Cybersecurity Trends

Edizione italiana, N. 1 / 2022

INTERVISTE VIP:

GUIDO SCORZA
MICHELE COLAJANNI
MAURO CERUTI

Folder Centrale: Cloud Security

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

Tra le nuvole.

Autore: Nicola Sotira

Che si tratti di lavoro da casa, o della tanto amata didattica a distanza sino alle transazioni finanziarie e processi aziendali, il Cloud e le tecnologie ad esso correlato sono alla base di questa trasformazione digitale e dei nuovi modelli di business. Si può tranquillamente azzardare nello scrivere che il Cloud è fattore abilitante del business.

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e 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.

La pandemia ha accelerato il percorso di trasformazione digitale e anche adesso, che le organizzazioni stanno lentamente riportandosi ai livelli *pre-Covid*, il Cloud continua a restare uno strumento rilevante per accelerare i piani di trasformazione digitale offrendo soluzioni digitali intelligenti, accessibili e agili. Con l'utilizzo di tecnologie Cloud, molte delle barriere d'ingresso per la trasformazione digitale sono ridotte facilitando l'implementazione di nuovi processi digitali anche alle industrie che tipicamente hanno poco a che fare con la tecnologia e che possono, invece, raccogliere i benefici di moderne soluzioni ed infrastrutture IT. Oggi, il Cloud consente elevata scalabilità, capacità di archiviazione, accesso semplificato e in linea con le nuove tecnologie mobile.

Ovviamente, quando si parla di Cloud anche il tema della sicurezza diventa rilevante e in quest'area i fornitori di servizi stanno investendo molto e, mediamente, proteggono molto bene la loro infrastruttura. Secondo una ricerca di Gartner, molte delle violazioni che vediamo, oggi, in questo dominio, sono errori di configurazione e postura attribuibili al cliente. I servizi nel Cloud richiedono un approccio di progettazione condiviso tra l'operatore Cloud e il cliente per avere successo.

Trovare il giusto equilibrio tra sicurezza e innovazione non è semplice e spesso si trasforma in una sorta di rompicapo complesso da risolvere per tutte quelle organizzazioni che si avventurano in un processo spinto di trasformazione. L'unico modo per risolvere il rompicapo è integrare i gruppi di trasformazione con i team di cyber security costruendo un percorso in cui la strategia di sicurezza è presente sin dall'inizio. Per garantire un giusto equilibrio occorre una solida strategia di cyber security assolutamente in linea con gli obiettivi della trasformazione digitale e del business. Una sicurezza che deve essere coinvolta nei diversi *stream* progettuali.

Su tutte queste considerazioni occorre inserire anche le tematiche di compliance e legislative. Altro tema nuovamente in discussione è il **Cloud Act** (legge federale americana del 2018) che consente a servizi segreti e Forze dell'ordine di poter accedere a tutti i dati archiviati dalle aziende americane anche se questi sono collocati al di fuori del territorio degli Stati Uniti. Norma che cozza non poco con quanto previsto dal GDPR, giusto per citare uno degli attori. Stati Uniti e Unione Europea stanno di nuovo tornando sul tema con gli americani che dichiarano di impegnarsi nell'assicurare che le attività di monitoraggio siano proporzionate agli obiettivi di sicurezza nazionale. Insomma, come leggerete in questo numero, diverse le partite aperte sul tema che ci fanno capire che vivere tra le nuvole richiederà un certo impegno. ■

La transizione al cloud, un percorso obbligato per tutti i settori.

Autore: Rossella Macinante

Il Cloud non rappresenta più un'opzione per le aziende, soprattutto per quelle che vogliono competere con successo e conseguire obiettivi di crescita, essendo uno dei principali abilitatori di nuovi modelli di business e offrendo quelle caratteristiche di flessibilità e scalabilità di cui le organizzazioni di qualunque settore non possono più fare meno.

BIO

Rossella Macinante è BU leader in NetConsulting cube degli ambiti Cybersecurity, Government e Finance, con un'esperienza consolidata nell'analisi delle evoluzioni tecnologiche che abilitano i processi di digitalizzazione delle imprese e, in particolare, sui trend della Cybersecurity presso le aziende italiane e sull'andamento dei suoi principali attori. Da 5 anni è responsabile del progetto Barometro Cybersecurity 4.0, che si struttura in una serie di incontri nel corso dell'anno su temi di rilevanza in ambito cybersecurity su cui si confrontano aziende della domanda e dell'offerta. Il Barometro, inoltre, si basa su una survey finalizzata a fornire un quadro esaustivo, costantemente aggiornato e completo sul livello di maturità in ambito Cybersecurity delle principali aziende e organizzazioni italiane.

Nel Barometro Cybersecurity 2021, la survey condotta da NetConsulting cube su circa 80 aziende ed enti della Pubblica Amministrazione, in prevalenza di grandi dimensioni, risulta che il 90% del campione ha implementato almeno una tipologia di servizio Cloud, con prevalenza di utilizzo di ambienti ibridi (circa il 51% del panel).

Fonte: Barometro Cybersecurity 2021

L'emergenza sanitaria ha accelerato il processo di migrazione per coloro che lo avevano già intrapreso e ha posto coloro che guardavano ancora al cloud con scetticismo di fronte a una strada a senso unico, in cui il cloud rappresentava l'unica soluzione per garantire continuità nell'erogazione dei servizi e in alcuni casi addirittura i fattori minimi per la sopravvivenza sul mercato.

Un 30% dal panel, in prevalenza dei settori Energy-Utility, Telecomunicazioni e Industria, risulta aver già migrato in Cloud carichi di lavoro superiori al 50%, a prescindere dal modello implementato. Inoltre, un ulteriore 42% ha già introdotto strategie multicloud, intese in particolare come l'utilizzo di fornitori differenti in ambienti infrastrutturali e di piattaforma. Anche in questo caso, Energy-Utility e le grandi aziende industriali sono i settori che hanno implementato con maggiore frequenza questo modello.

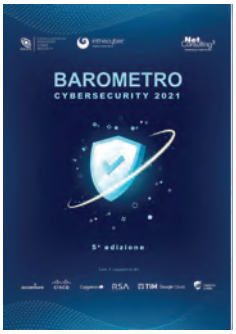
Ma una testimonianza ancora più significativa della portata dirompente che sta assumendo questa tecnologia è data dal fatto che la migrazione al cloud è inclusa nei piani strategici delle principali aziende italiane (Enel, Intesa Sanpaolo solo per fare qualche esempio) e si parla di cloud journey per indicare un percorso evolutivo che non riguarda solo un'innovazione delle architetture tecnologiche, ma anche un processo di cambiamento organizzativo e di change management

I rischi da considerare

Come tutte le tecnologie innovative, l'adozione del cloud deve tener conto di costi e benefici che la migrazione comporta e delle aree di attenzione che, se non valutate e analizzate in modo opportuno, possono trasformarsi in criticità. Una dei punti principali da considerare è la sicurezza nel cloud, con riferimento sia ai dati che vengono trasferiti nella nuvola sia alla governance della relazione con il cloud provider.

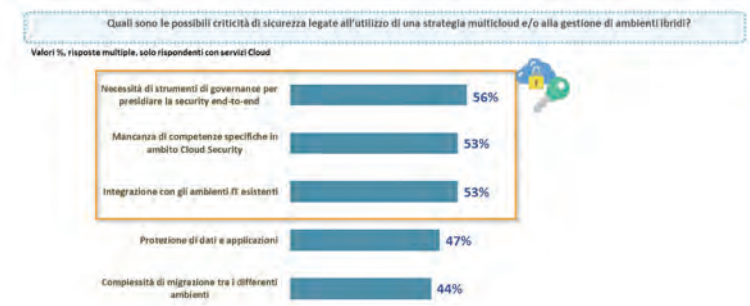
Non a caso, sempre con riferimento al panel del Barometro Cybersecurity, la necessità di avere strumenti di governance che consentano di presidiare la sicurezza con un approccio end-to-end, è citata come aspetto importante dal 55% delle aziende che adottano il cloud.

Ma è soprattutto la protezione dei dati nel cloud a rappresentare la principale preoccupazione per le aziende, tenuto conto anche delle normative vigenti come la GDPR. Nella Cloud Security Survey, indagine svolta dal SANS Institute su circa 300 aziende attive in tutto il mondo, che adottano le architetture di Public Cloud, protezione di dati, competenze interne, tematiche di integrazione e migrazione sono le principali criticità in tema di sicurezza.



Più in dettaglio, l'accesso non autorizzato ai dati da parte di estranei (56%) è la principale fonte di preoccupazione in termini di sicurezza. Possibile compromissione di dati e informazioni del Cliente presso i siti del service provider sono uno dei principali rischi che le aziende considerano nella migrazione al cloud.

I rischi relativi all'integrità o all'indisponibilità di dati possono essere determinati da diversi fattori, solo a titolo esemplificativo si citano: una cattiva configurazione degli ambienti e la vulnerabilità dei meccanismi di segregazione; l'intercettazione da parte di malintenzionati dei dati in transito dal cliente al cloud provider o tra i diversi siti del cloud provider; attacchi di Denial of Service finalizzati ad esaurire le risorse del Cloud Service Provider, rallentando l'accesso ai dati e ai servizi; la perdita o compromissione delle chiavi crittografiche, con possibile indisponibilità o sottrazione dei dati.



Fonte: Barometro Cybersecurity 2021

Tra gli altri elementi che minacciano la sicurezza aziendale, va segnalata la configurazione non adeguata e comunque non sicura delle API (54%), la mancanza di competenze/ formazione in materia di sicurezza del Cloud (53%), la scarsa visibilità di quali dati sono elaborati nel Public Cloud e su quali risorse (53%), la presenza di componenti applicative o istanze di calcolo non autorizzate (51%).

Al di là dei rischi tecnologici, sono da considerare attentamente anche i rischi organizzativi tra cui uno dei principali è il rischio di lock-in, che si traduce nella difficoltà nel cambiare fornitore o nel re-internalizzare i servizi. Tale dipendenza può essere dovuta alla mancanza di competenze specifiche e risorse internamente al Cliente o all'utilizzo di Cloud Service Provider che impiegano diffusamente tecnologie proprietarie poco interoperabili. In particolare, uno dei principali rischi di Lock in è legato alla portabilità dei dati.

Cloud Computing e GDPR

In un contratto di fornitura di servizi cloud, il cloud provider assume il ruolo di responsabile esterno del trattamento rispetto all'azienda o al soggetto che deposita i dati nel cloud, che è titolare del trattamento.

Il fornitore di cloud, quale responsabile, risponde per i danni occorsi ad un interessato solo in caso di non corretto adempimento degli obblighi previsti dalle norme in capo al responsabile stesso, oppure se ha agito in

modo difforme rispetto a quanto definito negli accordi contrattuali con il titolare del trattamento.

Un aspetto fondamentale riguarda le misure di sicurezza implementate dal fornitore di cloud computing. Pertanto, prima di procedere ad utilizzare un servizio di cloud, è necessario effettuare una mappatura dei dati che saranno elaborati esternamente, in modo da identificare dei cluster a cui corrispondano diversi livelli di tutela.

In tale prospettiva sarà, quindi, necessario ottenere le seguenti informazioni dal provider di cloud:

- l'eventuale utilizzo di tecnologie di archiviazione con separazione (fisica o logica) dei dati tra i vari "clienti" del provider;
- l'eventuale utilizzo di sistemi di etichettatura per impedire che i dati vengano replicati in determinati paesi o regioni;
- l'eventuale utilizzo di sistemi di cifratura dei dati e di gestione delle policy di accesso, con registrazione degli accessi tramite log;
- l'eventuale utilizzo di sistemi di comunicazione sicura (SSL/TLS) per l'accesso ai dati via browser.

Un aspetto importante riguarda la cifratura dei dati, generalmente fornita per la trasmissione o lo storage dei dati ma non nella fase di elaborazione, in quanto spesso il dato viene utilizzato dalla piattaforma per alimentare un sistema di intelligenza artificiale.

La nuova strategia di Cloud Nazionale

Il cloud è uno degli assi fondamentali della trasformazione digitale del Paese e della Pubblica Amministrazione ed è al centro della "Strategia Cloud Italia" che definisce obiettivi e linee guida per l'implementazione dei servizi cloud in Italia, affermando il principio cardine dell'approccio "Cloud First", già obiettivo strategico definito nel Piano Triennale per l'Informatica della PA 2019-2021, ribadito nella riedizione del Piano 2020-2022, che sottolinea come le pubbliche amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, debbano adottare primariamente il paradigma cloud, tenendo conto della necessità di prevenire il rischio di lock-in.

Controllo dei dati, autonomia tecnologica e sovranità digitale, resilienza sono gli aspetti fondamentali della nuova strategia di cloud nazionale che, peraltro, si riagganciano alla direttiva NIS e al Perimetro di Sicurezza Nazionale Cibernetica.

La strategia Cloud per la PA si declina quindi sulla base delle seguenti linee di indirizzo strategico:

- Classificazione dei Dati e dei Servizi secondo tre livelli: strategico, critico e ordinario. La classificazione dovrà tener conto del danno stimato per il sistema Paese che potrebbe derivare da una loro compromissione. Inoltre, la classificazione rappresenta uno dei principali criteri nella scelta del cloud provider e della modalità del servizio;
- Qualificazione dei Servizi Cloud: per semplificare e regolamentare l'acquisizione di servizi Cloud da parte delle PA, dal punto di vista tecnico (ad es. gestione operativa, sicurezza) e amministrativo (ad es. condizioni contrattuali);
- Polo Strategico Nazionale: che dovrà garantire adeguati livelli di continuità operativa e tolleranza ai guasti per i servizi strategici e critici della PA. A tale scopo, la strategia prevede che il PSN sia distribuito geograficamente sul territorio nazionale presso siti opportunamente identificati. La gestione operativa del PSN sarà affidata a un fornitore qualificato, selezionato tramite gara europea e l'infrastruttura sarà progettata nel rispetto degli standard di interoperabilità dei dati definiti a livello europeo, di conseguenza, con l'iniziativa Gaia-X per consentire il libero scambio di dati non personali tra i vari Stati membri interconnettendo i loro modelli cloud nazionali.

Come si comprende facilmente il tema dei dati e della loro classificazione è ancora una volta centrale, dal momento che determinerà la tipologia di cloud su cui dovranno risiedere, e nello stesso tempo è necessario avere delle linee guida puntuali e definite per consentire agli attori in gioco di effettuare le scelte in modo conforme con la normativa.

In conclusione, in considerazione delle possibili minacce e degli impatti che potrebbero avere sul business, qualsiasi processo di migrazione al cloud non può prescindere da un'analisi del rischio sui servizi esternalizzati che tenga conto di alcuni elementi, a partire dalla classificazione dei dati migrati verso il cloud in termini di strategicità per il business e/o di riservatezza. È evidente che l'essenzialità/criticità per l'azienda di ciascun servizio che viene migrato su cloud è un altro aspetto da prendere in considerazione insieme alla tipologia di cloud e al modello di servizio. Un ulteriore punto di attenzione riguarda la continuità del processo di analisi del rischio che dovrà essere reiterato periodicamente nel corso del rapporto per aggiornare la valutazione dei rischi e dei relativi impatti.

È fuori dubbio che il percorso di evoluzione verso il cloud è complesso e comporta investimenti sia in tecnologia che in skill, oltre che una riorganizzazione interna all'IT e ad altre funzioni (si pensi alle diverse competenze che dovranno avere i responsabili del procurement e degli uffici legali), ma si tratta di un processo che è inevitabile per i benefici che comporta e per poter tenere il passo con le evoluzioni del mercato. ■

Multi-Cloud ibrido: quali sfide ci attendono.

Autore: Federica Maria Rita Livelli

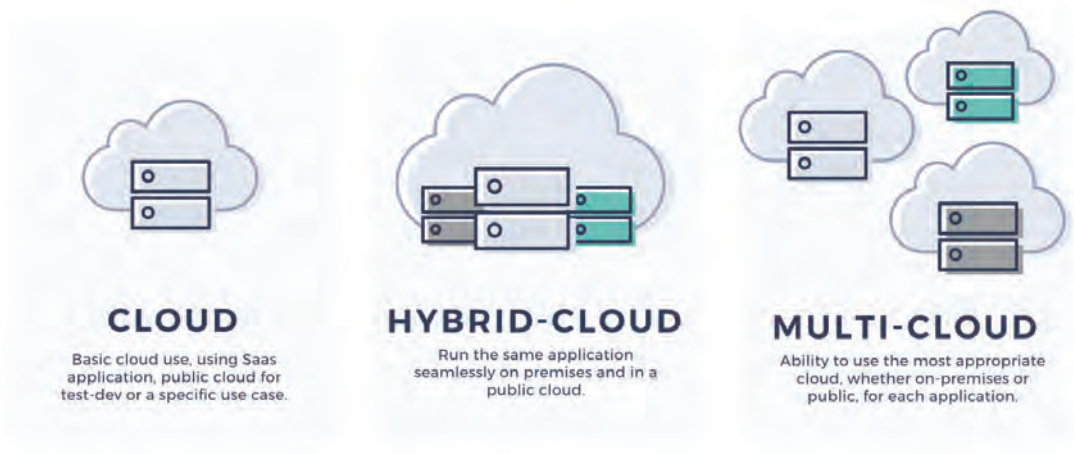
Scenario

L'adozione di modalità di lavoro flessibile è letteralmente esplosa con l'emergenza sanitaria degli ultimi due anni e, contemporaneamente, il cloud si è convertito in un fattore chiave della crescita aziendale, contribuendo ad accelerare l'implementazione di nuove tecnologie per migliorarne le prestazioni e accelerare il processo di digitalizzazione ed innovazione in atto.

In particolare, il mercato del cloud ibrido si sta sempre più sviluppando e, secondo la società di ricerca *Mordor Intelligence*, è destinato a registrare un aumento medio annuo (CAGR) del 21,06% nel periodo 2022-2026. Inoltre, si sta altresì affermando una crescente tendenza a adottare soluzioni di multi-cloud ibrido, come confermato dal recente studio *Enterprise Cloud Index (ECI)* e, precisamente: il 36% delle imprese intervistate a livello globale stanno già utilizzando soluzioni di multi-cloud ibrido e si ritiene che tale percentuale, in un orizzonte temporale di 1-3 anni, potrebbe giungere al 64%.

L'uso di piattaforme multi-cloud ibride rappresenta uno strumento fondamentale per garantire l'accesso alle risorse e ai servizi indispensabili per il lavoro in remoto e in mobilità e, la crescita significativa del mercato del multi-cloud ibrido rispetto a quello degli altri servizi cloud è determinata dal fatto che offre alcuni vantaggi richiesti dalle organizzazioni con un enorme set di dati e che necessitano di elaborazione.

Di fatto, l'utilizzo di un multi-cloud ibrido consente alle aziende di scalare le risorse di elaborazione ed eliminare la necessità di investire un capitale enorme per gestire picchi di domanda a breve termine, anche nei casi in cui l'azienda ha bisogno di liberare risorse locali per dati o applicazioni più sensibili.



Multi-cloud ibrido: come approcciarlo

È doveroso ricordare che l'ambiente multi-cloud ibrido elimina l'utilizzo di un singolo cloud, fornendo l'utilizzo di due o più cloud pubblici e anche di cloud privati e convertendosi in una leva strategica per garantire i processi aziendali e le regole del business estremamente *"agile"* ed *"adaptive"*.

Di fatto, grazie al multi-cloud ibrido le organizzazioni sono in grado di trasferire i carichi di lavoro ovunque (i.e. che si tratti di un cloud pubblico, di un data center on-premise o dell'edge) oltre a permettere alla funzione IT di acquisire tutta la flessibilità necessaria per accelerare la trasformazione digitale dell'organizzazione.

Inoltre, in termini di privacy e sicurezza, le organizzazioni altamente regolamentate possono utilizzare con successo il multi-cloud ibrido per conservare informazioni sensibili on-premise, mentre i carichi di lavoro meno sensibili sono trasferiti al cloud, garantendo prestazioni migliori e risparmi sui costi.

Inoltre, una strategia multi-cloud ibrida garantisce:

- una non dipendenza da un unico fornitore
- una maggiore flessibilità e scalabilità
- un maggior controllo granulare necessario per conformarsi a leggi complesse che possono variare notevolmente tra le giurisdizioni nazionali e regionali.

Tuttavia, la tecnologia da sola non basta e risulta essenziale, da parte da parte dei team IT aziendali, adottare un approccio ponderato, strategico e dettagliato per garantire una corretta ed efficiente implementazione del multi-cloud ibrido attraverso:

- l'analisi del contesto interno ed esterno in cui opera l'organizzazione in modo tale da ottenere un censimento dei prodotti hardware e software;
- l'identificazione di potenziali rischi a fronte dello scenario di attacchi informatici sempre più in aumento e la cyberwar in atto;
- la misurazione degli impatti dei rischi individuati;
- l'attuazione delle misure atte a ridurre al minimo la propria superficie di attacco;
- l'attuazione di una politica di sicurezza organizzativa complessiva.

L'organizzazione, in questo modo, è in grado di intraprendere un percorso di conoscenza delle interconnessioni tra business e sistemi informativi.

Risk Management, Business continuity & Cybersecurity vs. Multi-cloud ibrido

È doveroso ricordare che le organizzazioni, nel percorso di adozione del multi-cloud ibrido, possono trarre enorme beneficio dall'implementazione dei principi di

BIO

In possesso della certificazione Business Continuity - AMBCI BCI, UK e CBCP DRI, USA, Risk Management FERMA Rimap ®, consulente di Business Continuity & Risk Management, Federica Maria Rita Livelli svolge attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università. È membro di: Board ANRA; Board del BCI Italy Chapter; Comitato Scientifico di CLUSIT; Women for Cyber Security (Comitato Tecnico); varie commissioni tecniche UNI. È Docente di moduli di introduzione di: ISO 22301 - Business Continuity & Resilience (Università POLIMI–BOCCONI e Università di Verona, Università di Cagliari, Master Ambientale Università di Padova, Università di Castellanza LIUC); ISO 31000 - Risk Management (Università Statale di Milano e Università di Castellanza, LIUC); relatrice e moderatrice in diversi seminari, conferenze nazionali ed internazionali. Autrice di numerosi articoli su diverse riviste online oltre aver partecipato, in qualità di co-autrice, a: Edizioni 2019, 2020, 2021 e 2022 del Rapporto Clusit - Cyber Security; Libri tematici CLUSIT rif. Intelligenza Artificiale (2020) e Rischio Cyber (2021); Libro "Lo Stato in Crisi" (2021) ed. Angeli.

Risk Management, Business Continuity Management e Cyber Security Management. Queste discipline, di fatto, si convertono in leve strategiche e supportano le organizzazioni ne:

- la progettazione ed attuazione della strategia multi-cloud ibrido in un'ottica *risk-based* e *resilience-based*;
- il completamento del processo accelerato di digitalizzazione e innovazione in atto;
- una chiara visione della governance e della compliance aziendale;
- la conformità dei requisiti regolamentari e contrattuali del mercato in cui l'organizzazione opera.

Inoltre, le organizzazioni - sempre in un'ottica *risk-based* e *resilience-based* dell'organizzazione e in termini di processo di selezione del cloud provider - dovranno verificare altresì l'implementazione da parte del cloud provider dei principi di Risk Management, Business Continuity e Cyber Security, il quale dovrà essere in grado di:

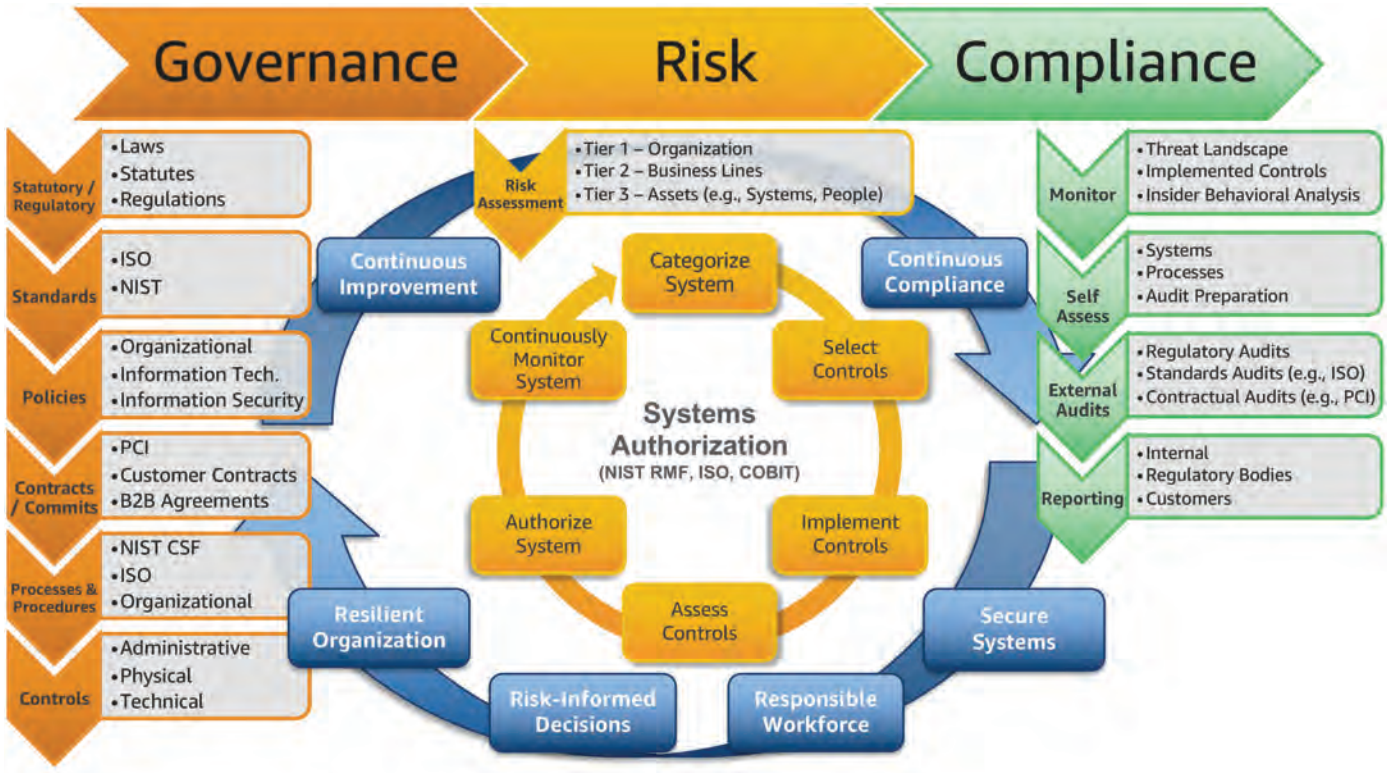
- dimostrare l'esistenza dei piani di continuità sia propri sia dei sub-fornitori;
- fornire le specifiche del data center utilizzato;
- garantire i servizi di connettività e l'alimentazione nei data center in caso di disastro/disruption;
- gestire efficientemente i guasti hardware (a tal proposito è auspicabile inserire contrattualmente la loro modalità di risoluzione);
- garantire un rapporto in termini di programmazione di test di ripristino e di emergenza;
- garantire l'autenticità, riservatezza, integrità e disponibilità dei dati.

La sicurezza del multi-cloud Ibrido

In uno scenario sempre più incerto dal punto di vista della cybersecurity risulta fondamentale non affidarsi completamente al multi-cloud ibrido per la sicurezza dal momento che, sebbene strumenti come l'autenticazione a due fattori, la crittografia e gli avvisi automatici possano aiutare a proteggere le reti, in realtà nessuna rete è inviolabile, soprattutto se non sono state applicate misure di sicurezza aggiuntive. Pertanto, una buona strategia di sicurezza del multi-cloud ibrido dovrebbe contemplare la garanzia di:

- una corretta configurazione;
- un aggiornamento delle patch dei sistemi hardware e software;
- l'archiviazione di backup dei dati e l'archiviazione offline.

