Cybersecurity Trends

Edizione italiana, N. 3 / 2022

INTERVISTE VIP:

- TEAM YOROI
- RICCARDO PORCU

Folder Centrale: Security vs Compliance

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Cybersecurity Trends

Leggi la rivista **online** quando
e dove vuoi!
Puoi scegliere tra news, articoli,
interviste, nuove sezioni,
approfondimenti,
rubriche e contenuti multimediali.

Scopri anche la nuova sezione
dedicata agli esperti della cyber security!
Al suo interno
Hacking Around e Technical Video.

Nella sezione Rubriche:
Bibliografia
Dalla Redazione
Dalle Aziende
Dalle Università
Eventi
Offerte di Lavoro

www.cybertrends.it

Indice

Bilanciare compliance e sicurezza nel dominio digitale.

Autore: Nicola Sotira

Sempre più aziende sono nel vortice della nuova sfida della trasformazione del loro business in digitale. In questo contesto le tecnologie come quelle del Cloud, IOT, mobile ci vengono incontro e promettono di migliorare i processi rendendo le aziende più innovative, flessibili e agili, tutti requisiti fondamentali per la crescita. In parallelo si stanno moltiplicando le normative, in particolare quelle relative alla sicurezza cyber e la privacy a tutela dei dati dei cittadini. La trasformazione digitale si trova così a ricercare un equilibrio tra i processi nel nuovo dominio e il rispetto delle normative sulla protezione dei dati. La piena convergenza di questi aspetti oggi impone alle organizzazioni da un lato di accelerare i propri processi di trasformazione digitale e dall'altro di ripensare la sicurezza, affinché sia realmente integrata in questa nuova filiera. Molte aziende si stanno orientando verso architetture Cloud, queste ultime permettono una migliore automazione valutando costantemente entrambi gli aspetti legati a sicurezza e rispetto della conformità normativa. Una delle problematiche che si deve affrontare in questo scenario è la continua evoluzione di questi servizi che, tipicamente, generano, raccolgono e analizzano grandi quantità di dati. La completa visibilità di questi ambienti diventa quindi di importanza rilevante in modo da consentire alle aziende il monitoraggio e la protezione constante di queste risorse gestendo in modo efficace anche gli aspetti di compliance. Compliance e sicurezza sono, spesso, viste nelle aziende come un ostacolo all'innovazione, processi che rallentano il processo di trasformazione, fenomeno, questo che avviene quando quest'ultima non va nella direzione di rendere più snelli e integrati i processi inerenti la sicurezza e la conformità. Occorre, pertanto, intraprendere il percorso di trasformazione digitale mediante l'adozione di tecnologie e processi che integrino gli aspetti di sicurezza e di conformità agli aspetti normativi rendendo così questo aspetto parte del processo digitale. Fondamentale è poi riuscire ad avviare le attività di conformità normativa focalizzandosi sui comparti in azienda a maggior rischio. Risulta quindi indispensabile una puntuale analisi dei rischi dinamica e il monitoraggio in tempo reale. Attività nelle quali gli strumenti di intelligenza artificiale, tra cui il machine learning, ci possono supportare nell'automazione, la raccolta dei dati e l'analisi di grandi quantità di dati al fine di identificare, o fare previsioni, su eventi ritenuti sospetti dal punto di vista sicurezza o darci visibilità su eventuali posture che possono non essere in linea con quanto previsto dalle normative. È evidente che al centro della trasformazione digitale del business si pone la creazione del valore. Creazione del valore sia per i clienti sia per la stessa organizzazione, quindi la digitalizzazione deve andare nella direzione del risparmio dei costi, l'incremento di efficienza operativa e un miglioramento complessivo dell'esperienza offerta al cliente. Su questi temi e nello stesso solco si devono muovere e integrare i temi di sicurezza e conformità alle normative. ■

BIO

Nicola Sotira è Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Sicurezza e compliance: come coniugarle in uno scenario digitale sempre più dinamico.

Autore: Corradino Corradi

Il tema information security vs compliance da sempre appassiona CRO, CISP e CSO; se ne parla da anni nei convegni e numerosi sono stati i tentavi, sia da parte dei teams di governance aziendale che di gestione del rischio, di conciliare i due aspetti ed evitare la manichea e semplicistica visione che pone la compliance semplicemente come un "alleato" o "nemico" della sicurezza informatica.

Il fatto che continuiamo a dibattere sul tema information security vs compliance, dimostra come la risposta non sia ovvia e può avere declinazioni diverse a seconda della dimensione della società alla quale si riferisce, del suo modello di business, della industria di riferimento e di conseguenza del suo livello di maturità nella gestione della governance del rischio e della sicurezza informatica. Particolarmente significativo è l'impatto

della compliance su progetti ed iniziative di sicurezza informatica in tutti quei settori dove è importate a livello politico e regolatorio il tema del "trust dei clienti" (si pensi al mondo bancario ed assicurativo) o il tema della protezione delle infrastrutture critiche nazionali (utility, telecomunicazioni, etc.) dei settori strategici a livello di *homeland security* (difesa, aerospaziale, etc.).

Vale quindi la pena entrare nel concreto delle normative di compliance; io lo farò basandomi sulla mia esperienza nel campo Telco in un orizzonte temporale di circa 20 anni, con l'obiettivo di dare una panoramica di altissimo livello, rimandando i lettori ad approfondimenti che si possono fare direttamente on line e sui numerosi siti dedicati alla spiegazione di queste normative (con tanto di possibilità di acquistare corsi di formazione e consulenza ad-hoc).

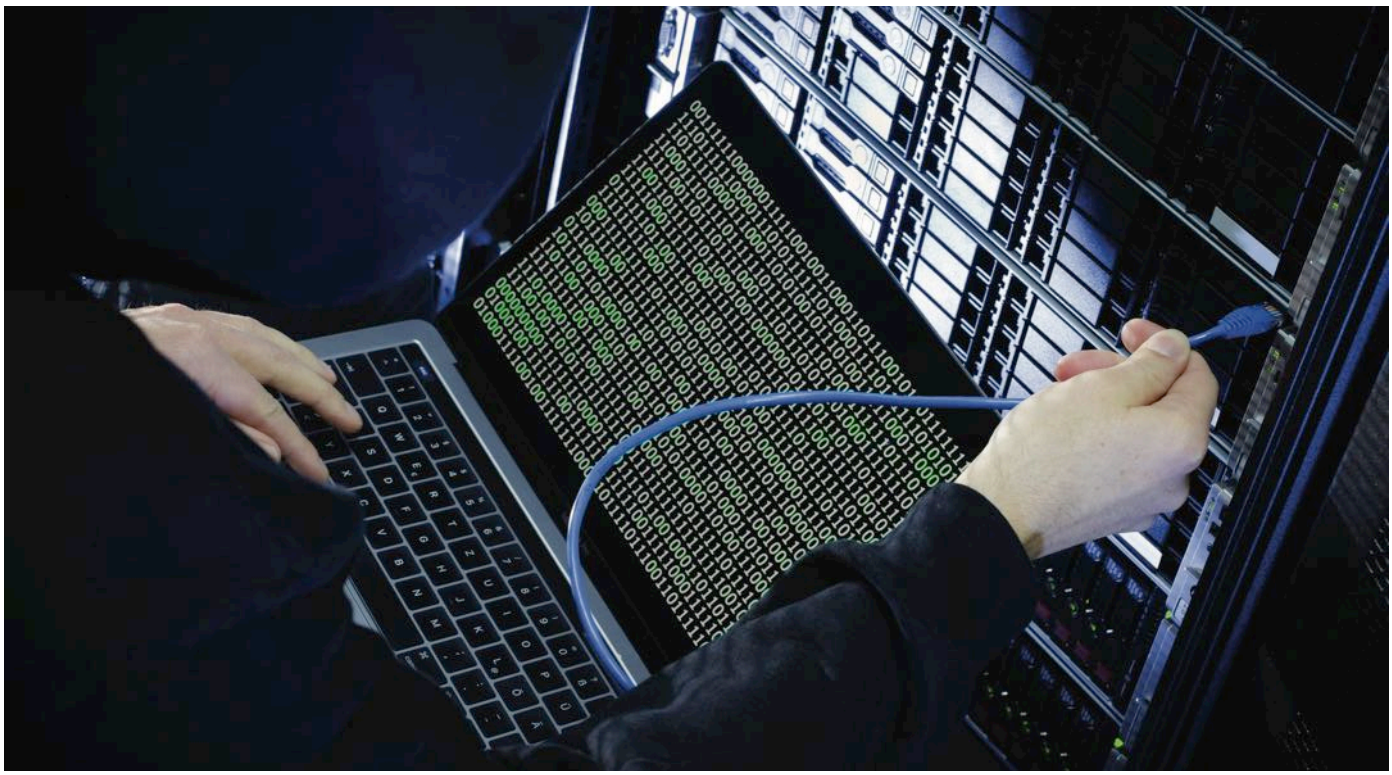
Un primo esempio di normativa con impatto sulla sicurezza informatica è stata la Sarbanes-Oxley Act (SOX), approvata nel 2002 dal Congresso degli Stati Uniti per proteggere azionisti e pubblico generale dagli errori di contabilità e dalle prassi fraudolenti in azienda; con essa sono stati introdotti i controlli di tracciabilità sui sistemi finanziari ma anche una più attenta gestione di ruoli e profili (IUAM) e il rafforzamento dei principi della *"segregation of duties"* e del *"need to know"*.

Sulla scia della normativa americana, l'Italia ha introdotto la legge 231/2001 che, per la prima volta nel nostro ordinamento giuridico, prevede il principio della responsabilità amministrativa delle persone giuridiche per specifiche tipologie di reato commesse da amministratori e dipendenti delle Aziende; la normativa disciplina anche i delitti informatici ed il trattamento illecito dei dati.

Un'altra area di compliance importante per la sicurezza informatica è quella che fa capo alla privacy, con riferimento in particolare alla *"data protection"*. In Italia per anni i responsabili privacy (ed in seguito il Data Protection Officer -DPO) hanno lavorato a fianco del CISO per la gestione delle misure minime di società informatica previste dall'allegato B della legge 196/2003.

Il cambiamento più significativo alla normativa privacy a livello Europeo è arrivato nel 2018 con il GDPR; tra i principi cardine della normava ci sono il *"privacy by design"* e *"privacy by default"*; *"privacy by design"* significa introdurre la gestione dei dati personali come uno step necessario dall'inizio della progettazione di un servizio o prodotto; *"privacy by default"* significa mettere in atto i principi di minimizzazione e limitazione dei tempi di conservazione dei dati *(data retention)*.

Entrambi i principi sottendono la necessita di un approccio "tecnologico" alla gestione e protezione del dati personali (di clienti, dipendenti io terze parti); approccio metodologico e relativo framework aziendale devono essere progettati per sfruttare al massimo le sinergie tra la funzione legale & compliance e la funzione di sicurezza informatica che si occupa prevalentemente della protezione delle applicazioni, della infrastruttura,



delle reti ("data on-fly") e dei database ("data at-rest") che quel dato personale utilizzano (data processing).

Negli utili anni è stata grande la spinta normativa per garantire la *"business resilence"*. Sempre a livello europeo è stata emanata nel 2016 la direttiva NIS (Network and Information Security) che impone agli operatori di servizi essenziali (energia, trasporto, banche etc.), in tutti gli Stati che fanno parte dell'Unione, l'adozione di misure tecniche e organizzative per rendere sicure le proprie reti e i sistemi informatici. Le società coinvolte inoltre sono tenute a comunicare all'autorità competente senza ingiustificato ritardo qualsiasi incidente di sicurezza che abbia un impatto significativo sulla continuità del servizio. I numerosi feedback ricevuti in fase di attuazione della normativa e l'evoluzione del contesto geo-politico hanno spinto la Commissione Europea a presentare una proposta di revisione sostanziale della Direttiva NIS (chiamata NIS 2).

Nel contesto italiano è di fondamentale importanza citare il ruolo della appena nata Agenzia Nazionale di Cybersicurezza (ACN) e le misure di sicurezza da poco emanate con l'obiettivo di proteggere il perimetro di sicurezza cibernetica nazionale.

Infine, per le aziende (soprattutto Business to Consumer) che gestiscono transazioni con Carte di credito, esiste lo standard di riferimento PCI-DSS che copre tutti gli aspetti tecnici ed organizzativi e di processo per la protezione delle carte e delle relative transazioni (sia a livello di *merchant* che di *acquirer* e *service provider*)

A mio avviso, la spinta normativa nel contesto italiano fatto prevalentemente da piccole e medie società è stato un volano per la sicurezza informatica ed uno stimolo per i responsabili legali e della compliance di tali realtà ad investire nella sicurezza informatica o semplicemente a definire il ruolo del CISO e del DPO.

Per grandi società con modelli di governance evoluti ed in grado di effettuare attività di enterprise risk management e/o con strutture di sicurezza complete (dal demand management di sicurezza, alla information security governance risk & compliance, dalla cyber-prevent alla cyber-defence) la normativa è stata un sicuro supporto tutte le volte che è stata *"principle driven"* evitando di entrate troppo nel dettaglio dei controlli o di fissate delle scadenze di compliance troppo ravvicinate (sotto i 24/36 mesi).

BIO

Corradino ha iniziato la sua carriera nell'ambito dell'Information Technology lavorando prima in Telecom Italia e poi in Ericsson Telecomunicazioni. Dopo aver partecipato ad alcune startup sia nella telefonia mobile che nel settore delle banche on line, è stato Data Protection Officer (DPO) e responsabile della funzione "ICT Security, Privacy and Fraud management" di Vodafone Italia dal 2002 al 2022. Da Giugno 2022 Corradino è il General Manager per information security Strategy, Architecture e Technical Excellence di MTN Group in Sud Africa. Oltre ad essere certificato CISM, CFE e CBCP, Corradino ha conseguito una laurea in ingegneria elettronica presso l'Università dell'Aquila ed un MBA presso la Warwick University. Corradino è membro dell'Advisory Board di alcuni osservatori italiani di cyber-security e privacy; dal 2018 al giugno 2022 è stato membro del direttivo di AIPSA.

Tutte le volte che le normative di sicurezza si sono spinte nel merito della definizione del livello di *"risk acceptance"* di specifiche industries o peggio ancora nella definizione di dettaglio dei controlli di sicurezza tecnici il rischio è stato multiplo: aggravio di burocrazia, perdita di vista della visione risk-based per passare a quella delle *"check the box"*, poca rilevanza con il passare del tempo di alcuni controlli tecnici.

Per concludere ben vengano le normative di compliance, perché spesso rappresentano un acceleratore per la sicurezza informatica e permettono ai CISO e DPO di porre il tema all'attenzione dei vertici dell'azienda; ma è importante sempre lavorare affinché Legislatori e Regolatori, sia a livello italiano che europeo, abbiamo un approccio *"principle driven"* non *"technology driven"*, con il rischio di definire ed imporre controlli tecnici che diventano immediatamente obsoleti con la sempre più rapida evoluzione tecnologia (vedi 5G e mobile, IOT, Cloud). ■

Compliance: una sfida per le organizzazioni.

Autore: Jelena Zelenovic Matone

Thomas Hobbes, un filosofo inglese, sostenne, e giustamente, che la conservazione della pace dipende dalla scienza... o dalla conoscenza. La celebrazione dei primi giorni di Internet ha lasciato ben presto il posto al timore e alle ambizioni distruttive di ottenere un vantaggio sugli altri corrompendo la rete. Non ci volle molto perché gli esseri umani adottassero il comportamento delle accuse e delle critiche. Quindi, siamo tutti d'accordo sul fatto che l'uso di Internet è uno dei fattori più critici per lo sviluppo economico globale e la sicurezza internazionale. Potremmo quindi facilmente affermare che ciò richiede un accordo unanime sulla necessità di una maggiore cooperazione internazionale per aumentare la stabilità e la sicurezza nel cyberspazio. Tuttavia, anche se questo non è ancora completamente in atto e stiamo ancora lavorando su questo, potremmo tornare ai nostri libri di testo e alle best pratice e condividere il modo in cui affrontiamo le varie minacce da professionisti nei tempi più emozionanti in cui viviamo.

BIO

Rispettata leader CISO, insignita del CISO dell'anno per il 2019 in Lussemburgo, Sentinel CISO Global 2020, EU CISO 2020 e Ambasciatore dell'anno 2021 in Lussemburgo, Jelena è esperta di Cybersecurity versatile e innovativa con enfasi sulla gestione del rischio di sicurezza informatica/ risk management, creazione di policy e procedure, sicurezza IT/ IS, operazioni IT, audit, mitigazione del rischio, miglioramento dei processi aziendali, governance IT, business process improvement, IT governance. Appassionata di partecipazione e incoraggiamento delle donne alla cybersecurity e ai programmi STEM. Prima del ruolo attuale, ha ricoperto il ruolo di Senior Operational Risk e ISO manager per un'altra istituzione dell'UE. All'inizio della carriera, ha gestito IT Audit and Compliance per Sobey's, uno dei due rivenditori nazionali di generi alimentari in Canada e Audit, Corporate Development, M&A e strategie di crescita e IT Audit per George Weston, una delle più grandi società di trasformazione e distribuzione degli alimenti in Canada quotata in borsa.

CONTROLLI IT: Le impostazioni di base.

I controlli informatici generali IT sono in uso da molto tempo. La mia carriera è iniziata con questi controlli di base, che sono ancora utilizzati e continuano a maturare. Questi controlli sono molto importanti e rappresentano un ottimo punto di partenza per ogni organizzazione per valutare la **cyber hygiene**.

È necessario iniziare con i controlli per comprendere e formulare i punti di vista di base sulla sicurezza di un'organizzazione. Non esiste

una soluzione o una soluzione una tantum per tentare di implementare tool costosi senza prima controllare e comprendere l'assetto tecnico dell'organizzazione.

Esaminare il panorama attuale e vedere dove sono i problemi. Se avete terze parti con cui lavorate, verificate la presenza di tali controlli; se non esistono, non esitate a presentarli voi stessi. Se non avete mai fatto nulla di simile, iniziate dalle revisioni trimestrali.

Inoltre, se l'azienda con cui state stipulando un contratto è già abbastanza grande, è probabile che saranno in grado di fornirti più materiale. Tali esempi sono la certificazione ISO, il reporting SOC 1, SOC 2 e molti altri rapporti relativi all'audit su cui potrete fare affidamento. La chiave è avere una ragionevole certezza che i controlli e la sicurezza delle informazioni della vostra organizzazione siano presi in considerazione, in una certa misura, quindi una sicurezza «ragionevole».

La prima cosa è identificare i controlli critici ponendosi alcune domande fondamentali:

1. Se il controllo fallisse, avrebbe un impatto sull'informativa finanziaria?
2. Controllo preventivo che non presenta il controllo investigativo?
3. Controllo investigativo che non presenta controllo preventivo?

I metodi di prova da considerare per tale esercizio sarebbero indagini sugli owner di processo e di controllo o sui membri chiave del team di gestione, un'ispezione della relativa documentazione di controllo, la re-performance dell'operazione di controllo utilizzando transazioni selezionate e l'osservazione del processo o della procedura di controllo in azione.

L'esecuzione di una combinazione di due o più dei quattro metodi può essere necessaria per testare ciascun controllo e i mezzi più efficaci per testare l'efficacia operativa. L'evidenza a supporto della conclusione del management in merito all'efficacia operativa è più affidabile se derivata da una combinazione dei metodi di prova.

Esaminiamo ora i requisiti iniziali. Facciamo riferimento a COBiT, per esempio. Per tale esercizio, soprattutto se non è mai stato fatto prima, consiglio COBiT light e i suoi tre pilastri: change management, operations management e ensuring system security.

Questo implica mettere in dubbio ogni controllo, porre le domande giuste internamente e contattare i fornitori per comprendere la loro posizione di sicurezza in base all'applicabilità.

Iniziare con le policies, i metodi di autenticazione, la gestione degli accessi, la sicurezza della rete, i log di monitoraggio e le domande giuste da porre:

- Guardare le policy esistenti.
- Cercare tutte le possibili policy che si adattino ai controlli attuali. Tali criteri potrebbero essere criteri di sicurezza della rete, sicurezza fisica, sicurezza del sistema operativo, criteri di sicurezza delle applicazioni, criteri di sicurezza del database, criteri di sicurezza del cloud e criteri di accesso degli utenti.
- Verificare l'esistenza della password e le regole della password. Assicurarsi che tali requisiti per la password corrispondano ai requisiti della policy dell'organizzazione.
- Verificare periodicamente la presenza di regole per la modifica della password dal sistema e assicurarsi che tali requisiti corrispondano a quelli della policy esistente.
- Rivedere e garantire la validità degli accessi privilegiati.

Network Security Governance

Per comprendere la network security governance, confermare l'esistenza di criteri e principi di sicurezza di rete per l'accesso e la sicurezza alla rete, consiglierei di prendere un campione di server e workstation da una sezione trasversale di business unit e dipartimenti e verificare se esistono programmi di protezione da software dannoso installati e abilitati sui dispositivi in rete. Se è presente, controllare il nome e la versione dei programmi. Controllare anche se sono presenti programmi configurati per filtrare il traffico in entrata, come e-mail e download, per proteggere da informazioni non richieste (ad es. spyware, e-mail di phishing). Dato l'aumento delle e-mail di phishing, soprattutto durante l'era del COVID, garantire che tali controlli vengano eseguiti è della massima importanza.

Quando si tratta di patch, consiglio di controllare se le patch di sicurezza vengono applicate automaticamente e regolarmente ai programmi o quando diventano disponibili. Se vengono applicate tali patch, verificare che non possano essere manomesse, il che significa che utenti non autorizzati non possono disabilitare tali programmi e che le patch siano centralizzate tramite un server specializzato.

Questo mi porta ad un altro punto importante: verificare che l'accesso a un server sia limitato agli utenti IT autorizzati, così come la sua gestione della configurazione sia riservata agli utenti IT autorizzati. Potreste chiedervi quali prove o esistenza di controlli cercare qui, e vi consiglio di cercare il registro degli accessi al data center e di controllare la revisione trimestrale degli utenti autorizzati. Applicherei gli stessi principi anche ai visitatori.

Per comprendere la postura delle organizzazioni potremmo considerare molti altri controlli del COBIT, pertanto consiglio ai lettori un approfondimento di tale framework.

Cloud: il vecchio, buono e spaventoso cloud

Le valutazioni del rischio cloud sono diventate più importanti negli ultimi dieci anni, poiché dipendiamo quotidianamente dal cloud. Dagli smartphone che usate ai dispositivi intelligenti in casa, dipendiamo dal cloud più che mai. Riuscite a immaginarvi senza cloud al giorno d'oggi?

Tuttavia, come proteggersi sul lavoro quando si sceglie una soluzione cloud. Ci sono diversi modi per affrontare questo argomento. Dipende principalmente dalle informazioni condivise con il provider di terze parti. Cosa condividerete con il provider è la prima domanda che dovresti porre. La condivisione di informazioni strettamente riservate dipenderà dalle normative e dalle policy di un'organizzazione. La condivisione delle informazioni personali dello staff va un gradino sopra e le normative dei paesi differiscono in modo significativo, come i requisiti GDPR dei paesi dell'UE.

L'aspetto più cruciale di tali valutazioni del rischio è coinvolgere il DPO (Data Protection Officer), il vostro team legale e il team CISO e Information Security.

La valutazione iniziale dovrebbe porre domande come:

- A cosa servirà la terza parte
  - L'azienda è responsabile di fornire il business case e di rispondere in dettaglio a tutte le domande
- Che tipo di informazioni avremmo sul cloud
  - In questo caso sarebbe necessario disporre già di una buona policy di classificazione delle informazioni per comprendere la riservatezza dei documenti che verranno inseriti nel cloud.

Information security policy

Se esistono policy di sicurezza applicabili ai servizi forniti? Se è così, allora vanno lette e comprese. Anche i service provider le dovrebbero rispettare.

E' necessario garantire e verificare l'esistenza di varie policy di sicurezza e procedure operative, ad esempio la policy per la gestione dei firewall dovrebbe essere:

- Documentata,
- In uso, e
- Nota a tutte le parti.

Organizzazione dell'information security

Queste sono alcune importanti domande quando si esaminano le terze parti. Porre domande come:

- Qual è la tua organizzazione in materia di sicurezza (ad es. avete un responsabile della sicurezza, a cui riferire/fare escalation)?
- Sicurezza delle risorse umane
- Quali sono i controlli in background effettuati sul personale con potenziale accesso ai dati dell'organizzazione?
- I dipendenti sono formati per non scegliere password fatte sulla base di dati personali che potrebbero essere pubblicamente accessibili?
- La policy di sicurezza viene rivista e approvata per completezza, integrità e accuratezza ogni anno?

Sicurezza fisica

La sicurezza fisica è sicuramente una parte importante della sicurezza delle informazioni. Qui potremmo porre le seguenti domande, al fine di comprendere la postura di sicurezza fisica:

- Quanto e quale personale ha un potenziale accesso ai dati dell'organizzazione?
- Come viene limitato l'accesso alle aree sensbili o contenenti i dati dell'organizzazione?
- L'accesso a questi locali è monitorato 24 ore su 24, 7 giorni su 7? L'accesso è dato e deciso?

- L'accesso alle porte di rete inutilizzate è disabilitato o sono presenti barriere fisiche per prevenire accessi non autorizzati? Criteri per questo?

- Con quale frequenza viene verificato l'integrità e l'accuratezza dell'accesso?

- Come e chi informa dell'accesso ai dati dell'organizzazione da parte di nuovi dipendenti o di quelli che hanno lasciato l'azienda? I visitatori di queste strutture sono sempre registrati e accompagnati?

- Le nostre procedure di risposta alle emergenze sono documentate e accessibili?

- Le apparecchiature IT business-critical sono supportate da UPS e periodicamente testate?

- Procedure per la distruzione sicura delle stampe cartacee? Dati dell'organizzazione sensibili protetti dalla stampa se non vi è alcuna necessità operativa per la stampa di tali documenti?

- Se l'attrezzatura deve essere rimossa dai locali aziendali, esiste una procedura efficiente per tracciare il movimento di tale attrezzatura?

Operations security

Nel campo dell'operations security si potrebbero considerare domande come:

- In che modo i dati dell'organizzazione vengono separati dai dati degli altri clienti (infrastruttura e backup)?

- Quali controlli per la prevenzione del data leakage sono in atto (ad es. presso i gateway e gli endpoint)? Quale livello di monitoraggio protettivo

(ad es. security accounting e audit) viene eseguito sui servizi dell'organizzazione?

- Utilizzate una qualsiasi forma di tecnologia di security event information management (SEIM), un Intrusion Detection System (IDS) o un Intrusion Prevention System (IPS)? Se sì, quali e come sono configurati?

- Quali sono i controlli a disposizione per impedire l'accesso non autorizzato/la manomissione dei log?

- Qual è il periodo di conservazione dei log? (assicuratevi di rispettare le normative governative, se applicabili)

- Quali controlli di protezione dal malware sono in atto sugli endpoint (ad es. desktop/laptop), e-mail e gateway Web?

- Con quale frequenza vengono aggiornate le firme antivirus?

- Qual è l'approccio alla gestione delle vulnerabilità, ad esempio, come monitori le potenziali vulnerabilità?

- Con quale frequenza eseguire la scansione delle vulnerabilità sulla rete e sulle applicazioni?

- Qual è il vostro processo di correzione della vulnerabilità?

- Come viene contattata l'organizzazione se è necessario un cambiamento urgente?

- Quali parametri di sicurezza e informazioni di gestione vengono forniti all'organizzazione come parte dei servizi?

Acquisizione, sviluppo e manutenzione del sistema

L'acquisizione, lo sviluppo e la manutenzione del sistema svolgono un importante ruolo nel garantire la cyber security posture nelle vostre organizzazioni.

Porre domande come queste:

- Seguite un processo formale di risk assessment per determinare i requisiti di sicurezza dei vostri servizi? In tal caso, dovete fornire i dettagli della metodologia.

- Seguire OWASP (www.owasp.org) o linee guida equivalenti per lo sviluppo di applicazioni sicure?

- Qual è il vostro processo di test e accettazione per i vostri servizi, comprese eventuali nuove applicazioni?

- Quale livello di test di sicurezza viene eseguito come parte di questo?

- Come vi assicurate che tutti i dati dell'organizzazione siano stati cancellati dalla vostra infrastruttura alla fine del ciclo di vita/fine del servizio?

Sicurezza della rete

In qualità professionisti, un altro ruolo fondamentale che si gioca come CISO è comprendere la sicurezza della rete di terze parti. Ricordare che siamo protetti solo quanto è protetto il nostro anello più debole con cui abbiamo a che fare. Domande quali:

- La rete stessa è protetta da procedure di autenticazione oltre alla protezione dei sistemi sulla rete?

- Sono state adottate misure per impedire che sistemi non autorizzati possano essere facilmente collegati alla rete?
- Il traffico di rete viene regolarmente monitorato per stabilire schemi di utilizzo normali?
- Viene eseguito periodicamente un analizzatore wireless per individuare eventuali dispositivi wireless non autorizzati che potrebbero essere stati collegati alla rete?
- Esiste un processo automatico per mettere in quarantena i sistemi che potrebbero essere stati contaminati da informazioni false senza spegnerli?
- Sulla rete vengono utilizzati sistemi di rilevamento e/o prevenzione delle intrusioni?
- Le firme vengono regolarmente aggiornate su entrambi?
- L'azienda utilizza il sistema di content filtering per controllare with "hostile active x, javascript, e java applets?

▸ Pensare ai noti attacchi DDoS attuali. I passaggi cruciali per garantire la remediation e vedere cosa stanno facendo anche le terze parti consistono nel verificare le loro capacità merito a:

- Rafforzamento della larghezza di banda
- Segmentazione sicura di reti e data center
- Implementazione mirroring e failover
- Applicazioni e protocolli configurati per la resilienza
- Rafforzamento della disponibilità e delle performance attraverso risorse come le content delivery networks (CDN) (CDNS)

Sicurezza delle comunicazioni

Occupiamoci di noi stessi con domande come:

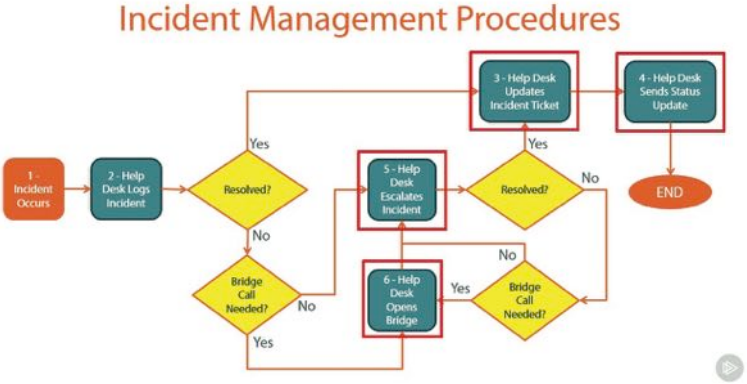
- Come viene garantita la sicurezza nella trasmissione dei dati?
- Come viene fornito l'accesso remoto al personale amministrativo/di supporto?
- Quali misure di disponibilità utilizzate per proteggerti da minacce ed errori?
- Utilizzi più ISP? Hai la protezione DDoS e, in caso affermativo, come?

Rapporti con i fornitori

Vi accertate di capire in che modo terze parti (i vostri sub-fornitori) possono accedere ai dati dell'organizzazione e come? Verificate i requisiti imposti ai vostri sub-fornitori per informarvi di un incidente di sicurezza informatica?

Information security incident management

Il vostro contratto con terze parti è la tua Bibbia. Ma per avere un contratto valido è necessario porre le domande giuste e definire i requisiti



dopo aver compreso le operazioni e i requisiti della propria organizzazione. Le domande sarebbero:

- Qual è la vostra procedura per gestire un incidente di sicurezza informatica?
- In quali condizioni l'organizzazione sarà informata di un incidente e la notifica all'organizzazione avverrà entro un determinato periodo?
- Come conterreste ed eliminereste un'infezione malware sui vostri sistemi/servizi e quale sarebbe l'impatto sui vostri clienti?
- Quale priorità verrà data al ripristino dei servizi dell'organizzazione in caso di incidente (ad esempio, se sono interessati più clienti, quale posto ha un'organizzazione nell'ordine di ripristino)?
- Quale supporto potete fornire per le indagini sugli incidenti forensi (ad es. da parte di un rappresentante dell'organizzazione)?
- In quali condizioni fornireste l'accesso ai vostri audit log?

