Cybersecurity Trends

Edizione italiana, N. 2 / 2021

INTERVISTE VIP:

MASSIMO RUSSO
ALDO FONTANAROSA

Folder Centrale: SecDevOps

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

Quando il codice conta

Autore: Nicola Sotira

Il tema della supply chain è stato messo in evidenza sia dalla pandemia sia dalla digitalizzazione che ha cominciato a correre. Sarebbe poi opportuno fare notare che gli ultimi attacchi ransomware stanno prendendo di mira sempre di più le enterprise, quasi abbandonando gli individui e le piccole realtà. Ed in questo contesto che vengono sfruttate proprio le vulnerabilità della filiera approvvigionamenti, ivi incluse le distribuzioni di software. Il tema sta diventando così rilevante che anche Google ha recentemente rilasciato una soluzione, *Supply Chain Levels for Software Artifacts*, per garantire l'integrità delle distribuzioni software in modo da prevenire modifiche non autorizzate. Per maggiori dettagli potete consultare https://github.com/slsa-framework/slsa .

Diventa sempre più rilevante anche il controllo della fabbrica del software, sia nel caso di fornitori e provider, sia nello sviluppo, qualora le organizzazioni sviluppino in casa soluzioni. Molte le sigle legate a questo tema come *DevOps, DevSecOps e SecDevOps*. Quando si parla *DevSecOps* si intende la modalità nella quale la sicurezza viene introdotta al termine delle attività di sviluppo, approccio che può presentare delle criticità e dove la parte di messa in sicurezza potrebbe diventare il collo di bottiglia.

Il termine *SecDevOps* è invece la sigla che individua la giusta dimensione, l'inclusione di tutti gli sforzi di sicurezza e buone pratiche nella pipeline di sviluppo e nella distribuzione. Ovvero, i requisiti di sicurezza sono presi in considerazione prima dello sviluppo, garantendo che la sicurezza delle applicazioni sia inclusa in tutto il ciclo di vita. Nella teoria abbreviata in questo acronimo viene anche previsto che i gruppi di sicurezza facciano parte del ciclo di vita del software; questo per evitare che i processi di sicurezza siano solamente goffe "riverniciate" o ripensate invece che essere nativi già in fase di sviluppo del codice.

Questo modello ha però un limite, funziona solamente se tutte le persone che compongono i gruppi di sviluppo ed i manager comprendono il valore intrinseco di questo processo. Occorre fare comprendere come la sicurezza nativa nelle applicazioni e sviluppo del codice possa influire sui risultati aziendali. Come sempre non è solo un tema tecnologico, ma soprattutto di persone e responsabilità.

Questo significa che sul tema SecDevOps si deve non solo focalizzarsi sull'integrazione della sicurezza nei processi ma affrontare anche le tematiche collegate come la collaborazione, la riservatezza delle informazioni e rafforzare il proprio ambiente di distribuzione lavorando ad una maggiore condivisione con una supervisione che tenga saldi questi obiettivi garantendo che le buone pratiche di sicurezza siano parte dell'intero ciclo di vita del software. ■

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.

Sicurezza e democrazia nell'infosfera delle piattaforme

Intervista VIP con Massimo Russo.

Autore: Massimiliano Cannata

"Lo stato nazione è una tecnologia sociale che ha avuto per secoli il compito di assicurare benessere, progresso e sicurezza alle persone. Questa invenzione della modernità non è più adatta ai bisogni della collettività, sono le piattaforme private che hanno preso il suo posto, dovremo perciò essere pronti a comprendere i nuovi equilibri politici ed economici che questo comporterà, per non rimanere completamente spiazzati". Questa la tesi di fondo di Statosauri (ed. Quinti Quarto) saggio di Massimo Russo, manager e giornalista, direttore di "Esquire Italia", che offre uno spaccato efficace del rapporto che lega democrazia e rivoluzione digitale.

"Il mondo continua a restringersi malgrado alcuni eventi ci abbiano portato a pensare diversamente. La pandemia ci ha fatto alzare barriere contro la paura, stimolando qua e là rigurgiti di sovranismo e strane nostalgie nazionaliste. Si tratta di vecchi arnesi destinati ad andare in disuso". Partirei da questa affermazione contenuta nel saggio per cercare di spiegare il neologismo utilizzato per titolare il saggio: "Statosauri". Cosa vuol dire esattamente?

Gli Stati nazionali sono una costruzione politica e sociale inadatta a gestire la complessità delle sfide del presente. Organismi del passato non più adeguati a un ecosistema differente. Partiamo dalla definizione di tecnologia. Secondo Treccani è una parola che «indica le tecniche utilizzate per produrre oggetti e migliorare le condizioni di vita dell'uomo: non si tratta quindi solo di realizzazioni concrete, ma anche di procedure astratte». In questo senso anche le costruzioni sociali sono tecnologie, come lo sono le città, le piazze, la natura divina del sovrano che fu necessaria per spiegare la derivazione in capo al re del suo potere. Dunque, anche gli Stati sono una tecnologia. Le tecnologie invecchiano e diventano obsolete. Mentre gli obiettivi e i bisogni che hanno portato alla loro affermazione sono più che mai vivi ed attuali. Parliamo di sicurezza, prosperità, sviluppo.

Nell'epoca delle piattaforme digitali, gli stati sono dunque destinati a un irreversibile declino?

L'epoca delle piattaforme, abilitata da internet e dal passaggio al digitale entro cui viviamo immersi, presenta uno scenario che poco ha a che fare con quello che ha dato origine allo stato moderno. I soggetti che se ne sono potuti giovare, grandi aziende private, pongono sfide che gli Stati non sono in grado di affrontare. La connessione permanente, l'intelligenza artificiale, l'aumento della capacità di calcolo, i modelli di business e di governo abilitati dai dati sono realtà difficilmente compatibili con realtà territoriali basate su paradigmi del secolo scorso. E ciò negli ultimi anni ha provocato

BIO

Massimo Russo è direttore di « Esquire Italia » e chief product officer Europe di Hearst. In precedenza ha diretto la divisione digitale di Gedi. È stato condirettore del quotidiano « La Stampa » e direttore di « Wired » . Ha scritto saggi sull'incontro tra giornalismo e società digitale, e ha collaborato con Treccani, Istituto Enciclopedia Italiana. Ha fatto parte della Commissione parlamentare incaricata di stendere una carta dei diritti su Internet. Laureato in Economia a Venezia, si specializzato in Giornalismo alla Luiss di Roma e ha lavorato alla Columbia University con una borsa di studio.

squilibri ormai evidenti. Gli Stati si basano su tre pilastri: la sovranità, che si è svuotata ed è diventata sovranismo, il popolo, ormai rappresentato dal simulacro del populismo e l'idea di confini e di territorio, polverizzata dal digitale. Occorrono nuove forme di ingegneria sociale in grado di cogliere queste opportunità e di misurarsi con queste sfide.

Il link motore del neocapitalismo

Il "capitale diventa un link" come viene detto nel suo saggio. Questa affermazione sottende un cambio di paradigma. Dobbiamo e possiamo concludere che il capitalismo tradizionale è giunto al capolinea?

La rete internet ha abilitato modelli economici molto diversi da quelli dell'epoca delle macchine. Prima

serviva un grande capitale per dare il via a un'impresa. Questo capitale era di solito immobilizzato. Pensiamo a un'industria, a un'istituzione finanziaria. Con la rete le connessioni con i tuoi utenti, il loro numero e la loro forza diventano più importanti che mai. Si può operare nella mobilità con il car sharing senza possedere mezzi di trasporto, raccogliere capitali per finanziare imprese con il crowdfunding, diventare un gigante dell'industria ricettiva senza possedere immobili. Le merci, inoltre, diventano sempre più software, pensiamo alle automobili il cui motore cambia caratteristiche con un aggiornamento del sistema operativo. Non significa che il capitalismo tradizionale sia finito. Ma chi sa utilizzare queste nuove opportunità può crescere con molta facilità, anche perché i costi marginali per la produzione di beni o servizi digitali sono decrescenti o tendenti a zero. Non è un caso se negli ultimi vent'anni il 52% delle aziende americane che faceva parte dell'indice Fortune 500 è sparito: acquisizioni, fallimenti, chiusure. E le prime cinque imprese per capitalizzazione sono tutte piattaforme digitali.

Sappiamo (più o meno) quali sono stati gli effetti che la pandemia ha generato sul fronte sanitario. Sul versante geopolitico lo scenario è in evidente mutazione. Cosa dobbiamo aspettarci?

La pandemia è stata un acceleratore dei processi di globalizzazione e di condivisione di conoscenza. Il che non vuol dire che al contrario, non assistiamo a spinte di senso contrario, a nuovi nazionalismi, all'erigersi di nuovi muri, al ritorno di chiusure. Ma si tratta di reazioni forti proprio perché significativi e ineluttabili sono i movimenti tettonici e globali a cui stiamo assistendo. Alcuni paesi potranno decidere di rimanerne fuori, di balcanizzare la rete e il digitale applicando anche ad essi i confini del '900. Ma questo significa anche tagliarsi fuori dai benefici che essi possono portare.

La fine del Leviatano

La diffusione del virus ha creato un bisogno di confinamento. In questa dinamica dobbiamo aspettarci una riemersione del Leviatano di Hobbes?

Il nascere dell'organismo statale in Hobbes, oltre che da ragioni di efficienza, era determinato soprattutto dalla paura della caduta nello stato naturale, della regressione al caos. La paura è una forza fondamentale, un istinto che ci permette di reagire rapidamente al pericolo. Ma nessuno vorrebbe compiere le scelte fondamentali della sua vita basandosi solo sulla paura. Inoltre, la paura è uno straordinario modello di business e di creazione del consenso politico. Infine, è un alibi che ci deresponsabilizza. Di solito indica un capro espiatorio sul quale addossare i nostri fallimenti: "È colpa degli stranieri", "No, delle big-tech", "Del grande complotto". Esercitare la libertà è faticoso.

Democrazia e tecnologia, potere dell'algoritmo come si declina la delicata catena di questi rapporti?

Cos'è un algoritmo? Un insieme di procedure per arrivare a un determinato risultato. Anche la ricetta per la crostata di frutta è un algoritmo. Si può avere paura di una ricetta? Non dobbiamo demonizzare le parole. Certo, la potenza di calcolo e l'intelligenza artificiale, l'uso dei dati, ci pongono nuove sfide, ma sono le sole tecnologie che possono davvero rimettere in moto l'ascensore sociale, creare prosperità, aumentare il numero delle nostre scelte, la qualità della vita. La questione è chi gestisce questo potere. Dobbiamo creare i presupposti perché ciò avvenga nel migliore dei modi. E per farlo le istituzioni devono iniziare a ragionare come piattaforme, mettere i dati a disposizione della crescita, trattare l'immigrazione come una risorsa e non una minaccia.

Bertrand Badie, nel celebre saggio "La fine dei territori" pubblicato 25 anni fa, ci aveva visto giusto?

Badie scriveva al compimento della prima fase della globalizzazione. Ora, con il digitale, la globalizzazione ha accelerato e cambiato di stato. La moneta, la libertà di espressione, il lavoro, i mercati non hanno più

alcuna connotazione territoriale. È proprio per questo che servono nuove tecnologie sociali per governare tale complessità.

Serve una "Costituzione" per Internet

Nella prospettiva di un capitalismo fondato, come dicevamo all'inizio, sulle piattaforme, il cittadino avrà la possibilità di esercitare la sovranità?

Il capitalismo è già fondato sulle piattaforme. Anche le produzioni tradizionali sono cambiate per sempre. Le merci sono software. La parte digitale della catena del valore dei beni è molto più rilevante della parte fisica, pensiamo alle automobili, avviate a trasformarsi in sistemi operativi. Il recupero della sovranità passa attraverso due cambiamenti: a livello sociale dalla trasformazione degli Stati nazionali in piattaforme, e a livello dei singoli dall'esercizio della responsabilità individuale. L'epoca digitale consegna a ognuno di noi nuovi poteri, che richiedono conoscenza e responsabilità per essere esercitati appieno. Serve una nuova alfabetizzazione. La libertà richiede impegno, ma del resto la democrazia non è garantita per sempre. La sua manutenzione dipende da ognuno di noi.

Rodotà si era battuto per la costituzione di Internet, a che punto siamo sul terreno del riconoscimento di questa nuova generazione di diritti?

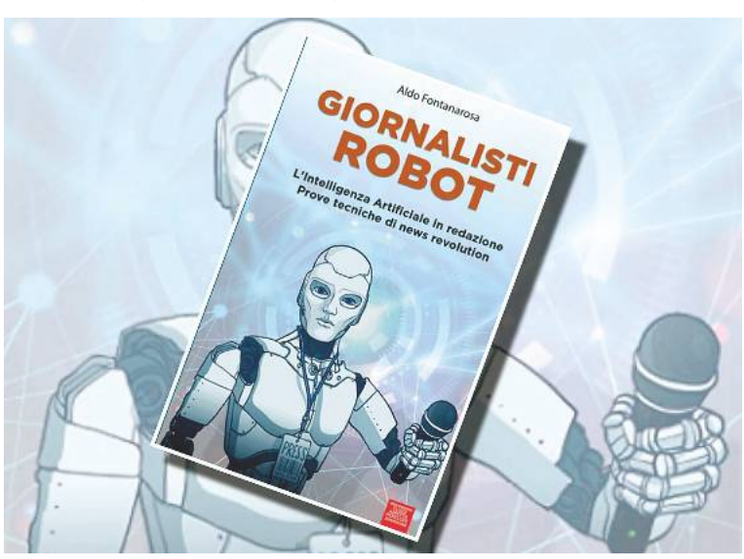
Ho avuto la fortuna di far parte della commissione parlamentare incaricata della stesura di una carta dei diritti per internet, guidata dal professor Rodotà. Credo che gran parte di quell'impianto teorico sia solido. Certo, migliorabile. Ma quando un documento che si occupa di argomenti così rilevanti nasce dall'incontro di diverse sensibilità, non bisogna avere paura delle mediazioni, se non sono compromessi al ribasso. L'applicazione pratica di quanto immaginato dalla carta, tuttavia, è davvero lontana. Esiste una finestra, un'opportunità. Ma dobbiamo muoverci con determinazione, lungimiranza e rapidità. L'Europa ha una cultura dei diritti collettivi, delle libertà individuali, rispetto delle diversità, possiede inoltre una conoscenza tecnologica sufficiente per costruire un umanesimo per l'epoca delle piattaforme. A patto che noi cittadini lo si desideri davvero. ■

Algoritmi e informazione: giornalismo e industria delle notizie cambiano volto

Intervista VIP con Aldo Fontanarosa.

Autore: Massimiliano Cannata

L'intelligenza artificiale entra in redazione, cambiando la macchina editoriale e il modo di produrre e confezionare le notizie. Aldo Fontanarosa, giornalista di Repubblica attento osservatore dell'innovazione in tutte le fenomenologie, nel suo ultimo saggio Giornalisti ROBOT guarda alla sua stessa professione, osservando con equilibrata fiducia l'orizzonte emergente che vede gli algoritmi scrivere in autonomia articoli al servizio di professionisti, che devono imparare a governare questo strumento straordinario. Rilettura critica di un'enorme quantità di dati e sensibilità etica devono essere messe in campo, per non trasformare l'infosfera, in cui viviamo ormai immersi, in una minaccia per la libertà e l'indipendenza dell'informazione.



Aldo Fontanarosa il suo scritto è un affresco fedele della contemporaneità, che vede uomini e macchine operare ormai in simbiosi. Quali scenari si aprono per chi fa il delicato mestiere del giornalista?

Gli scenari che hanno preso forma sono essenzialmente due. Nel primo gli algoritmi sono ormai in grado di scrivere notizie sostanzialmente

BIO

Aldo Fontanarosa si laurea in Scienze politiche all'Università "Federico II" di Napoli nel 1986, poi si specializza in giornalismo all'Università "Luiss" di Roma nel 1989. E' uditore alla Corte internazionale di Giustizia (L'Aia, 1987) e stagista alla Commissione europea (Bruxelles, 1988).
Giornalista professionista, lavora al quotidiano "La Repubblica" dal 1990. Per sei anni alla Cronaca di Roma, è ora alla sezione Economia dove si occupa di diritti dei consumatori, televisione e telecomunicazioni. Anche nel suo blog "Antenne" su Repubblica.it scrive di questi temi. Collabora con il radiogiornale di Radio Capital e con Repubblica Tv, emittente del Gruppo Gedi.
Ha insegnato alla Scuola Superiore di Giornalismo della Luiss, al Master in Comunicazione istituzionale della Luiss, al Master di Giornalismo dell'Università Lumsa di Roma, alla Facoltà di Scienze della Comunicazione dell'Università La Sapienza di Roma. Il suo ultimp saggio è "Giornalisti robot. L'intelligenza artificiale in redazione. Prove tecniche di news revolution" (Ulisse aspetta Penelope, 2020).

indistinguibili da quelle scritte dagli umani. Gli algoritmi partono da un set di dati strutturati. Mi riferisco, ad esempio, ai dati che sintetizzano l'esito di una partita tra Roma e Lazio o tra Milan e Inter. Sulla base di questi dati – risultato, pubblico pagante, ammoniti, espulsi, situazione di classifica, le altre gare della giornata – gli algoritmi realizzano articoli di sintesi puntuali e precisi, sfoggiando per altro abilità stilistiche spiccate. Sanno usare i sinonimi, evitano le ripetizioni, dimostrando, infatti, una padronanza sorprendente.

