Cybersecurity Trends

Edizione italiana, N. 1 / 2021

INTERVISTE VIP:

BORIS LA CORTE
FLAVIO VENTURINI
ARTURO DI CORINTO

Folder Centrale:
Rischi e pericoli delle supply chains

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

2	**Editoriale: Quando le nuvole bruciano.** Autore: Nicola Sotira
3	**Privacy, libertà e neurodiritti nell'information society. Intervista VIP con Boris La Corte.** Autore: Massimiliano Cannata
7	**La cyber security, disciplina in divenire che segna il cambiamento d'epoca che stiamo vivendo. A colloquio con Flavio Venturini.** Autore: Massimiliano Cannata
12	**Perché la pandemia ci ha dato una nuova prospettiva della cyber security.** Autore: Oliver Friedrichs
16	**Difendersi da malintenzionati esterni, interni e da criminali informatici.** Autore: Shawn Henry
19	**La sicurezza come valore condiviso. A colloquio con Arturo di Corinto.** Autore: Massimiliano Cannata
22	**Rischi Informatici delle Terze Parti, come gestirli.** Autore: Lisa Ventura
25	**Gli impatti dei recenti interventi normativi.** Autore: Maria Cristina Daga
31	**Monitoraggio efficace delle terze parti. Modalità e Tecniche per verificare la resilienza dei fornitori.** Autori: Paolo Carcano e Lorenzo Ramaccioni
37	**Il monitoraggio della propria catena di approvvigionamento.** Autore: Massimo Cappelli
40	**Bibliografia, a cura di Massimilano Cannata:** - Francesco Dall'Olio, Luciano Hinna, Mauro Marcantoni, Il Pentagramma del Diavolo - Roger Abravanel, Aristocrazia 2.0 - Antonio Calabrò, Oltre la fragilità

Quando le nuvole bruciano

Autore: Nicola Sotira

"Abbiamo un grave incidente su SBG2. Incendio dichiarato nell'edificio. I vigili del fuoco sono all'opera ma non hanno potuto controllare l'incendio in SBG2. L'intero sito è stato isolato, il che influisce su tutti i servizi in SGB1-4. Ti consigliamo di attivare il tuo piano di ripristino di emergenza." Ore 3.42 am, così il tweet del fondatore di OVH, Octave Klaba, annunciava il disastroso incendio nel datacenter di Strasburgo facendo fare un brusco risveglio a tutti quelli che pensavano che i dati nel Cloud fossero al sicuro e disponibili sempre, in una sorta di eternità digitale. L'incidente ha messo in luce diversi aspetti, la progettazione, il ripristino dei dati e il prezzo che siamo disposti a pagare per la tutela dei nostri dati. In casi come questi, infatti, è fondamentale avere sistemi di backup funzionanti insieme a procedure testate e consolidate di ripristino. Inoltre, alcuni clienti potevano avere servizi ulteriori, con riguardo a queste tematiche, occorreva ovviamente leggere bene la contrattualistica e attivare le sottoscrizioni a piani che avrebbero dato più garanzie in caso di problematiche di questa natura. Dovrebbe poi farci riflettere il fatto che tra le società che hanno dichiarato di essere impattate dall'incidente una di queste si occupa di crittografia e diverse operano nel settore del trading in Bitcoin. Il tema della resilienza e della continuità operativa diventa oggi per le aziende sempre più rilevante in un mondo dove le aspettative dei clienti sono sempre maggiori oltre alle nuove e stringenti richieste delle autorità di regolamentazione. In questo anno di pandemia fatto di chiusure e contagi che hanno intaccato anche la capacità produttiva, tutte le aziende hanno realizzato che il miglioramento della resilienza aziendale è fondamentale per rimanere competitivi, per poter mantenere la fiducia del mercato e, non ultimo, sostenere la stabilità finanziaria.

Una visione della resilienza più orientata ai servizi critici che orientata ai singoli sistemi e/o applicazioni, considerando anche le interconnessioni con gli altri attori del mercato. Su questa tematica occorre implementare il concetto di end-to-end, ovvero mappare le risorse critiche tra le persone, i processi, i dati, le strutture e oltre all'ecosistema interno occorre comprendere e includere anche le terze parti critiche.

Globalizzazione e connettività diffusa stanno rendendo le catene di approvvigionamento più complesse e amplificano l'impatto di qualsiasi problema, senza contare la continua spinta al miglioramento dell'efficienza e la riduzione dei costi operativi.

In questo contesto non c'è quindi da stupirsi se quegli eventi "cigno nero", oggi sembrano quasi regolari. Questo non significa automaticamente un incremento nella frequenza, ma sottolinea come, in un ambiente interconnesso a livello globale, problemi che un tempo restavano isolati oggi hanno ripercussioni su larga scala.

Le organizzazioni devono cimentarsi con questa nuova sfida che deve rivedere il concetto di rischio sulla catena di approvvigionamento e gestirne l'esposizione in modo da proteggere il valore del proprio business e la loro reputazione. ■

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.

Privacy, libertà e neurodiritti nell'information society

Intervista VIP con Boris La Corte.

Autore: Massimiliano Cannata

"Privacy e neurodiritti: La persona al tempo delle neuroscienze". Il tema della giornata europea della protezione dei dati personali ha aperto il sipario sulla sfera che possiamo considerare più avanzata della ricerca giuridica ed epistemologica.

La "nostra vita si fa dati, prima di farsi storia", fin dal primo vagito siamo registrati da un codice, da quel momento scatta un controllo silenzioso, che sulla spinta della rivoluzione digitale, si è fatto sempre più invasivo. "Sono passati quarant'anni – ha ricordato il giurista Pasquale Stanzione, Presidente dell'Autorità Garante dei dati personali - dalla Convenzione di Strasburgo, primo passo di una consapevolezza che attraverso le tappe importanti del GDPR e della definizione del Codice della Privacy hanno portato l'Europa alla definizione del Digital Service Act".

Abbiamo chiesto a Boris La Corte, Presidente dell'Associazione "Articolo 80, libertà e diritti nella vita digitale", *Privacy specialist* di SNFIA (il Sindacato delle Alte Professionalità del Settore Assicurativo) di gettare lo sguardo sulla nuova generazione dei diritti che stanno segnando lo sviluppo del digitale.

***Dott. La Corte la nostra vita è tracciata dai dati. Quali sono le tipologie di rischio connaturate all'espansione* dell'information society?**

Una buona parte dei reati in rete è una versione evoluta di fattispecie criminose già presenti nella realtà. Un esempio per tutti: il furto d'identità non è certo nato con Internet. Resto del parere che il peggior rischio, che riguarda tutte le fasce di età di utenti, sia quello dell'immaturità e

BIO

Boris La Corte è nato a Palermo il 18 aprile del 1969. Nel 1995 ha conseguito la laurea in Scienze Politiche con la votazione di 110/110 e lode, discutendo una tesi di diritto regionale ed un abstract sul federalismo. Funzionario di un primario gruppo assicurativo italiano per il quale si occupa di analisi dati sui sinistri stradali e tematiche privacy sui temi di antifrode e dispositivi black box. Privacy specialist di SNFIA (Sindacato nazionale delle alte professionalità del settore assicurativo. Milano), DPO certificato UNI 11697:2017, è attivo nella consulenza e nella formazione privacy e data protection. Coordinatore del Gruppo Aziendale Privacy del Policlinico di Palermo nonché docente ai corsi di formazione privacy dedicati ai ruoli amministrativi e sanitari dell'Azienda. Relatore al web meeting SNFIA "L'evoluzione del lavoro ai tempi del COVID-19" (2020). Relatore al corso di laurea magistrale in Tourism systems and hospitality management dell'Università di Palermo, sul tema: "Strutture ricettive ed ospitalità turistica: alto rischio di violazione GDPRD nel trattamento dei dati personali" (2019). Ha pubblicato "Data protection e ospitalità turistica" edito da Leima editore, Palermo 2019. Presidente dell'Associazione "Articolo 80. Libertà e diritti nella vita digitale" (www.articolo80.eu)

dell'incoscienza. Nella moderna, collettiva, sbornia sui servizi dichiarati "gratuiti" si è perso il senso della prudenza e dell'attenzione.

Se vogliamo vivere liberi, rispetto alla schiavitù del condizionamento, dobbiamo rafforzare le nostre conoscenze, che sono l'unico antidoto efficace che potrà proteggerci rispetto alle trame oscure di un "marketing inquinante".

Il video curato dall'Authority e diffuso su tutti i canali di comunicazione ha un titolo che suona come un alert: "i tuoi dati sono un tesoro". Non pensa che questo tesoro sia troppo esposto agli assalti del cyber crimine?

Molti comportamenti collettivi dimostrano una pericolosa superficialità, a cominciare dal diffuso desiderio di aderire ai servizi di posta elettronica gratuita. Registrare il proprio dominio, che può ospitare più indirizzi di posta costa meno di dieci euro l'anno. Questo "domicilio informatico" dovrebbe essere tenuto al riparo dalle multinazionali, che vogliono leggere e conservare la nostra corrispondenza, che contiene spesso informazioni sensibili. Abbiamo idea di quante ricette o prescrizioni mediche, vengono quotidianamente condivise fra medici e pazienti, attraverso i servizi di posta elettronica "gratuiti"? Stesso ragionamento vale per il cloud. Come è noto "la nuvola" conserva materiale personale e professionale, conservati in un hard disk esterno. Insomma, chiedersi perché aziende quali Microsoft e Google prevedano il salvataggio di default dei nostri documenti nel loro *cloud* chiamato "One Drive" non sarebbe sbagliato, al fine di alzare la soglia dell'attenzione. Se si considerano i costi che vengono affrontati dagli operatori per la gestione di questa gigantesca mole di dati, ci si rende conto del vantaggio competitivo che acquisiscono questi player per studiare, spiare e misurare tutti i nostri spazi di vita, e per affinare l'apprendimento automatico delle loro macchine (il c.d. machine learning) che di fatto sfrutta il vissuto degli utenti.

Una nuova età dei diritti

In occasione della giornata europea della privacy, ascoltando il parere degli esperti intervenuti non ha nascosto un certo turbamento. Cosa la preoccupa in modo particolare?

Lo sviluppo, eclatante e potenzialmente ancora da scoprire, della moderna tecnologia digitale, si rivolge ad ambiti che sono sicuramente idonei a migliorare la vita degli esseri umani e questo aspetto è sicuramente confortante. Ma chi governa l'evoluzione della società tecnologica? Chi decide la platea che può avere accesso a determinate conoscenze, privilegi, benefici e chi no? Nel mondo Occidentale siamo abituati a riconoscere legittimità ai Governi degli Stati in quanto espressione, più o meno diretta, della volontà popolare. Abbiamo studiato gli insegnamenti di Montesquieu e la teorizzazione del principio per cui "potere limita potere". La questione di cui parliamo non si risolve nell'ambito di un bilanciamento e di un equilibrio fra poteri dello Stato, perché sono in campo delle diverse "potenze", che sono aziende private, che hanno un DNA sovranazionale, che sfugge ad ogni controllo democratico degli stati nazionali. Consideriamo qualche numero per avere la dimensione del problema. Aziende come Amazon hanno un fatturato superiore di otto volte al PIL del Lussemburgo. È evidente che

queste realtà hanno un enorme potere di condizionamento sulle scelte della politica. Un social medium qual è Facebook batte moneta (Lybra), attività che ha da sempre definito la sovranità degli stati nazionali; mentre soggetti privati, come Elon Musk, conducono attività di ricerca spaziale, un tempo esclusivo appannaggio delle Agenzie governative.

Occorre anche dire che i player dell'hi –tech ci sono venuti in aiuto in questa fase emergenziale…

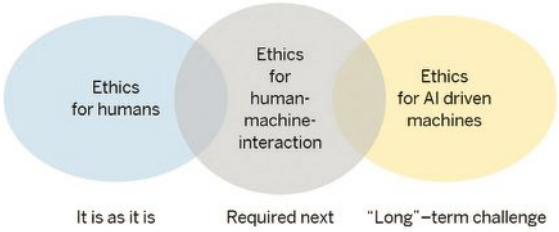
Nessuno vuole negarlo. La Pandemia ha visto l'Unione europea "genoflettersi" di fronte ai Giganti della ricerca farmaceutica, gli unici che possono "liberarci dal male" e salvarci dal virus. Tanti hanno ritrovato i propri parenti, durante il primo lockdown, grazie alle videochiamate di Whatsapp, il lavoro a distanza è stato garantito da Microsoft Skype e la didattica dei nostri figli da Google Classroom. Sono aspetti positivi, che devono anche generare una riflessione sulla concentrazione di competenze tecnologiche e strumenti economici di cui dispongono queste aziende che indirizzeranno il futuro del pianeta, senza un efficace bilanciamento dei poteri.

La triplice scansione Habeas corpus, habeas data, habeas mentem su cui ha insistito Pasquale Stanzione come va spiegata alla luce dell'evoluzione giuridica e culturale che ha segnato la storia dell'Occidente?

Il Regolamento Europeo sulla protezione dei dati fa costante riferimento ai diritti ed alle libertà delle persone. Noi siamo i dati che ci rappresentano. Esiste un legame indissolubile fra garanzie a tutela dell'individuo e limitazioni dei poteri assoluti. Ogni attività potenzialmente idonea a compromettere i diritti fondamentali della persona, deve essere valutata da soggetti terzi, indipendenti e che si muovono secondo un preciso dettato legislativo. Nella nostra quotidianità possiamo ritenere sufficientemente consolidato questo rapporto, che si identifica nella dinamica dei rapporti fra cittadino e Stato. Questo ci fa capire il motivo per cui nessuna limitazione fisica della libertà delle persone può essere sottoposta all'iniziativa di una componente singola, ma viene valutata e accuratamente soppesata da una serie di strutture indipendenti.

Il rischio di un "hackeraggio" del cervello emerso nel corso del dibattito è "fantascienza" o piuttosto un temibile dato di realtà?

"Non tutto ciò che è tecnicamente fattibile è giuridicamente lecito o eticamente ammissibile". Questa frase, utilizzata dal Presidente dell'*Authority* sintetizza il problema. La fattibilità tecnica è un muro sempre più scalabile. Ritorna il tema della titolarità del potere di governo dello sviluppo tecnologico, cui si sovrappone l'enorme fatica che i legislatori nazionali ed europei devono esercitare per tenere il passo dell'innovazione. Quando il diritto "arranca", il giudice non ha strumenti di sanzione, arriverà sempre in costante ritardo. Ma è sull'ammissibilità etica che il discorso diventa più complesso.



Antigone o Creonte

Intende dire che ritorna il dilemma tra "Antigone" e "Creonte", tra la legge non scritta e il diritto codificato?

Intendo dire che l'ammissibilità ha una radice soggettiva, non può essere scritta, né fissata. Il cervello umano si sa che è un insieme di impulsi e reazioni che possono essere sottoposti a controllo. Pensare che un microchip possa aiutare i malati di patologie quali Alzheimer o Parkinson è entusiasmante ma come non rimanere sbigottiti nel sentire che lo stesso microchip

può conservare i nostri ricordi? Quello scenario definito "proliferazione extra clinica dell'interfaccia cervello-computer", deve portarci ad alzare lo sguardo sui rischi di un'utilizzazione che travalicando lo stretto ambito medico-terapeutico apre scenari inquietanti, come inquietanti le notizie che arrivano dal mondo militare, dove la stretta simbiosi di biochimica e microtecnologia mira ad ottenere l'eliminazione della sensazione di fatica, dello stress, della paura, del sonno con il preciso orribile obiettivo di migliorare fino alle estreme conseguenze la performance dei soldati. Tali pratiche potrebbero essere sperimentate anche su uomini che detengono il potere, con conseguenze inimmaginabili sul piano delle scelte strategiche.

L'attività di lettura del cervello (*"brain reading"* n.d.r) si presta a interventi di "brain writing" che possono arrivare a condizionare il nostro cervello, riscrivendo opinioni, gusti, sentimenti e comportamenti consequenziali. Inutile sottolineare la gravità e la delicatezza del quadro che si sta delineando.

I fatti dell'attualità che hanno avuto esito tragico, vedi l'ultimo caso di Tik Tok, impongono nuove misure di monitoraggio e controllo inerenti l'uso dei media da parte soprattutto dei minori. Che idea ti sei fatto in merito?

Il mondo dei social media costituisce per i minori uno spazio di evasione rispetto ai limiti di autorità, controllo e repressione rappresentati dalla famiglia e

dalla scuola che non può essere negato. Detto in altri termini: i profili on line, dei ragazzi, sono spazi "personali pubblici" a disposizione del mondo, purché sottratti alla famiglia che, soprattutto nel periodo adolescenziale viene notoriamente vista come luogo coartazione e di soffocamento. Pensare ad un uso congiunto e mediato dalla presenza parentale è a mio giudizio un controsenso. Questo non vuol dire che non rimane centrale il tema dell'awareness e della formazione all'uso responsabile dei social media. In sintesi: lascerei ai giovani la gestione del mondo on line, a condizione che la "presenza silenziosa, discreta e vigile" dei genitori non manchi mai di accompagnare la loro "navigazione" nel mare aperto del web. ■

La cyber security, disciplina in divenire che segna il cambiamento d'epoca che stiamo vivendo

A colloquio con Flavio Venturini.

Autore: **Massimiliano Cannata**

Nel 2020 gli attacchi contro le infrastrutture critiche, quali danneggiamento, interruzione del servizio, furto dei dati a scopo eversivo sono aumentati in Italia del 246%, dato che corrisponde a un incremento del 78% delle persone indagate. Il quadro è reso ancora più fosco dalla "mafia digitale", fenomeno emergente e sempre più pervasivo, capace di rubare dati e di richiedere il "pizzo" di nuova generazione, che consiste nella richiesta di un riscatto da soddisfare in cripto valuta.

Sono cambiati strumenti e linguaggi, non è cambiata l'avida ricerca di guadagni da parte di organizzazioni a delinquere senza scrupoli, che hanno solo spostato la loro attenzione dal commercio reale a quello virtuale, dalle vie cittadine popolate di negozi e attività artigianali alle rotte virtuali, dove i confini si fanno più sfumati e gli affari ancora più interessanti. Questa escalation che riguarda realtà geografiche a tutte le latitudini, vede in particolare il nostro paese al 14esimo posto nella classifica delle nazioni europee più esposte al rischio. Il rafforzamento degli investimenti in sicurezza, insieme a un adeguamento normativo obbligato a tenere il passo dell'evoluzione di una criminalità informatica che ha assunto un profilo transnazionale, sono le priorità che figurano nell'agenda dei governi e nei piani di sviluppo delle imprese di tutto il mondo. ***Flavio Venturini***, *Innovation Director* di *Iconsulting*, in questa intervista realizzata per CST fa il punto sulle sfide che attendono un settore come quello della cybersecurity in costante divenire.

Ingegnere, la sicurezza informatica nella società del rischio è un asset strategico. Nell'orizzonte della "quarta rivoluzione" in cui reale e virtuale compongono il fitto intreccio che segna la nostra quotidianità, i maggiori pericoli per il business delle aziende ma anche per la stabilità degli stati arrivano da minacce globali, tecnologicamente sofisticate, difficili da prevenire. È il cyber spazio la nuova frontiera da proteggere?

La sicurezza digitale non può essere semplicemente vista come un tema di *compliance*, la corretta *governance* del rischio informatico presenta, infatti, degli impatti diretti su tutti i processi di business. Aziende e istituzioni non possono svolgere la loro normale attività produttiva in presenza di minacce

portate al cuore dell'organizzazione, che limitano il loro raggio di azione. In questo scenario diventa essenziale un innalzamento della consapevolezza del rischio cyber non solo tra i dipendenti ma in tutto l'ecosistema che ruota attorno all'impresa, le cosiddette terze parti dai fornitori, ai clienti, che devono conoscere i potenziali rischi e gli strumenti di difesa di cui l'organizzazione è dotata. Le imprese oggi vivono connesse, un "anello" debole può finire col "contagiare" tutta la catena del valore. Serve dunque una forte attenzione all'innovazione in tutti i gangli della produzione. Combattere la continua evoluzione degli hacker, che hanno dimostrato di saper affinare le loro tecniche di offesa con grande abilità, è un mestiere impegnativo che non può conoscere soste.

Come si declina il rapporto tra Intelligenza artificiale e Cyber security?