Le organizzazioni, in questo modo, saranno in grado di affrontare le sfide chiavi che l'adozione del multi-cloud ibrido comporta in termini di



sicurezza, conformità, fiducia, problemi di prestazioni e, ove necessario, attuare una strategia di trasformazione dei criteri aziendali, in modo tale da garantire:

- una governance migliore
- una maggiore conformità
- un maggior valore aziendale
- un aumento dell'efficienza operativa e privacy
- una mitigazione dei rischi di sicurezza
- una maggiore visibilità digitale e dei dati

Così facendo, sarà possibile attuare un approccio olistico atto a garantire una visibilità costante su end-point, sulle reti e persino su più ambienti cloud. Inoltre, l'adozione di un approccio zero-trust e l'introduzione di una maggiore automazione supportata da AI e ML possono contribuire ulteriormente a mantenere la sicurezza del multi-cloud ibrido, senza dimenticare che è altresì importante potersi avvalere di personale IT qualificato e continuamente aggiornato.

Ricordiamo che, soprattutto quando si tratta di infrastrutture critiche, la continuità di erogazione dei servizi di pubblica utilità ha la massima priorità e deve essere mantenuta, per assicurare che non si verifichino danni alle persone, all'ambiente, ai sistemi di processo. Pertanto, la sicurezza deve essere sempre più diffusa, aggiornata e strutturata secondo criteri solidi, validati e condivisi.

Ombre sull'orizzonte olistico

L' adozione del multi-cloud ibrido di questa tecnologia, pur essendo un punto di svolta per le organizzazioni, non è scevra di ombre. Di fatto, il multi-cloud ibrido, se da un lato fornisce alle organizzazioni la scalabilità e la flessibilità per rimanere competitive e innovative in uno scenario globale in continua evoluzione, dall'altro lato comporta una gestione di nuovi rischi per la sicurezza e rende sempre più necessario salvaguardare i dati aziendali a fronte di una varietà di fattori.

Conclusioni

Le organizzazioni - a fronte del continuo proliferare di problematiche legate alla cybersecurity - considerano come requisito fondamentale l'adozione di soluzioni IT resilienti e flessibili. Ne consegue che l'implementazione del multi-cloud ibrido si rivela come il percorso più naturale per gestire olisticamente i rischi, la continuità operativa e la cybersecurity dell'organizzazione. Tuttavia, considerate le ombre cui abbiamo appena accennato, l'organizzazione, per garantire la propria resilienza organizzativa ed operativa, dovrà implementare gli standard di cybersecurity del cloud, i principi di Risk Management e Business Continuity, oltre a incorporare le raccomandazioni e adottare le check list rese disponibili da organismi internazionali come la *Cloud Security Alliance (CSA)* in grado di chiarire le migliori pratiche e fornire linee guida su come gestire i vari tipi di cloud e i rischi che essi comportano. ■

Sicurezza e visibilità a 360° - dal codice al cloud.

Autori: Ivan Tresoldi e Andrea Rossini

Approccio Multi-Cloud: come cambia il perimetro di protezione?

Per comprendere il valore e l'opportunità del cloud, dobbiamo concentrarci su come le organizzazioni abbiano adottato ambienti hybrid e multi-cloud. Che si tratti di nuovi progetti o di fusioni e acquisizioni, il multi-cloud è la nuova normalità. Secondo Gartner, l'81% delle organizzazioni ha dichiarato di lavorare con due o più provider di cloud pubblico.

Come sempre, al proporsi di nuove opportunità, è necessario effettuare una nuova valutazione dei rischi, in quanto in una realtà multi-cloud e con sviluppo di applicazioni in modalità cloud native, si presenta di fronte a noi un nuovo perimetro di sicurezza rispetto a quanto siamo stati abituati a trattare in passato.

Di seguito andiamo a porre l'attenzione sui principali ambiti di sicurezza, in una realtà cloud-native e multi-cloud:

- La conformità (compliance), in particolare per i dati in cloud, è un rischio molto importante: secondo la Unit 42 di Palo Alto Networks, il 43% dei database cloud non è crittografato. Tale tipologia di configurazione, oltre ad essere non aderente alle normali best-practices, potrebbe risultare un'inadempienza rispetto ad uno o più requisiti dei principali compliance standard, con evidenti conseguenze.
- Vulnerabilità nelle applicazioni: indipendentemente dal fatto che si utilizzino macchine virtuali cloud, container o funzioni serverless, è necessario il continuo monitoraggio delle stesse al fine di rilevare la presenza di eventuali vulnerabilità. Il 91% di tutte le immagini container pubbliche analizzate dalla Unit 42 presentava almeno una vulnerabilità critica o di gravità elevata.
- Configurazioni di rete e comunicazioni non sicure che possono lasciare i dati e le applicazioni esposte: secondo la Unit 42, il 60% delle organizzazioni ha configurazioni di rete non sicure. Per applicazioni che operano in ambienti multi-cloud e ibridi, la protezione delle reti continua ad essere essenziale.
- Errate configurazioni di servizi cloud nativi: pensiamo ad esempio ad un oggetto storage (bucket) contenente dati sensibili, personali, finanziari, che venga erroneamente esposto pubblicamente. Questo tipo di configurazione non può essere prevenuta con i tradizionali meccanismi di protezione a livello network, in quanto una configurazione errata renderà immediatamente fruibili a chiunque su internet le informazioni contenute in esso, tramite un comune browser.
- Rischi legati alle identità ed ai privilegi (IAM): questo è ad oggi considerabile come il principale nuovo perimetro da proteggere. Alla maggior parte delle identità (utenti, ruoli, servizi ecc.) create nel public cloud, vengono assegnati privilegi eccessivi, non rispettando il noto principio del "least privilege". La Unit 42 evidenzia come il 66% delle organizzazioni in tutto il mondo utilizzi le chiavi di accesso (access keys) per più di 90 giorni. Un'identità con privilegi eccessivi può causare danni enormi con una singola chiamata API.
- La cosiddetta Software Supply-Chain, ossia tutto quanto ruota intorno alle pipeline CI/CD per la creazione di software e/o infrastruttura (IaC) ed alla provenienza dei diversi elementi che compongono le applicazioni moderne. In questo contesto troviamo moltissimi ambiti di possibile vulnerabilità che dobbiamo governare, in quanto molto spesso si attinge ad oggetti di cui non si conosce/governa l'esatta provenienza e la corretta configurazione, e

che potrebbero facilmente nascondere minacce: template IaC, dipendenze (pacchetti) vulnerabili, strumenti di gestione delle pipeline configurati in maniera errata, immagini container (in registry pubblici o privati) contenenti vulnerabilità critiche o codice malevolo, errata gestione dei privilegi, errata gestione di chiavi e secrets, mancato hardening degli strumenti di controllo di versione (VCS).

Questi sono alcuni esempi di come la superficie di esposizione si sia molto ampliata, portando con sé nuovi rischi e conseguentemente nuove tipologie di controlli e meccanismi di protezione che è necessario implementare, al fine di garantire la sicurezza di un bene prezioso come i nostri dati.

Le fasi di maturità nell'approccio al Cloud

Il primo modo in cui le organizzazioni sono passate al cloud è tramite migrazione in modalità lift-and-shift. Con questo approccio, le organizzazioni si sono concentrate sullo sfruttamento della virtualizzazione nel cloud pubblico per ridurre l'impronta (footprint) dei data center on-premises. Sebbene questo sia stato uno sforzo importante degli ultimi anni, ora vediamo le architetture delle applicazioni native del cloud, le cosiddette cloud-native applications, come il nuovo obiettivo per i nostri clienti.

Con questo nuovo approccio, le organizzazioni stanno sfruttando le tecnologie cloud native, in cui le architetture basate sui microservizi come container, Kubernetes, Platform-as-a-Service (PaaS) e serverless consentono di attivare e disattivare le applicazioni on-demand. Queste architetture consentono anche moderni flussi di lavoro basati su GitOps e DevOps, in cui le applicazioni vengono distribuite utilizzando l'automazione con rilasci settimanali, giornalieri, o addirittura ancora più frequenti. È importante sottolineare che le applicazioni cloud native possono essere eseguite in cloud pubblici o privati, per sfruttare i moderni stack tecnologici offerti dai provider di servizi cloud oppure dai principali attori dell'ecosistema self-hosted.

Man mano che i clienti avanzano nell'adozione del cloud riconoscono la necessità di un numero crescente di funzionalità e controlli necessari per proteggere i propri ambienti.

In Palo Alto Networks, lavorando quotidianamente a stretto contatto con numerose organizzazioni, riscontriamo come sia quelle che abbiano affrontato una migrazione lift-and-shift verso il cloud pubblico, sia quelle che siano nate con un approccio cloud-native o che vi stiano migrando, hanno in comune la ricerca di diverse funzionalità di sicurezza, tra cui:

BIO

Ivan Tresoldi è Prisma Cloud Solutions Architect in Palo Alto Networks. Ivan vanta più di vent'anni di esperienza nel settore IT ricoprendo vari ruoli strategici in società multinazionali e vendor, specializzandosi nella progettazione di soluzioni end-to-end che mappano i requisiti aziendali sulle soluzioni tecnologiche.

BIO

Andrea Rossini ricopre il ruolo di System Engineer Specialist per le soluzioni Cortex di Palo Alto Networks. Con oltre 20 anni di esperienza nel mondo della Cyber Security ha ricoperto diversi ruoli come Consultant, Business Unit Manager, System Engineer e Solutions Architect in società di consulting e multinazionali del settore. Grazie a questo esteso background di esperienze si è altamente specializzato nell'analisi e progettazione di soluzioni di Cyber Security, comprendendo come fornire soluzioni di sicurezza e coniugare le esigenze del business. Nel corso degli ultimi anni si è fortemente specializzato in tematiche di Cyber Resilience ed Incident Response. Andrea si è laureato in Informatica presso l'Università Statale di Milano dove ha successivamente conseguito il Master in ICT Security e possiede inoltre le certificazioni ISC2 CCSP, ITIL e CompTIA Security+.

- Visibilità, conformità e governance, per identificare le configurazioni errate delle risorse nel cloud pubblico, imponendo la governance sulle configurazioni e garantendo che gli oggetti creati nel cloud soddisfino i requisiti di conformità, che siano essi standard e regolamentazioni (e.s. PCI-DSS, GDPR ecc.) oppure standard proprietari, specifici della singola realtà interna all'organizzazione stessa. Ulteriore esigenza è sicuramente quella di rilevare le minacce avanzate, come il crypto mining o le compromissioni degli account.
- Implementare la "Workload Security", per proteggere i propri host, container e funzioni serverless. Le aziende vogliono proteggere i propri workload dalle vulnerabilità, prevenire le minacce che si presentano a runtime e proteggere le applicazioni Web e le API.
- Implementare funzionalità di sicurezza di rete come la microsegmentazione, per contenere il movimento laterale, e le funzionalità NGFW per prevenire in modo proattivo le minacce basate sulla rete.

- Gestire la Identity Security, un caso d'uso emergente che aiuta le organizzazioni a rafforzare la gestione delle identità e la gestione degli accessi, oltre a garantire che non siano utilizzate identità con privilegi eccessivi.

Le organizzazioni con approccio applicativo cloud native, che siano ospitate su cloud privati oppure pubblici, cercano inoltre di:

- Identificare le configurazioni errate il prima possibile nel processo di sviluppo Infrastructure-as-Code (IaC), la cosiddetta "Application Lifecycle Security". Ciò significa identificare le problematiche il prima possibile, quando si sta scrivendo il codice piuttosto che una volta che l'applicazione sarà già in esercizio (approccio noto come «shift left»).

Le organizzazioni ambiscono a gestire tali funzionalità in modalità integrata in un'unica piattaforma, invece di doverle gestirle in silos.

Purtroppo, secondo lo State of Cloud Native Security Report 2022, circa il 75% degli intervistati ha dichiarato invece di utilizzare più di 6 strumenti di sicurezza cloud. Gartner stima che le organizzazioni stiano integrando manualmente "10 o più strumenti di sicurezza disparati".

L'utilizzo di questo numero significativo di soluzioni puntuali aggiunge sfide per i team di sicurezza e introduce lacune nella visibilità, tra cui:

- Un quadro incompleto del rischio: se si dispone di più strumenti nella pipeline ed in fase di esecuzione, ad esempio uno strumento CSPM (Cloud Security & Posture Management), uno strumento autonomo di gestione delle vulnerabilità, più strumenti di protezione a runtime per diversi stack tecnologici ed un WAF, quello che mancherà sarà sicuramente una vista centralizzata del profilo di rischio.
- Più console portano a una maggiore complessità: se i team di sicurezza e infrastruttura cloud passano costantemente da una console all'altra, spendono tempo e risorse preziose per confrontare risultati e dati, piuttosto che affrontare problemi di sicurezza o gestire i rischi.
- La mancanza di policy centralizzate crea un sovraccarico aggiuntivo: le organizzazioni che utilizzano strumenti open source o soluzioni puntuali dedicano una notevole quantità di tempo alla creazione di policy e alla correlazione delle policy tra diversi fornitori e strumenti.

In un quadro così complesso, come possiamo quindi proteggerci dalle minacce, note e non-note, che la nuova realtà porta con sé?

Sarà necessario pensare non solo ad un approccio reattivo, quindi ad individuare le problematiche in essere e risolvere, ma sarà altrettanto fondamentale implementare un approccio proattivo, andando ad individuare quelli che sono i potenziali problemi prima che diventino problemi effettivi, risolvendoli all'origine.

Come posso proteggermi?

Per noi di Palo Alto Networks, la risposta è sicuramente Prisma Cloud, la nostra piattaforma di protezione delle applicazioni cloud native, che rientra nella categoria che Gartner ha definito CNAPP, ossia Cloud Native Application Protection Platform.

Caratteristiche peculiari che una piattaforma CNAPP come Prisma Cloud deve avere sono le seguenti:

- Proteggere infrastruttura, applicazioni, identità, reti e dati in un'unica piattaforma ed in logica multi-cloud.
- Garantire la flessibilità della protezione agentless e della protezione basata su agent per host, container e ambienti serverless.
- Integrazione dei controlli di sicurezza con gli strumenti SecOps, per risolvere rapidamente problemi e allarmi.
- Copertura completa per tutto il ciclo di vita dello sviluppo, dal codice al cloud.

Le numerose funzionalità che Prisma Cloud può garantire possono essere riepilogate come segue:

- **Cloud Code Security:** consente alle organizzazioni di integrare i controlli di sicurezza per i template IaC e le applicazioni cloud native nei tradizionali flussi di lavoro di sviluppatori e DevOps. Basato su strumenti open source di riferimento come Checkov, supportato dalla più ampia comunità di sviluppatori e DevOps. Inoltre, questa funzionalità consente ai team di sicurezza di gestire le policy in modo centralizzato e di visualizzare i risultati delle scansioni nella console di Prisma Cloud, mentre gli sviluppatori e i DevOps possono visualizzare i risultati nei rispettivi strumenti abituali (IDE e VCS) grazie alle integrazioni native con questi ultimi.
- **Cloud Security & Posture Management (CSPM):** include il monitoraggio dello stato di sicurezza del cloud pubblico, il rilevamento e la risposta alle minacce e il mantenimento della conformità per i framework (standard, regolamentazioni) interni ed esterni. Prisma Cloud supporta le 5 principali piattaforme cloud pubbliche (AWS, Azure, GCP, OCI, Alibaba) ed offre oltre 1000 policy predefinite.
- **Cloud Workload Protection (CWP):** protezione di host/VM, di container (standalone ed in ambienti Kubernetes, AKS, GKE, AKS, Openshift) e delle funzioni serverless, durante l'intero ciclo di vita delle applicazioni, su qualsiasi cloud ed on-premises. La funzionalità di Cloud Workload Protection può offrire diversi modelli di protezione, in modalità agentless oppure agent-based a seconda dei requisiti. La copertura garantita dalla Workload Protection include il vulnerability management, il compliance management, la protezione a runtime (network, file system, processi) e la protezione delle applicazioni Web e delle API con l'acronimo WAAS (Web Application & API Security)
- **Cloud Network Security (CNS):** queste funzionalità consente di monitorare e proteggere le reti cloud e di applicare il principio zero-trust secondo la logica della microsegmentazione. La peculiarità della funzionalità di microsegmentazione di Prisma Cloud è che quest'ultima si basa su una modalità chiamata identity-based, basata quindi sull'identità digitale dei

workload (ricavata dai metadati), e non sugli indirizzi IP, dato che in una realtà multi-cloud e in un'architettura a micro-servizi basata su container risulterebbe pressoché impossibile gestire regole di segmentazione basate su un costrutto come gli indirizzi IP.

▸ **Cloud Identity Entitlement Management (CIEM):** questa area emergente della sicurezza si riferisce all'applicazione (enforcing) delle autorizzazioni e alla protezione delle identità tra workload e cloud. Al momento della scrittura del presente articolo, Prisma Cloud supporta AWS ed Azure con integrazioni IDP che supportano Okta e Azure Active Directory.

Prisma Cloud è al centro dell'evoluzione di Palo Alto Networks, non solo come leader della sicurezza cloud globale con il 79% di copertura delle aziende della fortune 100, il 25% delle aziende facenti parte della global 2000 e oltre 2700 clienti, ma ha anche l'ambizione di divenire la soluzione di riferimento nell'ambito DevSecOps.

Per fare questo, con Prisma Cloud integriamo la sicurezza nelle tre fasi di Build, Deploy e Run del ciclo di vita di infrastruttura e applicazioni, supportando tutti i cloud e gli stack tecnologici più diffusi.

Nella fase Build, Prisma Cloud si integra con IDE, SCM e strumenti CI per scansionare le applicazioni alla ricerca di vulnerabilità e proteggere i template Infrastructure as Code da configurazioni errate. I risultati delle scansioni vengono riportati sia negli strumenti per sviluppatori e DevOps, sia nella console Prisma Cloud per la visualizzazione dei rischi, lo stato di conformità e la gestione delle policy.

Nella fase Deploy, Prisma Cloud integra i controlli di sicurezza nei flussi di lavoro e nelle pipeline (CI/CD) per prevenire implementazioni non sicure. Prisma Cloud offre le possibilità di implementare (enforcing) le policy di sicurezza nella pipeline di sviluppo al fine di bloccarne l'avanzamento in caso di configurazioni rischiose (es. build di un'immagine container con vulnerabilità critiche).

Nella fase di Runtime, Prisma Cloud protegge cloud e applicazioni con un approccio defense-in-depth, monitorando continuamente tutte le risorse, i diritti (entitlements) ed i dati del cloud pubblico, proteggendo al contempo le applicazioni su VM, container, Kubernetes e architetture serverless.

Prisma Cloud si integra con gli strumenti chiave del portfolio Palo Alto Networks, inclusi Cortex Xpanse, Cortex XSOAR, Cortex XDR e Wildfire, al fine di supportare i nostri clienti nel perseguire l'obiettivo di implementare un approccio "zero trust" proteggendo tutti gli utenti, le applicazioni, i dati, le reti e i dispositivi con un contesto completo in ogni momento, ovunque essi si trovino.

Come mantenere un'adeguata visibilità

Come detto, i progetti di Digital Transformation, che molte organizzazioni sono state costrette ad accelerare nell'ultimo periodo, hanno spinto ulteriormente verso il cloud. Questo, però, ha comportato nuove problematiche per la Cyber Security a cui, come spesso accade, il settore ha risposto con soluzioni mirate e puntuali.

L'implementazione di questo tipo di strumenti è assolutamente fondamentale per proteggere le risorse in cloud (dati, applicazioni, sistemi), ma non sufficiente. Altrettanto fondamentale è poterli sfruttare per aumentare la visibilità in ciò che succede negli ambienti cloud e incrementare le capacità di rilevamento delle minacce ad essi relative. Quando le risorse erano tutte all'interno delle proprie realtà aziendali era relativamente semplice averne piena visibilità e controllo. Ora che i processi di business si stanno spostando in cloud, è fondamentale lavorare per mantenere lo stesso livello di visibilità e controllo sulle proprie risorse così da poter ridurre e governare opportunamente il livello di rischio intrinseco in questo fenomeno nuovo. Secondo un report di Palo Alto Networks vengono aggiunti da ogni azienda mediamente 3.5 nuovi servizi ogni giorno sfruttando infrastrutture cloud[1], questo evidenzia quanto sia importante avere pieno controllo e conoscenza dei propri asset e delle possibili esposizioni ad essi associate. Workload, servizi e risorse in cloud possono sfuggire facilmente a processi di controllo e gestione pensati per ambienti on-premise statici. Diventa fondamentale dotarsi di strumenti per gestire la superficie di attacco rilevando i servizi esposti e verificando che i sistemi di protezione adottati siano adeguatamente implementati su di essi.

In aggiunta a ciò, è necessario che le diverse soluzioni di cloud security implementate vengano impiegate anche per completare e supportare la raccolta di dati e informazioni da integrare all'interno dei propri processi di Security Operation e Incident Response, utilizzandole così per arricchire di informazioni i vari sistemi di rilevamento.

È bene valutare fin da subito la scelta e l'implementazione di queste nuove tecnologie di cloud security in un'ottica strategica, per non correre il rischio di aggiungere ulteriore complessità ricavandone, di contro, solamente benefici limitati.

Alla complessità presente intrinsecamente in un'infrastruttura distribuita in cloud si andrebbe ad aggiungere ulteriore complessità portata dai nuovi sistemi di security adottati che, spesso anche perchè provenienti da fornitori o vendor differenti, non si integrerebbero tra loro e non migliorerebbero il livello di visibilità end to end.

Per migliorare il livello di visibilità end to end diventa, quindi, necessario pensare anche a:

- come gestire le informazioni generate dalle soluzioni di cloud security
- come integrarle nei processi di raccolta e analisi delle informazioni
- utilizzare opportuni modelli di detection per riconoscere le minacce relative ad ambienti cloud.

È purtroppo noto che le metodologie di sicurezza adottate per le infrastrutture on-premise non possono essere trasformate in modo semplice o diretto per adattarsi alle realtà cloud. Ecco perché risulta importante che le soluzioni di cloud security adottate diventino parte di una più ampia strategia: gli alert e i dati da essi generati devono poter confluire in un repository di informazioni comune, cui poter applicare i motori di analisi basati su Machine Learning, Artificial Intelligence e indicatori di Cyber Threat Intelligence appositamente studiati per ambienti cloud. Solo così diventa possibile rilevare anomalie che possano sottendere a una minaccia non rilevata dalla singola soluzione puntuale.

Riunendo, così, i dati raccolti dalla rete, dagli endpoint e dagli ambienti cloud e sfruttando la completezza delle informazioni raccolte, sarà possibile visualizzare in un'unica e completa sequenza temporale la relativa Kill Chain dell'attacco. Visualizzando l'attività e sequenziando gli eventi si faciliterà il lavoro dell'analista, aiutandolo a determinare la root cause della minaccia, la portata e il suo danno potenziale.

La sfida di governare ed orchestrare la crescente complessità

L'idea alla base dell'approccio XDR nasce appunto dalla volontà di ridurre drasticamente il fattore complessità che l'infrastruttura cloud necessariamente sottende.

Con XDR i team di Security Operation possono così avere:

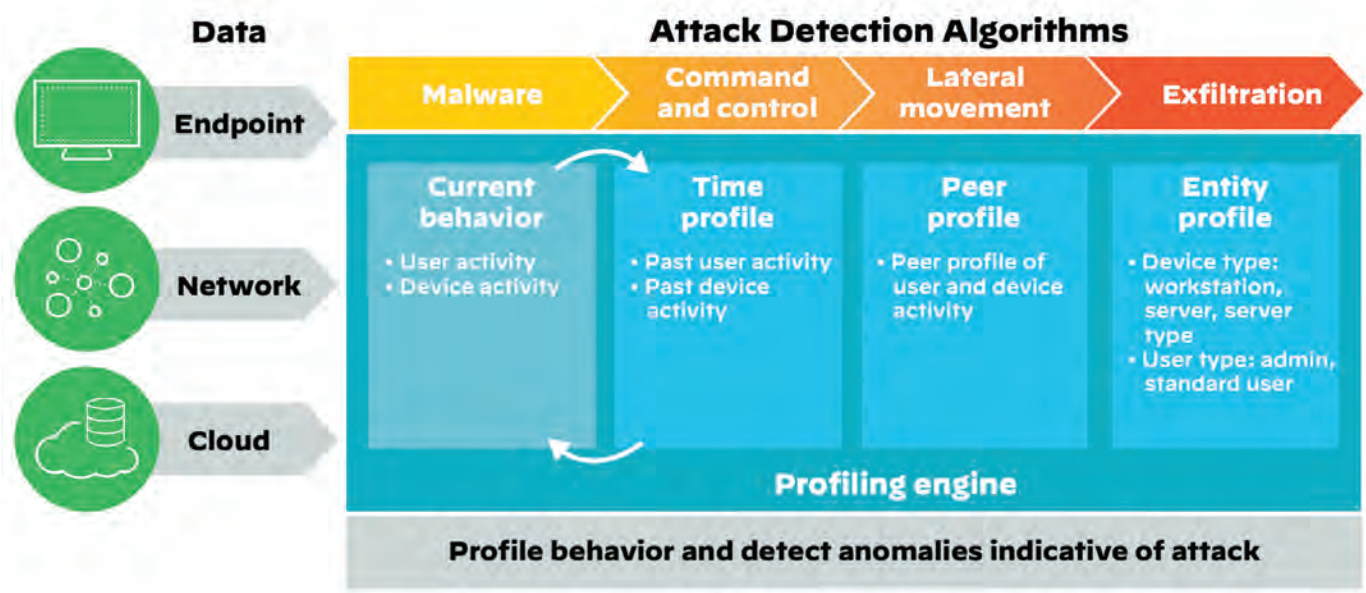
- un unico strumento su cui far confluire la telemetria e gli alert provenienti da tutte le soluzioni di sicurezza
- un unico cruscotto di controllo per le operazioni di detection, response e hunting.