Quello del giornalismo sportivo è un caso interessante, ma non crediamo l'unico …

Certamente no. Lo stesso meccanismo vale per gli articoli sui conti trimestrali, semestrali, annuali delle aziende. The Associated Press, la grande agenzia d'informazione statunitense, grazie all'algoritmo Wordsmith ha aumentato di dieci volte la produzione di pezzi sui conti economici delle imprese. Pensiamo che adottando lo stesso meccanismo si possono scrivere pezzi sulle previsioni metereologiche.

Fin qui siano dentro l'orizzonte del primo scenario. Vogliamo parlare del secondo?

Il secondo scenario vede donne e uomini, interpreti di un giornalismo di approfondimento e investigazione, servirsi dei software algoritmici più avanzati per realizzare le loro inchieste. Nel 2015, l'agenzia d'informazione The Associated Press – ancora lei - ha vinto il premio Pulitzer, massimo riconoscimento nel campo del giornalismo, grazie all'inchiesta Seafood from slaves. Donne e uomini dell'Associated Press hanno dimostrato che duemila persone vivevano in condizioni disumane in un'isola del Sud est asiatico, costrette ad estenuanti battute di pesca, giorno e notte. La pistola fumante, la prova degli abusi inflitti a questi schiavi è venuta dal satellite che – grazie a software di intelligenza artificiale – ha pedinato dal cielo le imbarcazioni degli schiavisti.

Un "passo oltre"

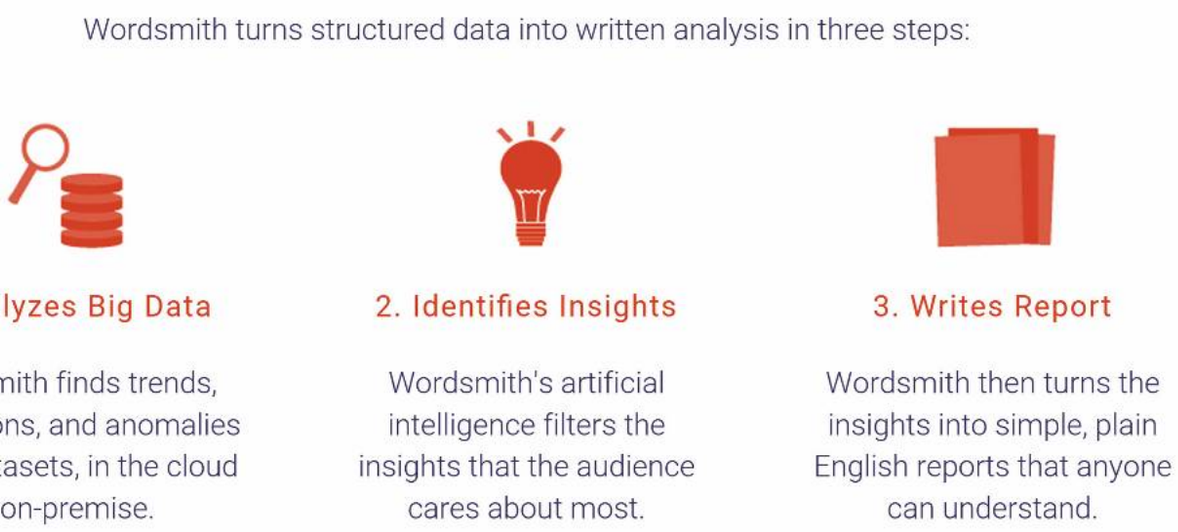
Emanuele Severino, Giuseppe Longo, Carlo Sini, solo per citare alcuni tra i massimi pensatori dell'ultimo secolo riferendosi alla complessa dinamica che caratterizza lo sviluppo della tecno scienza, hanno sostenuto in più scritti che "la contemporaneità è andata un passo oltre" rispetto alla rivoluzione apportata nella modernità dalla diffusione delle macchine. Che cosa c'è da capire di questo stravolgimento profondo, che sta cambiando non solo gli assetti organizzativi dell'impresa, ma il nostro stesso modo di vivere e relazionarci?

Innanzi tutto, occorre comprendere che l'Europa e i singoli Stati devono dotarsi di regole precise. Sono fiducioso che lo faranno, come è avvenuto per il regolamento Gdpr in materia di privacy, che è una soluzione molto efficace. L'intelligenza artificiale è una tecnologia positiva, virtuosa. Ma è anche invasiva e penetrante. Politici e amministratori devono semplicemente piantare una segnaletica stradale e dire agli algoritmi: in questa strada non entri, divieto d'accesso, qui devi svoltare a destra, qui rallentare la tua corsa.

Entrano i robot, paura in redazione. Abbiamo i mezzi per disinnescare questa istintiva paura?

Assolutamente sì. Bisogna spiegare ai cronisti – a quelli magari da poco assunti e ai giovani in cerca di lavoro - che un giornalismo di base, di routine sarà appaltato prima o dopo all'intelligenza artificiale. Questi professionisti, per disinnescare le paure e sterilizzare comportamenti difensivi, devono alzare l'asticella e impegnarsi in un giornalismo di qualità e approfondimento, multimediale e multisensoriale, che le macchine non sono ancora in grado di creare.

Algoritmi di libertà (ed. Donzelli) è un recente titolo di Michele Mezza, che si interroga sul rapporto tra



democrazia, tecnologie e informazione, spiegando come il dato è ormai divenuto un "asset sociale". Dobbiamo temere che l'intelligenza automatica, che elabora e riannoda percorsi di senso, possa togliere l'autonomia e la libertà al cronista in cerca della verità?

Nel 2016, due giornalisti della Süddeutsche Zeitung hanno ricevuto, da una fonte segreta che si faceva chiamare John Doe, 11 milioni e mezzo di documenti che hanno provato forme di elusione ed evasione fiscale tra le più gravi nella storia dell'umanità. Ne è nata l'inchiesta sui Panama Papers. Avere così tanti dati e documenti è come non averne. Undici milioni di immagini non sono esplorabili, consultabili. Senza l'intelligenza artificiale, l'inchiesta non sarebbe stata dunque possibile. Senza i software algoritmici, i giornalisti non avrebbero potuto creare una banca dati navigabile, trovare i nomi degli evasori, dimostrare la fondatezza delle accuse. Ricordo questo importante avvenimento in cui l'intelligenza artificiale non ha certo limitato l'autonomia del cronista, anzi: le ha semmai permesso di esprimersi.

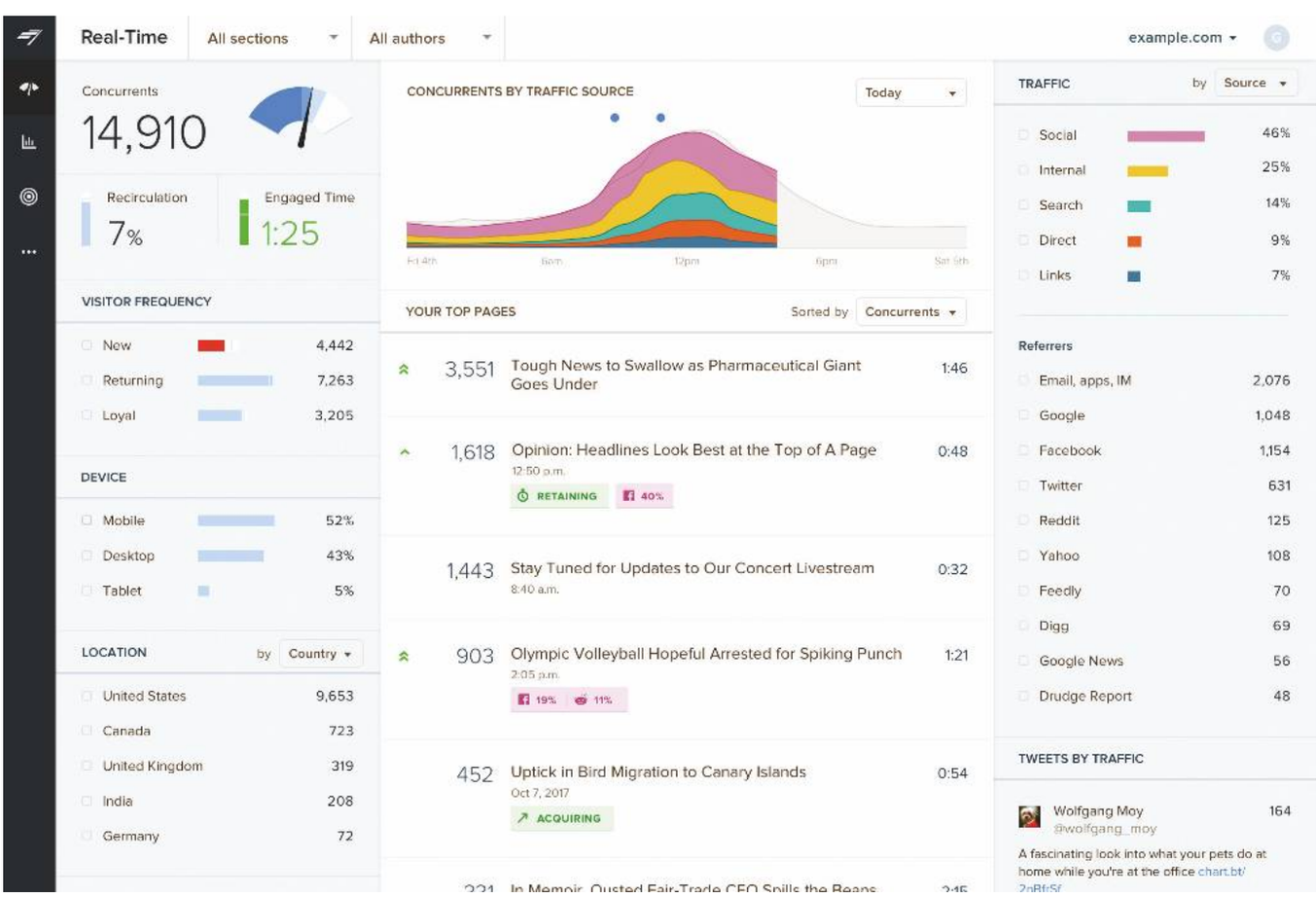
Twitter: ecco il nuovo direttore

La rivoluzione tecnologica è anche una rivoluzione che riguarda la confezione delle notizie e il modo di raccontare i fatti. Se Twitter può, come viene detto in un'interessante scheda del saggio, essere considerato come il direttore di un giornale nell'era del web, cosa dobbiamo aspettarci?

Tutti i grandi editori al mondo tendono l'orecchio alla Rete. Grazie a piattaforme di intelligenza artificiale come Chartbeat, possono disporre di un quadro preciso dei gusti, delle aspettative, delle preferenze dei navigatori dei siti e degli abbonati. Acquisite queste informazioni, gli editori e i giornalisti devono fare una scelta. Seguiranno forse i gusti dei navigatori nel tentativo di fare un traffico sempre maggiore? In questo caso, la Rete sarà il direttore ombra del sito, cosa che giudico negativamente. Il rischio che si presenta in questo modello è di inseguire l'ascolto e il gradimento del pubblico a ogni costo facendo dei clic sui pezzi un'ossessione, quasi una droga. Più virtuoso è l'atteggiamento degli editori e delle redazioni che conservano una piena autonomia di giudizio pur avendo una consapevolezza molto precisa delle aspettative del pubblico".

Machine learning e produzione delle notizie, come si coniuga questo binomio?

Gli algoritmi non sono software statici, non ripetono sempre la stessa cosa. Sono software che evolvono nelle loro competenze grazie all'esperienza e all'osservazione della realtà. Sono macchine che imparano appunto: "machine learning" per riprendere la sua definizione. Questa loro straordinaria attitudine torna utilissima anche nel giornalismo. Quando un algoritmo scrive bene, riceverà un semaforo verde dai programmatori umani: da quel momento, eviterà gli errori e ripeterà le sole azioni corrette. Inoltre, l'algoritmo imparerà dalla lettura degli articoli che gli



"Gemello digitale", legge morale e deontologia

umani hanno scritto in passato a conoscere a fondo il tema di cui si sta occupando al momento. Alla luce di queste sue attitudini, dobbiamo osservare che il *machine learning* risulta decisivo nel giornalismo dell'intelligenza artificiale.

La rete impone la dimensione dell'«intelligenza collettiva», per usare la nota definizione di Pierre Levy. Per un mestiere come il giornalismo legato alla firma, fatto di individualità, non crede che il cambio di prospettiva sia molto forte?

I giornalisti sono per definizione individualisti, se non addirittura narcisi. Non amano molto collaborare con colleghe e colleghi perché smaniosi di apparire come i soli artefici di uno scoop. Questo atteggiamento, a mio parere miope, si scontra con i nuovi modelli dell'era dell'intelligenza artificiale. L'ingresso degli algoritmi in redazione sta portando alla creazione di pool di professionisti chiamati a lavorare in gruppo. Non solo. Editori come Tamedia, in Svizzera, incoraggiano i loro cronisti a condividere le agende telefoniche e i documenti, che confluiscono in banche dati comuni, aperte e navigabili. Banche dati redazionali governate dall'intelligenza artificiale che ne garantisce la navigabilità.

Ognuno di noi ha un "gemello digitale" lo si è visto molto bene nella fase dell'emergenza sanitaria. Dobbiamo pensare che la pandemia ha cambiato l'informazione, che c'è un "avatar" in ogni redazione?

Ce ne sono di tanti tipi. Avatar è il software algoritmico che sbobina, per tuo conto, la registrazione di un'intervista, parola per parola. È un gemello servizievole, che ti solleva da un compito molto ingrato. Avatar sono i conduttori virtuali dell'agenzia d'informazione Xhinua, in Cina, che leggono il telegiornale in inglese e mandarino, con sembianze ed espressioni umane ormai perfette.

Un'ultima considerazione. Vorrei che ci soffermassimo sul delicato incrocio etica, comunicazione e potere. Nell'era dell'IOT e delle tecnologie diffuse è possibile trovare un equilibrio sostenibile tra questi fattori che pesano sul destino stesso delle nostre democrazie?

Le tecnologie evolvono e il loro controllo determina un forte potere in capo a chi le crea e a chi le utilizza, anche nella comunicazione. L'etica, che si fonda su principi universali, deve anch'essa evolvere per rispondere ai nuovi scenari. Anche il giornalismo degli algoritmi deve essere governato dalla legge morale e dalla deontologia. Un esempio su tutti: un articolo è stato scritto da un robot? Molto bene, a patto che venga sempre detto ai lettori, per rispondere a un principio sacrosanto fatto di trasparenza e di lealtà. ■

Secure SecDevOps: come gestire la sicurezza durante lo sviluppo e la progettazione di software e app

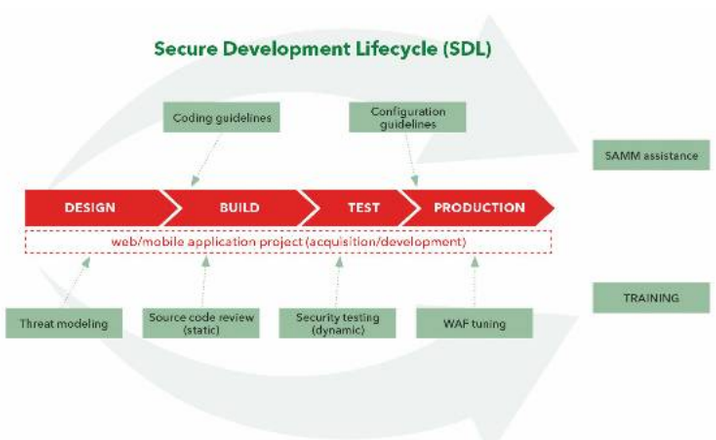
Autore: Lisa Ventura

La sicurezza delle applicazioni è fondamentale per il successo dello sviluppo e della progettazione di software e di app. Quando le organizzazioni ignorano i problemi di sicurezza, espongono le stesse a enormi rischi. Enormi quantità di dati sensibili vengono spesso archiviati nelle applicazioni aziendali e questi dati potrebbero essere rubati in qualsiasi momento e le aziende che non investono nella sicurezza finiscono con l'avere perdite finanziarie e danni reputazionali.

Oltre a ciò, i governi stanno ora applicando leggi e misure di protezione dei dati. L'UE con il GDPR richiede alle organizzazioni di integrare le garanzie di protezione dei dati nelle prime fasi dello sviluppo di software e app. Ignorare questi requisiti, può comportare loro multe consistenti.

Molte organizzazioni seguono la soluzione Secure Development Lifecyle (SDL). Ciò fornisce un approccio strutturato alla sicurezza del software e delle applicazioni ed è un insieme di pratiche di sviluppo per rafforzare la sicurezza e la conformità.

SDL (Secure Development Lifecycle) è un processo di sviluppo che prevede l'uso di diverse attività per aiutare a creare un sistema sicuro.



SDL è suddiviso in questi step:

- **Requisiti:** consiste nella verifica dei requisiti necessari per garantire la piena sicurezza e privacy dell'utente.
- **Implementazione:** la creazione di un codice con tecniche di programmazione difensive che riducono la vulnerabilità del sistema.
- **Verifica:** sviluppato per l'ispezione documentale, il test e la verifica del codice.
- **Rilascio:** comporta la creazione di un piano d'azione che preparerà completamente i team di supporto a risolvere i problemi.
- **Risposta:** eventuali bug o errori rilevati dopo la distribuzione del software possono essere facilmente rintracciati e corretti.
- **Formazione:** comporta la formazione di tutti i membri del team per garantire che tutti siano a conoscenza dei principi e delle tendenze di sicurezza e privacy
- **Design:** utilizzato per esaminare la superficie di attacco delle applicazioni per produrre un modello che contenga le principali minacce.