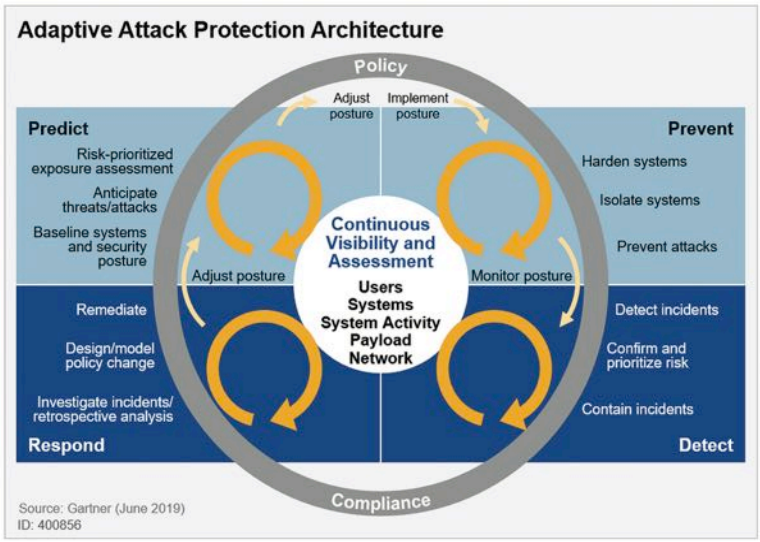
Non parlerei di Intelligenza artificiale, termine che preso in sé può essere fuorviante. Parlerei di *Data science* al cui interno ci sono competenze relative ai data base, a sistemi distribuiti a calcolo parallelo, dal *machine learning*, al *deep learning*. In questi ambiti rientra tutto quello che contribuisce a costruire soluzioni che possiamo definire anche di intelligenza artificiale. In particolare, quello che sta avvenendo sempre più velocemente nell'ambito delle soluzioni *cyber security* è un cambio di paradigma. Siamo passati dalla costruzione di soluzioni basate sulla programmazione, in cui a un preciso input corrispondeva un output che consentiva di reagire a una situazione potenzialmente critica, all'adozione di un paradigma in cui a partire dalla lettura dei dati (input e output) che il sistema ci mette a disposizione, si progettano soluzioni efficaci di contrasto grazie alla capacità di autoapprendimento dei software. È questo il cuore del *machine learning* e dell'intelligenza artificiale, individuabile in quella specifica capacità di lettura di eventi potenzialmente pericolosi, che una macchina, debitamente istruita dall'uomo, è in grado di assicurare.

La governance del rischio

L'automazione in che modo ha rafforzato la nostra capacità di individuare le vulnerabilità e di studiare le diverse tipologie di rischio?

L'universo delle applicazioni che si riferiscono ad aspetti comportamentali, piuttosto che al processamento del linguaggio naturale, ha modificato il modus operandi, facendo crescere molto velocemente le capacità delle macchine. Mentre prima per programmare c'era bisogno dell'analista che valutava il contesto e costruiva il programma adesso è lo stesso software che modella i suoi risultati autonomamente in funzione degli input. Si lavora ormai su modelli che ci aiutano nella previsione e nell'individuazione del rischio. Siamo passati dalla *governance* del controllo alla *governance*

del rischio. Nel passato ci concentravamo sull'adozione di regole fisse, sul controllo, sulla difesa passiva, adesso è la visione probabilistica che è divenuta prevalente. Questo ha dei riflessi importanti sull'adozione delle soluzioni di cyber security. Non esistono modelli definitivi. Qualsiasi modello comportamentale, è un modello che cambia nel tempo perché cambia il contesto, serve una cura continua, non esistono soluzioni valide una volta per tutte. Questo è vero in qualsiasi campo in cui si applica il *machine learning* e ancora di più in ambito cyber.

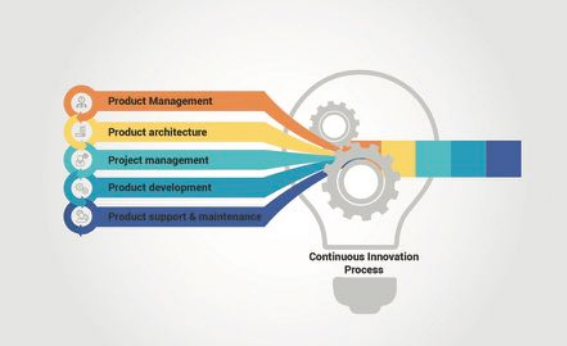


Cosa deve avere un buon manager della security in aziende che presentano un DNA fortemente segnato da strumenti di connettività diffusa?

I manager della Cyber sia in ambito pubblico che privato devono pensare a curare il ciclo di vita molto limitato di sistemi complessi, che necessitano di *tuning* e di innovazione continua per dare i risultati attesi. La sperimentazione non deve arrestarsi mai, partendo da questa convinzione *Iconsulting* ha deciso di sollecitare aziende pubbliche e private a dotarsi di una nuova struttura: il *data lab*, da affiancare ai sistemi di produzione. Un laboratorio che ponga attenzione all'efficacia degli algoritmi e dei sistemi in essere e nel contempo che sia capace di valutarne di nuovi risulta necessario nelle organizzazioni complesse. Tale ragionamento risulta valido non solo in ambito *cyber* ma anche in altri ambiti strategici pensiamo al marketing, solo per fare un esempio. In questo periodo le stesse modalità di acquisto e di comportamento sono mutate, sulla spinta di un catalizzatore imprevedibile quanto drammatico come è stata la pandemia. Sono fenomenologie che non si possono ignorare se si vuole fare impresa e sostenere i ritmi della competizione globale.

BIO

Flavio Venturini è Direttore della sede Iconsulting di Roma, nonché Industry Leader per il settore Pubblica Amministrazione Centrale. Flavio vanta un'esperienza più che ventennale come Solution Architect, Practice Director e Project e Program Manager in ambito Spazio, Difesa e Telco, sviluppata a livello internazionale in Inghilterra, Olanda, Spagna e Germania. Il ruolo in Oracle di Responsabile vendite Europa, Medio Oriente e Africa per la practice Big Data Analytics e di Country Leader per la vendita di licenze Analytics per l'Italia gli ha valso una solida esperienza di vendita di progetti e soluzioni nonché di prodotti. Oggi è alla guida della sede di Roma, dove supporta aziende e organizzazioni nel loro processo di innovazione. Nel suo percorso professionale in Iconsulting ha traguardato gli obiettivi strategici di Pubbliche Amministrazioni Centrali come il Ministero del Lavoro e delle Politiche Sociali e ISTAT e sta supportando il percorso verso la Data Digital Transformation di importanti aziende quali Poste, ENAV, Ford. Nel 2013 ha contribuito a creare, insieme al Professor Giuseppe Ragusa, il primo Master italiano in Big Data Analytics per LUISS Business School, di cui è stato direttore. Sempre per LUISS Business School da alcuni anni è il direttore scientifico dei Master Big Data per Executive.



La centralità del rapporto Uomo – macchina

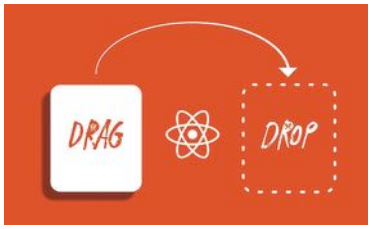
La gravità e nel contempo l'urgenza delle sfide impongono una centralità della sicurezza nelle organizzazioni produttive che non sempre viene riconosciuta. Non crede che siano oggi gli investimenti in capitale umano ad assumere una rilevanza strategica decisiva per il futuro delle imprese?

Da un punto di vista organizzativo va fatto un salto in avanti. In particolare, va compreso che le tematiche connesse alla *cyber security* non sono circoscrivibili

all'area dell'IT. Tutti gli asset digitali aziendali che sono poi il core di qualsiasi azienda hanno bisogno di protezione. Con la diffusione del *remote working,* imposto dalla pandemia, questa esigenza è diventata ancora più forte. Altro aspetto che va considerato è l'impatto che questa struttura organizzativa deve avere su tutta l'azienda. Il capitale umano deve esser reso consapevole dei rischi e come tale deve diventare esso stesso uno strumento di ausilio all'individuazione di fenomeni anomali, al fine di aiutare gli algoritmi a funzionare meglio. La macchina e l'uomo devono aiutarsi reciprocamente. Pensiamo ai *cyborg* l'uomo aiutato dalla macchina e viceversa, se vogliamo avere l'idea di un corretto modo di bilanciare

Ritorna di attualità la riflessione di Giuseppe O. Longo e del suo "simbionte", una creatura capace di sublimare, in una sintesi alta, biologia e cibernetica, schiudendo di fatto lo scenario affascinante e inquietante del "post-umano". Al di là delle fantasmagoriche definizioni, sta emergendo una domanda di diffusa sensibilizzazione a queste tematiche non più differibile, manifestata dagli uomini di business e dagli utenti. Nel prossimo Cert Star* Iconsulting *presenterà "RapidMiner". Può in sintesi illustrarci i requisiti di questo strumento che opera in ambito* data science*?

L'uso di RapidMiner permette di democratizzare l'intelligenza artificiale, perché permette di comprendere in maniera abbastanza immediata il flusso di



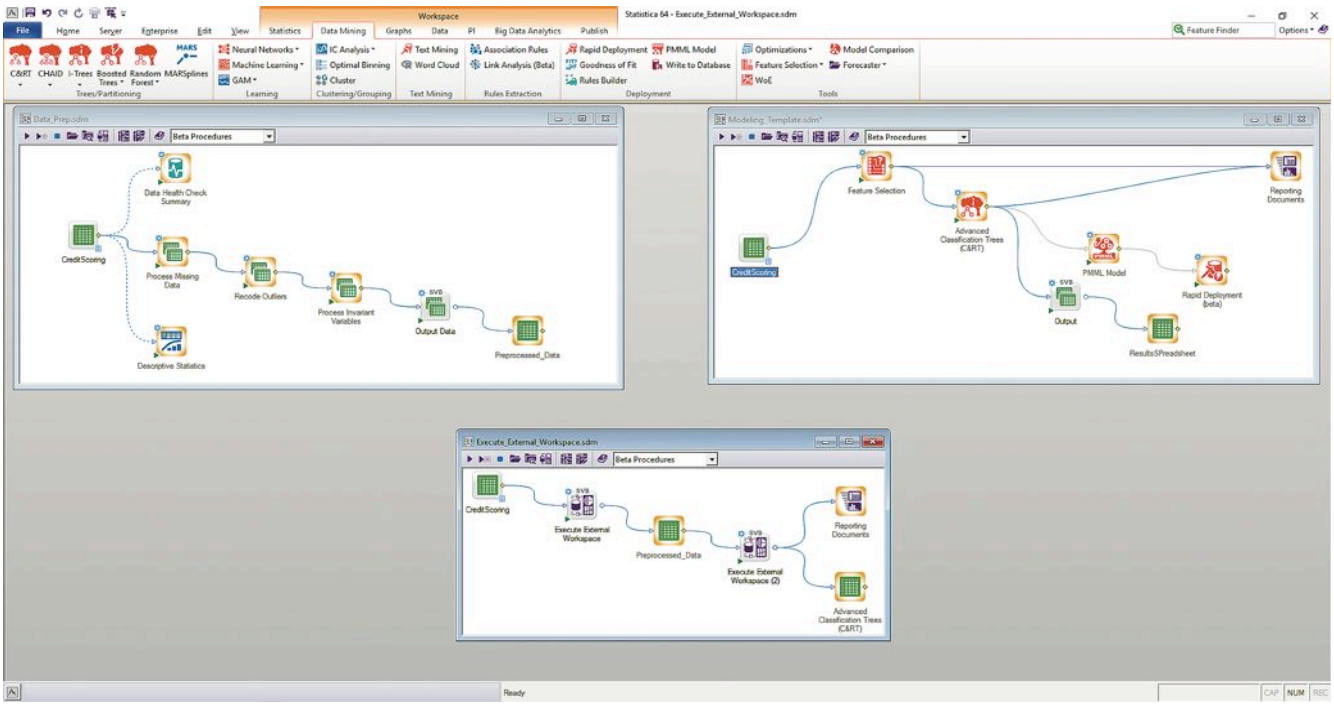
funzionamento di un sistema analitico, mettendo a disposizione un'enorme libreria di funzioni che lavorano in una particolare modalità, che in gergo tecnico si definisce *drag and drop*. Per capirci: "semplici" utenti di business, non necessariamente programmatori, né data scientist di professione, grazie a *RapidMiner* si possono costruire dei sistemi analitici, riuscendo a comprendere il comportamento degli algoritmi.

Uno strumento che serve a rendere dunque più facile la vita per chi si muove nella selva di numeri e modelli previsionali?

Semplificare è la parola chiave, che non vuol dire banalizzare, significa impegnarsi a interpretare correttamente i fenomeni al fine di aumentare il livello di conoscenza che abbiamo della realtà. Si parla molto di un tema che viene definito *explainability* perché spesso quando si scrive un programma in linguaggi riconducibili nella maggior parte dei casi nell'area disciplinare del *machine learning*, non risulta intelligibile per chi non ha un *pedigree* squisitamente tecnico. Utilizzando *RapidMiner* siamo nelle condizioni di mettere la macchina digitale a cuore aperto e quindi di interpretare l'"alfabeto" che ci racconta i comportamenti del sistema. Come se avessimo di fronte un motore di vetro finalmente trasparente e perciò comprensibile a tutti.

Cosa vuol dire in concreto?

Che siamo in grado di costruire degli attributi rappresentativi dei fenomeni. Ricordiamoci che il valore fondamentale in qualsiasi soluzione analitica è la comprensione del business. Chi non è esperto di uno specifico tema, difficilmente riesce a individuare gli attributi che rappresentano in



modo specifico il fenomeno sotto osservazione. Il binomio virtuoso che l'utente di business può instaurare con questo strumento, semplice ma al contempo sofisticato aumenta la potenza e l'efficacia delle soluzioni che siamo in grado di mettere in campo.

La condivisione delle informazioni come leva strategica

Il ruolo dei CERT sempre molto dibattuto. Dalle sue parole si capisce molto bene che queste strutture hanno una funzione molto importante nell'attività di individuazione e contrasto del cyber crimine, a patto che siano disposte ad aggiornare e ad ampliare il cruscotto della loro strumentazione. È una lettura corretta del suo pensiero?

Assolutamente sì. Più attrezzi si hanno a disposizione per comprendere e valutare i rischi e le minacce più efficace diventa l'azione della *cybersecurity*. Il data lab su cui stiamo lavorando vuole essere proprio questo strumento in più, che consente, tra l'altro, una cosa molto importante come l'integrazione dei dati. Avere più strumenti che forniscono indicazioni differenziate e che osservano tutti i canali attraverso cui potenziali minacce possono arrivare e riuscire a integrare questi dati fino a costruire una visione organica del contesto è una condizione essenziale per orientarsi nella complessità scientifica e tecnologica che caratterizza la società e le imprese di oggi. Il data lab risulta, inoltre, indispensabile per le organizzazioni interessate a definire una data platform di comunicazione, condivisione e scambio di dati e informazioni.

Le chiedo in conclusione di provare a gettare lo sguardo oltre. Quali prospettive si aprono per le aziende che hanno la responsabilità, che molti osservatori definiscono "civile", oltre che sociale, di compiere uno sforzo decisivo per aiutare l'umanità a uscire dal dramma di un'emergenza che appare senza fine?

La *Data science*, gli algoritmi, lo sviluppo di nuove discipline del sapere non possono prescindere dagli impatti sociali che il progresso per sua natura presenta. Da anni sono impegnato su questo fronte, che a mio

giudizio riveste un aspetto decisivo del mondo che verrà. Ricordiamoci che oltre il business, esiste una dimensione etica che non può essere ignorata. Social impact è una delle parole del futuro. Il mondo cambia da sempre: oggi a causa del Covid-19, ieri per la guerra in Vietnam, la crisi petrolifera, le torri gemelle. Nessuna paura, dunque, ma capacità di visione. C'è un tema forte che per la prima volta la trasformazione in atto ha reso chiaro anche alle persone più lontane dalla tecnologia: l'importanza del digitale. Viviamo "on life", come ha scritto in un recente brillante saggio Luciano Floridi, non possiamo più fare a meno del virtuale. L'universo è più digitale che analogico nel bene e nel male. Disporre di un antivirus sul pc diventa paradossalmente più importante che possedere un allarme a casa e questo dovrebbe bastare a capire la tendenza fondamentale del nostro tempo. La difesa degli asset digitali è una componente destinata a segnare la nostra epoca, per questo credo sia auspicabile che entri a far parte della *forma mentis* di una platea sempre più vasta di persone. Non possiamo permetterci di avere paura del cambiamento, altrimenti rischieremmo di piombare in una condizione di inaccettabile arretratezza. ■

Perché la pandemia ci ha dato una nuova prospettiva della cyber security. È il momento di mettere la cybersecurity al centro delle operation aziendali.

splunk>

Autore: Oliver Friedrichs,
VP of Security Products di Splunk.

"In questa situazione di incertezza..." è senz'altro una delle espressioni maggiormente utilizzate recentemente, ma è di certo tra le meno efficaci quando si tratta di decidere la strategia da intraprendere e di passare all'azione.

In genere, quando pianifichiamo la nostra vita personale abbiamo bisogno di fondamenta solide su cui poggiare le nostre scelte: la presenza della nostra famiglia, la nostra situazione economica, il nostro lavoro, il supporto dei nostri amici. Lo stesso avviene, anche se con forme diverse, quando pianifichiamo la nostra attività di business: in questo caso usiamo molteplici fonti informative, che possano permetterci di costruire basi solide e che ci assicurino un buon fatturato a fronte di un rischio di impresa che consideriamo accettabile.

Cosa accade quando pianifichiamo la difesa del business aziendale dalle minacce che il mondo cyber comporta? Al centro di tutto, come in qualunque processo aziendale, ci sono indubbiamente le persone:

i professionisti della cyber security, con il grande compito di mantenere i dati e le risorse tecnologiche di un'organizzazione al sicuro e funzionanti nonostante lo stravolgimento delle modalità di accesso e consumo delle risorse aziendali che il lavoro da remoto ci ha imposto nell'ultimo anno.

La rete è tutto un fiorire di informazioni relative alle nuove minacce cyber, ai percorsi più rapidi per la resilienza, al costo delle sanzioni per la non conformità, alle sempre presenti violazioni dei dati e all'importanza vitale di garantire che gli investimenti nella trasformazione digitale non si blocchino. Le sorgenti dati (o di informazione se preferite) non ci mancano di certo.

Ciò che è meno chiaro è come possiamo creare un valore culturale più duraturo e come possiamo valorizzare il lato umano di questi passaggi pratici, aspetti sui quali siamo stati decisamente carenti fino ad oggi. Quindi, quali sono i fattori che influenzano questa nuova cultura della cyber security?

A pesca di dati

Come essere umani siamo innatamente curiosi, ricerchiamo informazioni inerenti a qualsiasi aspetto della nostra vita personale e professionale utilizzando le più disparate sorgenti informative, anche le più dubbie.

Lo status di "remote workers" miscelato con la pandemia ci ha portato a ricercare informazioni su SARS-CoV-2 inizialmente, sui vaccini successivamente per culminare con le informazioni circa le varianti del virus. Tutto questo non ha fatto altro che inasprire la nostra sete di informazioni.

Essendo uno dei metodi più economici ed efficienti per raggiungere obiettivi su larga scala, non sorprende che il phishing o lo spear phishing

BIO

Con un ricco curriculum nella costruzione di quattro aziende di successo nel campo della sicurezza aziendale negli ultimi due decenni, Friedrichs ha recentemente ricoperto il ruolo di fondatore e CEO di Phantom. Prima di Phantom, Friedrichs ha fondato Immunet, acquisita da Sourcefire nel 2010 e componente chiave dell'acquisizione di Sourcefire da parte di Cisco nel 2013; ora prospera come Advanced Malware Protection (AMP) di Cisco. Friedrichs ha co-fondato SecurityFocus (Bugtraq) e ha guidato DeepSight, il primo sistema di allerta precoce su Internet, acquisito da Symantec nel 2002. Ha anche co-fondato Secure Networks e guidato Ballista (CyberCop), una delle prime soluzioni di gestione delle vulnerabilità del settore, acquisita da McAfee nel 1998. Friedrichs ha progettato e sviluppato un prototipo del primo prodotto commerciale di penetration-testing.

siano una delle principali tecniche utilizzate negli attacchi che abbiamo osservato durante lo scorso anno. Gli attaccanti stanno continuamente affinando tecniche consolidate in modo da instillare il senso di urgenza in maniera sempre più efficace. Il cyberspazio è una enorme fonte informativa per gli attaccanti stessi, che sempre più frequentemente utilizzano dati prelevati dai social network, arrivando fino a clonare i profili degli utenti, pur di risultare maggiormente credibili.