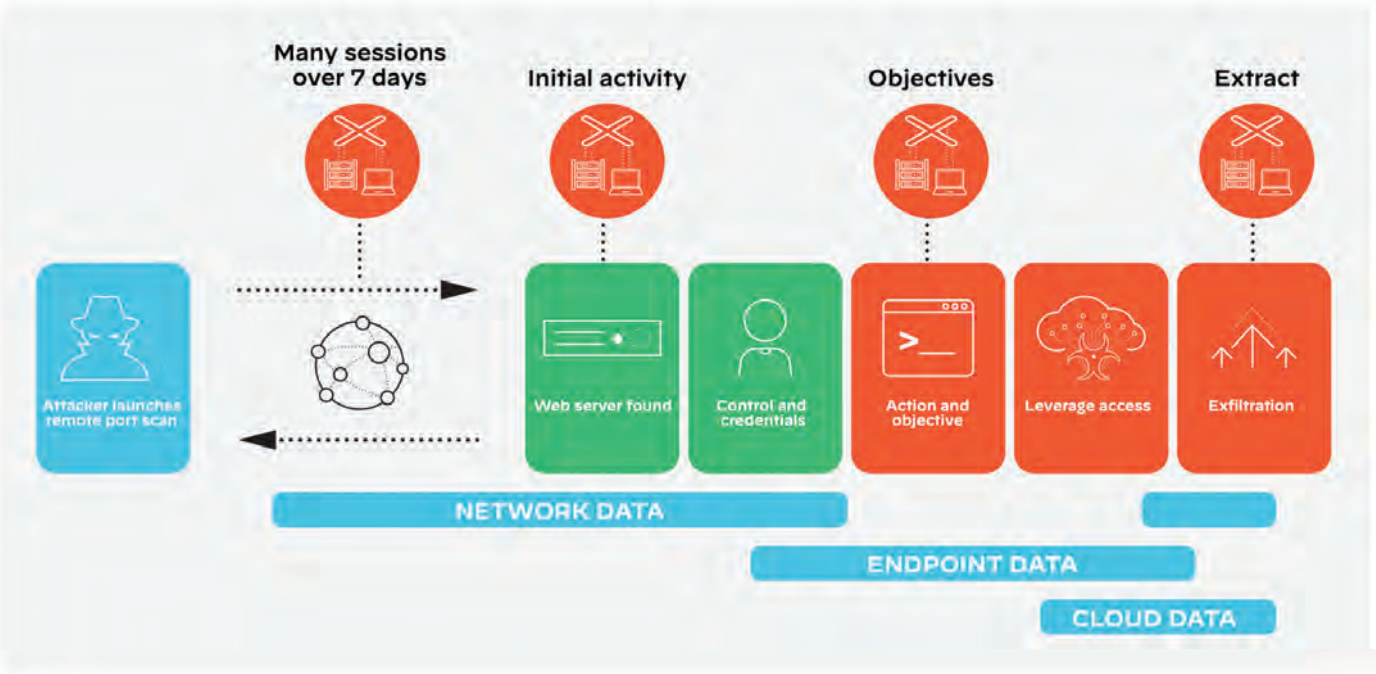
XDR riesce infatti ad integrare la telemetria proveniente dai workload nel cloud, dai container Kubernetis, dal traffico di rete, dalle informazioni e dalle attività relative alle identità in hosting nel cloud, per consentire ai team SOC di ampliare la propria copertura, dagli ambienti on-premise a quelli multi-cloud.

L'obiettivo finale da perseguire, infatti, non cambia tra ambienti on-premise, ibridi, cloud o multi-cloud: ridurre i tempi di detection (MTTD) e risposta (MTTR).

Seguendo questo approccio, il primo valore tangibile consisterebbe nell'avere una visibilità consolidata degli eventi, cui poter applicare metriche di detection avanzate, Risolto questo primo cruciale punto, bisognerebbe pensare poi all'implementazione di strumenti e processi per automatizzare le sequenze di gestione e risposta.

Le attività e i processi manuali rallentano, infatti, la risposta agli incidenti e aumentano il costo delle operazioni di sicurezza. Per questo motivo l'automazione diventa, quindi, il passo successivo e necessario per mantenere sotto controllo il livello di complessità nella gestione delle proprie infrastrutture.





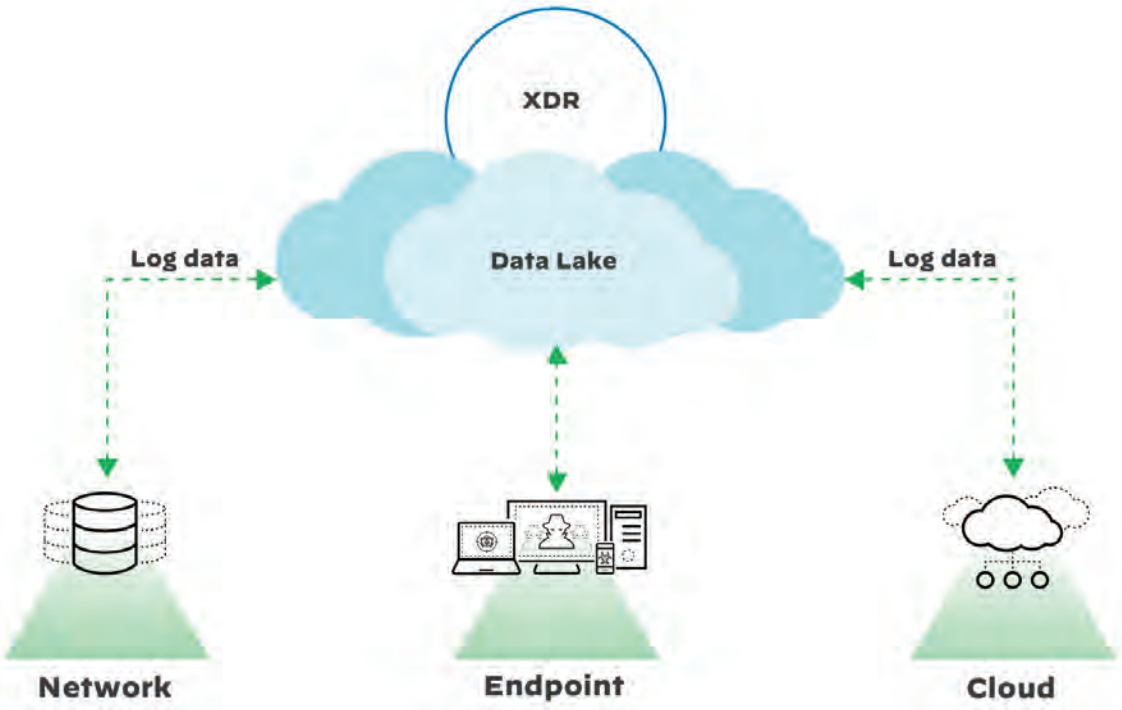
Una soluzione di automazione e orchestrazione della sicurezza (SOAR) risulta essere, quindi, lo strumento ideale per rispondere a queste esigenze.

Secondo studi di Palo Alto Networks l'implementazione di strumenti SOAR può consentire ai team sicurezza di standardizzare i processi in ambienti multi-cloud e on-premise e automatizzare la risposta per qualsiasi use case di cloud security, con tempi di risposta più rapidi del 67% e una riduzione del 95% degli alert che necessitano intervento umano[2].

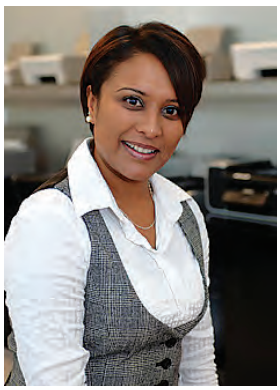
Sfruttando un SOAR è infatti possibile definire proprie logiche di orchestrazione attraverso ampie integrazioni, sia tecnologiche (prodotti) che di contenuti (intelligence), e playbook predefiniti in grado di automatizzare processi che includano logiche decisionali e un'ampia gamma di azioni su strumenti eterogenei. ■

1 Quantifying the Velocity of Digital Transformation https://expanse.co/blog/quantifying-the-velocity-of-digital-transformation/.

2 Dramatically Improve Incident Response ROI https://start.paloaltonetworks.com/measuring-the-roi-of-an-incident-response-platform



Il Cloud - Il potere della tecnologia. Ora.



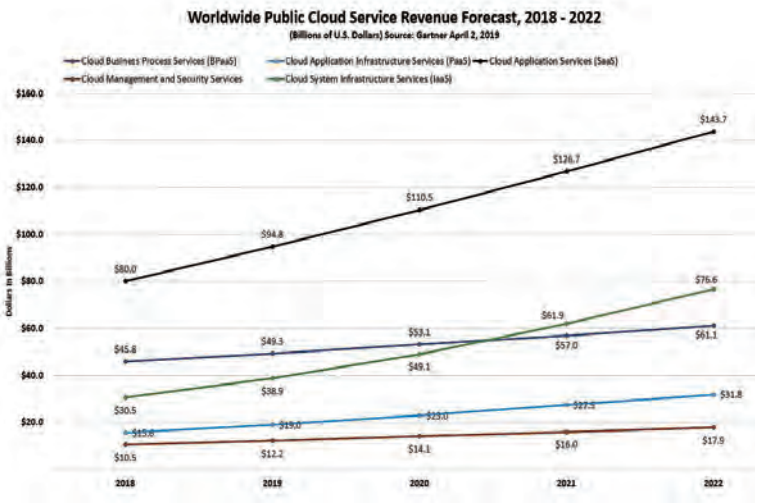
Autore: Raj Meghani

La storia del cloud moderno è iniziata quasi due decenni fa.

Circa due anni fa ho intervistato qualcuno chiedendo quali fossero le principali barriere all'adozione del cloud. La sicurezza era il denominatore comune - sicurezza dei dati e rischi generali di sicurezza. Eravamo nel 2019 e Gartner prevedeva che il 50% di tutte le imprese globali che utilizzavano il cloud avrebbero avuto una strategia *"all-in-cloud"* entro la fine del 2021.

Ma torniamo al giorno d'oggi. La pandemia del COVID-19 con l'adozione del home working ha fatto sì che aziende di tutte le dimensioni comprendessero come un'infrastruttura cloud possa offrire loro una soluzione scalabile, flessibile e conveniente.

Entro la fine del 2021, Forbes aveva previsto che l'83% del flusso di lavoro di un'azienda si sarebbe svolto tramite il cloud (pubblico, privato e ibrido). Gartner aveva previsto che le entrate del settore del cloud pubblico sarebbero salite del 21%, da 175 miliardi di dollari nel 2018 a 331 miliardi di dollari entro il 2022.



BIO

Raj Meghani è Chief Marketing Officer di BlockAPT, un'azienda all'avanguardia della cybersecurity, con sede nel Regno Unito, che offre alle organizzazioni un'esperienza di piattaforma unica, di comando e controllo, gestita a livello centrale. Raj è stata anche nominata direttore non esecutivo nel consiglio di amministrazione di Money Matters Bank. Raj è appassionata della trasformazione di scenari complessi in soluzioni semplici nella cybersecurity, nella tecnologia e nella trasformazione digitale. Raj ha oltre 20 anni di esperienza in imprese FTSE100/250 ad alta crescita, aiutando le aziende nel campo dei servizi finanziari, IT e professionali, in primis nelle strategie aziendali, le trasformazioni digitali, la crescita economica e la business continuity.
LinkedIn - https://www.linkedin.com/in/rajmeghani-a036482/
Twitter: https://twitter.com/blockapt
Sito web dell'azienda: https://www.blockapt.com

I numeri sono sbalorditivi e le opportunità per i fornitori come Microsoft Azure, AWS e Google sono in crescita man mano che la tecnologia cloud viene assimilata dalle infrastrutture aziendali e diventa il loro *modus operandi*.

Allora perché così tante organizzazioni stanno ancora lottando per superare alcuni ostacoli nell'adozione del cloud? Quali sono i principali «miti» e come si possono sfatare?

Ho già investito nei miei data center e la mia sicurezza è sufficiente.

Sia che l'infrastruttura sia *on premise* o sul cloud o su una combinazione delle due, molte organizzazioni non riescono a rilevare e identificare la fonte del crescente numero di cyberattacchi. Adottare sufficienti controlli di sicurezza è fondamentale per garantire la scalabilità e la continuità del business.

I fornitori di servizi cloud hanno investito miliardi per assicurarsi di avere implementato le giuste metodologie e strumenti di cybersecurity al fine di migliorare la sicurezza dei loro clienti e per continuare a farlo. Anche se le applicazioni *on premise* possono essere sicure, affidabili e consentire alle aziende di mantenere un certo livello di controllo, il semplice sforzo e il costo di gestire e mantenere l'hardware, le licenze software, le capacità di integrazione, la gestione della risposta agli incidenti, per non parlare del mantenimento di personale qualificato e della sua formazione continua, sono azioni costose che, se non vengono eseguite, aumentano l'esposizione al rischio dell'organizzazione e potrebbero essere una barriera sul fronte della scalabilità.

Passare al cloud mi farà automaticamente risparmiare denaro.

Non è sempre così. È un concetto abbastanza semplice perché, nel cloud, si paga solo per ciò che si utilizza. Non vi è nessun costo nascosto per l'hardware o l'acquisto di software, il consumo di energia, lo spazio, ecc.

Per esempio, nel caso di un server, una volta raggiunto il limite di spazio di archiviazione, ci si ritrova a dover acquistare un nuovo server per aumentare la larghezza della banda. Le aziende con un andamento periodico dei flussi di clienti che adottano una soluzione *on premise* potrebbero non trovare così conveniente questa soluzione quando i flussi di traffico ritornano a livelli normali e i loro server si ritrovano con un'alta percentuale di sottoutilizzo.

Secondo IDC, le imprese più importanti che spenderanno di più per il cloud computing quest'anno sono quelle che trattano un maggiore flusso di dati - cioè il recupero di grandi quantità di informazioni sensibili da diversi luoghi - ovvero il settore manifatturiero (20 miliardi di dollari), quello dei servizi professionali (18 miliardi di dollari) e quello finanziario-bancario (16 miliardi di dollari).

Ma *attenzione:* il cloud offre una lunga lista di servizi, strumenti e opzioni che possono far lievitare rapidamente i costi per un'azienda se questa non ha dovutamente preparato una lista dei requisiti dei quali ha bisogno. La maggior parte degli attori del cloud offrono certo strumenti per aiutare a gestire la fatturazione e i costi, ma l'onere di ottimizzare il cloud per soddisfare le proprie esigenze specifiche rimane a carico dell'organizzazione.

Se non è rotto, allora non aggiustarlo, giusto?

Sbagliato - a meno che non ci siano stretti vincoli normativi e legali sulla gestione dei dati. I sistemi di legacy, le applicazioni, l'hardware, ecc., provati e testati *on premise* non sono agili come una soluzione cloud. Se la tua azienda sta cercando di crescere e di aumentare la scalabilità, è necessario garantire che anche la tua infrastruttura IT possa essere scalabile. Se a tutto ciò aggiungiamo significativi risparmi sui costi e maggiori livelli di sicurezza offerti da un servizio cloud, sarà solo una questione di tempo prima che la trasformazione digitale cominci a dare risultati.

Avere i miei dati in sede è più sicuro che averli sul cloud.

Non è detto. Partendo dal dato che solo una organizzazione su 10 è apparentemente in grado di analizzare più del 75% degli eventi di sicurezza sia *on premise* che nel cloud, le preoccupazioni sulla sicurezza del cloud, la perdita di dati e la privacy dei dati restano ancora una grande sfida per le aziende di tutte le dimensioni.

Le PMI non stanno solo cercando di sopravvivere in questi tempi difficili, ma anche di risparmiare il più possibile senza compromettere la sicurezza dei dati dei loro clienti. Spesso prive di competenze e conoscenze in materia di sicurezza, il 40% di esse ha trovato più conveniente impiegare piattaforme cloud di terzi parti piuttosto che sostenere un sistema interno.

Recenti studi basati su tutti i servizi cloud dimostrano che gli strumenti di gestione e i servizi di sicurezza dovrebbero essere i segmenti in più rapida crescita con un miglioramento del 28,4%.

Con il tradizionale *set up on premise*, la responsabilità di mitigare le minacce informatiche è a carico dell'azienda. Essere immediatamente reattivi alle nuove patch, alle modifiche dei certificati di sicurezza, ecc. può spesso essere difficile e comportare degli *omissis*. I migliori fornitori di cloud, con la loro potenza economica, sono visti come i migliori nel "gioco" di adattamento continuo alle politiche di sicurezza, il rispetto delle norme di conformità, ecc. Nella maggior parte delle volte, riescono ad adattarsi più rapidamente e meglio rispetto a quanto possano fare le organizzazioni tradizionali. L'automazione gioca un ruolo chiave in questo caso: la collaborazione intelligente e un'ottima integrazione dei processi di controllo delle modifiche su diversi dispositivi, i firewall con una robusta intelligence sulle minacce, la gestione delle vulnerabilità e la capacità di risposta agli incidenti sono tutti elementi che potenziano l'ecosistema della sicurezza.

È interessante anche osservare che la maggior parte delle violazioni del cloud pubblico sono state commesse da configurazioni insicure da parte di un cliente aziendale. Gartner prevede che entro il 2025, il 99% delle falle di sicurezza del cloud saranno da attribuire al cliente e non ai fornitori di sicurezza.

Nessuna azienda è immune dai cyberattacchi - sia su cloud che *on premise* ci troviamo ad affrontare le stesse minacce ed esposizioni al rischio. La differenza sta nella responsabilità e nell'affidabilità.

La migrazione verso un ambiente cloud sarà dolorosa e dirompente.

Non è sempre così, perché dipende dallo stato attuale dell'infrastruttura di un'azienda. Un'azienda ha principalmente il controllo completo dei software, delle politiche e dei dati. La flessibilità di aumentare o diminuire l'utilizzo del cloud è conveniente e offre economie di scala.

Bisogna quindi trattare la migrazione al cloud come qualsiasi altro progetto di trasformazione digitale, da attuare con un'attenta pianificazione, una chiara strategia cloud e un piano di implementazione. L'implementazione rispetto a una soluzione *on premise* è spesso più veloce e meno dirompente per il business. La chiave è nella pianificazione. Pianificare. Pianificare. E pianificare ancora.

Quindi, i benefici dell'adozione del cloud sono chiari: secondo il rapporto di IDG, il 71% delle aziende cerca miglioramenti nella velocità e il 63% vuole maggiore flessibilità. Altri benefici includono:

- Risparmi sui costi operativi - nessun investimento in hardware fisico, nessuna formazione del personale per gestire l'hardware, migliore utilizzo dello spazio, pay per use, ecc.
- Vantaggio strategico competitivo - accesso alle ultime applicazioni, innovazione, analisi, ecc. per gestire meglio il vostro business e produrre entrate aggiuntive.
- Sicurezza e affidabilità - risposta in tempo reale ai cambiamenti con backup e ripristino controllati.
- Velocità - distribuisci la tua offerta più velocemente con meno di un clic.
- Facilità d'uso - l'automazione permette alle risorse di gestire efficacemente i compiti che richiedono tempo.
- Collaborazione - tra le varie aree geografie e i team in modo sicuro.
- Implementazione rapida - interruzione minima del business.

L'adozione del cloud è destinata a rimanere, ma è il modo in cui dobbiamo osservare questa trasformazione che fa la differenza.

Paul Maritz lo riassume bene - "Il cloud è questione di come si gestisce l'informatica, non dove si svolge l'informatica". ■

Sicurezza e privacy nei servizi in cloud: come verificarlo.

Autore: Giancarlo Butti

La possibilità di effettuare verifiche sui servizi forniti da cloud provider è un elemento irrinunciabile, che tuttavia si scontra con l'oggettiva difficoltà nel perseguire tale obbiettivo. Quali sono le possibili soluzioni?

La disponibilità dei servizi in cloud offre numerosi vantaggi per tutte le organizzazioni che possono avvantaggiarsi dall'uso di soluzioni standardizzate, pagate a consumo e fruibili da ogni postazione aziendale (o in smart working) indipendentemente dalla loro collocazione.

Considerando la molteplicità delle possibili soluzioni offerte dai ben noti modelli (IaaS, PaaS, Saas) la gestione della sicurezza è diversamente ripartita fra fornitore di servizi e fruitori dei medesimi.

Mentre per quanto attiene quanto è presidiato direttamente dai fruitori dei servizi, questo ovviamente ne ha un reale controllo, per quanto attiene la componente gestita dal fornitore di servizi ci si deve affidare a quanto da lui dichiarato.

Diventa quindi importante poter verificare in concreto se quanto formalizzato, solitamente nelle condizioni contrattuali, corrisponda alla situazione reale, ad esempio mediante il ricorso ad una attività di audit.

Tuttavia, la verifica circa il reale livello di sicurezza di un servizio in cloud non è un'attività semplice e richiede diversi requisiti preliminari per poter essere svolta:

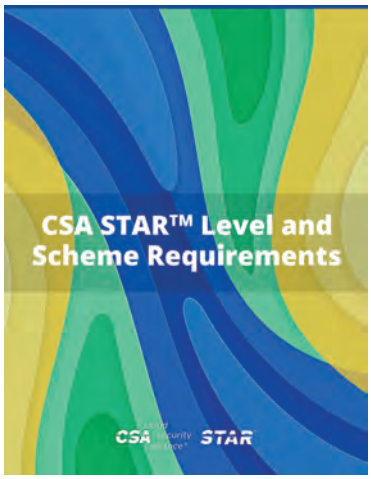
- deve essere prevista contrattualmente
- le condizioni imposte per poter svolgere una verifica devono essere ragionevolmente percorribili e possibilmente senza costi per il cliente (salvo ovviamente i costi che un'organizzazione sostiene per una qualunque attività di verifica, quali ad esempio quelle del personale, interno o esterno coinvolto)
- il fruitore di servizi che vuole effettuare l'attività di verifica deve disporre direttamente, o avvalendosi di servizi di terzi, di personale qualificato per svolgere tale tipologia di attività
- non deve interferire né con l'attività del fornitore, né con quella di altri clienti.

Non va inoltre dimenticato che la collocazione dei data center può costituire un problema circa la reale possibilità di effettuare una visita presso gli stessi.

Se effettivamente si è nelle condizioni di poter svolgere un'attività di verifica, per il suo svolgimento è possibile avvalersi di numerosi framework, resi disponibili da diversi enti ed associazioni, fra le quali in prima istanza la **CSA (Cloud Security Alliance)**.

Tali schemi sono disponibili in varie lingue, compreso l'italiano *(vedasi: www.cloudsecurityalliance.it)*.

CSA propone diversi schemi di verifica, che fanno riferimento a standard o anche a normative quali il GDPR.



La **BSI (Federal Office for Information Security)** tedesca ha pubblicato su questo tema il:

Referencing Cloud Computing Compliance Controls Catalogue (C5) to International Standards

nel quale sono mappati e messi a confronto i seguenti standard:

- ISO/IEC 27001:2013 (ISO - International Organization for Standardization)
- CSA Cloud Controls Matrix 3.01 (CSA - Cloud Security Alliance)
- AICPA Trust Service Principles Criteria 2014 (AICPA - American Institute of Certified Public Accountants)
- ANSSI Référentiel Secure Cloud 2.0 (Draft) (ANSSI - Agence nationale de la sécurité des systèmes d'information)
- IDW ERS FAIT 5 04.11.2014 (IDW - Institut der Wirtschaftsprüfer; ERS – Entwurf einer Stellungnahme zur Rechnungslegung; FAIT - Fachausschuss für Informationstechnologie)
- BSI IT-Grundschutz 14. Ergänzungslieferung 2014 (BSI)
- BSI SaaS Sicherheitsprofile 2014 Security (BSI)

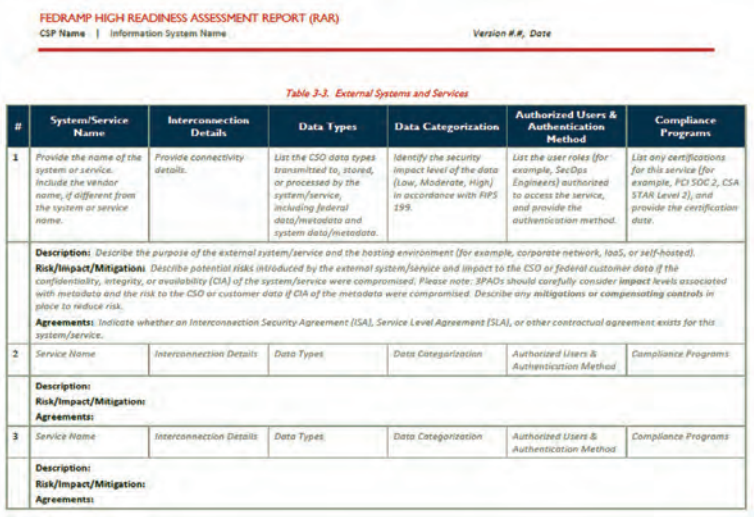
Altra utile fonte di riferimento può essere la **Federal Risk and Authorization Management Program (FedRAMP)**.

Infatti, le agenzie federali negli USA possono avvalersi solo di servizi cloud che abbiano superato un processo di validazione dal punto di vista della sicurezza.

L'elenco dei vari soggetti e la loro classificazione sono pubblici e possono costituire un buon punto di partenza nel processo di valutazione di un potenziale fornitore:

(https://marketplace.fedramp.gov/#!/products?sort=designation&status=Compliant)

Inoltre, la FedRAMP rende disponibile sia una check list (in formato Excel) sia template di report utili per la valutazione.



FEDRAMP HIGH READINESS ASSESSMENT REPORT (RAR)

CSP Name | Information System Name — Version #.#, Date

Table 3-3. External Systems and Services

#	System/Service Name	Interconnection Details	Data Types	Data Categorization	Authorized Users & Authentication Method	Compliance Programs
1	*Provide the name of the system or service. Include the vendor name, if different from the system or service name.*	*Provide connectivity details.*	*List the CSO data types transmitted to, stored, or processed by the system/service, including federal data/metadata and system data/metadata.*	*Identify the security impact level of the data (Low, Moderate, High) in accordance with FIPS 199.*	*List the user roles (for example, SecOps Engineers) authorized to access the service, and provide the authentication method.*	*List any certifications for this service (for example, PCI SOC 2, CSA STAR Level 2), and provide the certification date.*
	Description: *Describe the purpose of the external system/service and the hosting environment (for example, corporate network, IaaS, or self-hosted).* **Risk/Impact/Mitigation:** *Describe potential risks introduced by the external system/service and impact to the CSO or federal customer data if the confidentiality, integrity, or availability (CIA) of the system/service were compromised. Please note: 3PAOs should carefully consider impact levels associated with metadata and the risk to the CSO or customer data if CIA of the metadata were compromised. Describe any mitigations or compensating controls in place to reduce risk.* **Agreements:** *Indicate whether an Interconnection Security Agreement (ISA), Service Level Agreement (SLA), or other contractual agreement exists for this system/service.*					
2	*Service Name*	*Interconnection Details*	*Data Types*	*Data Categorization*	*Authorized Users & Authentication Method*	*Compliance Programs*
	Description: **Risk/Impact/Mitigation:** **Agreements:**					
3	*Service Name*	*Interconnection Details*	*Data Types*	*Data Categorization*	*Authorized Users & Authentication Method*	*Compliance Programs*
	Description: **Risk/Impact/Mitigation:** **Agreements:**					

Auditor skill

L'esecuzione di un'attività di verifica nell'ambito del cloud richiede competenze tecniche specifiche.

La precedente pubblicazione del **BSI (Referencing Cloud Computing Compliance Controls Catalogue (C5) to International Standards)** riporta al riguardo le seguenti indicazioni circa i requisiti di cui dovrebbe disporre un auditor che svolge un'attività in ambito cloud; avere almeno 3 anni di esperienza nell'ambito dell'attività di audit e la disponibilità di una delle seguenti certificazioni:

- ISACA - Certified Information Systems Auditor (CISA)
- ISACA - Certified Information Security Manager (CISM) or
- ISACA - Certified in Risk and Information Systems Control (CRISC)
- ISO/IEC 27001 Lead Auditor
- Cloud Security Alliance (CSA) – Certificate of Cloud Security Knowledge (CCSK)
- $(ISC)^2$ – Certified Cloud Security Professional (CCSP)

alle quali si possono aggiungere anche le seguenti:

- Cloud Security Alliance (CSA) – Certificate of Cloud Auditing Knowledge (CCSK)
- Shared Assessments - Certified Third Party Risk Assessor
- Shared Assessments - Certified Third Party Risk Professional

La stessa **ISACA (già Information Systems Audit and Control Association®)**, dettaglia ulteriormente lo skill richiesto agli auditor nella sua pubblicazione: **IS Audit/Assurance Program for Cloud Computing** nella

quale individua quello che ritiene essere il livello minimo di competenza richiesta (vedi Tab. 1).