Dopo aver adottato SDL, come puoi garantire le best practice per quanto riguarda lo sviluppo di software e app? Ecco alcuni modi per farlo che seguono la metodologia SDL:

1. Proteggi la fiducia del brand da parte dei tuoi clienti

Così come i criminali informatici si evolvono, anche i difensori si evolvono. Sono i difensori e le loro organizzazioni che devono stare un passo avanti ai criminali informatici poiché saranno ritenuti responsabili delle violazioni della sicurezza.

Le violazioni che causano indisponibilità del servizio, divulgazione di informazioni sui clienti e minacce alla continuità delle operazioni aziendali possono avere conseguenze finanziarie disastrose. Ma il vero costo sarà la perdita di fiducia nel marchio e la fiducia dei clienti.

Perdite come queste possono essere difficili da quantificare in termini monetari. Il riconoscimento che l'organizzazione è obbligata a proteggere i clienti dovrebbe motivare fortemente le organizzazioni a creare software più sicuro.

2. Comprendere la tecnologia del software

È fondamentale avere una conoscenza approfondita dei componenti infrastrutturali esistenti. Questi includono host hardenizzati, segregazione di rete e infrastruttura a chiave pubblica.

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/

Comprendere i componenti tecnologici all'interno del software è essenziale per determinare l'impatto sulla sicurezza e supportare le decisioni che migliorano la sicurezza del software.

3. Garantire la conformità a privacy, regolamenti e governance

La governance, il rischio e la conformità (GRC) sono fondamentali per molti settori oggi quando si tratta di sviluppo software sicuro.

È fondamentale comprendere le politiche interne ed esterne che governano le organizzazioni, la loro mappatura ai controlli di sicurezza necessari e il rischio

residuo dopo l'implementazione dei controlli di sicurezza nel software.

4. Il software dovrebbe essere progettato con funzionalità sicure

I problemi di sicurezza nella progettazione e altri problemi, come i difetti della logica aziendale, devono

essere esaminati eseguendo modelli di minacce e modelli di casi di abuso durante la fase di progettazione del ciclo di vita dello sviluppo del software.

Nella fase di modellazione delle minacce, viene utilizzata una tecnica strutturata iterativa per identificare le minacce identificando gli obiettivi di sicurezza del software e profilandolo.

5. Il software dovrebbe essere sviluppato con funzionalità sicure

I controlli che riguardano le funzionalità di sicurezza devono essere convalidati e dovrebbero essere messi in atto con revisioni del codice e test di sicurezza efficaci. Questo dovrebbe essere eseguito e complementare contemporaneamente al test di funzionalità.

6. Istruisci te stesso e gli altri su come creare software sicuro

Quando una persona istruita a sua volta educa gli altri, comporta un effetto sulla creazione della cultura della sicurezza di cui c'è tanto bisogno: creare una cultura che includa la sicurezza del software attraverso la consapevolezza e l'educazione che cambiano gli atteggiamenti. La sicurezza del software è responsabilità di tutti.

7. Conoscere le basi della sicurezza del software

Quando si tratta di software sicuro, ci sono alcune cose di base con cui devi avere familiarità: protezione dalla divulgazione, protezione dall'alterazione, protezione dalla distruzione e chi sta effettuando la richiesta. La conoscenza di questi aspetti base e di come possono essere implementate nel software è un must mentre offrono una comprensione contestuale dei meccanismi in atto per supportarle.

Implementando questa serie di suggerimenti sulle best practice, le organizzazioni possono garantire la sicurezza nei loro progetti di sviluppo di software e app. ■

DevSecOps: Di cosa si tratta?

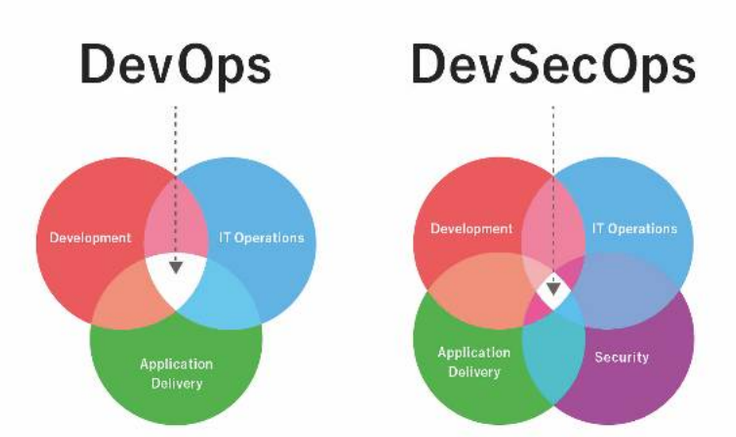
Autore: David Licursi

Mentre le tecnologie, i processi e, soprattutto, i cambiamenti culturali portati da DevOps hanno migliorato la capacità dei team di sviluppo software di generare prodotti affidabili in modo rapido ed efficace, la sicurezza non è stata fin dal principio un punto focale nella trasformazione dell'infrastruttura IT del cloud.

DevSecOps è una metodologia che cerca di affrontare questa lacuna rendendo operativa e rafforzando la sicurezza in tutto il ciclo di vita del software, dal Development, alla Security, alle Operations.

Le origini di DevSecOps

Per capire l'origine di DevSecOps, è utile guardare al movimento che gli ha dato il nome: DevOps. Nel caso di DevOps, i team di sviluppo e di operazioni IT avevano bisogno di allineare le priorità e la comunicazione ed utilizzare l'automazione integrata per portare sul mercato il software più velocemente ed in modo più affidabile. Nei dieci anni dalla sua invenzione, DevOps è stato ampiamente adottato ed il suo impatto è difficile da sottovalutare. Basti dire che la maggior parte dei progressi nello sviluppo del software negli ultimi dieci anni sono stati resi possibili grazie ad esso.

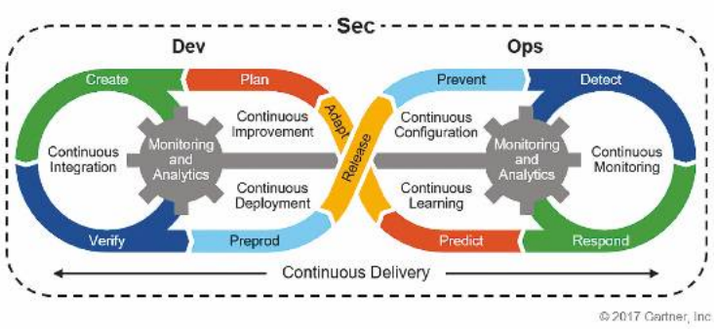


Simile alla relazione tra sviluppo e operazioni IT prima di DevOps, la maggior parte dei team di sicurezza e operazioni IT spesso operano in uno stato di disfunzione che porta a misure di sicurezza IT inefficaci e inadeguate.

DevSecOps è stato inventato principalmente per integrare le pratiche di sicurezza nello sviluppo del software invece di affrontarle ex post.

Definizione ed obiettivi di SecOps

DevSecOps è una metodologia che mira ad automatizzare i compiti di sicurezza cruciali, con l'obiettivo di sviluppare applicazioni più sicure.



La crescita di DevSecOps è trainata in parte dalla trasformazione dell›infrastruttura aziendale e dei modelli di fornitura IT, in quanto sempre

BIO

Ingegnere, David ha conseguito il dottorato di ricerca presso l'Università degli Studi di Udine e svolge attività didattica in ambito manageriale e ICT dal 2014 presso il medesimo Ateneo. È stato direttore della Divisione Telecomunicazioni e poi direttore della Divisione Innovation & Projects di insiel S.p.A. (Trieste) ed ora ricopre il ruolo di Chief Technology Officer presso S3K S.p.A. (Roma), realtà che opera nell'ambito della Sicurezza ICT. Iscritto all'Ordine degli ingegneri della Provincia di Udine, nella sua carriera professionale si è dedicato alla consulenza strategica in ambito ICT, alla progettazione e realizzazione di progetti innovativi in Italia e all'estero e all'attività forense. È fondatore di Digital4PRO, realtà operante nell'ambito dell'informazione e della formazione in ambito tecnologico e manageriale. Padre della splendida Sofia.

più imprese stanno approfittando dei modelli di cloud computing a basso costo e dei vantaggi di velocità e agilità che si ottengono attraverso il cloud.

DevSecOps è la pratica di promuovere una cultura in cui i problemi di sicurezza non iniziano né finiscono con il team di sicurezza.

Mentre un›azienda che condivide password in chiaro non userà controlli di accesso centralizzati da un giorno all›altro, il processo per diventare un team orientato a DevSecOps inizia con l›assicurarsi che il team di sicurezza non sia organizzato per silos e che l'orientamento alla sicurezza venga dall'alto nell'organizzazione.

DevSecOps è più di un sistema di sviluppo del software. È una filosofia, è un'organizzazione, è il ricorso alla tecnologia. DevSecOps incorpora una maggiore collaborazione tra programmatori, progettisti e responsabili della sicurezza per considerare le minacce che potrebbero colpire gli utenti ed il software durante l›intero ciclo di sviluppo.

Come implementare DevSecOps nelle organizzazioni

È chiaro che la sfida è come far funzionare DevSecOps nelle organizzazioni. Sia che vi troviate di fronte a una carenza di talenti nel campo della sicurezza, ad un'organizzazione a silos, a competenze obsolete o a grandi lacune nella percezione della sicurezza, è possibile integrare con efficacia DevSecOps ricorrendo alla giusta strategia.

Vediamo alcuni spunti per incorporare DevSecOps nei propri processi.

1. Partire dai vertici aziendali

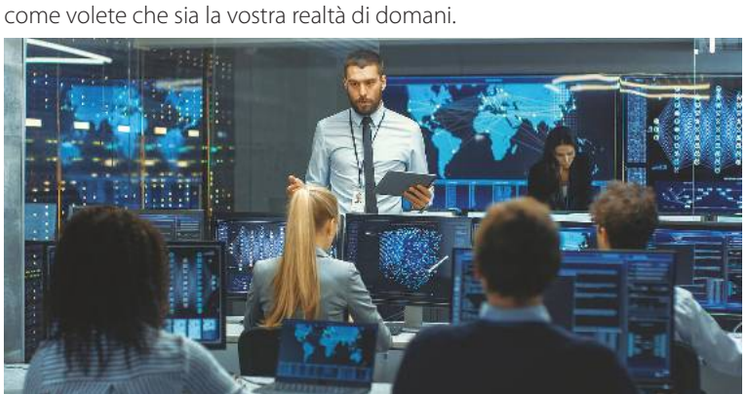
Se i dirigenti non hanno a cuore la sicurezza, non c'è modo che DevSecOps possa avere successo nella vostra organizzazione. La sicurezza ha anche benefici sul ROI, dall'accelerazione dei cicli di vendita all'apertura di mercati completamente nuovi. I dirigenti dovrebbero comprendere i vantaggi di DevOps e dovrebbero sostenere la necessità di processi sicuri e investimenti strategici sia nelle persone che negli strumenti per sostenere la causa DevSecOps.

2. Essere realistici sul posizionamento della vostra organizzazione

È importante capire cosa pensa il vostro team sull'integrazione di DevSecOps e comprendere quanta conoscenza ha su ciò che comporta l›implementazione di DevSecOps. È importante scoprire quali sono gli atteggiamenti dei diversi team e i ruoli verso il valore della sicurezza. L'attuale postura della vostra organizzazione insomma.

Ciò dovrebbe suggerirvi dove esistono lacune percettive e cosa ci vorrà per aprire gli occhi di tutti sulla vostra posizione reale, in modo da poter procedere con determinazione.

Al fine di integrare DevSecOps nella vostra organizzazione, tutte le parti interessate devono avere coscienza della realtà ad oggi e consapevolezza di come volete che sia la vostra realtà di domani.



3. Fornire una formazione SecOps

Alcune organizzazioni possono scegliere di sviluppare internamente la propria formazione e le proprie procedure DevSecOps. Altre possono scegliere di utilizzare strutture esterne e risorse di formazione consolidate. I corsi di terze parti sono facilmente disponibili e possono essere utilizzati per implementare rapidamente il processo di formazione.

I team DevOps devono apprendere come utilizzare gli strumenti di sicurezza e come incorporare le best practice di sicurezza nei propri flussi di lavoro.

I team di sicurezza, parimenti, devono imparare come codificare ed integrare i loro sforzi nei cicli di deployment continuo.

Non aspettatevi che questo processo avvenga organicamente, sarà necessario fare un investimento consapevole nell'allineamento e nell'educazione tra i team. Solo così DevSecOps avrà la possibilità di diventare una realtà nella vostra organizzazione.

4. Valutare i rischi e dotarsi di una lista di priorità

Considerando gli aspetti da affrontare in tema di sicurezza, dopo la formazione di cui ci siamo già occupati, risulta senz'altro vantaggioso iniziare con l'infrastruttura, perché è questa l'area che espone ai rischi più alti ed è più facile da mettere in sicurezza.

Assicuratevi di seguire le migliori pratiche di gestione della configurazione e di implementare gli avvisi di sicurezza che sono ben sintonizzati con la

vostra organizzazione. Proteggere la vostra infrastruttura avrà un effetto a catena su tutta l'organizzazione, dallo sviluppo software alle operazioni.

5. Lavorare in squadra

Uno dei vantaggi di DevSecOps è il miglioramento del lavoro di squadra tra tutte le aree coinvolte nella produzione del software.

Avere una più stretta collaborazione tra i team mitigherà il problema di mettere d'accordo i team di sicurezza e i team di sviluppo,

6. Fornire strumenti DevSecOps adeguati

Oltre ai popolari strumenti di sviluppo (GitHub, AWS, Microsoft…), alcuni strumenti di sicurezza possono aiutare ad implementare DevSecOps nella vostra organizzazione mantenendo la necessaria velocità operativa.

Le piattaforme di automazione possono gestire molte delle procedure di sicurezza e si accoppiano perfettamente con un processo DevSecOps ben documentato.

Le persone sono importanti, ma i cambiamenti culturali non avvengono (in DevOps o altro) senza la tecnologia che li abilita. Per DevOps, questo è stato l'automazione, l'infrastruttura-come-codice (IaaC) e la disponibilità di risorse cloud che hanno dato ad entrambi i team l'accesso alla velocità e alla precisione necessarie per attuare DevOps.

Mentre le soluzioni di automazione della sicurezza come SOAR (security orchestration, automation and response) hanno migliorato la capacità dei team di sicurezza di snellire i flussi di lavoro e identificare le minacce più velocemente, i team DevSecOps devono utilizzare gli strumenti esistenti e nuove soluzioni per coordinare l'azione automatizzata fino al rimedio e al reporting a ciclo chiuso.

7. Essere determinati nell'implementazione

Quando si tratta di implementare un programma DevSecOps integrato, la vostra organizzazione deve essere assolutamente determinata. Le implementazioni DevSecOps di maggior successo includono:

- **Strategia:** Anche le migliori ambizioni nei confronti dell'integrazione della sicurezza e delle operazioni possono disintegrarsi se non c'è una strategia perseguibile dietro di esse.
- **Responsabili chiaramente designati:** Bisogna coinvolgere le persone giuste. Meglio se con approccio top-down. Come abbiamo scritto, i dirigenti devono guidare la nave.
- **Formazione:** Ci può essere un grande divario di comprensione tra la sicurezza e i team DevOps, quindi è essenziale preparare i team e implementare un programma di consapevolezza della sicurezza in tutta l'organizzazione.
- **Processi chiari:** Con persone che ora lavorano insieme e che potrebbero non aver lavorato insieme prima, e con diversi strumenti necessari per svolgere il lavoro, sono necessari processi chiari e ben documentati.
- **Metriche di successo comuni:** Dopo aver profuso molto lavoro nel vostro piano DevSecOps, dovreste essere in grado di dimostrare che questo sta effettivamente funzionando. Dovreste dotarvi di alcune metriche o KPI, come il Mean Time To Know, per mostrare i miglioramenti quantitativi dalla vostra implementazione DevSecOps. Soprattutto, questi dovrebbero essere KPI condivisi tra i team.

Quali ostacoli si incontrano nell'implementare DevSecOps

La necessità di DevSecOps è probabilmente meglio evidente dal fatto che moltissime organizzazioni che hanno subito una violazione della sicurezza avrebbero potuto evitare l'incidente con una patch o una modifica di una configurazione. Per quali ragioni?

1. Non c'è abbastanza personale

È esperienza comune che le professioni legate alla sicurezza in particolare e all'ICT in generale stanno sperimentando una massiccia carenza di talenti. Anche una fornitura illimitata di esseri umani di talento, tuttavia, non potrebbe risolvere le sfide della sicurezza di oggi. I sistemi sono molto complessi e i criminali stanno diventando più veloci.

2. La velocità e l'adozione degli strumenti hanno la priorità sulla sicurezza

I team operativi si preoccupano assolutamente della sicurezza, ma vivono in un mondo governato dall'innovazione, dalla crescita e dall'uptime a cinque nove. I team operativi sono responsabili non solo di mantenere ambienti in rapida crescita e sempre più ingombranti, spesso composti da decine di migliaia di sistemi individuali, ma anche di utilizzarli per fornire sempre più valore all'azienda ed ai suoi clienti.