E anche la trasformazione digitale non poteva essere certamente ignorata dagli attaccanti. Durante lo scorso anno, il 36% degli attacchi ha infatti interessato soluzioni SaaS aziendali.

Questo elevato livello di personalizzazione, congiuntamente a un ottimo livello di italiano raggiunto dai messaggi personalizzati comporta una maggiore

difficoltà nell'identificazione degli attacchi di phishing, spesso anche da parte dei più esperti in tecnologia. La formazione del personale è un elemento fondamentale, non solo attraverso la comunicazione o dei corsi (indispensabili ma mai sufficienti), ma anche attraverso simulazioni ed esercizi periodici che possano permettere di mantenere il livello di allerta molto alto. Avete mai guardato distrattamente la vostra e-mail mentre vostro figlio/a correndo per casa rischiava di farsi male? So che sapete di cosa sto parlando. Spesso gli attaccanti ci trovano distratti, ed è anche su questo che molto spesso contano per far sì che le campagne di attacco vadano a buon fine.

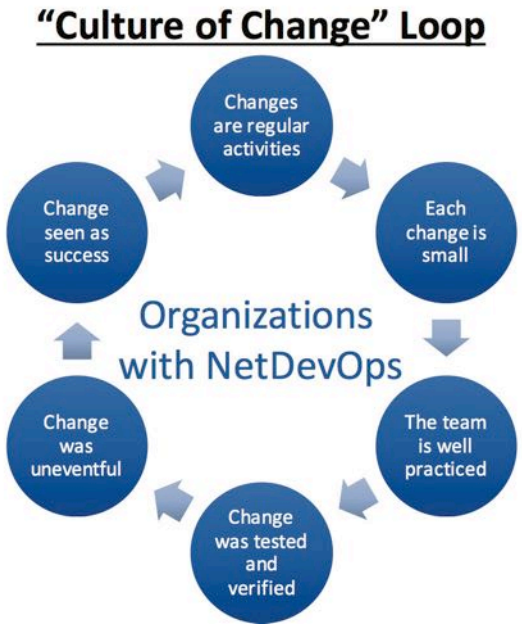
Sicuri di non avere backdoor?

Il "remote work" ci porta immancabilmente a lavorare in condizioni il cui livello attenzione è alterato da tutto quello che accade in casa: figli che seguono le lezioni in DAD, pacchi che arrivano dai corrieri più disparati, bambini al rientro dal nido che pretendono attenzione e i sempre ed immancabili call center che chiamano dai numeri più improbabili.

Questo alterato livello di attenzione comporta errori più frequenti: dati inviati a persone sbagliate o non affidabili e accentuata pigrizia nell'applicare le patch a sistemi operativi o applicazioni. Ammettiamolo, non siamo mai stati bravi nell'applicazione delle patch, e la situazione attuale non sta facendo altro che aumentare il nostro debito di vulnerabilità, esponendo le nostre aziende sempre di più.

Il panorama, tuttavia, è molto più complesso delle "semplici" patch di sicurezza non applicate: server cloud mal configurati (purtroppo la semplicità di provisioning spesso non comporta altrettanta attenzione nella configurazione sicura degli stessi), ambienti multi-cloud che spesso comportano maggiore complessità nel monitoraggio, API spesso implementate in fretta, password di default o non sicure e gli immancabili software non autorizzati installati sui sistemi aziendali. Problemi vecchi e nuovi che complicano lo scenario che stiamo vivendo. Non sorprende infatti che più di 1 organizzazione su 5 subisca un incidente informatico originato da una risorsa IT non autorizzata.

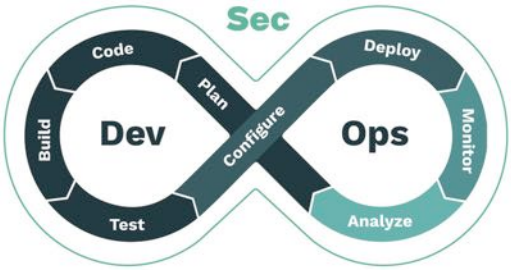
È necessario un cambiamento culturale per poter iniziare a porre rimedio alla situazione attuale: la cyber security deve diventare una responsabilità di tutti, in modo da mantenere gli attaccanti fuori dalle nostre case e fuori dal nostro business.



Un cambio di ruolo

Una ricerca pubblicata all'inizio della pandemia ha rilevato che il 47% dei team di sicurezza si è trovato riassegnato a compiti IT generici e il 90% lavora da remoto a tempo pieno (molto più che tempo pieno, di frequente). Questo, ovviamente, è preoccupante, maggiori responsabilità allocate nella stessa finestra temporale comporta inevitabilmente minor tempo dedicato a ciascuna di esse. Dall'altro lato, l'aspetto positivo di questa fusione di IT e cyber security è l'evangelizzazione di una platea IT più ampia su tematiche di sicurezza informatica soprattutto quando vi sono investimenti come DevSecOps che provano a rompere i silos.

Essere in grado di collocare le professioni della sicurezza dove è necessario, ma facendole integrare profondamente con il resto team IT, sarà una delle lezioni che avremo imparato lavorando durante una pandemia globale. Stabilire la priorità su dove si concentrano questi professionisti può anche consentire di automatizzare alcune attività a lungo termine. Pronti ad abbracciare la filosofia DevSecOps?



Disparità di competenze

Quello che non vorremmo avere è una mancanza di professionisti skillati in cyber security, un problema in crescita nel settore. Il crescente divario nelle competenze ha lasciato tante organizzazioni prive di professionisti della cyber security dedicati a svolgere le funzioni necessarie per proteggere l'azienda, con grande preoccupazione dei CISO.

Secondo un recente report Marlin Hawk, due terzi (66%) hanno affermato di soffrire di carenze di talenti perché i candidati non hanno le giuste conoscenze tecniche, mancano di esperienza o semplicemente non hanno la cultura adatta. È un problema che la maggior parte dei CISO (62%) pensa che peggiorerà nei prossimi cinque anni, ma - come molti cambiamenti in corso in questo momento - questo potrebbe essere stato solo accelerato dalla recente crisi.

Non è quindi questo il momento di diluire certi ruoli, ma piuttosto di utilizzare la loro riallocazione per rafforzare e aiutare a diffondere l'idea di sicurezza come valore fondamentale dell'azienda.

Il CISO del futuro

Il ruolo del CISO è quello di essere presente lungo tutta la catena di comando. Comunicando verso l'alto, i CISO sono saldamente inseriti nel board decisionale e spesso è loro compito colmare il gap tra la necessità di proteggere l'organizzazione e la direzione che si vorrebbe prendessero gli investimenti.

La gestione di una forza lavoro più ampia e la necessità di non abbassare mai la guardia, richiede la capacità di identificare un incidente di sicurezza in mezzo a una raffica di falsi positivi e avvisi a bassa priorità. Guardando al futuro, i CISO dovranno confrontarsi con una forza lavoro ancora più flessibile, costringendoli ad essere più agili che mai riguardo al panorama delle minacce.

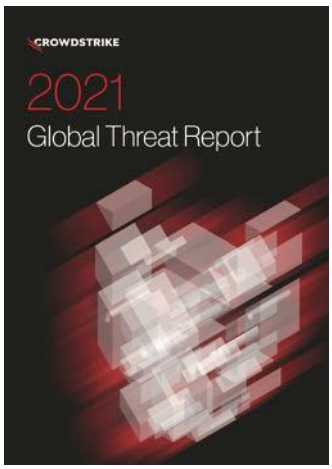
Le difficoltà e le sfide affrontate dalle nostre aziende negli ultimi mesi, hanno evidenziato che la sicurezza non è qualcosa che può essere deprioritizzato. Questo può essere un momento perfetto per i nostri team di cyber security per aiutarci a garantire che sicurezza, stabilità e fondamenta solide, sia in senso pratico che umano, siano al centro dei valori aziendali condivisi.

Adattamento italiano a cura di: Antonio Forzieri, EMEA Cyber Security Specialization and Advisory, Splunk ■

Difendersi da malintenzionati esterni, interni e da criminali informatici

Autore: Shawn Henry, Presidente di CrowdStrike Services e CSO di CrowdStrike

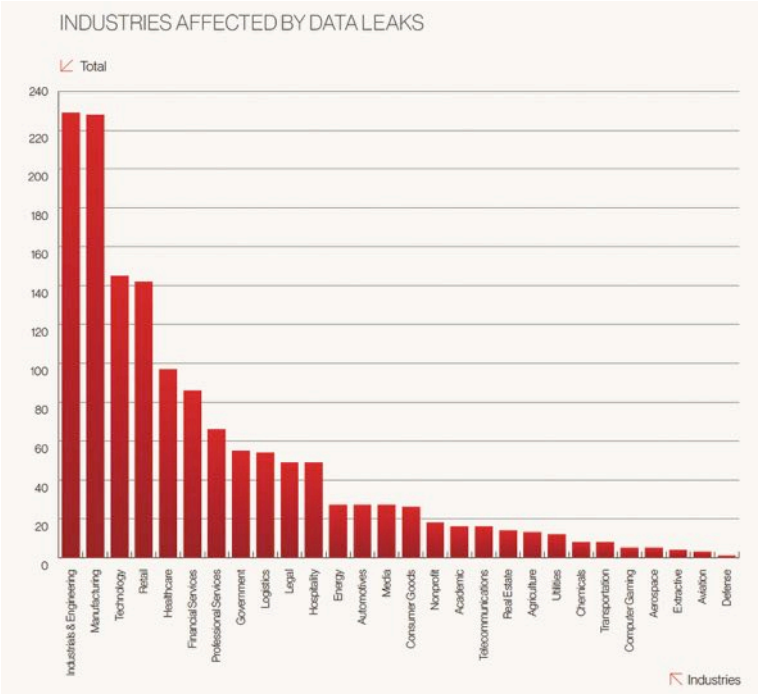
All'inizio del 2020 il panorama delle minacce appariva già completamente mutato rispetto allo stesso periodo dell'anno precedente. Come spiega il Global Threat Report 2021 di CrowdStrike, l'ecosistema eCrime continua a evolversi e maturare, e gli avversari appoggiati dagli stati nazione sono sempre più implacabili. Ora, a causa della pandemia di Covid-19, il panorama delle minacce è ancora una volta sull'orlo di una trasformazione epocale.



Sia i criminali informatici che gli stati nazione stanno facendo leva sui timori che il coronavirus alimenta nelle persone per lanciare campagne di social engineering volte a sottrarre informazioni private e dati finanziari. In questo contesto già abbastanza complicato si inserisce una terza minaccia – a volte inconsapevole ma altre, purtroppo, consapevole: i malintenzionati interni all'azienda.

Ora che la gran parte dei collaboratori lavora da remoto a causa delle misure di confinamento decise dai governi, si è spalancata la porta su un mondo completamente nuovo di vulnerabilità da sfruttare: reti WiFi pubbliche non sicure, dispositivi personali obsoleti e non protetti, autorizzazioni e modalità di accesso non conformi, tanto per citare qualche esempio. In più, per tentare di restare a galla durante l'emergenza sanitaria, le aziende inizieranno a rivalutare le spese operative nell'ottica di ridurle, e questa scelta probabilmente causerà licenziamenti o sospensioni.

Un dipendente licenziato, specialmente se contrariato o disperato, ha sempre rappresentato un rischio per l'azienda perché è un pericolo difficile da individuare, prevenire e sondare. Senza le opportune misure di



sicurezza, una minaccia di questo tipo può mettere seriamente in pericolo i dati sensibili dell'azienda. Esistono tre misure efficaci che consentono alle aziende di contenere i rischi informatici in questo periodo così difficile.

Le truppe si spostano nel cloud

Il primo passo per rendere sicuro un ambiente di lavoro remoto consiste nel gestirlo correttamente. Anche se i collaboratori si tutelano usando dispositivi protetti, VPN e autorizzazioni di accesso regolamentate, il rischio di violazione è sempre presente, specialmente se l'attacco proviene da malintenzionati interni all'azienda.

Per incidenti di questo tipo, è importante che il personale che si occupa della sicurezza sia in grado di rilevare, analizzare ed eliminare la violazione senza dover «inviare le truppe sul campo», specialmente ora che, a causa della pandemia, le trasferte del personale allungano i tempi di remediation ma mettono anche a repentaglio la salute delle persone.

La soluzione per rendere sicuro lo smart working è il cloud. Grazie al cloud i responsabili della sicurezza riescono ad avere piena visibilità sull'ambiente di lavoro aziendale, a prescindere dal numero di piccoli uffici casalinghi che ne fanno parte, e possono rispondere agli incidenti in modo agile, implementando da remoto soluzioni immediate con cui riparare i dispositivi compromessi. In più, il cloud semplifica enormemente la condivisione delle policy di sicurezza su tutti i dispositivi, personali e professionali, perché il personale IT può distribuire patch e autorizzazioni di accesso senza allontanarsi da casa. Dal punto di vista della gestione dei processi, i responsabili IT e della sicurezza possono implementare un modello di accesso basato sul «principio del privilegio minimo» valutando da remoto a quali dati sensibili ogni collaboratore ha accesso e limitando l'accesso alle sole risorse della rete necessarie per le sue mansioni. Qualora il collaboratore dovesse lasciare l'azienda, revocarne i diritti di accesso sarà pratico e veloce.

Combinare le capacità umane e la potenza dell'intelligenza artificiale

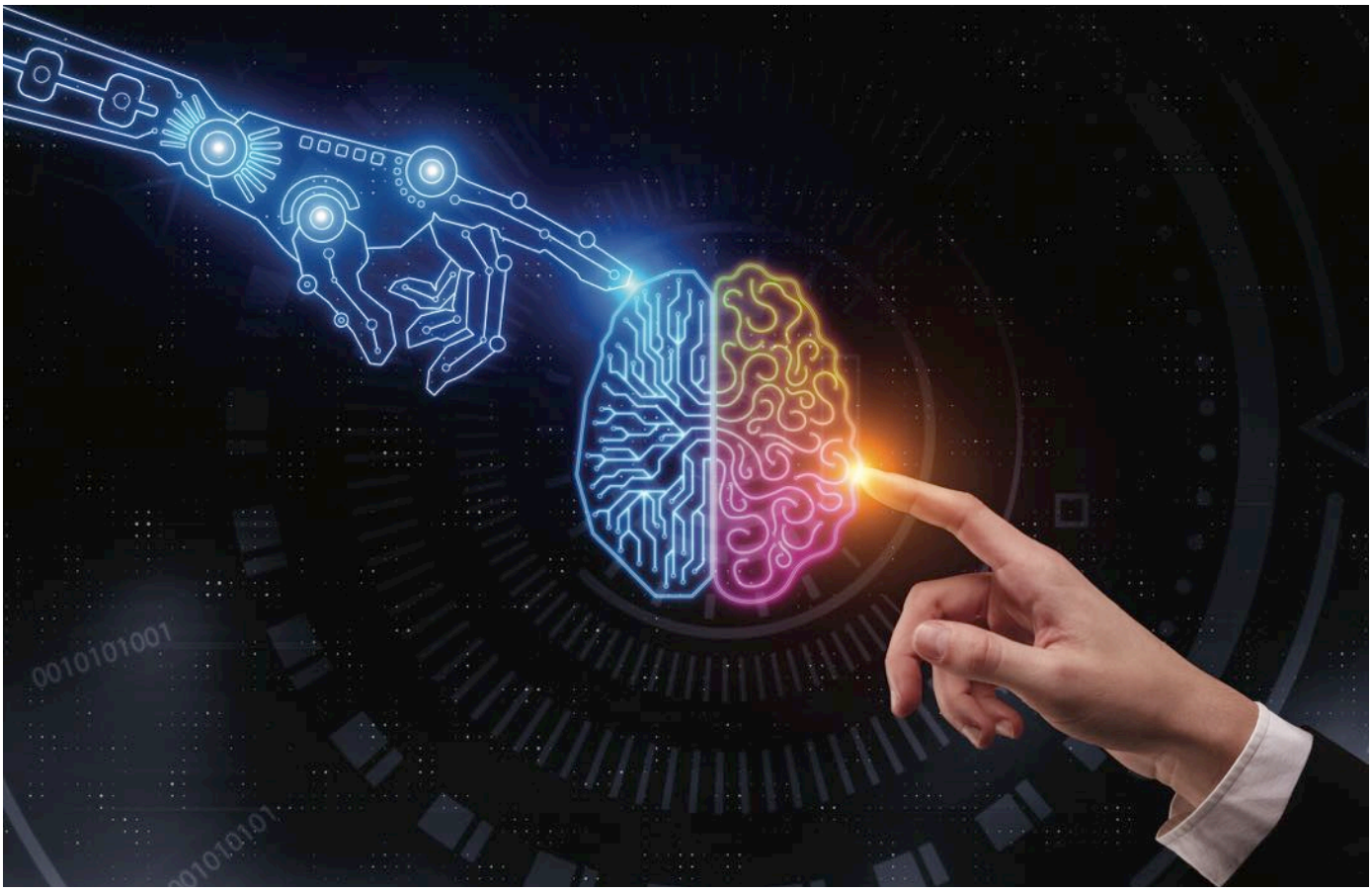
Quando si tratta di smascherare le attività di malintenzionati interni all'azienda, la difficoltà maggiore consiste nel separare le potenziali azioni dannose dalle «normali» attività lavorative prima che sia troppo tardi.

BIO

In qualità di Presidente di CrowdStrike Services, Shawn guida un team a livello mondiale di professionisti della sicurezza informatica che investigano e mitigano in modo aggressivo ed efficace gli attacchi mirati alle reti di computer. Sotto la sua guida, CrowdStrike è stato impegnato in significative operazioni proattive e di risposta agli incidenti in tutti i principali settori commerciali, proteggendo i dati e le reti sensibili delle organizzazioni. Nel 2012 Shawn era Executive Assistant Director (EAD) dell'FBI, sovrintendendo a metà delle operazioni investigative dell'FBI, comprese tutte le indagini criminali e informatiche dell'FBI in tutto il mondo, le operazioni internazionali e la risposta agli incidenti critici dell'FBI a importanti indagini e disastri. Durante i suoi 24 anni di carriera, ha ricoperto una vasta gamma di ruoli operativi e di leadership in quattro FBI Field Offices e presso il quartier generale dell'FBI. Shawn fa parte della Facoltà ed è membro del consiglio direttivo della National Association of Corporate Directors (NACD), dove insegna al Board e ai Direttori i complessi aspetti della cyber security. Attualmente fa parte dello Strategic Advisory Committee of the Global Cyber Alliance. Shawn ha conseguito una Laurea in Business Administration presso la Hofstra University e un Master of Science in Criminal Justice Administration presso la Virginia Commonwealth University. Si è laureato presso l'Homeland Security Executive Leadership Program del Naval Postgraduate School's Center for Homeland Defense and Security.

Distinguere le une dalle altre non è come cercare un ago in un pagliaio quanto piuttosto come cercare un ago tra una montagna di altri aghi, perché le azioni di un malintenzionato che lavora per l'azienda possono apparire legittime in superficie ma nascondere un intento dannoso. I malintenzionati interni all'azienda sono un problema «umano» che spesso richiede un intervento umano.

Per riuscire a seguire e monitorare in maniera proattiva qualsiasi attività sospetta prima che si verifichi una compromissione grave, i responsabili IT e della sicurezza dell'azienda devono essere adeguatamente equipaggiati. La loro «cassetta degli attrezzi» può contenere soluzioni che impediscono l'uso di chiavette per esportare i dati o che registrano i dati dei sistemi di



posta elettronica in modo granulare per far risaltare le e-mail che contengono IP aziendali reindirizzati a indirizzi e-mail personali ma, in fin dei conti, per smascherare un essere umano serve un altro essere umano. Per questo motivo, una squadra specializzata in threat hunting – interna all'azienda o esterna a contratto – è un elemento indispensabile in un mondo basato sullo smart working. Le squadre specializzate in threat hunting sono in grado di rilevare la presenza di tecniche «Living-off-the-Land» e di attività sospette usando tecnologie avanzate per il monitoraggio degli endpoint e l'analisi dei big data.

Una soluzione aziendale per un problema umano

Proteggere l'azienda dalle azioni di dipendenti malintenzionati non è una responsabilità esclusiva del team IT e della sicurezza. Così come i dirigenti e i consigli di amministrazione trovano il modo di salvaguardare i profitti adattandosi a una forza lavoro diventata improvvisamente remota, è necessario che l'IT, le risorse umane e i responsabili di tutte le unità operative facciano fronte comune.