Compliance

Molte delle domande che vorresti fare potrebbero già esistere negli audit indipendenti di terze parti. Quindi chiedete se hanno già tali audit in atto. Domande, come ad esempio:

- Le vostre operazioni sono soggette a processi formali di compliance?
  - Se sì, quali (ad es. SAS70, ISO27001)?
- A quali condizioni le terze parti, comprese le agenzie governative nazionali, possono accedere ai dati dell'organizzazione?
- Potrebbe informare l'organizzazione di tale accesso?
- Quali azioni di ricorso (ad es. compensazione finanziaria, risoluzione anticipata dei contratti, ecc.) sono disponibili in caso di incidente informatico?
- Come eseguite il miglioramento continuo dei processi e dei controlli di sicurezza?

Ulteriori informazioni

Chiedete ai fornitori di mostrarvi qualsiasi altra informazione che ritenete possa essere utile all'organizzazione per comprendere gli approcci e controlli per la prevenzione, il rilevamento e la risposta agli incidenti informatici nei servizi che forniscono.

EBA ICT Guidelines

EBA ICT Risk Guidelines	DNB Information Security Framework	DNB Cloud Computing Risk Assessment	BCBS239	EBA Cloud Outsourcing	GDPR	ECB Guidelines on Outsourcing	Payment Service Directive 2 (PSD2) Guidelines on Security and Operational risk
ICT Governance and Strategy							
ICT Risk Exposures and Controls	X	X	X	X	X	X	X
a. ICT availability and continuity risks	X	X	X	X	X	X	X
b. ICT security risks	X[1]	X	X	X	X	X	X
c. ICT change risks	X[2]	X	X	X	X	X	X
d. ICT data integrity risks							
e. ICT outsourcing risks	X	X	X	X	X	X	X

1. Regular and proactive threat assessments not sufficiently covered.

2. Security and vulnerability screening of changes and source code control not sufficiently covered.

Le linee guida dell'EBA stabiliscono requisiti per gli enti creditizi, le imprese di investimento e i service providers di pagamento sulla mitigazione e la gestione dei loro rischi legati alle tecnologie dell'informazione e della comunicazione (ICT) e mirano a garantire un approccio coerente e solido in tutto il mercato unico.

Sappiamo tutti che la complessità delle tecnologie dell'informazione e della comunicazione (ICT) e i rischi per la sicurezza sono in aumento e la frequenza degli incidenti relativi alle ICT e alla sicurezza (compresi gli incidenti informatici), insieme al loro potenziale impatto negativo significativo sul funzionamento operativo delle istituzioni finanziarie. A causa dell'interconnessione delle istituzioni finanziarie, gli incidenti legati alle ICT e alla sicurezza che rischiano di causare potenziali impatti sistemici sono casi molto frequenti.

Pertanto, le linee guida dell'EBA hanno risposto a questo problema descrivendo in dettaglio come le autorità di vigilanza dovrebbero coprire le ICT e i rischi per la sicurezza nell'ambito della vigilanza, specificando come le istituzioni finanziarie dovrebbero gestire l'esternalizzazione e descrivendo le aspettative per le ICT e la gestione dei rischi per la sicurezza per le istituzioni finanziarie.

Queste linee guida stabiliscono come gli istituti finanziari dovrebbero gestire le ICT e i rischi per la sicurezza a cui sono esposti. Inoltre, tali linee guida cercano di fornire agli istituti finanziari, a cui le linee guida si applicano, una migliore comprensione delle aspettative di vigilanza per la gestione dei rischi ICT e per la sicurezza. Iniziate esaminando le valutazioni di applicabilità a tali linee guida e le tue esigenze normative e di conformità organizzative.

Formazione e awareness

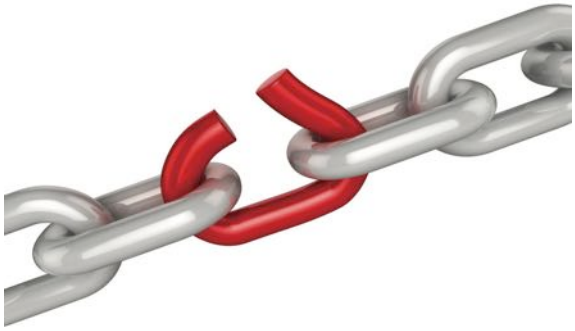
In questa sezione vorrei trattare il fattore di compliance più critico.

Se vogliamo essere protetti al 100%, dobbiamo disconnetterci - completamente! Ora, dubito che questo sarebbe possibile per chiunque. Immaginati senza Internet, notizie, programmi preferiti che guardate o senza parlare con familiari e amici in tutto il mondo.

Poiché le minacce informatiche e gli attacchi continuano ad aumentare e a diversificarsi in natura, i CISO sono sempre più impegnati proteggere le risorse di informazioni critiche nell'organizzazione. Inoltre, il loro compito è quello di proteggere i beni più preziosi delle loro organizzazioni. I CISO devono garantire che ogni dipendente riceva una awareness completa sui vari protocolli di sicurezza da seguire. Oltre alle varie strategie di sicurezza implementate, è anche responsabilità del CISO condurre regolarmente programmi di Security Awareness.

"Gli esseri umani sono l'anello più debole e i CISO devono ricordare che siamo tutti forti quanto il nostro anello più debole."

Ricordiamoci che gli attacchi social engineering sono un mix di competenze tecniche ma anche debolezze umane. Questa è la priorità numero uno per i CISO in



quanto offre ai cybercriminali e agli hacker una facile possibilità di accedere alla rete di informazioni. Pertanto, i CISO devono educare i dipendenti su:

- Come riconoscere una potenziale e-mail di phishing
- Come controllare e confermare i link prima di fare clic
- Come verificare se un allegato è sicuro
- Come verificare se l'e-mail proviene da una fonte attendibile
- Come utilizzare le barre degli strumenti anti-phishing
- Perché è fondamentale cambiare e diversificare regolarmente le password dei propri account di social media e di altri account online
- Perché è essenziale non utilizzare la posta elettronica di lavoro per gli account personali
- Utilizzo dei social media per la comunicazione aziendale
- Quali policy esistono all'interno di un'organizzazione e cosa richiedono esattamente

Educare il personale e creare awareness

Tutti i dipendenti, compresi gli esterni che lavorano per l'organizzazione, sono la prima linea di difesa. Proteggono la fortezza per cui lavorano.

Prendiamo l'esempio del Covid-19, dove inizialmente avremmo potuto affrontare meglio i rischi operativi. Pensiamo all'impatto psicologico sulle persone confinate in casa, che dipendono da Internet per qualsiasi interazione sociale, per lavorare in smart working e ai bambini, esposti a un maggiore rischio di dipendenza da Internet diventando facile preda per gli attacchi di tipo phishing e dei siti Web compromessi.

Nonostante avvisi e i le avvertenze tramite comunicazioni e-mail, circolari e programmi di formazione, è ancora possibile vedere persone che utilizzano password deboli o la stessa password per tutti gli account. Pertanto, i CISO devono includere regole per la creazione di password sicure nei loro programmi di awareness security. Di conseguenza, i dipendenti devono essere formati sulle best practice e sulle adeguate misure da adottare quando si tratta di gestire e-mail e scaricare allegati.

Si stima che l'80% - 90% degli attacchi di phishing avvenga tramite allegati e-mail e URL dannosi. Pertanto, un semplice clic su un URL dannoso è sufficiente per attivare un attacco di phishing indipendentemente dai sofisticati protocolli di sicurezza o software.

Barracuda Networks, leader mondiale nel networking, sicurezza, e-mail e protezione dei dati, ha condotto un'interessante indagine. I risultati del sondaggio mostrano che quasi il 7% delle persone ha risposto di non aver mai ricevuto alcuna formazione sulla sicurezza e il 29% ha risposto che la formazione veniva condotta solo una volta all'anno.

Corsi annuali di aggiornamento

Oltre la security awareness fornita a tutti i dipendenti dell'organizzazione, consiglierei di far seguire corsi di aggiornamento annuali alle persone sul lato dell'implementazione, agli amministratori e ai proprietari di aziende (soprattutto di applicazioni critiche).

Questi corsi aiuteranno principalmente ad aggiornare le conoscenze sulle policy e le procedure di sicurezza delle informazioni che devono essere seguite. Uno degli aspetti critici di questi corsi di aggiornamento annuali è che devono essere progettati tenendo conto delle attuali policy e procedure di sicurezza. I CISO devono garantire che questi corsi siano aggiornati alle policy più recenti, per timore che ciò possa causare confusione e problemi significativi.

Inoltre, dovrebbero essere sviluppati corsi su misura per i compiti più critici dell'organizzazione, dove ad esempio la rilevanza dell'organizzazione è la più alta. L'adattamento di simulazioni di phishing e la formazione di

questi dipendenti in seguito alla simulazione apporta un valore eccellente a tali organizzazioni.

Quindi è chiaro che in questa era digitale dinamica e in continua evoluzione, il valore e l'importanza di educare il personale, condurre revisioni di esperti e documentazione sistematica non possono essere più enfatizzati.

Revisioni trimestrali della sicurezza tecnica

Per completare l'articolo e le raccomandazioni, vorrei ricordare ai lettori le pratiche di assessment della sicurezza. La prassi dovrebbe essere eseguita almeno su base annuale e può aiutare principalmente a identificare le vulnerabilità nel sistema. È inoltre fondamentale condurre revisioni trimestrali della sicurezza per valutare lo scenario di sicurezza attuale. Se queste revisioni venissero eseguite in modo efficace, aiuterebbe a identificare i rischi residui. Il rischio residuo indica il numero massimo di attacchi informatici che si possono aggirare e superare. Se il numero rientra nei livelli accettabili, non è necessario premere il tasto d'emergenza. Altrimenti, è il momento di intraprendere un'azione seria per collegare tutte le vulnerabilità nel sistema.

Le organizzazioni non possono fare affidamento solo sui rapporti annuali di risk assessment in questo mondo iperconnesso. Alcune aziende arrivano addirittura al punto di condurre revisioni indipendenti da due diversi fornitori per garantire la sicurezza delle proprie risorse di informazioni digitali.

Ogni componente software e hardware dell'organizzazione necessita di manutenzione a intervalli regolari per mantenerlo aggiornato e proteggerlo dalle violazioni della sicurezza da parte degli hacker. Include tutti i server, desktop, router, software, ecc., e occorre prestare attenzione per applicare regolarmente tutte le patch più recenti e mantenerle aggiornate. Una revisione trimestrale della sicurezza aiuterà a identificare queste anomalie e a proteggere la vostra organizzazione, impedendo agli hacker di accedere alla vostra rete.

Conclusioni

Man mano che più dispositivi sono connessi all'Internet of Things, la società dovrà affrontare più sfide cyber. Noi, come professionisti, dovremmo cooperare tra le nostre comunità fidate e assistere nelle sfide che inevitabilmente ci stanno arrivando, o sono già arrivate, per per intervenire. Un ottimo inizio per tale condivisione sono gli articoli che scriviamo e i gruppi di pari che creiamo tra i nostri ambienti di fiducia. ■

Gestire Sicurezza e Compliance per Creare una Perfetta Alleanza nel nuovo dominio digitale.

Autore: Lisa Ventura

Sicurezza e compliance sono due concetti che spesso vanno di pari passo, ma contrariamente a quello che comunemente si pensa, non sono intercambiabili. È essenziale che i team interni al di fuori dei team di sicurezza, inclusi quelli di vendita, ingegneria, marketing e in particolare la C-suite, comprendano le loro nette differenze quando si tratta di proteggere le organizzazioni. Entrambi dovrebbero lavorare insieme armoniosamente e quando si tratta di obiettivi di compliance e sicurezza, spesso si riduce a un solo obiettivo: il rischio.

La gestione del rischio è la ragione per cui esistono sia la sicurezza che la compliance. Questo obiettivo condiviso dovrebbe ispirare uno sforzo congiunto per raggiungere questo scopo. Sia la sicurezza che la compliance progettano, stabiliscono e applicano controlli alle organizzazioni di progetto e avendo così tanto in comune sembra che dovrebbero essere alleati naturali.

Sicurezza vs Compliance

Esistono alcune differenze fondamentali tra sicurezza e compliance. I responsabili della sicurezza seguiranno le best practices del settore per proteggere i sistemi IT, in particolare a livello aziendale o organizzativo e saranno alla costante ricerca di come impedire agli aggressori di danneggiare l'infrastruttura IT dell'azienda e i dati aziendali e mitigare la quantità di danni che si potrebbe verificare in caso un attacco abbia successo.

Grazie all'aumento del know-how tecnico e della specializzazione, la sicurezza non si limita a una singola disciplina o campo. Invece, ci sono una miriade di aree su cui concentrarsi, come la gestione dell'infrastruttura e dell'architettura, la cyber security, i test e la sicurezza delle informazioni, che è probabilmente la politica più critica per qualsiasi organizzazione.

La compliance IT è il processo per soddisfare i requisiti di una terza parte, con l'obiettivo esplicito di consentire operazioni commerciali in

un particolare mercato e garantire che avvenga l'allineamento con le leggi, o addirittura l'allineamento con un particolare cliente. A volte si sovrappone alla sicurezza, ma i fattori alla base della conformità sono diversi. La conformità è spesso incentrata sui requisiti di una terza parte, come le politiche governative, i quadri di sicurezza, le normative del settore e il cliente/condizioni contrattuali del cliente. Ad esempio, nel Regno Unito molte organizzazioni insisteranno sul fatto che i loro fornitori siano certificati Cyber Essentials e Cyber Essentials Plus o siano in possesso di certificazioni ISO9001 e ISO27001.

Se diciamo che la sicurezza IT è una carota che esiste per motivare l'azienda a proteggersi dagli attacchi informatici, allora la compliance IT è il bastone. Il mancato rispetto delle normative di compliance può avere gravi conseguenze per le organizzazioni, ad esempio, perdita di fiducia dei clienti e danni all'organizzazione e implicazioni finanziarie e legali che potrebbero comportare il pagamento di sanzioni elevate o l'interruzione del lavoro in determinati mercati e aree geografiche. La compliance è spesso una delle principali preoccupazioni aziendali nei paesi in cui esistono leggi sulla privacy dei dati come il California Consumer Privacy Act negli Stati Uniti e il GDPR nel Regno Unito e in Europa e nei settori che hanno normative stringenti come la sanità e la finanza. Queste aree spesso richiedono sempre un livello di compliance molto più elevato.

In che modo Sicurezza e Compliance vanno di pari passo nel Mondo Digitale?

La natura dei moderni canali di sicurezza cloud spesso traduce la sicurezza e la compliance come questioni inestricabilmente collegate. Il fatto che i team di sicurezza e quelli di compliance lavorino insieme rende il business forte perché collaborare in questo modo dà visibilità e copertura reali, crea efficienze sui costi, consolida i toolsets e guida il cambiamento di trasformazione che alimenta la crescita aziendale. Avere un approccio adeguatamente unificato è più critico che mai in un momento che vede livelli di lavoro da remoto senza precedenti.

I rischi sono tutti molto reali e le minacce in gioco minacciano sia la compliance che la sicurezza che si scambiano e si manifestano insieme. Avere un'efficace strategia di sicurezza e compliance che agiscono insieme può aiutare a consentire alle organizzazioni di implementare alcuni principi importanti:

BIO

Lisa Ventura è una pluripremiata consulente, scrittrice e relatrice per la cyber security awareness. È la fondatrice di Cyber Security Unity, un'organizzazione di comunità globale che si dedica a riunire individui e aziende che lavorano attivamente nella cyber security per aiutare a combattere la crescente minaccia informatica. Lisa è anche una mental health coach ed è la fondatrice di #AllTogetherNow che offre aiuto e supporto a coloro che sono colpiti da bullismo e abusi nella cyber security e Infosec. Si dedica con passione ad aumentare la consapevolezza della crescente minaccia informatica per prevenire attacchi informatici e frodi informatiche e supporta attivamente le donne e coloro che sono neurodiversi nelle carriere nella cyber security. I suoi libri "The Rise of the Cyber Women: Volume 1 and Volume 2" sono stati pubblicati nel 2020 e nel 2021 con grande successo. Lisa fa parte dell'Advisory Group del West Midlands Cyber Resilience Center, fa parte del consiglio di Think Digital Partners in qualità di Cyber Security Advisor ed è membro dell'Advisory Council for the International Security Expo. Nel 2021 è stata nominata una delle "Most Inspiring Women in Cyber Security" di IT Security Guru e ha vinto il premio "Positive Role Model for Gender" ai National Diversity Awards di ITV News nel 2020. Ha anche vinto numerosi altri premi per il suo lavoro, tra cui Premio "Outstanding Contribution to Cyber Security" di SC Magazine. Maggiori informazioni su Lisa possono essere trovate su www.lisaventura.co.uk.

▸ Garantire che i toolsets non siano in silos

Alcune organizzazioni, ad esempio, si sono procurate clienti Slack separati per i reparti HR, compliance, sicurezza e legale. Questo tipo di lavoro in silos non è consigliato, gli strumenti devono estendersi all'intera organizzazione in modo che i team possano affrontare insieme le minacce e condividere la visibilità.

▸ Stabilire ruoli e responsabilità specifici

Anche se le organizzazioni dispongono di una suite di compliance e sicurezza all'avanguardia, la comunicazione è fondamentale. Gli stakeholders e gli imprenditori devono comunicare come sta cambiando

il loro approccio allo stack tecnologico. Ad esempio, se l'ufficio vendite si trova a fare più affidamento sui mezzi di comunicazione come WhatsApp, sia la sicurezza che la compliance devono essere informati. Se viene acquistato Microsoft Teams, devono saperlo entrambi. È l'unico modo in cui un'efficace cyber security policy e una compliance policy possono essere in sintonia. Tutto il personale deve avere una visione completa di come i vari canali vengono utilizzati dall'intera organizzazione.

I dati devono essere consultabili e completi

Con le organizzazioni che devono affrontare un'enorme quantità di dati che vengono raccolti nel tempo, i team di sicurezza e compliance avranno esigenze diverse. La conformità richiederà una registrazione completa e ininterrotta degli eventi, mentre la sicurezza richiede solo un rapido accesso a determinati eventi dal vivo. Le organizzazioni hanno bisogno di una piattaforma che implementi la conservazione dei registri completa e comprensiva. Hanno anche bisogno di piattaforme per avere piena visibilità a livello di parole e frasi di tutte le comunicazioni e che i registri di dati siano completamente consultabili. Se una piattaforma riesce a colmare con successo questo gap, consentirà alla sicurezza e alla compliance di operare dallo stesso punto di partenza e rimuovere i silos.

È necessaria una maggiore visibilità tra le organizzazioni

Una volta compreso uno scenario di rischio, si ha la necessità di un software in grado di tenere il passo con il volume delle comunicazioni digitali generate. Il monitoraggio manuale spesso non è affatto pratico. I rischi e i canali moderni sono spesso basati sul cloud, quindi, il tool utilizzato deve fornire una difesa del cloud-native. I team devono essere in grado di rilevare le minacce a livello di app e metterle in quarantena rapidamente prima che possano causare danni o raggiungere tramite VPN i sistemi aziendali. Le aziende più grandi richiederanno una rapida implementazione per i team multiregionali.

Unificare Sicurezza e Compliance per Maggiori Vantaggi

Gli stakeholder chiave di qualsiasi organizzazione vorranno maggiori vantaggi dalla collaborazione tra sicurezza e conformità. Ad esempio, il Chief Financial Officer o il Chief Marketing Officer vorranno garantire che i canali digitali siano rafforzati contro i rischi di compliance e sicurezza, in modo che possano aumentare la produttività senza aumentare i costi

dell'organico dell'organizzazione. Il dipartimento R&D o il Chief People Officer vorranno sapere immediatamente se si verifica una perdita di dati IT all'interno di una chat privata o un canale di collaborazione e i team di marketing e vendita vorranno garantire l'accurata rappresentazione di prodotti e servizi sul web e social media e vorranno anche essere informati di qualsiasi intento dannoso nel dark web. Queste richieste possono essere pienamente soddisfatte solo se sicurezza e compliance lavorano a stretto contatto.

Conclusioni Finali

Se le organizzazioni continuano a operare in silos, semplicemente non saranno in grado di tenere il passo. La natura del lavoro moderno è che i rischi per la compliance e la sicurezza spesso si manifestano negli stessi ambienti, di solito all'interno di un complesso e interconnesso insieme di dati, difficile da analizzare. Solo il lavoro di squadra può risolvere questa sfida e guidare un'efficace trasformazione digitale nei prossimi anni.

La sicurezza e la compliance spesso mirano entrambe allo stesso obiettivo: gestire efficacemente i rischi all'interno delle organizzazioni. Questo è il motivo per cui i due gruppi esistono e tale obiettivo condiviso dovrebbe richiedere uno sforzo combinato per raggiungerlo. Sia i team di sicurezza che quelli di compliance devono collaborare per stabilire, progettare e applicare i controlli. La sicurezza e la compliance nell'era del business digitale stanno aumentando in complessità e le organizzazioni dovrebbero lasciarsi alle spalle gli approcci statici e binari "blocca o consenti" del passato. Tenendo maggiormente conto del contesto, visibilità e intelligence per il mantenimento della sicurezza e la compliance nel processo decisionale, il rischio digitale sarà in gran parte rimosso. ■

Cybersecurity vs Compliance.

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Autore: **Michele Colajanni**

Nel momento in cui la società ha preso atto della gravità economica, sociale e politica del vivere in un mondo digitale insicuro, ha reagito con una proliferazione di certificazioni di cybersecurity. Quindi, è lecito chiedersi se la compliance sia o meno lo strumento migliore per proteggere la propria organizzazione dai pervasivi attacchi informatici. La risposta non può essere binaria in quanto molteplici elementi entrano in gioco nella valutazione: settore, management, maturità digitale e cyber, dimensione e ampiezza dei mercati interessati, visibilità. Con un'estrema semplificazione, è possibile individuare tre livelli di organizzazioni: evolute, pronte, immature, in cui le intermedie sono quelle che potrebbero beneficiare maggiormente di compliance.

Le prime probabilmente hanno già molteplici certificazioni, ma nei fatti hanno già superato il concetto di compliance, nel senso che sono in grado di sviluppare il proprio sistema di gestione della sicurezza basato sul risk management di tutti i processi esistenti. La cybersecurity by design delle nuove iniziative è integrata nelle linee di business e nella supply chain, ma soprattutto nelle persone, nei processi e nelle scelte tecnologiche. Le responsabilità per le decisioni critiche sono assegnate formalmente a un team e anche l'incident management è un processo maturo e testato. Il personale della cybersecurity partecipa regolarmente ai tavoli del business promuovendo anche nuovi approcci per gestire la sicurezza a livello di filiera e/o di settore. Il rapporto con molti fornitori cyber tende a essere bidirezionale per molteplici servizi quali threat intelligence, info-sharing, real-time e predictive analytics, malware hunting. Anche in Italia esistono organizzazioni a questo livello di maturità ed è piacevole e utile poter interagire con loro.

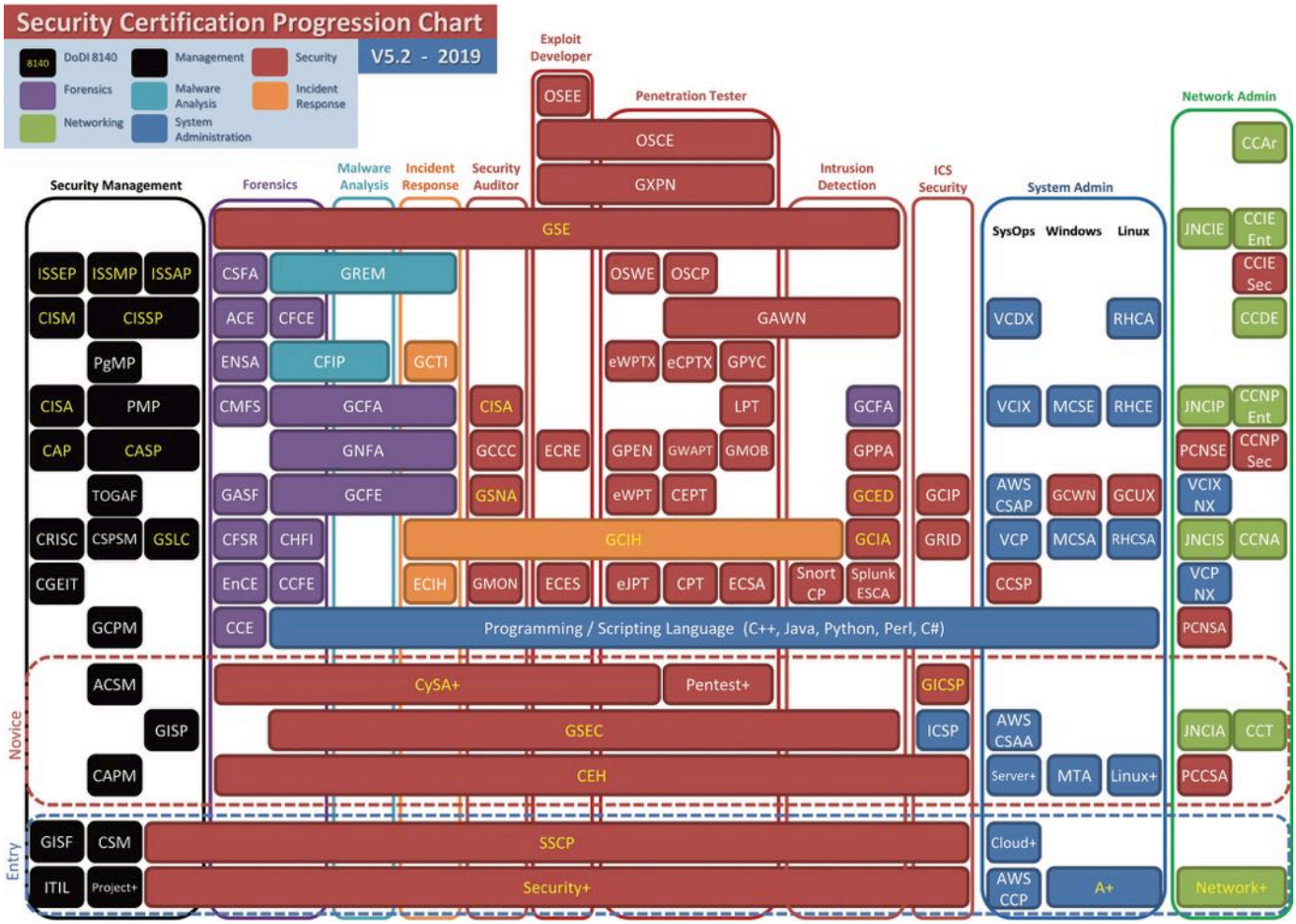
Alle organizzazioni di terzo tipo appartengono quelle immature a livello cyber, che sono dotate di storici firewall e antivirus, e che hanno bisogno di evolvere a livello tecnologico e organizzativo prima di affrontare gli oneri richiesti da una certificazione o da un servizio di *penetration testing* al fine di conoscere la propria (inevitabilmente pessima) postura cyber. Per accedere con un accettabile livello di sicurezza al magico mondo dei servizi Internet e poi della certificazione bisogna prima adottare un insieme di quelle che oggi rappresentano le minime misure di sicurezza informatica. Senza voler entrare nella diatriba di quali siano i provvedimenti assolutamente necessari, un'ispirazione *vendor independent* per alcuni accorgimenti fondamentali può essere rappresentata dalle misure previste dalla PCI-DSS o addirittura da un sottoinsieme di queste, per le organizzazioni

meno mature. Solo in seguito alla loro adozione e implementazione, si può valutare se intraprendere o meno la strada della certificazione.

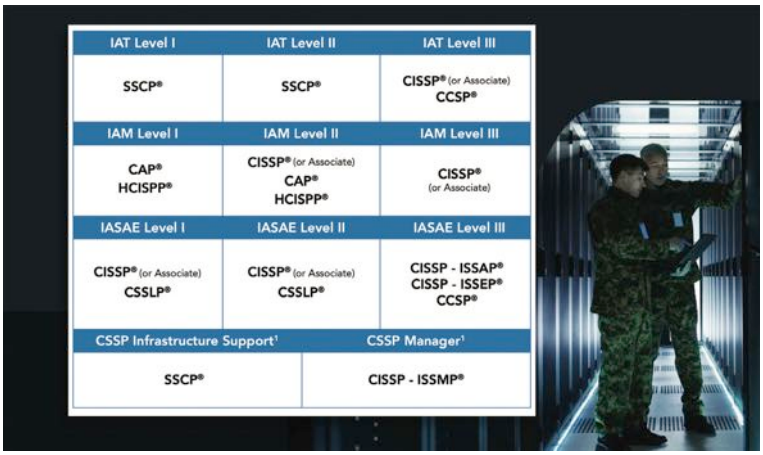
La risposta alla tipica domanda sull'utilità rispetto alla effettiva sicurezza è semplice e perentoria: dipende tutto dal top management. Se il Board ci crede, la certificazione è un ottimo mezzo (non un fine!) per migliorare la postura cyber di un'organizzazione. Se, al contrario, l'obiettivo è di immagine o di necessità, la certificazione diventa un impegnativo esercizio formale che ha un suo scopo (ad esempio, la partecipazione a un bando, la soddisfazione del cliente o del mercato), ma ben diverso da quello della sicurezza.

Questa dicotomia si riscontra anche tra gli esperti che amano suddividersi tra certificatori ed esperti cyber ("I do security, not certification"); con un reciproco sguardo di sdegno, quando invece è dalla collaborazione che si potrebbero ottenere i risultati migliori. I secondi, tecnologicamente competenti, sono portati a fidarsi della forza dell'innovazione tecnologica per risolvere i problemi di sicurezza. La storia dimostra il contrario. Al contrario, i certificatori puntano soprattutto alla messa a punto dei processi e relative responsabilità in quanto sono questi che si vanno a certificare e non la qualità del risultato finale. Nei Paesi in cui si crede solo in parte alla serietà e puntigliosità dei princìpi anglo-germanici che sottendono le certificazioni (il nostro è tra questi, ma non il peggiore), si possono ottenere para-certificazioni che non implicano alcuna sicurezza.

Questo mondo esiste, è un mercato ben noto, ma non è quello di nostro interesse. Analoghi problemi, a livello internazionale, si riscontrano nell'ambito delle auto-certificazioni. Ad esempio, molte organizzazioni, che lavoravano per il Dipartimento della Difesa statunitense senza dover operare sulle informazioni classificate, avevano la possibilità di effettuare auto-dichiarazioni rispetto alla propria postura di cybersecurity. Un controllo a campione ha evidenziato che più del 90% di queste dichiarazioni erano



"estremamente generose". Da qui, è emersa una stretta energica che ha condotto il Dipartimento a emanare una certificazione ben più onerosa, di processo e di risultato, che sta destando preoccupazioni in circa trecentomila fornitori e sub-fornitori.