I team di sicurezza e quelli operativi lavorano con strumenti e flussi di lavoro completamente separati che richiedono la traduzione delle informazioni ogni volta che vengono scambiate tra i team. Questo rende quasi impossibile la verifica ed il reporting.

3. L'innovazione supera in velocità la sicurezza

Mentre le innovazioni di prodotto e servizio avanzano a velocità frenetica spinte dal mercato, la sicurezza rimane affannosamente indietro. Questo non significa che non ci siano state innovazioni di sicurezza, ma la maggior parte di esse sono state una reazione alle vulnerabilità e alle lacune create dal mutevole panorama ICT, piuttosto che sforzi proattivi per contribuire a modellarlo in modo sicuro.

I vantaggi di DevSecOps

Possiamo di seguito evidenziare i principali vantaggi che derivano dall'incorporazione di DevSecOps nel processo di sviluppo:

- **Ritorno sull'investimento:** Il beneficio numero uno è il Return on investment (ROI) rispetto all'adozione di misure di sicurezza secondo le organizzazioni a silos;

- **Miglioramento della produttività:** Con le procedure di sicurezza dispiegate nell'intero processo di sviluppo, le operazioni sono nel complesso più produttive;
- **Risorse ridotte:** Il miglioramento delle prestazioni fornisce un migliore utilizzo dello storage e dei servizi cloud, riducendo o utilizzando meglio le risorse;
- **Meno problemi di sicurezza nel cloud:** Le operazioni DevSecOps adottano misure per migliorare la sicurezza delle piattaforme cloud e diminuire il rischio di problemi e minacce legate a queste piattaforme;
- **Meno interruzioni delle applicazioni:** Migliori implementazioni di sicurezza si tradurranno probabilmente in meno problemi con l'applicazione sviluppata. Meno tempi di inattività significa una migliore esperienza utente e un migliore ambiente di sviluppo;
- **Migliori procedure di controllo:** In Agile e altri metodi di sviluppo, i controlli di sicurezza avvengono verso la fine del processo di sviluppo. DevSecOps fornisce valutazioni più ponderate e fluide;
- **Riduzione degli errori di configurazione:** Implementando un'organizzazione DevSecOps scende l'incidenza degli errori di configurazione;
- **Gestione proattiva delle vulnerabilità** conosciute;
- **Conformità agli standard:** Le politiche per la conformità con gli standard appropriati sono automaticamente controllate e applicate;
- **Automazione:** Le procedure di sicurezza chiave, così come i compiti delle figure coinvolte, in DevSecOps sono automatizzate;
- **Migliore sicurezza in ambienti cloud:** DevSecOps è meno legato a specifiche soluzioni basate sull'hardware. Piuttosto, si concentra su pratiche di sicurezza ben definite che possono essere automatizzate in particolare negli ambienti cloud;
- **Migliore comunicazione tra i team:** La collaborazione tra team significa meno casi di perdita di informazioni chiave con riferimento alla sicurezza.

Conclusioni

La velocità del business sta sollecitando cambiamenti radicali nel modo in cui si affrontano lo sviluppo del software, la gestione delle Operations IT e la Security. Vi è infatti l'esigenza di accorciare i tempi della messa in produzione e di aggiornamento continuo del software, un problema affrontabile solo con la piena sinergia dei processi coinvolti, attraverso metodi come DevSecOps.

In fondo non si tratta di una scelta. Lo scenario dettato dal mercato e dalle possibili minacce suggerisce un'inevitabile adesione al modello completo DevSecOps.

Se la vostra azienda costituisce un nuovo team di sviluppo, o qualora si costituisca una nuova azienda, la scelta più opportuna è sicuramente quella di aderire fin dall'inizio alla metodologia DevSecOps. In questo caso, il vantaggio competitivo nei confronti della concorrenza è determinante nel successo sul mercato.

Da ultimo sottolineo come il dimenticare di mettere in atto, sin dalla progettazione e prima che inizi il trattamento dei dati, tutte le misure tecniche ed organizzative necessarie ad attuare i principi di protezione dei dati, si configuri essenzialmente come un'inosservanza dell'art. 25 del GDPR. ■

SecDevOps: perché è importante e da dove partire

Autore: Elena Mena Agresti

Quante volte abbiamo sentito parlare di DevSecOps e SecDevOps? Spesso utilizzati impropriamente come sinonimi nascondo invece una differenza sostanziale. Per capirla basata notare la posizione del termine "Sec" nella parola.

DevSecOps presenta la sequenza "Dev", "Sec" e "Ops" e si riferisce ad una modalità con la quale prima viene effettuato lo sviluppo di un software (Dev), poi sono presi in considerazione gli aspetti di Sicurezza (Sec) e infine l'Operation (Ops).

SecDevOps prevede invece la sicurezza "Sec" all'inizio della pipeline ancor prima dello sviluppo (Dev). Adottando questo approccio gli aspetti di sicurezza dalle politiche, linee guida, standard di sviluppo, requisiti di sicurezza saranno integrati in tutto il ciclo di vita del software. Inoltre, questa modalità si trasforma in un circolo virtuoso riuscendo a formare naturalmente tutto il team sul ruolo e gli aspetti di security. Infatti, mentre nell'approccio DevSecOps il team di Sviluppo continuerà a creare il software indipendentemente dai requisiti di sicurezza nel SecDevOps dovrà adottarli fin dall'inizio acquisendo nel tempo competenze e sensibilità sulla materia.

È necessario sottolineare inoltre l'effort richiesto nei due approcci. Nel primo, DevSecOps, la security viene considerata quasi come un layer aggiuntivo da prendere in considerazione solo a software definito. Implementare i requisiti di sicurezza in questa fase potrebbe risultare molto oneroso, meno efficace o di difficile implementazione. Non a caso spesso si ripiega sull'assunzione del rischio preferendo mandare in esercizio un sistema seppur non completamente sicuro pur di rispettare il time to market.

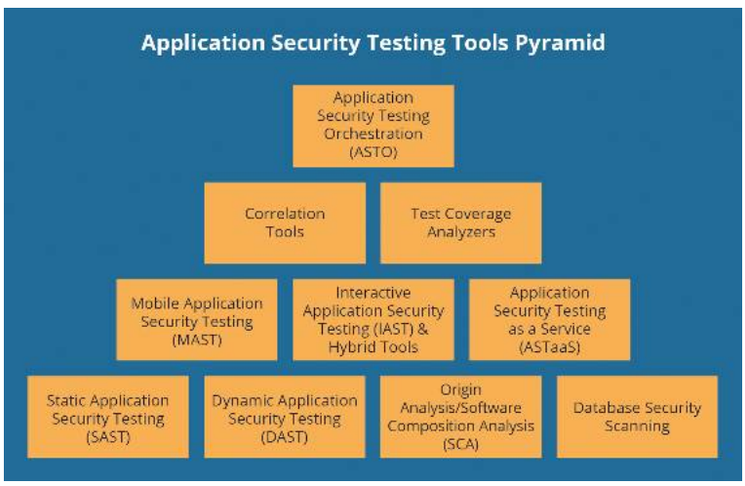
Un corretto approccio anche in linea con gli ultimi standard, normative e direttive internazionali è il SecDevOps. Ma come metterlo in campo? Quale può essere un corretto approccio?

BIO

Laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma, opera per la Fondazione GCSEC e il CERT di Poste Italiane. Esperta di compliance, standard internazionali, governance dell'information security, gestione dei rischi, security audit, formazione eawareness, ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security.
È stata responsabile scientifico di tre corsi di master in cyber security istituiti nel 2015-2016 con l'Università della Calabria e Poste Italiane eattualmente collabora con numerose università italiane in corsi di cyber security. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Membro di Europrivacy e della Oracle Community for Security, è Lead Auditor ISO/IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

Il principio base è considerare la sicurezza nelle primissime fasi di definizione di un nuovo software alla stregua degli obiettivi e requisiti di business e non come layer aggiuntivo. Questo richiede un cambiamento culturale dell'azienda e nei modelli organizzativi e procedurali condividendo la responsabilità della sicurezza tra tutti i team.

È sicuramente utile automatizzare le attività e adottare strumenti di testing in tutte le fasi dello sviluppo. Sono disponibili numerose tecnologie a disposizione degli sviluppatori per rilevare i difetti di sicurezza prima che vengano integrati in una versione finale del software. Tra questi troviamo le tecnologie tradizionali SAST e DAST o le più recenti IAST e RASP che vanno a sopperire le difficoltà delle prime in merito nella gestione di librerie e dei framework presenti nelle app moderne. Ognuno di questi tool potrebbe essere utilizzato in diverse fasi del ciclo di vita del software.



La tecnologia SAST (Static Application Security Testing), in modalità "white box", consente di identificare le vulnerabilità di sicurezza presenti nel codice sorgente già nelle prime fasi del ciclo di vita dello sviluppo senza la necessità di eseguire il codice sottostante. La risoluzione delle vulnerabilità inoltre è meno onerosa e più veloce. È tuttavia un'analisi statica, non può riconoscere le vulnerabilità del codice in esecuzione che rileva invece la tecnologia DAST (Dynamic Application Security Testing). DAST inserendo degli errori in un›applicazione in esecuzione, in genere app web, identifica vulnerabilità e bug comuni (es. SQL injection e cross-site scripting) e mette in risalto i problemi di runtime non identificabili da un'analisi statica.

Elementi delle tecnologie SAST e DAST tra loro complementari sono integrati nella tecnologia IAST (Interactive Application Security Testing) producendo risultati più accurati verificando una gamma più ampia di regole di sicurezza rispetto a SAST o DAST. Pensati per essere eseguiti nell›application server, come agent non richiedono l'istallazione di plug-in né la modifica di applicazioni o attività di penetration test. L›analisi viene condotta dall›interno dell›applicazione attraverso l'inserimento di funzionalità in determinati punti dell›esecuzione dell'applicazione. Le tecnologie IASR rilevano, infatti, in tempo reale problemi di sicurezza analizzando il traffico e il flusso di esecuzione delle applicazioni. Non è necessario modificare le applicazioni, né condurre specifiche attività di penetration testing.

Di recente adozione è anche la tecnologia RASP (Run-time Application Security Protection) uno strumento di test che consente a un›app di eseguire controlli di sicurezza continui su sé stessa e di rispondere agli attacchi in tempo reale terminando la sessione di un utente malintenzionato e avvisando i difensori dell›attacco.

È importante sottolieare che pur rispondendo ad una serie di carenze delle SAST e DAST, le nuove tecnologie IAST e RASP possono avere un effetto negativo sulle prestazioni delle applicazioni.

Una tecnologia abbastanza recente e molto utile per proteggere la catena di fornitura del software è, invece, la tecnologia SCA (Software Composition Analysis). La SCA non effettua l'analisi statica e dinamica del software ma verifica le librerie, i framework e i componenti di terze parti utilizzati all›interno della tua applicazione, un aspetto assolutamente da non sottovalutare!

Sono numerosi ormai gli incidenti di sicurezza causati da prodotti di terze parti non adeguatamente verificati sui quali sono state sfruttate vulnerabilità applicative e/o aggiunte componenti malevole.

Considerare le terze parti non è più un optional ma un requisito minimo. Non a caso sono in fase di sviluppo diversi framework in questo ambito. Tra tutti ricordiamo SLSA[1] (Supply chain Levels for Software Artifacts) il framework di Google volto a proteggere la pipeline di sviluppo e distribuzione del software end-to-end e mitigare le minacce in ogni anello della sua catena.

La soluzione si ispira all'"Autorizzazione binaria per Borg" interna di Google e si basa su due principi fondamentali la **non unilateralità**, ovvero nessuno può modificare l'artefatto software in qualsiasi punto della catena di fornitura del software senza un'esplicita revisione e approvazione da parte di almeno un'altra "persona di fiducia" e la **verificabilità**, ovvero l'artefatto software può essere ricondotto in modo sicuro e trasparente alle origini e alle dipendenze originali leggibili dall'uomo. Lo scopo principale è l'analisi automatizzata di fonti e dipendenze, nonché indagini ad hoc.

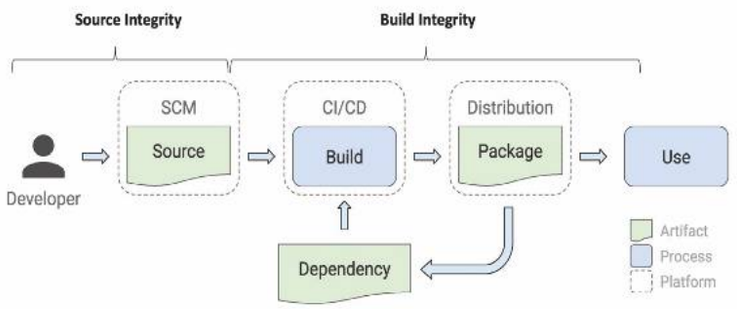
SLSA include al suo interno serie di standard, strumenti per automatizzare la creazione di metadati per l'auditing,

un processo di accreditamento per certificarne la conformità agli standard e controlli tecnici (ancora in woking progress).

Il framework presenta anche un approccio a quattro livelli di protezione SLSA.[2] Più il livello è alto maggiore sarà la protezione dagli attacchi. Ad oggi livello corrispondono delle garanzie di integrità incrementali. Dal livello SLSA1 che richiede il processo di compilazione completamente automatizzato e che generi la provenienza, al livello SLSA4 che oltre a includere tutti i livelli precedenti aggiunge requisiti ancora più stringenti quali sono la revisione obbligatoria di tutte le modifiche da parte di due diversi sviluppatori.

Non parliamo quindi di un semplice elenco di regole e best practice. Come affermato da Kim Lewandowski del Google Open Source Security Team e Mark Lodato del Binary Authorization for Borg Team *"In its final form, SLSA will differ from a list of best practices in its enforceability: it will support the automatic creation of auditable metadata that can be fed into policy engines to give "SLSA certification" to a particular package or build platform".*

Di seguito alcuni esempi di attacchi che si possono verificare in ongi anello della catena di fornitura e una tabella su come SLSA può essere utile[3].



In conclusione, prima le organizzazioni introdurranno il modello SecDevOps e prima riusciranno a fronteggiarle lo scenario di minacce e ad essere competitive sul mercato. Non sarà una transizione immediata ma graduale. Il primo passo sarà dunque indurre un cambiamento culturale e organizzativo distribuendo le responsabilità della security e innescando un circolo virtuoso di formazione.

Sarà indispensabile comprendere e considerare ogni tipologia di software e componente utilizzata nell'organizzazione così come adottare gli strumenti di testing in tutte le fasi del ciclo di vita del software. Un'attenzione particolare dovrà essere risposta alla gestione dei rischi legati alle terze parti, negli ultimi anni molto sottovalutata. ■

1 https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html
2 https://github.com/slsa-framework/slsa
3 https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html

	Threat	Known example	How SLSA could have helped
A	Submit bad code to the source repository	Linux hypocrite commits: Researcher attempted to intentionally introduce vulnerabilities into the Linux kernel via patches on the mailing list.	Two-person review caught most, but not all, of the vulnerabilities.
B	Compromise source control platform	PHP: Attacker compromised PHP's self-hosted git server and injected two malicious commits.	A better-protected source code platform would have been a much harder target for the attackers.
C	Build with official process but from code not matching source control	Webmin: Attacker modified the build infrastructure to use source files not matching source control.	A SLSA-compliant build server would have produced provenance identifying the actual sources used, allowing consumers to detect such tampering.
D	Compromise build platform	SolarWinds: Attacker compromised the build platform and installed an implant that injected malicious behavior during each build.	Higher SLSA levels require stronger security controls for the build platform, making it more difficult to compromise and gain persistence.
E	Use bad dependency (i.e. A-H, recursively)	event-stream: Attacker added an innocuous dependency and then updated the dependency to add malicious behavior. The update did not match the code submitted to GitHub (i.e. attack F).	Applying SLSA recursively to all dependencies would have prevented this particular vector, because the provenance would have indicated that it either wasn't built from a proper builder or that the source did not come from GitHub.
F	Upload an artifact that was not built by the CI/CD system	CodeCov: Attacker used leaked credentials to upload a malicious artifact to a GCS bucket, from which users download directly.	Provenance of the artifact in the GCS bucket would have shown that the artifact was not built in the expected manner from the expected source repo.
G	Compromise package repository	Attacks on Package Mirrors: Researcher ran mirrors for several popular package repositories, which could have been used to serve malicious packages.	Similar to above (F), provenance of the malicious artifacts would have shown that they were not built as expected or from the expected source repo.
H	Trick consumer into using bad package	Browserify typosquatting: Attacker uploaded a malicious package with a similar name as the original.	SLSA does not directly address this threat, but provenance linking back to source control can enable and enhance other solutions.