I responsabili delle unità operative devono collaborare e farsi promotori di iniziative strategiche volte a informare e istruire il consiglio di amministrazione sui rischi crescenti e sempre nuovi legati alla sicurezza e sulla necessità di investire adeguatamente per dotarsi delle politiche, delle risorse e degli strumenti necessari per proteggere l'azienda. A prescindere dal reparto in cui lavorano, molti dipendenti godono di una qualche forma di accesso privilegiato alla rete, ai sistemi e ai dati riservati dell'azienda. Fare in modo che tutti i livelli aziendali siano consapevoli degli accessi privilegiati di cui gode ogni collaboratore, del tipo di informazioni riservate che gestisce e dei processi da seguire per far uscire in sicurezza un dipendente dall'azienda sono misure fondamentali per mettersi al riparo da attacchi interni.

Ordinaria amministrazione in tempi straordinari

L'emergenza sanitaria causata dal Covid-19 sta sconvolgendo la normalità delle nostre vite lavorative. Tuttavia, questo non significa che le misure adottate per proteggere la tua azienda in questo momento andranno perse. Scegliendo in modo oculato tecnologia, persone e processi, le aziende possono realizzare e mantenere una barriera solida contro le minacce interne ed esterne che si rivelerà utile anche quando la forza lavoro non sarà più costretta a casa. Una volta messe in atto queste soluzioni, sarà meno complicato anche smantellare un «ufficio casalingo» qualora un dipendente decidesse di lasciare l'azienda. Le aziende e i collaboratori potranno così continuare il proprio cammino in tutta sicurezza, anche quando le loro strade si dividono. ■

La sicurezza come valore condiviso

A colloquio con Arturo Di Corinto.

Autore: **Massimiliano Cannata**

In questa intervista Arturo di Corinto, psicologo cognitivo, esperto di innovazione tecnologica, collaboratore di quotidiani e riviste di settore che svolge un'intensa attività di insegnamento, affronta un particolare aspetto della sicurezza: quello legato al rapporto tra la *supply chain* e l'articolata catena di clienti e fornitori che costituisce l'ecosistema di riferimento per tutte le aziende che operano in mercati complessi.

Sicurezza e* supply chain. *Professore come si declina questo rapporto, sempre più al centro delle attenzioni del management?

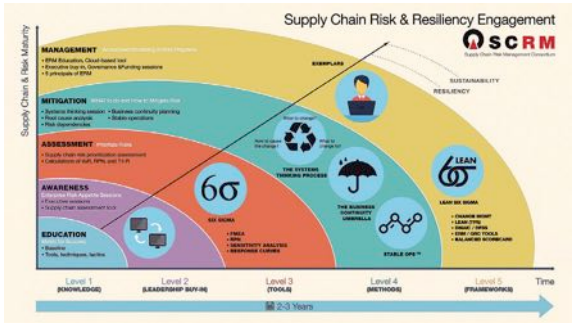
Si tratta di un tema complesso. Gestire il rischio sicurezza per la supply chain è cruciale per aziende e istituzioni che erogano servizi o realizzano prodotti che integrano nelle proprie soluzioni componenti forniti da terze parti. Se questo tipo di servizio è il core business dell'azienda se ne coglie subito l'importanza per il management. Trattandosi però di un tipo rischio che deriva dalle relazioni coi propri fornitori, diretti e indiretti, la sua cattiva gestione può avere conseguenze sia su scala nazionale che internazionale. Ce lo ha dimostrato l'attacco alla *supply chain* di *SolarWinds* che ha avuto come conseguenza l'esposizione di dati, informazioni e sistemi in tutto il mondo, anche in settori delicati, come quello nucleare negli USA. Ma il tema riguarda molto da vicino tutte le aziende che per la Direttiva europea NIS (Network and Information Security) sono Operatori di Servizi Essenziali o Fornitori di Servizi Digitali.

Una catena di fornitori poco attenta alla tutela del business e alla riservatezza dei dati può diventare un punto di debolezza per la sicurezza dell'impresa?

Ogni rapporto di fornitura di prodotti e servizi tra aziende - design, ricerca, implementazione, verifica, distribuzione, manutenzione, test - dipende dall'infrastruttura ICT, sia per i servizi erogati all'utente finale sia, più in generale, per i processi produttivi. Attaccare l'infrastruttura ICT significa di fatto pilotare la *supply chain* per fini illeciti o criminali.

Quali tipologie di rischio si associano alle cosiddette "terze parti"?

Il rischio è direttamente proporzionale alla complessità della *supply chain*, al target e alla capacità operativa degli attaccanti. Per contrastare il cyber



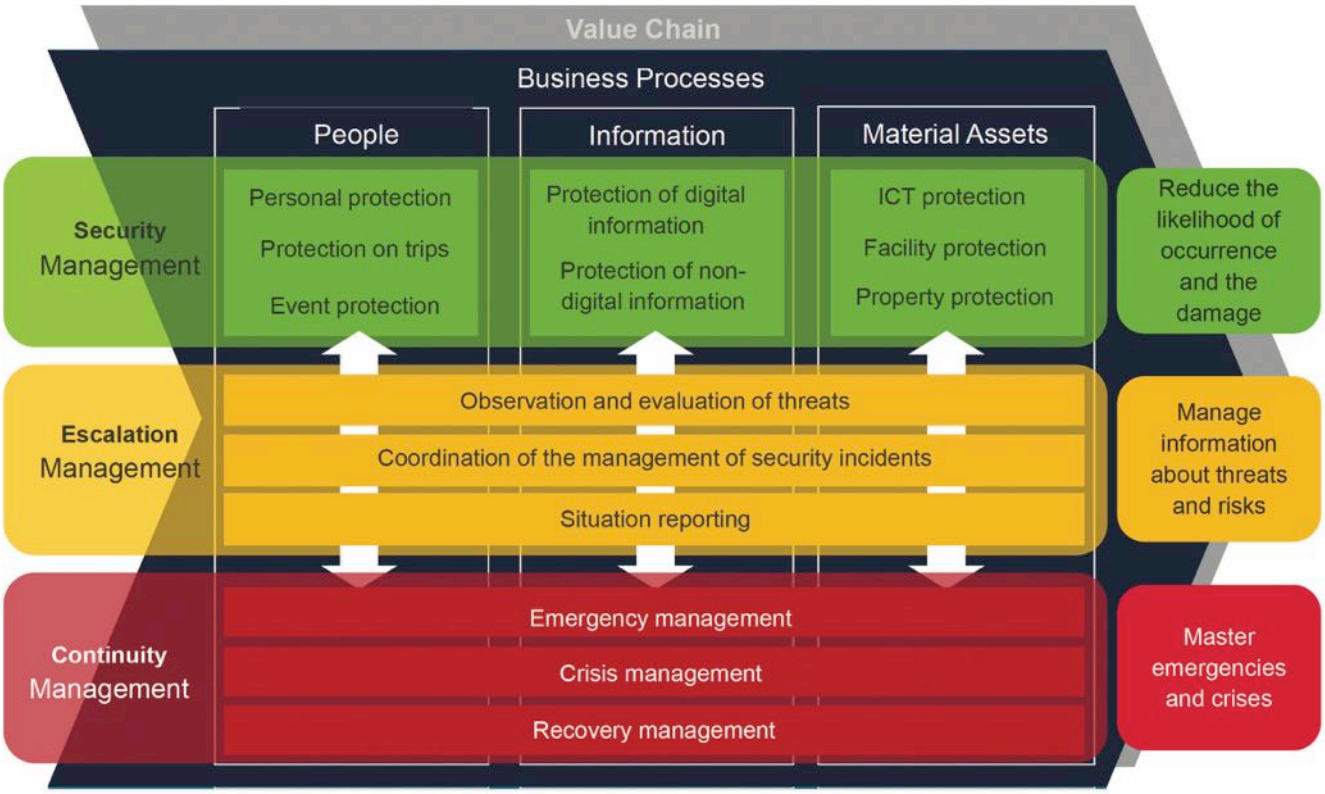
risk associato alla supply chain bisogna identificare e contestualizzare i "modelli di attacco" (Threat model) anche a seguito di un'azione di cyber threat intelligence. Per capirci: quando parliamo di attacchi alla supply chain si passa dalla contraffazione degli apparati all'esfiltrazione dei dati, una condizione che deve imporre un deciso innalzamento della soglia di attenzione insieme a un potenziamento degli strumenti di monitoraggio.

In che cosa consiste l'attività di monitoraggio?

In letteratura si parla di varie opzioni di protezione e il monitoraggio è solo una di queste. La sequenza ideale procede dalla Gestione dell'identità alle azioni di ripristino. Un'organizzazione si può definire resiliente, laddove si definisce resiliente per la capacità di mettere in atto una corretta "Gestione dell'identità" attraverso questi passaggi: il personale viene identificato, le sue credenziali autenticate, e infine viene autorizzato ad accedere alle risorse di produzione e distribuzione, in base al proprio ruolo e ai propri compiti. Poi ci sono i Programmi di addestramento e la sensibilizzazione del personale che servono a incrementare la consapevolezza e la capacità di prevenzione e reazione agli incidenti di sicurezza. Molto importante è la definizione delle policy di sicurezza, cioè dei processi e delle procedure di protezione dei processi produttivi e distributivi *(Information Protection Processes and Procedures)*.

Possiamo spiegare, in sintesi, per quale ragione?

Perché da queste dipendono le procedure di manutenzione, che sono di enorme importanza e che vanno pianificate e controllate secondo le *policy di sicurezza*. È infatti fondamentale applicare quelle soluzioni tecniche necessarie a proteggere le comunicazioni che intercorrono tra fornitori e clienti per arrivare al *Response Planning*, il piano di risposta agli incidenti informatici veri e propri. Solo in un secondo momento può intervenire il monitoraggio con un'attività detta di *Security Continuous Monitoring*, che si espleta quando l'infrastruttura ICT e gli asset aziendali vengono attivamente monitorati per rilevare eventuali incidenti di sicurezza in corso o passati. Nel caso di un attacco portato a segno vanno, in particolare, eseguite le attività di ripristino in maniera coordinata con le parti interessate, sia interne che esterne.



Responsabilità condivisa e rischio reputazionale

Il rischio reputazionale va trattato con gli stessi strumenti che vengono utilizzati per tutelare la sicurezza di servizi e prodotti?

Bisogna considerare che il rischio reputazionale è sempre altissimo, ma una comunicazione onesta e trasparente fa la differenza. Ormai tutti sappiamo che non esiste il rischio zero nel cyberspace, quindi l'affidabilità di un'azienda non può fondarsi sull'assunto presuntuoso che caratterizza la posizione di chi è convinto di non subire attacchi o nella negazione di un incidente, quanto sulla capacità di gestire correttamente l'incidente e di coinvolgere gli *stakeholder* nel loro ruolo di soggetti interessati dall'incidente stesso.

Nell'intrattenere rapporti commerciali esiste un particolare rischio che è quello relativo al sistema paese con cui ci si confronta. Quando ci si confronta con organizzazioni che operano oltre frontiera come si definisce il perimetro delle responsabilità?

A giudicare dalla cronaca recente dei cyber attacchi, le aziende non sono tutte sufficientemente attrezzate su questo versante così delicato. Oggi con la Nis e la legge sul Perimetro Nazionale di Sicurezza Cibernetica le cose stanno cambiando. La *Golden Power* stessa ci aiuta a definire il concetto di responsabilità, ma l'errore è dietro l'angolo e i problemi causati dalla dipendenza da sistemi legacy penalizza le aziende meno avvertite.

BIO

Arturo Di Corinto è ricercatore e docente in psicologia cognitiva e della comunicazione. Professore universitario di tecniche di giornalismo, digital media e creative writing. Attualmente è ricercatore presso il Center for Cybersecurity and International Relations Studies dell'Università di Firenze. Già docente alla Stanford University, alla Sapienza di Roma e all'Accademia di Belle Arti di Carrara, è stato direttore del Master in comunicazione pubblica e istituzionale presso Link Campus University Roma. Ha diretto il laboratorio Open Source - Logos - della Sapienza di Roma. È stato Direttore della Comunicazione del Laboratorio Nazionale di Cybersecurity, ed ha servito in diverse posizioni presso la Presidenza del Consiglio dei Ministri come esperto di comunicazione pubblica, presso il Cnipa, oggi Agid, e presso il Dipartimento per la Digitalizzazione e l'Innovazione della PA (DDI). Consulente RAI TV, UE, ONU, ISFOL, CGIL. Giornalista esperto di innovazione, ha lavorato per Il Sole24Ore, Wired e L'Espresso. Attualmente scrive per Il Manifesto e La Repubblica. Ha un blog su Il Fatto Quotidiano e su AGI. Ha pubblicato oltre 40 libri sul mondo digitale, tra cui Revolution Open Source (Feltrinelli/Apogeo, 2005), I nemici della Rete (Rizzoli, 2011), Un dizionario hacker (Manni, 2014), "Trent'anni di futuro. Quando Internet è arrivata in Italia" (Manni Editori, 2017). Autore e inviato per il programma televisivo di Rai Uno "Codice. Tutta la vita è digitale", il suo ultimo libro è Riprendiamoci la rete! Piccolo manuale di autodifesa digitale per giovani generazioni (Eurilink, 2019).

Contatti: a.dicorinto@unilink.it / www.dicorinto.it / @arturodicorinto

L'Enterprise Governance Risk and Compliance *è una disciplina che sta prendendo piede. Le norme, quelle relative alla certificazione, ma non solo, sono adeguate a garantire la sicurezza della* supply chain *in tutto il suo sviluppo e articolazione?*

Non bastano ma aiutano. Piuttosto mi chiederei perché così poche realtà sono certificate e perché lo sono solamente in certi contesti. Anche qui, mi auguro che le nuove norme possano determinare un cambiamento culturale profondo, che è quello di cui abbiamo maggiormente bisogno. ■

Rischi Informatici di Terze Parti, come gestirli

Autore: Lisa Ventura

Ogni giorno, senza eccezioni, molte aziende subiscono attacchi alla sicurezza informatica che possono essere onerosi e distruttivi. Questi attacchi possono anche danneggiare seriamente la loro reputazione, incidere sui profitti, sull'immagine aziendale e sulla fiducia dei consumatori. Possono comportare la perdita di clienti, di vendite e la riduzione dei profitti. Le leggi sulla protezione dei dati e sulla privacy richiedono alle organizzazioni di gestire la sicurezza di tutti i dati personali in loro possesso, sia del personale che dei loro clienti. Se questi dati vengono deliberatamente o accidentalmente compromessi, le organizzazioni possono essere soggette a sanzioni normative e a pesanti multe.

Oltre a tutto ciò, quando parliamo di vasti ecosistemi di dati, c'è un altro problema ancora più critico che molte grandi aziende devono affrontare: la gestione della privacy e dei rischi informatici relativi alle informazioni che forniamo alle terze parti e oltre. Questo è noto come rischio informatico di terze parti.

Secondo uno studio del Ponemon Institute, nel 2020 le organizzazioni di terze parti rappresentavano il 42% di tutti i casi di violazione dei dati, scendendo solo leggermente dal 44% dei casi nel 2008. Le violazioni dei dati di terze parti sono ancora la forma più onerosa di violazioni a causa di ulteriori spese di consulenza per indagare su di esse.

Le aziende spesso condividono i dati con i service provider e i loro subappaltatori per migliorare la fornitura dei servizi e ridurre i costi. In questo processo, i dati cambiano proprietà più volte mentre la documentazione, spesso contenente informazioni che identificano direttamente la loro attività e i clienti, viaggia attraverso l'ecosistema dei dati. Le terze parti sono spesso custodi delle informazioni originali, quindi è fondamentale sapere quali misure di cyber security stanno adottando per salvaguardare queste informazioni più a valle della value chain.

Se una terza parte con cui hai a che fare venisse violata, potrebbe costringere la tua organizzazione a rispondere a incidenti che sono completamente al di fuori del tuo controllo o che hanno origine da una

fonte indiretta. Sfortunatamente, l'effetto a catena sulla tua organizzazione potrebbe essere altrettanto grande come se la tua organizzazione subisse direttamente un attacco informatico. Potresti non avere l'obbligo di risponderne direttamente in base alle attuali normative sulla violazione dei dati, ma la tua organizzazione potrebbe comunque subire elevati danni reputazionali a causa dell'incidente. Inoltre, i tuoi clienti potrebbero anche essere maggiormente bersaglio di criminali informatici che cercano di sfruttare una violazione dei dati indipendentemente da come o dove è iniziato l'incidente originale.

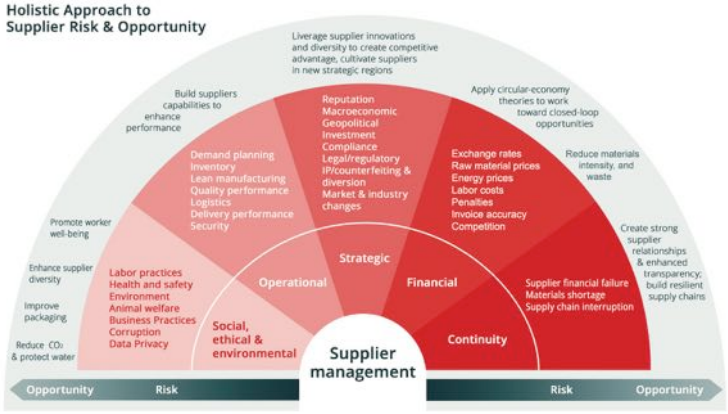
Indipendentemente dal settore in cui ti trovi, dalla sanità all'alberghiero, devi considerare i rischi della tua documentazione che viaggia attraverso grandi ecosistemi di dati. Come puoi gestire i rischi per la protezione dei dati quando una grande quantità di dati provenienti dalla tua organizzazione viaggia fuori dal tuo controllo e nelle mani di terze parti? Con l'aumento del numero di terze parti collegate e delle tecniche di attacco informatico e vettori di rischio, le best practices di gestione del rischio di terze parti (TPRM) si stanno evolvendo rapidamente. Ecco alcuni modi in cui puoi gestire il rischio informatico di terze parti all'interno della tua organizzazione:

Classificare i fornitori in categorie specifiche in base al loro rischio

Per farlo con successo, dovresti i seguenti passaggi:

‣ Costruire un framework per la categorizzazione di terze parti

Ciò dovrebbe aiutare a identificare quali partner necessitano di una valutazione più approfondita in base al loro ruolo nelle attività dell'organizzazione, nonché alle dimensioni e alla criticità del rapporto commerciale.



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/

‣ Sviluppare un workflow per esaminare l'intersezione tra criticità e rischio

Se lavori dal framework di categorizzazione, i risk manager saranno in grado di utilizzare strumenti di quantificazione del rischio di sicurezza informatica per creare portafogli delle terze parti, in questo modo, il rischio informatico e l'impatto/criticità aziendale possono essere considerati simultaneamente.

‣ Stabilire una cadenza stringente per rivolgersi frequentemente ai fornitori ad alto impatto

Ciò dovrebbe essere fatto attraverso un approccio analitico che combini insieme criticità aziendale e rischio.

▸ Garantire un rischio appropriato quando si tratta di trasferimento di dati

Un approccio semplice di questo tipo tiene conto dell'intersezione tra rischio e criticità del fornitore e spesso richiede che i fornitori dispongano di un'assicurazione con protezione integrativa.

Le organizzazioni possono anche utilizzare queste quattro soluzioni per la gestione dei rischi di terze parti:

▸ Mappare adeguatamente il flusso dei dati

Mantenere i record di dati durante tutto il ciclo di vita, aiuterà a prioritizzare la data governance e a implementare meccanismi forti o tracciare facilmente i dati tra i fornitori. Tale disciplina dovrebbe essere applicata attraverso l'assegnazione di *data ownership* e *accountability* implementando un sistema di controllo, identificando data custodians e applicando security policy.

▸ Valutare in che modo le terze parti proteggono i propri dati

Valutare le terze parti in base agli attributi di rischio quali il volume delle transazioni, il tipo di sensibilità dei dati e i dati regolamentati e prendere in considerazione l'impatto dell'evoluzione della privacy e delle regolamentazioni sui dati in base al luogo dove i dati vengono elaborati. Condurre valutazioni e assessment di queste entità e dei controlli di sicurezza che hanno implementato per la protezione delle informazioni dell'organizzazione.