L'insieme delle certificazioni richieste dal DoD Americano © ISC2.org

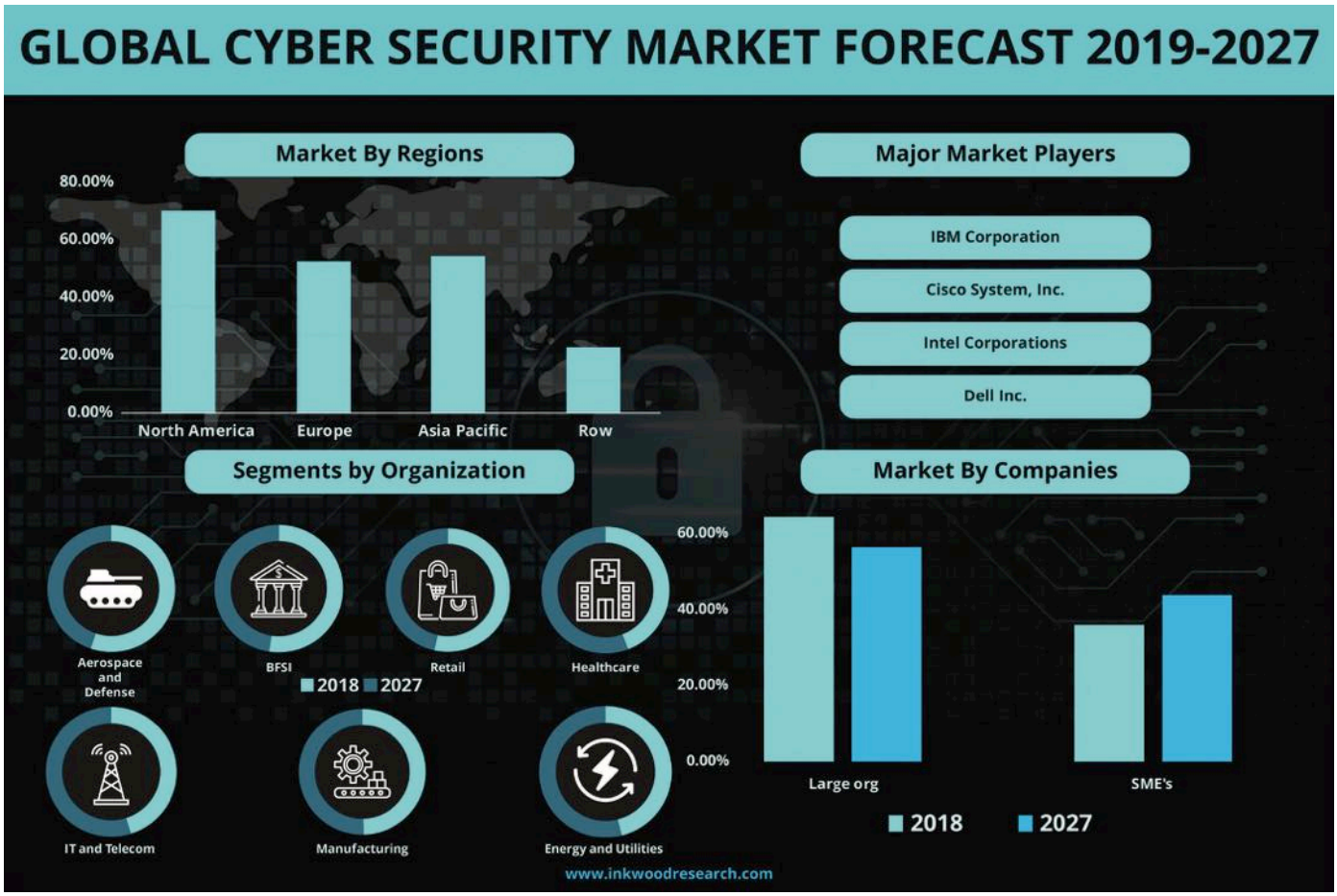
Il desiderio di pervenire a una vera certificazione può emergere solo dal Board in quanto è un processo complesso, oneroso in termini economici e di risorse umane, irto di ostacoli che solo l'endorsement da parte del top management può consentire di superare. Si potrebbe puntare a certificare l'intera organizzazione, ma è un approccio da sconsigliare. Meglio operare all'inizio su di un dipartimento e poi espandersi a macchia d'olio. Vi sono molteplici motivazioni al riguardo. Innanzitutto, è più facile persuadere un manager e un gruppo di persone motivate che convincere un'intera organizzazione. Spesso, anche per le gare, non è necessario che tutta l'organizzazione sia certificata, ma solo i processi, le infrastrutture e le informazioni che riguardano il campo di applicazione della fornitura. Il terzo elemento è che raramente è buona la prima: se l'organizzazione non ha pregresse esperienze di certificazione, il percorso richiede un tipico approccio *trial-and-error,* e relativo apprendimento dagli errori. Una volta ottenuta la certificazione di un dipartimento, l'espansione diventa più semplice, anche perché alcuni dei dipendenti potrebbero essere impiegati per propagare la metodologia più adatta. Il know-how e la coesione aziendale ne beneficiano. E nella cybersecurity il trust è la base di tutto.

Oggi si avverte una certa "stanchezza" delle aziende nei confronti delle certificazioni tradizionali: più si moltiplicano più vengono avvertite come adempimenti formali, ma non sostanziali. Si effettuano perché sono sempre più necessarie per rimanere nel mercato e per tutelarsi nei confronti delle norme, ma si stanno perdendo le motivazioni e lo spirito guida originali. Il desiderio che traspare da molti è la necessità di integrare la certificazione della qualità dei processi con quella della qualità del prodotto o del risultato: se investo, il certificato mi deve offrire delle garanzie. Al contrario, oggi non si ha alcuna garanzia che un'azienda certificata ISO/IEC 27001 sia più sicura di una non certificata. La garanzia è sui processi, sulla consapevolezza, sui ruoli, sulle responsabilità, sulla documentazione. Non poco, ma non tutto quello che serve.

D'altro canto, se si volesse, il sistema di gestione della sicurezza potrebbe includere dettagliate misure tecnologiche da implementare così come potrebbe prevedere misure per il monitoraggio continuo e

BIO

Michele Colajanni è professore ordinario presso il Dipartimento di Informatica: Scienza e Ingegneria dell'Università di Bologna e titolare dei corsi di Cybersecurity e di Scalable and Reliable Services. Laureato presso l'Università di Pisa e conseguito il titolo di dottore di ricerca in Ingegneria dell'Informazione presso l'Università di Roma Tor Vergata, è divenuto ricercatore presso il medesimo Ateneo nel 1994 e visiting researcher presso l'IBM T.J. Watson Research Center. È stato professore associato di Ingegneria Informatica presso l'Università di Modena e Reggio Emilia dal 1998 e ordinario dal 2000. Ha fondato molteplici attività di ricerca e formazione concernenti la sicurezza informatica e la big data analytics, quali il Centro di Ricerca Interdipartimentale sulla Sicurezza nel 2007, il master universitario di Sicurezza Informatica e Disciplina Giuridica dal 2002 al 2012, i master di Cyber Defense Governance e Digital Forensics per lo Stato Maggiore Difesa dal 2012 al 2020. Direttore del Corso di Perfezionamento universitario in Security Manager dal 2010 al 2018, del CyberLab istituito con la Tel Aviv University con patrocinio del MAECI, della Cyber Academy orientata agli hacker etici e del Corso di Perfezionamento in "Cyber Security Management" presso la Bologna Business School dal 2018, e fondatore del summer camp RAgazze Digitali. Svolge un'intensa attività formativa e divulgativa in sedi nazionali e internazionali e collabora, su tematiche di cybersecurity, cloud e Big Data con amministrazioni pubbliche e aziende in ambito finanziario, difesa, energia e manifatturiero. È membro dell'Accademia Nazionale di Scienze, Lettere e Arti di Modena, componente dell'Advisory Board dell'AIPSA, del WG "Cyber security" del Comitato Tecnico AIPCR "Guida Connessa ed Automatica" del MIT, presidente dell'European Center for Advanced Cyber Security, del CdA della Fondazione Telefono Azzurro e vincitore del premio Unicef "Ragno d'oro" per la categoria "Ricerca e innovazione" nel 2017.



periodici sistemi di verifica e controllo da parte di terzi. Ma queste attività aumenterebbero i costi e i tempi, e complicherebbero la possibilità di ottenere la certificazione. Pertanto, non essendo strettamente necessarie, pochi sono disponibili ad auto-introdurre misure aggiuntive. Tuttavia, la motivazione sarebbe ovvia: così facendo si migliorerebbe concretamente la postura di sicurezza della propria organizzazione. E quindi si ritorna alla domanda iniziale su cosa voglia investire prioritariamente il Board: *certificazione* o *maggiore sicurezza?* Ovviamente la prima: un risultato chiaro, un bollino da esporre, un biglietto di ingresso ai bandi di gara. Si faccia attenzione che l'alternativa non è la garanzia di sicurezza, ma una inquantificabile maggiore sicurezza.

È terribile da ammettere, ma più di trent'anni di sicurezza informatica non sono riusciti a proporre un indice, una misura, un KPI (il ROSI, ahimè, non ha funzionato) che potesse rendere "vendibile" la sicurezza agli occhi di un CEO, di un CFO o di un qualunque C-level che è abituato a ragionare sul ritorno dei propri investimenti. È stata una dura lezione ricevuta da un CEO di una grande banca durante una pausa pranzo attraverso conti annotati su di un foglietto che conservo gelosamente. Dati alla mano, ho dovuto ammettere che ci sono ben pochi altri investimenti aziendali con così scarse garanzie di risultati.

Anche perché "migliore" non è una misura: migliore di quanto rispetto a prima? E quanto la nuova postura è vicina o lontana dall'asintoticamente irraggiungibile perfezione? Nessuno può dirlo; infatti, nessun fornitore, consulente o esperto fa affermazioni di questo tipo. E se le facesse, sarebbe da allontanare al più presto. Il dilemma è tutto qui. Per il bene dell'organizzazione, bisogna riuscire a convincere il CEO a investire su procedure e tecnologie di cybersecurity, onerose sia dal punto di vista finanziario sia da quello di inevitabili complicazioni dei processi di business, ma senza offrire misurabili miglioramenti né garanzie di risultato.

Perché la cybersecurity è proprio questa: una maratona che coinvolge tutta l'organizzazione senza un vero traguardo, ma con tappe intermedie che i bravi esperti e consulenti sanno individuare e promuovere. A differenza della certificazione, la cybersecurity è difficilissima da "vendere".

Per disporre adeguati investimenti, serve una sensibilità e una cultura approfondita sul tema cyber che consentano di cogliere sia la complessità del problema - detto senza enfasi - più grande che abbiano mai dovuto affrontare i difensori sia l'inevitabilità del rischio del famoso quanto reale "non se ma quando".

L'alternativa motivazionale della **paura**, per un pericolo scampato o per un danno subìto, è la peggiore quanto purtroppo ancora la più utilizzata e, nei fatti, convincente. La paura è una leva motivazionale pessima in quanto non consente di ragionare con la freddezza e i tempi necessari della cybersecurity che richiede: pianificazione, organizzazione, individuazione delle competenze e operatività per ottenere benefici a medio-lungo termine. La paura, al contrario, induce alla fretta di individuare il fornitore più prossimo e non sempre il migliore. Istiga a sprecare energie per individuare e punire i colpevoli o più spesso i capri espiatori. E, una volta individuati, si è indotti a eliminare competenze preziose che spesso sono le stesse che hanno pregato inutilmente gli attuali "carnefici" a investire più risorse in sicurezza. Ma, essendo difficile "venderla", tali profetiche richieste sono rimaste inascoltate per anni. Del resto, non è un caso che i greci, che hanno còlto per primi i fondamentali del mondo, predispongano un terribile destino per Cassandra.

In un Paese che non crede agli investimenti in prevenzione, è inevitabile che il marketing più efficace della cybersecurity sia in mano ai criminali informatici. A me non piace né alimentare cassandriche paure né attendere passivamente sulla riva del fiume. E allora ben venga la compliance quale primo passo per smuovere la cultura aziendale rispetto alla cybersecurity, in quanto ogni certificazione è fondamentalmente un processo di miglioramento continuo. E anche se all'inizio il soddisfacimento dei requisiti può essere formale, è meglio di niente. Il seme è stato piantato, la consapevolezza dei dipendenti e del management è aumentata anche nelle certificazioni più fittizie, e soprattutto qualche giovane "cireneo" preposto allo scopo è stato individuato; questi crescerà perché la sfida della cybersecurity appassiona.

Col tempo, diventerà più facile innestare in questa piantina qualche ramo di concretezza tecnologica, di verifica e di conseguenti provvedimenti cyber. Anche perché, ed è probabilmente il suo merito maggiore, la compliance di cybersecurity costringe l'azienda a formalizzare e svolgere le attività secondo buone e chiare regole: consapevolezza, visione, individuazione delle responsabilità, delega e controllo. In un mondo in cui tutto è digitalizzato, probabilmente il miglior ritorno dell'investimento della certificazione non deriva da garanzie di protezione contro attacchi informatici, bensì dal miglioramento dell'operatività, scalabilità e resilienza dei propri processi di business in rete. ■

Sicuri perché conformi o conformi perché sicuri?

Autore: Giancarlo Butti

Negli ultimi anni vi è stata una evoluzione nelle normative che regolamentano anche gli aspetti di sicurezza in ambito ICT. Si è passati da una visione impositiva in merito alle misure di sicurezza da adottare ad una responsabilizzazione dei soggetti, chiamati a rispettare la normativa, nella individuazione di quali siano le misure più idonee alla loro specifica situazione.

Gli esempi relativi al passaggio da una visione prescrittiva delle misure di sicurezza ad una responsabilizzazione nella loro scelta da parte di quanti sono tenuti a implementarle sono numerosi e probabilmente, il più noto, non fosse altro che per la immensa platea a cui si rivolge è costituito dal GDPR.

Se infatti la versione pre GDPR del Codice in materia di protezione dei dati personali normava in una serie di articoli (31 - 36) ed in un allegato tecnico (l'allegato B, ora abrogato) una precisa serie di misure di sicurezza che i Titolari erano obbligati ad implementare (con conseguenze penali in caso di inadempienza), nel GDPR, ed in particolare nell'articolo 32 (ma non solo), viene chiesto ai Titolari di effettuare una valutazione di quali misure di sicurezza adottare successivamente ad una analisi dei rischi sui diritti e libertà delle persone fisiche.

Articolo 32 - Sicurezza del trattamento (C83)

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: …*

Il tutto è espresso a dire il vero, in una forma un po' criptica per chi non è del mestiere, tanto e vero che l'obbligo di effettuare questa (e altre) analisi dei rischi è per lo più ignorato e si confonde tale adempimento con la valutazione di impatto richiesta dall'articolo 35 (Valutazione d'impatto sulla protezione dei dati) sempre del GDPR.

In effetti non è così intuitivo che il tenendo conto …del rischio di varia probabilità e gravità, significa che è necessario effettuare un'analisi dei rischi (combinazione di probabilità di accadimento di un evento avverso, della probabilità che l'evento produca un danno e dell'impatto).

E non è nemmeno così intuitivo che la richiesta di effettuare tale valutazione è perentoria, costituendo quindi un obbligo al quale il Titolare o il Responsabile non possono sottrarsi. Come vedremo questa stessa formulazione riguarderà anche altri aspetti ed è utilizzata in particolare negli articoli 24

Articolo 24 - Responsabilità del titolare del trattamento (C74-C78)

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei ***rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche****, il titolare del trattamento mette*

in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78)

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei ***rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*** *costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

In particolare, l'articolo 25 esprime, sempre in forma un po' criptica (ma al riguardo è utile consultare le specifiche Linee guida dell'EDPB) quello che è l'ambito per il quale è necessario adottare, a cura del Titolare, adeguate misure tecniche ed organizzative.

L'articolo cita espressamente la minimizzazione, ma riguarda più in generale i principi.

Quali sono gli altri principi di protezione dati che devono essere attuati ai quali fa riferimento l'art. 25?

L'articolo del GDPR che descrive in modo esplicito e completo i principi è l'art. 5 Principi applicabili al trattamento di dati personali, che così recita:

1. I dati personali sono: (C39)

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

BIO

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari; consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni.
Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, whitepaper, manuali tecnici, corsi, seminari, convegni. Svolge regolarmente corsi in ambito privacy, audit ICT e conformità presso ABI Formazione, CETIF, ITER, INFORMA BANCA, CONVENIA, CLUSIT, IKN, Università degli studi di Milano.
Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali e una decina on line. Ha pubblicato 21 fra libri e whitepaper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT…
È socio e proboviro di AIEA, socio del CLUSIT e di BCI. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico e GDPR di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti, SOC, di UNINFO sui profili professionali privacy, di ASSOGESTIONI sul GDPR.
È membro della faculty di ABI Formazione, del Comitato degli esperti per l'innovazione di OMAT360 e fra i coordinatori di www.europrivacy.info. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/ IEC27001, CRISC, ISM, DPO, CBCI, AMCBI.

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica

o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Fra i principi compaiono alla lettera **f) l'integrità e la riservatezza**, come componente della sicurezza dei dati personali.

Ecco, quindi, un altro articolo che fa espresso riferimento alla sicurezza e su come essere conformi al GDPR rispetto a questo aspetto.

Evidenzio che mentre nell'art. 32.1 si fa riferimento ai diritti e libertà delle persone fisiche come oggetto di tutela (il reale oggetto di tutela del GDPR, come previsto dall'art. 1 del GDPR stesso), l'articolo 5.1.f è più specificatamente dedicato ai soli dati personali (riprendendo in parte l'approccio del vecchio Codice).

Anche in questo caso l'analisi del rischio e le relative misure tecniche ed organizzative sono obbligatorie e non altrimenti definite.

Anche in questo caso si sarà conformi solo se si sarà sicuri (perlomeno per i principi previsti dall'articolo 5.1.f).

È fuori tema, ma lo evidenzio, che il rispetto di tutti gli altri principi elencati dall'art. 5.1 trascende le semplici misure di sicurezza, ma richiede l'adozione di altre misure, capaci ad esempio di garantire la qualità dei dati.

Si tratta di misure particolarmente impegnative, anche se per nulla innovative in quanto già richieste dalla precedente normativa (anche se non specificatamente sanzionati in caso di mancata implementazione e pertanto per lo più disattese).

In sintesi, quello che si desume da questo nuovo approccio nell'ambito della tutela della protezione dei dati personali (o meglio dei diritti e libertà delle persone fisiche) è che si è passati da una prospettiva che prevedeva che un trattamento fosse sicuro se era conforme (rispettava cioè le puntuali misure previste dalla normativa), ad una in cui si è conformi se si è sicuri.

Questo tipo di approccio è comune a molte delle più recenti normative in ambito europeo e sicuramente ha dei vantaggi quali il fatto di mantenere la normativa scollegata sia dalle evoluzioni delle minacce, sia dalla evoluzione delle misure di sicurezza.

Nondimeno tale approccio ha anche dei limiti; l'assenza di alcun punto di riferimento può costituire un problema sia per il soggetto che deve decidere

in merito a quali siano le misure adeguate, sia per chi deve verificare la conformità alla norma.

Il GDPR prescrive solo un paio di misure di sicurezza obbligatorie, la 32.4 relativa all'attività di istruzione dei soggetti autorizzati al trattamento dei dati

Articolo 32 - Sicurezza del trattamento (C83)

…

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

e la 25.2, nella parte dedicata alla minimizzazione dei soggetti che hanno accesso ai dati.

Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (C75-C78)

…

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Per quanto attiene altre misure di sicurezza eventualmente implementabili, l'art. 32.1 si limita a darne una breve elencazione, non esaustiva e per nulla obbligatoria:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

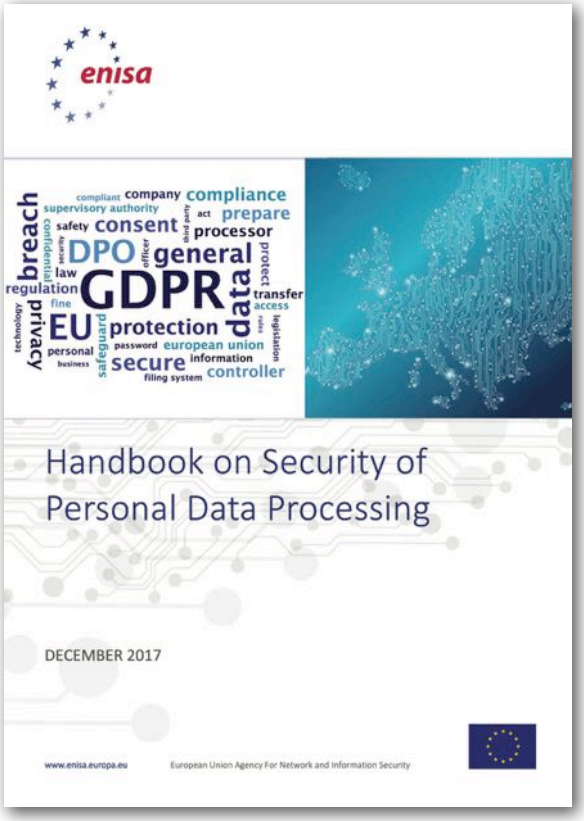
In assenza di punti di riferimento, qualunque contestazione effettuata da un soggetto esterno, come ad esempio un ente preposto alla verifica del rispetto da parte di un Titolare in merito alla sua conformità ai requisiti del GDPR potrebbe essere in realtà oggetto di contestazione.

Rispetto a una situazione oggettivamente non facile da gestire, quali sono gli strumenti di cui può avvalersi un Titolare per essere sicuro (e quindi conforme)?

Prima di tutto il ricorso a quanto proposto direttamente dalle Autorità Garanti.

Il CNIL, l'AEPD e anche la nostra Autorità propongono sia direttamente, sia indirettamente, metodologie sia per la valutazione del rischio (in particolare la nostra Autorità rimanda alla metodologia proposta da ENISA), sia raccolte di misure di sicurezza che è possibile adottare.

Ma è in particolare la metodologia di ENISA che può agevolare il lavoro del Titolare.



Tale metodologia ha infatti il grosso vantaggio di offrire un approccio molto semplice alla valutazione del rischio, ma soprattutto di proporre, in funzione del livello di rischio individuato, un elenco di misure di sicurezza per contrastarlo.

È evidente che in questo caso, essendo la metodologia di ENISA ufficialmente riconosciuta dalle Autorità Garanti, si ha la massima confidenza in merito alla propria conformità se si adottano le misure suggerite.

Esiste anche un'altra possibilità per avere qualche indicazione su cosa sia opportuno implementare per essere considerati conformi, e cioè esaminare quelle che sono le prescrizioni che le Autorità Garanti hanno riportato nei loro provvedimenti sanzionatori relativamente alle misure di sicurezza.

Ovviamente sarà necessario in questo caso ricondurre alla propria situazione quanto disposto dall'Autorità.

POLITECNICO MILANO 1863 SCHOOL OF MANAGEMENT | osservatori.net digital innovation

Da ultimo può essere utile consultare anche quanto prodotto da enti di ricerca o associazioni, quali ad esempio i rapporti dell'Osservatorio del Politecnico di Milano nell'ambito della protezione dei dati e cybersecurity. ■

La compliance nella security: boost del cambiamento o forza inibitrice?

Autore: Greg Day

A seconda dei settori di attività, il rapporto tra sicurezza e compliance può assumere connotazioni anche molto diverse. Alcuni sostengono che gli standard, siano essi governativi o di natura regolamentare, abbiano dato origine a una lotta continua tra il tenere il passo e l'affrettarsi dietro al cambiamento.

I più all'avanguardia direbbero che la compliance può persino fungere da forza inibitrice. Da una parte, perché può togliere tempo al fare, ovvero, alla focalizzazione sul controllo della cybersecurity. Dall'altra, perché soffoca l'innovazione, laddove è obbligatoria. Altri potrebbero invece asserire che la compliance è positiva per la sfera cyber, poiché definisce una linea guida, un set di standard minimo a cui tutti dobbiamo allinearci, ad esempio alzando l'asticella dell'igiene informatica di base. In passato, ho avuto la fortuna e l'onore di collaborare con Betty Shave, che ha lavorato alla Convenzione di Budapest[1] da cui è scaturito il quadro normativo per la criminalità informatica. Ho chiesto a lei come poteva, tale quadro, preservare la sua rilevanza; mi ha risposto che si basava sul danno causato e non sulla tecnologia che lo ha permesso.

Quando l'UE ha introdotto la direttiva NIS e il GDPR, ha usato un termine comune: cybersicurezza allo "stato dell'arte". Questo termine così astratto consente alle aziende di tracciare il possibile e l'applicabile. Tuttavia, ciò richiama due sfide: (1) tutte le aziende sono realmente in grado di tracciare tutto ciò che può accadere e (2) hanno la giusta metrica per farlo?

In un recente articolo[2] ho parlato di una metrica fondamentale, "Detection Efficacy", che viene solitamente dimenticata. Troppo spesso coincide con un focus errato che viene dettato da direttive che regolano cosa dovrebbero

BIO

Greg Day è vicepresidente e global field CISO per Cybereason in EMEA. Prima di Cybereason, Greg ha ricoperto posizioni di CSO e CTO in Palo Alto Networks, FireEye e Symantec. Greg, leader di pensiero rispettato e sostenitore di lunga data di una cyber security più forte e proattiva, ha aiutato molte forze dell'ordine a migliorare il rilevamento dei comportamenti dei cybercriminali. Inoltre, in precedenza, ha insegnato analisi forense sui malware ad agenzie di tutto il mondo e ha lavorato come consulente per il Council of Europe sul cybercrime e la National Crime Agency del Regno Unito. Attualmente fa parte del comitato consultivo del settore della cyber security di Europol.

fare le aziende, anziché come farlo. In questo esempio, usare tool allo stato dell'arte è molto vantaggioso se i dati che raccolgono possono essere aggregati con un elevato grado di fedeltà tramite l'automazione, anziché l'intervento umano. Questo ci riporta al perché, all'ultima RSA Cybersecurity Conference, due fra i temi più scottanti sono stati l'open XDR e l'uso di grafici per le grandi analisi di dati di cybersicurezza.

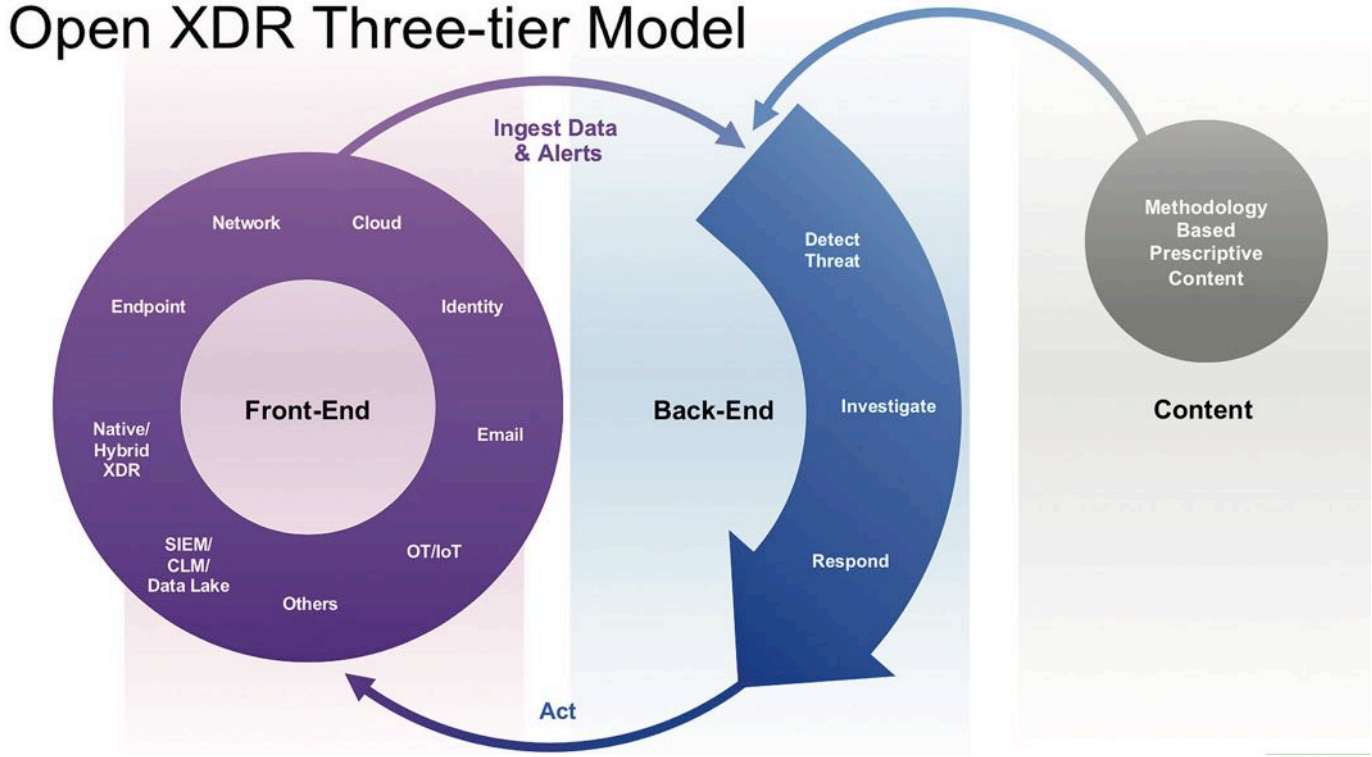
Probabilmente, di anno in anno emergerà sempre un nuovo metodo per il rilevamento delle minacce e, di certo, l'ambito da analizzare crescerà; tuttavia, non si sta evolvendo alla stessa velocità la gamma delle abilità umane nel gestire entrambi questi nuovi tool e tutti i dati che generano. In effetti, guardando alle statistiche di recruiting, sebbene stiamo formando e preparando più persone all'ingresso nel settore della cybersecurity, l'unica cosa che sembra crescere è la lacuna di competenze: ci stiamo affannando, ma siamo ancora pressoché fermi.

Contemporaneamente, si sta riducendo il tempo che le aziende concedono ai team di sicurezza per gestire gli attacchi, sia per via del fatto che "dipendono" dalle conseguenze degli attacchi, sia perché il ransomware ha drasticamente aumentato la velocità dell'impatto. Si crea quindi un paradosso: siamo chiamati a fare di più con meno, mentre la superficie d'attacco si amplia sempre più. Perché e come questi due trend potrebbero avere conseguenze sulla cybersecurity?

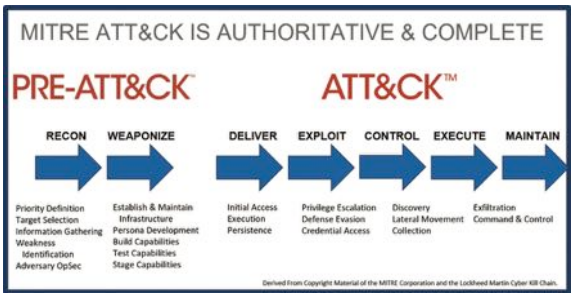
È ormai chiaro che, ad oggi, per rilevare la maggior parte degli attacchi informatici serve ben più che una sola capacità; abbiamo bisogno di molteplici abilità, sia per essere in grado di penetrare a sufficienza nella complessità degli attacchi e capire se siano quelli che effettivamente crediamo essere, sia per dotare di efficacia e validazione quel risultato. In passato, abbiamo visto i principali vendor del settore della sicurezza costruire piattaforme, e poi sviluppare API al loro interno.

Tuttavia, purtroppo diversi vendor sperimentano ascesa e declino in breve tempo e molti CSO vogliono un approccio agnostico verso i vendor, sia per sfruttare ciò che hanno già sviluppato, sia per avere un margine per modificare e adattare man mano che si evolve tutto quello che è lo "stato dell'arte".

Le soluzioni open XDR vengono in aiuto; molte derivano da soluzioni EDR di successo, che prendevano tipicamente i dati degli endpoint e li correlavano per ricavarne azioni. Usando questo approccio, si fornisce una sorta di architettura che consente di acquisire tanti e diversi feed sulla sicurezza, dalla rete, dal cloud e da



altri touch point della telemetria. Questo approccio dovrebbe inoltre prevedere metodi di rilevamento delle informazioni note e sconosciute, ma anche altre funzionalità simili, come tool e log di gestione dell'identità. Tutti questi elementi devono essere raccolti in un'unica struttura dati. Perché più si "vede", più si dovrebbe essere in grado di capire, ma la parte fondamentale che fa il successo di qualsiasi tool XDR è il modo in cui questa tecnologia aggrega i diversi set di dati, al fine di consentire l'applicazione della smart analytic. Per quanto mi riguarda, il MITRE ATT&CK è stato fondamentale nel gettare le basi affinché ciò fosse possibile.