DevSecOps: Integrare la sicurezza in ogni aspetto del ciclo di vita di distribuzione del software

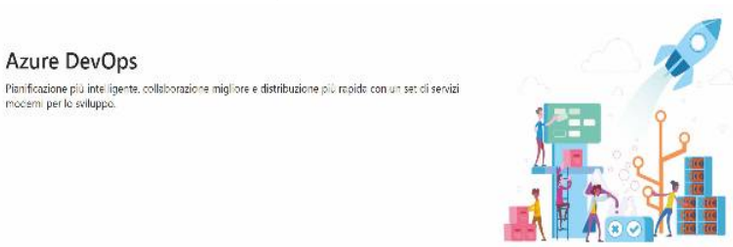
Autori: Alessandro Nava, Matteo Creati

Negli ultimi anni stiamo assistendo ad un cambiamento epocale dell'approccio al rilascio di software e creazione di nuove applicazioni in generale. I nuovi processi di DevOps prevedono infatti un forte cambiamento culturale che porta i team di sviluppo e operation ad una maggiore collaborazione per far fronte ad una pressione imposta dal business che non si era mai vista.

Il Time To Market richiesto per rilasciare al mercato nuovi servizi è estremamente sfidante e ha portato le strutture a supporto del business a dover rilasciare nuove funzionalità e soluzioni in tempi molto ridotti.

A queste velocità è facile immaginare come chi si occupi di sviluppo abbia la necessità di focalizzarsi il più possibile sul coding lasciando la definizione degli ambienti di sviluppo alle operation che a loro volta, per far fronte alla agilità richiesta, hanno trovato nel Cloud, la velocità e automazione necessarie per raggiungere gli obiettivi di rilascio richiesti dal business.

Le nuove practice e soluzioni hanno permesso agli sviluppatori di passare allo sviluppo agile spostando la strategia da applicazioni monolitiche a soluzioni a microservizi garantendo cicli di sviluppo molto più veloce, e cambiando così il modello operativo.



IDC ha previsto che entro 5 anni verranno realizzate fino a 500 milioni nuove applicazioni, che corrispondono al numero di applicazioni create negli ultimi 40 anni *(IDC FutureScape: Worldwide IT Industry 2019 Predictions)*.

E questi cambiamenti hanno portato anche nuove sfide per i CISO che si trovano a definire la strategia di sicurezza in ambienti Cloud e Multi Cloud in modo completamente diverso rispetto all' on premise. In passato,

BIO

Alessandro Nava,
Sr. Enterprise Security Executive
In Microsoft ha la responsabilità del business per le soluzioni di Security, Compliance e Identity nel mercato FSI. Ha seguito da vicino i processi analisi del dato in ambito anti-frode e gestione del rischio per importanti istituti finanziari, prima di iniziare a occuparsi di compliance, cyber security e di Zero Trust in ambito Cloud e Multi-Cloud.

BIO

Matteo Creati,
Cloud Solution Architect
In Microsoft ha la responsabilità di sviluppare il business Azure con focus su soluzioni di Security sia in Cloud che nel mondo Hybrid. Ha una forte esperienza in ambito Identity e Security, si occupa anche di sviluppare ed implementare soluzioni Open Source in Azure.

infatti, la Security era responsabilità di team dedicati che intervenivano a posteriori, ma le nuove metodologie DevOps, i nuovi cicli di sviluppo cloud-native, piu veloci e frequenti, hanno portato la Security ad essere sempre più continua e integrata in tutte le fasi dei processi di sviluppo, spostando l'attenzione all'inizio della pipeline CI/CD e automatizzando le attività di controllo, con l'obiettivo di non rallentare il ciclo di sviluppo.

Ma con la nuova metodologia DevSecOps, anche gli sviluppatori sono chiamati a ripensare la creazione del codice e a condividere con molta più frequenza feedback e informazioni sulle vulnerabilità note ai team di sicurezza. Questo nuovo approccio "Security By Design", porta ad un cambiamento culturale mai visto in precedenza e non secondario.

Diverse ricerche di mercato ci fanno notare come negli ultimi anni, più del 70 % delle vulnerabilità, arrivano dalle applicazioni e Forrester *(Forrester's State of Application Security, 2021 Report)* conferma come il passaggio al lavoro remoto abbia infatti spinto le aziende a fare ancora più affidamento sulle applicazioni, e questo spiega perché le applicazioni web sono oggi la forma più comune di attacco, seguita da vulnerabilità del software.

Secondo il NIST *(National Institute of Standards and Technologies)*, il costo di fix delle vulnerabilità, una volta che il codice è in produzione, può essere 60 volte più oneroso rispetto che nelle fasi di sviluppo. Se pensiamo ad esempio come i processi di Infrastructure as Code (IaC), aiutino a scalare e ridurre i tempi di sviluppo, ci rendiamo subito conto come vulnerabilità o mis-configurations non identificate all'inizio del processo, possano essere esponenzialmente replicate alle velocità del cloud.

In scenari come questi, così fluidi ed eterogenei, un errore che rileviamo è quello di utilizzare ancora soluzioni specifiche per il singolo processo *(single-point solutions)* e non un approccio a piattaforma, coprendo così solo una parte del problema e creando competenze verticali che non garantiscono un passaggio trasversale di competenze nei team, e portando l'azienda a dover gestire numerosi contratti a condizioni diversi tra numerosi fornitori.

Una piattaforma di sicurezza nativamente integrata nei processi di sviluppo aiuta le best practices DevSecOps ad aumentare la visibilità ed a gestire in modo olistico e ZeroTrust tutta una serie di problematiche quali vulnerability assessment, runtime security, la micro segmentazione a livello Multi Cloud, la governance degli access ecc.

Grazie ad Azure Security Center e le funzionalità di Azure Policies e Azure Compliance Manager, i team di sicurezza possono iniziare ad avere un primo controllo del rischio, della postura e compliance delle risorse a livello Cloud e Multi Cloud (CSPM). Le best practice suggerite da Microsoft basano il loro valore nella protezione che Azure Security Center può offrire per la gestione degli accessi e nelle fasi iniziali di sviluppo, spostando sempre più a sinistra la protezione dei workload, per esempio identificando vulnerabilità nelle immagini dei container (Azure Container Registry), proteggendo le istanze del servizio Azure Kubernetes oppure sfruttando Azure Arc per proteggere workload fuori Azure (CWPP).

L'adozione di Github è chiaramente un primo passo per migliorare la postura in termini di sicurezza del mondo DevOps. Ma è solo l'inizio.

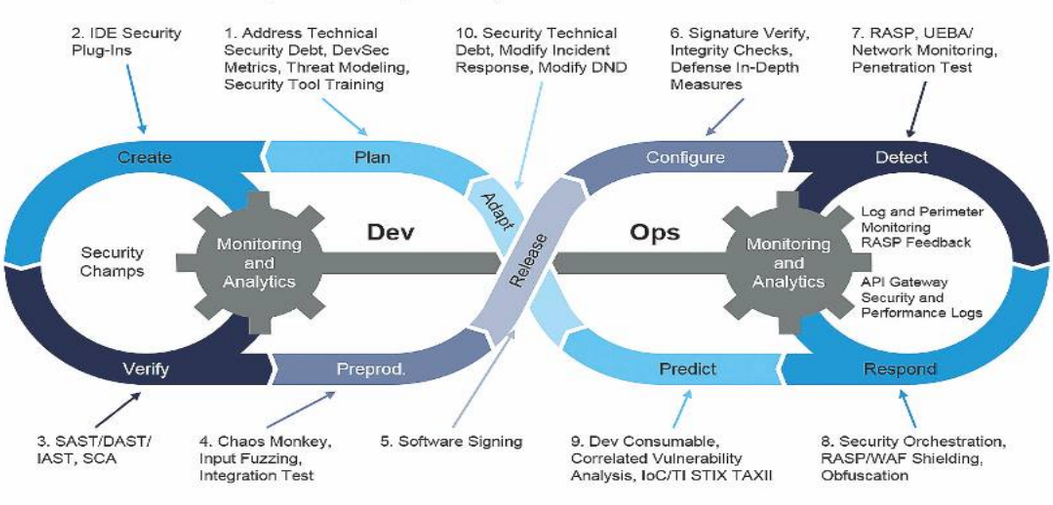
Molte sono le strategie atte a modificare il codice sorgente tramite il quale è possibile veicolare un attacco informatico. Il caso di Solarwinds è solo l'ultimo. La risposta di Microsoft per cercare di mitigare queste vulnerabilità prende il nome di **DevSecOps**.

DevSecOps, si basa sui principi di DevOps , ma aggiunge una maggiore attenzione alla sicurezza. Con DevSecOps, la sicurezza diventa una parte centrale dell'intero ciclo di vita dell'applicazione e riesce anche a forzare una standard di lavoro per un gruppo anche distribuito. Questo concetto è "Shift-Left Security": spostamento della sicurezza permette di intercettare criticità dalle prime fasi di sviluppo includendo anche la gestione di vulnerabilità dei framework utilizzati per lo sviluppo.

Microsoft e GitHub offrono soluzioni che permettono di eseguire codice certificato in ambienti di produzione, esaminando anche la relativa tracciabilità soprattutto per i componenti di terze parti in uso.

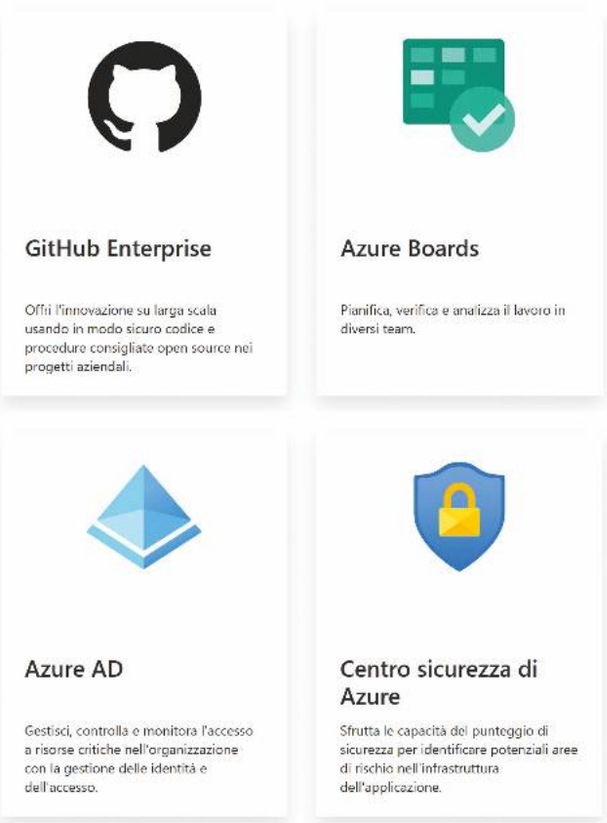
Questa unione ha permesso di gestire in modo strategico la sicurezza in tutte le fasi di gestione delle applicazioni.

Gartner's Model for a Complete Security Development Toolchain



ID: 368366

I quattro componenti in Azure che garantiscono questa sicurezza end-to-end in Ambienti DevSecOps sono:



GitHub, la piattaforma per sviluppatori più diffusa al mondo, offre funzionalità avanzate che contribuiscono alla protezione del codice e delle dipendenze delle applicazioni con:

- GitHub Advanced Security sfrutta CodeQL, il motore di analisi semantica del codice per identificare vulnerabilità nel codice.
- Identifica e correggi i problemi di sicurezza nelle dipendenze usando gli avvisi di sicurezza e gli aggiornamenti automatici della sicurezza (Dependabot).

Grazie all'uso di Azure Pipelines per l'integrazione continua, il codice viene compilato e inserito in pacchetti in un contenitore Docker cifrati e formati, specialmente su repositories di tipo privato.

Le immagini applicative di produzione vengono archiviate in Azure Container Registry, dove vengono analizzate automaticamente per rilevare vulnerabilità grazie all›integrazione con il Centro sicurezza di Azure.

Tramite il Centro di Sicurezza (Aure Defender) è possibile governare l'intera supply chain del software. Tutte le nuove applicazioni create sfruttano codice scritto da terze parti, inclusi componenti open source. Benché questo approccio offra vantaggi chiari, incrementando la produttività e migliorando la collaborazione, crea anche difficoltà correlate al controllo e alla protezione della supply chain per il software.

Spesso ci si trova a capire come integrare controlli di questo tipo su ambienti collaudati ed in esercizio.

Spesso per i CISO questo tipo di approccio richiede uno studio più o meno complesso e spesso tende a far percepire una situazione di rallentamento delle attività. È utile in questi casi utilizzare una strategia tecnica di implementazione secondo questi 3 pillars:

Questa strategia permette di accelerare l'adozione dei servizi di sicurezza di DevSecOps in modo strutturato.

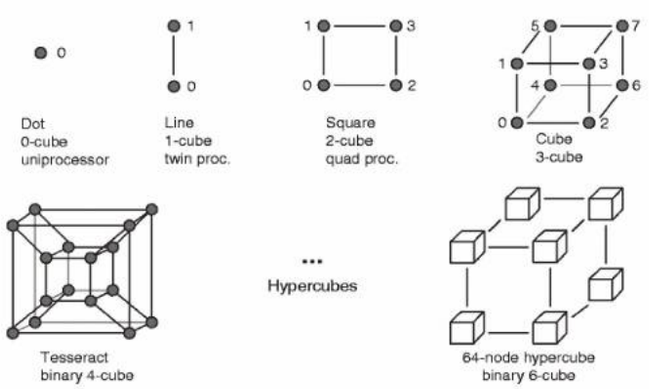
Microsoft si trova in una posizione privilegiata perché conosce molto bene le sfide in ambito DevOps, ed è anche molto attenta a garantire competenze verticali e consulenti in grado di seguire end-to-end i processi DevSecOps.

Vi invitiamo a seguire la nostra Security Community (Sign In) per webinars, video e aggiornamenti e contattarci direttamente o attraverso i nostri partners per ricevere maggiori informazioni. ■

Dalla processazione parallela al computer quantistico

Autore: Francesco Corona

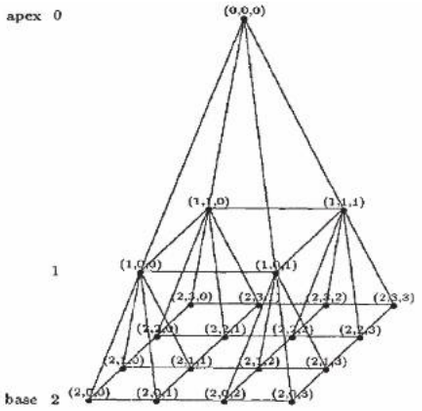
La legge di Moore è inesorabilmente vera: **la potenza di calcolo di un computer raddoppia una volta ogni due anni**, ma lo stesso Moore ha recentemente precisato che questa progressione si fermerà nei prossimi 10 anni a meno di un salto computazionale quantistico. Già sul finire degli anni '80 questo scenario fu entusiasticamente confermato dallo sviluppo di alcuni progetti di ricerca internazionali in ambito supercalcolo che coinvolsero l'Italia. In particolare, dal 1989 al 1993 prima e dopo la guerra del Golfo, l'Italia fu protagonista di un progetto di ricerca avanzato, del quale ebbi il privilegio di far parte. L'attività fu condotta a Roma e specularmente ad Orlando in California dal gruppo americano Bell Atlantic (con la controllata californiana BA Video Service) in partnership con il gruppo italiano a partecipazione pubblica STET, ora Telecom Italia, ed in particolare con la neonata società di servizi digitali STREAM SpA che anni dopo venne ceduta a Sky Italia. Il progetto in questione prevedeva la realizzazione di una piattaforma digitale di TV interattiva con flussi di dati digitali (per lo più film di prima visione e documentari) in streaming MPEG2 a 1,5 Mbps su doppino telefonico e l'installazione, presso i 300 utenti sperimentatori, di un innovativo set-top box ADSL prodotto da alcune società italiane ed in particolare da una prestigiosa azienda italiana, l'Italsiel del gruppo Italtel che purtroppo scomparve come la stessa STREAM nel rivolo delle successive privatizzazioni facendo perdere un know how aziendale inestimabile ed a vantaggio di capitali privati.

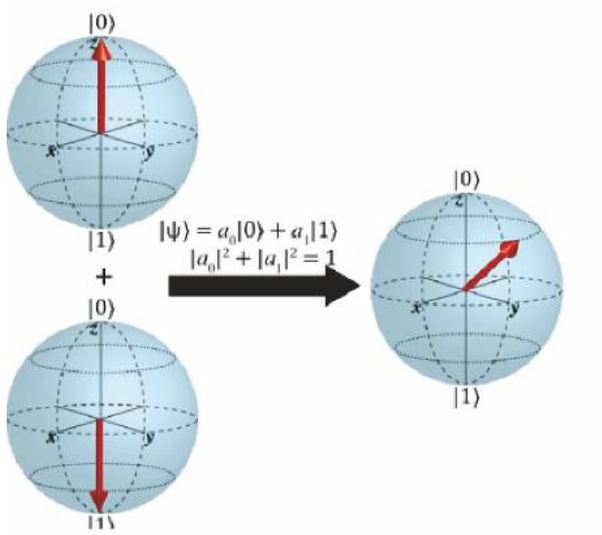


In quegli anni, STREAM, in anteprima mondiale e battendo sul tempo gli stessi partners americani erogò per prima un servizio denominato VideoMagic di Video On Demand e PayTV su doppino telefonico. Le infrastrutture tecnologiche che costarono alle casse di STET oltre 10Mld di lire, furono predisposte presso la centrale telefonica di Lanciani a Roma e prevedevano un multiplexer sviluppato a partire da una **matrice ipercubica** all'interno di un supercalcolatore NCUBE a 512 processori (vedi schema in figura a 64-nodi, ovvero 8 cubi di 8 processori per un totale di 64 processori disposti ad ipercubo) che opportunamente programmata con tecniche di processazione parallela *(array processor and parallel processing[B008])*, fungeva da ***pumping machine*** per l'invio di flussi di dati MPEG2 a 1.5 Megabit per secondo. Inoltre, con l'architettura logica dei processori NCUBE organizzati in strutture di interconnessione piramidale o a matrice ipercubica ed utilizzati come risorse di calcolo su viste vettoriali, era altresì possibile effettuare l'encoding massivo dei contenuti multimediali in standard mpeg2 (tipicamente film successivi alla prima visione), che venivano poi

BIO

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





memorizzati con tecniche innovative di *striping verticale* e *mirroring* e successivamente indicizzati in una particolare Storage Area in alta affidabilità con totale parallelizzazione dei flussi di dati pronti per essere fruiti dagli utenti. Le stesse società americane che presero parte alla sperimentazione ovvero NCUBE e Bell Atlantic cui si aggiunse successivamente IBM, sono ora tra le principali collaboratrici del Dipartimento della Difesa americano per tramite del MIT *(Massachusetts Institute of Technology)* e della Lockheed Martin sui nuovi scenari di calcolo quantistico e di algoritmi di crittografia quantistica per il settore difesa che trassero spunti non indifferenti di ricerca applicata da quelle lontane esperienze italiane a cavallo tra gli anni '80 e '90.