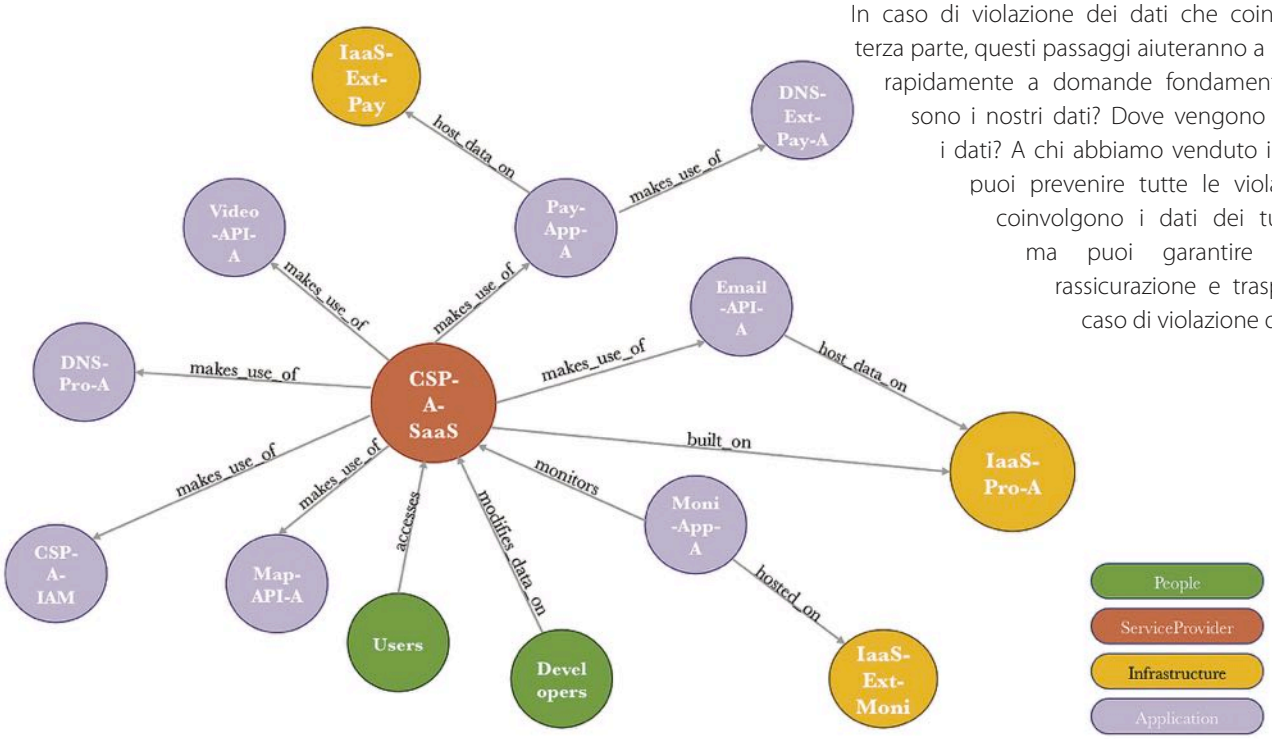
▸ Utilizzare i migliori standard e best practice del settore

Creare profili di rischio attraverso l'uso di cyber security assessment delle terze parti. I report di intelligence sulle minacce informatiche forniscono dati comparati tra terze parti rispetto alle best practice del settore e queste informazioni potrebbero essere la base per la creazione di profili di rischio.

▸ Creare un playbook degli incidenti informatici e sottoporlo a stress test

Assicurarsi che il piano di risposta agli incidenti informatici sia coerente con gli altri piani definiti per affrontare le minacce chiave alle tue operazioni aziendali. I componenti dovrebbero includere la formazione di tutti i membri dell'organizzazione e lo svolgimento di una prova di pianificazione delle minacce, nonché l'assegnazione della responsabilità per la comunicazione con le parti interessate e i media, in caso di violazione dei dati. Il playbook dell'incidente dovrebbe essere sottoposto a stress test con scenari realistici e includere un portale clienti interattivo per la condivisione di informazioni e una hotline specifica per rispondere alle domande del pubblico.

In caso di violazione dei dati che coinvolga una terza parte, questi passaggi aiuteranno a rispondere rapidamente a domande fondamentali: Come sono i nostri dati? Dove vengono conservati i dati? A chi abbiamo venduto i dati? Non puoi prevenire tutte le violazioni che coinvolgono i dati dei tuoi clienti, ma puoi garantire chiarezza, rassicurazione e trasparenza in caso di violazione dei dati. ■



Tipologia e contenuto dei contratti di outsourcing. Gli impatti dei recenti interventi normativi.

Autore: Maria Cristina Daga

Negli ultimi anni la sicurezza della supply-chain nel mondo finanziario è stata posta sotto attenzione da parte dei regolatori nazionali e europei. Il modello di sourcing di governo e di responsabilità posta in capo agli enti e agli istituti finanziari è stato disegnato e via via rafforzato, tanto da trovare difficilmente eguali in altri settori.

BIO

Maria Cristina Daga è Avvocato, Associate Partner at P4I. Si occupa di tematiche legali e contrattuali nell'ambito della sicurezza informatica del settore bancario. La sua esperienza nel settore bancario include la gestione delle esternalizzazioni con riferimento alla Circolare di Banca d'Italia n. 285/2013 e alle Linee Guida EBA. Nel mondo dei servizi di pagamento ha sviluppato competenze in materia di trasparenza bancaria, sicurezza dei pagamenti e risoluzione delle frodi on line, anche avanti l'ABF e l'Autorità Giudiziaria.

Gli adempimenti, anche di natura contrattuale, posti in capo agli istituti finanziari nonché ai fornitori di servizi trovano la loro cornice normativa nelle ***"Linee Guida (EBA/GL/2019/02) in materia di esternalizzazioni"*** dell'Autorità Bancaria Europea (EBA, European Banking Authority), del 25 febbraio 2019.

La costruzione di un contratto che contenga previsioni chiare e puntuali nonché una struttura in linea con i contenuti minimi disciplinati dalla normativa è il primo strumento di *compliance* in grado di assicurare una vita stabile e duratura al rapporto con i fornitori di servizi. Altresì, è lo strumento che garantisce - e che dovrebbe garantire - le possibili *"vie di fuga"* dal rapporto con gli stessi fornitori.

L'obiettivo della presente trattazione è quello di illustrare il perché sia importante redigere un testo contrattuale puntuale e in linea con le reciproche esigenze dei contraenti.

Scenario normativo: cosa è cambiato e cosa cambierà

Il settembre del 2020 rappresenta un punto di partenza importante per la resilienza operativa digitale nel settore finanziario e ciò anche in considerazione del notevole impatto che gli interventi regolatori avranno

sui contratti di outsourcing rispetto ai nuovi obblighi da disciplinare.

In data 23 settembre 2020 è stato pubblicato il **34° aggiornamento della Circolare 285/2013** che, di fatto, recepisce, in attuazione, gli Orientamenti dell'EBA in materia di esternalizzazione (Guidelines on outsourcing, EBA/GL/2019/02). Le principali modifiche riguardano il Capitolo 3 *"Il sistema dei controlli interni"* e il Capitolo 4 *"Il sistema informativo"* della Parte I, Titolo IV, della Circolare.

Si segnala sin da subito che, con la nuova versione della Circolare 285/2013, non si parla più di *"funzione operativa importante"* ma di *"funzione essenziale o importante"*, così come previsto dal Titolo IV, Capitolo 3, Sezione I, art. 3.

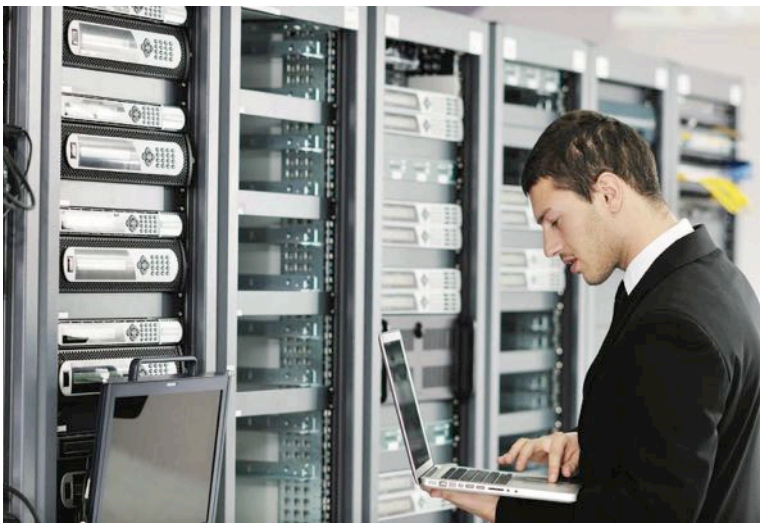
Tra i vari interventi di modifica effettuati nella Circolare, vi è anche l'inserimento nei contratti di outsourcing di clausole dettagliate su diritti di accesso e audit, sicurezza e integrità dei dati, strategie di uscita e continuità operativa. In altri termini, la Circolare 285 rinvia pedissequamente agli Orientamenti dell'EBA (paragrafo 13 e ss) per quanto concerne l'elencazione tassativa delle condizioni contrattuali da prevedere quali requisiti minimi, fatta eccezione per le specifiche previsioni nell'ambito dell'esternalizzazione del sistema informativo previste dalla Sezione VI del Capitolo 4 che sopravvivono alla modifica normativa introdotta con l'aggiornamento EBA.

Inoltre, in data 24 settembre 2020 la Commissione europea ha presentato una proposta di regolamento sulla resilienza operativa digitale nel settore finanziario che si pone il duplice obiettivo di ridurre i rischi legati all'utilizzo di tecnologie informatiche nell'ambito finanziario e di superare la frammentazione normativa all'interno dell'Unione. La disciplina di settore si affiancherebbe al quadro normativo applicabile in materia di sicurezza informatica introdotto con la Direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (la c.d. Direttiva NIS).

Il regolamento è concepito per garantire un solido meccanismo di monitoraggio dei rischi relativi alle tecnologie digitali o dell'informazione offerte ed erogate da terzi soggetti. Tale obiettivo si realizzerà in primo luogo, con il rispetto delle norme basate su principi che si applicano ai sistemi di monitoraggio, da parte degli istituti finanziari, del rischio derivante dalla fornitura di servizi erogati da terzi. In secondo luogo, il regolamento dovrà armonizzare gli elementi essenziali del servizio e dei rapporti con i fornitori terzi in tutte le fasi del rapporto con esso, ovvero la stipula, l'esecuzione, l'estinzione e la fase post-contrattuale.

Nell'esigenza di rafforzare i meccanismi di controllo del rischio si fa sempre maggiore la convinzione che nonostante esistano norme generali in materia di esternalizzazione, contenute in atti legislativi adottati dall'Unione nel settore dei servizi finanziari, il monitoraggio della dimensione contrattuale non è sempre saldamente radicato in tale legislazione e mai così effettivo da renderlo un sistema efficace ai fini della rilevazione dei rischi. **In altri termini, il monitoraggio della dimensione contrattuale dovrà essere sostanziale e non più meramente formale.**

Nella relazione del regolamento, si legge che *"i contratti che disciplinano il rapporto dovranno contenere una descrizione completa dei servizi, l'indicazione*



delle località in cui i dati devono essere trattati, descrizioni complete del livello dei servizi accompagnate da obiettivi di prestazione quantitativi e qualitativi, disposizioni pertinenti in materia di accessibilità, disponibilità, integrità, sicurezza e protezione dei dati personali, nonché garanzie per l'accesso, il ripristino e la restituzione in caso di inadempienze dei fornitori terzi di servizi di TIC, termini di preavviso e obblighi di segnalazione dei fornitori terzi di servizi di TIC, diritti di accesso, ispezione e audit da parte dell'entità finanziaria o di un terzo designato a tale scopo, chiari diritti di estinzione e strategie di uscita dedicate."

Tali elementi contrattuali, di fatto, non aggiungono nulla di nuovo rispetto a quanto già previsto da EBA e ora anche da Banca d'Italia, tuttavia uno spunto interessante è rappresentato dal seguente passaggio: *"Dato che alcuni di questi elementi contrattuali possono essere standardizzati, il regolamento incoraggia il ricorso volontario a clausole contrattuali standard per l'utilizzo del servizio di cloud computing che dovranno essere definite dalla Commissione.* Tuttavia, è già da anni che la Commissione tenta di intervenire

sulla tipicità dei contratti cloud attraverso l'adozione di clausole standard, ma ad oggi nessuna pronuncia risulta essere stata mai emessa sul tema. L'utilizzo volontario di clausole contrattuali standard elaborate dalla Commissione per i servizi di cloud computing potrebbe costituire un'ulteriore preziosa risorsa per gli istituti finanziari e per i loro fornitori di servizi, accrescendo il livello di certezza del diritto in merito all'utilizzo di servizi di cloud computing da parte del settore finanziario, in completa conformità con le prescrizioni e le aspettative definite dal regolamento sui servizi finanziari.

In altri termini, la costruzione di un contratto solido, oltre che a rispettare i requisiti minimi previsti dalla norma, deve garantire – nel breve e nel lungo periodo – le tutele reciproche delle parti contraenti ed essere costantemente monitorato sia con riferimento alle performance del fornitore, sia con riferimento alla corretta esecuzione degli obblighi ivi previsti.

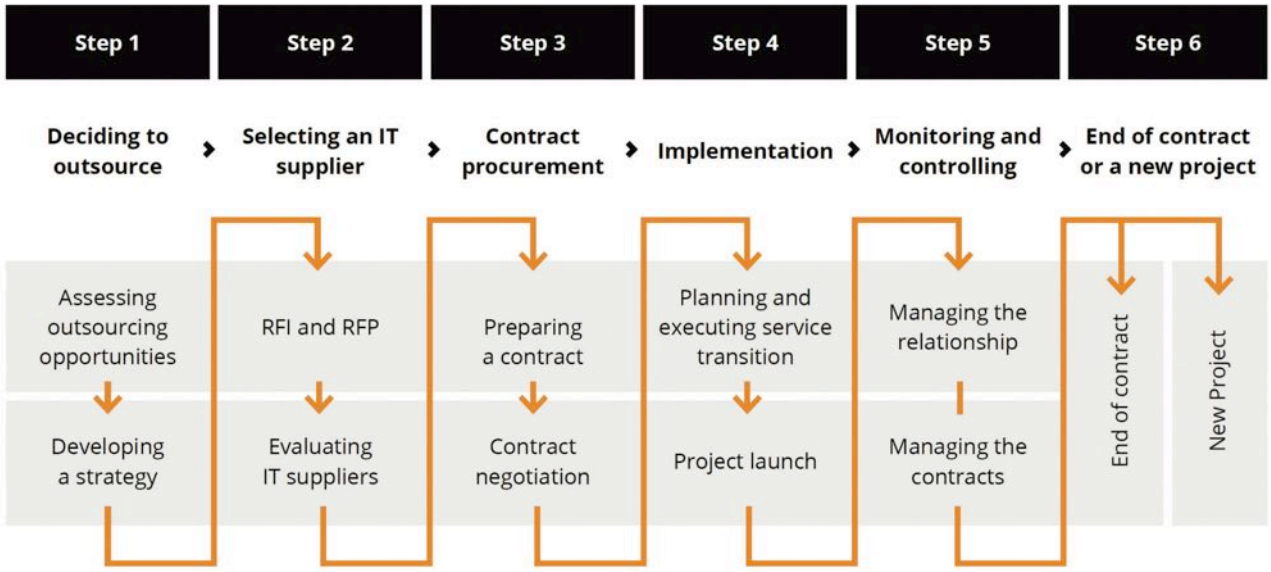
Perché è importante effettuare una corretta valutazione preventiva del fornitore per una completa impostazione dei contenuti contrattuali?

La valutazione preliminare dei rischi dell'accordo e del fornitore è lo strumento che consente di individuare, in modo corretto e completo, le necessarie previsioni contrattuali finalizzate alla mitigazione dei rischi e alla definizione di un sistema di monitoraggio in grado di rilevare l'effettiva performance del fornitore, anche in termini di rispetto dei livelli di servizio concordati.

Dunque, la valutazione dei rischi dovrebbe essere condotta sulla base di criteri chiari e puntuali e le metodologie di valutazione dovrebbero essere robuste e testate sotto differenti scenari di stress, facendo riferimento a più fonti informative. Inoltre, le risultanze di valutazioni basate su metodi quantitativi dovrebbero essere integrate dalle valutazioni qualitative, al fine di mitigare il rischio di modello, richiedendosi anche un aggiornamento costante della documentazione.

Pertanto, prima di concludere l'accordo di esternalizzazione, indipendentemente dalla tipologia di esternalizzazione [quindi dalla criticità e/o essenzialità], gli istituti finanziari sono tenuti a:

1. valutare se l'accordo di esternalizzazione riguarda una funzione essenziale o importante;
2. valutare se le condizioni di vigilanza per l'esternalizzazione siano soddisfatte;
3. individuare e valutare tutti i rischi dell'accordo di esternalizzazione conformemente a quanto previsto dalle Linee Guida EBA;
4. effettuare un'adeguata due diligence sul potenziale fornitore di servizi;
5. individuare e valutare i conflitti di interesse che l'esternalizzazione può generare.



In tal senso, EBA indica i criteri di rischio su cui orientare tale analisi, ponendo l'accento – tra le altre cose – sulla necessità di ***"individuare e classificare le funzioni interessate e i relativi dati e sistemi in base alla loro sensibilità e alle misure di sicurezza richieste"***, nonché di "***effettuare un'analisi approfondita, basata sul rischio***, *delle funzioni e dei relativi dati e sistemi che potrebbero essere o che sono stati esternalizzati e fronteggiare i potenziali rischi, in particolare i rischi operativi, inclusi i rischi legali, ICT, di conformità e reputazionali, nonché eventuali limitazioni alle attività di controllo connesse ai paesi in cui sono prestati o è probabile che siano prestati i servizi esternalizzati e in cui sono conservati o è probabile che siano conservati i dati".*

Tra i principali adempimenti relativi alla valutazione dell'accordo e del fornitore, gli istituti finanziari sono dunque tenuti a costruire e/o utilizzare i parametri definiti nella propria **tassonomia dei servizi**, al fine di individuare e classificare la corretta qualifica dell'approvvigionamento, in termini di acquisto o di esternalizzazione.

In altre parole, in coerenza con la tassonomia dei servizi sarà, di fatto, necessario effettuare una completa **mappatura delle diverse tipologie di fornitura**, supportata e guidata dai criteri di valutazione dell'esternalizzazione (anche attraverso regole di ingaggio ben definite).

Nell'ambito del processo per la gestione degli approvvigionamenti, ove si inneschi la fase valutativa, sarà inoltre necessario definire i ruoli e le responsabilità di tutti i soggetti e/o funzioni coinvolte nella gestione dell'accordo di esternalizzazione, inclusi quelli decisionali, nonché predisporre la documentazione necessaria per garantire *l'accountability* di questa preliminare fase valutativa.

Definito il processo valutativo ed effettuata l'analisi dei rischi del fornitore e dell'accordo secondo i criteri previsti da EBA, gli istituti finanziari potranno articolare le previsioni degli accordi contrattuali in funzione degli scenari di rischio rilevati.

Quali sono i contenuti minimi che disciplinano i contratti FOI e i contratti di esternalizzazione? Quali ulteriori peculiarità per i servizi cloud?

Gli istituti finanziari devono assicurare che l'esternalizzazione di funzioni relative alle attività bancarie e/o finanziaria, avvenga solo se siano soddisfatti i requisiti minimi indicati dalle linee guida EBA.

I contratti di esternalizzazione devono contenere una descrizione della funzione esternalizzata che verrà svolta, gli obblighi finanziari delle parti e la durata del contratto. Gli enti e gli istituti finanziari dovrebbero assicurare che la funzione di audit interno sia in grado di esaminare la funzione esternalizzata utilizzando un approccio basato sul rischio, così da garantire i diritti di accesso di informazioni e di audit.