Ad ogni modo, esattamente come nel caso del cubo di Rubik, che ha 43 trilioni di combinazioni, avere a disposizione tutti i dati non vuol dire avere anche la risposta giusta; si deve agire trasversalmente alle combinazioni, con un obiettivo. Inoltre, focalizzandoci sulle cattive azioni, abbiamo cambiato la nostra prospettiva in molti modi. Tuttavia, un attaccante non tenta di acquisire semplicemente un accesso: il suo obiettivo è rubare dati e rilasciarli a seguito di un riscatto. Noi dobbiamo fare lo stesso, ovvero smettere di guardare alle cattive azioni e poi cercare di indovinare l'obiettivo, piuttosto dobbiamo rilevare e capire cosa ha realmente fatto l'attaccante.

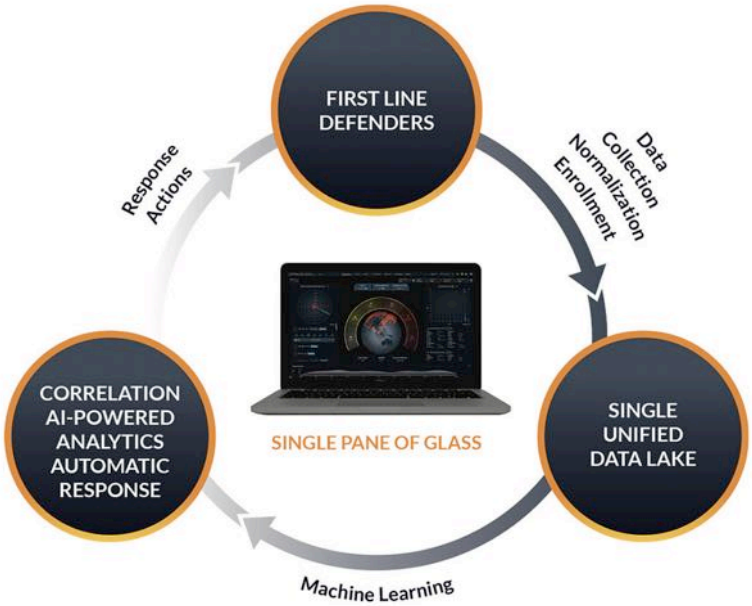
È qui che entrano in gioco i grafici dei dati. Dobbiamo rilevare tutti i dati ed essere in grado di ricostruire in modo dinamico tutte le relazioni che intercorrono tra loro, per vedere il quadro completo. Dobbiamo capire qual è l'obiettivo effettivo dell'attaccante, non quello che ci aspetteremmo sulla scorta dell'enciclopedia delle cyber minacce.

L'altro aspetto che diventa sempre più prezioso quando iniziate a guardare agli attacchi informatici come un tutt'uno, da una prospettiva XDR anziché da quella dei cyber tool, è il fatto di poter valutare continuamente l'efficacia di tutti i vostri tool. Se questi ultimi creano solo tanta confusione, fornendo rilevamenti poco importanti, allora dovrete decidere se continuare a usarli o meno. Molti saranno "nel mezzo", poiché magari emettono alert fondamentali, ma allo stesso tempo fanno anche tanto "rumore". Correlando tutti i dati, potrete regolare al meglio ciascuna capacità di riduzione del rumore e focalizzarvi sugli alert che contano davvero.

Alcuni staranno pensando che è quello che fa già oggi il loro SIEM, mentre la SOAR si occupa dell'intera "orchestrazione". Di certo, il SIEM è un tool fantastico per aiutarvi ad aggregare i dati, tuttavia, non li inserisce in una struttura dati comune, con una rappresentazione grafica di ciò che ha effettivamente fatto l'attaccante nella vostra azienda e non vi guiderà di certo in relazione ai successivi passi da fare, che dovrebbero risultare da quanto scoperto. Similmente, le soluzioni SOAR consentono l'automazione di task ripetitive e possono essere programmate per raccogliere, correlare ed estrapolare dati sulla sicurezza. L'aspetto più importante è che possono agire in base ai risultati, ma solo basandosi sulla programmazione logica che gli è stata fornita. Inoltre, approcciando la sfida dal basso verso l'alto, consentono di raccogliere dati e poi di decidere cosa farne, di trascrivere le routine necessarie e poi di programmare, tramite SOAR, i passaggi per eseguire tali azioni.

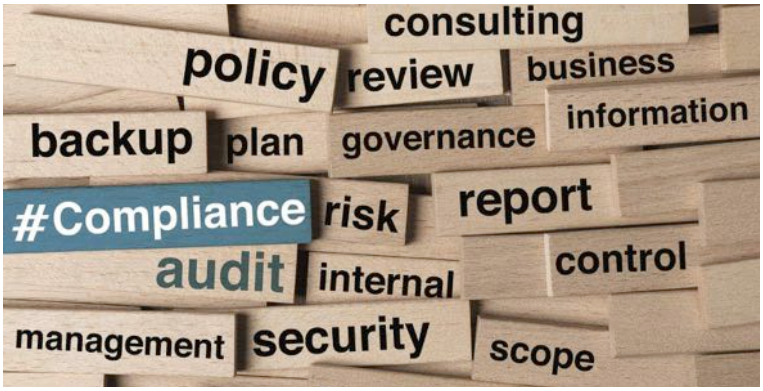
Una buona soluzione open XDR dovrebbe iniziare, per quanto mi riguarda, dall'esatto opposto: dagli eventi effettivi che accadono oggi nella mia azienda, dal mio modo di avere fiducia nella telemetria. Ed è proprio questo il punto: come avere fiducia. E, sulla base di ciò che è accaduto nella mia azienda, quali dovrebbero essere i passaggi successivi.

Ora, entrambi gli approcci hanno i propri sostenitori, e molte aziende adottano uno o l'altro. Tuttavia, è come dibattere su sicurezza e compliance.



O, per usare un modo di dire, tentare di stabilire chi è nato prima, l'uovo o la gallina. Se ci concentriamo sui giusti risultati, avremo processi intrinsecamente corretti, quindi la compliance dovrebbe rappresentare un semplice esercizio di verifica. Ma potreste asserire che se ci concentriamo sui processi dovremmo ovviamente giungere ai giusti risultati.

Esattamente come l'uovo e la gallina, questi due elementi, se isolati, non esisterebbero. La sicurezza e la compliance sono la stessa cosa, esattamente come avere un approccio bottom-up o top-down. Tuttavia, nella cybersecurity la realtà non è quasi mai una dolce via di mezzo. Non possiamo girare attorno alla compliance, accertandoci di aver messo in atto tutti i tool e i processi giusti. Il pericolo sta nel perdere di vista l'obiettivo e in questo settore, in cui mancano apprendisti capaci e la portata continua a crescere (il paradosso del tempo), dobbiamo continuare a guardare avanti e a interrogarci per capire se abbiamo messo in atto i tool e i processi giusti sulla base dei rischi odierni e su quelli che prevediamo saranno, per le aziende, i rischi di cybersecurity di domani. Questo vuol dire, analizzare tutto dall'alto in basso, e costruire un processo ottimizzato basato su obiettivi mirati.



Alcuni ora penseranno che tutto questo vada ben oltre la capacità e l'ambito delle risorse di cybersecurity che hanno a disposizione. Potrei sfruttare una buona soluzione XDR che utilizza grafici per ridurre le competenze necessarie per attuare una cybersecurity allo stato dell'arte, ma c'è un'alternativa semplice: usare la sicurezza as-a-service. A questo punto, il rapporto tra sicurezza e compliance cambia ancora una volta. Non potrete più definire e monitorare i vari passaggi, poiché ora è un servizio a pagamento, basato sulla conoscenza, la competenza e le capacità di terzi. E sì, non potete esternalizzare i requisiti previsti dai regolamenti e, come abbiamo visto di recente dalle revisioni della direttiva NIS, non basta più chiedersi se sono in atto i giusti controlli; dovete anche essere in grado di verificarli su base continua.

Se potessi darvi tre spunti, sarebbero questi.

1 La compliance deve essere una linea guida, la metrica serve a verificare se state agendo correttamente e per vedere i risultati attesi. Se in un mondo cyber in rapido cambiamento nella vostra metrica non state osservando alcun cambiamento, allora forse dovreste guardare più a fondo. Non dovremmo mai confondere la buona igiene informatica di base, che è una componente della compliance, con il buono stato complessivo della cybersecurity allo stato dell'arte.

2 Dobbiamo abbandonare un approccio bottom-up alla sicurezza, con tool che fanno cose magnifiche, ma necessitano di un enorme intervento umano. Nel mondo cyber, la competenza umana è una risorsa scarsa. Con un approccio top-down, capiamo quale problema stiamo cercando di risolvere, magari l'interruzione dell'attività e il danno commerciale. Cosa serve per raggiungere tale obiettivo? Né di un altro tool, né di più dati. Ma di un approccio strategicamente diverso. Questo non vuol dire dover ricominciare da capo, ma, per essere concentrati sul risultato, dobbiamo ammodernare e rafforzare le fondamenta su cui si basano i nostri tool e processi di sicurezza. Dobbiamo superare il paradosso del tempo!

3 L'uovo e la gallina: avere una buona sicurezza è impossibile senza una metrica chiara che misuri valore e successo e consenta il miglioramento continuo. A ogni modo, non possiamo lasciarci distrarre troppo della metrica e dai requisiti normativi tanto da perdere di vista l'obiettivo principale. La chiave sta nel modo in cui questi due elementi si intersecano. Nella sfera cyber, non si tratta di capire quale elemento è arrivato per primo. Bensì, di sapere in che modo ciascuno di essi guida l'evoluzione continua. Abbiamo bisogno di una buona metrica dell'igiene informatica, ma anche di una metrica che ci parli di fattori come l'efficacia del rilevamento, altrimenti riconosceremo che la grande abilità e i processi a cui ci siamo affidati per anni non sono più adatti al raggiungimento dell'obiettivo. Allo stesso modo, le capacità sono preziose se possono essere usate. Efficacia ed efficienza sono tanto importanti quanto la capacità! - Se servono migliaia di persone che per ore stanno lì a controllare la validità di un approccio, allora dobbiamo chiederci se quello è il giusto investimento da fare.

Il mondo della cybersecurity continuerà a evolversi, in un mondo economico in cui i margini di profitto si stanno riducendo sempre di più. L'innovazione può apportare grandi opportunità, ma prevede anche dei rischi. La compliance può fungere sia da catalizzatore del cambiamento che da forza inibitrice. La chiave del successo è stare al passo con i cambiamenti della cybersecurity, ma anche con la compliance. Non permettete ad altri di scrivere la vostra storia. ■

1 https://www.coe.int/en/web/cybercrime/the-budapest-convention
2 https://www.cybereason.com/blog/why-detection-efficacy-should-be-in-your-top-metrics

Compliance vs Security.

Autore: Alberto Perini

L'ambito della sicurezza informatica vede oggi decine di standard, controlli e regole che rendono davvero difficile, soprattutto per le piccole e medie imprese, capire cosa fare e come proteggersi non solo dai criminali informatici ma anche de eventuali ripercussioni dovute a controlli non superati. Allo stesso tempo l'esigenza di mettere in sicurezza il patrimonio informativo aziendale è sempre più sentita, con minacce crescenti più o meno dirette ed estremamente variegate e creative. Il valore che hanno acquisito i dati richiede inevitabilmente maggiori funzioni di controllo a livello di management come strumento per la gestione del rischio, sia in fase preventiva che nella successiva elaborazione di un evento avverso.

Secondo previsioni Gartner[1], quest'anno il mercato dell'Information Technology toccherà, a livello globale, i 4,5 trilioni di dollari, ed è atteso nei prossimi anni in costante in crescita.

Table 1. Worldwide IT Spending Forecast (Millions of U.S. Dollars)

	2021 Spending	2021 Growth (%)	2022 Spending	2022 Growth (%)	2023 Spending	2023 Growth (%)
Data Center Systems	216,337	11.4	226,475	4.7	237,021	4.7
Enterprise Software	604,946	14.4	671,732	11.0	751,937	11.9
Devices	787,417	13.0	813,699	3.3	804,253	-1.2
IT Services	1,186,103	10.7	1,279,737	7.9	1,391,742	8.8
Communications Services	1,444,324	3.4	1,462,712	1.3	1,494,167	2.2
Overall IT	**4,239,127**	**9.0**	**4,454,354**	**5.1**	**4,679,119**	**5.0**

Source: Gartner (January 2022)

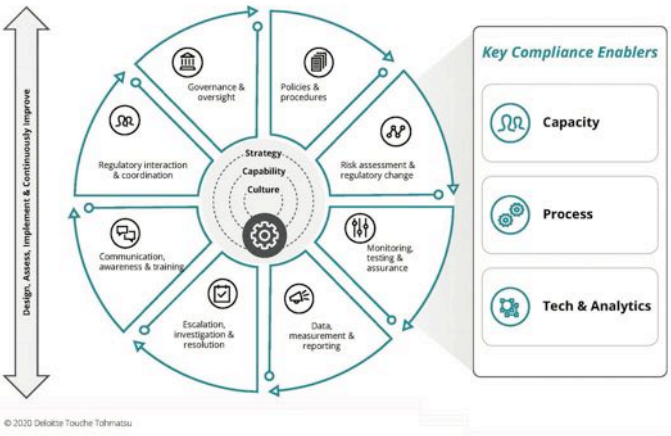
Così come continuano a crescere i crimini informatici. Uno scenario che pone continue e complesse sfide per la security e la compliance. Infatti, se comprendere e gestire le modalità di acquisizione e conservazione delle informazioni diventa prioritario, rispettare i regolamenti assicura un livello di sicurezza accettabile? Come la compliance può incontrarsi e non scontrarsi con la cyber security? Proviamo a fare un po' di chiarezza.

Cosa si intende per compliance.

Il termine inglese compliance significa esattamente conformità. Nello specifico rispettare delle regole ben definite, o attenersi a determinati principi. Si può allora concepire la compliance come uno strumento a disposizione delle aziende per allinearsi nei confronti delle problematiche relative alla sicurezza informatica e allo stesso tempo permettere di decifrare le minacce per pianificare interventi mirati.

Nello specifico la compliance si focalizza sulla tipologia di informazioni gestite da un'organizzazione individuando quali sono i requisiti richiesti nel caso specifico per assicurarne la protezione. Infatti, i requisiti di conformità sono diversi e variano a seconda di diversi fattori: possono essere definiti da leggi specifiche oppure da appositi organismi o anche da grandi gruppi privati come l'industria dei pagamenti. Così può accadere che un'azienda debba allinearsi a diversi framework (i requisiti richiesti), e già questa comprensione non è semplice.

Compliance Risk Management Framework (CRMF) Wheel



Norme e regolamenti prendono in considerazione ben più di quello che è la sicurezza delle informazioni, abbracciando rischi legali e finanziari ma anche fisici. La sicurezza diventa in questo modo un insieme definito di processi e strumenti implementati per assicurare efficacemente la protezione degli asset informativi. Anche se molto spesso per gli operatori di sicurezza la compliance non è una priorità, questa rimane un elemento

di estrema importanza a livello di governance, ancor più in un contesto globale dove la digital transformation gioca un ruolo essenziale.

La sicurezza delle informazioni.

La compliance trova dunque la propria necessità nelle crescenti minacce informatiche alla sicurezza dei dati. L'evoluzione di tali minacce ha portato a modificare il tipo di approccio alla sicurezza che da puramente tecnico è divenuto più olistico, implementando attività sui piani fisico, tecnico e amministrativo. Riservatezza, integrità e accessibilità sono divenute le parole chiave per chi si occupa di sicurezza delle informazioni. Garantire che informazioni sensibili siano gestite solo da chi è autorizzato, assicurare che le informazioni siano corrette e renderle accessibili, cioè disponibili, quando è necessario. Questo è ciò a cui mirano di fatto sia la compliance che la security. La gestione della sicurezza delle informazioni deve tenere in considerazione i processi di risk assessment e di risk management. In primo luogo, deve conoscere ciò che protegge, a partire dai dati stessi fino a chi ne ha accesso, deve mettere in atto tutte quelle azioni atte a prevenire eventuali violazioni ed infine deve avere la consapevolezza che non è possibile raggiungere un livello di rischio pari a zero, pertanto è necessario prevedere come gestire efficacemente eventuali incidenti che non si è riusciti ad evitare, coerentemente con le normative di riferimento. In quest'ottica, tra i problemi rilevanti interni alle aziende va evidenziata la difficoltà a rendere attuabile, in termini di tecnologia e di controlli, quanto stabilito nelle policy.

Si comprende così come si possa essere sicuri ma non conformi oppure conformi ma non sicuri. Sicurezza e compliance rispondono a esigenze diverse ma guardano ad obiettivi comuni completandosi a vicenda. La sicurezza risponde a un'esigenza interna di protezione mentre

BIO

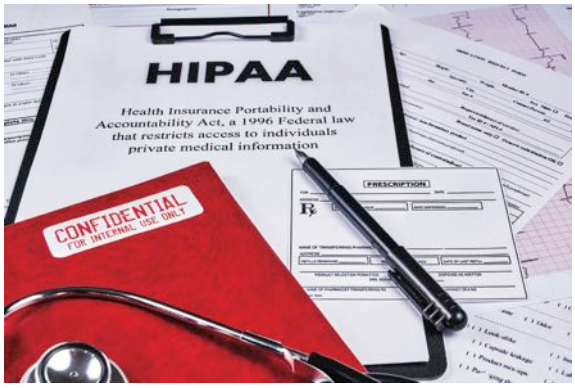
Fondatore di Cyber Ducks, network dedicato alla cyber security, Alberto Perini attualmente ricopre in Azimut Holding il ruolo di CISO. È anche responsabile delle certificazioni di sicurezza, del team GRC e degli standard e della conformità NIST - ISO27001 - 62443 ISA / IEC standard per il dominio dei sistemi di controllo industriale (ICS) per i progetti. Precedentemente in DI.GI International, ha avuto l'opportunità di lavorare sulle strategie e il processo iniziale di Competence Center e SOC durante il passaggio di DI.GI International nel gruppo Softlab. Precedentemente ha lavorato per la sede centrale di Alascom Italia come responsabile della BU per la sicurezza delle informazioni e responsabile della sicurezza informatica per IT/OT/IoT/ICS analizzando nuove minacce di sicurezza e cyber, sempre alla ricerca di nuove soluzioni. È stato attivamente coinvolto nella ricerca e sviluppo come consulente tecnologico per il progetto BI-REX di innovazione sui big data e eccellenza nella ricerca sulla Cybersecurity OT in collaborazione con le Università di Bologna, di Imola, Reggio e di Ferrara. Ha lavorato come responsabile della sicurezza informatica e ricercatore per Sphere Soc con sede in Germania, sviluppando progetti SOC, e per varie società di sicurezza informatica con sede in Italia, Regno Unito e Svizzera, collaborando con diversi vendor israeliani e statunitensi.

la compliance di fatto deve soddisfare delle esigenze esterne all'azienda stessa e termina nel momento in cui tali esigenze sono soddisfatte. Diversamente la sicurezza non ha mai veramente un termine, ma richiede una continua applicazione, revisione e miglioramento. Rispondere ai requisiti dei framework di riferimento può essere complicato ed impegnativo ma una volta fatto si è a posto, pur dovendo eventualmente mantenere degli aggiornamenti. Ma ottenere livelli di sicurezza accessibili è un lavoro costante che coinvolge non solo i sistemi di sicurezza e le tecnologie coinvolte ma anche la formazione degli operatori con lo sviluppo di una

consapevolezza del rischio che induca a minimizzare gli errori umani e l'implementazione di procedure di test e controllo per verificarne l'efficacia. Sicurezza e compliance sono quindi diverse ma entrambe necessarie ed è fondamentale comprendere quali sono i requisiti richiesti dalle varie normative.

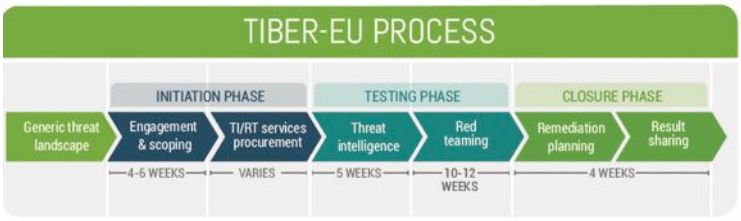
Alcuni protocolli e regolamenti.

Il panorama delle norme e dei regolamenti nel settore è molto variegato e come già accennato la stesse organizzazione può dover essere conforme a più di un modello e non necessariamente un modello deve essere applicato a tutte le organizzazioni. Ad esempio, negli Stati Uniti l'HIPAA, che sta per Health Insurance, Portability and Accountability Act, è una legge che riguarda il settore sanitario ed è finalizzata alla protezione dei dati sensibili sanitari, mentre gli standard PCI-DSS riguardano la sicurezza dei dati delle carte di credito con cui vengono effettuati gli acquisti e mira a ridurre il rischio di frodi aumentando i controlli sui dati dei titolari.



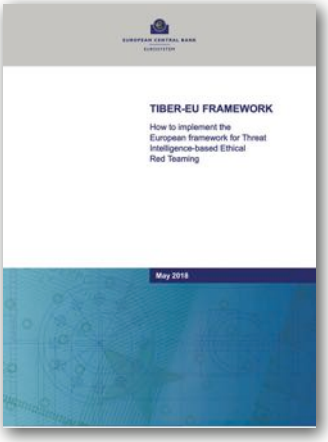
Ci sono poi gli standard ISO 27000 che definiscono requisiti minimi per la sicurezza delle informazioni ai quali le aziende possono decidere se essere conformi oppure no, ottenendo la certificazione.

A livello Europeo sono interessanti in particolare il nuovo DORA (Digital Operational Resilience Act), che dovrebbe entrare in vigore entro fine anno e il TIBER-EU, un framework che risale a pochi anni fa finalizzato alla verifica della sicurezza dei sistemi informatici.



1. La Digital Operational Resilience Act

Dora è il nuovo regolamento europeo che si pone l'obiettivo di uniformare i paesi membri nell'approccio alla resilienza digitale e interessa uno dei settori più critici, quello finanziario. Lo scopo è mitigare i rischi della digitalizzazione stabilendo delle linee guida uniformi per la sicurezza delle infrastrutture informatiche. L'applicabilità riguarda quindi sia il settore finanziario tradizionale, con gli istituti di credito e le compagnie assicurative ma anche i fornitori di criptovaluta o le emittenti di token.



Il regolamento si struttura su 5 macro aree: la prima riguarda l'ICT Risk Management, con i requisiti richiesti per una più efficace gestione dei rischi; la seconda riguarda la segnalazione e la gestione degli incidenti; la terza si pone l'obiettivo di stabilire linee guida per condurre test periodici in base al profilo di rischio specifico; la quarta area prende in considerazione i fornitori di servizi ICT; infine la quinta area mira a sensibilizzare in merito alla condivisione delle informazioni relative alle minacce informatiche.

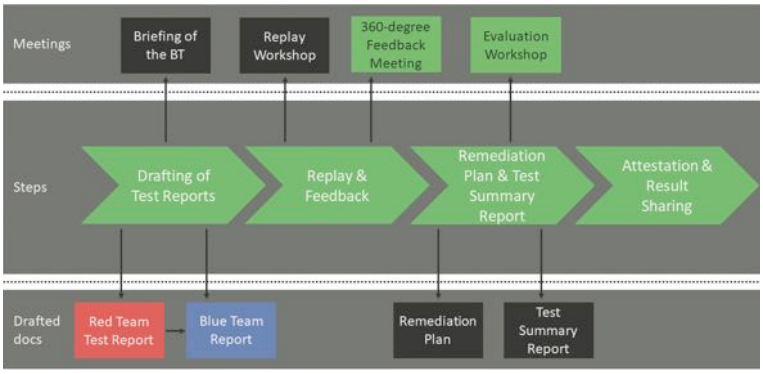
Particolare rilievo è dato ad una corretta assegnazione dei ruoli, con personale dedicato all'identificazione dei rischi, alle misure di prevenzione, alla gestione degli incidenti e alla formazione. Inoltre, si richiede di sviluppare sistemi resilienti, capaci di mitigare l'impatto di una minaccia.

Anche l'aspetto della comunicazione e dello scambio di informazioni si rivela cruciale, e gli operatori sono invitati a creare processi di gestione del rischio seguendo specifici criteri di classificazione e informazione.

2. Il framework TIBER-EU

Un altro interessante framework è TIBER-EU che serve per allineare, a livello europeo, l'esecuzione di test per la sicurezza informatica. L'adesione è su base volontaria, come hanno fatto ad esempio la Banca d'Italia o la Consob. TIBER-EU è stata recepita a livello italiano dalla Guida nazionale TIBER-IT nella quale vengono definite metodologie, fasi dei processi, modelli dei test e ruoli dei soggetti coinvolti. Nella pratica i test simulano le tattiche dei criminali informatici per attaccare le infrastrutture di rete, con l'obiettivo di individuare debolezze e punti di forza e migliorarne così la sicurezza.

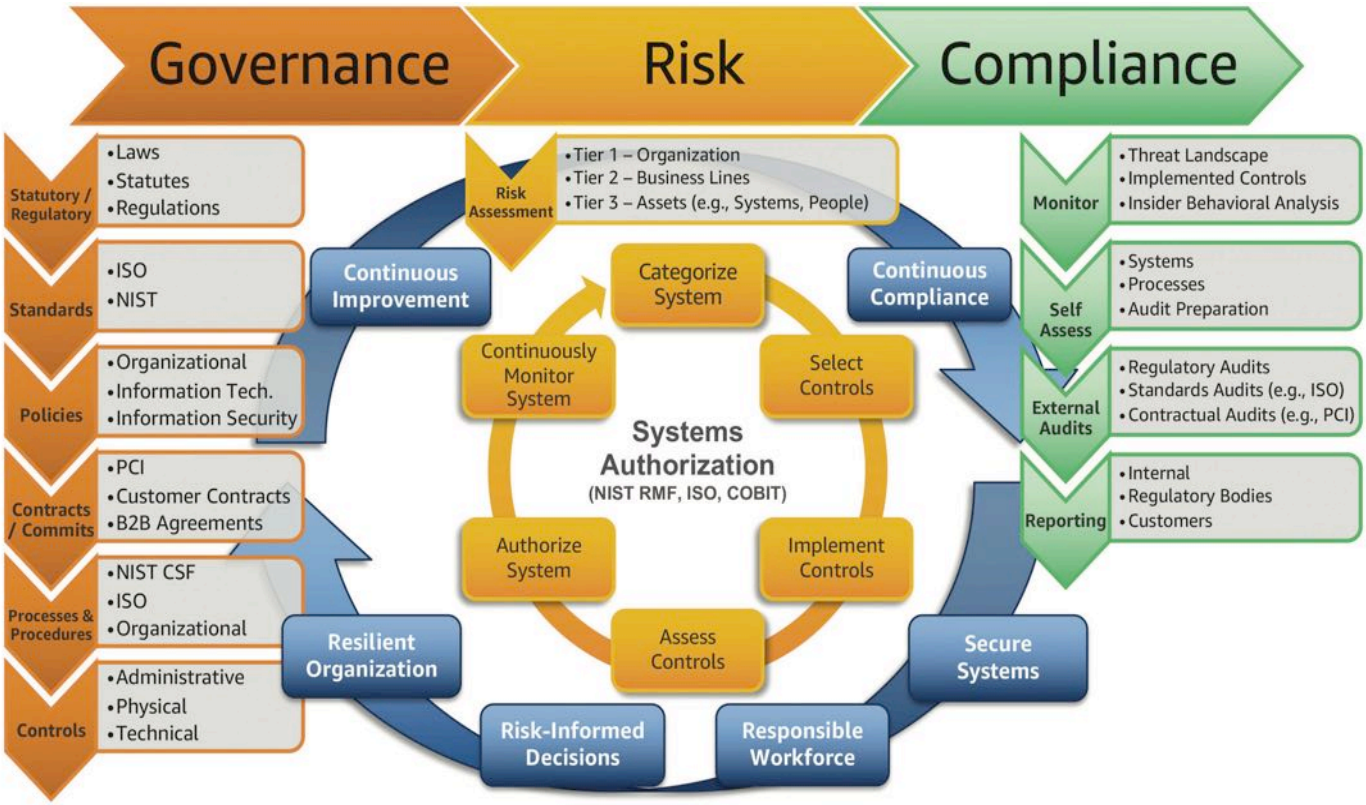
Il test coinvolge cinque squadre: il blue team, che sono le persone nell'azienda target incaricate della sicurezza, l'azienda che esamina le minacce ed effettua una ricognizione, il red team, ossia le persone esecutrici dell'attacco, il white team, le uniche persone nell'azienda target che sono a conoscenza del test e collaborano con l'autorità, il TIBER cyber team, che opera all'interno dell'autorità e verifica la corretta esecuzione del test e il suo riconoscimento.



Sicuri e conformi.

Lo scenario, dunque che si prospetta è quello di una integrazione sempre maggiore tra security e compliance, con l'individuazione di soluzioni su misura, che tengono cioè conto delle dimensioni effettive dell'ambiente di riferimento con tutto ciò che deve essere protetto e la sua localizzazione. La mancanza di una tale consapevolezza può infatti condurre all'implementazione di strategie di sicurezza inefficaci. Se la compliance aiuta ad ottenere questa consapevolezza, la security deve avere il compito di assicurare non solo policy adeguate ma anche tutta la struttura tecnologica necessaria al raggiungimento di obiettivi soddisfacenti. ■

1 https://www.gartner.com/en/newsroom/press-releases/2022-01-18-gartner-forecasts-worldwide-it-spending-to-grow-five-point-1-percent-in-2022



Serve un modello che permetta alle idee di diffondersi nel rispetto delle regole e degli equilibri del libero mercato.

Intervista VIP a Gabriele Faggioli.

Autore: Massimiliano Cannata

Il recente G7* Digital Track *che ha visto impegnati le Autorità Garanti di diverse nazioni europee ha affrontato tra i vari temi: la definizione degli strumenti per il trasferimento internazionale dei dati, la certificazione relativa a questo delicato processo; le tecnologie di miglioramento della privacy (PET); gli standard di anonimizzazione; il rafforzamento dei principi di minimizzazione dei dati per affrontare le sfide della sorveglianza commerciale. Si tratta di aspetti che coinvolgono il mondo accademico, l'industria, e il settore pubblico. Professor Faggioli, quali scenari si aprono sul fronte della sicurezza e della protezione dei dati?

L'attenzione sul tema della protezione dei dati personali è ormai elevatissima sia sul fronte dei normatori che sul fronte dei consumatori. Negli ultimi mesi abbiamo assistito anche ad operazioni di "segnalazione" massiva di pretesi comportamenti illeciti che, seppur a mio avviso non pienamente condivisibili nei modi, hanno messo in luce alcuni problemi importantissimi legati ai flussi transfrontalieri di dati. Se da un lato questa attenzione è ovviamente positiva, in chiave di tutela dei diritti delle persone, è pur vero che in alcuni passaggi si ha talvolta la sensazione di una complessità regolatoria e di un approccio interpretativo fin esagerato. Una cosa è certa: le imprese hanno sempre più l'interesse a usare i dati personali che possono raccogliere e quindi il mercato dei fornitori, caratterizzato da moltissime start-up, sta continuamente evolvendosi proponendo soluzioni software e servizi sempre più potenti. Abbiamo quindi forze contrapposte che rappresentano interessi ampiamente contrastanti con tutti i problemi interpretativi, applicativi e imprenditoriali del caso.

Per la PA è valido lo stesso ragionamento?