Tab. 1 - IS Audit/Assurance Program for Cloud Computing – Minimum skill

Cloud computing incorporates many IT processes. Because the focus is on information governance, IT management, network, data, contingency and encryption controls, the audit and assurance professional should have the requisite knowledge of these issues. In addition, proficiency in risk assessment, information security components of IT architecture, risk management, and the threats and vulnerabilities of cloud computing and Internet-based data processing is required. Therefore, it is recommended that the audit and assurance professional who is conducting the assessment has the requisite experience and organizational relationships to effectively execute the assurance processes. Because cloud computing is dependent on web services, the auditor should have at least a basic understanding of Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security (WS-Security or WSS) Standards (www.oasis-open.org). It is also important that the auditor has sufficient functional and business knowledge to assess alignment with the business strategy. Professionals holding the CISA certification should comply with ITAF standard 1006 Proficiency.

Auditor esterni

Vista l'oggettiva difficoltà nella esecuzione di un audit in ambito cloud non va esclusa:

- la possibilità di avvalersi di audit di terze parti indipendenti, commissionate direttamente dal fornitore di servizi cloud e da questi resi disponibili, ad esempio, sul proprio sito; è il caso questo di **LogMeIn**, (produttore fra gli altri di **GoToMeeting**).

- l'esecuzione di attività di audit svolta congiuntamente ad altri clienti.

Su tali temi **ESMA** nella sua guida sugli **Orientamenti in materia di esternalizzazione a fornitori di servizi cloud** recita che le imprese potrebbero avvalersi di:

a) certificazioni di terzi e relazioni di audit esterno o interno messe a disposizione dal fornitore di servizi cloud;

b) serie di audit svolti congiuntamente con altri clienti dello stesso fornitore di servizi cloud o audit congiunti espletati da un revisore esterno designato da più clienti dello stesso fornitore di servizi cloud.

Vincolando tuttavia tali possibilità ad una serie di elementi:

In caso di esternalizzazione di funzioni essenziali o importanti, un'impresa dovrebbe avvalersi delle certificazioni di terzi e delle relazioni di audit esterno o interno di cui al paragrafo 37, lettera a), solo se:

a) ha accertato che l'ambito delle certificazioni o delle relazioni di audit comprende i sistemi principali del fornitore di servizi cloud (ad esempio, processi, applicazioni, infrastruttura, centri dati), i controlli fondamentali

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.

individuati dall'impresa e la conformità agli obblighi di legge pertinenti;

b) sottopone a valutazione accurata e periodica il contenuto delle certificazioni o relazioni di audit e verifica che non siano obsolete;

c) assicura che i controlli e i sistemi principali del fornitore siano compresi anche nelle versioni successive della certificazione o della relazione di audit;

d) è soddisfatta della parte incaricata della certificazione o dell'audit (ad esempio per quanto riguarda le qualifiche, le competenze, la ripetizione/verifica degli elementi concreti contenuti nel fascicolo di audit sottostante e la rotazione della società di certificazione o di audit);

e) si è sincerata che le certificazioni siano rilasciate e che gli audit siano espletati conformemente a norme pertinenti e che comprendano anche una verifica dell'efficacia dei controlli essenziali in atto;

f) ha il diritto contrattuale di chiedere l'ampliamento dell'ambito delle certificazioni o delle relazioni di audit per includervi taluni sistemi e controlli rilevanti del fornitore di servizi cloud; il numero e la frequenza di tali richieste di modifica dell'ambito dovrebbero essere ragionevoli e giustificati in un'ottica di gestione dei rischi;

g) conserva il diritto contrattuale di effettuare audit individuali in loco a sua discrezione in relazione alla funzione esternalizzata.

La già citata CSA ha realizzato uno schema che rappresenta, in ordine di rilevanza, le varie tipologie di audit che possono essere effettuati in ambito sicurezza e privacy di un servizio in cloud: il **CSA STAR Level and Scheme Requirements**.

Tale schema prende in considerazione 3 diversi livelli, in funzione sia della frequenza con cui viene svolta l'attività di audit, sia del soggetto che svolge questo tipo di attività.

Spesso questi audit vengono effettuati nel rispetto di standard predefiniti, quali ad esempio il SOC2 o SOC3, standard di audit definiti dall'**AICPA (Association of International Certified Professional Accountants)** (Tab. 2).

Association of International Certified Professional Accountants®

Tab. 2 - Service Organization Control Reports® (AICPA)

- SOC 1® Report Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting This meets the needs of user entities' managements and auditors as they evaluate the effect of a service organization's controls on a user entity's financial statement assertions. These reports are important components of user entities' evaluation of their internal controls over financial reporting for purposes of compliance with laws and regulations and for when user entity auditors plan and perform financial statement audits.
- SOC 2® Report Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®) For those who need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality or privacy. These reports can play an important role in oversight of the organization, vendor management programs, internal corporate governance and risk management processes, and regulatory oversight. Stakeholders who may use these reports include management or those charged with governance of the user entities and of the service organization, customers, regulators, business partners and suppliers, among others.
- SOC 3® Report Trust Services Principles, Criteria, and Illustrations Designed to accommodate users who want assurance on a service organization's controls related to security, availability, processing integrity, confidentiality or privacy but do not have the need for the detailed and comprehensive SOC 2® Report. It can be used in a service organization's marketing efforts.

Gli aspetti privacy

Oltre ai temi strettamente connessi alla sicurezza non meno importanti sono quelli legati al rispetto della normativa privacy.

Questi ultimi potrebbero in realtà risultare anche vincolanti circa la reale possibilità di utilizzare una determinata soluzione in cloud.

I temi da considerare sono diversi, ma in particolare ciò che costituisce un vincolo che potrebbe essere insormontabile è costituito dalla localizzazione delle piattaforme utilizzate in quanto la loro eventuale collocazione al di fuori dello spazio economico europeo (UE + Norvegia, Liechtenstein, Islanda), ed in particolare negli USA, potrebbe risultare non conforme e non sanabile.

Un'analisi in questo senso non solo è opportuna, ma è anche obbligatoria ed è tutt'altro che semplice.

Va infatti considerato che molto spesso l'utilizzo di alcuni servizi in cloud si avvale a sua volta di altri servizi in cloud. In particolare, le piattaforme che offrono i servizi infrastrutturali sono quasi sempre basate su Azure, AWS, Google…

In alcuni casi alcuni servizi consentono di selezionare la localizzazione delle piattaforme da utilizzare, ma spesso questo non vale per alcune tipologie di dati.

Inoltre, molto spesso l'uso di soluzioni in cloud si avvale di diversi subfornitori e per ognuno di questi è necessario procedere alla valutazione della loro reale collocazione.

La maggior parte di prodotti utilizzati ogni giorno da milioni di utenti per la gestione delle videochiamate e dei webinar in realtà prevede una qualche forma di trattamento di dati personali negli USA.

Il trasferimento dei dati, come riporta il sito dell'Autorità Garante:

è consentito ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati (art. 46 del Regolamento UE 2016/679). Al riguardo, possono costituire garanzie adeguate:

- *senza autorizzazione da parte del Garante:*
  - *gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);*
  - *le norme vincolanti d'impresa (art. 46, par. 2, lett. b)*
  - *le clausole tipo (art. 46, par. 2, lett. c e lett. d)*
  - *i codici di condotta (art. 46, par. 2, lett. e)*
  - *i meccanismi di certificazione (art. 46, par. 2, lett. f)*
- *previa autorizzazione del Garante:*
  - *le clausole contrattuali ad hoc (art. 46, par. 3, lett. a)*
  - *gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b)*

In assenza di ogni altro presupposto, è possibile trasferire i dati personali in base ad alcune deroghe che si verificano in specifiche situazioni (art. 49 del Regolamento UE 2016/679).

Tuttavia, come riportato nelle FAQ relative alla sentenza della **Corte di giustizia dell'Unione europea** nella causa C-311/18 — Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems, l'**EPDB** così si esprime:

La Corte:

- *ha esaminato la validità della decisione n. 2010/87/CE della Commissione europea sulle clausole contrattuali tipo ("SCC") e ne ha ritenuto la validità. Infatti, la validità di tale decisione non è in dubbio per il semplice motivo che le clausole tipo di protezione dei dati di cui alla suddetta decisione non sono vincolanti per le autorità del paese terzo verso il quale i dati possono essere trasferiti, avendo esse natura contrattuale*
- *ha dichiarato invalida la decisione sull'adeguatezza dello scudo per la privacy (Privacy Shield)*

quindi

La possibilità o meno di trasferire dati personali sulla base di SCC dipende dall'esito della valutazione che dovrà compiere, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto. Le misure supplementari unitamente alle SCC, alla luce di un'analisi caso per caso delle circostanze del trasferimento, dovrebbero garantire che la normativa statunitense non interferisca con l'adeguato livello di protezione garantito dalle SCC e dalle misure supplementari stesse.

Se si è giunti alla conclusione che, tenuto conto delle circostanze del trasferimento e delle eventuali misure supplementari, non vi sarebbero adeguate garanzie, occorre sospendere o porre fine al trasferimento di dati personali. Tuttavia, se si intende continuare ciononostante a trasferire i dati, occorre informarne la SA competente.

Nonostante tali indicazioni riguardano qualunque stato al di fuori dello SEE, la sentenza fa riferimento in particolare alla normativa USA che consente l'accesso ai dati personali da parte delle autorità federali.

Per adempiere al requisito sopra indicato, in merito ad una puntuale valutazione relativa ai singoli trasferimenti, è possibile utilizzare modelli di valutazione proposti ad esempio da IAPP, liberamente scaricabili dal relativo sito.

Altro aspetto fondamentale è la valutazione del ruolo privacy assunto dai vari attori coinvolti.

L'utilizzo di un servizio in cloud comporta molto spesso la designazione del fornitore quale responsabile del trattamento.

Nel GDPR il responsabile del trattamento ha delle reali responsabilità in solido con il Titolare, ad esempio per quanto attiene il risarcimento danni, ed è anch'esso sanzionabile.

Il rapporto fra Titolare e Responsabile va regolamentato mediante un contratto i cui contenuti sono specificatamente indicati nella normativa.

La corresponsabilità fra Titolare e Responsabile è ovviamente un elemento di garanzia per il Titolare.

Tuttavia, quello che troppo spesso ci si dimentica è che il Titolare potrebbe a sua volta fornire servizi ai propri clienti tramite il servizio in cloud. Se questo avviene e se il Titolare nello svolgimento di tale attività viene a sua volta designato quale Responsabile da parte di un suo cliente, il servizio cloud assumerà il ruolo di sub responsabile nei confronti del cliente del Titolare.

Questo fatto è tutt'altro che irrilevante.

Infatti, il sub responsabile non risponde né dal punto di vista sanzionatorio, né da quello risarcitorio.

In altre parole, le responsabilità nei confronti di un soggetto di cui si trattano i dati (e anche di altre persone) si ferma al Responsabile.

Quindi se il cloud provider effettuerà una qualche violazione alla normativa o procurerà dei danni ai clienti del Titolare, sarà solo lui a risponderne. Sarà poi il Titolare che potrà rivalersi sul servizio in cloud, con tutte le limitazioni del caso circa la reale possibilità di recuperare qualcosa.

Quindi valutare la reale capacità di un soggetto esterno che offra un servizio in cloud di garantire un elevato livello di sicurezza è fondamentale, in particolare se tale servizio viene utilizzato non solo all'interno dell'azienda, ma anche per l'erogazione di un servizio a terzi. ■

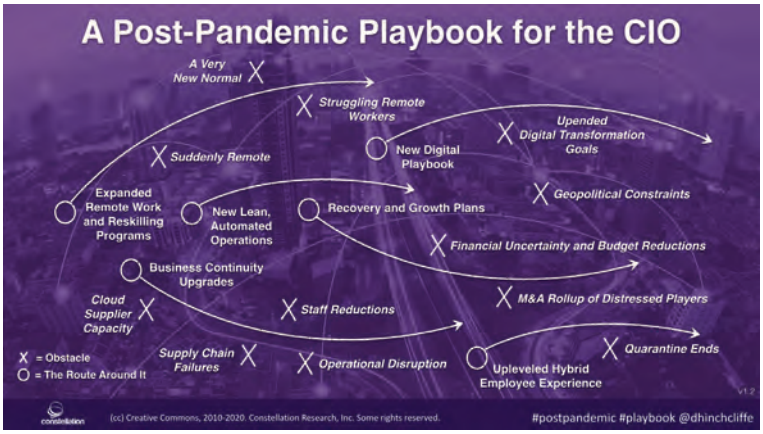
L'importanza di proteggere il Cloud in un mondo post-pandemico.

Autore: Lisa Ventura

Sono trascorsi quasi 2 anni da quando le organizzazioni a livello globale hanno dovuto cambiare e passare rapidamente a un modello di lavoro "smart" a causa della pandemia globale di COVID-19. Mentre alcuni dipendenti stanno iniziando lentamente a tornare in ufficio, molte organizzazioni hanno ora adottato un modello ibrido che permetta al personale di lavorare sia fuori sede che in sede. Ciò ha portato a una crescente dipendenza dall'infrastruttura cloud, che è uno strumento essenziale per consentire la collaborazione e la continuità aziendale. La sicurezza del cloud, quindi, è più essenziale che mai.

I servizi cloud erano qualcosa di "bello da avere", ma ora sono diventati un fattore abilitante per il business. Attualmente, il 92% delle organizzazioni utilizza ambienti cloud pubblici, privati o ibridi, secondo un rapporto IDG.

Oltre a svolgere un ruolo importante nel disaster recovery e nella resilienza operativa, il cloud computing e l'infrastruttura facilitano il flusso di informazioni, rendendo più facile per i dipendenti accedere a ciò di cui hanno bisogno e collaborare con gli altri, anche comodamente da casa.



Ma questo vantaggio è anche uno svantaggio. Le informazioni sono facilmente accessibili ai dipendenti ovunque si trovino, ma lo stesso vale anche per i cybercriminali che cercano di sfruttare le vulnerabilità del sistema. Con una superficie di attacco molto più ampia sul cloud, c'è una grande necessità di solidi controlli di sicurezza e una crescente domanda di personale esperto. Ma cos'è il cloud e in che modo può avvantaggiare la tua organizzazione?

Cos'è il cloud computing?

Il cloud computing è la fornitura di servizi informatici inclusi database, storage, networking, server, storage, software, analisi e intelligence su Internet ("il cloud") per offrire una migliore innovazione e risorse.

La sicurezza del cloud varia in base alla categoria di cloud computing utilizzata. Ci sono quattro aree principali del cloud computing:

- Servizi cloud pubblici, gestiti da un provider di cloud pubblico — Questi includono software-as-a-service (SaaS), Infrastructure-as-a-service (IaaS) e Platform-as-a-service (PaaS).
- Servizi di cloud privato, gestiti da un provider di cloud pubblico — Questi servizi forniscono un ambiente informatico dedicato a un cliente ma gestito da terzi parti.
- Servizi cloud privati, gestiti da personale interno — Questi servizi sono un'evoluzione dei data center tradizionali in cui il personale interno gestisce un ambiente virtuale che controlla.

- Servizi cloud ibridi — Le configurazioni di cloud computing privato e pubblico vengono combinate, ospitando carichi di lavoro e dati in base a fattori quali costi, sicurezza, operazioni e accesso. L'operazione coinvolgerà il personale interno e, facoltativamente, il provider di cloud pubblico.

Quando si utilizza un servizio di cloud computing fornito da un provider di cloud pubblico, i dati e le applicazioni sono spesso ospitati presso terzi parti. Questa è una differenza fondamentale tra il cloud computing e l'IT tradizionale in cui la maggior parte dei dati è conservata all'interno di una rete autocontrollata. Comprendere la responsabilità della sicurezza della tua organizzazione è il primo passo per costruire una strategia di sicurezza cloud.

Le sfide della sicurezza nel Cloud

Poiché i dati nel cloud pubblico sono archiviati in un provider di terze parti e vi si accede tramite Internet, sorgono diverse sfide nella capacità di mantenere un cloud sicuro. Queste sono:

Visibilità dei dati nel cloud — In molti casi, si accede ai servizi cloud al di fuori delle reti aziendali e da dispositivi non gestiti dall'IT. Ciò significa che il team IT deve controllare il servizio cloud stesso per avere piena

visibilità sui dati, al contrario dei tradizionali mezzi di monitoraggio del traffico di rete.

Controllo dei dati cloud — Nell'ambiente di un provider di servizi cloud di terze parti, i team IT hanno meno accesso ai dati rispetto a quando si controllavano server e applicazioni nelle proprie sedi. Per impostazione predefinita, ai clienti cloud viene concesso un controllo limitato e l'accesso all'infrastruttura fisica sottostante non è disponibile.

Accesso ai dati e alle applicazioni cloud — Gli utenti possono accedere alle applicazioni e ai dati cloud tramite Internet, rendendo inefficaci i controlli di accesso basati sul perimetro della rete del data center tradizionale. L'accesso dell'utente può avvenire da qualsiasi luogo o dispositivo, inclusa la tecnologia bring-your-own-device (BYOD). Inoltre, l'accesso privilegiato da parte del personale del provider di servizi cloud potrebbe aggirare i tuoi controlli di sicurezza.

Compliance di sicurezza del cloud — L'uso dei servizi di cloud computing aggiunge un'altra dimensione alla compliance normativa e interna. Il tuo ambiente cloud potrebbe dover rispettare requisiti normativi come HIPAA, PCI e Sarbanes-Oxley, nonché requisiti di team interni, partner e clienti. Anche l'infrastruttura del provider cloud, così come le interfacce tra i sistemi interni e il cloud, sono incluse nei processi di compliance e gestione del rischio.

Violazioni native del cloud — Le violazioni dei dati nel cloud sono diverse dalle violazioni locali, in quanto il furto di dati spesso si verifica utilizzando funzioni native del cloud. Una violazione nativa del cloud consiste in una serie di azioni in cui gli attaccanti riescono a far "atterrare" il proprio attacco sfruttando errori o vulnerabilità in una distribuzione cloud senza utilizzare malware, "espandono" il proprio accesso attraverso interfacce mal configurate o con protezione non sufficiente per individuare dati preziosi e "esfiltrano" quei dati nella propria posizione di archiviazione.

Errata configurazione — Le violazioni native del cloud spesso ricadono sulla responsabilità della sicurezza del cliente cloud, che include la configurazione del servizio cloud. La ricerca mostra che solo il 26% delle aziende può attualmente controllare i propri ambienti IaaS per errori di configurazione. L'errata configurazione di IaaS spesso funge da porta d'ingresso a una violazione nativa del cloud, consentendo all'attaccante di accedere, muoversi ed esfiltrare i dati. La ricerca mostra anche che il 99% delle configurazioni errate passa inosservato in IaaS dai clienti cloud.

Disaster recovery — La pianificazione della sicurezza informatica è necessaria per proteggere gli effetti di una violazione dei dati. Un disaster recovery include policy, procedure e strumenti progettati per consentire il ripristino dei dati e permettere a un'organizzazione di continuare le operazioni e il business.

Minacce interne — Un cattivo dipendente può utilizzare I servizi cloud per esporre un'organizzazione a una violazione della sicurezza informatica.

Soluzioni di sicurezza cloud

Le organizzazioni che cercano soluzioni di sicurezza cloud dovrebbero considerare quanto segue quando si tratta delle principali sfide di sicurezza cloud di visibilità e controllo sui dati cloud.

Visibilità nei dati cloud — Una visione completa dei dati cloud richiede l'accesso diretto al servizio cloud.

Le soluzioni di sicurezza cloud ottengono questo risultato attraverso una connessione API (Application Programming Interface) al servizio cloud. Con una connessione API è possibile conoscere:

- Quali dati vengono archiviati nel cloud.
- Chi utilizza i dati cloud.
- I ruoli degli utenti con accesso ai dati cloud.
- Con chi gli utenti cloud condividono i dati.
- Dove si trovano i dati cloud.
- Da dove si accede e si scaricano i dati cloud, incluso da quale dispositivo.

Controllo sui dati cloud — Una volta che hai visibilità sui dati cloud, applica i controlli più adatti alla tua organizzazione. Questi controlli includono:

Classificazione dei dati — Classifica i dati su più livelli, come sensibili, regolamentati o pubblici, man mano che vengono creati nel cloud. Una volta classificati, i dati possono essere bloccati dall'ingresso o dall'uscita dal servizio cloud.

Data Loss Prevention (DLP) — Implementa una soluzione DLP cloud per proteggere i dati dall'accesso non autorizzato e disabilitare automaticamente l'accesso e il trasporto dei dati quando viene rilevata un'attività sospetta.

Controlli di collaborazione — Gestisci i controlli all'interno del servizio cloud, come il downgrading delle autorizzazioni di file e cartelle per utenti specifici a editor o visualizzatore, la rimozione delle autorizzazioni e la revoca dei collegamenti condivisi.

Crittografia — La crittografia dei dati nel cloud può essere utilizzata per impedire l'accesso non autorizzato ai dati, anche se tali dati vengono esfiltrati o rubati.

Accesso dei dati e alle applicazioni cloud — Come per la sicurezza interna, il controllo degli accessi è una componente vitale della sicurezza cloud. I controlli tipici includono:

Controllo dell'accesso degli utenti — Implementa controlli di accesso al sistema e alle applicazioni che garantiscono che solo gli utenti autorizzati accedano ai dati e alle applicazioni nel cloud. Un Cloud Access Security Broker (CASB) può essere utilizzato per imporre i controlli di accesso.

Controllo dell'accesso al dispositivo — Blocca l'accesso quando un dispositivo personale non autorizzato tenta di accedere ai dati cloud.

Identificazione del comportamento dannoso — Rileva gli account compromessi e le minacce interne con l'analisi del comportamento degli utenti (UBA) in modo che non si verifichi l'esfiltrazione di dati dannosi.

Prevenzione del malware — Impedisce al malware di entrare nei servizi cloud utilizzando tecniche come la scansione dei file, l'inserimento nella whitelist delle applicazioni, il rilevamento del malware basato su algoritmi di machine learning-based e l'analisi del traffico di rete.

Accesso privilegiato — Identifica tutte le possibili forme di accesso che gli account privilegiati possono avere ai tuoi dati e alle tue applicazioni e mette in atto controlli per mitigare l'esposizione.

Conformità — I requisiti e le pratiche di conformità esistenti dovrebbero essere ampliati per includere dati e applicazioni che risiedono nel cloud.

Valutazione del rischio — Esamina e aggiorna le valutazioni del rischio per includere i servizi cloud. Identificare e affrontare i fattori di rischio introdotti dagli ambienti cloud e dai provider. Sono disponibili risk databases per i fornitori di servizi cloud per accelerare il processo di valutazione.

Compliance Assessments — Esamina e aggiorna le valutazioni di conformità per PCI, HIPAA, Sarbanes-Oxley e altri requisiti normativi delle applicazioni.

Perché la sicurezza del cloud è importante?

Secondo una recente ricerca, 1 azienda su 4 che utilizza servizi cloud pubblici ha subito un furto di dati. Un ulteriore 1 su 5 ha subito un attacco mirato contro la propria infrastruttura di cloud pubblico. Nello stesso studio, l'83% delle organizzazioni ha dichiarato di archiviare informazioni sensibili nel cloud. Con il 97% delle organizzazioni in tutto il mondo che utilizza oggi i servizi cloud, è essenziale che tutti valutino la propria sicurezza nel cloud e sviluppino una strategia per proteggere i propri dati. Nel Regno Unito, il governo sta svolgendo un ruolo centrale nell'adozione della tecnologia cloud e incoraggiando le organizzazioni a prendere in considerazione l'adozione anche di essa.

Dal suo lancio nel 2013, la Cloud First Policy del governo del Regno Unito è stata un'iniziativa tecnologica di punta e un aspetto importante nel Technology Code of Practice. La policy afferma che le organizzazioni dovrebbero valutare le soluzioni cloud prima di considerare qualsiasi altra opzione. La policy è stata riesaminata nel 2019 da funzionari governativi e poi hanno dichiarato che sarebbe stata confermata nell'ottobre 2019, dimostrando che il cloud si impone come metodologia approvata per modernizzare l'infrastruttura ICT del settore pubblico del Regno Unito.

Con l'avvento di sfide uniche come il COVID-19, il settore pubblico aveva bisogno di soluzioni digitali per soddisfare i propri requisiti in rapida evoluzione. Sebbene l'obiettivo immediato sia limitare la perdita umana, sociale ed economica, operare nella nuova normalità indica anche una pressione aggiuntiva sull'IT del governo negli anni a venire. I dipendenti pubblici del Regno Unito devono utilizzare i canali digitali per informare e fornire servizi ai residenti. Allo stesso tempo, molte funzioni sono diventate completamente digitali durante la pandemia, aumentando la domanda di comunicazioni omnicanale.

La visione del Governo del Regno Unito per G-Cloud

Il framework G-Cloud è stato sviluppato per aiutare gli enti governativi del Regno Unito a diffondere la Cloud First Policy e a reperire fornitori adeguati.

Il framework è stato progettato per incoraggiare l'uso di servizi multi-tenant condivisi e gestiti da più gruppi.

HM Government G-Cloud

Le risorse condivise, l'infrastruttura, il software e le informazioni possono essere forniti a una vasta gamma di utenti finali come utility, con modello pay-by-use, per utente al mese. È dinamicamente scalabile, agile e facile da inserire e uscire dal servizio. G-Cloud non è una singola entità; è un programma continuo e iterativo che consentirà l'uso di una gamma di servizi cloud e modificherà il modo in cui il governo del Regno Unito si procura e gestisce l'ICT. Adottando il cloud, il governo sarà in grado di utilizzare e condividere i servizi ICT più facilmente e consentirà il passaggio da soluzioni ICT personalizzate ad alto costo a servizi standard e intercambiabili a basso costo. Significa cambiare la cultura del governo per adattarsi alle soluzioni offerte dal mercato e non creare approcci personalizzati non necessari.

I vantaggi saranno:

Molte altre soluzioni di base – Una gamma dei migliori servizi ICT del settore disponibili immediatamente in modo che i dipendenti pubblici possano utilizzare ciò di cui hanno bisogno quando ne hanno bisogno e non creare servizi duplicati che non possono essere condivisi.

Flessibilità e libertà – La possibilità, se necessario, per i dipartimenti e le organizzazioni di cambiare facilmente i service provider senza lunghi cicli di approvvigionamento e implementazione, nessun "vincolo" a contratti lunghi e la libertà di adottare rapidamente un valore migliore e soluzioni all'avanguardia.

Pronto e facile da usare – Soluzioni complete già assicurate per la sicurezza, le prestazioni e la gestione dei servizi. Accesso pronto che consente efficienze in termini di costi e può essere utilizzato insieme a soluzioni on-premise dedicate, se necessario.

Basso costo – Servizi pagati in base all'utilizzo, guidati da una forte concorrenza su prezzo e qualità. Costi trasparenti insieme a metriche relative alla qualità e all'ambito del servizio per un confronto e un controllo più semplici.

Mercato competitivo – Una gamma di service providers che migliorano costantemente la qualità e il valore delle soluzioni che offrono, dalle piccole organizzazioni che forniscono prodotti di nicchia all'hosting su larga scala e alla capacità dei server dei computer.

Dato l'aumento delle interazioni online, la trasformazione digitale nel governo non riguarda più semplicemente l'innovazione, ma la gestione della scala, l'efficienza operativa e la garanzia del rapporto qualità-prezzo dei contribuenti, mentre le aspettative degli utenti, le tecnologie e i servizi dei fornitori stanno cambiando rapidamente.

Nel contesto del COVID19, il Software as a Service (SaaS) diventa fondamentale per garantire la richiesta di scalabilità e costi ridotti, nonché una più semplice integrazione di servizi digitali, automazione, efficienza e interazioni migliorate. In un ulteriore sviluppo nell'evoluzione del cloud computing e della sicurezza nel Regno Unito, il governo del Regno Unito ha firmato un Memorandum of Understanding (MoU) triennale con Microsoft nel 2021 per aiutare le organizzazioni del settore pubblico a continuare a sfruttare i vantaggi del cloud computing e delle applicazioni aziendali.