Il principio di Heisemberg[B006]

La fisica quantistica nasce dalla scoperta della doppia natura corpuscolare ed ondulatoria del fotone di luce. Un principio chiave alla base della fisica quantistica è il principio di indeterminazione di Heisenberg (a fianco in una foto del 1927). Questo principio sostiene che **non è possibile conoscere, simultaneamente e con precisione assoluta, alcune particolari coppie di caratteristiche di un oggetto quantistico, ad esempio la posizione e la quantità di moto**. Se si cerca di misurare esattamente la posizione di un elettrone, si perde la possibilità di verificarne la quantità di moto. Se, invece, si misura con precisione assoluta la quantità di moto, si perdono inevitabilmente informazioni sul luogo in cui l'elettrone si trova. Va inoltre sottolineato che queste sono limitazioni sempre valide anche se sussistono perturbazioni introdotte dall'apparato di misurazione. Secondo la meccanica quantistica questa soglia di indeterminazione non è concettualmente eliminabile.

Il computer quantistico[B003]

La computazione classica si basa sul modello della Macchina di Turing con il concetto classico di bit che può assumere i valori 0 o 1. Definito nel 1936 dal matematico inglese Alan Turing e successivamente rielaborato da Von Neumann negli anni '40, il modello di Macchina di Turing è alla base degli attuali sistemi di calcolo elettronico. Successivamente il fisico Feynman dimostrò che nessuna Macchina di Turing classica poteva simulare certi fenomeni fisici senza incorrere in un rallentamento esponenziale delle sue prestazioni. Al contrario, un **"simulatore quantistico universale"** avrebbe invece potuto effettuare i calcoli in maniera più efficiente. Nel 1985 Deutsch formalizzò queste idee nella sua **Macchina di Turing Quantistica Universale**. L'introduzione del nuovo modello di calcolo provocò degli effetti nel campo della complessità computazionale ed in particolare per i possibili scenari di rottura di chiavi di criptazione. Difatti nel 1994 il ricercatore Shor ebbe a dimostrare che il problema della fattorizzazione dei numeri primi si può ricondurre a tempistiche polinomiali per mezzo di un algoritmo quantistico. In un computer quantistico l'unità fondamentale di informazione è il quantum bit o qubit[B007]. Per spiegare questo concetto dobbiamo fare uso di una notazione matematica, conosciuta come notazione di Dirac. Per rappresentare lo stato di un qubit si utilizza un vettore unitario in uno spazio vettoriale complesso a due dimensioni. Come è noto lo stato di un bit classico viene descritto mediante i valori 0 ed 1, per il qubit invece la rappresentazione degli stati è fornita dalla formula:

$$\alpha\begin{pmatrix}1\\0\end{pmatrix}+\beta\begin{pmatrix}0\\1\end{pmatrix}\equiv\begin{pmatrix}\alpha\\\beta\end{pmatrix}.$$

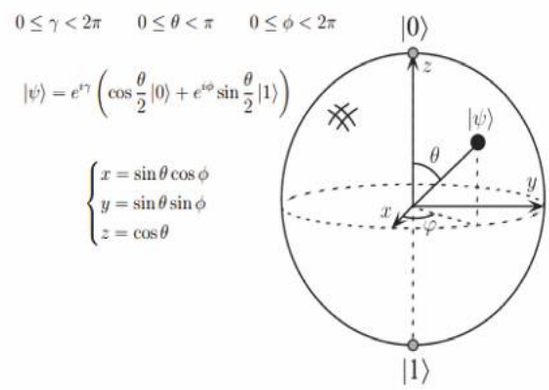
Tali stati sono spesso chiamati *sovrapposizioni* (superpositions).

È possibile inoltre utilizzare la rappresentazione detta BRA KET della stessa formula ovvero:

$$|?\rangle=\alpha|0\rangle+\beta|1\rangle$$

dove α e β sono numeri complessi tali che $|\alpha|^2+|\beta|^2 = 1$. Da ciò deduciamo che gli stati quantistici dipendono da valori di probabilità di α e β che si muovono de facto in una sfera geometrica, aprendo scenari interessanti per la risoluzione di problemi di crittografia ellittica come proposti da Neal Koblitz e Victor Miller e che possono essere descritti da equazioni in coordinate polari. Lo stato |⊠> dell'equazione precedente può infatti essere

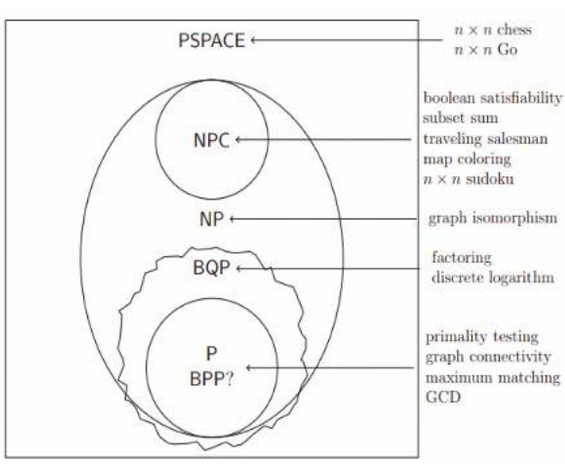
riformulato secondo la normalizzazione di Bloch con tre parametri indipendenti dei quali $e^{i\gamma}$ e $e^{i\emptyset}$ sono valori trascurabili mentre i parametri $\emptyset$ *e* θ sono associati a punti di una sfera secondo le regole riportate in figura.



Un'importante caratteristica distintiva tra qubit e bit classici è che due o più qubit possono manifestare un *entanglement* quantistico. L'*entanglement* quantistico è una proprietà non locale di due o più qubit che consente ad un insieme di qubit di esprimere una correlazione maggiore di quella possibile nei sistemi classici. Una sorta di interconnessione superposizionale che lega un qubit ad uno o più qubit e che consente ad esempio di ottenere informazioni di un qubit agendo sul qubit correlato. Ciò viene mutuato in fisica quantistica dai movimenti di spin di due elettroni collegati. Circuiti quantistici che collegano i qubit, registri quantistici e porte logiche controllate ad esempio CNOT completano il modello di un computer quantistico.

Complessità computazionale

Nella computazione classica abbiamo principalmente due classi di complessità temporale: la classe P (Polinomial) e quella NP (Non Polinomial o NPC Non Polinomial Completed ovvero un problema NP di difficile risoluzione, per esempio, quello del commesso viaggiatore). Nella prima si hanno tutti i problemi che si possono risolvere efficientemente, cioè mediante un algoritmo deterministico in tempo polinomiale, mentre la seconda comprende tutti quei problemi risolvibili da una macchina di Turing non-deterministica in tempo polinomiale. Un'altra importante classe di complessità è denotata con il nome PSPACE, dove si introduce la componente spaziale, ad esempio una scacchiera organizzata a matrice n x n dove muoversi all'interno. I risultati finora ottenuti in complessità computazionale stabiliscono la seguente relazione gerarchica: **P <= NP <= PSPACE**. Con l'introduzione degli algoritmi probabilistici è stata introdotta una nuova classe chiamata BPP (Bounded Polynomial Probabilistic). Questa classe comprende tutti quei problemi che si possono risolvere in tempi polinomiali (citiamo ad esempio il GCD *Greatest Common Divisor*) e con una probabilità di errore molto bassa. La teoria della complessità computazionale quantistica fa dunque riferimento al Modello della Macchina di Turing Quantistica. In questo contesto si è proceduto a definire la classe BQP che comprende tutti i problemi che si possono risolvere con una probabilità di errore piccola usando un circuito quantistico polinomiale. Il risultato ottenuto è il seguente: **BPP<= BQP <= PSPACE**



Crittografia quantistica

La crittografia quantistica offre qualcosa che non è possibile realizzare nel dominio classico. Permette di distribuire (o più precisamente, di generare casualmente) una chiave segreta su un canale di comunicazione aperto. Le leggi della fisica come le conosciamo oggi garantiscono che qualsiasi tentativo di intercettazione su questo canale aperto introdurrà errori nel chiave, e quindi l'intercettazione viene sicuramente rivelata. La crittografia quantistica non può trasmettere in modo sicuro un'informazione predeterminata; può generare in modo sicuro solo una chiave casuale. Una volta generata, questa chiave casuale può essere successivamente utilizzata in un cifrario simmetrico, come l'one-time pad o uno dei moderni cifrari simmetrici, per trasmettere dati in modo sicuro su un canale di comunicazione classico. Un canale di crittografia quantistica in esecuzione genererà costantemente nuovo materiale chiave segreto. Pertanto, la crittografia quantistica sta risolvendo il problema più difficile dei moderni crittografia, quella della distribuzione delle chiavi. La crittografia quantistica utilizza stati quantistici, come le polarizzazioni di singoli fotoni, trasmettere bit di informazione. Non è possibile fare una copia perfetta di uno sconosciuto stato quantistico [10], che preclude la sua misurazione precisa da parte di un intercettatore. Forse il lettore ricorderebbe il principio di indeterminazione di Heisenberg: se si misura la posizione precisa di una particella, tutte le informazioni sulla sua quantità di moto vengono perse e viceversa. Esistono molte coppie di proprietà che non possono essere misurate con precisione simultaneamente: per esempio, gli stati orizzontale-verticale e diagonale di polarizzazione dei fotoni sono una di queste coppie[B009].

Un protocollo che permette lo scambio di una chiave tra due utenti e garantisce che questa non possa essere intercettata da terzi senza che i due se ne accorgano è chiamato BB84, dal nome dei suoi ideatori, Bennet e Brassard. Immaginiamo che Alice e Bob dispongano di un canale quantistico e di uno classico (quindi

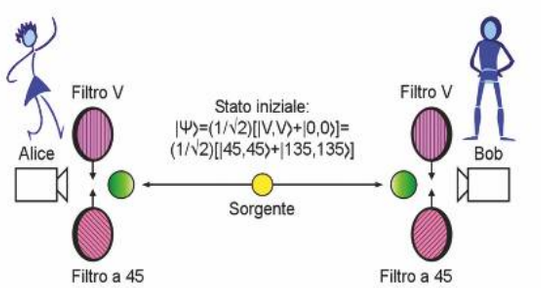
Base	0	1
+	↕	↔
×	↗	↘

passibile di intercettazione) su cui scambiare dati. Sul canale quantistico Alice invierà fotoni con una determinata polarizzazione scelta a caso tra quattro possibili, ad esempio: **0°**, **45°**, **90°**, **135°**. Queste orientazioni determinano rispettivamente le basi: **+** e **x** non ortogonali tra di loro. Per ogni base, un'orientazione è interpretata come **0** e l'altra come **1**. [B010]

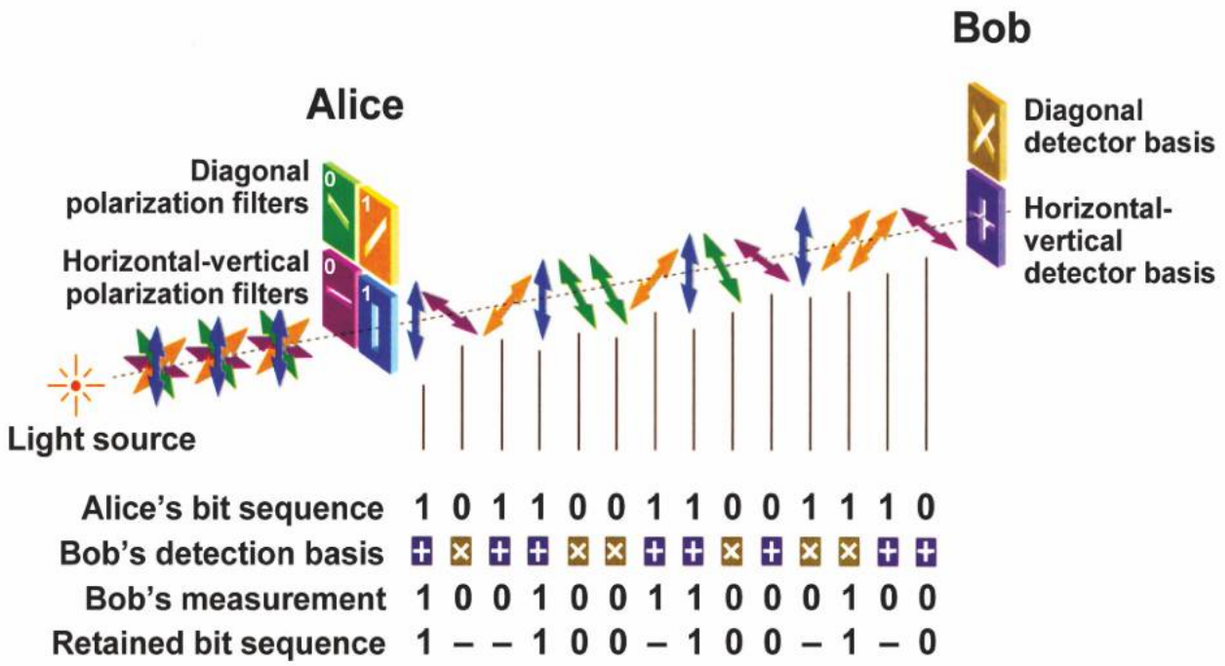
Bob, ricevuti i fotoni dovrà effettuare una misura su di essi per scoprire con che polarizzazione sono stati spediti. Sarà quindi costretto a scegliere fra due diverse misure che, per il principio di indeterminazione di Heisenberg, non sono compatibili: con la prima può scoprire la polarizzazione dei fotoni se questi sono nella base **+**, con l'altra misura può scoprire la polarizzazione se i fotoni sono nella base **x**, in nessun caso è possibile ottenere queste due misure contemporaneamente. Se Bob sceglierà la misura sbagliata rispetto alla base usata da Alice, il risultato della misura sarà casuale, ovvero 0 oppure 1 con probabilità del 50%. Quindi anche un eventuale attaccante si troverebbe nella stessa situazione di Bob: infatti quando la spia intercetta i fotoni dovrà anch'essa scegliere tra le due misure possibili e se sceglie quella sbagliata ottiene un risultato casuale. Inviata una quantità sufficiente di fotoni, Bob invierà ad Alice pubblicamente le basi che ha utilizzato per le misurazioni, ma non cosa ha misurato ed Alice renderà note le basi che ha utilizzato per polarizzare i fotoni, ma non la polarizzazione degli stessi. I due potranno così scartare tutti i fotoni per i quali Bob ha scelto la base sbagliata. A questo punto Alice e Bob possederanno una chiave segreta comune ad entrambi valida per cifrare il messaggio. Per essere sicuri che la spia non abbia intercettato la chiave basta notare che se questa avesse in qualche modo intercettato i fotoni nel loro tragitto tra Alice e Bob, per il principio d'indeterminazione, ne avrà necessariamente modificato le caratteristiche introducendo quindi degli errori nella misura di Bob anche nei bit che dovrebbero risultare corretti. Quindi, se dopo aver scartato i bit, la chiave di Bob risulta diversa da quella di Alice, vuol dire che la spia ha intercettato i fotoni e che la chiave non è sicura.

Un secondo protocollo proposto da Artur Ekert nel 1991[B011], creato per consentire lo scambio di una chiave crittografica in modo sicuro tra due utenti, si basa sul principio fisico dell'entanglement quantistico. Questo algoritmo utilizza coppie di fotoni appunto entangled, cioè fotoni con particolari caratteristiche di correlazione. Supponiamo di avere una sorgente che emette con regolarità, ad esempio ogni secondo, una coppia di fotoni entangled che si propaghino in versi opposti, uno verso il mittente (Alice) e l'altro verso il destinatario (Bob). Supponiamo inoltre che lo stato della coppia dei fotoni sia dato dall'equazione seguente:

$$|\psi\rangle = \frac{1}{\sqrt{2}}[|1,V\rangle\,|2,V\rangle + |1,O\rangle\,|2,O\rangle] = \frac{1}{\sqrt{2}}[|1,45\rangle\,|2,45\rangle + |1,135\rangle\,|2,135\rangle]$$



Un sistema così preparato permette di ottenere dei fotoni nello stesso stato di spin cioè, se il primo ha una certa orientazione di spin anche il secondo dovrà avere necessariamente la stessa orientazione. Alice e Bob si dovranno essere precedentemente accordati di eseguire misure di polarizzazione lungo le due direzioni prescelte (appunto 0° e 45°), ma non sulla successione delle misure da eseguire. Ciascuno dei due sceglierà quindi in maniera perfettamente casuale la direzione lungo cui



eseguire ciascuna misura individuale. Si può notare che la scelta delle due direzioni lungo cui verranno eseguite le misure può essere resa pubblica.

