.net www.soluzioniaziendali.net