Il Memorandum of Understanding è intitolato "Digital Transformation Agreement 2021» e consente a tutte le organizzazioni del settore pubblico idonee di beneficiare di sconti e condizioni vantaggiose per Microsoft 365, Azure e, per la prima volta, Dynamics 365 e Power Platform servizi cloud.

L'accordo rinnova il Memorandum of Understanding esistente come accordo triennale e durerà dal 1 maggio 2021 ad aprile 2024. È stato negoziato tra Microsoft e Crown Commercial Service.

Il rapporto tra il gigante tecnologico e il governo si è concentrato sempre più sui servizi cloud da quando il governo ha lanciato la sua Cloud First Policy nel 2013, che è stata rivalutata nel 2019 e rimane una politica tecnologica di punta, secondo Microsoft.

Questa non è l'unica azienda ad aver firmato un Memorandum of Understanding con il governo del Regno Unito. AWS ne ha firmato uno a novembre dello scorso anno per aiutare ad accelerare la spinta alla

trasformazione digitale del settore pubblico e aumentare il livello di partecipazione tra i fornitori di servizi cloud più piccoli.

Nel giugno 2021, UK Cloud ha firmato un memorandum per consentire all'azienda di offrire i propri servizi al settore pubblico direttamente o indirettamente attraverso la sua comunità di partner. Il mese precedente, Google Cloud ha firmato un accordo simile per fornire il cloud computing alle agenzie del settore pubblico del paese.

Inoltre, negli ultimi anni la politica del Regno Unito basata sul cloud-first è stata molto influente nel plasmare le abitudini di acquisto IT del governo britannico. Con oltre 4,9 miliardi di sterline di acquisti cloud effettuati tramite il framework di appalti G-Cloud dal suo lancio nel 2013 - l'81% dei quali attraverso il governo centrale - ha avuto un'influenza fondamentale sul modo in cui il settore pubblico pensa al modo in cui accede, gestisce e archivia i dati, incoraggiando il settore pubblico ad adottare opzioni infrastrutturali più flessibili ed efficienti in termini di costi. Il successo della politica è più evidente nel modo in cui ha ampliato in modo significativo il pool di prodotti e servizi IT disponibili per le organizzazioni governative, con il 45% proveniente da piccole e medie imprese (PMI).

Ciò è servito a promuovere sia l'adozione del cloud che la fornitura di servizi pubblici digitali, lavorando in parallelo con il framework G-Cloud per fungere da motore per ridurre i costi e consentire la scalabilità all'interno di Whitehall e del settore pubblico in generale. Tuttavia, nonostante il suo impatto positivo, la politica è attualmente in fase di revisione da parte del Crown Commercial Service (CCS) e del Government Digital Service (GDS).

Come si stanno spostando gli obiettivi di sicurezza del Cloud

Quando la Cloud First Policy è stata introdotta per la prima volta, ha incaricato tutti i dipartimenti del governo centrale di adottare un approccio basato sul cloud pubblico per gli acquisti di tecnologia. Le organizzazioni del settore pubblico sono state incoraggiate a "considerare e valutare appieno le potenziali soluzioni di cloud pubblico prima di considerare qualsiasi altra opzione" quando si procurano servizi nuovi o esistenti, il tutto per garantire un buon rapporto qualità-prezzo.

Per comprendere i cambiamenti in atto, è necessario considerare l'adozione generale dell'infrastruttura cloud in più settori. Ad esempio, quando le aziende hanno iniziato ad adottare il cloud pubblico, sono state attratte da vari vantaggi come la capacità di esternalizzare le responsabilità di gestione chiave, ottenere la scalabilità necessaria per supportare un'azienda in crescita e, in particolare, ottenere

BIO

Lisa Ventura, CEO & Fondatrice della UK Cyber Security Association, è una pluripremiata consulente per la Cyber Security, inoltre è CEO e fondatrice della UK Cyber Security Association (UKCSA), un'associazione dedicata a soggetti e aziende che lavorano attivamente nel settore della cyber security nel Regno Unito. Lisa con passione si impegna ad aumentare la consapevolezza per la cyber security, in modo da rendere gli altri più cyber consapevoli nel business e per aiutare a prevenire gli attacchi informatici e le frodi informatiche. È una leader di pensiero, una relatrice in varie conferenze ed eventi di sicurezza informatica, tecnologia e IT e autrice di varie pubblicazioni a livello globale. Il suo primo libro "The Rise of the Cyber Women: Volume One" è stato pubblicato nell'agosto 2020 e il suo secondo libro "The Varied Origins of the Cyber Men: Volume One" è stato pubblicato nel novembre 2020, entrambi con grande successo. Lisa fa parte dell'Advisory Group per il nuovo West Midlands Cyber Resilience Center, del consiglio di Think Digital Partners e di Cyber Security Valley UK. È anche una forte sostenitrice delle donne nella cyber security, nel divario di competenze informatiche e nella neurodiversità. Nel 2020 è stata nominata Infosec Superwoman of the Year da CISO Magazine e ha vinto numerosi altri premi per il suo lavoro, tra cui il premio "Outstanding Contribution to Cyber Security" di SC Magazine. Ulteriori informazioni su Lisa sono disponibili su www.lisaventura.com. Il sito web della UK Cyber Security Association è www.cybersecurityassociation.co.uk.
Contatti: @cybergeekgirl and @ukcybersecassoc / https://www.linkedin.com/in/lisasventura/ https://www.facebook.com/lisaventurauk/

significativi risparmi sui costi. Dopo sei anni, le organizzazioni stanno riconsiderando la loro strategia a causa di fattori quali costi imprevisti e crescenti problemi di sicurezza nel cloud pubblico.

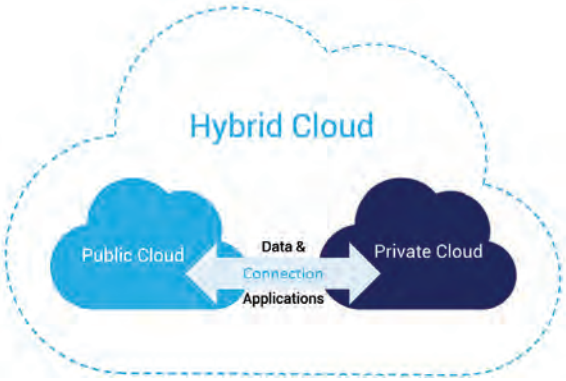
Le aziende si stanno rendendo conto che un approccio universale non è la risposta data la complessità della moderna infrastruttura IT. Oggi, le organizzazioni hanno costi complessi, requisiti di sicurezza e conformità che devono essere soddisfatti, spingendo molte persone a riflettere più attentamente su dove archiviare i propri dati. Di conseguenza, è preferibile un approccio ibrido che incorpori una combinazione di piattaforme cloud locali, private e pubbliche.

La sicurezza del Cloud seve essere al passo con i tempi

Il passaggio a una strategia ibrida è una tendenza definita che si sta riscontrando in tutto lo spazio IT e qualcosa che il settore pubblico del Regno Unito sta attualmente riconoscendo.

Dal punto di vista dei costi, le aziende di molti settori si sono rese conto che i costi possono aumentare rapidamente nel cloud pubblico, soprattutto se è necessario accedere regolarmente ai dati. Alcuni provider addebitano i costi in base all'accesso e all'utilizzo, che potrebbero non rappresentare un buon rapporto qualità-prezzo man mano che le organizzazioni e i loro dati crescono. Tuttavia, questa mancanza di chiarezza sui costi esatti coinvolti non è un problema con i sistemi cloud on-premise e privati, il che significa che le aziende non devono preoccuparsi di essere colpite da addebiti imprevisti. Un approccio ibrido offre il meglio di entrambi i mondi con carichi di lavoro specifici configurati per garantire che i dati hot vengano archiviati in locale e solo i dati cold vengano spostati nel cloud pubblico. Ciò consente di controllare la spesa eccessiva per i dati a cui si accede di frequente.

Un approccio ibrido può anche offrire molti vantaggi in termini di sicurezza e conformità, entrambi aspetti vitali per gli enti governativi. Sebbene il cloud pubblico non sia intrinsecamente insicuro, le organizzazioni hanno meno controllo nel garantire la sicurezza dei propri dati. Al contrario, l'infrastruttura on-premise fornisce garanzie che i dati si trovano all'interno dell'ambiente protetto dell'organizzazione e che solo un numero selezionato di persone può accedervi.



Ciò alimenta il problema della conformità, che è una grande preoccupazione sia per il settore pubblico che per quello privato. I sistemi on-premise rendono più facile per le organizzazioni sapere esattamente dove risiedono i propri dati, il che è prezioso ai fini della conformità e ideale per carichi di lavoro contenenti informazioni sensibili come documenti governativi.

In definitiva, la Cloud First Policy del Regno Unito è lì per rendere gli enti governativi consapevoli e confidenti dei vantaggi del cloud. Ma il governo ora si rende conto che non ha bisogno di destinare tutti i suoi fondi al cloud pubblico per godere di tutti i vantaggi offerti dal cloud, in linea con la più ampia tendenza del settore dell'adozione del cloud ibrido e, di conseguenza, del data repatriation.

Gli enti governativi dovrebbero essere liberi di avvalersi di tutte le opzioni per riflettere una gamma completa di soluzioni di archiviazione se vogliono davvero ottenere risparmi sui costi, motivo per cui è improbabile che l'attenzione sulle opzioni di cloud ibrido scompaia presto. La rivalutazione della Cloud First Policy è assolutamente necessaria ed è probabile che si riveli una mossa positiva per il governo e il settore pubblico del Regno Unito. ■

Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.
Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

Scaricatele su: www.distrettocybersecurity.it/linee-guida-itu

www.itu.int/cop

I sistemi giuridici vanno "aumentati", se vogliamo governare lo sviluppo della tecno-scienza.

Intervista VIP con l'avv. Guido Scorza.

Autore: Massimiliano Cannata

"Nella società globalizzata nella quale viviamo l'ambito naturale di vita dell'uomo e delle imprese e il mondo intero si dovrebbe lavorare di più sull'identificazione di una sorta di nuova *lex mercatoria* dell'ecosistema digitale che su esercizi di "nazionalizzazione" di servizi digitali. Ciò non toglie – spiega **Guido Scorza** componente dell'Autorità Garante per la Protezione dei Dati personali tra i massimi esperti di diritto dell'informatica applicato alle nuove tecnologie - che soprattutto in un momento nel quale sempre più dati finiscano sulle cosiddette nuvole (come il cloud in questo momento al centro dell'attenzione dei più), si debba fare il possibile per garantire ai cittadini europei che, "lassù" i dati, a cominciare da quelli personali, siano al sicuro almeno come "quaggiù" e, anzi, se possibile, più al sicuro".

Avvocato, i Garanti europei hanno lanciato un'indagine coordinata relativa all'utilizzazione dei servizi* cloud *da parte del settore pubblico. Comincerei col chiederLe a che punto siamo su questo nuovo fronte?

Sul punto bisogna essere estremamente chiari e rifuggire qualsiasi genere di ipocrisia istituzionale. Viviamo in un'epoca di neo-colonialismo digitale. Il nostro Paese, così come l'intera Unione europea, è in una condizione di evidente dipendenza tecnologica rispetto ad alcune economie straniere: Stati Uniti e Cina, innanzitutto. È una condizione di fatto figlia di una lunga stagione nella quale dapprima non si sono comprese le caratteristiche di quella che oggi abbiamo imparato a chiamare economia digitale e, quindi, quando tardivamente si sono capite, si sono fatte scelte sbagliate incapaci di supportare la nascita, in Europa, di piattaforme e servizi digitali capaci di competere sui mercati globali con quelli offerti prima dalle corporation americane e poi dalle società cinesi. Ma, questa, ormai è storia. Ora si sta correndo ai ripari ma si gioca di riconcorsa e illudersi di ribaltare la situazione attuale è, forse, velleitario specie se si sceglie di farlo provando a ergere fragili confini digitali.

BIO

Guido Scorza è componente dell'Autorità Garante per la protezione dei dati Personali e già Responsabile degli affari regolatori italiani e dell'UE nel Team di trasformazione digitale presso l'ufficio della Presidenza del Consiglio dei Ministri, oggi Consigliere giuridico del Ministro per l'innovazione. Docente presso diverse università tra cui l'Università Europea Di Roma, di Roma Tre, degli Studi Internazionali di Roma, di Pisa, di Bologna sui temi del diritto dell'Infomatica e delle nuove tecnologie. Ha esercitato la libera professione quale socio fondatore dello studio E-Lex Studio Legale, specializzato in diritto civile, diritto commerciale, privacy, proprietà intellettuale ed industriale, nonchè al diritto antitrust. Ha agito quale responsabile dei dati personali per diverse aziende inclusa la Kuwait Petroleum Italia S.p.A. e la Userbot S.r.l.

Meno Privacy vuol dire meno libertà

La nostra vita è "tracciata" dai dati. Un video curato dall'Authority particolarmente evocativo parla di questo "nuovo tesoro" da proteggere. Quali sono le principali tipologie di rischio connesse alla nostra vita personale e lavorativa, legate all'espansione dell'information society?

Il rischio maggiore è quello di perdere la nostra libertà di autodeterminazione in relazione a una pluralità di scelte da quelle di consumo a quelle culturali sino ad arrivare a quelle relative alla nostra salute e alle cose della politica. Più soggetti terzi – sempre più spesso, peraltro, in maniera poco trasparente – raccolgono e trattano dati capaci di consegnare loro un enorme conoscenza sulle nostre inclinazioni, le nostre preferenze e le nostre debolezze, più tali soggetti – anche grazie agli algoritmi di intelligenza artificiale e ai *big data* – acquisiscono l'abilità di orientare, guidare, talvolta persino determinare ogni genere di nostra decisione. Meno *privacy* significa meno libertà.

In un recente convegno internazionale che si è tenuto a Palermo si è parlato di ruoli di responsabilità e controllo della Privacy in ambito sanitario. Gli esperti intervenuti si sono soffermati, in particolare, sul ruolo del DPO. Si può fare un bilancio sui vantaggi che l'introduzione di questa figura ha apportato nei contesti produttivi?

Forse è ancora presto, a poco più di tre anni dall'entrata in vigore delle nuove regole e dall'introduzione nel nostro Ordinamento della figura del DPO per fare bilanci attendibili. Si è, indiscutibilmente, trattato di una misura apprezzabile che, in generale, sta contribuendo in maniera significativa, almeno, alla diffusione della cultura della privacy in contesti pubblici e privati nei quali, prima, tale cultura non esisteva. Guai, però, a negare che, come in molte cose della vita, la differenza la fanno le persone. Ci sono DPO che, in una manciata di mesi, hanno accresciuto enormemente la qualità delle organizzazioni nelle quali operano e ci sono DPO che si sono lasciati travolgere dalle organizzazioni nelle quali operano senza riuscire ad apportare alcun contributo significativo. La scelta di un DPO è una scelta strategica dell'ente – pubblico o economico che sia – e deve essere fatta nel modo più rigoroso possibile lasciandosi guidare dalla ricerca delle maggiori competenze disponibili sul mercato. Se si affronta tale scelta come se si trattasse di una formalità burocratica alla quale adempiere, non si fa un buon servizio né alla propria realtà aziendale o amministrativa, né, più in generale, al diritto alla privacy.

L'"errore" di Cartesio

Mi rifaccio a un passaggio dell'intervento che ha tenuto nel capoluogo siciliano: **"Abbiamo accettato supinamente dopo l'11 settembre una compressione forte della nostra libertà di agire e di muoverci. Da quel momento – ha ricordato - anche se è cessato quel pericolo non siamo più tornati indietro, questo deve far riflettere sui percorsi da seguire in una società segnata da criticità ricorrenti. Quello che appare sempre più evidente è la difficoltà a trovare un bilanciamento tra i diritti universali, la libertà e la sicurezza. Impresa sempre ardua per ogni legislatore a qualsiasi latitudine si trovi ad operare, se pensiamo che sarà chiamato a ridisegnare il campo delle norme, entro cui si costruiscono quelle relazioni sociali, che fanno comunità e che sono alla base del nostro vivere civile". *Non vorremmo certo trovarci nei "panni scomodi" del legislatore, quali scenari si aprono sul terreno del delicato bilanciamento tra sicurezza e libertà?***

La situazione è tradizionalmente delicata con picchi – come quelli registrati dopo quel famoso undici

settembre del 2001 e negli anni della pandemia – emergenziali. Solo il diffondersi di una reale cultura dei diritti fondamentali – privacy inclusa – può cambiare significativamente le cose. Bisogna ricordarsi che, in democrazia, non esistono diritti, ovvero diritti capaci di fagocitare altri diritti e che la compressione di un diritto dovrebbe essere accettabile solo nella misura minima necessaria per consentire l'esercizio di un altro diritto e per il tempo strettamente necessario al raggiungimento di tale risultato. Soprattutto, non dovremmo mai dimenticare le parole di Louis Brandeis, uno dei padri del diritto alla privacy, in una celeberrima dissenting opinion mentre era giudice alla Corte Suprema degli Stati Uniti d'America: *"L'esperienza dovrebbe insegnarci a essere più preoccupati di proteggere la libertà quando un governo persegue scopi benefici. Gli uomini sono naturalmente all'erta per respingere l'invasione della loro libertà da parte di governanti malvagi. I più grandi pericoli per la libertà si nascondono nell'azione insidiosa di governi ben intenzionati ma incapaci di comprendere le conseguenze delle loro azioni sulle libertà e i diritti fondamentali."*

In un affascinante saggio, "L'errore di Cartesio", richiamato dal filosofo Giacomo Marramao in occasione della giornata europea della Privacy che ogni anno l'Autorità Garante organizza, Antonio Damasio chiama in causa il celebre pensatore del "cogito", responsabile di non aver tenuto conto che la "sostanza" dell'individuo è costruita su un fitto intreccio di ragione e passione. "La mente è un idea del corpo, mentre il cervello è un sentire il corpo emozionalmente", la mente non svela, per dirla in sintesi, la nostra identità. Questa suggestione ci fa comprendere molto bene che la nostra biografia è qualcosa che va oltre la biologia. Quali sono le implicazioni sul complesso piano dei neurodiritti?

La mente non è certamente la nostra identità ma nella mente prendono forma e, in parte, azione la più parte delle nostre scelte che danno forma alla nostra identità. L'accesso di terzi alla nostra mente e ai nostri pensieri ormai divenuto realtà espone la nostra libertà di plasmare la nostra identità a un rischio enorme. Non è lontano il giorno nel quale il nostro pensiero potrà essere eterodeterminato e, quel giorno, noi ci troveremmo ad essere non chi vorremmo essere ma chi, soggetti terzi, decideranno noi si debba essere. Ieri, tutto questo, era possibile solo nei romanzi di fantascienza.

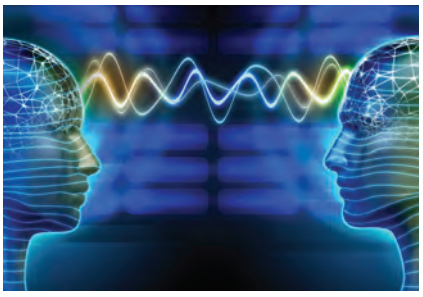
La Tecnoscienza e la prospettiva del "metaverso"

Il prepotente sviluppo della tecnoscienza impone una sempre maggiore capacità dell'uomo di governarla. Tema delicatissimo su cui ha lavorato per una vita Stefano Rodotà invocando una "Costituzione per Internet" oltre che una tutela efficace di quello che definiva il "corpo elettronico", anticipando tante delle questioni che sono esplose negli ultimi anni. Quello di Rodotà è destinato a rimanere un sogno da confinare nel regno dell'utopia?

Credo che quello di Stefano resti, in questa stagione della vita del mondo, l'unico scenario capace di garantire che il *"metaverso"* che verrà non rappresenti una delle ultime stagioni delle nostre democrazie. Nessuna utopia, quindi ma un progetto, il più solido di tutti, di scongiurare il rischio di una prepotente privatizzazione di ogni dinamica di governo dell'esistenza umana. Senza una carta universale dei diritti, saranno, inesorabilmente, i termini d'uso dei grandi fornitori di servizio a decidere cosa chiunque di noi può fare o non fare, dire o non dire e, dunque, a scrivere il futuro dell'intera umanità.

Discipline come il* Brain-raiding*, competenza che consente di leggere il pensiero, e di interpretare la superficie, che credevamo insondabile, delle motivazioni profonde che innescano l'azione del soggetto, che implicazione possono avere sul piano della disciplina giuridica?

Se il pensiero diventa accessibile a prescindere da ogni sua manifestazione e se diviene hackerabile, ci sono interi sistemi regolamentari, da quelli in materia negoziale e a quelli relativi alle cose della democrazia che andranno radicalmente ripensati e riscritti. Sin qui la volontà inespressa – in qualsivoglia dimensione – è improduttiva di effetti giuridici. Ma, naturalmente, questo stato di cose non potrà restare tale se, domani, anche i pensieri inespressi saranno – come in parte già sono – conoscibili da chiunque.



La triplice scansione* Habeas corpus, habeas data, habeas mentem *che si sta profilando con lo sviluppo della tecnoscienza, come va declinata nell'orizzonte filosofico e culturale posto a fondamento del sistema giuridico occidentale?

Il "metaverso" sarà un mix di realtà virtuale e realtà aumentata. In un contesto di questo genere anche i nostri sistemi giuridici andranno "aumentati" per renderli capaci di governare fenomeni che si arricchiranno – e, in parte, si sono già arricchiti – di nuove dimensioni. *L'habeas mentem* è, semplicemente, in questa prospettiva una nuova dimensione del diritto all'autodeterminazione dell'individuo da garantire e proteggere contro ogni esercizio di compressione. ■

Strumenti, cultura, consapevolezza, ecco il terreno di sfida della cybersecurity.

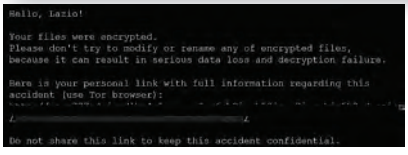
A colloquio con Michele Colajanni.

Autore: Massimiliano Cannata

"Non esistono zone franche, le organizzazioni sono tutte molto esposte, perché il business corre sui binari digitali. Lo stiamo vedendo in questi giorni tragici, in cui all'emergenza sanitaria si è aggiunto il dramma della guerra. Il rischio corre su un duplice binario: reale e virtuale, nessuna delle due componenti può essere trascurata. Malgrado le evidenze non abbiamo ancora compiuto quel salto culturale che ci può consentire di capire realmente che la sicurezza è un fatto di sistema, va perseguita e attuata coinvolgendo attori istituzionali, politici oltre che imprenditoriali". Michele Colajanni non ha dubbi: la sicurezza è un termine critico, lo sviluppo delle tecnologie amplia le aree da proteggere, non esistono isole felici. Proteggere dati e informazioni è un must, cui nessuno può sottrarsi.

Professore, i recenti attacchi, sferrati al sistema sanitario del Lazio e del Veneto hanno avuto degli impatti gravi per la vita di milioni di utenti. La* cybersecurity *non è più un tema per "appassionati" cultori, perché ha ricadute enormi sulla collettività. Qual è il suo giudizio in merito?

Avremmo dovuto comprendere da tempo, quanto fosse strategico il tema della sicurezza sul piano dello sviluppo della civiltà e della democrazia. L'aggravante di questa fase che stiamo vivendo è data dal fatto che gli "attaccanti" che minacciano la nostra "tranquillità" non si fanno alcuno scrupolo, sono sempre più interessati a estorcere denaro, nel più breve tempo possibile. Gli hacker, che dominano la scienza, non sono più gli originari "romantici" sabotatori solitari, né tanto meno dei "simpatici e abili" smanettatori del web, come una certa letteratura li ha per lungo tempo consegnati al nostro immaginario. Ci troviamo di fronte a organizzazioni a delinquere, con criminali che vendono servizi ad altri criminali, andando a costituire una rete di protezione difficile da contrastare.



Nella geografia del rischio l'Italia come si colloca?

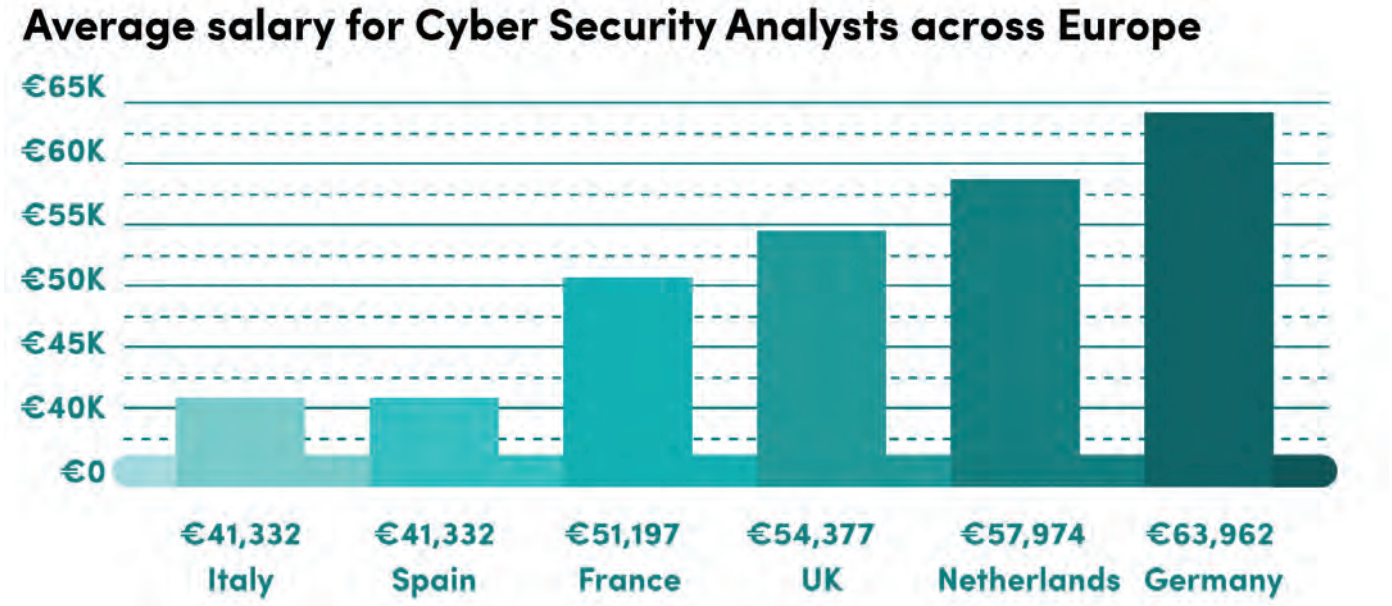
Diciamo subito a scanso di equivoci che nessuna organizzazione aziendale, né istituzione in nessun paese del mondo può ritenersi completamente al sicuro, neppure negli USA paese considerato leader in questo campo. Bisogna aumentare i livelli di difesa, servono strumenti, certo, ma anche cultura e consapevolezza. L'Italia è

oggettivamente più indietro, anche se l'istituzione di un'agenzia per la cyber security va letta come un importante passo avanti.

Si parla molto di collaborazione tra pubblico e privato, su questo fronte qual è lo stato dell'arte?

Al di là della retorica ancora poco è stato "messo a terra". Le aziende sono molto competitive, dovrebbero imparare e aprirsi maggiormente alla logica collaborativa, anche le istituzioni dovrebbero fare dei passi avanti in questa direzione. Bisognerebbe trovare delle forme di inventivo che facciano da catalizzatore, al fine di accelerare processi che si presentano ancora troppo lenti rispetto ai ritmi dell'evoluzione scientifica e tecnologica.