L'esternalizzazione comporta il trattamento di dati personali o riservati; pertanto, gli enti e gli istituti finanziari devono accertarsi che il fornitore

di servizi adotti misure tecniche e organizzative adeguate sia per proteggere tali dati, sia per assicurare gli adeguati standard di sicurezza informatica. L'accordo di esternalizzazione deve consentire espressamente all'ente o all'istituto finanziario il diritto di recesso, ponendo termine al contratto, conformemente al diritto applicabile, nel caso in cui si verificassero specifiche situazioni indicate nelle linee guida. Gli accordi di esternalizzazione tra enti e fornitori di servizi devono fare riferimento ai poteri di raccolta delle informazioni e di indagine delle autorità competenti e delle autorità di risoluzione di cui all'articolo 65, paragrafo 3, della direttiva 2013/36/UE e all'articolo 63, paragrafo 1, lettera a), della direttiva 2014/59/UE nei confronti dei fornitori di servizi situati in uno Stato membro, e devono altresì assicurare tali diritti nei confronti dei fornitori di servizi situati in paesi terzi. Gli enti e gli istituti finanziari devono assicurarsi di poter porre termine agli accordi di esternalizzazione senza interrompere indebitamente le proprie attività operative, senza limitare il rispetto degli obblighi normativi e senza pregiudicare la continuità e la qualità dei servizi forniti ai propri clienti. Infine, l'accordo di esternalizzazione deve facilitare il trasferimento della funzione esternalizzata a un altro fornitore o la sua reintegrazione all'interno dell'istituto bancario. L'accordo pertanto dovrà indicare gli obblighi in capo all'attuale fornitore in caso di trasferimento della funzione esternalizzata, obblighi concernenti anche il trattamento dei dati e l'indicazione di un periodo di transizione durante il quale il fornitore continuerebbe a svolgere la funzione esternalizza, così riducendo i rischi di interruzione del servizio.

Nel caso in cui la banca esternalizzasse una funzione essenziale o importante, le linee guida richiedono delle misure più stringenti e specifiche oltre quelle previste per i contratti di esternalizzazione. Nello specifico, le linee guida prevedono contenuti minimi quali la chiara descrizione della funzione esternalizzata che viene svolta, la normativa di riferimento, una clausola che indichi se la sub-esternalizzazione della funzione essenziale o importante sia consentita, il luogo in cui la funzione verrà esternalizzata e il luogo in cui verranno conservati e trattati i relativi dati. L'accordo deve prevedere anche il diritto dell'ente o dell'istituto finanziario di effettuare un monitoraggio costante della performance del fornitore di servizi; gli obblighi di reportistica che il fornitore di servizi è tenuto ad effettuare nei confronti dell'istituto bancario; una clausola che indichi se il fornitore debba stipulare un'assicurazione obbligatoria contro determinati rischi; i requisiti per l'attuazione e la verifica dei piani di emergenza dell'impresa; disposizioni che assicurino l'accesso ai dati di cui la banca è titolare in caso di insolvenza, risoluzione o cessazione dell'attività del fornitore di servizio; l'obbligo del fornitore di servizi di cooperare con le autorità competenti e le autorità di risoluzione dell'ente o dell'istituto finanziario, e con altri soggetti da questi designati; il diritto illimitato degli enti, degli istituti finanziari e delle autorità competenti di ispezionare e sottoporre a verifiche di audit il fornitore di servizi per quanto riguarda la funzione essenziale o importante esternalizzata. Con riferimento ai diritti di accesso, le banche nell'ambito dell'accordo di esternalizzazione di funzioni essenziali o importanti, devono assicurare che il fornitore di servizi riconosca loro e alle autorità competenti, comprese le autorità di risoluzione, e a qualsiasi altro soggetto nominato dagli enti o dalle autorità competenti, pieno accesso

a tutti i locali aziendali, diritti illimitati di condurre ispezioni e verifiche di audit in relazione all'accordo di esternalizzazione. Nel contratto di esternalizzazioni di funzioni essenziali o importanti, gli enti e gli istituti finanziari devono dotarsi di una strategia di uscita documentata, che sia in linea con la propria politica di esternalizzazione e i propri piani di continuità operativa, tenendo conto quanto meno della possibilità di indicare i seguenti termini agli accordi di esternalizzazione: dissesto del fornitore di servizi; deterioramento della qualità della funzione eseguita e interruzioni effettive o potenziali delle attività causate dall'inadeguata o mancata esecuzione della funzione; insorgenza di rischi rilevanti per lo svolgimento adeguato e continuativo della funzione. Infine, qualora durante la vigenza del contratto dovesse determinarsi una circostanza che possa far ritenere esistente o potenzialmente esistente un conflitto di interessi fra le parti, ciascuna delle parti dovrà comunicare all'altra per iscritto tale circostanza.

Il fine è quello di valutare l'adozione di opportune cautele per gestire la circostanza stessa in modo da limitare e/o monitorare gli effetti del conflitto di interessi.

Con riferimento alle peculiarità dei contratti di esternalizzazione cloud si evidenzia una particolare attenzione alla sicurezza dei dati e dei sistemi informatici. Infatti, gli enti e gli istituti finanziari devono definire i requisiti di sicurezza dei dati e dei sistemi nell'ambito dell'accordo di esternalizzazione e monitorarne costantemente il rispetto. Nel caso dell'esternalizzazione a fornitori di servizi cloud e di altri accordi di esternalizzazione che comportano il trattamento o il trasferimento di dati personali in paesi extra UE o riservati, gli enti e gli istituti finanziari devono adottare un approccio basato sul rischio con riferimento al luogo (paese o regione) dove sono conservati e trattati i dati e alla sicurezza delle informazioni. Inoltre, l'ente o l'istituto finanziario devono verificare che chiunque esegua la verifica di audit, abbia le capacità, le conoscenze adeguate e necessarie per eseguire tali verifiche di audit e/o valutazioni efficaci. Lo stesso vale per il personale

dell'ente o dell'istituto che esamina le certificazioni di terzi o le risultanze delle verifiche di audit effettuate dai fornitori di servizi.

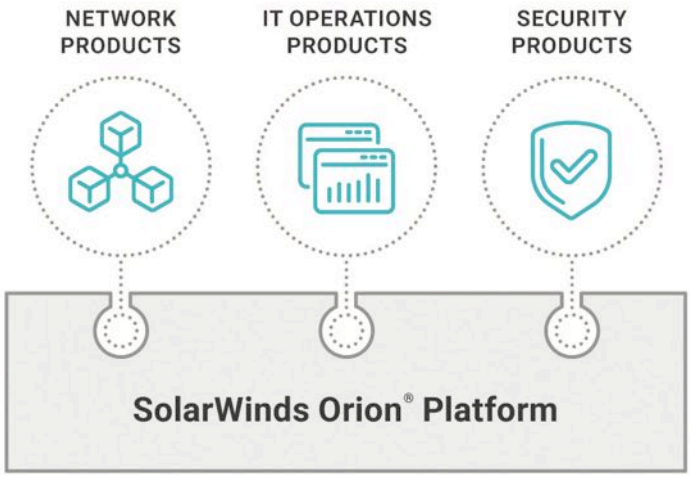
La disciplina del subappalto nei contratti di outsourcing

Se il contratto di esternalizzazione prevede la possibilità che il fornitore di servizi sub-esternalizzi funzioni essenziali o importanti ad altri fornitori di servizi, gli enti e gli istituti finanziari devono tener conto dei rischi associati alla sub-esternalizzazione (compresi i rischi aggiuntivi che possono sorgere se il subcontraente ha sede in un paese terzo o in un paese diverso da quello del fornitore di servizi) e del rischio che le lunghe e complesse catene di sub-esternalizzazione riducano la capacità degli enti o degli istituti finanziari di vigilare sulla funzione essenziale o importante esternalizzata, nonché la capacità delle autorità competenti di esercitare una efficace vigilanza su essi.

L'accordo deve individuare specificatamente le tipologie di attività che sono escluse dalla sub-esternalizzazione. Le linee guida EBA inoltre affermano che gli istituti finanziari devono acconsentire alla sub-esternalizzazione solo nel caso il cui il subcontraente si impegni a rispettare tutte le leggi, gli obblighi normativi e gli obblighi contrattuali applicabili, riconoscendo al medesimo ente e all'autorità competente gli stessi diritti contrattuali di accesso e di audit previsti per il fornitore di servizi. Il fornitore di servizi potrà essere chiamato a supervisionare i subfornitori di servizi. Qualora dal processo di sub-esternalizzazione dovessero emergere o aumentare dei rischi sostanziali per la funzione essenziale o importante, l'istituto finanziario potrebbe esercitare il proprio diritto di opporsi alla sub-esternalizzazione e/o porre termine al contratto. ■

Monitoraggio efficace delle terze parti. Modalità e Tecniche per verificare la resilienza dei fornitori.

Autori: Paolo Carcano e Lorenzo Romaccioni



L'evoluzione delle minacce cyber correlate alle terze parti / quarti parti

Oggi qualunque organizzazione, piccola o grande che sia, opera in un contesto sempre più dinamico, interconnesso ed integrato. L'introduzione e l'utilizzo di nuove tecnologie ha allargato i confini delle singole organizzazioni, rendendo necessaria un'attività di presidio estesa a tutti i principali stakeholder, fornitori ed outsourcer inclusi. Accanto a questa rapida evoluzione tecnologica, anche gli attacchi cyber sono cresciuti in modo esponenziale: tra le nuove tipologie di attacco, la catena di fornitura diventa un target di primaria importanza per procurare impatti diretti ad una specifica organizzazione. É di poche settimane fa la notizia dell'attacco hacker alla supply chain della piattaforma Orion di SolarWinds che ha consentito al gruppo hacker Cozy Bear o APT29, di spiare per mesi, più di 250 fra aziende e agenzie governative USA. Di fatto il monitoraggio dei fornitori diviene imprescindibile per garantire la sicurezza dell'azienda stessa.

Le organizzazioni che hanno adottato controlli sulle terze parti sono solite circoscriverli alla fase contrattuale e di prima negoziazione. Tuttavia, in questo caso le attività di assessment a cui sottoponiamo i fornitori forniscono una fotografia statica della sicurezza.

Tale "snapshot", infatti, non riflette quel dinamismo quasi frenetico in cui il fornitore opera né tantomeno i rischi informatici che quotidianamente fronteggia.

Senza una visione continua sul fornitore/outsourcer e sulla relativa security posture, le aziende non possono comprendere appieno i rischi indiretti che devono affrontare e che derivano dalla propria filiera di fornitori.

Per mantenere una vista quanto più precisa ed aggiornata della cyber posture dei propri fornitori e outsourcer, è necessario avvalersi di un mix tra attività "point-in-time", tipicamente eseguita durante una valutazione contrattuale o all'inizio del contratto e tecniche continuative di valutazione. In particolare:

- le valutazioni puntuali vengono realizzate per fornitore/outsourcer mediante un'analisi accurata e approfondita della cyber posture dello stesso. Come già accennato tale tipologia di valutazione avviene in genere in fase di prima contrattualizzazione per avere contezza dei livelli di esposizione al rischio informatico della terza parte;

BIO

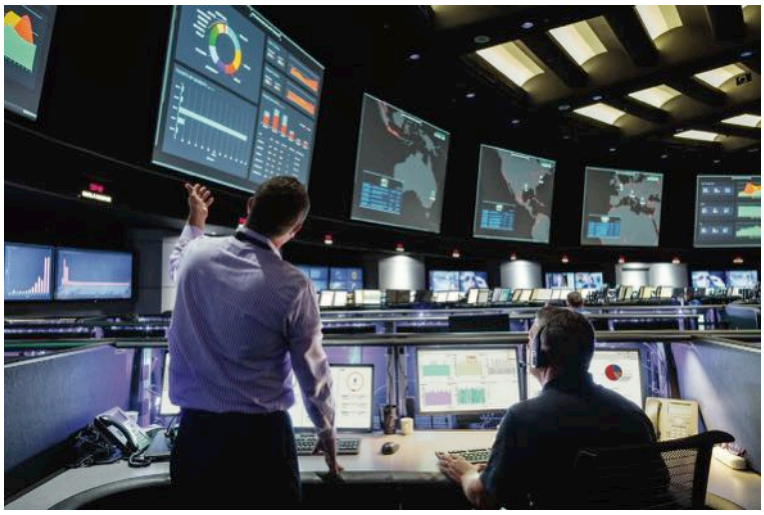
Paolo Carcano è Partner dell'area Technology di PwC Advisory con oltre 21 anni di esperienza nell'ambito dell'Information Security. E' esperto di Security Strategy & Governance, Compliance a normative di sicurezza e Continuità Operativa avendo gestito e coordinato iniziative progettuali all'interno di importanti realtà nazionali e multinazionali con particolare riferimento al mercato dei Financial Services. Dal 2014 in PwC, supporta i principali gruppi bancari sui temi relativi all'Information Security Governance (impianti normativi per la sicurezza), Certificazioni di sicurezza (predisposizione di controlli richiesti per la ISO 27001:2013, Certificazione PCI-DSS), Data Privacy (DPS, Responsabili esterni, Amministratori di sistema, logging), Business Continuity, Identity & Access Management.

Lorenzo Romaccioni è un Senior Associate presso l'ufficio PwC di Milano. Ha maturato una profonda conoscenza del settore Security partecipando ad attività in diversi progetti complessi e intersettoriali (tra cui, ad esempio, finanziario, telecomunicazioni, automotive, trasporti, ecc.) riguardanti le attività di Compliance ISO 27001, monitoraggio dei fornitori, costruzione di SOC, soluzione Cloud, Licensing Compliance Assessment. Negli ultimi tre anni ha gestito diversi progetti all'interno di una delle principali realtà bancarie italiane in merito allo sviluppo e alla progettazione di Security Operation Center (SOC), all'implementazione di processi di governo e gestione della sicurezza e alla definizione delle relative metriche e indicatori.

▸ le tecniche continuative di valutazione, invece, consentono di disporre in "real time" di un quadro aggiornato della cyber posture di un fornitore o outsourcer. Tali tecniche forniscono tuttavia informazioni generiche e non di carattere specifico poiché basano le proprie considerazioni su un'analisi massiva di dati pubblici/configurazioni esposte su internet e come tali difficilmente riconducibili a fenomeni interni all'azienda oggetto di indagine.

Perché ricorrere ai Big Data per una Outside-in Assessment?

Nel corso degli ultimi anni il mercato Cyber ha visto fiorire decine di Vendor - BitSight, SecurityScorecard, RiskRecon solo per citarne alcuni - con soluzione di Big



Data analytics atte a quantificare la cyber posture di una specifica realtà aziendale a partire da un mix di tecniche che sfruttano analisi dei dati pubblici disponibili in rete, tecniche di cyber intelligence ed informazioni di natura economica.

Tutte queste soluzioni scansionano i vari domini web e altre fonti di informazione per correlare veri e propri set informativi ad una specifica realtà aziendale. Sicuramente queste soluzioni basate su piattaforme di Big Data analytics possono migliorare in modo esponenziale i programmi di Third Party Risk Management esistenti, senza poterli comunque sostituire.

Un'analisi basata sui Big Data, infatti, consente di ricollegare facilmente informazioni presenti su sistemi disparati e non collegati - ad esempio social media, e-mail, messaggi di testo, transazioni finanziarie, scambi, viaggi e intrattenimento - e rivelarne affinità e correlazioni. Tuttavia, spesso le fonti informative da cui i Big Data attingono informazioni, possono non risultare aggiornate. C'è sicuramente da aggiungere che alcune aziende fornitrici, soprattutto le PMI che costituiscono la spina dorsale dell'impianto industriale italiano, per scelta o per "obsolescenza" potrebbero generare un numero ridotto di "tracce digitali" nel web, andando così a vanificare qualunque ricorso ai Big Data.

Il consiglio pertanto è quello di avvalersi di strumenti di Big Data analytics non come unica "opzione" per valutare i fornitori, ma come ausilio per avere panoramiche di partenza sulle terze e quarte parti di cui si vuole dare contezza, da approfondire poi per mezzo di assessment specifici.

Tecniche per un monitoraggio efficace delle terze parti

Un monitoraggio continuo ed efficace atto a garantire la sicurezza delle terze parti implica una valutazione basata tanto sulla costanza delle rilevazioni quanto sull'accuratezza delle stesse. La combinazione di queste due misure consente di disporre di informazioni atte a definire la *cyber posture* del fornitore o outsourcer considerato. Come accennato esistono diverse tecniche utilizzabili, tra cui:

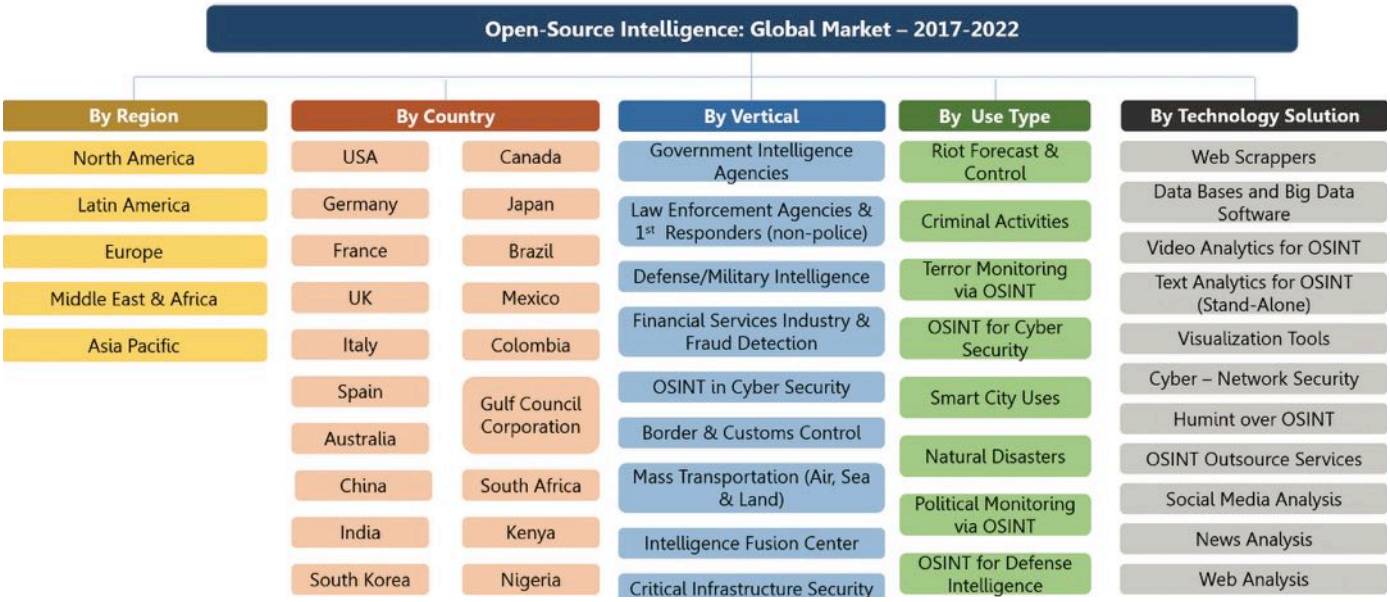
- **OSINT** ("Open Source INTelligence"), ovvero tutte quelle attività atte a raccogliere informazioni di pubblico dominio. Nel contesto legato al monitoraggio/gestione sicura delle terze parti, tali attività consentono di collezionare qualsiasi informazione relativa ad una specifica entità. Più in particolare informazioni relative alla cyber posture possono essere raccolte partendo da:
  - analisi della *configurazione* SSL dei web server;
  - scanning della web application del fornitore;
  - test su come è configurato il dominio DNS;
  - forum specialistici di hacker;
  - attività di intelligence sul dark web.

  Ulteriori fonti informative, non direttamente correlate all'ambito sicurezza ma che possono fornire dati di contesto, sono certamente:
  - resoconti finanziari;
  - informazioni di mercato;
  - social networks;
  - siti web per la ricerca di lavoro / forum di recensioni aziendali o inserzioni di recruitment.

  Tali fonti possono fornire campanelli di allarme, su cui basare ulteriori indagini. Ad esempio, se un report finanziario indica che i profitti di un fornitore stanno diminuendo o che sta spendendo meno del previsto in aree quali l'R&D, questo potrebbe indicare anche un taglio significativo alla spesa per la sicurezza.

  Le analisi eseguite per mezzo di raccolta OSINT potrebbero d'altro canto collezionare informazioni obsolete e non esatte: proprio per questo motivo è necessario perimetrare la ricerca.

- **Security Rating:** servizi a pagamento i cui dati si basano per lo più sulle risultanze di attività OSINT. Il valore aggiunto rispetto all'OSINT risiede nel fornire anche una valutazione generale del livello di esposizione al rischio di un determinato fornitore o outsourcer. Tali rating si basano su differenti criteri, tra cui:
  - suscettibilità agli attacchi man-in-the-middle;
  - suscettibilità a malware;
  - validità dei certificati SSL / TLS;
  - esistenza di vulnerabilità note;
  - data beach noti che il fornitore ha subito.



I differenti vendor che si apprestano ad erogare una tale tipologia di servizio forniscono report dettagliati in cui illustrano i risultati e i razionali sottostanti. Nonostante la mancanza di approfondimento, tali report vengono aggiornati più volte al giorno, quindi sono in grado di fornire una rappresentazione, seppur generale, automatizzata e continuamente aggiornata del livello medio di esposizione al rischio cyber di un determinato fornitore.