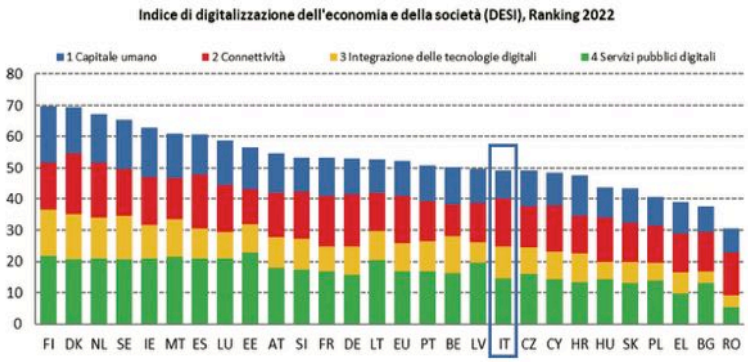
La pubblica amministrazione appare meno coinvolta ma basta vedere le polemiche sul green pass o su alcuni progetti di scoring in talune città italiane per rendersi conto che il tema "dati personali" è primario anche in ambito pubblico. Il paradosso sta nel fatto che a fronte di norme sempre più puntuali e talvolta restrittive che spingono alla minimizzazione quando non alla anonimizzazione, ne abbiamo altre che aprono all'open banking, ai servizi aperti e interconnessi. Sono le due facce della stessa medaglia: il progresso si porta dietro la necessità di dati e informazioni che devono essere protetti e devono essere gestiti nel rispetto dei principi normativi. Trattandosi di norme ampiamente interpretative e non oggettive nella loro applicazione, ed essendo impossibile una norma che anticipi il mercato, assisteremo sempre a una situazione di caos ordinato.

La guerra e la "frontiera digitale"

La guerra alle porte dell'Europa ha aperto un terreno critico anche sul fronte della sicurezza informatica. Attacchi sempre più sofisticati colpiscono istituzioni, settori strategici (come infrastrutture, ospedali) partiti politici. Quali strumenti vanno messi in campo per proteggere la "frontiera digitale" che assume una rilevanza decisiva per la tutela non solo dei singoli, ma anche degli Stati?

Personalmente ritengo che l'Italia sia indietro di 20 anni. L'indice DESI (Digital Economy and Society Index: è un indice introdotto dalla Commissione Europea nel 2014 per misurare i progressi dei Paesi europei in termini di digitalizzazione dell'economia e della società) parla chiaro: siamo terzultimi in Europa per popolazione con competenze digitali almeno di base (42%), contro una media UE del 56%, e quartultimi per competenze digitali avanzate (22%), contro una media UE del 31%; la quota di imprese che ha offerto formazione in ambito ICT ai propri dipendenti si ferma al 16%, contro una media europea del 20%; siamo ultimi nel continente per quota di laureati in ambito ICT sul totale della popolazione con una laurea (1,3% rispetto a un valore UE del 3,9%).

	Italia		UE
	posizione in classifica	punteggio	punteggio
DESI 2022	18	49,3	52,3



In tema di spesa in sicurezza informatica posso dire che l'Italia nel 2021 ha speso 1,5 miliardi di euro complessivamente (0,08% del PIL). Per contro, UK spende lo 0,25% del PIL in sicurezza informatica (il triplo di noi per di più con un PIL molto più alto), Germania e Francia lo 0,16% del PIL (il doppio dell'Italia).

Una situazione di certo non rosea, che dovrebbe sollecitare una presa d'atto oltre e interventi istituzionali mirati. Si intravede qualche spiraglio?

A mio avviso le azioni messe in campo a livello nazionale (l'Agenzia, il perimetro nazionale di cybersicurezza, il polo strategico nazionale e la strategia nazionale) sono ampiamente condivisibili e vanno sostenute. Da una parte serve per forza alzare la competenze digitali in particolare sul tema cybersecurity (anche perché mancano moltissime figure professionali essendoci un mercato del lavoro ampiamente recettivo in questo momento), dall'altra parte si devono mettere a fattor comune gli investimenti spingendo sui servizi di cloud computing (non solo in ambito PA ma anche nel mondo privato). "Aumentare gli investimenti" corretto sostenerlo, ma ricordiamoci che non è possibile pretendere maggiore spesa in periodi di difficoltà economiche complessive.

BIO

Gabriele Faggioli è Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica), Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano e senior advisor degli Osservatori della Digital Innovation del Politecnico di Milano (dove è Adjunct Professor). È CEO di Digital360 S.p.A. e di Partners4innovation S.r.l. (società controllata da Digital360 S.p.A.). È stato membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. Specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amminstrativa degli enti e nel diritto dell'editoria e del markerting, Gabriele ha pubblicato diversi libri fra cui, da ultimo, "I contratti di cloud computing" (Franco Angeli), "I contratti per l'acquisto di servizi informatici" (Franco Angeli), "Computer Forensics" (Apogeo), "Privacy per posta elettronica e internet in azienda" (Cesi Multimedia) oltre ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.

Il Garante della Privacy nella relazione annuale si è soffermato su un duplice aspetto: la nuova direttiva NIS 2 giudicando "lungimirante la scelta dell'UE di aggiornare a fine 2020 la strategia di cybersecurity", e l'istituzione dell'agenzia nazionale per la cybersicurezza. Cosa dobbiamo aspettarci dall'introduzione di questi due tasselli nel corpus nella normativa vigente?

L'Italia ha ora un corpo normativo completo. La strategia nazionale guiderà gli investimenti e gli interventi in ottica di priorità nei prossimi anni e le aziende impattate dalla NIS prima e dalla NIS 2 ora saranno tenute ad adottare posture cyber di assoluto livello. Speriamo che tutto ciò sia di traino per tutte le aziende non impattate direttamente dalle normative di cui sopra che comunque rappresentano la grande maggioranza delle imprese italiane. Sappiamo bene che oggi i danni causati da un cyberattacco sono spesso estremamente rilevanti quindi indipendentemente dalle normative è mandatorio per imprenditori e manager rendersi conto dei rischi che corrono le loro aziende. Lo stesso identico discorso vale per le pubbliche amministrazioni. Siamo di fronte a un passaggio epocale. Finalmente la tematica non è più lasciata alla buona volontà di qualche manager illuminato o a qualche normativa. Ora esiste un disegno complessivo, di respiro non solo italiano. Sono certo che in questo quadro di insieme l'Agenzia saprà essere guida per tutti.

AGID | Agenzia per l'Italia Digitale

La sfida del GDPR

L'entrata in vigore del GDPR è un passo importante. A che punto sono le organizzazioni produttive nella* compliance *delle misure previste, a cominciare dall'istituzione del DPO, figura centrale per l'attuazione di efficaci misure di prevenzione e di* governance *del rischio informatico?

Penso che si debbano fare alcune distinzioni. Dal mio punto di osservazione penso di poter affermare che le grandi imprese soprattutto nel settore B2C hanno fatto passi importantissimi nella direzione della compliance. Diversa è la galassia delle PMI dove invece ci sono a mio avviso ampie sacche di criticità. Per le pubbliche amministrazioni vale lo stesso discorso ma teniamo presente la difficoltà di avere budget adeguati per molti enti pubblici. Per quanto riguarda i DPO la mia sensazione è che il livello medio sia valido. Non mi entusiasmano per niente le polemiche di chi a tutti i costi vuole vedere negativamente il fatto che si stata creata una famiglia professionale che, come tutte le altre, ha eccellenze e livelli qualitativi inferiori. D'altronde, l'esistenza di diverse fasce di professionalità vale per tutti i settori di mercato. Penso che stia ai titolari del trattamento, in base alle proprie specificità, capire il livello di professionalità necessario e di conseguenza valutare la necessità di impegnare risorse economiche adeguate.

La* compliance *costa, non per tutte le aziende è facile stare al passo con quanto richiesto dalle normative vigenti. Quale è la sua opinione in merito?

Penso che si stia esagerando con i costi di compliance. Le aziende sono costrette a investire risorse importantissime. Capisco perfettamente l'esigenza di innalzare il livello di attenzione e di cultura sui temi della compliance per la prioritaria necessità di tutelare i diritti delle persone e una gestione sana delle imprese e pubbliche amministrazioni. Ma questi costi non devono diventare così alti da limitare e frenare l'innovazione e gli investimenti produttivi altrimenti diventano odiosi e incomprensibili. Inoltre, ci si deve chiedere se il livello di compliance richiesto dalle norme e applicato nel mercato sia omogeneo in tutta Italia e perlomeno in tutta Europa, perché se così non fosse ci sarebbero elementi distorsivi della concorrenza inaccettabili.

Gigacapitalisti e libero mercato

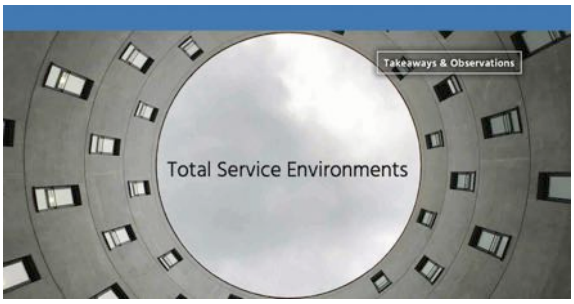
La protezione dei dati ha delle ricadute sugli equilibri geopolitici. Cina Stati Uniti Europa stanno discutendo della possibile definizione di una "sovranità digitale". Di che cosa si tratta in concreto?

La sovranità digitale si raggiunge con il controllo delle infrastrutture digitali e dei dati. Questo postula che tecnologie e dati risiedano nello spazio geografico e giurisdizionale a cui appartengono. Devo dire che come obiettivo non mi appassiona.

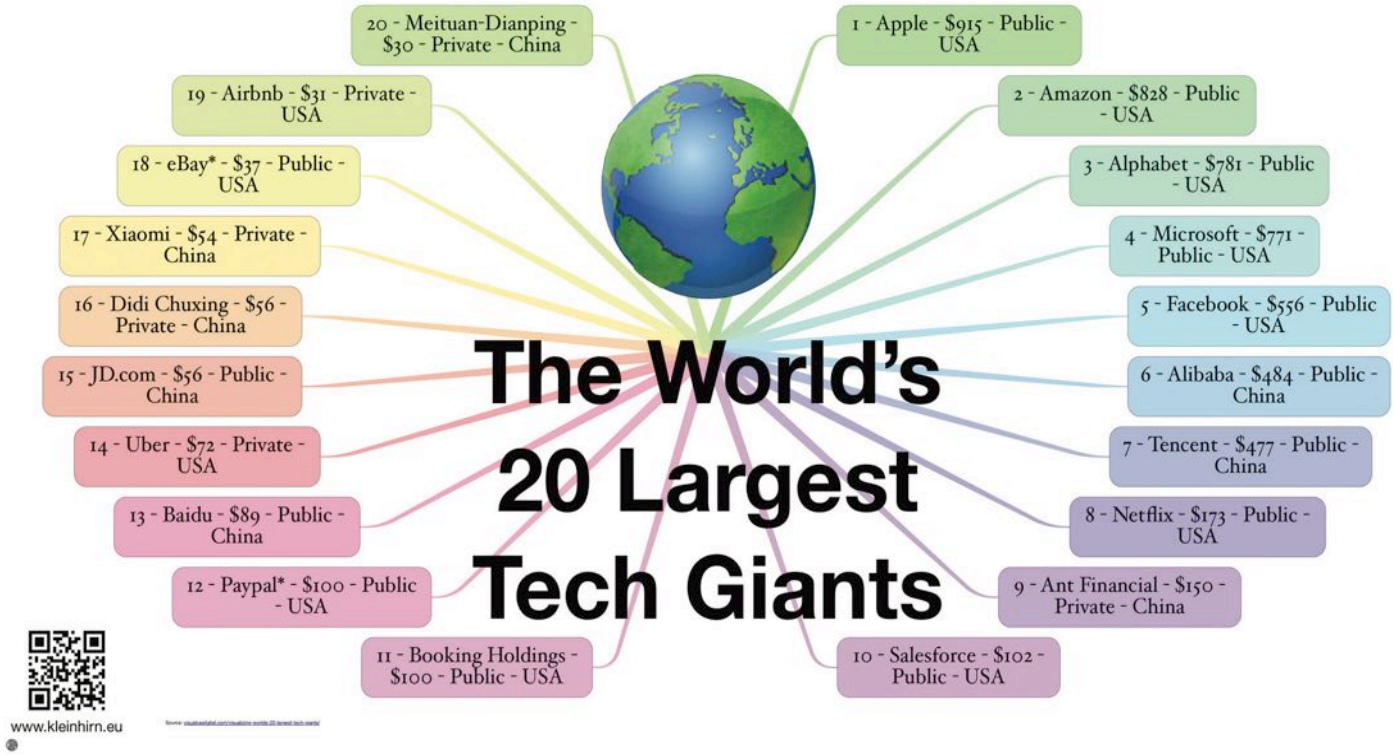
Personalmente sono enormemente più europeista e aperto a una visione globale del mondo, ma indipendentemente dal mio pensiero, la sovranità digitale è quasi impossibile senza l'autonomia tecnologica. E l'Italia è lontanissima da esserlo. Il problema risiede nel fatto che neanche l'Europa lo è, perché dipende soprattutto dagli Stati Uniti. Purtroppo dopo tanti anni di globalizzazione stiamo assistendo a una de-globalizzazione o forse a una frammentazione. Questo non penso porterà alla sovranità digitale europea quanto invece a una polarizzazione verso due o massimo tre centri di potere tecnologico. Il mondo aperto per noi sarà più piccolo di prima e si avrà meno la possibilità di creare valore unendo tecnologie di aree del mondo diverse. Da un altro punto di vista per le aziende produttrici di un blocco si creano quote di mercato in territori più vicini. Insomma, credo che ci saranno, come in tutte le fasi storiche, vantaggi e svantaggi e ci sarà chi crescerà e chi sarà spazzato via dal mercato.

L'edizione del 2019 del Rapporto sull'Internet Society ha denunciato lo strapotere delle piattaforme digitali coniando la definizione di* total service environments. Gig economy *e strapotere delle piattaforme minacciano la libertà democratica in molti Paesi. Che tipo di compliance va adottata per limitare il potere dei "gigacapitalisti" che questi strumenti controllano?

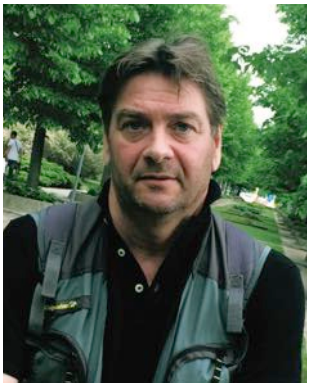
Penso sia uno dei più importanti temi politici del nostro tempo. Non è pensabile che queste imprese si autoregolamentino e tantomeno che lo faccia il "mercato". Non hanno strumenti adatti nemmeno le Autorità. Se si lascia che queste imprese si sviluppino per decenni trascinando con se un infinità di realtà più piccole, si permette che arrivino ad avere fatturati pari a PIL di intere nazioni non si può poi pretendere di intervenire in maniera radicale all'improvviso. Serve una strategia di lungo periodo e lungimirante. Se da un lato infatti è vero che queste piattaforme



presentano profili potenzialmente minacciosi per le libertà democratiche, è pur vero che contribuiscono enormemente alla libertà democratica di ognuno di noi. Aver unito il mondo, permettere a miliardi di persone di entrare in contatto, aver aperto infiniti mercati, aver contribuito alla alfabetizzazione digitale sono solo alcuni degli impatti positivi di queste imprese. Non vanno demonizzate come non vanno idolatrate. Bisogna riuscire a impedire le derive antidemocratiche e gli usi distorti di queste piattaforme anche innalzando la cultura digitale dei cittadini. In questo senso le scelte politiche e il ruolo della scuola (vorrei dire e delle famiglie, se non fosse che spesso i genitori sono più ignoranti digitalmente dei figli) sono le due chiavi di volta su cui serve muoversi. La compliance segue alle scelte politiche ma non penso che serva un modello punitivo. Serve un modello che permetta alle idee di correre veloci senza per questo arrivare a uno strapotere tale da rendere queste imprese indipendenti rispetto al mercato e alle regole. ■



L'importanza strategica delle conformita' (compliance) agli standard nella sicurezza dello spazio cibernetico.



Autore: Francesco Corona

Premessa

Possiamo definire la conformità (Compliant) alla sicurezza informatica come il metodo di gestione del rischio organizzativo allineato con misure di sicurezza e controlli predefiniti su come la riservatezza, l'integrità e la disponibilità dei dati vengono garantite dalle sue procedure tecnico-amministrative. Le normative maggiormente utilizzate in Europa e nei Paese occidentali possono riassumersi nella NIST (National Institute of Standards and Technology) americana e nella NIS (Network Information System) europea, per entrambe possiamo associare l'iniziativa italiana del così detto Framework Nazionale per la Cybersecurity nonché iniziative per la sicurezza delle piattaforme Cloud, il GDPR e l'ISO 27000 che analizzeremo più dettagliatamente. Inoltre metodologie e standard specifici per la sicurezza degli Endpoint ovvero i nodi (dispositivi o network elements) di accesso alle reti che costituiscono il 70% dei bersagli andati a buon fine in attacchi alle organizzazioni pubbliche e private. A tutto questo, deve aggiungersi il nuovo pacchetto di regole europee per la finanza digitale, provvisoriamente approvato e che va sotto il nome di DORA (Digital Operational Resilience Act). Tale pacchetto dovrà coesistere con la NIS europea e con le normative già implementate nell'ambito delle Supply Chains connesse alle attività primarie del business finanziario.

Un corretto approccio metodico alla gestione delle conformità non potrà che aumentare la resilienza delle organizzazioni, dei servizi erogati e delle strutture preposte alla sua attuazione. Nel presente articolo, partendo da una analisi generale delle più diffuse normative e standard di sicurezza, cercheremo di fornire un semplice ma efficace approccio metodico integrato alla gestione delle varie conformità. Tale approccio risulta valido sia per i regolamenti generali attraverso modelli comparativi interoperativi, sia per la sicurezza specifica degli Endpoint attraverso strumenti tecnologici di Governance come ad esempio i SIEM (Security Information and Events Management) e/o piattaforme di Intelligenza Artificiale.

Le normative principali di riferimento [B002]

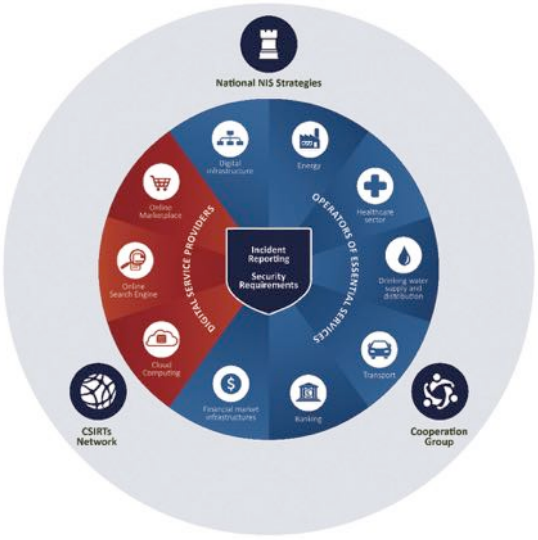
NIST Cybersecurity Framework organizza il suo materiale «core» in cinque funzioni (Identify, Protect, Detect, Respond, Recover) che sono

BIO

Francesco Corona è docente e direttore del master di Hacking ed Ingegneria della Sicurezza presso Link Campus University Rome, già docente a contratto presso la Facoltà di ingegneria gestionale di Roma2 Tor Vergata Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca in ambito MIUR ed attività professionale d'impresa nel settore della sicurezza per conto di primari player nazionali ed internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria.

suddivise in un totale di 23 «categorie». Per ciascuna categoria, definisce una serie di sottocategorie di risultati e controlli di sicurezza informatica, con 108 sottocategorie in tutto utilizzabili per implementare viste particolareggiate in funzione degli obiettivi di sicurezza da raggiungere. Per ogni sottocategoria, la normativa fornisce anche la voce «Risorse informative» che referenziano sezioni specifiche di altri standard di sicurezza delle informazioni, tra cui ISO 27001, COBIT, NIST SP 800-53, ANSI/ISA-62443. NIST viene quindi utilizzata per creare mappe del Cybersecurity Framework più accessibili a piccole e medie imprese. Una declinazione tutta italiana della NIST americana è rappresentata dal **Framework Nazionale per la Cybersecurity** che presenta la stessa identica configurazione di categorie e sotto categorie con alcune varianti migliorative sul Maturity and Severity model rispetto al più semplice modello americano.

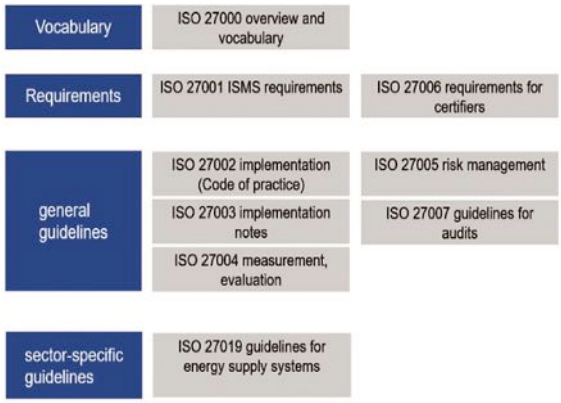
NIS europea. Con il Decreto Legislativo 18 maggio 2018, n.65, pubblicato sulla Gazzetta Ufficiale n. 132 del 9 giugno 2018, l'Italia ha dato attuazione, recependola nell'ordinamento nazionale, alla Direttiva UE 2016/1148, detta Direttiva NIS gestita dall'Agenzia Europea ENISA (European Network and Information Security Agency) ed intesa a definire le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi. Il decreto si applica agli Operatori di Servizi Essenziali (OSE) e ai Fornitori di Servizi Digitali (FSD) ed ai CSIRT (Computer Security Incident Response Teams). Gli OSE sono i soggetti, pubblici e/o privati, che forniscono servizi essenziali per la società e l'economia nei settori dell'energia, dei trasporti, settorembancario e sanitario, delle infrastrutture dei mercati finanziari, della utilities di fornitura e distribuzione di acqua potabile e delle infrastrutture digitali. Gli FSD sono le orgnizzazioni che forniscono servizi di e-commerce, cloud computing, search engine con sede sociale sul territorio nazionale. Gli obblighi previsti per gli FSD non si applicano alle imprese che hanno meno di 50 dipendenti ed un fatturato non superiore ai 10 milioni di Euro. I CSIRT appartenenti alla rete europea di ENISA sono strutture



governative di mezzi e risorse umane che operano per la sicurezza nazionale nel settore cyber in special modo per l'Incident Management, Information Sharing nonchè l'Intelligence sulla minacca. L'Italia si è dotata nell'agosto 2021 dell'ACN (Agenzia per la Cybersicurezza Nazionale) che ha avviato i primi programmi nazionali strutturati di cybersecurity a difesa del sistema paese in fae di completamento.

Il regolamento generale sulla protezione dei dati **GDPR** (General Data Protection Regulation), regolamento UE n. 2016/679, è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato sulla Gazzetta ufficiale dell'Unione Europea (UE) il 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018. Con questo regolamento, ci si propone di rafforzare la protezione dei dati personali di cittadini dell'Unione europea e dei residenti nell'UE, sia all'interno che all'esterno dei confini dell'UE, restituendo ai cittadini il controllo dei propri

dati personali, semplificando il contesto normativo che riguarda gli affari internazionali, unificando e rendendo omogenea la normativa privacy dentro l'UE. Il testo affronta anche il tema dell'esportazione di dati personali al di fuori dell'UE e obbliga tutti i titolari del trattamento dei dati (anche con sede legale fuori dall'UE) che trattano dati di residenti nell'UE ad osservare e adempiere agli obblighi previsti. Dalla sua entrata in vigore, il GDPR ha sostituito i contenuti della direttiva sulla protezione dei dati (Direttiva 95/46/CE) e, in Italia, ha abrogato gli articoli del codice per la protezione dei dati personali (d.lgs. n. 196/2003) con esso incompatibili.



ISO/IEC 27001 ISMS Information Security Management Systems Family of Standards anche nota, in Italia, come famiglia di norme SGSI (Sistemi di Gestione per la Sicurezza delle Informazioni), è uno standard di sicurezza informatica redatto dalla ISO. Raggruppa un insieme di norme internazionali che si prefiggono di proteggere le informazioni che vengono mantenute ed elaborate da un'organizzazione.

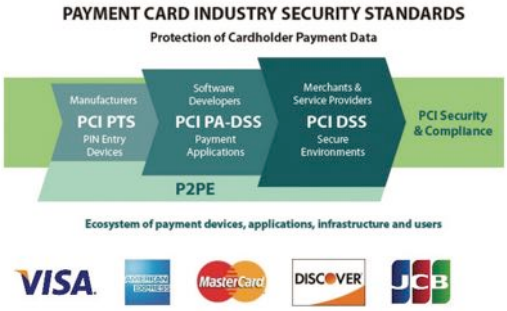
Attraverso questa famiglia di norme, le organizzazioni possono sviluppare ed implementare attraverso certificazioni, un proprio sistema per la gestione della sicurezza informatica per le informazioni finanziarie, la proprietà intellettuale ed i dati dei dipendenti, di clienti o di terzi. Le informazioni vengono protette da possibili attacchi informatici, errori umani, calamità naturali o da qualsiasi altra vulnerabilità che si può presentare durante l'utilizzo di un sistema informatico. Le norme delle serie definiscono i requisiti per creare un SGSI e per coloro che certificano questi sistemi; forniscono una guida per progettare, attuare, mantenere e migliorare un SGSI; esprimono le linee guida nei vari ambiti di utilizzo di un SGSI; valutano la conformità di un SGSI. Tutte le organizzazioni sono incentivate a valutare il rischio informativo, quindi a trattarlo in base alle loro esigenze. Data la natura dinamica del rischio e della sicurezza delle informazioni, il SGSI incorpora attività di miglioramento continuo per rispondere ai cambiamenti delle minacce, delle vulnerabilità o degli impatti degli incidenti. A questo punto non possiamo fare a meno di citare la più ampia normativa ISO sulla gestione dei rischi aziendale e le problematiche di sicurezza nota come ISO 31000 della quale la ISO 27001 è una appendice separata progettata per i Sistemi informativi.

DORA (Digital Operational Resilience Act) approvato a marzo 2022 ma non ancora operativo, costituisce il Pacchetto Europeo di Finanza Digitale che imporrà alle organizzazioni finanziarie di garantire la resilienza di tutte le tecnologie nello stack di erogazione dei servizi e nelle rispettive supply chains loro afferenti facendo della **responsabilità** una milestone fondamentale: **se si possiede una risorsa, allora si è responsabili per essa**. Anche le infrastrutture e le applicazioni di terze parti vengono incluse nell'area di responsabilità dell'organizzazione. Difatti è un avanzamento rispetto alla già nota direttiva dei pagamenti digitali PSD2 di cui abbiamo già discusso in altri articoli tant'è che si parla già della prossima PSD3 come inscindibile da DORA. Tale pacchetto non escluderà pertanto l'utilizzo di tecnologie block-chain da noi già affrontate in [B001]. DORA si applicherà a tutte le imprese finanziarie, sia di investimento che assicurative, nonché alla gestione delle criptovalute e servizi di crowdfunding. DORA coesisterà in modo nativo con la Direttiva NIS già recepita nelle legislazioni nazionali europee e questo risulta essere un grosso vantaggio per la sicurezza nazionale ed europea. Tuttavia un problema serio è stato evidenziato nei vari gruppi di lavoro DORA, in particolare l'esistenza di una difficoltà nel tracciare le dipendenze di terze parti tecnologiche inserite all'interno della catena di valore dei servizi finanziari (Supply Chain), problema superabile solo con una precisa e completa mappatura dei servizi in Cloud dell'istituto finanziario e delle terze parti coinvolte che raccomandiamo possano provvedere ad un serio censimento.

La supervisione di DORA avviene attraverso un Forum di Vigilanza costituito dalle AEV (Autorità Europea di Vigilanza) e dalle autorità nazionali, con la BCE (Banca Centrale Europea) e altre entità come osservatori. Tali Autorities istituiscono la sorveglianza delle istituzioni finanziarie e dei fornitori di tecnologia. Rendere l'innovazione compatibile con la regolamentazione è una delle maggiori sfide competitive nell'Unione Europea e in particolare nel settore finanziario, in piena dinamica di trasformazione con l'arrivo di blockchain e AI associate ai nuovi servizi che ribadiamo dovranno essere necessariamente censiti nelle loro essenze digitali.

Regulatory compliance gestite da SIEM

In un precedente articolo [B006] abbiamo discusso del fatto che un SIEM al quale releghiamo funzioni di Security Governance in special modo per il monitoraggio degli Endpoint attraverso agents, dovrà sempre più soddisfare delle compliance ad ampio spettro verso MITRE, NIST 800-53, PCI DSS, TSC, HIPAA, GDPR, che andremo ad esplicitare brevemente di seguito.



PCI DSS. L'Ente responsabile degli standard di protezione PCI (PCC Security Standards Council) è costantemente al lavoro per monitorare le minacce e potenziare gli strumenti del settore dei pagamenti elettronici. Grazie al miglioramento continuo, agli standard di protezione PCI e grazie alla formazione di professionisti della sicurezza, l'Ente mantiene un alto livello globale di sicurezza verso i clienti del mondo bancario evitando compromissione dei dati della carta di pagamento.

TSC. In ottica SOC-SIEM (SOC=Security Operational Center), nei così detti Trust Services Criteria (TSC) dell'AICPA. I SOC Response Team devono disporre di tutti i controlli applicabili ed essere in grado di fornire tempestivamente prove dell'efficacia di tali controlli. I criteri per i servizi fiduciari (TSC) necessari ad ottenere la certificazione SOC 2 e quindi soddisfare i più recenti standard del framework, sono relativi a controlli che le organizzazioni devono implementare nell'infrastruttura IT. Le cinque categorie di criteri di controllo sono riportate in figura. Va da sé che uno strumento come il SIEM, in grado di supportare tali controlli, faciliterà l'approccio ad un SOC certificato anche e soprattutto in ottica CLOUD.

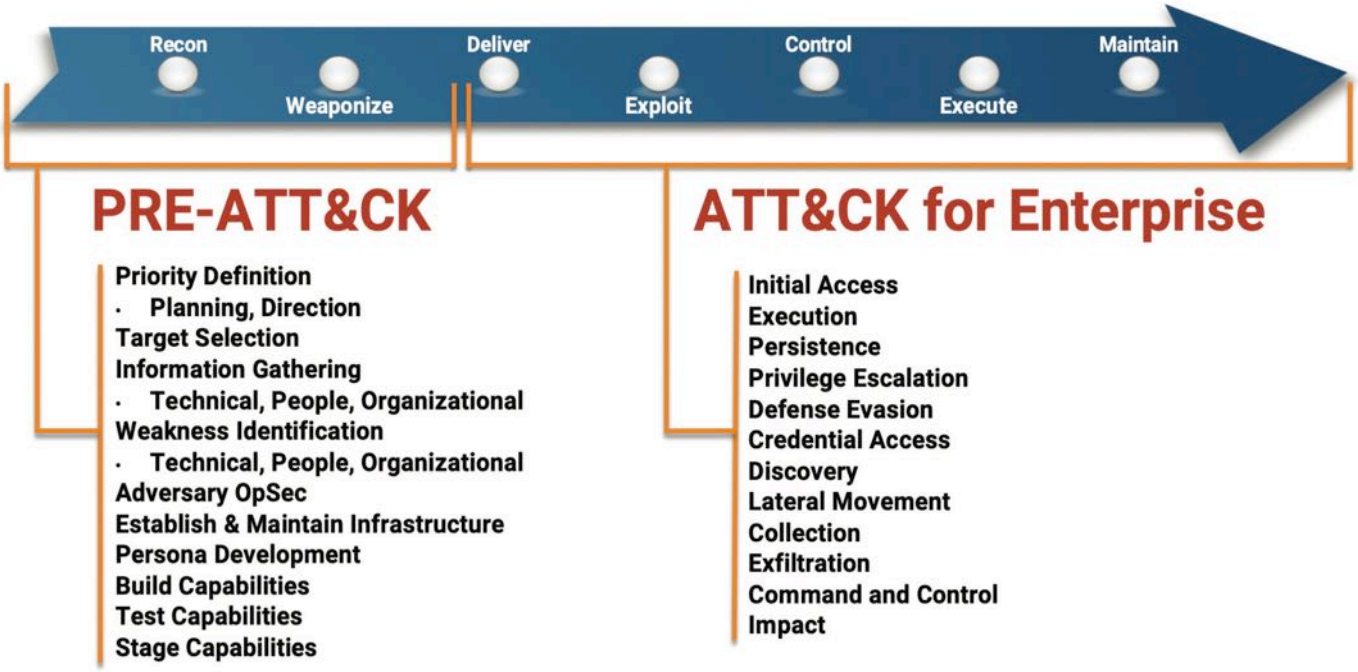
HIPAA. L'Health Insurance Portability and Accountability Act (HIPAA) è una legge federale degli Stati Uniti che definisce i requisiti per il trattamento dei dati sanitari protetti dei privati. La compliance HIPAA è regolamentata dall'HHS (Department of Health and Human Services) e l'OCR (Office for Civil Rights) che ha il compito di farla rispettare. L'HIPAA compliance deve essere parte integrante della cultura aziendale di ogni entità che opera nel settore sanitario al fine di garantire la privacy, la sicurezza e l'integrità dei dati sanitari protetti.