Lei svolge il suo lavoro all'Università, altro attore importante nella partita dell'innovazione e dello sviluppo. Le nuove generazioni come si



pongono rispetto a una grande questione come quella relativa all'uso consapevole dei media?

I giovani sono molto più avanti, competenti e sensibili di quanto siamo comunemente portati a credere. Cerchiamo di valorizzarli prima che siano gli altri paesi a sottrarci le migliori intelligenze. Insegnando cyber security mi confronto giornalmente con studenti dell'ultimo anno di corso, li trovo molto motivati, purtroppo vengono puntualmente delusi dal mondo del lavoro. La doccia fredda arriva da lì. Il nostro limite rimane quello della gestione dei talenti, senza una connessione vera tra università e mondo del lavoro le nostre rimangono, purtroppo, parole al vento.

Il ministro Colao in occasione del Forum di Cernobbio nello scorso autunno ha annunciato la nascita di un* cloud *di stato. Cosa comporterà sul piano del cambiamento degli standard di protezione?

Credo che la strategia sia in generale corretta. Si parla da molto tempo di cloud per il mondo della PA, l'esigenza viene da lontano ma non ha ancora trovato un'adeguata realizzazione. È un cantiere aperto che deve anche trovare i cittadini pronti a vigilare e a intervenire perché dalle parole si possa passare, anche in questo caso, a fatti concreti.

Smart working, IOT, tecnologie applicate al lavoro, il mondo è sempre più popolato da infoappliances. Della "rivoluzione in corso" che cosa dobbiamo comprendere?

Che siamo di fronte a un profondo cambiamento delle organizzazioni produttive, non alla mera sostituzione di strumenti vecchi con apparati più nuovi e magari più sofisticati. La stessa cultura del lavoro deve evolversi, come la misurazione delle prestazioni. Alt alla logica del cartellino, cominciamo a valutare chi è veramente capace di dare un

valore aggiunto, di conferire qualità a processi, agendo con originalità e spirito di autonomia. Tutti i dipendenti saranno in prima fila in questa nuova stagione, purché si riesca ad allentare il senso rigido della gerarchia, per lasciare posto a un rapporto paritario, che faciliti il confronto sui temi del futuro. La sicurezza non può che giovarsi di questo, perché ha bisogno di un terreno di autentica condivisione di esperienze e competenze, per rafforzarsi. Stiamo creando l'Internet delle cose. Sarebbe opportuno che fin dalla progettazione vengano rispettati certi protocolli di protezione. Macchine intelligenti, sistemi automatici, la loro sicurezza non è solo un fatto relativo alla protezione dei dati, perché attiene alla società, presa nel suo complesso. ■

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.

Sicurezza, complessita' e crisi Planetaria.

Intervista VIP con Mauro Ceruti.

Autore: Massimiliano Cannata

Lo scenario che ci rivela la crisi, che nella guerra in corso in Ucraina sta avendo l'espressione più drammatica, prefigura un nuovo corso della civiltà, dello sviluppo e della mondializzazione. Per affrontare positivamente le sfide del futuro e per resistere alle tentazioni regressive è necessario un cambiamento di paradigma, un nuovo modo di costruire la nostra conoscenza del mondo, in grado di coglierne la complessità. Come ha detto Albert Einstein: "Non si risolve un problema con i modi di pensare che l'hanno generato". Le parole di Mauro Ceruti, filosofo, tra i principali esponenti a livello mondiale del pensiero complesso fanno vedere molto bene come il tema della sicurezza, sia legato a una molteplicità di fattori interdipendenti, che impongono una visione interdisciplinare e una corretta *governance* dei sistemi complessi.

Professore, la sicurezza non è un concetto astratto. Il conflitto nell'Est Europa fa vedere un duplice teatro reale e virtuale. Le tecnologie giocheranno un ruolo fondamentale, mentre purtroppo si conta la perdita di tante vite umane e cresce il numero dei rifugiati a dismisura. Una crisi rilevatrice, Lei ha commentato. Può spiegare perché?

Ho parlato di "crisi rilevatrice" perché non possiamo continuare a leggere la contemporaneità usando le lenti interpretative del '900. La sicurezza, dopo la fine del leviatano e dell'idea di nazione figlia della cultura del secolo scorso non può essere garantita con strumenti ormai desueti. Non siamo di fronte a un "nuovo '39". Anche se i due terzi dell'esercito russo sono schierati in Ucraina, la disponibilità dell'atomica frena qualsiasi istinto interventista da parte delle forze Nato. Insomma, non ci può essere spazio per quella sottovalutazione e per quello che definirei lo spettro della semplificazione, che nel passato ha aperto il campo all'escalation di Hitler e del nazifascismo, innescando un terrificante effetto domino. Oggi, per una sorta di eterogenesi dei fini, la guerra sta facendo emergere uno spirito unitario, nel cuore del vecchio Continente, che credevamo sopito per sempre.

Complessità e riduzionismo

La teoria della complessità si sta prendendo la rivincita sul "riduzionismo". Quali scenari si aprono in un momento così difficile che vede il sovrapporsi dell'emergenza sanitaria che aveva già spossato l'Europa, con l'emergere nel "neoimperialismo zarista" manifestato da Putin, che sta mettendo sotto scacco gli equilibri del pianeta?

La difficoltà del momento storico che stiamo vivendo dovrebbe dimostrare come la pretesa di prevedere tutto nel gioco delle interconnessioni sistemiche e globali sia una pretesa vana. Non possiamo controllare tutti gli anelli retroattivi innescati dall'azione e dalla tecnica umane nel mondo e sulla natura. Mai come oggi abbiamo avuto a disposizione una potenza così grande, attraverso le nuove tecnologie. E mai come oggi abbiamo avuto a disposizione una potenza così grande, nella medicina in particolare.

Ma in questa potenza si nasconde una nuova fragilità. Nel mondo globale, tutto è connesso. Viviamo in un'ecumene completamente umanizzata, dove ogni evento locale può comportare conseguenze che possono amplificarsi su scala globale. Capire i segnali anche più deboli, in sistemi lontani dall'equilibrio come quelli in cui ci muoviamo risulterà perciò decisivo per capire dove stiamo andando.

Seguendo il suo ragionamento appare chiaro che siamo dunque avviluppati in un paradosso. Le tecnologie pervasive dovrebbero renderci più sicuri, più padroni del nostro destino invece…

La fragilità ci segna e ci accomuna, mentre sta emergendo una nuova condizione umana, profilata dall'inedito e simultaneo aumento di potenza tecnologica e di interdipendenza planetaria. In passato, il sorgere e l'evoluzione della vita sulla Terra ha reso il pianeta un unico sistema integrato fatto di aspetti biotici e di aspetti geologici e fisico-chimici del tutto inscindibili. Oggi, gli sviluppi della storia umana hanno aggiunto complessità a complessità: con il risultato che il destino dell'entità planetaria è intrinsecamente interdipendente con i nostri sviluppi politici, sociali, economici, culturali. Questo aumento di potenza e di interdipendenza motiva l'ipotesi dell'Antropocene.

Quali sono le conseguenze di questa prospettiva?

Dobbiamo concepire la Terra come un unico sistema dinamico complesso, autoregolato, con componenti fisiche, chimiche, biologiche e *anche* umane, non dimentichiamoci che l'umanità è diventata una grande forza della natura. E il cambiamento causato dall'uomo è, a sua volta, un processo multidimensionale, che perciò richiede una comprensione multicausale. Una comprensione in grado di intrecciare i cambiamenti umani sociali, politici ed economici con le loro diverse conseguenze ambientali, fisiche, chimiche, geologiche, su scala locale e globale. Natura e società sono diventate una cosa sola, con l'Antropocene, la possibilità di distinguere tra storia umana e storia naturale è, infatti, finita per sempre.

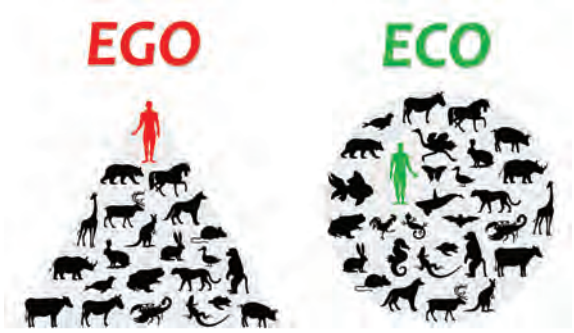
BIO

Mauro Ceruti è Professore Ordinario di Filosofia della scienza presso l'Università IULM di Milano, dove insegna Filosofia della Complessità. È Membro del Comitato Scientifico della *Association Européenne Modélisation de la Complexité* (MCX), ed è stato Ricercatore presso la *Faculté de Psychologie et Sciences de l'Éducation* dell'Università di Ginevra, e, a Parigi, presso il CETSAP, *Centre d'Études Transdisciplinaires - Sociologie, Anthropologie, Politique* del CNRS; Docente presso molte Università, Preside della Facoltà di Scienze della Formazione dell'Università di Milano-Bicocca, Preside della Facoltà di Lettere Filosofia dell'Università di Bergamo; Presidente della SILFS - Società Italiana di Logica e Filosofia della Scienza; Membro del Comitato Nazionale per la Bioetica della Presidenza del Consiglio dei Ministri.
Fra i suoi libri, tradotti in molte lingue, segnaleremo: *Il secolo della fraternità. Una scommessa per la Cosmopolis*, Castelvecci, Roma 2021; *Abitare la complessità. La sfida di un destino comune*, Mimesis, Milano 2020 (con F.Bellusci); *Sulla stessa barca,* Qiqajon, Magnano 2020; *Il tempo della complessità,* Raffaello Cortina, Milano 2018; *Evoluzione senza fondamenti,* Meltemi, Milano 2019; *La fine dell'onniscienza,* Studium, Roma 2015; *Il vincolo e la possibilità*, Raffaello Cortina, Milano, 2009; *La danza che crea*, Raffaello Cortina, Milano 1989; *La nostra Europa,* Raffaello Cortina, Milano 2013 (con E. Morin); *Origini di storie,* Feltrinelli, Milano 2009 (con G. Bocchi).

"Il secolo della fraternità"

La sicurezza in questo "universo di partecipazione" dove si colloca?

La sicurezza è un termine critico, che per definizione assume una molteplicità di significati. La rivoluzione digitale di fatto ha dilatato, all'estremo, l'orizzonte delle responsabilità umane, individuali e collettive verso le specie viventi, verso gli ecosistemi naturali, verso il pianeta nella sua interezza, verso la possibilità stessa della sopravvivenza della nostra specie. Le conseguenze delle azioni umane si dilatano nello spazio e nel tempo. Un manager che opera nella security non può non tenere



conto della complessità di un tale scenario, adottando una visione unilaterale, perché corre il rischio di non assicurare quella tutela di cui individui e organizzazioni hanno bisogno.

Passare dall'interdipendenza tecno-economica, all'interdipendenza solidale, per recuperare un equilibrio sostenibile, questa la tesi di fondo de:* "Il secolo della fraternità" *(ed. Castelvecchi) il saggio che ha pubblicato con Francesco Bellusci. È questa la strada che può tirarci fuori dalla "lunga notte" entro cui siamo precipitati?

Cominciare col riconoscere la nostra fragilità e vulnerabilità, che vuol dire riflettere sulla dimensione relazionale del soggetto e delle sue interdipendenze biologiche, sociali, affettive, può essere un passo decisivo. È, infatti, questa la via che conduce al sentimento di fraternità, che può aiutarci a corregge quella concezione semplicista e individualistica della libertà, termine che fa sempre coppia con la sicurezza in un delicato e sofferto bilanciamento.

Non pensa che la prassi politica, in un orizzonte problematico come quello che abbiamo davanti, non abbia tempo per coltivare la fraternità?

Al contrario credo che il principio di fraternità deve ispirare sia la protezione delle *antropodiversità* sia la protezione delle biodiversità. La solidarietà è stato ed è il motore delle politiche di Welfare a livello nazionale, mentre la fraternità è il motore della costruzione di politiche di una communizzazione globale che ci

costringe anche al rispetto degli equilibri della biosfera, perché *"nessuno si salva da solo"*. Questa sfida deve tradursi in obiettivi politici e sociali concreti.

Quali per esempio?

A livello globale urge una svolta nelle forme della cooperazione internazionale, che facciano entrare stabilmente la sicurezza del "pianeta" nell'agenda politica; a livello nazionale-locale è necessario estendere le forme della poliarchia e della partecipazione democratica attraverso una riattivazione del ruolo dei corpi intermedi. Come dimostra anche la vicenda europea del *Recovery plan*, occorre l'impegno da parte di tutti per trasformare le interdipendenze riconosciute in reale *solidarietà:* solidarietà che è strumento essenziale per abitare la complessità e affrontare l'imprevedibile.

"Abitare la complessità" è il titolo di altro suo recente scritto, realizzato sempre con la collaborazione di Bellusci. Uno spettro si aggira: "l'uomo semplificato". Può in conclusione spiegare ai lettori di Cybersecurity Trends di che cosa si tratta?

Con Bellusci trattiamo nel saggio le conseguenze di un errore tragico che incombe: quello di estendere sulla società e sulle relazioni umane i vincoli e i meccanismi non umani della macchina artificiale, di ridurre l'umano e la percezione di noi stessi a un insieme di "dati". L'affidarsi agli algoritmi non deve renderci ciechi di fronte alla complessità del reale e far disabituare la nostra mente ad essere complessa! Per questo occorre un nuovo umanesimo, veicolato da nuovi modelli educativi e nuovi insegnamenti. *Abitare la complessità* è, detto in altri termini, la via maestra per avviare una nuova fase della mondializzazione, in cui tutto è connesso, per abitare in un modo nuovo e non (auto)distruttivo il nostro pianeta, e per riconoscersi in quello che è un destino comune. ■

L'efficacia del phishing: gli elementi utili per un adeguato livello di difesa.

Autore: **Luca Nilo Livrieri, Senior Manager sales engineers for Southern Europe**

Una delle migliori difese contro lo spionaggio digitale è la formazione, anche intesa quale grande opportunità per mettere a disposizione dei professionisti della cybersecurity uno strumento in più per sensibilizzare ed educare, in maniera semplice, gli utenti finali sul tema del ransomware.

Il termine «phishing» risale al 1995 e consiste in una tattica di attacco informatico che è stata utilizzata da una vasta gamma di avversari: dagli script kiddies alle organizzazioni sponsorizzate dagli stati-nazione. Eppure, la più grande minaccia che il phishing presenta ai professionisti della sicurezza informatica non risiede nella tattica in sé, ma nel danno che essa può causare.

Uno dei metodi più efficaci per proteggersi da tale minaccia è quello di educare le persone ad individuare e segnalare un tentativo di phishing. Ma in cosa consiste la minaccia del phishing e quali sono le pratiche ottimali per affrontare questo problema persistente?

Il phishing è una tecnica di ingegneria sociale che utilizza le e-mail per spingere o ingannare gli utenti a cliccare su link web o allegati che appaiono come legittimi, ma che, invece, sono stati progettati per compromettere il computer del destinatario o ingannare quest'ultimo a rivelare le proprie credenziali o altre informazioni sensibili. La pratica risiede proprio nella capacità degli avversari – siano essi singoli criminali o organizzazioni sponsorizzate dagli stati-nazione – di creare messaggi che appaiono come legittimi: un'e-mail di phishing può, ad esempio, sembrare provenire dalla propria banca, datore di lavoro o responsabile, può usare tecniche per estorcere informazioni e camuffarsi in un'agenzia governativa.

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.

Sia che si tratti di un singolo criminale o di un'organizzazione sponsorizzata dagli stati-nazione, le motivazioni legate ai tentativi di phishing sono molteplici. In una e-mail di phishing un avversario può tentare di:

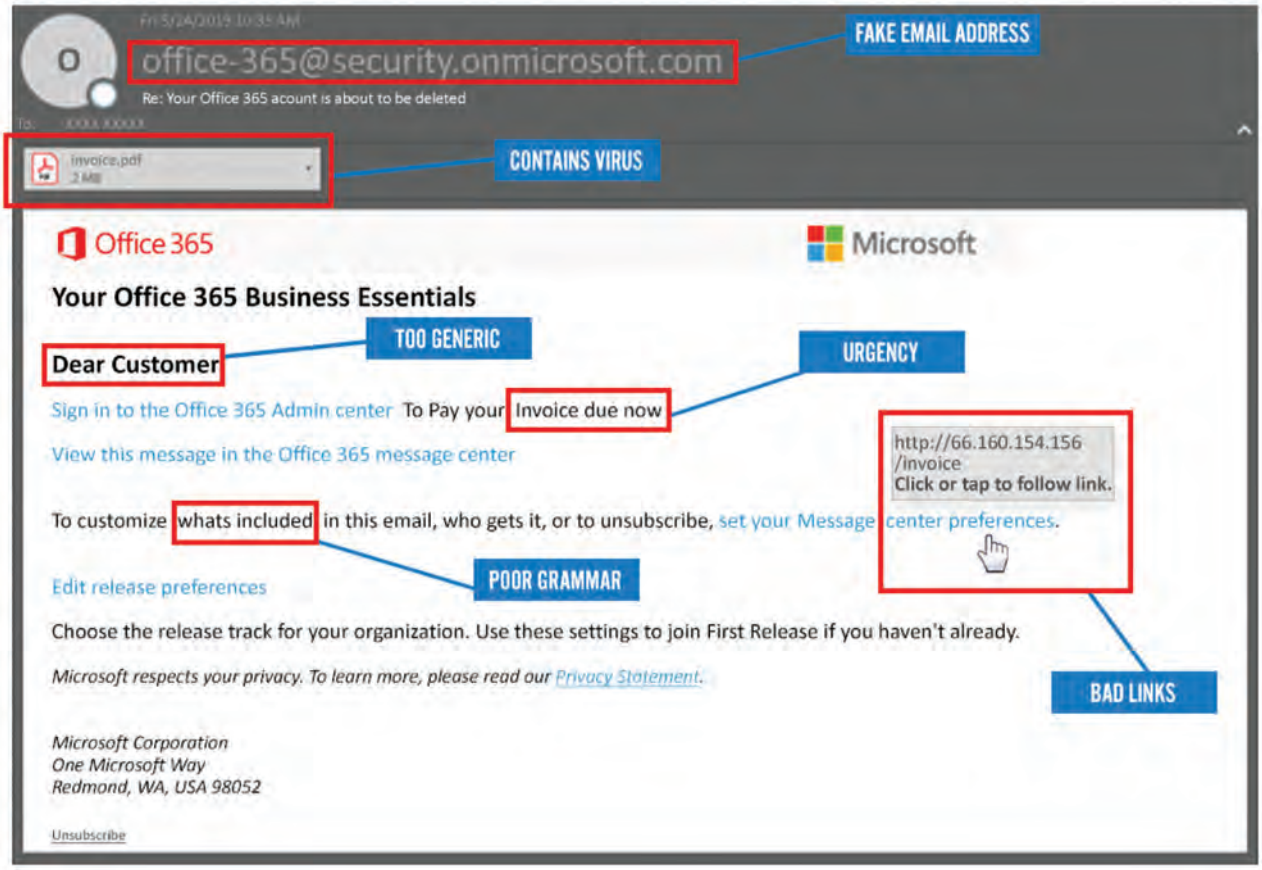
- rubare le credenziali dell'account per estorcere denaro alla persona o all'azienda;
- rubare le credenziali dell'account di lavoro per risalire al datore di lavoro;
- diffondere software malevoli per avere accesso al PC di lavoro, personale o alla rete per rubare la proprietà intellettuale.

A prescindere da quale sia la motivazione, il phishing fornisce agli avversari un metodo di attacco a basso rischio che offre un alto potenziale di guadagno finanziario. Ed è per questo che la minaccia del phishing mantiene i CISO pronti: gli avversari usano infatti la tattica più e più volte proprio perché funziona. Gli utenti sono spesso occupati e distratti, inclini a cliccare sui link senza prestare troppa attenzione alla fonte e i dati lo confermano: le aziende hanno, in media, un tasso di clic del 10%, dunque con un'alta probabilità gli utenti cliccheranno su un link illegittimo e forniranno informazioni o credenziali del loro account ad un phisher.

Un tipico attacco di phishing comporta l'invio di massa di e-mail per indurre chiunque a cliccare su link dannosi. L'intento potrebbe essere quello di diffondere un ransomware, rubare le credenziali di un account esistente, acquisire informazioni per aprire un nuovo account fraudolento o, semplicemente, compromettere un endpoint. Poiché tutti hanno un indirizzo e-mail, e poiché la tattica offre diverse opzioni per l'avversario, il phishing è una questione di numeri in un ambiente ricco di bersagli, in cui solo un numero relativo basso di persone deve essere ingannato affinché l'avversario possa trarne profitto.

Un'altra tipologia di attacco, anche se meno diffuso, è lo spear-phishing, una tattica più specializzata in cui l'avversario prende di mira specificamente i dirigenti di alto profilo o altri ruoli sensibili all'interno di un'azienda. Per creare un'e-mail di spear-phishing, l'avversario raccoglie informazioni sui suoi obiettivi, solitamente facilmente accessibili tramite siti web aziendali o social media quali LinkedIn, Facebook e Twitter. L'avversario utilizza tali informazioni per creare e-mail altamente personalizzate per invogliare l'utente a cliccare su un link, con l'obiettivo di rubare informazioni sensibili dal loro computer o rete, utilizzare tali informazioni per colpire altri dipendenti attraverso la compromissione delle e-mail aziendali per estorcere denaro.

Il phishing è difficile da combattere con la sola tecnologia. Seppur esistano molte soluzioni in grado di prevenire tali attacchi, la maggior parte di esse è stata pensata per essere utilizzata in modo reattivo, piuttosto che proattivo. Di conseguenza, fino al 20% di mail di phishing riuscirà ad essere inviata. Inoltre, in alcuni casi, come quando l'account e-mail aziendale di una società è compromesso e utilizzato per inviare e-mail di phishing, la



tecnologia anti-phishing non riuscirà a fermare una seconda mail inviata da una fonte legittima.

Fermare il phishing, quindi, non è solamente una questione di tecnologia, ma richiede l'attenzione di tutti. Le persone devono essere formate a riconoscere un potenziale tentativo di phishing e prestare costantemente attenzione, così da segnalare eventuali tentativi al personale addetto alla sicurezza informatica aziendale.

Ecco cinque segnali a cui prestare attenzione e che necessitano di essere segnalati:

1 un'e-mail inaspettata che richiede un'azione come cambiare una password, inviare denaro, acquistare carte regalo o accedere ad un sito web;

2 un'e-mail il cui corpo sembra essere legittimo, ma è stato inviato da un noto sito di posta elettronica gratuita o da un dominio web sconosciuto (ad esempio, un'e-mail che sembra provenire dal fornitore locale di energia elettrica, ma in realtà è stata inviata da un account @gmail);

3 un'e-mail con parole scritte in modo sbagliato, contenenti errori grammaticali o con una formattazione distorta;

4 un'e-mail che sembra contenere allegati sospetti;

5 un'e-mail che contiene link web che sembrano legittimi ma che si rivelano provenire da domini web falsi o sconosciuti (ad esempio passando il cursore su di essi).

Spesso, le e-mail di phishing sono facili da individuare e possono essere facilmente segnalate. Altre, tuttavia, possono essere meno riconoscibili. Ogni volta che non si è completamente sicuri della legittimità di un'e-mail è opportuno segnalarla al team di sicurezza e aspettare le loro indicazioni prima di compiere qualsiasi azione.

Il phishing - e l'ingegneria sociale in generale - semplicemente funziona poiché quasi tutti hanno un indirizzo e-mail. Parallelamente, la natura fiduciosa delle persone, insieme alla volontà di aiutare gli altri, rende gli utenti spesso suscettibili di attacchi di phishing manipolatori. Proteggere se stessi e la propria organizzazione da questi cyberattacchi è un gioco di squadra che richiede l'essere vigili e saper prestare attenzione agli indizi sospetti, così da segnalarli al personale addetto a tale funzione. ■

La nostra memoria sta diventando un crogiolo di "conoscenze sconosciute"?

Autore: Laurent Chrzanovski

L'anno scorso, in un saggio sociopsicologico in memoria di Donald Rumsfeld, il popolare filosofo Slavoj Zizek ha ricordato il discorso del 2002 del defunto segretario della difesa statunitense, poco prima della guerra in Iraq. In questo discorso, intenzionalmente o no, Rumsfeld menzionava concetti essenziali della filosofia greca, cioè *le incognite sconosciute* ***(unknown unknowns)***, le *incognite conosciute* ***(known unknowns)*** e i noti noti (cose che sappiamo di sapere) ***(known knowns).*** Eppure, mancava un concetto nato molto di recente: le conoscenze sconosciute ***(unkown knowns).***

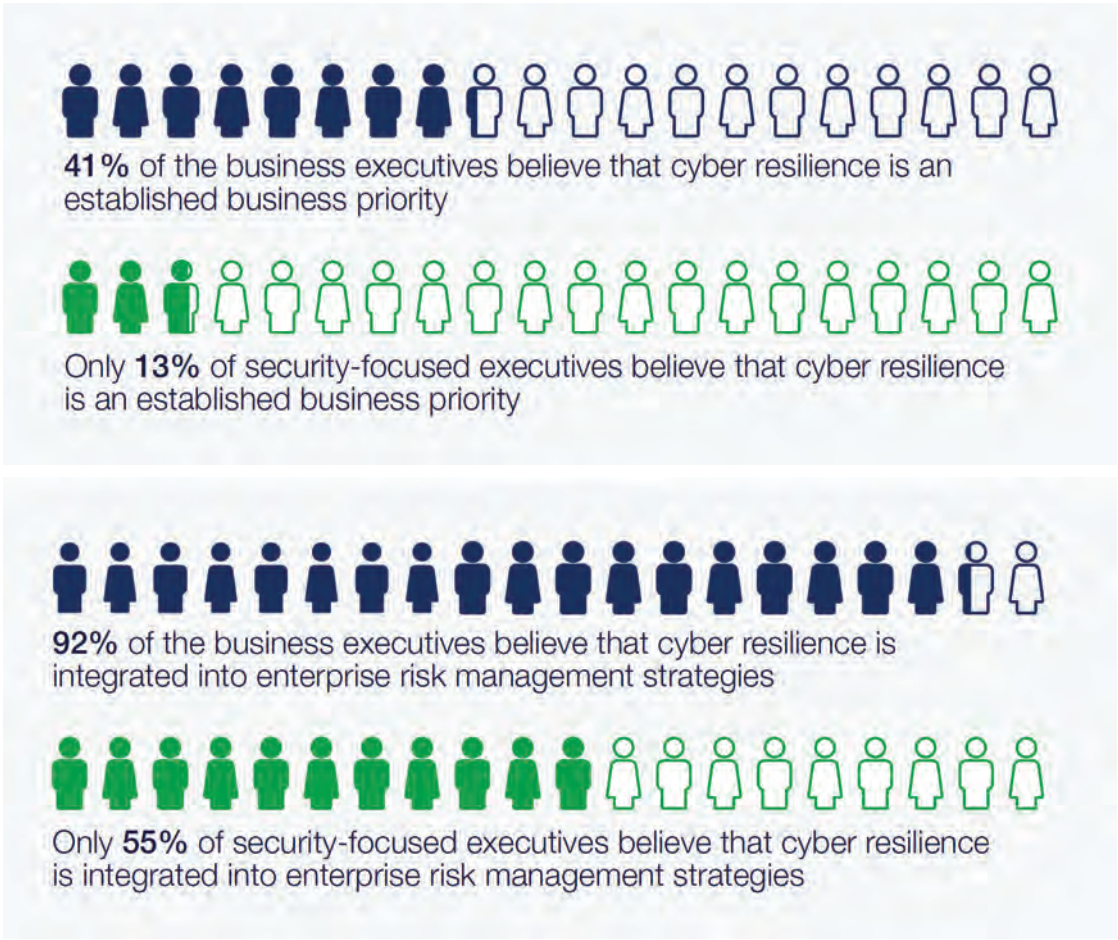
Come il filosofo tedesco Jürgen Habermas (2) ha sottolineato dal 2020, la nostra mente è così satura di informazioni che la nostra memoria è piena di conoscenze che abbiamo già... dimenticato. Questo fenomeno è profondamente radicato tra gli *"individui collegati ai media"*, cioè la maggior parte di noi che vive nei paesi sviluppati. La quantità di "notizie fresche" assorbite quotidianamente invade la nostra mente critica e spinge nell'oblio informazioni più vecchie, spesso essenziali, soprattutto le conoscenze ricevute ma che sono state poco o mai applicate nella nostra vita reale.