Ovviamente rientrando tra le metodologie che si appoggiano ai Big Data, i Security Rating forniscono una valutazione limitata circa la sicurezza del fornitore, non potendo definire con certezza se il servizio acquistato dall'azienda o il fornitore siano realmente sicuri.

▸ **Soluzione Interne di Sicurezza:** molti fornitori o outsourcer accedono direttamente alla rete aziendale del cliente, il che significa che i rischi cyber che caratterizzano la terza parte possono avere impatti diretti all'interno dell'infrastruttura dei clienti serviti. Onde evitare ciò il Responsabile della Sicurezza deve prevedere degli accorgimenti che rientrano nel novero dei presidi tradizionali:

- prevedere una classificazione delle informazioni, che garantisca l'applicazione del requisito del "Need to Know";
- prevedere soluzioni atte ad evitare data loss e data leak (DLP);
- garantire un adeguato sistema di Digital Rights Management (DRM);
- implementare un processo di gestione delle identità e degli accessi (IAM) con soluzioni di Strong Authentication (Autenticazione a due fattori);
- eseguire analisi sul traffico di rete;
- prevedere soluzioni atte alla raccolta centralizzata dei log e degli eventi generati da applicazioni e sistemi in rete (SIEM);
- prevedere un CASB, qualora siano presenti servizi in Cloud acceduti dai fornitori, in modo da applicare quei controlli specifici per la protezione del patrimonio informativo aziendale.

L'adozione di soluzioni di network discovery come di CASB permette di individuare fenomeni di Shadow IT, ovvero prodotti e servizi acquisiti o utilizzati al di fuori del processo di Procurement aziendale. L'analisi del traffico di rete, IAM, DLP e DRM consentono invece di monitorare l'accesso del fornitore e le relative attività salvaguardando l'azienda da eventuali Data Leak.

Tali soluzioni seppur non forniscono "punteggio" circa la cyber posture dei fornitori, sono in grado tuttavia di produrre informazioni ed indici da integrare all'interno del più vasto processo di monitoraggio efficace delle terze parti.

Ovviamente prima di "invitare" un fornitore all'interno della propria infrastruttura di rete esponendola quindi alle cyber threats che caratterizzano il fornitore, si consiglia di valutare se sia realmente necessario fornirgli i diritti di accesso o sia più conveniente fornirgli un proprio laptop con accesso limitato o una macchina virtuale su cui lavorare.

Meccanismi di share information: nonostante nel corso degli ultimi anni tutte le principali normative hanno incluso al loro interno clausole mandatorie che sottolineano l'importanza di segnalare ai propri stakeholder, eventi/incidenti di sicurezza informatica (Circ.285, GDPR, NIS, ecc.), ancora oggi molti fornitori tendono a essere riluttanti nel fornire suddette informazioni, in particolar modo quando questi eventi di sicurezza comportano implicazioni dirette sui propri clienti. Nonostante alcuni fornitori si dimostrino trasparenti e ben disposti alla condivisione di tali informazioni, altri potrebbero condividere solo ciò che è necessario in termini di obblighi contrattuali o regolamentari.

In tal caso il Responsabile della Sicurezza deve includere all'interno degli stessi contratti clausole precise che disciplinano le modalità e i tempi di condivisione non solo di eventi significativi di sicurezza, ma anche di risoluzione delle vulnerabilità critiche sui sistemi del fornitore. Proprio per rafforzare tali meccanismi, si sono venute a creare apposite organizzazioni come la Customer Security Programme (CSP) SWIFT, che fornisce ai membri della comunità SWIFT report giornalieri incentrati su transazioni di grandi dimensioni o insolite, a cui tutti i partecipanti possono accedere. Lo stesso meccanismo è adottato come requisito cogente nel contesto della PSD2.

Self-Assessment del fornitore: rappresentano lo strumento tradizionale impiegato dalle organizzazioni per avere contezza della cyber posture dei propri fornitori. I self-assessment si configurano generalmente come fogli di calcolo excel basati su domande personalizzate sul fornitore e mappate con i principali standard di settore (ISO / IEC 27001, NIST Cyber Security Framework, ecc..). Dal punto di vista informativo tali valutazioni rientrano tra le modalità puntuali, fornendo di conseguenza una istantanea della cyber posture del fornitore.

Il contenuto e la profondità dei Self-Assessment possono differire a seconda di una serie di fattori (il tipo di servizio offerto dal fornitore, la relativa dimensione, la criticità della fornitura erogata). Il principale valore aggiunto da tale tipologia di valutazione risiede nella possibilità di concentrare alcune domande su determinate aree di interesse.

D'altro canto, tale modalità di valutazione riscontra vari limiti, tra cui:

- possibilità che il fornitore inserisca informazioni errate, così da sfalsare le risultanze;
- fornitori più piccoli con reparti IT composti da pochi individui potrebbero non avere la capacità di compilare il self assessment;
- fornitori di grandi dimensioni chiamati a rispondere con più team, potrebbero fornire risposte diverse sulle stesse tematiche;
- presenza di domande poche chiare.

Come già accennato tali assessment sono spesso realizzati in fase di prima contrattualizzazione per avere contezza dei livelli di esposizione al rischio informatico del fornitore. Le organizzazioni dovrebbero prevedere un processo periodico di aggiornamento di tali valutazioni, definendo la frequenza con cui procedere con tali self-assessment all'interno degli stessi contratti. Gli aggiornamenti inoltre dovrebbe soffermarsi solo su determinate aree di interesse in cui sono state identificate punti di debolezza o cambiamenti significativi

▸ **Presenza di certificazioni di sicurezza:** Conseguire certificazioni consente di dar prova ai propri stakeholder di aver implementato adeguati presidi di sicurezza. Le certificazioni di sicurezza, infatti, dimostrano la conformità a ben noti standard di sicurezza (ISO / IEC 27001, SWIFT, PCI-DSS, ecc.), tuttavia considerare tali certificazioni come garanzia generale di sicurezza, potrebbe condurre a conclusioni errate. Tipicamente, infatti, le aziende certificano solo una quota parte dei propri sistemi. In tal caso la certificazione è da considerarsi limitata a quali/quanti sistemi rientrano all'interno del perimetro certificato.

▸ **Valutazione della sicurezza in loco:** tale modalità, che si conforma essere la più invasiva nei confronti del fornitore, rappresenta la modalità più efficace per valutare i presidi di sicurezza di un fornitore. Le valutazioni in loco sono generalmente condotte da Team di verifica terzi al fine di assicurare indipendenze e oggettività nelle rilevazioni. Ovviamente affinché si possa disporre di una valutazione onsite, deve essere prevista all'interno dei contratti una clausola specifica sul "diritto di audit". Permettendo ispezioni onsite è possibile verificare di persona il funzionamento dei presidi di sicurezza tanto di governo quanto operativi previsti dal fornitore. Un valore aggiunto potrebbe essere dato dalla conduzione di *penetration* test direttamente da parte del team di verifica.

Come già accennato, per garantire un monitoraggio efficace della propria filiera di fornitori, in grado di offrire sia una visione overall del livello di sicurezza garantito sia viste di dettaglio su determinate aree/servizi/fornitori critici, è raccomandabile utilizzare contemporaneamente più tecniche. Facciamo l'esempio che si voglia monitorare un fornitore certificato ISO / IEC 27001, si potrebbe:

- chiedere se la certificazione conseguita sia aggiornata, quando e quale perimetro/servizi copre;
- verificare tramite valutazioni OSINT eventuali eventi critici occorsi negli ultimi 2 anni;
- includere il fornitore all'interno delle ricerche quotidiane svolte dallo strumento di Security Rating in modo da disporre real time di un livello medio di esposizione al rischio;
- inoltrare semestralmente/annualmente un questionario self-assessment customizzato, incentrato di volta in volta su specifiche aree di interesse (es. incident management, gestione degli endpoint, ecc.);
- programmare eventualmente ispezioni onsite in caso in cui all'interno del self-assessment siano emersi punti di attenzione che necessitano un approfondimento.

Le diverse tecniche di monitoraggio appena descritte non solo devono essere integrate assieme, così da produrre risultati significativi durante l'intero ciclo di vita dei fornitori, ma devono essere inseriti all'interno di un più vasto processo che correla la mera analisi a specifiche attività di reporting delle informazioni.

Gli aspetti indispensabili da presidiare per implementare un monitoraggio efficace

Come abbiamo potuto esaminare, le diverse tecniche di monitoraggio rientrano in un processo più ampio a sua volta basato su una serie di aspetti indispensabili per garantire un monitoraggio efficace delle terze parti e quarte parti. Di seguito vengono riportate tali necessità:

- definire razionali tramite cui classificare e prioritizzare i propri fornitori: molte aziende, soprattutto, le più grandi, potranno vantare migliaia tra terze e quarte parti che gravitano attorno al proprio business. Un monitoraggio efficace di tutti questi fornitori potrebbe richiedere un effort non sostenibile dall'azienda, pertanto è necessario individuare in primis quelli che sono i fornitori legati ai processi critici per poi espandere gradualmente le attività di monitoraggio anche ai restanti fornitori in base alla criticità degli stessi;
- revisionare periodicamente e in caso aggiornare le condizioni contrattuali stipulate con i propri fornitori. Le clausole contrattuali, infatti potrebbero venire meno a fronte di modifiche organizzative (es. acquisizioni o fusioni) realizzate;
- prevedere clausole contrattuali che consentano di richiedere evidenze specifiche ed effettuare attività di monitoraggio dei fornitori in loco. Clausole di tal natura permettono ad una società di mantenere un governo effettivo nei confronti della propria catena di fornitori.

Un ulteriore step evolutivo potrebbe prevedere la possibilità di porre in essere opportune action verso quei fornitori con un livello di presidio non in linea con le baseline definite dall'organizzazione.

É importante segnalare come sempre più si stiano diffondendo anche in Italia servizi gestiti di Third Party Risk Management che consentono di delegare a terzi l'esecuzione del monitoraggio periodico delle terze parti e come, con l'evolvere della tecnologia in campo, si possa arrivare all'esecuzione di controlli sempre più approfonditi ed automatizzati anche nei confronti delle terze parti. ■

Il monitoraggio della propria catena di approvvigionamento

Autore: Massimo Cappelli

Garantire la sicurezza della propria supply chain non è cosa semplice. Per supply chain, in questo articolo, intendo tutti quei soggetti fornitori di servizi o prodotti, esterni all'azienda, il cui contributo è necessario per la produzione del valore.

Secondo alcune statistiche prodotte dal Ponemon Institute e da Recorded Future, il 59% delle organizzazioni ha subito un data breach, partito dalle proprie terze parti. Il controllo dei propri fornitori è una tematica non nuova. Il controllo del fornitore deve seguire un ciclo di vita, un vero e proprio programma che potrebbe essere diviso in 3 fasi principali: entrata; permanenza; uscita.

Entrata: Prima di intraprendere iniziative di collaborazione, solitamente, si effettuano tutta una serie di controlli relativi alla solidità e affidabilità di un'azienda. Si controllano i bilanci, la proprietà, eventuali pendenze, collaborazioni con altre aziende, il grado reputazionale, etc. etc. Da questo genere di controlli, con lo scorrere del tempo, si è passati a verificare la presenza di certificazioni di conformità e di qualità del prodotto e del servizio. Per quanto riguarda la sicurezza delle informazioni, si richiede spesso le certificazioni ISO2700x. I più lungimiranti richiedono la presenza di sistemi di gestione di Business Continuity e Disaster Management. In alcuni casi, il fornitore, se vuole collaborare con alcune aziende deve anche permettere di effettuare dei test molto invasivi sui propri prodotti e servizi. Non sempre questo è consentito o è possibile, soprattutto nel reparto tecnologico. Il fornitore deve dare il consenso affinché questi test vengano effettuati e non sempre ciò avviene. Inoltre, eseguire questi test, come ad esempio, l'analisi dinamica e statica di un software sono molto costosi e richiedono competenze tecniche molto elevate. Ulteriori controlli devono essere effettuati anche su potenziali compromissioni del fornitore stesso. Ci possono essere informazioni sul web che riportano data breach avvenuti nei confronti del fornitore e anche queste informazioni devono essere tenute in considerazione.

Permanenza: La fase successiva è quella della permanenza. L'azienda deve continuare a monitorare il fornitore e verificare che la sua affidabilità e solidità sia mantenuta. In ambito di information security, se il fornitore accede ai sistemi aziendali, deve poter essere monitorato e controllato. Deve avere delle VPN dedicate. I log di accesso devono essere raccolti e analizzati. Chi accede, da dove accede, con cosa accede, quando accede, perché vi accede. Stessa cosa vale per le piattaforme che vengono acquisite. Si dovrebbe monitorare le attività delle piattaforme, sapere tutte le iterazioni

BIO

Massimo Cappelli è operations planning manager presso la Fondazione GCSEC, oltre che responsabile delle attività di Early Warning, Brand Protection, Information Sharing e Cyber Threat Intelligence nella struttura CERT di Poste Italiane. Nella sua passata esperienza ha lavorato come consulente in Booz Allen Hamilton e Booz &Company nella practice Risk, Relisience and Assurance.

che svolgono all'interno del processo, quali informazioni trattano e dove le trattano (sui datacenter aziendali, in cloud, presso datacenter del fornitore, etc. etc.). Tutto questo monitoraggio dovrebbe essere real-time con sistemi di alerting pronti a scattare in caso di anomalie. Se un fornitore cambia device o regione geografica da cui si collega, se una piattaforma non si limita a trattare le informazioni necessarie alle sue attività, etc. etc., il sistema deve poter alzare una bandierina di allarme per verifiche ulteriori. Queste analisi richiedono capacità di raccolta dati e di analisi più o meno automatizzate. Inoltre, richiedono anche competenze elevate. Pertanto, è importante predisporre i propri sistemi alla raccolta di questi dati e al loro trattamento. Questo per quanto riguarda il monitoraggio delle attività day by day effettuate con l'azienda. È necessario considerare anche il perimetro esterno aziendale ed effettuare dei monitoraggi preventivi su eventi che impattano il fornitore e potrebbero impattare anche la nostra azienda. Se un fornitore subisse un data breach, l'azienda indirettamente potrebbe esserne impattata. Un sistema di raccolta informazioni del web, in tutte le sue accezioni è utile per mantenere un occhio verso l'esterno e intercettare potenziali segnali di compromissione. Un metodo semplice potrebbe essere di correlare la propria lista fornitori con fonti di intelligence su data breach in modo da avvisare automaticamente l'azienda nel momento in cui viene pubblicata qualche notizia relativa al proprio fornitore. Ovviamente più fonti di intelligence si ha e più queste sono profilate per cercare informazioni sulla propria supply chain, più efficace sarà il risultato. Questo però potrebbe essere molto dispendioso in termini economici.

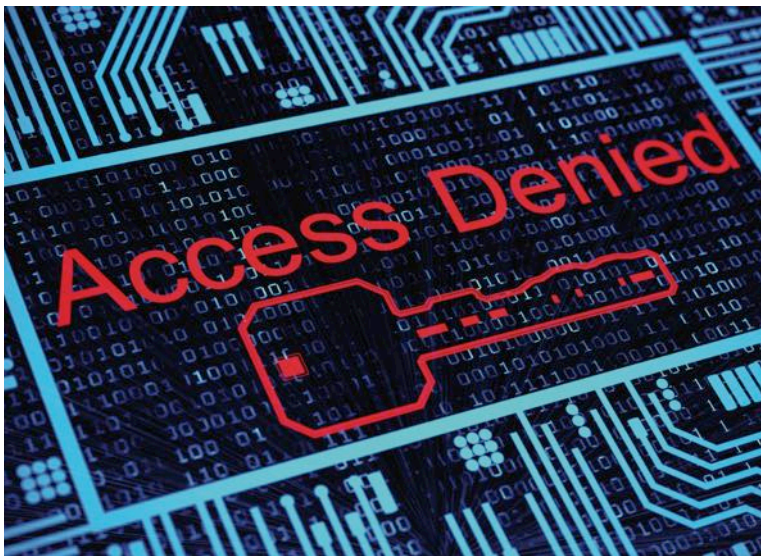
Stessa operazione dovrebbe essere effettuata su tutti i fornitori e non solo sui fornitori di Sistemi Informativi. Le informazioni più strategiche per l'azienda potrebbero risiedere nei computer del top management e in quello dei loro collaboratori esterni, come studi di consulenza legale, di consulenza finanziaria e così via. È opportuno monitorare tutti i fornitori e cercare di categorizzarli in base alle informazioni che gestiscono.

L'attività di monitoraggio dei fornitori richiede un forte coordinamento e collaborazione stretta fra diverse funzioni. Per questo, è necessaria anche una integrazione di processi fra funzioni di business, funzione acquisti, funzione di amministrazione e controllo e funzione di security. I tempi per lo screening devono essere ridotti al minimo per non appesantire il processo di acquisizione.

Uscita: La fase finale è la chiusura del contratto. Questo significa bloccare gli accessi alle VPN e chiudere eventuali flussi informativi da e verso il fornitore. Questo passaggio è molto importante. Spesso viene protratto nel tempo e tralasciato, soprattutto se il fornitore non è strettamente nel mondo

IT in cui c'è una maggiore consapevolezza di queste tematiche. Quindi si trovano accessi a cartelle condivise, VPN ancora attive e flussi informativi ancora esistenti fra azienda e fornitori che possono andare dall'ambito HR a quello commerciale o finanziario.

La parte di monitoraggio ovviamente non può essere trascurata. Se la vita del fornitore in azienda terminasse nel tempo T0, precauzionalmente sarebbe opportuno mantenere il monitoraggio di intelligence almeno per un anno successivo alla chiusura del contratto. Seppure i rapporti siano conclusi, ci potrebbero essere informazioni aziendali ancora in giro. Un anno non è né tanto né poco, dipende sempre poi dalla capacità di monitoraggio e di raccolta informativa che un'azienda ha.



È molto importante che in tutte e tre le fasi vi sia una forte componente di sensibilizzazione di tutti gli attori coinvolti. Il perimetro di sensibilizzazione si allarga ai fornitori e si deve essere certi che questi abbiano assimilato le policy di sicurezza aziendale e che le rispettino. ■

Cybersecurity Trends

Visita la nuova sezione For Expert

www.cybertrends.it/category/hacking-around

Il fattore umano nella cyber security

Valori e strategie da costruire insieme

A cura di Nicola Sotira

MANAGEMENT

TOOLS

GLOBAL CYBER SECURITY CENTER

FrancoAngeli

Bibliografia

Mauro Marcantoni, Luciano Hinna, Francesco Dall'Olio,
Il pentagramma del diavolo,
Franco Angeli ed.

La burocrazia come il colesterolo, se troppo alta diventa letale

"Il pentagramma del diavolo", il saggio di Mauro Marcantoni, Luciano Hinna e Francesco dall'Olio, rispettivamente un sociologo, uno tra i massimi esperti del settore pubblico, e un giurista e magistrato, ha un titolo già in sé evocativo. La burocrazia è stata sempre un alibi, un paravento di cui il potere si è servito per consolidare rendite di posizione e per giustificare ritardi. Anche il nuovo esecutivo Draghi dovrà misurarsi con questo mostro, non ha caso ha messo in cima all'agenda la sburocratizzazione. Sarà la volta buona? Meglio essere cauti visto i precedenti. "La burocrazia – commenta Hinna -è un po' come il colesterolo: se è nella misura giusta fa bene e si identifica con le regole di funzionamento che servono e senza le quali non avremmo lo Stato. Se è troppo, però, diventa patologia e fa danni incredibili sia sotto il profilo economico che quello sociale".

Tutti vorrebbero eliminarla, non c'è stato ministro (ora assistiamo al "ritorno" di Brunetta il ministro dei "fannulloni"), che non ne abbia fatto la bandiera per avviare una stagione di riforme, eppure impera viva e vegeta. "Per una buona riforma non bastano le norme, servono anni di accompagnamento di pressione sull'implementazione, quando invece il ministro di turno ha appena il tempo di predisporre un decreto, ma poi per i soliti avvicendamenti di governo, quello stesso ministro che aveva sognato e pensato la riforma deve passare la mano a chi arriva il quale, visto che le cose non funzionano si sente in obbligo a sua volta di proporre l'ennesima riforma e così via per anni". La lotta alla burocrazia è insomma un susseguirsi di opere incompiute un lusso che non potremo più permetterci dal momento che nel *Recovery Plan* un ruolo importante per il rilancio del paese dovrà giocarlo proprio la Pubblica Amministrazione. "Questo dato di realtà – prosegue l'analisi di Hinna - ha generato una sorta di coazione a ripetere: quella di un'autopsia troppe volte praticata". Un'immagine lugubre che vale la pena spiegare seguendo il ragionamento degli autori: "in tutta la sua ombra lugubre l'autopsia è uno di quei processi che non si possono ripetere due volte, deve per forza di cose essere fatta bene alla prima e deve avere valenza per più scopi diversi. La nostra burocrazia, invece, impasta e rimpasta la stessa materia più volte facendo lievitare tempi e costi. L'adozione di modelli per la gestione della qualità considerando i cittadini non sudditi, ma clienti/utenti, potrebbe essere una soluzione di facile applicazione. Nulla di nuovo sotto il sole: sono decenni che il concetto è inserito nelle norme di riforma, ma la burocrazia sembra sorda ai richiami della qualità".