GDPR. General Data Protection Regulation (Regolamento Generale sulla Protezione dei Dati), ovvero il Regolamento Europeo NIS 2016/679 che ribadiamo chiarisce come i dati personali debbano essere trattati, raccolti, utilizzati, protetti e condivisi. Un SIEM che consenta di poter gestire adeguatamente dei report periodici che soddisfano la normativa GDPR/ISO 27001/Framework NIST è da preferire rispetto ad altre soluzioni.

NIST 800-53. Costituisce uno standard di conformità alla sicurezza creato dal Dipartimento del Commercio degli Stati Uniti e dal National Institute of Standards in Technology in risposta alle capacità tecnologiche in rapido sviluppo di soggetti avversari. Il NIST 800-53 è obbligatorio per tutti i sistemi informativi federali degli Stati Uniti ad eccezione di quelli relativi alla sicurezza nazionale. Le sue linee guida possono essere adottate da qualsiasi organizzazione che gestisca un sistema informativo con dati sensibili o regolamentati. Fornisce un catalogo di controlli sulla privacy e sulla sicurezza per la protezione da una varietà di minacce, dai disastri naturali agli attacchi ostili.

MITRE framework

MITRE è un framework che implementa una tipica Cybersecurity Kill Chain a 7 step, messa in relazione con specifiche Tecniche Tattiche e Procedure (TTP) necessarie ad indentificare e studiare gli attacchi cyber tenendo conto anche dei movimenti laterali di un avversario. Originariamente pensato con due ambienti fondamentali: PRE-ATT&CK e ATT&CK nel 2020, MITRE ha pubblicato ATT&CK v8. Questa versione rimuove



il dominio PRE-ATT&CK dalla chain, sostituendo il suo ambito con due nuove tattiche in Enterprise ATT&CK Reconnaissance e Resource Development. La struttura di ATT&CK consiste in 14 Tattiche che delineano il **"perché"** dell'approccio di un attaccante e quindi rappresentano l'obiettivo del suo attacco. Le tecniche ATT&CK sono del tipo **"Come"** un avversario raggiunge un determinato obiettivo. Le **Procedure** sono i passaggi specifici che un avversario compie per eseguire e implementare una tecnica. Queste tecniche rappresentano i vari modi in cui un cyber-attack può raggiungere obiettivi target. Questo approccio, implementato in un SIEM fornisce una soluzione completa e molto economica per prevenire e mitigare minacce alla sicurezza informatica.

Un esempio di modello cross reference

Le normative esposte possono essere adottate anche singolarmente dalle organizzazioni coinvolte e quindi per realizzare un modello integrato tra differenti normative e standardizzazioni è necessario metterle in relazione attraverso tabelle di Cross Reference equiparando gli articoli corrispondenti nelle diverse normative e standard e comunque l'utilizzo di SIEM di nuova generazione facilitano in questo approccio.

Nella tabella sottostante sono ad esempio posti a confronto gli articoli del GDPR con quelli della ISO27001 e con quelli della NIST-Framework Nazionale Cybersecurity in un lavoro di ricerca svolto con i miei studenti del Master in Cybersecurity[B004]

	GDPR	Iso 27001:2013	Framework cybersecurity
Security Policy	Art 32, Art 24	A.5	GV-1
Ruoli e responsabilità	Art 32 (4)	A.6.1.1	AM-6, GV-2, AT-2, AT-3, AT-4, AT-5, DP-1, CO-1,
Politica controllo accessi	Art 5.1 (c)	A.9.1.1	DS-5,
Inventario degli asset	Art 24, Art 32	A 8	AM-1, AM-2, AM-5, DS-3,
Responsabilità e procedure operative	Art 24, Art 32	A.12.1	BE-4, DS-7, IP-1, IP-3,
Relazioni con i fornitori	Art 28, Art 32	A.15	BE-1, MA-2, CM-6,
Gestione incidenti di sicurezza	Art 4 (12), Art 33, Art 34	A.16	IP-8, IP-9, AE-2, DP-4, DP-5 RP-1, CO-1, CO-2, CO-3, AN-1 AN-2, AN-3, AN-4 MI-1, MI-2, IM-1, RP-1,
Business continuity	Art 24, Art 32	A 17	BE-5, IP-4, IP-9, IP-10
Risorse umane	Art 32 (4)	A 7	GV-2, AT-1, AT-2, AT-3, AT-4, AT-5, DS-5, IP-11,
Formazione e consapevolezza	Art 32 (4)	A 7.2.2	AT-1, AT-2, AT-3, AT-4, AT-5,
Controllo accessi	Art 32	A 9	AC-1, AC-4, DS-5, PT-3,
Monitoraggio e gestione dei log	Art 32	A.12.4	PT-1, CM-3, AN-1
Sicurezza delle attività operative	Art 32	A.12	BE-4, RA-1, RA-5, DS-4, DS-6, DA-7, IP-1, IP-3, IP-4,IP-12, PT-1, CM-3, CM-4, CM-5, CM-8, AN-1, MI-2, MI-3,

TAB.1 – Cross Reference | Descrizione | GDPR | ISO 27001 | Framework Nazionale

Risulta evidente che procedendo con la consultazione di questi riferimenti incrociati (facilmente implementabile a livello software) è possibile avere sotto controllo tutti i processi di certificazione e le normative obbligatorie nonché misurare l'adeguamento da una ad un'altra normativa mantenendo la garanzia del rispetto degli obblighi di legge.[B004]

Ricordiamo al lettore che Il 70% degli attacchi informatici andati a buon fine ha origine dall'Endpoint, ovvero dai dispositivi che si connettono direttamente ad Internet. L'Endpoint è diventato quindi l'epicentro della

minaccia. Difenderlo con soluzioni avanzate che mappino il dominio di tutte le normative in ambito Cyber è la migliore strada per aumentare la resilienza delle organizzazioni.

Garantire la conformita'

Garantire la conformità alla sicurezza informatica è ora più che mai essenziale e se non si attua tale processo, è possibile ingenerare gravissime perdite non solo economiche ma anche reputazionali. Abbiamo osservato che esistono moltissimi controlli e numerosi requisiti imposti da più organismi di regolamentazione e gruppi industriali privati. Inoltre, le organizzazioni multinazionali devono affrontare l'ulteriore e importante sfida di dover aderire a una molteplicità di normative globali e locali di diverse giurisdizioni e autorità di regolamentazione in differenti aree geografiche. La sfida continuerà a crescere con l'aumento della frequenza, dei volumi e della gravità degli attacchi, il che porterà gli standard e le organizzazioni governative a rendere i requisiti di conformità ancora più severi. Le aziende che risultano non conformi devono affrontare inoltre potenziali multe e sanzioni, per non parlare del danno d'immagine. L'unico modo per ridurre il rischio di violazione, mitigare i costi associati di risposta e ripristino, evitare le multe salate e i danni alla continuità del business garantendo contestualmente l'equità del marchio risulta essere quello di assicurarsi che la protezione sia solida e che tutti aderiscano alla conformità alla sicurezza informatica. In un panorama di attacchi in continua evoluzione bisogna tener presente che le minacce alla sicurezza informatica emergono e cambiano molto rapidamente, rendendo molto difficile per le organizzazioni e per le autorità di regolamentazione essere "sul pezzo".

Competere con la sofisticatezza di chi progetta gli attacchi è una sfida ancora più grande in quando è necessario stare continuamente al passo con le tecnologie in rapida evoluzione. Per garantire la conformità alle norme di sicurezza è dunque necessario disporre di competenze interne ampie e variegate, che includono una conoscenza approfondita di molteplici normative, minacce informatiche, processi, controlli e tecnologie di sicurezza informatica. Senza una tale vasta esperienza, è impossibile creare un programma efficace e completo ed eseguire accuratamente l'ambito, il monitoraggio e la riparazione necessari per garantire la sicurezza e dimostrare la conformità. Testare regolarmente i programmi di sicurezza è vitale. Questo è il motivo per cui è essenziale e persino strategico garantire che i fornitori di soluzioni e servizi che supportano, implementano e mantengono i programmi, nonché i controlli e le tecnologie di sicurezza informatica dell'organizzazione, siano tutti certificati per SOC 2, GDPR, HIPPA e PCI DSS, ISO 22301 e ISO/IEC 27001. La ISO 22301 è importante per essere l'applicabilità per simulazioni di hacking, indagini forensi, intelligence informatica, formazione e costruzione e gestione di centri operativi di sicurezza. Tuttavia è importante notare che la protezione dell'organizzazione da un attacco cyber richiede di andare oltre gli standard di conformità del settore, oltre le tecnologie di Governance, oltre le certificazioni, oltre i limiti tecnico-amministrativi imposti dalle tecnologie e questo significa disporre di un Responce Team inteso come Capitale Umano dell'Impresa, certamente ben addestrato, ma con competenze superiori in termini di **percezione avanzata della Situation Awareness** in grado di superare dal punto di vista umano l'elemento tecnologico e gli stessi approcci basati su tecniche AI.

Riferimenti bibliografici

[B001] https://www.cybertrends.it/psd2-e-nuove-monete-virtuali/

[B002] per le definizione delle normative si faccia riferimento all'enciclopedia Wikipedia

[B003] https://www.consilium.europa.eu/it/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

[B004] GDPR Gestione Privacy by design per PMI e PA. Tesi Master in Cybersecurity – Link Campus University A.A.2017/18 - G.Pensili, S.Massaini, Relatore prof. F.Corona.

[B005] Infrastrutture Critiche Finanziarie. I nuovi modelli. Protezione e simulazione (cybertrends.it)

[B006] Un approccio Open source alla gestione delle vulnerabilità - Rivista Cybersecurity Trends (cybertrends.it) https://www.cybertrends.it/un-approccio-open-source-alla-gestione-delle-vulnerabilita/ ■

Sicurezza e compliance integrata, binomio inscindibile nel nuovo capitalismo di "comunità".

Autore: Lucio Gioacchino Insinga

Riflettere oggi su compliance e sicurezza, significa acquisire la consapevolezza di che cosa vuol dire "abitare la complessità". Siamo dentro una "comunità di destino", fatta di interdipendenze sempre più difficili da dipanare. Per fare impresa non basta poter disporre di un elevato corredo di conoscenze tecnico-giuridiche ed economico finanziarie. Serve un *"quid"*, un "di più" misurabile nella capacità ermeneutica di lettura del tempo presente, abilità che l'imprenditore deve imparare ad affinare, perché da essa dipende ogni *chances* di successo. Solo se collocata in quest'ottica trasversale il binomio compliance e sicurezza può, se ben vissuto e attuato creare valore, non risolvendosi unicamente in un freddo adempimento burocratico, che l'imprenditore deve subire come un costo, o forse ancor peggio come un peso intollerabile. Parare di sicurezza e delle norme che la rendono possibile, ci riconduce subito alla responsabilità come termine critico. Non occorre, anche se rende l'idea scomodare il dualismo classico *nomos* vs *ethos*, rappresentato dalle figure mitiche di Creonte e Antigone, capaci di esprimere la tensione essenziale tra imperio della legge che definisce il campo della liceità e la dimensione del dover essere, che chiama in causa l'essere individuale.

Victorine Angélique Genève-Rumilly, La mort d'Antigone, Primi del Novecento (© Museo di Grenoble, France).

Sono almeno tre i livelli di analisi che vanno presi in esame per comprendere la compliance oggi: giuridico se ci si sofferma sulle parti dedicate allo sviluppo e all'inquadramento normativo; teoretico-filosofico, che vuol dire capacità di lettura critica del presente; strategico, perché non è in gioco solo l'adempimento della norma in questa delicata fase di trasformazione, ma la tutela del core business in tutte le sue articolazioni insieme all'indirizzo più generale che imprese grandi e piccole, dovranno imboccare nella dinamica della competizione, giocata ormai tutta su scala globale.

La "messa in regola" non basta

È evidente che siamo di fronte a un cambio di passo: non possiamo soffermarci sulla "messa in regola", statica ritualità di un tempo che non esiste più, l'asse della valutazione dell'efficacia ed efficienza della *performance* aziendale va ruotata sugli impatti che ogni scelta economica-finanziaria proietta sugli *stakeholders* e sulla comunità di interessi verso cui si rivolgono le attività del business. Lo sviluppo di un doppio legame tra azienda e territorio è un aspetto centrale, insieme alla necessità di sviluppare una "cultura del confronto", intersettoriale (tra il settore pubblico e privato) e infrasettoriale (tra grandi player e la piccola impresa) destinata a segnare un diverso assetto di sistema, realizzabile nella dinamica di una vera e propria "rivoluzione copernicana" imperniata sul nuovo paradigma di un *"capitalismo comunitario"* (cfr Roberto Panzarani, *Il nuovo paradigma (ed. Lupetti)*.

Il case history della Società Diddi Dino & figli può essere utile per comprendere il tempo nuovo che stiamo attraversando, perché afferma un principio molto netto, che vale la pena esplicitare: *"vogliamo affermare una cultura orientata all'esigenza di correttezza e trasparenza nella conduzione degli affari"*. Nella sintesi dell'enunciato è leggibile un manifesto programmatico che contiene una molteplicità di aspetti che sono in questo momento al centro del dibattito pubblico: la trasparenza negli affari come motore del business e non come suo ostacolo; l'etica che deve tornare a fare da riferimento, quale *"nome nuovo da dare al pensiero"*, per usare la definizione di Edgar Morin, oggi centenario sociologo francese primo teorico fondatore della complessità, la sicurezza che è figlia del rigore e della trasparenza con cui le attività di business vengono sviluppate.

Transizione tecnologica e cultura del diritto

Le aziende sono attualmente poste di fronte a una duplice inaggirabile priorità: "transizione ambientale" e "tecnologica". Le azioni messe in atto dalla Diddi, dalla formulazione del codice etico, alla messa a punto del sistema sanzionatorio, alla definizione di un assetto organizzativo idoneo alla prevenzione dei reati vanno nella giusta direzione, perché frutto di una visione includente che fa ben comprendere come il lavoro di mappatura delle vulnerabilità, di rafforzamento delle strategie di cyber security e di prevenzione dei reati, debbano tendere

BIO

Dottore Commercialista - Revisore Legale dei Conti e Innovation Manager certificato Bureau Veritas, vanta oltre 25 di esperienza manageriale nella conduzione d imprese e nella gestione di operazioni straordinarie. E' stato premiato con menzione dell'A.I.F (Associazione Formatori Italiani, per il progetto Ethical Value project per la diffusione dei codici etici e del modello di controllo previsto dal. D.Lgs. 231/2001, nelle PMI. In tale materia è autore di due libri: *"La responsabilità sociale. Le PMI alla prova del modello 231(Plenum Editore 2017) e la Compliance Integrata per l'attuazione del modello 231 (Princeri Editore 2022)*. Curioso delle nuove tecnologie e delle operazioni finanziarie correlate è il primo professionista che porta al successo un'operazione in Italia di un aumento di capitale in Bitcon e, sempre per *Primiceri editore è autore deli libro Come finanziare l'impresa. Attori strumenti e metodi per potenziare la crescita* Nel 2016 fonda Management Capital Partner s.r.l. che oggi all'attività di advisor ha associato quella di BUSINESS ANGEL e ciò gli ha consentito di investire in 5 società con l'innovativa formula del work for equity che permette alle startup di poter beneficiare dell'esperienza di un manager a costo zero. E' attivamente presente in tutti i cda di dette società.

a coinvolgere il corpus dell'azienda in tutte le sue componenti. Nessun discorso sulle regole può essere fatto se istituzioni e imprese continuano a mostrarsi incapaci ad attuare la logica della rete, mantenendo degli steccati che di fatto frenano ogni possibilità di crescita. Alla "R" di "Resilienza" concetto su cui si sta giustamente insistendo in questa fase, va aggiunta la "R" di "Riscatto", perché implica la duplice dimensione dell'etica e dell'economia, quali parametri che vanno oltre il PIL ricomprendendo la categoria dello sviluppo umano.

Le "4E"

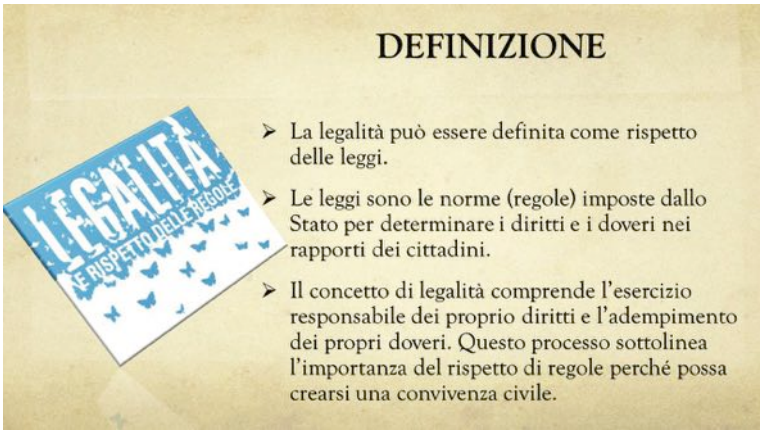
Adottando la politica delle «4E» *(Efficacia, efficienza, economicità ed etica)* e procedendo con la creazione di uno «SCI», la società Diddi Dino & Figli S.r.l. ha voluto dare prova alla propria organizzazione, di essere in grado di conciliare esigenze legislative, organizzative, operative,

economiche e funzionali, evitando ridondanze, duplicazioni e costose burocratizzazioni, a vantaggio dell'adozione di una reale *Compliance integrata*.

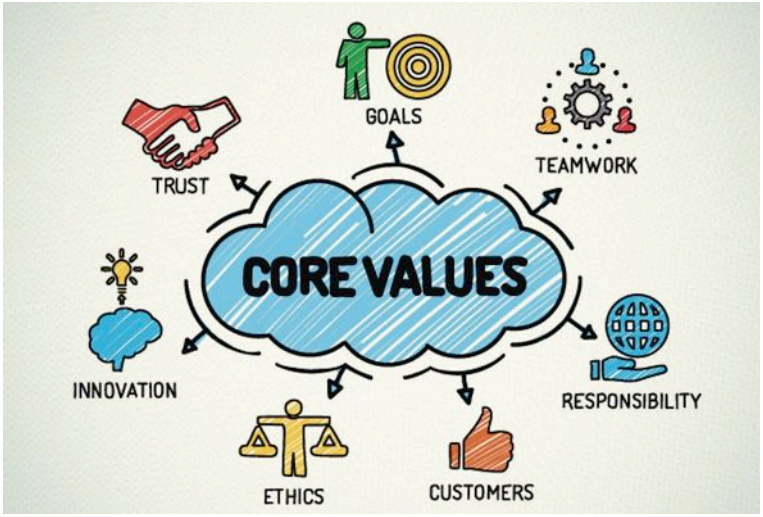
Giova a questo proposito ricordare che il modello previsto dal d.lgs. 231/2001, non è riservato soltanto alle aziende di medie e grandi dimensioni che possono contare su *budget* di spesa proporzionati alla loro dimensione organizzativa; alcuni aspetti organizzativi che attengono alle PMI dimostrano il contrario. Il sistema di gestione dei rischi aziendali, può attecchire, infatti, meglio dove risiede un limitato numero di soggetti apicali ed un numero limitato di soggetti subordinati, nella cui sfera la condivisione dei protocolli, la modifica dei processi e delle soluzioni adottabili, operano con una metrica snella e di rapida applicazione. Inoltre, una gestione operativa del vertice è, essa stessa, garanzia della regola introdotta rivelandosi un esempio applicabile in molte realtà imprenditoriali. D'altra parte, parrebbe palesemente illegittima, la norma che obbliga un imprenditore a dotarsi di risorse esterne indipendenti ed autonome a presidio dei singoli sistemi, se ciò economicamente non è sostenibile.

In cambio di questa «autonomia e libertà organizzativa» l'altra faccia della medaglia è rappresentata dal fatto che risultando controllore e controllato, l'imprenditore in caso di sinistro, anche penalmente rilevante «non poteva non sapere». Quest'ultima considerazione fa comprendere molto bene cosa vuol dire rischio e responsabilità nella società complessa, introducendo un ulteriore duplice livello di analisi.

Primo: l'importanza delle regole e più in generale la cultura del diritto, sono il pavimento di quel contratto sociale che trova il suo riflesso più alto e diretto nella nostra Costituzionale.



Il secondo aspetto attiene al rigore con cui viene affrontato il delicato binomio etica ed economia, cui si faceva prima riferimento, in un momento in cui si parla molto di neoumanesimo digitale, i principi valoriali di un modello di sviluppo economico non possono prescindere dalla centralità della persona, dalla solidarietà, dalla promozione delle relazioni, dal rispetto dei diritti universali.



Senza queste componenti non ci può essere compliance, non esiste sicurezza, ma nemmeno la possibilità di definire il contratto sociale posto a tutela della civile convivenza di popoli, nazioni, civiltà. ■

La "simulazione immersiva": un seminario del Cert Star dello scorso luglio ha aperto un dibattito con le aziende top del settore.

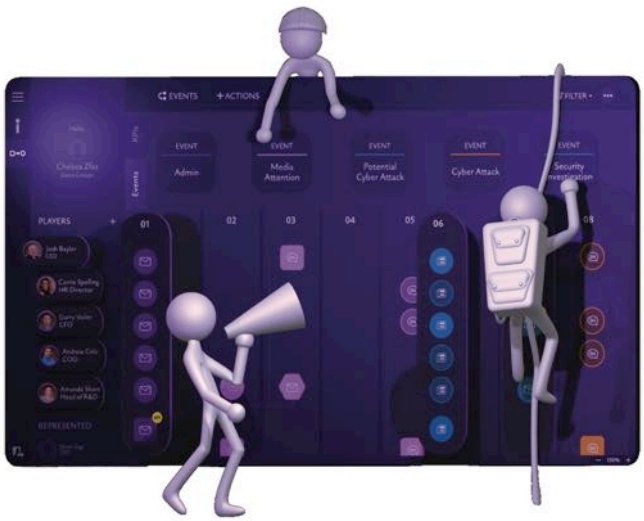
Intervista VIP a Iljana Mari.

Autore: Massimiliano Cannata

Il ***Cert Star*** che si è tenuto nello scorso mese di luglio, curato da *Obiectivo Technology Srl,* ha avuto come focus la gestione di un incidente di cyber security attraverso la realizzazione di una *"simulazione digitale immersiva"* applicata al delicato ambito della cyber security. Ne abbiamo parlato con Iljana Mari, *Sales e Operation Manager* della stessa azienda.

Quali sono le peculiarità di questo servizio che ha riscosso l'interesse di aziende "top", che si muovono in svariati ambiti di business?

Il servizio proposto da Obiectivo in occasione dell'evento Cert Star è basato sulla piattaforma di simulazione digitale immersiva **Cyber Jumanji**. **Cyber Jumanji** consente di raggiungere molteplici obiettivi, come esercitare il personale coinvolto nella gestione delle emergenze di information e cyber security (ma non limitatamente a queste), verificare completezza ed



adeguatezza delle procedure definite, verificare nuove procedure prima di renderle operative. La caratteristica della piattaforma è di mettere alla prova le capacità decisionali e di reazione in emergenza, riuscendo a simulare la pressione e lo stress a cui si è sottoposti nella realtà. La piattaforma consente inoltre di simulare l'interazione con ruoli aziendali e con persone esterne all'organizzazione che non possono essere coinvolti in sistemi di simulazione più tradizionali. Ad esempio, è possibile simulare la presenza con organi di stampa, top management, forze dell'ordine, enti regolatori che possono inviare richieste, fornire informazioni, mettere stress…. Esattamente come accade nella realtà!

Le imprese hanno sempre più bisogno di migliorare le loro capacità di risposta rispetto ad attacchi cyber che mettono sotto scacco reti e sistemi e che, come l'attualità dimostra ampiamente, molto spesso sono in grado di insinuarsi in ambiti molto delicati per la vita collettiva: sanità, infrastrutture critiche, TLC, vertici istituzionali, fino ai partiti politici. La piattaforma che avete presentato può aiutare ad affrontare queste situazioni che potremmo definire al "limite"?

Una piattaforma di simulazione immersiva è una vera innovazione rispetto all'approccio standard utilizzato oggi per la gestione di questi temi, poiché permette non soltanto di simulare la realtà in maniera veramente realistica, ma anche verificare quegli aspetti che sono tipicamente trascurati in questi casi, come ad esempio la parte organizzativa e di processo che sono invece fondamentali per l'organizzazione nella corretta gestione di un evento di crisi.

Per architettare e realizzare simulazioni così sofisticate, quali competenze avete messo in campo?

Il team di gestione delle simulazioni è costituito da nostri consulenti senior che hanno lunga esperienza in ambito information & cyber security e nella definizione dei piani di emergenza basati sugli standard di riferimento di settore. Il team collabora con il Cliente per l'implementazione del processo di gestione delle emergenze. La collaborazione con il Cliente viene richiesta anche per la definizione delle caratteristiche specifiche dello scenario (ad esempio: attacco DDOS ad un sistema, attacco ransomware ma anche terremoti, incendi, allagamenti totali o parziali, ecc) da simulare che non deve essere reso noto ai partecipanti alla simulazione per non perdere "l'effetto sorpresa"

Possiamo soffermarci sui benefici procedurali e organizzativi che le aziende possono trarre dalla pratica razionale e sistematica della simulazione?

Come detto precedentemente questo servizio è una vera rivoluzione ed il progetto si pone un triplice obiettivo. In prima battuta quello di verificare l'adeguatezza della procedura end to end e la sua applicabilità in contesto operativo e definirne un'eventuale ottimizzazione della stessa. In secondo luogo, la possibilità di evidenziare eventuali criticità operative ed organizzative e definire piani di remediation puntuali e customizzati. Infine, aspetto non meno importante, la creazione di un'esperienza di apprendimento dinamica che tenga costantemente formato il team operativo.

La capacità decisionale fa la differenza. Lo si sta vedendo nei contesti più difficili, basti pensare alla guerra che è arrivata nel cuore dell'Europa, alle porte di casa nostra, una gravissima "social war" che, come ha detto molto bene il Garante della privacy, si è ben presto trasformata in "cyber war". La simulazione immersiva, genera "stress reale" riesce ad "allenare" il management nell'assunzione delle responsabilità e nel corretto dosaggio di tutte quelle relazioni con attori terzi, che sono indispensabili se si vogliono governare le situazioni di emergenza?

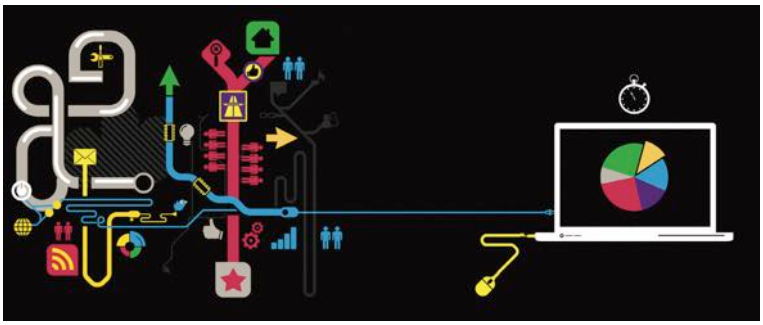
Uno degli ambiti maggiormente coinvolti in questo tipo di attività è proprio quello del processo decisionale. **La simulazione immersiva** consente di rinforzare il livello di preparazione e la capacità reattiva perché è in grado di valutare la capacità di risposta e quella decisionale degli attori coinvolti, il livello della conoscenza che hanno delle procedure interne e la loro capacità di esercirle correttamente, nonché la capacità di reagire sotto stress. In questo modo i partecipanti alle simulazioni sviluppano competenze, capacità di reazione ed intuizioni rilevanti ai fini del raggiungimento dell'obiettivo, risultato questo che sarebbe difficilmente

raggiungibile con altre metodologie più convenzionali. Punto di forza è la possibilità di testare la capacità decisionale e di reazione in quelle situazioni dove lo scenario non è immediatamente classificabile. Ad esempio, nel caso in cui si verifichi il crollo di un immobile a seguito di un terremoto, la situazione si presenta alquanto chiara: è necessario trovare una sede alternativa. Ma cosa succede in caso magari di allagamento di una parte dell'immobile? Il piano di emergenza deve essere attivato oppure no? In questi casi la capacità di analisi e di decisione è fondamentale per il business aziendale, ma troppo spesso i comitati di gestione non sono addestrati a fare

le valutazioni del caso. Con **Cyber Jumanji** invece questa cosa è possibile e viene molto apprezzata.

Proliferano i test dedicati alla* business continuity *presenti sul mercato. Il modello progettato da Obiectivo presenta canoni di indubbia originalità. Possiamo spiegare perché?

L'originalità del servizio sta proprio nella sua caratteristica principale e cioè la possibilità di simulare potenziali situazioni di disastro, in un contesto che possiamo definire "real time - simulato" al fine di preparare l'organizzazione ad affrontare il "real time - reale". Questa è appunto come già precisato in precedenza una vera "rivoluzione" in questo settore rispetto alle attività convenzionali, perché permette non soltanto di simulare la realtà in maniera veramente realistica ed offre la possibilità dello sviluppo delle competenze a cui facevo riferimento poc'anzi, ma permette anche di oggettivare i risultati della simulazione e quindi di definire puntuali remediation plan.



Tra i benefici attesi dalla pratica della simulazione, viene indicata la comunicazione. Sicurezza e comunicazione in che rapporto stanno?

La comunicazione è fondamentale in questo tipo di situazioni. Deve essere tempestiva, esaustiva, ma soprattutto efficace e coordinata per permettere un corretto flusso delle informazioni all'interno ma anche all'esterno dell'organizzazione. Un coretto flusso di informazioni può velocizzare il ripristino dello stato di normalità e può sicuramente prevenire fuga di informazioni scorrette verso l'esterno che possono creare significanti danni d'immagine all'azienda. La tempestività d'altro canto è sicuramente un elemento altrettanto rilevante nel gestire la situazione e l'emergenza nel miglior modo possibile e ove possibile anticipare possibili reazioni a catena disastrose mettendo in campo le azioni correttive in tempi brevi.

In questo frastagliato orizzonte, i giornalisti che ruolo devono svolgere quando c'è da affrontare e raccontare uno scenario critico?

Per quanto riguarda il rapporto con la stampa, questo di solito è un punto dolente delle simulazioni…. Abbiamo infatti notato che molte aziende non hanno piani di comunicazione verso l'esterno in situazioni di disastro, e spesso i partecipanti rispondono senza avere titolo a giornalisti (simulati) che richiedono notizie. Questo è scorretto oltre che pericoloso. In caso di disastro/emergenza la comunicazione verso l'esterno deve essere chiara e coordinata: spargere notizie in modo non coordinato né controllato può generare più danni dell'incidente stesso.

Sappiamo che la sicurezza assoluta non esiste, è piuttosto un "tendere verso...". Il rischio è, infatti, contessuto al nostro percorso esistenziale, risultando percepibile sia nella prospettiva umana che lavorativa. Di quali strumenti e conoscenze dovremo dotarci per rendere se non altro "sostenibile" quel senso di paura che attraversa le nostre vite, che è poi, come ha osservato Ulrich Beck, un tratto distintivo della contemporaneità?

BIO

Iljana è Sales & Operation Manager di Obiectivo Technology Srl. Si occupa dello sviluppo commerciale e realizzazione delle sales proposition. Cura della continua crescita delle relazioni con i Clienti attraverso la creazione di rapporti di fiducia e competenze professionali. Coordina la delivery di progetti complessi e gruppi di lavoro articolati.
È stata in precedenza Direttore di sede e Account manager presso Consulcesi Group, il più grande network in Europa dedicato ai professionisti della Sanità.