Arrivando al mondo della cybersecurity, la radice stessa del problema che genera i comportamenti umani appena descritti dai filosofi è diventata una preoccupazione reale. Al problema della *"sovra-informazione"* (misurata dalla quantità di materiale caricato e poi scaricato/letto sul web ogni minuto, in tutto il mondo) viene dedicato almeno un intero capitolo nel *Global Cybersecurity Outlook 2022* del World Economic Forum pubblicato il mese scorso (3).

Nuovi dati creati/visti in un minuto.
© Global Cybersecurity Outlook 2022, p. 12, figura 3

Dall'alto verso il basso: esperti di business contro esperti di sicurezza

Il rapporto del WEF sottolinea, all'interno degli "unknown knowns", come sia diventato più grande che mai il divario medio tra la fiducia dei membri del consiglio di amministrazione *("business executives")* sulle politiche e di conseguenza sui sistemi utilizzati all'interno della loro azienda e le paure



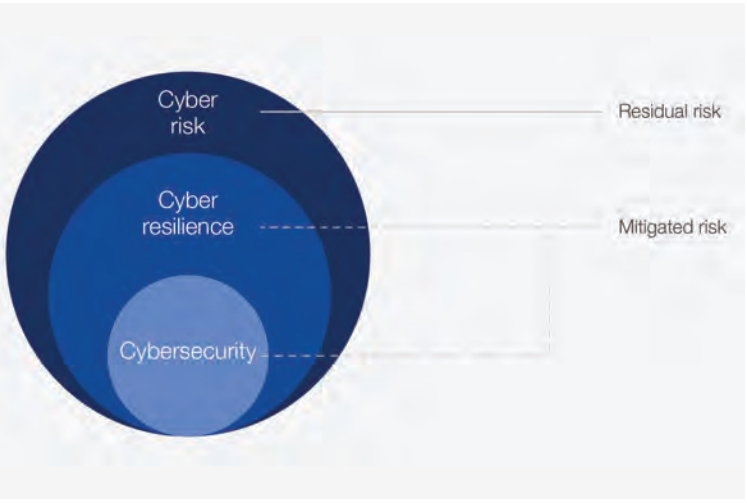
Fiducia nella priorità e nell'integrazione della resilienza informatica, le opinioni degli specialisti di business rispetto a quelle degli specialisti della sicurezza.
© Global Cybersecurity Outlook 2022, p. 19-20

dei team di sicurezza della stessa azienda *("security-focused executives")*. Su questo argomento si basa un ampio capitolo del rapporto: *"gli esperti di cybersecurity si trovano sempre più in una posizione precaria a dimostrazione che il divario tra i business leaders ed i security leaders aumenta".*

Il *Global Cybersecurity Outlook* sottolinea una serie di misure molto importanti da adottare immediatamente in tutti i settori aziendali, al fine di colmare questo divario che rappresenta una delle ragioni principali dell'incapacità nel contrastare adeguatamente forme molto primitive di cyber-attacchi riusciti durante la pandemia (phishing, scams e pure spams, ecc.).

Ancora una volta, il punto focale è uno degli argomenti che abbiamo trattato da tempo: la mancanza di inclusione del CISO e/o del CSO in seno ai membri del consiglio d'amministrazione, o ancora la mancata obbligatorietà di una loro presenza almeno durante le riunioni a carattere decisionale; queste sono tra le principali fonti di problemi che vanno poi a minare l'insieme della sicurezza aziendale.

Inoltre, la più grande differenza (e fonte di molti problemi), nel campo del *modus cogitandi* tra i business



Relazioni tra rischio informatico, resilienza informatica e sicurezza informatica.
© Global Cybersecurity Outlook 2022, p. 16

leader e gli specialisti della sicurezza, si evidenzia nel concetto che gli specialisti del business hanno della cybersecurity e della cyber resilienza: la maggior parte dei business leader considera i due domini come un tutt'uno e non mette in relazione le differenze, le specificità e le esigenze di ciascun ambito, all'interno della cornice più ampia della *governance* della cybersecurity.

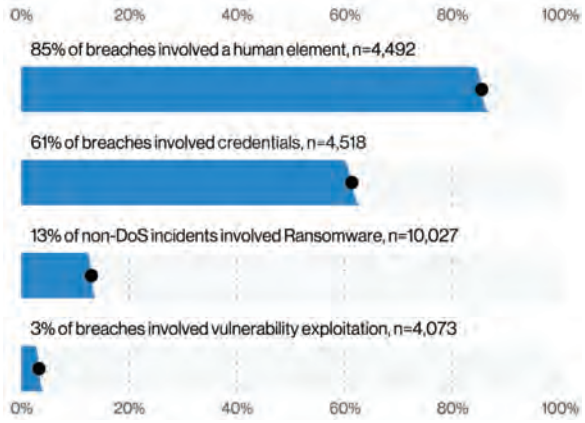
La quantità record di cyberattacchi andati a buon fine osservata nel 2021 affonda le sue radici, secondo tutti i rapporti, in tutta una serie di decisioni inopportune prese durante i periodi di lockdown, alla quale si è aggiunta la continua trasformazione del mondo del lavoro che ha visto il passaggio dal lavoro in ufficio allo smart working, senza la preventiva implementazione di cambiamenti/adattamenti essenziali nei sistemi di sicurezza.

L'Outlook del WEF e gli altri rapporti menzionano anche che abbiamo raggiunto un punto critico di carenza di competenze nella cybersecurity, tema già trattato nella nostra rivista. Tuttavia, in relazione a questo argomento, sarebbero da rivedere i numeri dati da Forbes, dal WEF e da altre fonti, poiché riflettono anche l'incapacità di troppe istituzioni educative di fornire corsi e formazioni ad ampio spettro, esattamente come quelli descritti da ***Marco Essomba in un precedente numero*** della nostra pubblicazione: assumendo che la cybersecurity abbia sette livelli (stacks), la nuova generazione di esperti di cybersecurity dovrebbe essere in grado di padroneggiare almeno due se non tre di essi, con l'aiuto dalle nuove tecnologie ormai disponibili sul mercato.

Tutti i fattori sopra citati hanno avuto e continueranno ad avere gravi conseguenze sui costi assicurativi, che è la terza grande sfida per il mondo della cybersecurity per il 2022. Sfida presente nella *"Top 10 cybersecurity challenges"* proposto da E. Saygeh nelle previsioni annuali pubblicate da Forbes (4). Molte assicurazioni, i cui premi per la copertura cyber sono saliti alle stelle nel 2021, si rifiuteranno ormai di accettare di assicurare aziende che non hanno una politica rigorosa e completa di cybersecurity, che tenga conto sia del fattore tecnologico nonché umano, in particolare quest'ultimo avrà come punto di partenza la formazione obbligatoria per ogni singolo dipendente dell'azienda per sensibilizzare alla cyber security.

Dal basso verso l'alto: una costante mancanza di formazione sulla consapevolezza a tutti i livelli

I costi degli incidenti per le imprese, durante gli anni della pandemia, hanno raggiunto dei record. Come ha sottolineato il *Data Breach Investigations Report 2021* di Verizon (5), l'85% delle violazioni ha coinvolto l'ormai tradizionale anello debole, ovvero l'umano.



Verizon, Data Breach Investigations Report 2021, fig. 7, p.7

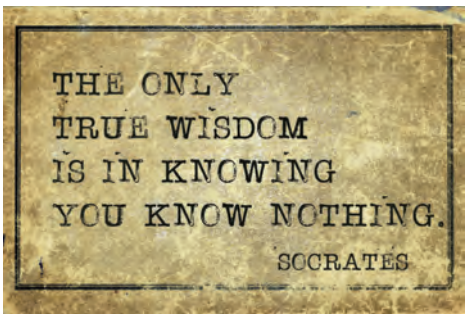
Nonostante la formazione nel campo della sicurezza sia una grande preoccupazione per tutti i settori d'attività, pochissimi, come le società di sicurezza, banche, o aziende industriali specifiche, come quelle dell'high-tech o del lusso, hanno intrapreso il compito costante di formare tutto il personale, dai dipendenti che effettuano le pulizie di notte sino al CEO, e questo su base regolare. Come Clive Madders (6) ha sottolineato di recente, è solo attraverso la formazione di una cultura della consapevolezza della cybersecurity che un'azienda può davvero diventare sicura. Oltre alla tecnologia necessaria, l'autore insiste sul fatto che *"Fortificare la prima linea (leggi: i dipendenti) è spesso il miglior metodo di difesa"*, ricordando lo scarso uso, fatto da molte aziende, delle essenzili linee guida pubblicate dal NIST già nel 2018, *"Cybersecurity is everyone's job"* (7).

Le conseguenze di anni di cybersecurity awareness mal pensata e soprattutto mal diffusa, sotto forma di documenti pdf o di poster sintetici di una pagina, sono state ampiamente palesate durante la pandemia. Queste "conoscenze" sono state in gran parte dimenticate da troppi impiegati che lavorano ormai a distanza, e che hanno, in risposta a "banali" mail di phishing, inserito la loro password, user id o altri dati sensibili, cliccato su link malevoli e, così facendo, hanno esposto le loro aziende a gravi problemi di sicurezza. Lo stress unito all'ignoranza, come è ben sottolineato dal recente studio *"Why employees violate cybersecurity policies"* dell'Università di Harvard (8), ha reso possibile tutto ciò. In un contesto di stress lavorativo quotidiano, le

tre ragioni principali riconosciute dai dipendenti per cui hanno aggirato le politiche di sicurezza si indentificano nelle seguenti risposte:

- "per svolgere meglio i lavori assegnati"
- "per ottenere qualcosa di cui avevo bisogno"
- "per aiutare gli altri a fare il loro lavoro".

Per comprendere meglio la ricerca di Harvard, una ricerca psicologica più approfondita dal titolo *"The Role of User Behaviour in Improving Cyber Security Management"* (9) è da considerarsi una lettura obbligatoria. Essa ci permette, lungi da focalizzarsi su un eventuale cattivo impiegato , di comprendere, tra le diverse categorie di ego che ogni dipendente umano può avere, quali sono quelle che portano ai più grandi errori e quindi a comportamenti poco sicuri. Lo studio spazia così dall'iper-confidenza in sé stesso all'impulsività e, soprattutto, a un sempre crescente desiderio di essere proattivo (cioè "pensare al futuro") per piacere ai superiori oppure per affrontare meglio lo stress legato alla quantità crescente di richieste supplementari da parte del diretto superiore. Tutti questi fattori portano a dimenticare le basi dell'igiene digitale e a non applicare le politiche di sicurezza che, troppo spesso, sono state e sono tutt'ora poco spiegate e quindi mal comprese già dal primo giorno della loro attuazione.



Per finire dove abbiamo iniziato, non c'è più tempo per permettersi il lusso di cercare di ricordare le *"conoscenze sconosciute"*. Per far fronte alla quantità sempre crescente di nuove tecnologie che usiamo, così come le specifiche modalità d'uso di ogni singolo prodotto, i loro punti di forza e naturalmente le loro debolezze, c'è bisogno di una nuova strategia (anche usando tecniche ludiche come quella della *gamification*) e di una sensibilizzazione dal basso verso l'alto, includendo assolutamente anche lo strumento più vulnerabile e, nonostante ciò, il più utilizzato: lo smartphone.

I dipendenti, se ben formati, dovrebbero essere soddisfatti del fatto che stanno imparando qualcosa di utile. Se si parte dal paradosso socratico descritto da Platone: **"ἔν οἶδα ὅτι οὐδὲν οἶδα" (so di non sapere)**, cioè da un atteggiamento di umiltà unito a molta apertura mentale, i dipendenti capiranno come evolvere ed agire in sicurezza non solo nel loro lavoro ma anche nella loro vita personale, proprio imparando le basi dell'igiene digitale e della cybersecurity. Anche il ruolo dei leader aziendali dovrà cambiare, premiando i team e gli individui non solo per la produttività ma anche per le politiche di sicurezza ben applicate. ■

BIO

Dottore di ricerca in Archeologia romana dell'Università di Losanna, Laurent ha poi ottenuto un diploma post-dottorale in Storia e Sociologia presso l'Accademia delle Scienze della Romania, l'abilitazione UE a dirigere Dottorati di ricerca nel campi della Storia e delle scienze affini. Oggi, Laurent è professore presso la Scuola dottorale e postdottorale dell'Universita' Statale di Sibiu. Tiene regolarmente corsi post-dottorato in Università di prestigio in diversi paesi dell'UE, in primis a Varsavia. E' autore/redattore di 31 libri, di oltre un centinaio di articoli scientifici e di altrettanti articoli destinati al grande pubblico.
Nel campo della cybersecurity, Laurent è membro e consulente contrattuale del gruppo di esperti dell'ITU. Ha fondato e gestisce ogni anno il trittico di congressi PPP "Cybersecurity Dialogues" (Romania, Svizzera, Italia) organizzati in collaborazione con un grande numero di istituzioni specializzate, internazionali e nazionali. Nello stesso spirito e con lo stesso spirito e con i stessi partner, è fondatore e redattore capo e redattore capo di Cybersecurity Trends, la prima rivista trimestrale di sensibilizzazione alla sicurezza informatica per adulti, pubblicata in quattro varianti adattate ad altrettanti ecosistemi lingusitsici e culturali. Il suo campo di studio è focalizzato sulla relazione tra i comportamenti umani nel mondo digitale e il bisogno di trovare il giusto equilibrio tra la sicurezza e la privacy per l'utente finale, cioè "l'e-cittadino" che siamo tutti diventati.

(1) Slavoj Zizek: Come l'approccio catastrofico di Donald Rumsfeld "incognite sconosciute" sull'Iraq può aiutarci ad affrontare la crisi di Covid, RT, 04.07.2021
https://www.rt.com/op-ed/528359-donald-rumsfeld-iraq-covid/
(2) Jürgen Habermas su Corona: "So viel Wissen über unser Nichtwissen gab es noch nie», Frankfurter Rundschau 10.04.2020
https://www.fr.de/kultur/gesellschaft/juergen-habermas-coronavirus-krise-covid19-interview-13642491.html
(3) World Economic Forum, Global Cybersecurity Outlook 2022, gennaio 2022
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
(4) E. Saygeh, Predicting What 2022 Holds For Cybersecurity, Forbes, 6 gennaio 2022
https://www.forbes.com/sites/emilsayegh/2022/01/06/predicting-what-2022-holds-for-cybersecurity/
(5) Verizon, Data Breach Investigations Report 2021. DBIR, autunno 2021
https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report
(6) Clive Madders, Protect Your Organization by Cultivating a Culture of Cybersecurity Awareness, 28 dicembre 2021
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/protect-your-organization-by-cultivating-a-culture-of-cybersecurity-awareness/
(7) NIST, Cybersecurity is Everyone's Job, 2018
https://www.nist.gov/news-events/news/2018/10/cybersecurity-everyones-job
(8) C. Posey, M. Schoss, Ricerca: Perché i dipendenti violano le politiche di sicurezza informatica, Harvard Business Review, 20 gennaio 2022
https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies
(9) A.A. Moustafa, A. Bello and A. Maurushat, The Role of User Behaviour in Improving Cyber Security Management, Frontiers in Psychology 12 (2021),
https://www.frontiersin.org/article/10.3389/fpsyg.2021.561011

Perimetro di Sicurezza Nazionale Cibernetica – L'approvvigionamento di beni, sistemi e servizi ICT.

Autore: Gianluca Bocci

Non so con quali armi si combatterà la terza Guerra Mondiale, ma posso dirvi cosa useranno nella Quarta: bastoni e pietre!

Albert Einstein

Il D.L. 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133 istituisce il c.d. **Perimetro di Sicurezza Nazionale Cibernetica** (d'ora in avanti **Perimetro**) con l'obiettivo di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici (d'ora in avanti **beni ICT**) delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati (d'ora in avanti **Soggetto\i**) da cui dipende l'esercizio di una funzione essenziale dello Stato ovvero la prestazione di un servizio essenziale. Con l'istituzione del Perimetro, sono stati successivamente pubblicati i decreti a carattere attuativo (V. Fig.1) con i dettagli e tecnicismi utili per la corretta applicazione della legge.

Con l'attuazione del primo decreto attuativo, il D.P.C.M. del 30 luglio 2020, n. 131, nel comparto della difesa, dell'interno, dello spazio e aerospazio, dell'energia, delle telecomunicazioni, dell'economia e finanza, dei trasporti, dei servizi digitali, delle tecnologie critiche[1] e degli enti previdenziali/lavoro, sono stati individuati i Soggetti appartenenti al Perimetro, nonché per ciascuno di essi, le relative funzioni e servizi essenziali, la cui interruzione o compromissione potrebbe arrecare un pregiudizio per la Sicurezza Nazionale.

Rimane distinta la funzione essenziale dal servizio essenziale nella misura in cui, la prima, tipicamente espletata da un soggetto pubblico, assicura la continuità dell'azione di Governo e degli Organi Costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti, mentre il secondo, erogato sia ad un soggetto pubblico, sia privato, assicura il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato.

Inquadrato il tema del Perimetro nel contesto della Sicurezza Nazionale, è importante sottolineare come con lo stesso, si pone l'attenzione nei confronti di realtà che, pur **non trattano informazioni classificate** mediante i loro Beni ICT, sono comunque ritenute di fondamentale importanza per la sicurezza del sistema Paese; per tale ragione e, non a caso, il legislatore nazionale, ravvisando la rilevanza di tali Soggetti e delle informazioni da essi trattati, per gli interessi dello Stato ha deciso di tutelare quest'ultimo attraverso l'istituzione, prima del Perimetro e poi della c.d. Agenzia di Cybersicurezza Nazionale (d'ora in avanti **ACN**).

Il Perimetro, insieme all'applicazione del c.d. Decreto NIS che recepisce sul territorio nazionale la Direttiva UE 2016/1148 del Parlamento Europeo e del Consiglio, con il fine di tutelare il business in riferimento al mercato digitale, chiude il cerchio rispetto alle esigenze e dunque alla garanzia di disporre

di un sistema di protezione più ampio e completo del dominio cibernetico nazionale.

Per garantire la tutela poc'anzi accennata, nel rispetto di quanto previsto nei decreti attuativi declinati dal D.L. 21 settembre 2019, n. 105, ricordiamo quali sono gli adempimenti che vincolano i Soggetti inclusi nel Perimetro, con un particolare focus sul DPR del 5 febbraio 2021, n. 54 e il DPCM del 15 giugno 2021, in materia di approvvigionamento dei beni ICT.

Figura 1 - Disposto normativo in materia di Perimetro Nazionale di Sicurezza Cibernetica

Identificazione e trasmissione dell'elenco dei beni ICT

Il DPCM del 30 luglio 2020, n. 131, già richiamato all'inizio di questo articolo, rappresenta le fondamenta per la corretta applicazione di quanto disposto con la pubblicazione e l'entrata in vigore dei diversi decreti attuativi che sottendono al Perimetro; infatti, il DPCM appena citato, impone ai Soggetti individuati, di identificare e trasmettere l'elenco dei beni ICT che caratterizzano le funzioni e i servizi essenziali, beni ICT che sono "centrici" e pertanto rappresentano il fulcro per la corretta applicazione delle disposizioni dettate dalla norma nella sua interezza. In particolare, l'elenco dei beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale o una loro compromissione con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni trattate, tali da arrecare un pregiudizio per la sicurezza nazionale, rimane determinato in esito all'**analisi del rischio** condotta dal Soggetto, sulla funzione o il servizio essenziale di sua pertinenza. L'analisi del rischio rappresenta dunque un passaggio fondamentale nell'adempimento di tutto quanto richiesto nell'ambito del Perimetro, al punto che possiamo senza dubbio ritenere l'intero impianto normativo di tipo *"Risk Based"*. La trasmissione dell'elenco dei beni ICT, inizialmente fatta dai Soggetti al DIS, vedrà d'ora in poi interessata l'ACN per tutto ciò che concerne gli aggiornamenti, previsti con cadenza almeno annuale, ivi compreso il primo inoltro da parte dei nuovi Soggetti che via via nel tempo verranno inclusi nel Perimetro.

Misure di sicurezza e notifica degli incidenti

Con il DPCM del 14 aprile 2021, n. 81, è richiesto ai Soggetti inclusi nel Perimetro di adottare una serie di misure di sicurezza per i beni ICT identificati. Le misure di sicurezza sono organizzate in due distinte categorie e indicate nell'allegato B dello stesso DPCM. Le misure di sicurezza appartenenti alla

BIO

Gianluca Bocci, laureato in Ingegneria Elettrica presso l'Università La Sapienza di Roma ha conseguito un Master Universitario di 2° livello presso l'università Campus Bio-Medico di Roma in "Homeland Security - Sistemi, metodi e strumenti per la Security e il Crisis Management". Certificato CISM, CISA, Lead Auditor ISO/IEC 27001:2013 e 22301:2012, CSA STAR Auditor e ITIL Foundation v3, ha maturato una pluriennale esperienza nel settore della sicurezza informatica, coordinando iniziative utili a garantire la conformità alle normative vigenti in materia di sicurezza cibernetica e lo sviluppo di programmi di crisis, business continuity e incident management. Precedentemente ha realizzato e coordinato un programma di sicurezza delle applicazioni mobili, anche attraverso attività di ricerca e sviluppo realizzate con il mondo accademico. Presso importanti multinazionali ICT, in qualità di Security Solution Architect, ha supportato le strutture commerciali nell'ingegneria dell'offerta tecnico-economica per Clienti di fascia enterprise, con particolare riferimento ad aspetti di Security Information and Event Management, Security Governance, Compliance e Risk Management.

categoria A, di natura organizzativa\procedurale, devono essere adottate dal Soggetto entro sei mesi dalla prima comunicazione dei beni ICT mentre quelle appartenenti alla categoria B, di natura tecnologica, entro 30 mesi. Il criterio alla base delle diverse tempistiche è fondamentalmente dovuto alla complessità degli interventi necessari all'implementazione delle stesse misure. A prescindere dalla categoria di appartenenza, tutte le misure di sicurezza trovano riscontro nei controlli previsti nel Framework Nazionale per la Cybersecurity e la Data Protection[2] che si ispira al Framework di Cybersecurity del NIST (National Institute of Standards

and Technology). Il Framework Nazionale per la Cybersecurity e la Data Protection, oltre a fornire uno strumento per organizzare i processi di cybersecurity nelle organizzazioni pubbliche e private di qualunque dimensione, introduce con la sua versione 2.0, aggiornata nel 2019, elementi utili per tenere in debito conto le disposizioni del GDPR per la protezione dei dati personali.

Lo stesso DPCM richiede ai Soggetti in Perimetro di notificare allo CSIRT Italia[3], tutti gli incidenti che impattano sui beni ICT identificati. Gli incidenti d'interesse sono quelli indicati nella tassonomia organizzata in due distinte tabelle riportate nell'allegato A del medesimo DPCM; nella tabella 1 sono indicati gli incidenti meno gravi che devono essere notificati entro sei ore, mentre nella tabella due quelli più gravi che devono essere notificati entro un'ora. I predetti termini decorrono dal momento in cui si è venuti a conoscenza, a seguito delle evidenze ottenute, anche mediante le attività di monitoraggio, test e controllo di un incidente riconducibile a una delle tipologie individuate nell'allegato A.

Approvvigionamento di nuovi beni ICT

Con il DPR del 5 febbraio 2021, n. 54 rimangono definite le procedure, le modalità e i termini per consentire le valutazioni da parte del Centro di Valutazione e Certificazione Nazionale[4] (d'ora in avanti **CVCN**) e dei Centri di Valutazione[5] (d'ora in avanti **CV**) sui prodotti in acquisizione da parte dei Soggetti inclusi nel Perimetro e che sono necessari per l'esercizio di una funzione essenziale dello Stato o per la prestazione di un servizio essenziale. Con il DPCM del 15 giugno 2021 è stato invece identificato l'elenco delle categorie e dei beni ICT (V. Fig.2) per i quali i Soggetti dovranno necessariamente applicare le suddette procedure.

Figura 2 - D.P.C..M 15 giugno 2021 - Elenco delle categorie

Secondo quanto previsto dal DPR del 5 febbraio 2021, n. 54, l'approvvigionamento dei beni ICT si articola nelle seguenti fasi (V. Fig. 3):

- verifiche preliminari
- preparazione all'esecuzione dei test
- esecuzione dei test di hardware e di software

La **fase di verifica preliminare** ha inizio con la comunicazione da parte del Soggetto verso il CVCN o il CV di voler procedere con l'acquisto di beni ICT necessari per l'esercizio di una funzione essenziale dello Stato o per la prestazione di un servizio essenziale che appartengono alle categorie individuate nel DPCM del 15 giugno 2021; in tal senso, la comunicazione viene fatta prima che:

- è avviata la procedura di affidamento per la fornitura di beni ICT;
- è concluso un contratto relativo alla fornitura di beni ICT, ove non è prevista la procedura di affidamento;
- oppure la procedura è espletata attraverso una centrale di committenza.

La comunicazione è corredata da una serie di indicazioni che riguardano il bene ICT che s'intende acquisire, come ad esempio: i dati identificativi del Soggetto stesso, la descrizione generale del bene, il suo impiego\ destinazione d'uso, la categoria di appartenenza e la descrizione delle informazioni che deve trattare. In aggiunta, il Soggetto fornisce anche l'analisi del rischio associata al bene ICT, anche in relazione all'ambito operativo di impiego.

Dalla data di comunicazione, entro quarantacinque giorni[6], Il CVCN o il CV avvia e completa il procedimento di verifica e valutazione del bene ICT attraverso l'analisi della documentazione ricevuta e la predisposizione di un provvedimento con il quale definisce le eventuali condizioni e test di hardware e di software che intende svolgere sui beni oggetto di acquisizione. Condizioni e test che, insieme alle eventuali prescrizioni per l'utilizzo del bene, dovranno essere recepite dal Soggetto per essere integrate nel bando di gara o del contratto.

Decorsi i termini indicati senza che il CVCN o il CV si sia pronunciato, il Soggetto può proseguire nella procedura di affidamento, svincolandosi di fatto dagli ulteriori obblighi previsti dalla specifica norma e di seguito richiamati.

Successivamente all'aggiudicazione della gara o della stipula del contratto, per procedere con la **preparazione all'esecuzione dei test**, il Soggetto provvede a comunicare al CVCN o al CV i riferimenti del fornitore e ogni elemento utile ad individuare in modo univoco l'oggetto della fornitura, così che possa essere verificato se, quanto acquisito, è stato già sottoposto

a precedenti valutazioni o lo sia in quel momento per altre procedure di affidamento in corso. Una verifica il cui esito è pertanto fondamentale per stabilire se è necessario o meno proseguire con l'esecuzione dei test.