Tipologie di computer quantistici e simulatori

Nel prossimo futuro il computer quantistico sarà molto utilizzato per alcune casistiche risolutive dove la componente Non Polinomiale (NP) dello spazio delle soluzioni e quindi la natura probabilistica risulta una predominante. Citiamo alcuni di questi scenari: reti neurali ed intelligenza artificiale, chimica e biochimica, scenari di controllo dei domini della conflittualità (aria, acqua, terra, spazio e dominio cibernetico), settori finanziari e di trading, algoritmi predittivi, alte energie ed energie rinnovabili, biotecnologie e virologia, tecnologie dei materiali e nano tecnologie, simulazioni e test previsionali, cybersecurity, crittografia ed analisi malware.

Un computer quantistico è costituito da tre parti fondamentali:

1. lo spazio di alloggiamento dei qubit
2. un metodo per il trasferimento dei segnali ai qubit
3. un computer per l'esecuzione di programmi tradizionali.

Le tecnologie usate per i qubit sono molto sensibile alle sollecitazioni ambientali. I segnali possono essere inviati ai qubit usando diversi metodi, tra cui microonde, laser e tensione elettrica. Il computer quantistico deve inoltre affrontare numerose problematiche, in primis la correzione degli errori, nonchè la scalabilità dei qubit con il relativo aumento della frequenza degli errori. A causa di queste limitazioni, la disponibilità di un PC quantistico per il mercato desktop è una ipotesi ancora lontana, tuttavia un computer quantistico per attività di laboratorio e di ricerca sarà una possibilità concreta[B005] dei prossimi anni. L'alloggiamento dei qubits verrà mantenuto ad una temperatura prossima allo zero assoluto attraverso raffreddamento ad elio o con altre soluzioni per massimizzarne lo stato di coerenza. Altri tipi di alloggiamento dei qubit usano una camera sottovuoto per ridurre le vibrazioni e stabilizzarli.

Nella foto il supercomputer quantistico Q di IBM.

Recentemente IBM ha mostrato un qubit superconduttore tridimensionale, sviluppato in collaborazione con Yale University. IBM ha usato un qubit di tipo 3D (Q1,Q2,Q3) per estendere fino a 100 microsecondi il periodo in cui il qubit mantiene i suoi stati quantistici coerenti. Questo valore supera la soglia minima necessaria per permettere schemi di correzione d'errore e permette agli scienziati di iniziare a focalizzarsi su aspetti ingegneristici di più ampia portata anche d tipo commerciale. Secondo analisti ed esperti del settore, soprattutto per applicazioni in campo militare, il miglior compromesso sarà la mappatura tra architetture di processori ipercubici con circuiti qubit quantistici a superconduttore e con risoluzione in tempistiche polinomiali di problemi NP riconducibili a scenari di mappatura ipercubica [B002]. Saremo quindi difronte ad una nuova generazione di **computer ibridi** che supereranno i limiti attuali imposti dalla legge di More con le sue limitazioni verso un nuovo orizzonte degli eventi più consono alle esigenze di coniugare i fenomeni naturali con la tecnologia e consentire all'uomo di raggiungere traguardi evolutivi di portata epocale.

Bibliografia Utile

[B001]https://www.semanticscholar.org/paper/Dilation-d-embedding-of-a-hyper-pyramid-into-a-Ho-Johnsson/ffe06b272ec19fb5eb976b5ee516c099a8965e36

[B002] https://innovationorigins.com/en/multidimensional-hypercube-quantum-physicists-discover-new-atomic-state/

[B003] Emma Strubel, Quantum Tutorial, Spring 2011

[B004] https://aimath.org/workshops/upcoming/hypercubequantum/

[B006] Principio di indeterminazione di Heisenberg - YouTube

[B007] How Does a Quantum Computer Work? - YouTube

[B008] Dan I. Moldovan Parallel Processing. From Application to Systems, Morgan Kaufmann, California 1993.

[B009] Vadim Makarov, Quantum cryptography and quantum cryptanalysi, Trondheim, March 2007

[B010] Wikipedia crittografia quantistica

[B011] https://youtu.be/LaLzshlosDk ■

DORA e l'evoluzione della normativa nell'ambito della continuità operativa

Autore : Giancarlo Butti

In un precedente articolo avevamo analizzato le normative in ambito cyber che regolamentano il mondo finanziario.

In questo articolo effettuiamo lo stesso percorso riferendoci alle normative in ambito business continuity e alla loro evoluzione verso quella che viene definita resilienza operativa.

L' occasione di affrontare questo argomento ci viene data dalla predisposizione, la cui pubblicazione si ritiene imminente, del Regolamento in materia di Resilienza operativa dell'UE: REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014. Si tratta del cosiddetto **DORA** (Digital Resilience Operation Act) che riprende il concetto di resilienza operativa già citato in precedenza in un documento emesso **dal Basel Committee on Banking Supervision: Principles for Operational Resilience**, pubblicato nella sua versione definitiva nel marzo 2021.

Tuttavia solo le ultime normative parlano di continuità operativa o che comunque comprendono tale argomento.

Pur limitandoci a considerare alcuni delle principali autorità che hanno emanato normativa sull'argomento l'elenco è lungo e ha origini lontane.

Cominciamo proprio con il **Basel Committee on Banking Supervision** che cita tale materia nelle seguenti pubblicazioni (in ordine cronologico):

- *Prassi corrette per la gestione e il controllo del rischio operativo - Febbraio 2003*
- *High -level principles for business continuity - August 2006*
- *Principles for effective risk data aggregation and risk reporting - January 2013*
- *Progress in adopting the Principles for effective risk data aggregation and risk reporting - March 2017*
- *Cyber-resilience: Range of practices - December 2018*

L'**European Banking Authority**, negli ultimi anni ha citato il tema della continuità operativa in diversi documenti, fra i quali:

- *EBA/GL/2017/05 - Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP)*
- *EBA/GL/2017/11 - Orientamenti sulla governance interna*
- *EBA/GL/2017/17 - Orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2)*
- *EBA/GL/2019/02 - Orientamenti in materia di esternalizzazione*
- *EBA/GL/2019/04 - Guidelines on ICT and security risk management*

La pubblicazione, Guidance on cyber resilience for financial market infrastructures, è stata invece rilasciata nel Giugno del 2016 da **Committee on Payments and Market Infrastructures - Board of the International Organization of Securities Commissions.**

Anche il **parlamento europeo** tratta l'argomento in alcune normative.

Ad esempio, nella così detta PSD2 del novembre 2015: *Direttiva 2015/2366* e anche indirettamente nella *Direttiva 2016/1148,* la così detta NIS.

Per quanto riguarda specificatamente l'Italia, la **Banca d'Italia** in particolare aveva emanato nel luglio del 2004 una specifica Circolare avente come oggetto: Continuità operativa in casi di emergenza.

A tale prima circolare ne seguirono altre fino ad una prima raccolta organizzata nella Circolare 263 che poi è diventata la Circolare 285.Non è possibile in questa sede effettuare un'analisi completa delle singole normative, ma è interessante notare come ciascuna di essa introduca qualche elemento di novità che ha reso sempre più articolato il quadro di riferimento a cui si devono adeguare le istituzioni finanziarie.

Ad esempio, la *Circolare 285* richiede in forma generica che siano resi disponibili piani settoriali per la risoluzione di varie situazioni e che sia garantita la continuità del sistema informativo, indipendentemente da quale che sia la causa dell'interruzione.

È evidente che il solo piano di DR non è in grado di fronteggiare tutte le situazioni di discontinuità, in quanto pensato solitamente per permettere la ripartenza del CED in un'altra località in caso di distruzione totale o parziale del CED primario.

Un attacco informatico, un ramsomware e molte altre tipologie di eventi non trovano soluzione nel piano di DR, ma devono disporre di specifiche soluzioni.

A questo proposito è assolutamente esplicito quanto normato in *Guidance on cyber resilience for financial market infrastructures - June 2016*, emesso da **Committee on Payments and Market Infrastructures - Board of the International Organization of Securities Commissions** che recita:

"c. Third, certain cyber attacks can render some risk management and business continuity arrangements ineffective. For example, automated system and data replication arrangements that are designed to help preserve sensitive data and software in the event of a physical disruptive event might in some instances fuel the propagation of malware and corrupted data to backup systems".

EUROPEAN CENTRAL BANK

Mentre la **BCE** si spinge oltre e nel suo *Cyber resilience oversight expectations for financial market infrastructures - December 2018* dichiara:

"…automated system and data replication arrangements that are designed to help preserve sensitive data and software in the event of a physical disruptive event might, in some instances, fuel the propagation of malware and corrupted data to backup systems".

Evidenziando come in questo caso una soluzione pensata per garantire la continuità se non correttamente gestita può rilevarsi non solo inutile, ma anche dannosa e come quindi la predisposizione di soluzioni debba essere soggetta a continue revisioni in funzione del mutare degli eventi.

Altre normative sono più o meno dello stesso tenore, enfatizzando come gli attacchi cyber siano un possibile evento di minaccia per la continuità operativa.

Ad esempio, negli *Orientamenti sulla valutazione dei rischi relativi alle tecnologie dell'informazione e della comunicazione (Information and Communication Technology - ICT) a norma del processo di revisione e valutazione prudenziale (SREP),* **EBA** richiede espressamente che siano disponibili:

"viii. soluzioni per proteggere attività o servizi Internet critici (ad es. servizi di e-banking), ove necessario e appropriato, da attacchi "denial of service" e da altri attacchi informatici provenienti da Internet mirati a impedire o disturbare l'accesso a tali attività e servizi".

Mentre il **Basel Committee on Banking Supervision** nel *Cyber-resilience: Range of practices recita:*

"…To safeguard the availability and continuity of critical business activities in case of exceptional events or crises (eg cyber-attacks), regulators typically request that financial institutions analyse these activities, to design and implement appropriate plans, procedures and technical solutions, and to adequately test mitigating measures".

Un altro aspetto evolutivo è il maggior peso che nelle normative viene dato al controllo dell'operato delle terze parti coinvolte nei processi aziendali, e sulle quali le istituzioni finanziarie non hanno un pieno controllo.

Al di là delle attività di analisi precontrattuale per verificare la reale capacità di tali soggetti di essere in grado di operare anche in caso di incidenti di varia natura, **EBA** nel suo documento *EBA Guidelines on ICT and security risk management* si spinge oltre ed arriva a dichiarare:

"1.7.3. Piani di risposta e di ripristino

86. Inoltre, nell'ambito dei piani di risposta e di ripristino, gli istituti finanziari dovrebbero considerare e attuare misure di continuità per mitigare gli effetti delle inadempienze dei fornitori terzi, che sono di fondamentale importanza per la continuità dei servizi ICT di un istituto finanziario (in linea con le disposizioni degli orientamenti dell'ABE in materia di esternalizzazione (EBA/GL/2019/02)".

Come ultimo esempio dello sviluppo subito dalla normativa, prendiamo in considerazione la modalità con cui valorizzare i parametri di valutazione di una BIA (Business Impact Analysis) e cioè la valutazione dell'evoluzione nel tempo del fermo di un processo/servizio. Tale valutazione non è da confondere con l'analisi dei rischi per due motivi. Il primo è che tale valutazione si limita a considerare gli impatti e non la probabilità di un evento, in quanto considera l'evento come accaduto e quindi certo. La seconda è che non esprime un unico valore, ma l'evoluzione della perdita attesa in funzione del trascorre del tempo dal momento della interruzione del processo/servizio analizzato.

Di norma tali valutazioni, si fanno esprimendo un valore qualitativo (alto, medio, basso…), abbinato a volte ad un range di valori che identificano delle perdite operative, reputazionali, rischi legali…

Tale tipo di metrica non è più in linea con le più recenti aspettative degli enti che regolano il settore, che iniziano a richiedere valutazioni di tipo quantitativo.

Ne sono un esempio alcuni documenti in particolare di **EBA**, che nel suo documento *Orientamenti sulla governance interna* così recita:

*"211. Al fine di stabilire un piano efficace di gestione della continuità operativa, un ente dovrebbe analizzare attentamente la propria esposizione a gravi interruzioni delle attività e valutare (dal punto di vista **quantitativo e qualitativo)** le possibili ripercussioni di tali eventi, ricorrendo a un'analisi dei dati e degli scenari interni e/o esterni".*

Mentre nelle *Guidelines on ICT and security risk management* recita:

*"78. Nell'ambito di una solida gestione della continuità operativa, gli istituti finanziari dovrebbero condurre un'analisi di impatto aziendale (Business Impact Analysis-BIA) esaminando la propria esposizione a diverse interruzioni dell'operatività e valutando i loro potenziali impatti (anche in termini di riservatezza, integrità e disponibilità), con un approccio sia **quantitativo che qualitativo**, utilizzando dati interni e/o esterni (ad esempio, dati di fornitori terzi rilevanti per un processo aziendale o dati di pubblico dominio che possono essere utili per l'analisi di impatto sull'operatività), e condurre inoltre un'analisi di scenario".*

Ed infine negli *Orientamenti sulle misure di sicurezza per i rischi operativi e di sicurezza dei servizi di pagamento ai sensi della direttiva (UE) 2015/2366 (PSD2)* recita:

6.2 Al fine di impiantare una solida gestione della continuità operativa, i prestatori di servizi di pagamento dovrebbero attentamente analizzare la propria esposizione a gravi interruzioni dell'operatività e valutare, dal punto di vista quantitativo e qualitativo, le possibili ripercussioni di tali eventi, ricorrendo ad analisi interne e/o esterne dei dati e degli scenari.

Torniamo ora alle due normative che introducono il concetto di Resilienza operativa.

Il Comitato di Basilea ha redatto i **Principles for Operational Resilience,** come conseguenza principalmente della pandemia, alla quale attribuisce una serie di effetti impattanti sulla capacità di operare delle banche:

"Pandemic-related disruptions have affected information systems, personnel, facilities and relationships with third-party service providers and customers. In addition, cyber threats (ransomware attacks, phishing, etc) have spiked, and the potential for operational risk events caused by people, failed processes and systems has increased as a result of greater reliance on virtual working arrangements".

La normativa introduce il concetto di resilienza operative che viene definita come *"the ability of a bank to deliver critical operations through disruption".*

Le banche devono essere in grado *"to absorb operational risk-related events, such as pandemics, cyber incidents, technology failures and natural disasters, which could cause significant operational failures or wide-scale disruptions in financial markets."*

In particolare, la normativa riconosce che esistono una serie rischi per cui è impossibile una prevenzione e quindi è necessario essere preparati per affrontarli.

"Recognising that a range of potential hazards cannot be prevented, the Committee believes that a pragmatic, flexible approach to operational resilience can enhance the ability of banks to withstand, adapt to and recover from potential hazards and thereby mitigate potentially severe adverse impacts.

Operational resilience is an outcome that benefits from the effective management of operational risk.3 Activities such as risk identification and assessment, risk mitigation (including the implementation of controls) and the

BIO

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

monitoring of risks and control effectiveness work together to minimise operational disruptions and their effects. In addition, management's focus on the bank's ability to respond to and recover from disruptions, assuming failures will occur, will support operational resilience. An operationally resilient bank is less prone to incur untimely lapses in its operations and losses from disruptions, thus lessening incident impact on critical operations and related services, functions and systems. While it may not be possible to avoid certain operational risks, such as a pandemic, it is possible to improve the resilience of a bank's operations to such events".

Per ottenere questo risultato il Comitato individua una serie di 7 principi che riportiamo nella loro sintesi:

Governance

Principle 1: Banks should utilise their existing governance structure11 to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimise their impact on delivering critical operations through disruption.

Operational risk management

Principle 2: Banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience approach.

Business continuity planning and testing

Principle 3: Banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.

Mapping interconnections and interdependencies

Principle 4: Once a bank has identified its critical operations, the bank should map the internal and external interconnections and interdependencies that are necessary for the delivery of critical operations consistent with its approach to operational resilience.

Third-party dependency management

Principle 5: Banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intragroup entities, for the delivery of critical operations.

Incident management

Principle 6: Banks should develop and implement response and recovery plans to manage incidents18 that could disrupt the delivery of critical operations in line with the bank's risk appetite and tolerance for disruption. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.

ICT including cyber security

Principle 7: Banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the bank's critical operations.

L'approccio del **Regolamento UE** sulla resilienza ha un approccio in parte sovrapponibile.

Anche in questo caso la prima parte è dedicata alla governance; l'organo di gestione sarà tenuto a mantenere un ruolo attivo e cruciale nel dirigere il quadro di gestione dei rischi relativi alle TIC[1] e dovrà garantire il rispetto di una scrupolosa igiene informatica.

Il Regolamento prosegue con prescrizioni relative ai rischi che riguardano le TIC, prevedendo la predisposizione di un ciclo per la loro gestione (identificazione, protezione e prevenzione, individuazione, risposta e ripristino, apprendimento, evoluzione e comunicazione).