La risposta sintetica potrebbe essere "consapevolezza". Consapevolezza vuol dire essere formati ed informati circa i rischi che si corrono nel "mondo virtuale" che virtuale ormai non è più tanto. Se le persone sapessero che una password come "qwerty" può essere indovinata in millesimi di secondo probabilmente la cambierebbero, salvaguardando la sicurezza dei propri conti online, dell'accesso alla propria email e – più in generale – della propria identità digitale. Sembrano banalità, ma ancora nel 2022 ci troviamo a combattere con gli stessi problemi che avevamo 20 anni fa, e questo a causa della scarsa preparazione e formazione all'uso della tecnologia. Dal punto di vista aziendale, la questione cambia poco: manca consapevolezza! Lo abbiamo visto più volte nel corso della nostra attività nelle aziende: i collaboratori consapevoli sono di grande aiuto nel creare una barriera forte rispetto ai rischi cyber ed accettano più volentieri di modificare la propria prassi lavorativa per cambiare, ad esempio,

una password più spesso. Anche nella gestione delle emergenze questo ragionamento vale al 100%: persone formate ed informate (e quindi consapevoli) reagiscono con metodo e con chiarezza di intenti. E questo, ai fini dei risultati, fa una differenza fondamentale! ■

Rispetto delle regole, sicurezza e innovazione. L'adozione di una compliance 2.0 rende tutto possibile.

Intervista al team CSM di Yoroi.

Autore: Massimiliano Cannata

CSM (Customer Success Management) è la struttura di Yoroi costituita quest'anno che si caratterizza per l'utilizzazione di risorse con skill tecnico molto avanzato che presidiano tematiche trasversali, in virtù della profonda esperienza/attitudine acquisita nella gestione dei rapporti diretti con il Cliente. Le risposte alle domande che seguono non sono attribuibili a un unico interlocutore, in quanto sintesi di un confronto a più voci realizzato con tutto il gruppo di lavoro. Nella discussione emerge l'interessante declinazione di un service management che assume la connotazione 2.0.

Compliance: da adempimento a opportunità. Cosa occorre fare per compiere un "salto", non solo organizzativo, ma logico- culturale nelle imprese che devono affrontare il mercato in un contesto sempre più difficile?

La Compliance incarna da sempre, per le aziende, una sorta di "tornado ricorrente" che, con estrema freddezza e violenza travolge e sconvolge l'assetto interno penalizzando la prediletta operatività. Questo fa sì che la percezione delle indicazioni provenienti da Leggi, Regolamenti e Direttive si traduca costantemente in attività statiche, e spesso difficili da interpretare e "scaricare a terra", che l'Azienda, nel suo complesso, subisce senza alcuna personalizzazione. La vera sfida sta nel dare un significato differente ai requisiti "canonici" trasformando quelle indicazioni statiche e rigide, che da questi discendono, in regole dinamiche e adattabili al proprio contesto, applicando un processo di "assorbimento attivo e di contestualizzazione personalizzata".

Quali sono i vantaggi per l'azienda generati da questo cambio di atteggiamento?

L'adozione di una diversa "vista" permette all'Azienda di rivedere il proprio assetto interno con una "bussola autorevole e insindacabile" che indirizza le principali azioni richieste in modo oggettivo, così individuando il quadrante dei livelli attesi entro cui posizionarsi, affiancato da interventi di carattere soggettivo che vedono impegnata tutta la popolazione aziendale in una rivisitazione dei propri processi e delle proprie risorse. La consapevolezza di essere parte di un progetto di reingegnerizzazione aziendale, dove ciascuno può contribuire portando valore aggiunto alla fase di personalizzazione, renderà quelle stesse Norme, da sempre recepite come adempimento necessario e onerosa attività ricorsiva, in opportunità di scomporre, approfondire e reinventare la propria realtà rendendola più simile a quella che si vorrebbe.

Norme ed esigenze di business devono trovare un momento di conciliazione in ambienti e organizzazioni complesse. Quali strumenti vanno messi in campo e quali competenze occorrono per attuare questa "sintesi operativa" decisiva per migliorare gli standard di competitività?

Ogni volta che si parla di Compliance e di obblighi normativi la prima preoccupazione delle Aziende è quella di non penalizzare operatività e priorità di business per attività che, secondo la comune percezione, sono considerate come un costo e per nulla un investimento. Eppure, bisognerebbe ricordare che l'aderenza ai requisiti cogenti è presupposto e condizione necessaria all'esercizio del business, anzi, può esserne altresì moltiplicatore di valore se si considera che il rating di legalità, per esempio, attribuisce consistenti vantaggi proprio per l'accesso a strumenti al servizio del business. Le stesse certificazioni aziendali, in ambito Sistemi di Gestione, sono abilitanti per l'aggiudicazione di appalti e gare, senza contare che sono obbligatorie per esercitare l'attività, in taluni casi. Lo stesso Dlgs 231/01 accorpa in sé moltissime norme che si ripercuotono severamente nella pratica di ogni giorno, indipendentemente dalla complessità, anche soltanto per accedere a fondi UE e/o per lavorare con la P.A.

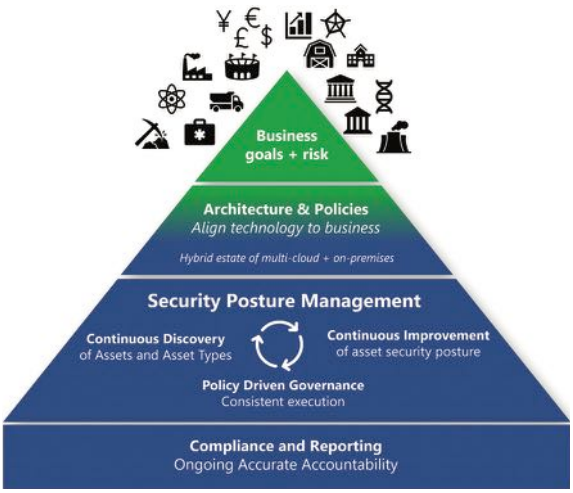
Gli uomini di business di solito, però, mal sopportano la "camicia di forza" rappresentata da regole e procedure. Come se ne esce?

Non si deve fare l'errore di pensare che, per conciliare gli aspetti normativi con le esigenze di business esista un "guru" capace di sintetizzare problematiche e regole e restituire un bignami del "cosa fare e quando". Questo processo di armonizzazione richiede la combinazione e il lavoro di skill diversi, senza dubbio con un taglio organizzativo, risorse con competenze legali e di

processo, esperti di risk management e di audit (soprattutto in ambito sistemi di gestione e controllo interno), con un contributo della parte più tecnica per quelli che saranno poi gli aspetti di declinazione operativa. Il mandato aziendale in termini di "governance strutturata" deve essere il primo passaggio, la linea guida, la visione che ogni risorsa aziendale deve percepire, oltre che il processo a cui tutti devono partecipare per contribuirne alla riuscita.

La rivoluzione tecnologica ha modificato i concetti di vulnerabilità e rischio, come si attua una corretta* governance *della sicurezza in uno scenario in costante e rapida mutazione?

Le Aziende, nella maggior parte dei casi, sono abituate a gestire la complessità dividendola in "silos". Questa scelta, per certi versi, può essere condivisibile poiché favorisce la sempre efficace segregation di ruoli e responsabilità, nonché la capacità di granularizzare i risultati di ciascun dominio fino all'ultimo bit. Se proviamo però a spostarci a un livello più alto e immaginiamo un ruolo Direzionale che abbia bisogno di una vista di sintesi eloquente e sostenibile per riportare lo stato attuale in ambito compliance e/o per rispondere a specifiche richieste da parte di Autorità, Istituzioni e/o Terze parti interessate, ivi compresa una Casa Madre, come si possono riassumere queste elaborazioni quando le informazioni sono "sparpagliate" o, addirittura, non codificate? Quanti interlocutori si dovranno coinvolgere con il conseguente costo "operativo"? Oggi la Governance esige il passaggio



da una vista verticale ad una visione orizzontale, una sintesi efficace e certificata di tutti quei parametri significativi idonei a misurare la postura di sicurezza aziendale. Questi parametri non riguardano solo aspetti tecnologici, ma anche processi e organizzazione, finendo col coinvolgere altre strutture oltre alla IT.

Si impone, dunque, una sensibilità diffusa e trasversale per tutte le questioni che hanno degli impatti sulla tutela aziendale?

Quello che risulta prioritariamente necessario è rivedere i parametri che oggi, anche e soprattutto alla luce degli ultimi "sconvolgimenti sociali" (degna traduzione e dimostrazione del più impensabile Black Swan), vanno integrati con componenti nuove che contribuiscono a configurare ulteriori scenari di rischio e altrettante vulnerabilità/ricadute dagli effetti devastanti. Oggi, per fare un esempio, lo smartworking diventa un'istituzione, non più una modalità di lavoro eccezionale e improvvisata; sono proliferate tecnologie artigianali e strumenti fai da te che si portano dietro moltissime criticità, così come il digital media Marketing e le politiche di utilizzo del Cloud non sempre correttamente contrattualizzate e definite in termini di perimetro di responsabilità. La nuova governance è una governance che attinge da fonti di ultima generazione, fonti che devono essere necessariamente considerate e tradotte in controlli specifici, correlati fra loro e codificati.

Modelli come la 231 ma anche un articolato decreto come il GDPR impongono la messa in esercizio di una* compliance integrata. *Aziende e istituzioni sono pronte a contemperare, senza perdere la visione di insieme: le best practices operative con una quotidianità fatta di un fitto microcosmo di controlli e verifiche?

Oggi "Integrazione" è la parola d'ordine, un "must" da cui è impossibile prescindere; integrazione di competenze, di tecnologie, di metodologie e di controlli, un approccio completo e complesso alla governance aziendale. L'ottimizzazione delle risorse disponibili e la capitalizzazione delle attività di analisi e implementazione sono elementi chiave per una gestione matura e virtuosa della propria organizzazione; questo vuol dire che il Management dovrà essere in grado, da un lato, di individuare gli skill idonei ad impostare e portare a termine il percorso di integrazione, dall'altro, di studiare e implementare meccanismi di controllo e sistemi di cross check capaci di raccogliere e riassumere le indicazioni mandatarie (normative e regolamenti) e i requisiti abilitanti per il business (linee guida e best practices), in modo razionale e coerente con il contesto operativo.

L'impianto (o Sistema di Gestione) "integrato", includerà tutti i punti di controllo da verificare e monitorare per garantire il costante mantenimento dei livelli di conformità attesi, scomponendo i singoli processi in fase di analisi e accorpandone i risultati in un sistema codificato di indicatori e regole "congruente", efficiente ed efficace. Questa sintesi richiede un grande sforzo, soprattutto iniziale, da parte del Management e di tutto il personale aziendale coinvolto, ma a valle di questo primo sacrificio, una volta creato l'impianto documentale e la matrice di controllo, si tratterà esclusivamente di monitorarne l'attualità e l'effettiva applicazione, curandone l'aggiornamento e la manutenzione evolutiva (non solo in termini di organizzazione e tecnologie a supporto, ma anche rispetto ai cambiamenti nel panorama normativo).

"Rating di conformità" è un termine sempre più ricorrente. Possiamo spiegare di che si tratta e in quale misura questo indice esercita un peso sui livelli di performance delle imprese?

Una delle principali sfide per le Aziende resta sempre quella di poter definire il proprio livello di conformità. Quando si parla di Compliance Rating, e, nello specifico per quanto riguarda Yoroi, di *Cybersecurity Compliance risk rating,* si intende il risultato di un'attività di indagine, profonda e mirata, su un ampio set di domini che costituiscono, in questa specifica fase storica, i maggiori driver da applicare per indagare la postura aziendale che definisce i profili di sicurezza. Si può passare da un first check up, che posiziona immediatamente l'Azienda all'interno di range predeterminati di Compliance Rating, all'effettiva diagnosi che, viceversa, costituisce il risultato di un'indagine modulare e cross referenziata su tutti i domini identificati come rilevanti ed efficaci per il calcolo del rating.

Questa diagnosi, in concreto, che cosa ci dice sullo stato di salute dell'impresa?

Tradotta in valore numerico (debitamente supportato da algoritmi di calcolo certificati), la diagnosi è una fotografia che costituisce la base di partenza del percorso di adeguamento/miglioramento. L'Azienda potrà

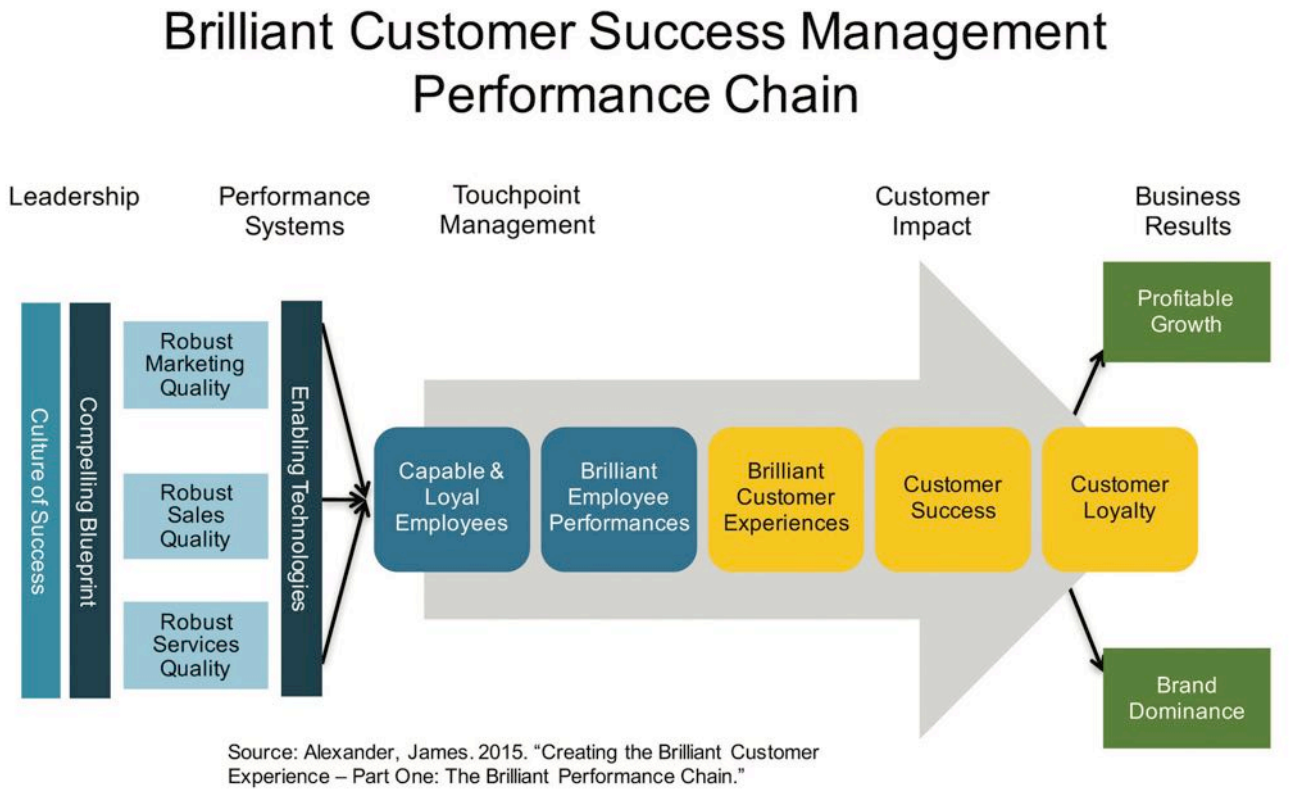
applicare questo metodo di valutazione esclusivamente a se stessa, oppure decidere di capitalizzare questo strumento/metodologia applicandolo alla propria catena di fornitura, con ciò rispettando e garantendo i principali obblighi di selezione, monitoraggio e controllo che ad essa vengono richiesti da Leggi e Best Practices. Il Cybersecurity Compliance Risk Rating diventa quindi strumento di misurazione e di accreditamento. Al di là del valore numerico si nasconde un sistema documentale complesso e sostenibile capace di fungere da evidenza e/o da reportistica a supporto di qualsiasi richiesta interna/esterna.

Compliance e innovazione rappresenta un altro binomio antitetico. Possono trovare una conciliazione?

Se si riesce a slegare la Compliance dal suo aspetto prettamente statico, portandola ad un livello superiore, con i processi di integrazione e innovazione che vengono dalla personalizzazione e dalla reingegnerizzazione della propria realtà e, perché no, anche delle proprie risorse (skill misti, tecnologie evolute, sviluppi proprietari, etc.), di fatto la linea di confine tra attività obbligatoria e opportunità si assottiglia, aprendo la strada ad una Compliance 2.0 e, prima ancora, ad Aziende 2.0! Si tende sempre a pensare che tecnici e "legali" parlino due lingue diverse, ed è senza dubbio vero, soprattutto per quanto riguarda il modo di interpretare i concetti di riferimento e di declinarli poi nella quotidiana operatività.

La "babele" determinata dalla diversità dei linguaggi è superabile?

È possibile trovare un linguaggio comune, almeno per alcuni aspetti, un perimetro di collaborazione dove esiste un vocabolario standard che permette alle due anime di comunicare e creare nuovi paradigmi, favorendo in tal modo il passaggio dalla "teoria" alla pratica, perché è solo con la pratica che si fa innovazione! Per fare degli esempi pratici di questo tipo di "goal", basti pensare che un modello di Compliance Management efficace può essere esportato, come standard di riferimento, alle diverse unità operative di un Gruppo di Aziende, anche di matrice geografica differente. Altro esempio a valore aggiunto può ritrovarsi nei casi in cui un'Azienda, in base alla sua esperienza, riesce a trasformare il proprio modello di gestione della Compliance in servizio al Cliente finale, differenziando ed arricchendo il portafoglio di offerta. Riuscire a trasformare un'attività identificata per la maggior parte in comandi spesso troppo generici e/o addirittura inapplicabili, in un processo operativo reale, misurabile ed ingegnerizzabile, restituisce la governance ai singoli e contribuisce alla responsabilizzazione in termini di obiettivi e risultati. Detto in sintesi: non si tratterà più di fare qualcosa che arriva dall'alto subendone il carico senza trarne beneficio, questa imposizione diventerà, viceversa, un'occasione per applicarne i suggerimenti secondo la propria inclinazione, con la sensazione di aver così contribuito a quel processo decisionale più alto che tendiamo a vedere sempre lontano e distinto da noi. ■



Source: Alexander, James. 2015. "Creating the Brilliant Customer Experience – Part One: The Brilliant Performance Chain."

Compliance vs sicurezza: antitesi superabile se mettiamo al centro l'uomo.

Intervista VIP a Riccardo Porcu.

Autore: Massimiliano Cannata

L'adempimento delle procedure non basta, per attuare delle strategie efficaci di cyber security – spiega Riccardo Porcu nell'intervista - bisogna saper esercitare logica collaborativa, visione d'insieme, capacità di trovare costantemente la sintesi tra "microcosmo" e "macrocosmo", nella consapevolezza che viviamo in un sistema di reti e di relazioni connotati da forte instabilità ed elevati fattori di rischio". Il progetto Academy, tratteggiato nel corso della discussione, innovativo per metodologia e contenuti, apre un interessante scenario sulla costruzione di leadership manageriali sul corretto posizionamento della sicurezza nelle organizzazioni produttive.

BIO

Riccardo Porcu è Direttore Generale della direzione generale dell'innovazione e sicurezza IT, presso assessorato agli Affari generali e riforma della Regione Sardegna ha ricoperto il ruolo di Direttore presso diverse amministrazioni pubbliche. È stato Professore di "Comunicazione Pubblica" presso l'Università degli Studi di Sassari ed è autore di numerose ricerche ed articoli scientifici in vari ambiti disciplinari.

Direttore Porcu, Sicurezza e Compliance, sono termini che presentano molti aspetti in antitesi. Come si declinano in contesti organizzativi e produttivi complessi?

Vorrei sottolineare un primo aspetto all'inizio di questa conversazione: la sicurezza non è un bene delegabile, perché ha molto a che fare con i comportamenti agiti da ogni singolo attore dell'organizzazione. Il fattore umano resta centrale quando si devono affrontare tematiche come la protezione di reti e sistemi. La sicurezza è architettura, visione di insieme, comunicazione, non bastano profili tecnici, pur importanti per gestirla, perché sono messe in discussione le logiche che reggono l'intero impianto organizzativo delle istituzioni e delle imprese. *Compliance* vuol dire "adeguarsi" alle norme, ma sarebbe riduttivo se ci soffermassimo solo su questo aspetto. Il processo che si sviluppa quando si attuano azioni di cyber security ha una radice statistica, ingloba una pluralità di figure, coinvolgendo un teatro molto ampio di attività e di settori di business. Tornando alla sua domanda iniziale direi che la sicurezza comprende il concetto di *compliance* e, nel contempo, lo travalica.

Se non c'è, come si evince dalla sua riflessione, alcuna contraddizione tra sicurezza e compliance, possiamo evidenziare i punti di convergenza?

Adempiere alle procedure riveste un'importanza decisiva, la gestione dei flussi e delle vulnerabilità che si presentano, e che sono anche dovute a potenziali "errori umani" risponde alla logica della complessità, che non può non tener conto del fatto che oggi ci muoviamo in un "universo di partecipazione" dominato dalle leggi del caos. Chi si occupa di *cyber security* deve saper conciliare "microcosmo" e "macrocosmo", gli attaccanti che si insinuano nelle strutture hanno, infatti, un atteggiamento subdolo difficile da prevedere. Sono abilissimi nello sfruttare superficialità commesse dagli attori dell'organizzazione spesso inconsapevolmente, in assoluta buona fede. Per questa ragione un atteggiamento che va bandito è quello dell'autocompiacimento, sovente si è portati a pensare che siccome c'è andata sempre bene, quello che facciamo e abbiamo fatto in termini di protezione degli asset funzionerà sempre. Tanti recenti fatti di cronaca dimostrano che non è proprio così.

La fallibilità di Popper e il ruolo della formazione

La rivoluzione tecnologica ha modificato i concetti di vulnerabilità e rischio, come si attua una corretta* governance *della sicurezza in uno scenario in costante mutazione?

Dobbiamo imparare ad accettare la fallibilità popperiana, che è sempre un indizio di progresso della scienza e della conoscenza. La domanda che dobbiamo porci non è: "ci sarà un attacco?", ma: "quando ci sarà un attacco...". L'approccio riduzionista non è più adatto a leggere la realtà entro cui ci muoviamo, così come appare fuorviante l'approccio di tipo sanzionatorio. La parola chiave è collaborazione. Nessuna realtà organizzativa può avere attualmente le risorse necessarie per far fronte alle esigenze di cyber security, che sono crescenti in ragione della progressiva digitalizzazione degli ambiti in cui ci muoviamo, e non mi riferisco ovviamente solo al lavoro. Non esistono insomma realtà produttive impermeabili al rischio. Dal paradigma del controllo rigido di un perimetro fisico, dobbiamo passare al paradigma della *governance* di sistemi lontani dall'equilibrio, mutevoli, per nulla statici e per definizione in continua evoluzione, perciò difficili da focalizzare e misurare.

Quello che descrive è un "salto" non solo normativo, ma culturale e organizzativo. La PA è pronta a compiere questo passo?

Occorre precisare che esistono più PA. In Italia abbiamo più di seimila comuni che contano meno di seimila abitanti. Le realtà più strutturate possiedono risorse per far fronte anche alle esigenze di formazioni, che sono cruciali in questa fase di cambiamento epocale. Le Regioni e la PA a livello centrale devono diventare un punto di riferimento nell'adozione di strategie collaborative, per consentire al paese la transizione digitale ed energetica. È necessaria una cabina di regia che faccia da polo attrattore dell'innovazione, erogando servizi di sicurezza e più in generale servizi IT per le comunità che hanno bisogno di adeguarsi a standard di connettività sempre più sofisticati. Insisto molto, anche nei corsi che curo per l'Università, sul concetto di cross management. La mia direzione si è fatta parte attiva per la creazione di un nucleo interdisciplinare, non previsto dalla pianta organica e che andrebbe al più presto ricompreso in una legge ad hoc, che ha come *mission* il *macthing* di profili e competenze. Il corredo tradizionale dei saperi non appare infatti più idoneo per affrontare il vento della trasformazione, che rischia di travolgerci se non ci attrezziamo in fretta. Questo vale sia per il pubblico che per il privato.

Art. 3 della Costituzione: giustizia, sicurezza e buon governo si toccano

Per sviluppare un'adeguata strategia di cyber security, le aziende che fanno ricerca in questo ambito, insistono sull'importanza della formazione, della collaborazione, della cooperazione, del dialogo costante tra capi e dipendenti. Più facile a dirsi che a farsi, non crede?

Non c'è nulla di scontato quando parliamo di temi caldi come la sicurezza, che investono la collettività, nessuno

escluso. La Regione Sardegna si è ispirata all'art.3 della Costituzione. Il passaggio cruciale in cui si parla di "rimozione degli ostacoli" alla partecipazione di tutti alla vita democratica, credo vada posto all'attenzione dell'opinione pubblica, a tutti i livelli. L'uguaglianza sostanziale è un valore essenziale del nostro stare insieme. Abbiamo creato un'Academy strutturata in quattro indirizzi, nella convinzione in questa partita, che attiene a delle scelte politiche fondamentali, anche la sicurezza riveste un ruolo di primo piano, perché sicurezza e buon governo si toccano.

Digital Innovation Hub
DIH Sardegna

Il Garante della Privacy, Pasquale Stanzione, ha sottolineato nella sua relazione annuale, la stretta connessione che esiste tra umanesimo digitale e protezione dei dati, tracciando un nesso molto forte tra un duplice ambito di riflessione:* "rule of law" *e* "rule of technology". *Si tratta di un parallelismo troppo ardito quello tracciato dal giurista?

Il riferimento storico che mi piace richiamare è il Rinascimento, come ha scritto recentemente il filosofo Marramao dovremmo guardare con intelligenza al passato per guardare con maggior fiducia al futuro. "Essere stati è la condizione per essere", Fernand Braudel, ha ragione il grande storico degli Annales. Quando, la mia direzione ha deciso di dare un apporto per potenziare il polo strategico nazionale ci siamo trovati, non a caso, a Firenze. In questa splendida città, tra il XV e il XVI secolo l'Italia ha affermato il suo primato, è stata per l'ultima volta al centro del mondo. Donatello, Michelangelo, Raffaello il genio universale si è manifestato in queste menti eccelse. Lo spirito collaborativo di cui parlo, deve rifarsi alla grandezza di questi esempi, i team che operano nella sicurezza devono avere una trasversalità propositiva e creativa. Torno alla riflessione iniziale, ribadendo il carattere non delegabile della sicurezza. Se non si conoscono i linguaggi dell'organizzazione e i comportamenti conseguenti da adottare, non si può avere né tanto meno sviluppare alcuna capacità di reazione nelle situazioni di crisi.

Il progetto Academy

Le Academy che avete progettato rispondono a una visione integrata della sicurezza?

Rispondono ad alcune finalità ben delineate. È sempre più diffusa la necessità di attuare un "rinascimento digitale", senza di cui risulta impossibile mettere in campo delle collaborazioni qualificanti. Tutti desideriamo uscire al più presto dal tunnel della crisi, bisogna per questo produrre oggetti e progettare servizi che permettano una crescita reale. *"Interaction Mind"*, primo dei quattro indirizzi della nostra Academy ha questo preciso scopo: affinare la capacità di interagire, di creare team collaborativi e gruppi ad alta capacità assecondando le potenzialità di cui dispone la neocorteccia del nostro cervello. *"Organize your mind"* scandisce il secondo step, propedeutico alla creazione del cross management e alla riorganizzazione di strutture e servizi. *Security mind* è l'indirizzo dedicato alla formazione di funzionari e manager della sicurezza consapevoli delle conseguenze legate alla trasformazione digitale.

"New public mind" è la parte dei nostri corsi che guarda al settore pubblico, ambito cruciale che deve affrontare questa stagione di cambiamento con responsabilità, metodo, consapevolezza. Quando parliamo della PA, ci riferiamo a quella che rimane la prima "azienda" del Paese. Dalla collaborazione interistituzionale e dall'evoluzione della PA dipenderà lo sviluppo del sistema paese nel suo complesso.

La visione interdisciplinare implica un diverso posizionamento della sicurezza nel contesto delle organizzazioni produttive?

La direzione generale presso la Regione Sardegna che mi è stata affidata aveva prima del mio arrivo la seguente denominazione: "affari generali e società dell'informazione", ho modificato la dizione trasformandola in "innovazione e sicurezza IT", nella convinzione che per guidare il cambiamento occorre un grande lavoro di *change management*. Voglio ringraziare a questo proposito il Presidente della Regione Sardegna, Christian Solinas e l'Assessore Regionale agli Affari generali, Personale e Riforma, Valeria Satta per il *committment* e la programmazione concordata. Il loro apporto è stato essenziale per portare avanti i progetti e per dare effetto concreto al generale bisogno di innovare, che tutti avvertiamo. Non dimentichiamo che

la sicurezza non è un affare da ingegneri in "camice bianco" ma è legata a un miglioramento costante a tutto tondo delle risorse umane, che va perseguita con attività di *coaching* molto mirate.

Si riferisce all'importanza di porre in essere efficaci e innovative attività di* awareness*?

Awareness nella mia visione vuol dire sviluppare capacità di essere collegati a un mondo multidimensionale. L'universo è in espansione, non vedo perché dirigenti e manager non debbano sentire l'esigenza di allargare costantemente il proprio raggio di azione. Torna ancora una volta la filosofia del rinascimento, soprattutto quel nesso inscindibile tra macrocosmo e microcosmo, che avevo già richiamato. Grandi maestri, come Eugenio Garin, ci hanno fatto vedere tutte le implicazioni legate al passaggio dal cosmo chiuso all'universo infinito. A questa costellazione di concetti, aggiungerei la libertà come valore. La sicurezza è intimamente legata al concetto di libertà. Non dobbiamo costruire "regimi vessatori" per garantire la sicurezza. La tutela del corpo fisico ed elettronico, la difesa della sfera intima e della privacy devono contemperare la libertà di espressione e di movimento di cui ognuno di noi deve godere. Credo abbia ragione il Garante, torno al tema della *compliance,* quando invocando responsabilità e attenzione da

parte delle imprese chiamate a rispettare le normative vigenti, sgombra il campo dalla prospettiva di un diritto "tiranno", facendo riferimento proprio alla privacy. Lo si è visto nella pandemia: dal giusto bilanciamento tra privacy e diritto all'informazione è dipesa la possibilità di intervenire e di salvare molte vite somministrando con puntualità e capillarità terapie e vaccini.

Compliance e diritti della persona

Nella tutela del corpo elettronico etica e tecnologia si toccano. Possiamo dire che siamo di fronte a un'ulteriore declinazione della compliance?

A patto di interpretarne il significato in maniera ampia. Nomos, ethos e patos si toccano come ci ha insegnato per primo Platone. Chi opera nella sicurezza si muove su questi tre versanti: la legge, il dover essere, e il pathos la preoccupazione e la paura che le nostre certezze vengano messe a rischio da insidie e pericoli sempre più difficili da individuare, prevenire, contrastare. Una *compliance* avvertita deve tenere conto dei dritti della persona nel disegnare i regolamenti.

La comunicazione che funzione può avere nella* compliance *della sicurezza?

Una funzione decisiva. La comunicazione non è una disciplina in più, è una competenza che deve stare dentro i processi, contribuendo, grazie a un rigoroso lavoro sul linguaggio, a fugare le ambiguità e a chiarificare messaggi, procedure, *policies.* Una *compliance* priva di una reale comprensione delle norme sarebbe un controsenso. Il linguaggio è il nostro mondo come sosteneva Heidegger. La Scuola di Palo Alto ha fondato molte delle sue teorie sul concetto di retroazione, per cui risulta decisivo quello che i miei interlocutori capiscono, i significati cui accedono, non quello che dicono i capi o i responsabili, magari *ex cathedra,* esercitando una pressione gerarchica ormai fuori dal tempo. Per dirla in sintesi: i dirigenti che hanno competenze manageriali in grado di gestire la comunicazione hanno oggi un'arma in più.