Nello caso in cui si dovesse procedere con i test, il Soggetto, insieme al fornitore, dovrebbero svolgere tutte quelle attività propedeutiche e indispensabili per la loro esecuzione, ad es. provvedere all'allestimento di un ambiente di test adeguatamente rappresentativo della realtà di esercizio, fornire una descrizione generale dell'architettura dell'oggetto di valutazione e delle sue funzioni, fornire una descrizione delle funzionalità di sicurezza implementate nell'oggetto di valutazione, fornire una descrizione dei test funzionali e di sicurezza già eseguiti dal fornitore o dal produttore o da una parte terza, comprensivi dei relativi risultati.

Completate dunque le attività propedeutiche e Comunicata la disponibilità all'**esecuzione dei test**, il CVCN o il CV entro sessanta giorni concludono le prove, inviando al Soggetto e al fornitore il c.d. rapporto di valutazione contenente l'esito della valutazione. Qualora l'esito della valutazione fosse positivo, il Soggetto, recepite le eventuali prescrizioni di utilizzo del bene acquisito, finalizza l'approvvigionamento con l'esecuzione del contratto. Viceversa, l'esito della valutazione fosse negativo, il Soggetto sarebbe obbligato a sospendere o risolvere il contratto. Anche in questo caso, qualora il CVCN o il CV non si pronunciasse entro i termini stabiliti, il Soggetto sarebbe libero di procedere con l'esecuzione del contratto.

Per l'esecuzione dei test entrano in gioco anche i c.d. Laboratori Accreditati di Prova (d'ora in avanti **LAP**) che, ottenuto l'accreditamento dal CVCN, per specifico mandato lo possono sostituire nelle prove di laboratorio. I LAP costituiscono un network con il quale il CVCN di fatto estende la sua capacità di rispondere alle esigenze di approvvigionamento dei Soggetti secondo determinate e specifiche regole. La rete è costituita con l'ausilio di aziende private e le possibilità offerte dai finanziamenti previsti nell'ambito del Piano Nazionale di Ripresa e Resilienza; le aziende ricomprendono ampi settori della tecnologia dal momento che le valutazioni si muovono su più direttrici, le principali quelle che riguardano il software ma anche l'hardware secondo molteplici declinazioni.

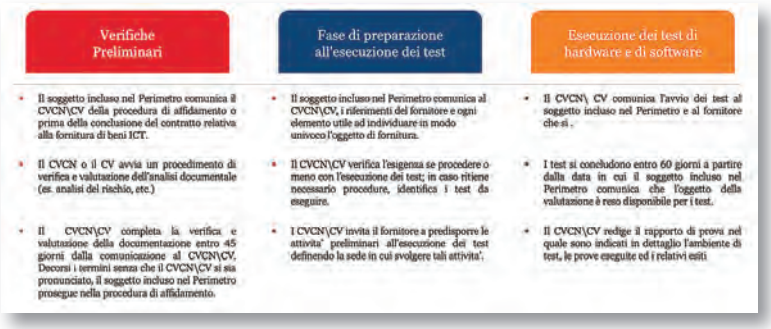


Figura 3 - Richiami alle principali attività previste dal DPR 05\02\21, n°54

Conclusioni

Il DPR del 5 febbraio 2021, n. 54 avrà dunque un impatto non trascurabile sui processi aziendali, in particolare quelli che disciplinano l'acquisto di componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione e per il trattamento dei dati, funzionalità per garantire la sicurezza dei dati stessi ma anche per la supervisione e il controllo, l'attuazione e l'automazione dei sistemi industriali e infrastrutturali.

Tra gli impatti principali non vi è dubbio per quel che riguarda la dilatazione dei tempi di acquisito di determinati beni ICT. Abbiamo accennato ai tempi di attesa per le verifiche preliminari e per l'eventuale esecuzione dei test, tempi che possono anche allungarsi in particolari condizioni; ad esempio, per la verifica preliminare, i quarantacinque giorni possono essere prorogati, se pur una sola volta, di ulteriori quindici giorni, qualora l'oggetto della fornitura è costituito da beni, sistemi e servizi ICT integrati tra di loro, oppure è basato su tecnologie di recente sviluppo per le quali non si dispone di metodologie di test consolidate, oppure interagisce con componenti che erogano altre funzioni essenziali o servizi essenziali. Ne consegue che, nell'ambito della programmazione delle iniziative progettuali, a partire dalla pianificazione dei budget fino alla predisposizione dei bandi di gara e dunque all'esecuzione dei contratti, non si potrà non tener conto di questa nuova variabile. Tra gli impatti, rilevante è anche quello degli oneri economici che dovranno essere sostenuti da tutti gli attori coinvolti nell'applicazione della nuova disciplina.

Si evince in generale, come l'articolazione del Perimetro, nella sua interezza, imponga per buon senso, che i Soggetti si dotino di un'organizzazione e di regole per garantire che i molteplici adempimenti, dunque non solo quelli in materia di approvvigionamenti, siano opportunamente indirizzati e nel pieno rispetto delle tempistiche imposte. In tal senso sarà necessario predisporre linee guida e procedure per individuare processi, attività, ruoli e responsabilità che concorrono al raggiungimento degli obiettivi previsti dal Perimetro ma anche ottenere, ancora una volta, in quanto determinante, il *"commitment del top management"* per favorire un ambiente adatto e collaborativo allo svolgimento delle tante e diverse attività. ■

1 Tecnologie critiche di cui all'articolo 4, paragrafo 1, lettera b), del Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio del 19 marzo 2019.
2 https://www.cybersecurityframework.it/framework2
3 https://csirt.gov.it/segnalazione
4 istituito presso il Ministero dello sviluppo economico e di prossimo trasferimento presso l'ACN
5 istituiti presso il Ministero degli Interni e il Ministero della Difesa
6 Il termine dei quarantacinque giorni è prorogabile una sola volta di quindici giorni nei casi di particolare complessità identificati nell'art. 4, comma 6 del DPR del 5 febbraio 2021, n. 54.

Riccardo Meggiato
La scienza del crimine
Ed. Hoepli

Le tracce in rete hanno più peso di quelle biologiche e fisiche Gli investigatori devono tenerne conto

Con quaranta libri realizzati e più di trecentomila copie vendute, Riccardo Meggiato, perito forense e consulente Tecnico di Parte è un esperto di successo. La scienza del crimine, suo ultimo scritto è destinata ad accendere la curiosità di un vasto pubblico. Si tratta di un viaggio alla scoperta delle scienze forensi che parte dall'omicidio più enigmatico e più famoso della storia: quello di Giulio Cesare per arrivare ai giorni nostri. Anche se è cambiato lo scenario investigativo popolato da sofisticati strumenti tecnologici, adoperati da investigatori perennemente oscillanti tra il reale e il virtuale, rimane l'enigma, e quel velo di incertezza che spinge gli inquirenti di ogni epoca a ricercare la verità oltre ogni ragionevole dubbio.

Le scienze forensi accendono l'immaginario collettivo e fanno irruzione nella quotidianità, basti pensare alla letteratura e alla filmografia sull'argomento. Meggiato, come nasce questo lavoro?

C'è una storia curiosa dietro alla genesi de "La scienza del crimine". Sono un analista forense in ambito digitale, sono sovente chiamato a prendere visione diretta della "scena del crimine" e quando questo non avviene ho comunque accesso alla documentazione relativa ai casi di cui mi occupo. La formazione scientifica di cui mi avvalgo, unita a una discreta capacità divulgativa, che mi permette di spiegare concetti complessi in modo facile, spinge avvocati, agenti e professionisti a chiedermi spesso chiarimenti, in merito a svariati reperti e metodologie, al fine di chiarire i dubbi che emergono in sede investigativa. Mi sono accorto che il corpus delle risposte era talmente ricco da poterne fare un libro, non mi pare, infatti, che ci sia niente di simile nel panorama editoriale attuale.

Quali sono i principali target di riferimento?

Il pubblico di riferimento è molto ampio. Dai semplici curiosi, appassionati di serie TV e romanzi crime, a giornalisti, scrittori che vogliono aggiungere elementi scientifici ai loro lavori, ma anche chi ha bisogno di uno strumento veloce e divertente per apprendere le principali tecniche e procedure delle scienze forensi.

"Per avere a che fare con il crimine servono regole e metodo". Ha fondato un'agenzia di cyber security. Quanto ha contato l'esperienza sul fronte "virtuale" nella elaborazione e scrittura di questo saggio?

È stato prezioso tutto il bagaglio di know-how accumulato in questi anni. Il lavoro sviluppato nell'ambito della cyber-security e dell'informatica forense educa alla precisione e all'attenzione nel cogliere ogni dettaglio, ogni sfumatura, che si tratti dell'analisi di file di log o dell'esame di un codice malevolo. Per altro quando occorre interfacciarsi con clienti che dell'argomento sanno poco o nulla, o anche nel caso in cui bisogna esporre delle evidenze di fronte a una Corte, ci si allena a utilizzare un linguaggio comprensibile, alla portata. La chiarezza, ricordiamolo, rimane un valore importante, soprattutto quando si toccano versanti così delicati.

Il cyber crimine invade le pagine dei quotidiani. Veloci, spregiudicati, competenti, gli hacker mettono sotto scacco aziende e istituzioni. Le "tracce in rete" hanno lo stesso peso di quelle di cui "parla" Andreotti nella citazione che apre il volume?

Anche se in genere mi piace dare opinioni poco allineate, di fronte all'evidenza di attacchi sempre più complessi non si può che confermare l'opinione prevalente che sottolinea l'escalation del fenomeno a tutte le latitudini. Quello che è più difficile percepire, specie da chi non è addentro al settore, è che la sofisticazione degli attacchi aumenta in modo esponenziale, mentre la capacità di prevenirli e mitigarli cresce in modo più lineare. Per questa ragione il gap appare in costante aumento. Se consideriamo questo aspetto possiamo comprendere perché le tracce in rete, hanno un peso ancora più importante di quelle biologiche, o comunque fisiche. Credo che un progetto valido di sicurezza dovrebbe tenerne conto, soprattutto in rapporto alle attività di *assessment e threat intelligence* determinanti per il nostro settore, rispetto a cui non ci spendiamo mai abbastanza

Le tecnologie stanno cambiando la lettura della scena del crimine. Quali competenze bisogna mettere in campo?

Mi rifaccio in maniera sintetica a un aneddoto che può essere molto utile per rispondere alla sua sollecitazione. Tempo addietro, in un procedimento giudiziario importante, nel quale figuravo come consulente tecnico di parte, produssi l'analisi di un determinato file. Nelle contro-deduzione, la controparte questionò sull'incomprensibilità delle informazioni che avevo prodotto. E sa cosa stavano contestando? Del codice esadecimale, perché il loro consulente non sapeva di che si trattasse. Quindi, da una parte, oggi, abbiamo di certo il problema di riuscire a scremare enormi quantità di dati, e l'apprendimento di linguaggi come Python o R è prezioso, ma dall'altra vedo che mancano competenze per poi procedere nell'analisi verticale del dato. Si tratta di mancanze gravi, se pensiamo che buona parte degli sviluppatori di malware utilizza

il linguaggio C e assembly per realizzare i propri *tool*, e che questi *malware*, poi, li troviamo alla base del 90% dei casi di truffa sui quali lavoriamo.

Da questo ragionamento dobbiamo trarre che sono sufficienti poche competenze e relativamente di basso livello per poter gestire eventi complessi nell'ambito della cyber-security e dell'informatica forense?

Certamente no, ma che occorre partire da queste competenze, per poi apprendere tutto il resto e tutto ciò che di nuovo c'è da imparare. È un lavoro di una complessità inimmaginabile e credo che buona parte di questa complessità derivi dalla necessità di rimanere sempre aggiornati. Questo è il motivo per cui, dedico due ore al giorno allo studio: libri, paper scientifici, sono il mio *"pane quotidiano"*.

Polizia, carabinieri, ingegneri informatici dovranno sempre di più lavorare in team pluridisciplinari. Siamo pronti a praticare una logica collaborativa?

Ammetto che le cose sono migliorate moltissimo, da quando nella metà degli anni novanta ho iniziato a lavorare in questo settore. Sia perché certe professionalità non sono più viste come figure "strane" e perciò da isolare, sia perché anche chi non conosce per nulla l'argomento, sta cominciando a "masticare" alcuni concetti base e la nomenclatura essenziale. Un plauso particolare credo, comunque, che lo meritino le Forze dell'Ordine, che stanno lavorano moltissimo nella formazione su questi argomenti.

Minacce reali e minacce virtuali. Quali scenari si aprono per il futuro e quali strategie di contrasto vanno attuate?

Con il conflitto tra Russia e Ucraina abbiamo avuto modo di toccare con mano, come forse mai era avvenuto, i risvolti che una minaccia virtuale può apportare nel mondo reale e viceversa. Mentre discutiamo la Russia sta predisponendo la disconnessione all'Internet globale. Lo fa per massimizzare la propria propaganda interna, ed evitare influenze esterne sulla popolazione, ma anche per sfatare possibili attacchi digitali. Per questo motivo, credo che ci sia da compiere uno sforzo in termini di consapevolezza generale che faccia comprendere l'assoluta continuità che ormai si è venuta a creare tra mondo fisico e universo virtuale. Occorre fare capire, per intenderci, che quando si parla di un "attacco informatico" non bisogna necessariamente pensare ai computer degli uffici, piuttosto bisogna preoccuparsi dei sistemi elettronici che comandano il funzionamento delle casse in un ospedale, dei servizi di autenticazione agli account bancari, dei sistemi domotici di casa che regolano antifurti, tapparelle e termostati; delle industrie manifatturiere, del traffico aereo e via così lungo una catena di implicazioni molto ampia.

Il salto di prospettiva che Lei invoca non è da poco. Quanto tempo servirà?

Difficile dirlo. Proveniamo da secoli di civiltà analogica, passare a una concettualizzazione digitale del mondo non può essere immediato. Quando mi capita di insegnare nelle aziende e nelle università, più che puntare alle procedure, parto sempre con esempi che nulla, in apparenza, hanno a che fare con il pc. Spiego poi agli allievi come si è arrivati a quell'attacco. Le loro facce la dicono lunga, quando scoprono che si trattava di un attacco di matrice informatica.

Ritengo che finché perdurerà tanto sbigottimento, i problemi da risolvere non mancheranno.

Da Giulio Cesare a oggi anche se sono passati davvero tanti secoli, individuare movente e colpevole rimane un enigma per qualsiasi investigatore. Il connubio tra le "tracce" e i "soggetti" apre un campo di possibilità difficile da presidiare. Il fascino legato alla conduzione delle indagini sta tutto in questa irriducibile incertezza, che rende sempre sfuggente l'identità del criminale "reale" o "virtuale" che sia?

Credo proprio di sì. Tale considerazione vale anche per i professionisti che lavorano con me. È l'incertezza la leva che mi spinge a non cedere di un millimetro, a non lasciare mai nulla di intentato, a perseguire la verità fino a raggiungerla. La sfida è quella che ci porta a ricostruire un caso fino ad arrivare alla sua origine. L'uomo vive di istinti primari ed elementari. Per analogia possiamo dire che la stessa eccitazione la provavamo da bambini quando giocavamo a guardia e ladri, anche se siamo ormai passati dal mondo analogico a quello digitale. Si tratta mi rendo conto di un modo elegante per dire che il tempo passa inesorabilmente. D'altra parte, l'immutabilità del divenire, come ci ha insegnato Eraclito, non è una componente essenziale della partita che stiamo giocando? Perché allora stupirsi? ■

Michael Grothaus
Trust No One. Inside the World of Deepfakes.
Londra (Hodder & Stoughton), 2021, 279 p.

Autore: Laurent Chrzanovski

In un mondo pieno di *"informazioni"*, i metodi utilizzati per catturare l'attenzione dei lettori digitali, che spesso accedono alle notizie attraverso il minuscolo schermo del loro smartphone, consistono nella combinazione di un'immagine-choc seguita da un titolo volontariamente esagerato. La maggior parte delle persone, passando da una "notizia" all'altra, si limiterà a tenere a mente questa associazione binaria.

Bibliografia - Cybersecurity Trends

Nel mondo digitale, la chiave del successo di un'"info" è semplice: più accattivante è l'immagine e più emotivamente provocatorio è il titolo, più grande sarà l'audience; peggio: non importa se il testo dell'articolo stesso è molto più equilibrato, perché ben pochi vanno oltre il trinomio immagine-titolo-riassunto/sottotitolo.

In questo contesto, spicca ormai l'uso del deepfaking delle immagini, una tecnica che si è evoluta drammaticamente nell'ultima decade – benché sia nata quasi in contemporanea con la fotografia per diventare poi una costante nella propaganda pubblicata da alcuni regimi: possiamo ricordare ad esempio la stampa sovietica, che rimosse tempestivamente dalle immagini ufficiali tutti i primi comunisti giustiziati per ordine di Stalin.

L'autore del saggio si è reso conto dell'importanza e della qualità raggiunta oggi dai deepfaker quando ha chiesto a un amico di *"ridare vita"* a suo padre, deceduto nel 1998, realizzando un clip *"come se fosse stato girato oggi"*. Questo suo 'sogno' è stato realizzato usando come base vecchi video VHS, che una volta digitalizzati sono stati inseriti in alcuni tool di intelligenza artificiale estremamente sofisticati. Il risultato è stato più che sorprendente, visto che anche la qualità del videoclip era in altissima definizione, nettamente superiore a quella della fonte originale.

Come giornalista, Michael Grothaus ha quindi deciso di indagare il fenomeno ed ha intervistato numerosi specialisti che utilizzano gli ultimi strumenti disponibili per creare immagini e videoclip "artificiali", che includono anche la voce originale di ogni personaggio. Ma la parte più interessante del libro, da leggere come un romanzo dark, è il ruolo sempre più grande assunto dai deepfake all'interno del numero di immagini a cui tutti accedono quotidianamente in rete. La narrazione perfetta, lo stile dell'autore e la sequenza logica dei capitoli hanno reso questo volume un best-seller, apprezzato persino da alcuni dei quotidiani più importanti del mondo anglosassone (1) (2).

La scoperta più importante è che secondo la maggioranza degli specialisti è ormai finita l'era dei deepfake usati per modellare le opinioni. In altre parole, oggigiorno i deepfake sono sempre meno usati per cercare di distruggere la reputazione di un CEO o nel tentativo di influenzare un'elezione (quindi parte delle psy-ops). Su questo argomento, la straordinaria campagna fatta da RepresentUS per mettere in guardia gli americani sui deepfake, utilizzando le dichiarazioni trasmesse create al 100% dall'AI del presidente russo Putin e del leader nord-coreano Kim Jong-Un, ha avuto un effetto formidabile sull'aumento della consapevolezza dei cittadini (3).

Non c'è da essere soddisfatti, perché come sottolinea l'autore, viviamo ormai in un mondo molto più perverso, dove i deepfake sono comunemente usati non per cambiare la mente delle persone, come Grothaus esplicita, ma *"di nutrirle con quello che vogliono [vedere]"*. I deepfake sono quindi molto spesso mirati a soddisfare il narcisismo, il (vano) tentativo di perdere qualsiasi paura della morte, ma anche a indurre il sentimento di una sessualità soddisfatta o di un autocontrollo perfettamente padroneggiato. Questo può rendere il mondo digitale sconnesso da qualsiasi realtà a tal punto che i nostri innati sensi di ricerca del fatto, della verità e della fiducia da accordare o no agli altri potrebbero essere seriamente minati, generando effetti a dir poco disastrosi in tutti gli aspetti della nostra vita quotidiana e sulle nostre interazioni sociali. ■

(1) Peter Pomerantsev, Trust No One: Inside the World of Deepfakes di Michael Grothaus recensione - la superarma della disinformazione, The Guardian, 16.12.2021
https://www.theguardian.com/books/2021/dec/16/trust-no-one-inside-the-world-of-deepfakes-by-michael-grothaus-review-disinformations-superweapon
(2) Shanti Das, recensione di Trust No One di Michael Grothaus - uno sguardo allarmante ai deepfakes, The Times, 07.11.2021
https://www.thetimes.co.uk/article/trust-no-one-by-michael-grothaus-review-an-alarming-look-at-deepfakes-q233pldf6
(3) Karen Hao, Deepfake Putin è qui per avvertire gli americani del loro destino autoinflitto, Harvard Technology Review 29.09.2020
https://www.technologyreview.com/2020/09/29/1009098/ai-deepfake-putin-kim-jong-un-us-election/

La *compliance integrata* per l'attuazione del Modello 231
Mirjana Petrovich
Lucio Gioacchino Insinga
Fabrizio Rossi
Ed. Primiceri

La *compliance integrata* nel capitalismo di "comunità"

Autore: Massimiliano Cannata

Si viene presi da un senso di positiva armonia dopo la lettura di questo importante lavoro di approfondimento sul Modello 231, che colloca la realtà aziendale nella più vasta cornice di una responsabilità sociale e verrebbe da aggiungere "civile" che gli imprenditori e i manager devono avvertire in una fase drammatica come quella che l'intero pianeta sta vivendo.

Lo studio di **Mirjana Petrovic, *Lucio Gioachino Insinga,* e Fabrizio Rossi** va oltre la connotazione di un manuale d'uso,

perché rimette molte cose al loro posto, operazione non semplice in questa fase di cambiamento d'epoca. Il messaggio che gli autori lanciano, non solo al pubblico o agli addetti ai lavori ma al target più ampio del corpo collettivo interessato a sapere qualcosa in più sul futuro che ci attende, è molto chiaro: nella "società delle catastrofi", attraversata da continue emergenze, per reggere l'impatto della tempesta perfetta, che oggi si è materializzata nella pandemia, ma che domani potrà assumere altre imprevedibili sembianze, bisognerà puntare sulla competenza e sulla capacità di leadership se vogliamo uscire dal lungo tunnel fatto di declino e di paura entro cui siamo piombati.

Parlare del D.lgs. 231 che ha determinato delle profonde trasformazioni strutturali e tecnico organizzative per milioni di imprese, vuol dire sottolineare l'importanza della responsabilità come valore precipuo dell'impresa. Responsabilità è un termine critico, difficile da maneggiare che ci riconduce nell'alveo del dualismo classico tra *nomos* ed ethos, tra Creonte e Antigone, tra l'imperio della legge che definisce il campo della liceità e la dimensione del dover essere, che mette in campo l'individuo. Sono almeno tre i livelli di analisi, che si possono utilizzare per scandagliare il corpo di questa interessante e ben documentato volume:

- *giuridico* se ci si sofferma sulle parti dedicate allo sviluppo e all'inquadramento normativo;
- *filosofico*, apprezzabile nella capacità di lettura critica del presente, dote che appare molto spiccata nei tre autori;
- *strategico*, appare infatti evidente, che non è in gioco solo l'adempimento della norma, ma l'indirizzo più complessivo che imprese grandi e piccole, dovranno imboccare nella dinamica della competizione, che si gioca su scala globale.

Il *case History* cui è dedicata la parte conclusiva del libro, che racconta l'esperienza della Diddi Dino & Figli S.r.l afferma un principio, 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 l'etica che deve tornare a fare da riferimento. 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 e di prevenzione dei reati, deve tendere a includere il corpus dell'azienda in tutte le sue componenti.

Va detto che questa visione, che comincia a maturare in alcuni scritti precedenti di Lucio Insinga (basti in questa sede ricordare: *Come finanziare* l'impresa, pubblicato dallo stesso Primiceri e *La responsabilità sociale, Ed. Plenum*) rientra in un filone di ricerca che fa vedere molto bene come 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 complesso, abilità che l'imprenditore deve imparare ad affinare, perché da essa dipende ogni *chances* di successo. Solo se collocata in quest'ottica trasversale la norma giuridica può contribuire a 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.

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, che emerge come uno degli aspetti centrali della trattazione, lascia presagire l'affermazione di 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",* come sostiene Roberto Panzarani, docente di governo dell'innovazione tecnologica dell'Università Cattolica di Roma, tra i massimi esperti di fenomenologia del cambiamento nelle organizzazioni complesse, in un interessante saggio: *"Il nuovo paradigma (ed. Lupetti)*. ■

Italiadecide Rapporto 2021 Ed. Il Mulino

Fiducia sostenibile e collaborazione istituzionale per avviare la ripresa

Autore: Massimiliano Cannata

"Fiducia sostenibile": due termini per inquadrare l'obiettivo cui dobbiamo tendere per imboccare la strada della ripresa. Lo sostiene il Rapporto 2021 di *Italiadecide: "Una fiducia sostenibile.*

La collaborazione tra pubblico e privato per la transizione ecologica". (ed. Il Mulino). Dalla diffidenza che ha storicamente segnato le relazioni tra il pubblico e il privato, alla collaborazione che si impone nel contesto del rinnovato slancio di un'Europa intenzionata a superare la drammatica pagina della pandemia, il cambio di indirizzo presenta le sembianze di una svolta epocale.

La transizione ambientale, individuata priorità di questa delicata fase, si concretizza nella definizione di una strategia ecologica globale che presuppone un disegno trasversale, aperto a tutti i livelli di governo. Per la PA si apre dunque una nuova stagione fondata sulla cultura del confronto e dell'ascolto senza di cui risulterà impossibile progettare e attuare politiche efficaci. Le criticità nelle relazioni tra i diversi poteri dello Stato esistono, come evidenziato con puntualità nello studio, la sfida consiste nel superare vecchie gelosie di ruolo e funzione, legati ai rapporti gerarchici che hanno dimostrato di non reggere alla prova della storia. "L'alternativa – commenta la Presidente di *Italiadecide* Anna Finocchiaro - non si gioca tra riforma e conflitto, non abbiamo più tempo né per l'una, né per l'altro, ma sull'affermazione di una diversa cultura istituzionale, che deve esercitare con metodo e pazienza le possibilità della cooperazione e della collaborazione fiduciaria tra diversi poteri in vista dell'interesse generale". Una vera e propria rivoluzione copernicana quella prospettata: se, infatti, le istituzioni imparano a "fare rete", liberate dal cappio della burocrazia, avranno maggiori possibilità di reggere l'urto delle continue emergenze da cui è attraversata la "società delle catastrofi". Lo stiamo vedendo in queste settimane in cui il virus ha ripreso a correre: perché la tempesta perfetta non abbia il sopravvento, appare indispensabile la collaborazione tra i soggetti pubblici, rappresentati dai livelli regionali e di governo delle città e i soggetti privati, comunità, cittadini, imprese, solo uno sforzo corale potrà trainarci fuori dalla crisi. Questo capovolgimento di prospettiva comporta l'affermazione di un modello "condiviso" di amministrazione pubblica non più centrata sul binomio tradizionale di comando e controllo. Sulla comunità dei saperi dovremo cominciare a "ricostruire" il Paese post pandemia. La sfida ambientale apre spazi inediti di coinvolgimento che potranno dare respiro alle nostre città, che hanno vissuto un secondo Capodanno senza "luminarie", prigioniere della paura. Riempire questi spazi di idee, progetti, ma soprattutto di nuove leadership capaci di rivitalizzare la politica facendola uscire dalla sterilità di vecchie ritualità è l'augurio migliore che possiamo farci per un 2022 che vorremmo contrassegnato da una rinnovata fiducia per i valori di un'Italia democratica. ■

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.cybersecuritytrends.ro

www.swissacademy.eu

www.cybertrends.it

EUCACS
EUROPEAN CENTER FOR ADVANCED CYBER SECURITY

inthecyber
intelligence & defense advisors

Net Consulting³
Empowering your Digital Business

BAROMETRO CYBERSECURITY

SPECIALE CLOUD SECURITY

GESTIONE DI GOVERNANCE E SICUREZZA NELLA MIGRAZIONE AL CLOUD

Con il supporto di:

accenture · cisco · Capgemini · RSA · TIM Google Cloud · TINEXTA CYBER

CERT STAR

Competizione Blue Team

7 aprile 2022
#savethedate

info@cybertrends.it

Cybersecurity Trends