La "sindrome" dei 5 anelli

Lo studio propone di cambiare rotta partendo da una proposta concreta: ripensare la struttura del Dipartimento della Funzione Pubblica per trasformarla da ministero senza portafoglio in una agenzia tecnica, un'autority indipendente come ne abbiamo altre con commissari tecnici (ingegneri gestionali ed economisti aziendali) che rimangono in carica 6 o 7 anni, tempo necessario per pensare una riforma, accompagnarla ed incidere realmente sulle strutture organizzative della PA.

Un suggerimento, da cogliere al volo a nostro giudizio, anche perché potrebbe servire a superare quella che gli studiosi definiscono la sindrome dei cinque anelli che costituiscono gli elementi del DNA della nostra burocrazia. "Il primo anello è la palude delle norme: 220 mila, troppe, fatte male, spesso alla deriva ed in contrasto tra loro; il secondo anello è costituito dall'eccessivo numero di arbitri a fondo campo, le varie magistrature ed autority, tutte pronte ad alzare il cartellino rosso o il cartellino giallo. Il risultato è scontato, è quella che viene definita burocrazia difensiva: il povero dirigente pubblico pagato per esercitare un minimo di discrezionalità sotto l'incubo del danno erariale e dell'abuso di ufficio finisce per paralizzarsi. Il terzo elemento è il modello burocratico in senso stretto: un modello superato, in affanno, che amministra e non gestisce, che confonde gli obiettivi con i compiti, che tenta di risolvere i problemi organizzativi a colpi di norme, che è ancorato ad un modello weberiano che non esiste più nei fatti, ma che purtroppo sopravvive nelle regole e nelle norme, come lo *smart working* in periodo di Coronavirus ha ampiamente dimostrato. Il quarto elemento è l'impermeabilità della pubblica amministrazione all'innovazione, un fenomeno legato alla resistenza ai cambiamenti, alla età media del suo personale, alla sua base culturale prevalentemente giuridica, rinforzata da una formazione ancora giuridica e dallo scarso livello di digitalizzazione che fa sì che il patrimonio di dati di cui la PA dispone costituisca una sommatoria di semplici dati senza diventare mai informazione utile e migrare verso la conoscenza condivisa per il paese". Tema cruciale rimane la qualità del capitale umano. Come è noto la PA manca da sempre di un modello organizzativo che nei fatti mortifica il talento di 3 milioni e duecentomila dipendenti pubblici di cui ha fatto sempre a meno perdendo una grande occasione per creare quella intelligenza collettiva di cui avremmo invece un gran bisogno. Il quinto elemento ha a che fare con i cittadini, rimasti purtroppo ancora sudditi che non pretendono ma subiscono, che si rassegnano e non protestano, che si fanno schermo della burocrazia per non lasciarsi coinvolgere nei processi di innovazione".

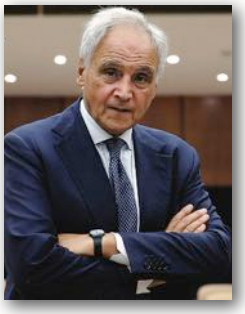
Steve Jobs diceva che il patrimonio più grande che un'azienda può sfruttare è lo scontento dei propri clienti: se è vero esiste un grande potenziale patrimonio da sfruttare ad una condizione, ovvero che i clienti della pubblica amministrazione riescano ad andare oltre l'usuale lamentela, per chiedere sempre di più, lo fa l'utente Amazon con sistematicità, non si vede perché non si debba seguire lo stesso modello quando si ha di fronte lo Stato nella sua articolazione di prossimità rispetto al pubblico dei cittadini.

Il martello e il punteruolo

Il testo si conclude con una duplice immagine ad effetto: il "martello" e il "punteruolo". "Immaginiamo la pubblica amministrazione come una scultura da realizzare, una realtà da rimodellare. Una punta penetra più di una superficie piatta, ma ha un effetto molto localizzato. Se vogliamo non bucare la superficie ma rimodellarla, c'è bisogno di un martello, di un approccio diverso, capace di intervenire sulla forma dell'oggetto. Questo secondo approccio è più impegnativo e richiede azioni ripetute, precise e distribuite ad arte su tutta la superficie lavorata. Nel caso della burocrazia, agire di punta può essere utile, ma non è mai risolutivo, come la storia ci ha dimostrato. In altri termini, se cerchiamo di riformare gli apparati burocratici agendo solo al loro interno o su singoli punti, saremo destinati a risultati deludenti o parziali, proprio perché molte disfunzioni dipendono da realtà istituzionali formalmente esterne, ma strettamente connesse funzionalmente. Se non vogliamo rimanere prigionieri degli insuccessi di sempre, è indispensabile il coraggio e la lucidità di un approccio alternativo, appunto di sistema. C'è bisogno di ridisegnare in modo organico la configurazione della Pubblica Amministrazione che vogliamo, agendo di martello e di punteruolo". Mente e mano, dunque, ha ragione il grande sociologo statunitense Richard Sennett (cfr. L'uomo artigiano ed. Feltrinelli n.d.r) devono concorrere agendo in sinergia se vogliamo realmente sconfiggere quel "pentagramma del diavolo", fatto di resistenze oscure, di abitudini, di convenienze, di pigrizie, di palleggi di responsabilità. ■

Roger Abravanel
Aristocrazia 2.0
Solferino ed.

Premiamo il merito e usciremo da una crisi "senza tempo"



Roger Abravanel, *director emeritus* di McKinsey, scrittore e saggista, da anni ha imbracciato una battaglia molto precisa, che appare chiara dai suoi titoli di maggior successo, conosciuti e venduti in tutto il mondo: "Meritocrazia", "Italia cresci o esci", "La ricreazione è finita". Chiara la tesi di fondo, che è anche il *fil rouge* di queste ricerche: senza un adeguato investimento negli asset intangibili della conoscenza e della competenza e senza un adeguato riconoscimento del merito, non ci può essere né futuro, né tanto meno sviluppo; continuare, dunque, a perdere tempo e denaro mortificando le intelligenze, è una tattica sconsiderata e suicida. La società dell'informazione, entro cui viviamo immersi, ha il sapere come primo vero carburante; è il nuovo petrolio che l'Italia ha il torto di continuare a ignorare, privilegiando logiche di selezione delle élites fondate sul privilegio,

la rendita, la raccomandazione, istituto forse vetusto, ma sempre abilmente praticato alle nostre latitudini.

L'ultimo lavoro, ***Aristocrazia 2.0***, per iniziativa del "Forum della meritocrazia", associazione presieduta da Maria Cristina Origlia, giornalista e scrittrice, è stato presentato di fronte a una platea qualificata di giovani impegnati a vario titolo a praticare l'innovazione in diversi ambiti sociali e lavorativi. Un modo originale per entrare nel cantiere vero di chi opera realmente ogni giorno nel tentativo di rimuovere tutte quelle incrostazioni che da troppi anni non ci consentono di decollare. "Da quasi mezzo secolo – spiega l'autore nella premessa del saggio – l'Italia appare incapace di sfruttare le grandi trasformazioni economiche. Dall'economia industriale, siamo passati all'economia post-industriale, all'economia della conoscenza, fatta di innovazione, digitale, scienze della vita, finanza avanzata, ma non stiamo curando a dovere nessuno di questi aspetti con il risultato che in trent'anni abbiamo perso l'equivalente del reddito della Grecia e del Portogallo messi insieme".

"La particolare congiuntura dettata dalla svolta solidaristica europea e dall'opportunità rappresentata dal flusso ingente di risorse legate alla Next generation Eu, cui si sovrappone l'avvento del nuovo esecutivo guidato da Mario Draghi, potrebbero finalmente costituire l'ecosistema adatto per una svolta economica e sociale, non solo dell'Italia ma finalmente anche dell'Europa – ha commentato la Origlia in sede di presentazione del saggio. Malgrado questo, c'è ancora ancora molta dispersione e superficialità, che distoglie le classi dirigenti dal loro compito essenziale che dovrebbe essere quello di progettare il futuro, adottando uno sguardo lungo". Accade, invece, che siamo "prigionieri del presente", per usare una fortunata immagine poi divenuta un libro di Giuseppe De Rita e Antonio Galdo, ci dimeniamo dentro la "trappola della modernità" senza saperne governare le leggi, senza capirne il senso di questo mutamento d'epoca. Il rischio più immanente è che l'economia italiana non riesca mai più a trovare quel punto di svolta che attendiamo invano dall'ultima crisi, quella del 2008.

Nel saggio emerge in maniera inequivocabile la denuncia della sostanziale incapacità dimostrata dalle nostre élite a sfruttare le grandi trasformazioni epocali che ci hanno portato dall'alto forno al pc, in una sostanziale modifica del paesaggio umano economico e sociale delle nostre città. "Perché la pandemia non diventi un mito" mette in guardia Alessandro Baricco in una brillante raccolta di aforismi (Quello che stavamo cercando ed. Feltrinelli n.d.r.) tornare al pensiero razionale attraverso la porta della conoscenza può essere decisivo: *"Il mito è una rete strappata non produce ordine, non spiega la realtà, la fonda nominando senza disciplinare, enumera ma non calcola…"*. Abravanel inconsapevolmente sembra seguire il suggerimento, (il suo libro è infatti uscito prima rispetto a quello dello scrittore torinese) il suo lavoro offre sempre numeri molto precisi che spiegano le fenomenologie del cambiamento in maniera

lucida, incontrovertibile. Gli esempi riportati nel testo fanno, infatti, vedere che un'aristocrazia 2.0 di manager e imprenditori illuminati esiste già, non si tratta di una definizione accademica, né di una "classe vuota" per usare la terminologia della logica classica.

Mentre compiamo lo sforzo di intuire cosa accadrà domani, volgere lo sguardo indietro può essere un altro esercizio utile. "Nel secolo scorso si è sviluppata la meritocrazia, milioni di giovani si sono impegnati nell'educazione superiore per migliorare il loro status economico e sociale. L'economia della conoscenza – riprende l'analisi di Abravanel - di questo ultimo secolo ha fatto esplodere il premio per questa nuova élite, gli uomini più ricchi degli USA hanno studiato nelle grandi università, così sono nate le critiche nel mondo anglosassone a una nuova aristocrazia dell'istruzione e del talento che oltre ad essere iper-ricca favorisce in mille modi i figli nell'accedere alle migliori università. La meritocrazia avrà pur fallito nelle pari opportunità (è disposto ad ammettere lo studioso), ma ha creato milioni di buone opportunità, per i giovani che emulando le élites investivano nella migliore istruzione e facevano carriera nelle grandi imprese. È avvenuto in Occidente e avviene sempre più in Asia dove la selezione per la migliore istruzione sta diventando il motore dello sviluppo". Emblematico il caso della Corea, dove il 70% dei giovani sono laureati ha un reddito pari al doppio, in alcuni ambiti al triplo di quello dei genitori".

È evidente che siamo troppo lontani dal modello preso in esame. Da noi l'ascensore sociale è bloccato da un pezzo, siamo il fanalino di coda per numero di laureati e il paese con più donne nei cda ma pochissime donne nel top management. Eccellenza, competizione, ambizione sono mancate, insieme a una politica illuminata, che avrebbe dovuto incentivare il talento e l'istruzione. Come se non bastasse le nostre università si sono chiamate fuori dalla competizione globale del sapere e le migliori languono nelle classifiche globali. La nostra economia è rimasta nelle mani della vecchia aristocrazia, responsabile dell'ecatombe delle grandi imprese industriali, della vendita di quelle del made in Italy (un elenco lungo così…) e di un crescente digital gap in quelle che rimangono.

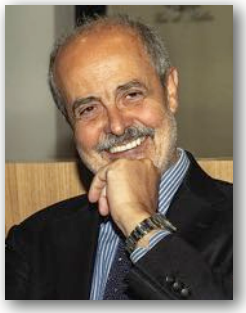
In questo quadro a tinte fosche si aggiunge un'aggravante: *"nell'anno della paura nera il sistema-Italia si presenta come una ruota quadrata che non gira (cfr. Rapporto Censis 2020 n. d .r.) il conto più salato lo stanno pagando proprio i giovani e le donne: per loro già persi quasi 500.000 posti di lavoro. Cosa resterà dopo lo stato d'eccezione se solo il 13% è pronto a tornare a rischiare aprendo un'impresa"*. Difficile essere ottimisti se anche gli animal spirits stanno evaporando con la paura, per cui bisognerà ricreare prima di tutto un clima di fiducia, se vogliamo invertire il percorso discendente che ci sta portando verso l'abisso.

Altro bubbone, che il saggio guarda da vicino, la burocrazia (cfr. recensione de Il pentagramma del diavolo in questo numero) che strangola lo sviluppo non per colpa dei troppi fannulloni ma della paralisi decisionale provocata dalla sfiducia nello stato e un timore della corruzione che non hanno eguali in Occidente, e che hanno portato alla degenerazione di un potere giudiziario totalmente autoreferenziale.

Cosa fare dunque per non soccombere? Sono almeno tre i versanti da battere, che si ricavano dalla lettura del testo: creare le condizioni perché si possa affermare un capitalismo immune dallo "statalismo di ritorno post pandemia" che si sta diffondendo a macchia d'olio; ricondurre i migliori capitali del *private equity* verso le aziende sane che operano nel mercato globale; la progressiva emersione di un sistema scolastico e universitario capace di ricercare e premiare l'eccellenza. Ma tutto sarebbe vano se nel contempo non si trovasse il modo di individuare pesi e contrappesi che rendano maggiormente responsabile la magistratura e più in generale il sistema giudiziario, la cui *mission* dovrebbe essere principalmente orientata a garantire l'efficienza, la trasparenza e l'equità della macchina dello stato, interessandosi meno al gioco ideologico e agli intrighi di potere. ■

Antonio Calabrò,
Oltre la fragilità,
Bocconi ed.

Alzare lo sguardo oltre la crisi, per essere costruttori di futuro



Utopia e riformismo coraggioso. Per affrontare l'anno appena iniziato, accogliendo l'invito del Presidente Mattarella a essere "costruttori di futuro", avremo bisogno di un equilibrato mix di queste due componenti. Sostiene questa tesi *Antonio Calabrò*, direttore della Fondazione Pirelli e vicepresidente di Assolombarda nel saggio *"Oltre la fragilità"* (ed. Bocconi), un appello, teso a scuotere il paese scosso da un'emergenza che sembra non avere mai fine. "Dentro ogni crisi vi sono straordinari segnali di rilettura dell'esistente, che possono se ben interpretati, aiutarci nell'opera di ricostruzione di un nuovo equilibrio del mondo. L'esercizio del pensiero simbolico, ci ha insegnato il grande pensatore del '900 Ernest Cassirer, può aiutarci a superare l'inerzia che ci avvolge e a trovare l'energia per trasformare il cattivo presente". L'utopia è, infatti, quell'orizzonte di possibilità, senza di cui non potremmo vivere, così come non saremmo capaci di lavorare senza avvertire la necessità di operare delle scelte concrete. Ed è su questo passaggio che si innesta la denuncia più netta contenuta nello scritto. "In troppi hanno dimostrato di non aver compreso il senso della pandemia. Ne abbiamo avuto prova quando abbiamo creduto che l'estate portasse con sé il messaggio "liberi tutti". Ci siamo così adagiati e quando, come era prevedibile, si è abbassato il livello del contagio

abbiamo perso l'occasione per prendere provvedimenti anche minimi, ma utili e concreti quali: il tracciamento, l'assunzione di personale medico e paramedico, disposizioni intelligenti riguardanti la scuola, non certo riconducibili alla ridicola trovata delle rotelle da sistemare sotto i banchi." Per guardare oltre questa ora buia non servono inutili tatticismi, ma decisioni rapide, che dovranno impattare su un duplice registro: definizione di sussidi rapidi e certi per quelle categorie, e sono tante, che hanno pagato un prezzo altissimo in questo lungo difficile anno e contemporaneamente una corretta elaborazione di strategie di medio lungo periodo. Una buona attuazione del *recovery found* sarà decisiva per attuare un cambio di passo, anche se lo spettacolo di scarsa compattezza dell'esecutivo che sta andando in scena in questi ultimi giorni non può certo contribuire a ricostruire quel clima di fiducia nella collettività, necessario al rilancio di un paese allo stremo. La qualità delle *élites,* non sempre all'altezza bisogna dire, sarà il presupposto di ogni possibile ipotesi di rilancio. Anche su questo aspetto Calabro non sembra disposto a fare sconti: "abbiamo una classe dirigente per molti aspetti inadeguata, inutile nasconderlo, non solo in Italia, troppa attenta a *like* e sondaggi e scarsamente capace di pensare al lungo periodo, ma è con questa che dobbiamo fare i conti. Spero che si possa creare un incrocio virtuoso tra il senso di responsabilità delle forze sociali, Confindustria, sindacati, la buona capacità di governo che alcune regioni hanno dimostrato e la consapevolezza di quella parte dell'opinione pubblica più avvertita che può dare l'esempio, aiutando la classe politica a prendere decisioni pensate, equilibrate e condivise".

Quella che si sta giocando è una partita fondamentale della ricostruzione delle regole su cui si regge il patto sociale. Ridare aspettative positive a un corpo collettivo sfiduciato, che vede milioni di persone, giovani e donne in prima linea, guardare con preoccupazione al loro futuro e a quello dei loro figli è un dovere etico, per una civiltà planetaria che va rifondata sui valori della cultura, dell'inclusione e della responsabilità sociale. Bisognerà insomma avere *"Il coraggio di liberare il bene",* come scrive nella postfazione del libro Mons. Gianni Zappa, evidenziando una crescente domanda di senso che caratterizza la terribile "ora buia" che stiamo vivendo. Il lavoro di Calabrò si sofferma in conclusione su un binomio chiave della contemporaneità, quello tra politica e scienza. La pandemia ci ha insegnato che scienze umane e tecnologie, medicina e ingegneria, politica e conoscenza degli algoritmi sono ambiti disciplinari che devono costantemente confrontarsi per migliorare la qualità dell'analisi e la capacità previsionale, che sarà decisiva per progettare il futuro. "Credo – commenta l'autore – che sia venuto il momento di lavorare per far crescere una diffusione della scienza, al riparo dai dogmatismi. L'algoritmo è una "creatura" dell'uomo, non un termine assoluto cui dobbiamo affidare il nostro destino. Non è un dato neutro. Perciò occorre formare persone capaci di interpretarlo e costruirvi un senso, una indicazione densa di valori morali, in un'ottica multidisciplinare. Serviranno ingegneri e filosofi, fisici e perché no? Poeti. Il percorso che faremo sarà segnato da uno stretto rapporto tra umanesimo e tecnologia, da una cultura politecnica che dovrà portarci a una maggiore consapevolezza della complessità che viviamo". Il messaggio di Calabrò si rivolge in particolare all'impresa responsabile, che deve impegnarsi a praticare un'innovazione aperta, di ampio respiro, costantemente orientata a costruire una storia di cambiamento. ■

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

CERT STAR

CERT STAR è un programma di incontri a porte chiuse dedicato ai **CERT** e ai **SOC** italiani volto ad alimentare le **competenze**, promuovere la **cooperazione** e la **condivisione** di esperienze. Nel corso degli incontri sono analizzate a livello tecnico **operativo** le principali **tematiche** "core" dei team di security.

INCONTRI 2021

- **Febbraio e dicembre** Competizione Red Team
- **31 Marzo** Intelligenza Artificiale e Cyber Security
- **Aprile** Cyber Threat Intelligence
- **Giugno** Cloud Security
- **Luglio** Ransomware
- **Settembre** Threat Hunting
- **Novembre** Incident Response

NOVITÀ

- Incontri online
- Attività di laboratorio
- Competizioni Read Team
- Momenti di condivisione
- Webinar
- Momenti conviviali

BUCHAREST 5+

CHOICE FOR CYBER

Government of Romania

www.bucharest4cyber.ro