Chiuderei questa conversazione se mi permette dal punto in cui abbiamo iniziato: la sicurezza è un valore non delegabile. Per questa ragione la creazione di leadership collaborative, aperte in termini culturali e di visione non può non contemplare la comunicazione quale asset strategico, utile ad affrontare una corretta *governance* del cambiamento, nel contesto di una società evoluta, in perenne divenire. ■

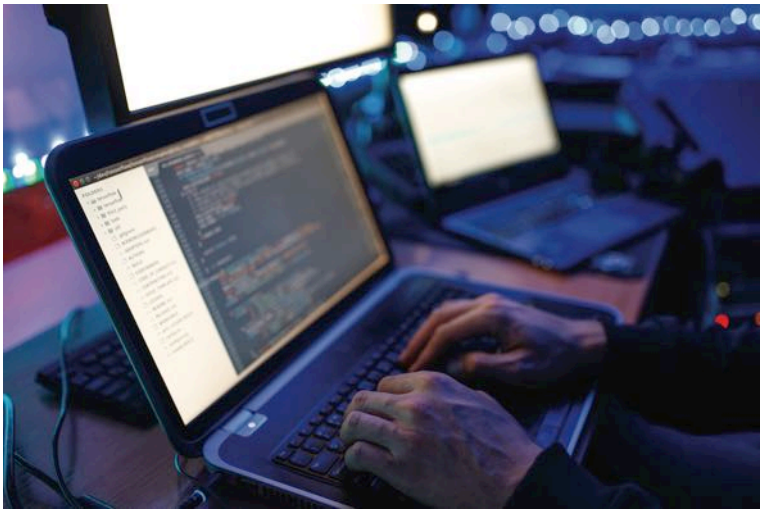
La collaborazione tra CrowdStrike e la Cloud Security Alliance punta a garantire un modello di sicurezza Zero Trust pervasivo.

CrowdStrike collabora con i leader di settore Okta e Zscaler per supportare il nuovo Zero Trust Advancement Center.

Autore: **Luca Nilo Livrieri**

I problemi di sicurezza che oggi riguardano le organizzazioni, in realtà, non si sono evoluti molto negli ultimi trent'anni. Password deboli e condivise, configurazioni errate e vulnerabilità sono problematiche che hanno tormentato l'industria per anni e che persistono tuttora. Ciò che è cambiato è la velocità e il livello di sofisticatezza su cui gli avversari di oggi fanno leva per rafforzare queste – apparenti – debolezze.

C'è una percezione errata secondo cui fermare i malware significa fermare le minacce. Questo è importante, ma non è sufficiente, perché - secondo quanto si evince dal Global Threat Report 2022 di CrowdStrike - gli avversari continuano ad aumentare i loro attacchi malware-free: il 62% di tutti gli attacchi, infatti, è privo di malware e caratterizzato da attività di "hands-on-keyboard" degli avversari. Gli attaccanti sono abili a sfruttare le credenziali dell'utente e l'identità, superare i sistemi di difesa legacy, muoversi lateralmente attraverso l'infrastruttura, abusare dei sistemi ed infine eseguire i loro attacchi.

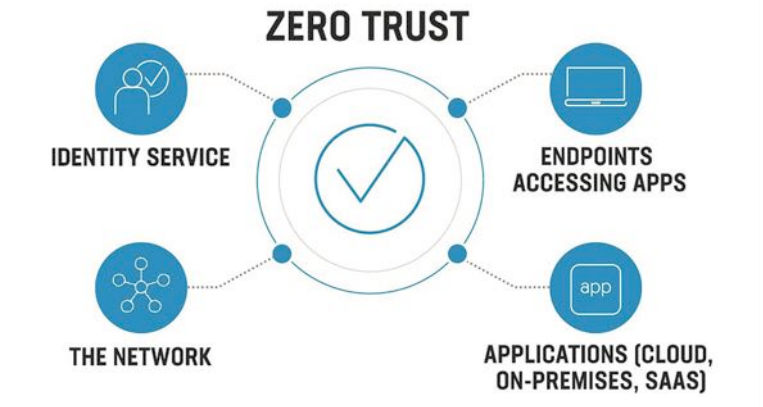


Nelle aziende moderne, le identità e le credenziali dell'utente si intrecciano con i dispositivi che si è soliti usare, con i servizi in cloud a cui si accede e i dati ne fluiscono attraverso. Questa intersezione rappresenta il punto in cui si concentra il rischio aziendale. Le strategie di sicurezza Zero Trust assicurano il livello di protezione necessario a garantire la sicurezza dell'infrastruttura e dei dati nelle organizzazioni odierne. Ciò, tuttavia, richiede all'industria la capacità di compiere passi significativi verso tale approccio.

Per tali ragioni, CrowdStrike ha deciso di collaborare con i leader di settore Okta e Zscaler per supportare la Cloud Security Alliance nel lancio dello Zero Trust Advancement Center, un'importante iniziativa che darà alle organizzazioni le intuizioni, la formazione e la comunità richiesti per implementare le strategie Zero Trust.

Perchè lo Zero Trust e perché adesso

Gli attacchi basati sull'identità sono diventati uno dei principali strumenti dei nemici informatici. Attacchi di alto profilo e fortemente sofisticati come SUNBURST, che si è propagato a cascata attraverso migliaia di partner e organizzazioni della supply chain, sfruttano l'architettura di autenticazione sottostante e permettono agli autori delle minacce di mascherarsi come dipendenti legittimi, muoversi lateralmente e raggiungere le destinazioni prese di mira.



Allo stesso tempo, il passaggio ad una forza lavoro distribuita ha creato una nuova ed enorme superficie di attacco che gli avversari cercano di sfruttare. Oggi, infatti, i dipendenti lavorano attraverso reti differenti e da diversi luoghi di lavoro, è dunque sempre più complesso mantenere la visibilità e rendere sicuri gli endpoint dagli attacchi informatici. I workload in cloud continuano ad essere adottati ad un ritmo mai visto e potrebbero superare gli endpoint nei prossimi cinque anni. Ne consegue un aumento significativo del rischio aziendale, dove un'infiltrazione su un endpoint o workload può mettere l'azienda a rischio violazione.

BIO

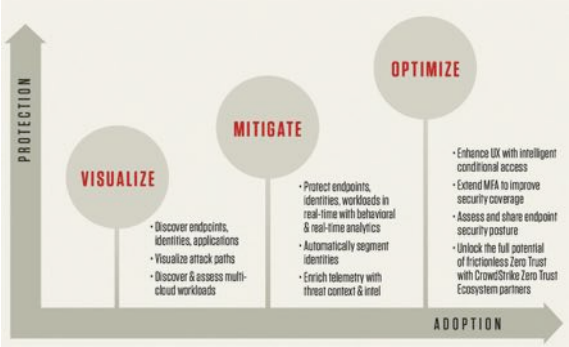
Luca Nilo Livrieri è l'SE Manager di Crowdstrike per il Sud Europa. L'ingresso in Crowdstrike avviene nel maggio 2021, con la responsabilità di seguire lo sviluppo e la crescita della struttura di prevendita nel Sud Europa. Partecipa ormai da parecchi anni come relatore a diversi eventi nazionali e internazionali su privacy, sicurezza, cloud e digital transformation fra cui Security Summit, ISMS forum, IDC e Cybertech. Prima di Crowdstrike, Livrieri è stato manager per l'Italia, la Spagna e il Portogallo della struttura prevendita di Forcepoint. Ha maturato esperienze come membro dell'"Office of the CSO" e Senior SE per il mercato enterprise, e la formazione e affiancamento del canale di rivendita in Websense e Surfcontrol. Prima di svolgere il ruolo di SE ha lavorato come consulente Gfi-Ois per la programmazione web presso alcune importanti aziende italiane.
Precedentemente ha conseguito la Laurea magistrale in Comunicazione nella Società dell'Informazione, con tesi specialistica presso il dipartimento di informatica dell'Università Degli Studi Di Torino.

Lo Zero Trust è un approccio che può minimizzare l'impatto di una violazione fornendo all'azienda una visione olistica dell'identità autorizzata. Applicando una convalida continua, in tempo reale e automatizzata basata sul rischio per l'accesso a qualsiasi risorsa, sia essa in cloud, on-premise o ibrida e attraverso qualsiasi tipo di tecnologia (inclusi i sistemi legacy e i dispositivi non gestiti), le organizzazioni possono ridurre o fermare notevolmente il movimento laterale e l'escalation dei privilegi durante una compromissione.

La metodologia Zero Trust è un concetto che può essere distorto. Per anni, i vendor hanno provato a ridefinire lo Zero Trust per allinearsi alle loro attuali capacità di prodotto. Tuttavia, lo Zero Trust non è una soluzione puntuale. Si tratta di costruire una strategia di difesa in profondità affinchè tutte le risorse abbiano perimetri basati sull'identità che sono continuamente monitorati per i comportamenti degli utenti e gli attributi dei dispositivi per garantire che l'accesso con il minor numero di privilegi alle risorse aziendali sia continuamente applicato. Questo deve avvenire a prescindere da dove utenti, applicazioni e dispositivi sono posizionati o localizzati. Lo Zero Trust è fondamentalmente dinamico e, per essere efficiente, richiede un approccio moderno alla sicurezza.

I singoli prodotti e le soluzioni di sicurezza informatica top di gamma non saranno più in grado di mantenere il passo con l'ambiente odierno. Ai clienti non dovrebbe essere richiesto di cambiare i loro investimenti ogni volta che arriva una nuova minaccia. Ciò di cui hanno bisogno è una migliore piattaforma di sicurezza che consenta loro di lavorare meglio e di ridurre i requisiti di personale, in cui ogni fornitore si può concentrare sulle proprie competenze.

Ecco perchè CrowdStrike ha costruito un ecosistema Zero Trust robusto e con integrazioni semplici, estendendolo con leader di settore come Okta e Zscaler per collaborare e proteggere i clienti dalle minacce attuali e future.

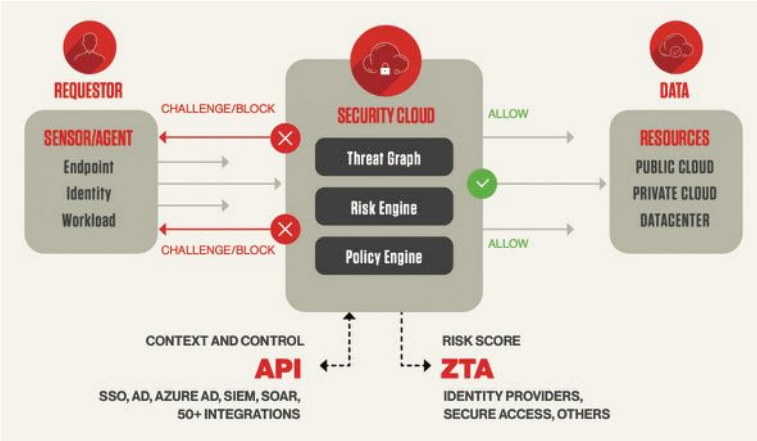


CrowdStrike rafforza lo Zero Trust attraverso dispositivi, identità e dati

La soluzione Zero Trust di CrowdStrike è costruita sull'architettura best-of-platform e rappresenta la base per difendersi dagli attacchi moderni: endpoint e workload, identità e dati. Un approccio orientato all'avversario con l'obiettivo di fornire un livello di sicurezza senza precedenti, efficiente ed efficace, sia che l'ambiente del cliente si trovi nel cloud, on-premise o in un ambiente ibrido, e su qualsiasi tipo di tecnologia, compresi i sistemi legacy e i dispositivi non gestiti.

Un approccio di piattaforma unificata che collega la macchina sia all'identità che ai dati per fornire una protezione Zero Trust completa, attraverso il leggero agente Falcon® di CrowdStrike sull'endpoint. Ciò consente ai clienti di convalidare l'utente, il comportamento associato ad esso o alla credenziale, le politiche dell'organizzazione associate ai dati o alle risorse cui si accede. Riunire tutto questo in tempo reale permette di prendere decisioni tempestive e di stabilire se l'accesso debba essere concesso, negato o contestato in modo condizionato.

CrowdStrike intende continuare ad innovare per fornire soluzioni incentrate sul cliente che risolvono i problemi. Con il built-in CrowdStrike Store ed un maturo set di API, tra cui integrazioni profonde con Zscaler e Okta, i clienti possono estendere i loro investimenti esistenti per aumentare ulteriormente le protezioni e applicare una strategia di difesa in profondità attraverso utenti, applicazioni e dispositivi. Nel corso del 2022, CrowdStrike perseguirà inoltre la sua crescita del supporto di CrowdStrike Falcon Zero Trust Assessment (ZTA) con i suoi partner strategici. Recentemente, ha annunciato il supporto ZTA per le piattaforme macOS e Linux, estendendo la protezione completa con un approccio incentrato sull'identità e sui dati in tutte le piattaforme.



Cosa riserva il futuro

La nascita del concetto "Zero Trust" risale ad un decennio fa, ma il suo momento è adesso. Nel 2021, l'amministrazione Biden ha emesso un ordine esecutivo che sottolinea l'uso di capacità come il rilevamento e la risposta degli endpoint (EDR) e Zero Trust. Proprio queste misure aiuteranno ad affrontare le minacce sofisticate che oggi hanno un impatto su quasi tutti i settori.

CrowdStrike ha recentemente annunciato una partnership con la Cybersecurity and Infrastructure Security Agency (CISA) per implementare la piattaforma CrowdStrike Falcon e proteggere gli endpoint e i workload critici della CISA e quelli di più agenzie federali. Una dimostrazione di come l'industria può rendere operativo lo Zero Trust e costruire sul progresso degli standard esistenti di Zero Trust come il NIST 800-207.

La collaborazione con la Cloud Security Alliance e i partner Zscaler e Okta si propone di accelerare l'implementazione di standard di settore Zero Trust completi che preparano i clienti al successo nell'applicazione di un approccio "Trust No One, Verify Always" per proteggere un ambiente di minacce sempre più complesso. ■

Security Mind

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

La Psicologia associata alla Cyber Security

Quando si parla di Cyber Security oltre ad investie in tecnologie è importante investire sulla consapevolezza del personale, analizzando il fattore umano nel contesto della sicurezza informatica, attingendo a contributi multidisciplinari per esempio le scienze sociali, la psicologia e la sociologia.

Per quanto si possano usare sistemi informatici aggiornati ed efficaci, gran parte del rischio degli incidenti informatici ricade proprio sulle scelte del singolo e dei suoi comportamenti automatici.

Che si tratti di un'analisi di controllo, di un'azione di remediation o di altre azioni specifiche, ciò che contribuisce a fare la differenze è sviluppare quella che lo psicologo Daniel Goleaman chiama "Intelligenza Emotiva", ossia la particolare abilità legata all'uso corretto delle emozioni, che ha come obbiettivo quello di rendendere l'individuo più consapevole di come le proprie emozioni possono influenzare le azioni.

I Cyber criminali influenzano i comportamenti degli individui rendendoli vulnerabili nel cyber spazio, sfruttano le vulnerabilità tra cui:

FIDUCIA IRRAZIONALE

Quando utilizziamo le interazioni sul web, vengono a mancare alcuni indicatori tradizionali che abbiamo a disposizione nelle interazioni fisiche, con una conseguente sottovalutazione dei potenziali pericoli.

AUTOMATISMO

Inserire dati personali o fare click sono azioni automatiche che richiedono poco tempo.

PAURA E STRESS

Spesso i cyber criminali utilizzano le email con contenuti che allertano e spaventano i destinatari, sfruttando l'istinto di sopravvivenza creano una minaccia con delle possibili conseguenze negative.

ACCUDIMENTO

Gli esseri umani spesso instaurano relazioni sociali con l'obiettivo di aiutare altre persone, questo comportamento viene utilizzato dai cyber criminali per le frodi sentimentali.

In conclusione possiamo affermare che la miglior difesa contro il crimine informatico è la conoscenza e la consapevolezza degli aspetti tecnici e delle dinamiche che intercorrono tra l'attaccante e la vittima.

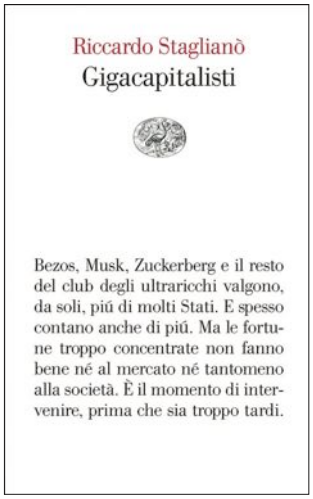
Pertanto una maggior consapevolezza si traduce in una minore esposizione degli individui a diventare delle vittime.

La nostra Missone è passare dall' Informazione alla Trasformazione

Riccardo Staglianò Giga Capitalisti Einaudi

Autore: Massimiliano Cannata

I giganti del capitalismo digitale e le nuove povertà



"Gigacapitalisti", "gigworkers", il male sta nelle parole, aveva ragione Pirandello. "Giga" il bisillabo più in uso nell'era di Internet contiene in sé tutte le contraddizioni di una società polarizzata tra ricchi e poveri. Colin Crouch nel saggio *Se il lavoro si fa gig (ed. Il Mulino)* ha tratteggiato un interessante affresco dei "nuovi poveri", gli "intermittenti" del capitalismo digitale. "Il lavoro – scrive lo studioso – ormai si accende e si spegne come fosse lampadina, le aziende lo attivano quando ne hanno bisogno, scaricando sul singolo responsabilità e oneri. Assumono e poi licenziano senza alcun ammortizzatore dipendenti di cui non hanno più bisogno". Questa grave distorsione del libero mercato chiama in causa le istituzioni, soprattutto le associazioni di categoria, rimasti spesso "afoni", incapaci di affrontare le profonde trasformazioni del sistema economico e produttivo, che stanno aprendo la strada alla post democrazia. Per comprendere le dinamiche in atto a livello globale può venire in soccorso il lucido pamphlet di Riccardo Staglianò, (*Gigacapitalisti* ed. Einaudi) che mette a fuoco con efficacia quello che accade sul versante opposto a quello dei nuovi poveri, si tratta di quel variegato territorio popolato dai signori del mondo globale, i "padroni delle piattaforme" digitali. "L'edizione del 2019 del rapporto sull'Internet Society - commenta il giornalista inviato di Repubblica - ha coniato l'espressione giusta, parlando di *total service environments*. Sono gli ambienti a servizio totale, che avvolgono la nostra esistenza, immergendola in una infosfera, fatta di tecnologie, strumenti, applicazioni sofisticate, con cui viviamo in simbiosi. Non c'è da stupirsi se i Rockefeller di oggi, rispondono al nome di Musk che va nello spazio, di Bezos che si candida a diventare come il controllore dell'emporio unico dell'umanità, di Zuckemberg che socializzando la rete ha modificato il nostro modo di relazionarci e di stare nel mondo. Epoche distanti si potrebbe dire, ma connotate da una profonda analogia: "allora come ora il vento di una rivoluzione profonda avrebbe rimodellato le basi materiali della civiltà, da contadina a industriale ieri, da industriale a digitale oggi". Se Rockefeller nei primi anni del '900 controllava l'80% del petrolio mondiale, Google detiene attualmente il 90% del mercato delle ricerche in Europa e quasi il 70% in America. Carnegie aveva rimpiazzato il ferro con l'acciaio reinventando l'edilizia, Ford aveva inventato l'era dell'automobile, Bill Gates introducendo un pc in ogni casa e Larry Page hanno messo nelle mani di ciascun utente tutta la conoscenza del mondo, consegnandoci l'enorme responsabilità di saperla gestire". Mentre il *Leviatano* di Hobbes appare, così, in declino, i "sultani del silicio", i soggetti privati che prendono forza, scompaginando equilibri che sembravano immodificabili. Servirà, ha sottolineato Pasquale Stanzione nella relazione annuale dell'Autorità Garante della Privacy, una corretta *governance* della *gig economy* per scongiurare il rischio di un nuovo caporalato digitale. Nel generale ridisegno degli assetti di potere l'Unione sarà chiamata a definire un *Corpus iuris* all'altezza delle sfide che si profilano. Concentrare ogni spinta riformatrice nella ricerca di un equilibrio tra *rule of technology e rule of law*, è divenuto un imperativo categorico che bisogna mettere in pratica per arginare le povertà crescenti e la strisciante "colonizzazione del pensiero", che, lo ha denunciato Luciano Violante, rischia di incidere sulla libertà cognitiva, imprescindibile garanzia di ogni altro diritto fondamentale. ■

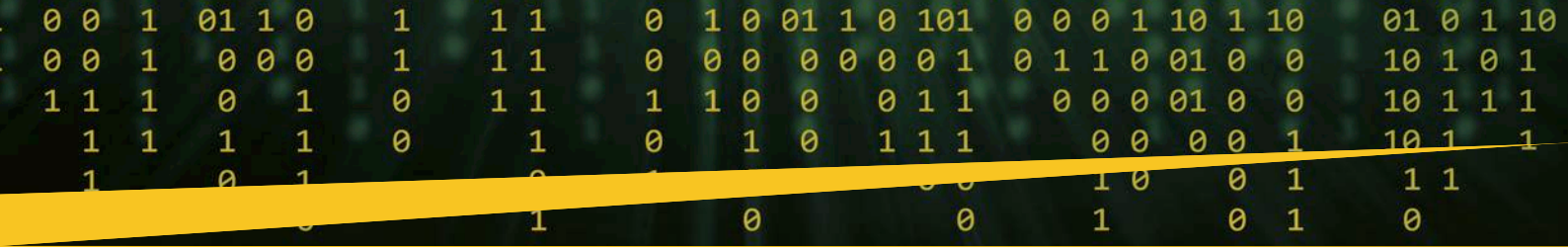
I "poteri privati" delle piattaforme e le nuove frontiere della privacy (a cura di Pasquale Stanzione) Ed. Giappichelli

Autore: Massimiliano Cannata

L'età delle piattaforme nella società del rischio

Il saggio *I "poteri privati" delle piattaforme e le nuove frontiere della privacy,* curato dal presidente dell'Authority di settore Pasquale Stanzione, tematizza molto bene il delicato rapporto che oggi sussiste tra evoluzione del diritto e sviluppo tecnologico. Età delle piattaforme è la definizione utilizzata dagli studiosi per descrivere il contesto entro cui siamo ormai tutti immersi. Il potere di controllo e di indirizzo che i "padroni" della Rete hanno acquisito giustificano questa etichetta, che descrive molto bene i nuovi equilibri economici che si stanno facendo strada.

I contributi che compongono lo studio, firmati dai massimi esperti del settore, abbracciano una pluralità di versanti: i dati come beni giuridici, le dinamiche del consenso sul trattamento delle informazioni nella dimensione europea, il delicato fenomeno della "monetizzazione" della privacy che si sta verificando in diversi paesi,



il nuovo modello giuseconomico che sta emergendo in seguito alla proliferazione dei network, la giurisprudenza applicata a *Facebook*, il binomio piattaforme e visibilità del potere.

Da uno sguardo sinottico emerge in maniera netta come la protezione delle informazioni è ormai divenuta un fattore determinante che travalica lo stretto ambito dei tecnicismi chiamando in causa gli equilibri geopolitici. "Paesi come la Cina – commenta il Garante – stanno facendo coincidere spazio fisico e virtuale, confini territoriali e risorse informative, imponendo un regime vessatorio fatto di censure e controlli che cozza con il DNA stesso della rete, nata come presidio della libera circolazione delle idee". Per converso va anche detto che in realtà come gli USA si discute di declinare in forme nuove l'dea di sovranità digitale, a dimostrazione di quanto stretto sia ormai il rapporto tra ICT ed equilibri democratici. Il processo di *"datificazione"* della vita collettiva sta ridisegnando, infatti, gli assetti di potere e le strategie di gestione del consenso.

Rule of low e rule of technology

L'UE sta tentando di trovare una linea strategica coerente per non rimanere spiazzata dalle trasformazioni in atto. La spinta riformatrice, che da più parti si sta facendo sentire, dovrà contemperare *rule of low e rule of technology.* Attorno a questo complesso binomio che chiama in causa i fondamenti del diritto positivo ruota lo strumento regolatorio dell'*artificial Intelligence Act* che ha introdotto alcune misure finalizzate ad un uso corretto dell'intelligenza artificiale. Rimodulare il perimetro del tecnicamente possibile, sulla base di ciò che si ritiene giuridicamente accettabile, è il nuovo imperativo categorico che governi, istituzioni e imprese dovranno tenere ben presente. Non si tratta, come si può evincere dalla molteplicità delle posizioni espresse dagli autori di questo lavoro, della "fredda rivalsa" di alcuni cultori del diritto, ma più semplicemente della ricerca di una reale sostenibilità etico-giuridica che riguarda gli assetti futuri della "super società". Per governare il cambiamento, regolare la convivenza nell'orizzonte mutante dell'Infosfera servirà uno sforzo politico - istituzionale senza precedenti, che darà l'occasione all'opinione pubblica italiana ed europea di valutare la qualità delle classi dirigenti protagoniste in questo delicato momento storico.

Il *Digital services Act* e il Digital Markets Act sono gli istituti preposti a una regolazione del potere privato delle piattaforme. Risulterà necessario, nello scenario che si sta aprendo, rafforzare una tutela ad ampio spettro degli utenti, che va attuata insieme a un controllo puntuale dei flussi informativi che si muovono nel circuito crossmediale, sempre più esposti a un processo di sfruttamento e di monetizzazione, che è il risvolto più inquietante legato allo sviluppo *dell'information society.*

"Algoritmo d'oro" la definizione del presidente emerito della Corte Costituzionale Giovanni Maria Flick (cfr. CST. N 2 2022) appare calzante. L'immagine biblica del *"vitello d'oro"* torna prepotente, mentre si profilano gli utenti, si scava nelle loro abitudini per indurre bisogni fittizi da sfruttare commercialmente. Lo "spionaggio" sotto traccia non ha limiti, si estende fino a ricomprendere lo stato di salute degli individui allo scopo di colpire le vulnerabilità e di speculare sulla fragilità dei soggetti. "Lo stiamo vedendo – spiega Flick - in quello che sta avvenendo con la guerra in Ucraina, e lo abbiamo visto prima con la pandemia. Una "babele di voci" non sempre competenti e realmente interessate a scandagliare i fatti con la massima obiettività possibile si rincorrono, con il risultato che le lingue si confondono e confluiscono in un "linguaggio unico" (tra uomo e uomo, tra uomo e macchina, tra macchina e macchina) come quello della piana di Ur dove si iniziò a costruire la torre di Babele. L'interesse che muove tutto è duplice, ed è facilmente individuabile: potere e profitto".

Sul pendio molto pericoloso di uno sfruttamento indebito del nostro "corpo elettronico", paventato da Flick, rischia di scivolare l'Europa tutta, come "comunità patria del diritto occidentale. Esiste il rischio – denuncia Stanzione – di una rifeudalizzazione dei rapporti sociali, generata da una discriminazione, neanche tanto sottile, attuata sulla base di informazioni illecitamente acquisite. *Fake news* e narrazioni fuorvianti e spesso ideologizzate che ci allontanano dalla realtà stanno, così, riportando l'orologio della storia molto indietro nel tempo, facendoci respirare atmosfere che speravamo fossero definitivamente superate.

Le conseguenze politiche di questo articolato e contraddittorio complesso quadro evolutivo non sono di poco conto. Il lavoro su piattaforma dando vita alla *"Gig economy"* sta infatti creando i presupposti per un nuovo "caporalato", che prospetta il rischio di un'involuzione sociale che investe la qualità stessa della democrazia. Una *governance* corretta del digitale consentirebbe di scongiurare le azioni di *targeting* politico, funzionali a condizionare il consenso, fino a pregiudicare l'esito delle competizioni elettorali. "La potenza di calcolo, di cui oggi disponiamo, ha una capacità di "colonizzare il pensiero" incidendo sulla libertà individuale e sui diritti fondamentali", l'allarme espresso dall'ex presidente della Camera Luciano Violante tocca il punto cruciale di una partita impegnativa. Il capitalismo delle piattaforme non è solo un capitalismo cognitivo, perché si traduce in un "capitalismo delle affezioni" (la definizione è di Eric Sadin), in grado di influenzare scelte e comportamenti.

Habeas mentem e psicopolitica

Il filosofo Aldo Masullo ha introdotto la categoria della "psicopolitica", siamo un passo oltre la "biopolitica" teorizzata da Foucault. Non si tratta di disquisizioni dotte, l'uso di sofisticati algoritmi e dell'IA nelle forme più avanzate ci mette in possesso di una facoltà di governo della mente, con conseguenze inquietanti. Stiamo acquisendo la possibilità di condizionamento delle regioni più remote della volontà individuale, che non possono lasciarci indifferenti. Il documento stilato dal G7 dei Garanti europei lo scorso sette e otto settembre sotto la presidenza del Commissario federale tedesco che sollecita la definizione di un "modello etico" per l'uso dell'intelligenza artificiale, dimostra quanto urgente sia intervenire per disciplinare un ambito di ricerca che sta al confine tra psicologia, scienze cognitive, neuroscienze, e intelligenza artificiale.

Bibliografia - Cybersecurity Trends

In conclusione sarebbe auspicabile che l'ampio e appassionante perimetro argomentativo affrontato da questa pubblicazione divenisse la base di riferimento per la messa in campo di un progetto politico di ampio respiro finalizzato a una governance responsabile ed eticamente orientata dell'innovazione su scala globale.

Ha probabilmente ragione Guido Scorza, tra i massimi esperti di diritto dell'informatica e delle nuove tecnologie che su queste colonne ci ha già messo in guardia: "in un contesto in cui il pensiero diventa accessibile a prescindere da ogni sua manifestazione, divenendo potenzialmente hackerabile, anche i nostri sistemi giuridici andranno "aumentati" per renderli capaci di governare fenomeni che si arricchiranno di nuove dimensioni. *L'habeas mentem* è in questa dinamica la nuova dimensione del diritto all'autodeterminazione dell'individuo, che va garantita e protetta contro ogni tentativo di limitazione e compressione".

Come si vede siamo appena all'inizio, il lavoro di comprensione della rivoluzione tecnologica in atto richiederà ancora molto tempo oltre all'impegno delle migliori intelligenze che si muovono nel Pianeta. ■

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

www.swissacademy.eu

www.cybertrends.it

web for your business
swiss webacademy

In partnership with / In parteneriato con:

THALES
Building a future we can all trust

Organize / Organizzano:

CYBERSECURITY DIALOGUES
- MEDITERRANEAN -
3rd Edition - October 12-13, 2022

UN MONDO POST-PANDEMICO IN GUERRA: CYBER-ATTACCHI A 360°

SOLUZIONI PER DIFENDERE IL VOSTRO BUSINESS.

www.cybersecurity-dialogues.org

Under the Patronage of / Con il patrocinio di:

COMUNE DI FIRENZE

CONFINDUSTRIA Toscana

CONFINDUSTRIA FIRENZE

FEDERMANAGER TOSCANA

Camera di Commercio Firenze
dal 1770 la casa delle imprese

Confservizi Cispel Toscana

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI FIRENZE

In partnership with / In partenariato con:

Gendarmerie nationale

Centre de recherche de l'EOGN

POLICE GENEVE

Regional Cyber Competence Center RC3 Western Switzerland

ROMANIA CENTRUL NATIONAL CYBERINT SERVICIUL ROMAN DE INFORMATII

OSSERVATORIO NAZIONALE PER LA CYBER SECURITY, RESILIENZA E BUSINESS CONTINUITY DEI SISTEMI ELETTRICI

START4.0

Center for Cyber Security and International Relations Studies

FIC Forum International de la Cybersécurité

Location / Indirizzo: Firenze, Innovation Center, Lungarno Soderini 21


findings
information
organisation
process
audit
incidents
application
key
management
system
continuity
plan
Compliance
practices
auditor
internal site
help
passwords
data
firewall
access
risk
financial
scope
penetration
loss
backup
procedures
meeting
report
technical
disaster