È prescritto di istituire e mantenere strumenti e sistemi di TIC resilienti, tali da ridurre al minimo l›impatto dei rischi relativi alle TIC, identificare costantemente tutte le fonti di rischi relativi alle TIC, introdurre misure di protezione e prevenzione, individuare tempestivamente le attività anomale, mettere in atto strategie di continuità operativa e piani di ripristino in caso di disastro come parte integrante della strategia di continuità operativa.

Le misure di sicurezza devono anche garantire l›integrità, la sicurezza e la resilienza delle infrastrutture e attrezzature fisiche che supportano l›uso della tecnologia nonché del personale e dei processi collegati alle TIC.

Vengono anche definite degli specifici test per verificare la resilienza operativa digitale e le entità identificate dalle autorità competenti come significative dovrebbero avere l›obbligo di svolgere prove avanzate mediante test di penetrazione basati su minacce.

Anche il Regolamento da grande rilievo alla gestione dei rischi derivanti da soggetti terzi, tramite stipula, esecuzione, estinzione e fase post-contrattuale.

I fornitori terzi di servizi di TIC critici saranno inoltre sottoposti a un quadro di sorveglianza da parte di autorità di sorveglianza capofila.

Da ultimo specifici articolo sono dedicata alla condivisione delle informazioni su minacce e soluzioni e segnalazione di incidenti connessi alle TIC.

Conclusione

L'evoluzione della normativa va verso una gestione integrata, proattiva e misurabile dei rischi che minacciano la continuità operativa delle istituzioni finanziarie, ma anche gli altri settori possono beneficiare dalle idee proposte, coscienti del fatto che l'ambito a cui sono destinate è uno dei più critici. ■

Le paure degli italiani e il fenomeno dei "panofobici"

In Italia i reati nell'ultimo anno sono calati del 18,9%, questa la buona notizia. L'insicurezza però resta alta, soprattutto nei corpi sociali più fragili. Risultano in aumento le richieste di aiuto al numero antiviolenza e stalking: +72%, mentre circa sei milioni di italiani hanno paura di tutto: sono i panofobici. Una voce importante del Rapporto ***Censis e Federsicurezza*** *è quella dedicata alla criminalità digitale: le "zone oscure" del web sono in espansione e il cybercrime gode di "ottima" salute.*

Nel 2020 in Italia sono stati denunciati complessivamente 1.866.857 reati. Complice la pandemia, si è registrata una riduzione del 18,9% rispetto all'anno precedente, con 435.055 crimini in meno. Gli omicidi -16,4%, le rapine -18,2%, i furti -33,0%, i furti in appartamento -34,4%. Nonostante ciò, per due terzi degli italiani (il 66,6% del totale) la paura di rimanere vittima di un reato non è diminuita e per il 28,6% è addirittura aumentata. È quanto emerge dal «2° Rapporto sulla filiera della sicurezza in Italia» di *Censis* e *Federsicurezza*. Occhio però alla "infosfera, in particolare al *cybercrime*, che è proliferato con la pandemia.

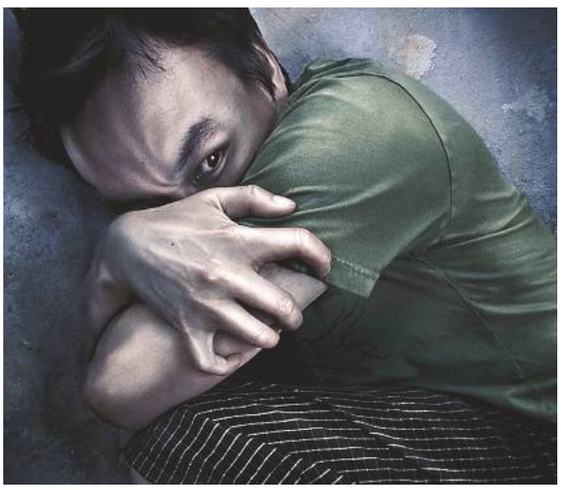
Tipologie reati	Reati					
	2020 (*)	*di cui:* mar-apr	2019-2020	*di cui:* mar-apr	var. % 2019-2020	*di cui:* mar-apr
	v.a.		*differenza assoluta*		*var. %*	
Omicidi volontari	266	40	-52	-27	-16,4	-40,3
Rapine	19.847	1.762	-4.429	-2.405	-18,2	-57,7
in pubblica via	10.995	880	-2.312	-1.309	-17,4	-59,8
in abitazione	1.557	154	-261	-153	-14,4	-49,8
Furti	717.766	52.938	-354.010	-126.280	-33,0	-70,5
in abitazione	108.525	7.139	-56.804	-17.421	-34,4	-70,9
Totale reati	**1.866.857**	**199.954**	**-435.055**	**-186.393**	**-18,9**	**-48,2**

Nel 2020 sono state commesse 241.673 truffe e frodi informatiche, il 13,9% in più rispetto all'anno precedente (nel 2010 erano state solo 96.442).

Tipo di reato	Reati 2020 v.a.	Var. % var. % 2010-2020	Var. % var. % 2019-2020
Truffe e frodi informatiche	241.673	150,6	13,9
Delitti informatici	18.888	216,2	17,0
Totale reati	**1.866.857**	**-28,8**	**-18,9**

I rischi connessi all'utilizzo della rete rischiano di rallentare i processi di innovazione e la cultura del digitale. Lo dimostra l'atteggiamento di molti utenti: un italiano su tre (il 31,3% del totale) non si sente sicuro quando fa operazioni bancarie online. Uno su quattro (il 24,9%) ha paura di utilizzare i sistemi di pagamento elettronici per fare acquisti in rete. Le percentuali salgono nettamente tra le persone più avanti con gli anni e tra quelle con bassi livelli di istruzione. Altro lascito sinistro di questo difficile periodo della storia che abbiamo vissuto e sperimentato, l'istintiva diffidenza verso gli altri. Il 75,4% degli italiani dichiara di non sentirsi sicuro quando frequenta luoghi affollati (la percentuale scende del 67% tra i più giovani). Il 59,3% ha paura di camminare per strada e di prendere i mezzi pubblici dopo le otto di sera (la percentuale resta al 59,8% anche tra i più giovani).

È evidente che siamo dentro l'orizzonte di un'inedita insicurezza generata dal timore del contagio. Il trend analizzato dai ricercatori fa vedere molto bene come sarà la sfera sanitaria a pesare sempre



sugli equilibri di vita, per ciascuno di noi. Dobbiamo sperare che cessate le restrizioni, le piazze torneranno ad assumere un profilo di normalità, e le relazioni possano rifluire, finalmente senza condizionamenti.

Donne e lockdown

Il lockdown è stato pagato a caro prezzo dalle donne. Chiuse in casa sono state maggiormente esposte alla violenza di partner e conviventi. Le richieste di aiuto al numero antiviolenza e stalking 1522 sono fortemente aumentate. Da marzo a ottobre 2020 le chiamate sono state 23.071: un anno prima, nello stesso periodo, erano state 13.424 (+71,9%). La paura innesca dei comportamenti che condizionano fortemente la qualità della vita: il 75,8% ha paura di camminare per strada e di prendere i mezzi pubblici di sera, l'83,8% ha paura di frequentare luoghi affollati, l'88,5% ha paura di incontrare persone sconosciute sui social network, il 76,3% ha paura di condividere immagini sul web, il 22,5% ha paura di stare a casa da sola di notte.

I panofobici nella società del rischio

Fronte particolare quello rappresentato dai panofobici. Secondo il Censis e Federsicurezza ci sono oltre 6 milioni di italiani che hanno paura di tutto, e che vivono in uno stato di ansia costante. Prevalgono le donne: sono quasi 5 milioni, il 17,9% della popolazione femminile complessiva. I panofobici sono presenti anche tra i giovani: se ne contano 1,7 milioni, pari al 16,3% dei giovani con meno di 35 anni.

Altro fenomeno emergente: la sicurezza privata. Negli ultimi dieci anni è enormemente cresciuta in termini di numeri, funzioni svolte, capacità tecniche e professionali. Con il Covid la categoria ha anche ampliato i propri compiti, per garantire, tra l'altro, il rispetto del distanziamento interpersonale nei luoghi rimasti aperti. Il risultato di questa "nuova incidenza" appare positivo: se infatti il 50,5% degli italiani esprime fiducia nelle guardie giurate e negli operatori della sicurezza privata, il 55,7% è addirittura convinto che il settore avrebbe bisogno di un maggiore riconoscimento sociale. Per il 62,8% del campione interpellato persiste una scarsa consapevolezza da parte della popolazione in merito al lavoro che questi professionisti della security svolgono. Cambiare atteggiamento sarebbe necessario nella società in cui l'emergenza è divenuta una costante e il rischio una componente insopprimibile delle nostre vite. ■

Lei ha/avrebbe paura di:	Genere		Totale	Differenza Donne
	Maschio	Femmina		
Camminare/prendere mezzi pubblici dopo le otto di sera	41,6	75,8	59,3	+34,2
Frequentare luoghi affollati (stadio, discoteche, ecc.)	66,4	83,8	75,4	+17,4
Incontrare di persona qualcuno conosciuto sui social/on line	60,4	88,5	75,0	+28,1
Condividere/scambiare video, immagini on line	61,9	76,3	69,4	+14,4

Non cadere dalle nuvole: tre elementi per una strategia di sicurezza cloud efficace

Autore: Stefano Lamonato

CROWDSTRIKE

In ambito aziendale, sicurezza significa molto più che semplice protezione: significa promuovere le operazioni di sviluppo, le iniziative commerciali e tutti gli aspetti connessi all'IT e all'intelligenza umana. Per realizzare questa visione, è necessario integrare tra loro gli strumenti di sicurezza e assegnare correttamente le responsabilità per evitare confusione e aiutare i team a difendere i complessi ambienti cloud da cui le aziende dipendono così pesantemente.

Molte aziende si stanno rendendo conto che l'investimento in un unico cloud non è più l'approccio giusto. Dal momento che ogni servizio cloud, pubblico o privato, propone opportunità e strumenti diversi – come funzioni avanzate basate sul machine learning o costi di archiviazione particolarmente convenienti – la gran parte delle aziende sta cercando di sfruttare la potenza della strategia multi-cloud come meglio può. Per soddisfare le esigenze dei team DevOps e di pluralità di ambienti cloud che le aziende utilizzano, è necessario adottare una piattaforma unificata e implementare impostazioni di sicurezza omogenee su tutte le risorse. Oltre ad automatizzare i controlli di sicurezza, la soluzione deve garantire la conformità di host e container indipendentemente dal cloud provider scelto. Per creare una strategia di sicurezza cloud efficace, le aziende devono definire dei protocolli di sicurezza basati su tre elementi: unificazione, automazione e integrazione.

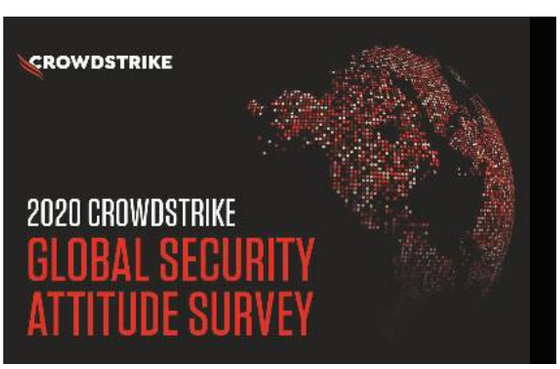
Implementare soluzioni unificate

Osservando con attenzione lo stato attuale della sicurezza, risulta evidente che gli attaccanti possono anche essere gli stessi, ma l'ambiente che ci impegniamo a difendere è molto diverso. Gli strumenti di sicurezza tradizionali non sono in grado di proteggere adeguatamente l'infrastruttura basata sul cloud. Pur se adattati e resi più moderni, non sono stati concepiti per gestire ambienti dinamici e sono del tutto inutili per contrastare i tipi di attacchi che gli ambienti cloud devono sopportare. Gli strumenti di sicurezza convenzionali introducono lacune enormi in termini di visibilità e protezione. Poiché molti responsabili della sicurezza hanno dovuto affrontare le problematiche causate da soluzioni puntuali, c'è stata una spinta verso la creazione di soluzioni *ad hoc* nel tentativo di rimediare alle carenze e alla mancanza di integrazione.

Per proteggere il cloud, serve il cloud! Una piattaforma nata per il cloud è scalabile e si adatta facilmente alle esigenze delle aziende, includendo nel suo perimetro di protezione dai container fino ai microservizi. Queste

piattaforme, grazie alla visibilità completa che assicurano e alla ricerca continua dei workload, aiutano a individuare le vulnerabilità e a risolvere i problemi del codice prima della fase di produzione consentendo, in ultima analisi, ai team DevOps di integrare la sicurezza nei processi CI/CD.

Il passaggio repentino allo smart working ha obbligato le aziende a inserire la sicurezza del cloud tra le priorità per permettere ai dipendenti di collaborare. Lo studio di CrowdStrike sulle pratiche globali di sicurezza intitolato "2020 Global Security Attitudes" ha rilevato che, in risposta al passaggio allo smart working, nel Regno Unito il 21% degli intervistati ha rinnovato i propri strumenti di sicurezza e accelerato l'adozione delle tecnologie cloud. Nonostante alcune aziende abbiano già provveduto, molte altre dovranno evolvere in questa direzione se vogliono essere sicure di essere protette e consentire ai team DevOps di continuare a innovare. È interessante notare anche quanto la pressione del lavoro da remoto abbia fatto aumentare il tempo medio che serve alle aziende per individuare la presenza di un intruso nel proprio ambiente. Nel Regno Unito, questo tempo è aumentato di più del 50% in un solo anno passando da 39 ore nel 2019 a 61 ore nel 2020.



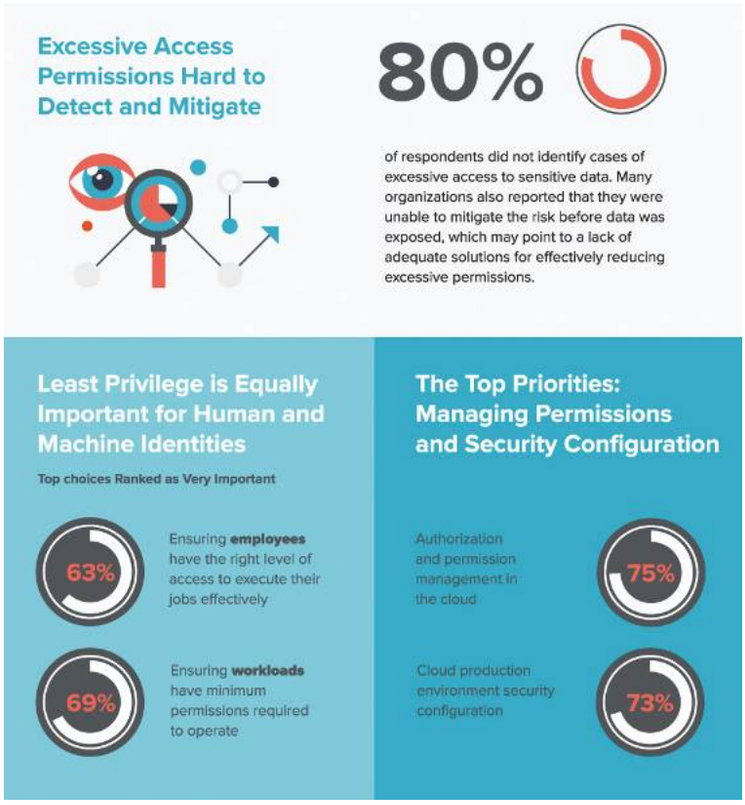
È indispensabile che le soluzioni di sicurezza riescano a funzionare alla stessa velocità dei team DevOps, e che abbiano la flessibilità di operare su qualsiasi cloud e servizio senza intralciare i workload, la protezione e la visibilità. Le soluzioni di sicurezza devono essere all'altezza del mondo multi-cloud e multi-servizio in cui viviamo.

Il segreto sta nell'automazione

I team di sviluppatori lavorano con tale velocità che tra la concezione di un'idea e la sua realizzazione possono intercorrere pochi giorni o settimane. Lo stesso vale, in particolar modo, per i microservizi creati per realizzare le applicazioni, il cui ciclo di vita può durare anche solo qualche secondo e che sono la dimostrazione perfetta di quanto siano dinamici gli ambienti cloud. Le aziende devono avere piena visibilità su quali servizi sono attivi, chi li sta utilizzando e dove. Anche solo tentare di esercitare questo tipo di controllo manualmente o con una soluzione obsoleta è fuori questione. È qui che entrano in gioco il rilevamento e il monitoraggio automatici delle risorse: questi due processi rendono tutto visibile senza incidere sulle prestazioni aziendali.

L'integrazione della sicurezza nelle pipeline CI/CD ottimizza i processi perché potenzia la qualità. Il principale vantaggio che deriva dall'automazione è la possibilità di eliminare velocemente e tempestivamente rischi e vulnerabilità già nelle prime fasi dei processi. È però altrettanto importante prevenire l'introduzione di falle della sicurezza attraverso i modelli IaC (Infrastructure-as-Code). Un'indagine di IDC dello scorso giugno a cui hanno partecipato 300 CISO ha evidenziato che gli errori di configurazione della sicurezza negli ambienti di produzione sono la principale preoccupazione per il 67% dei intervistati. In realtà, gli errori di configurazione possono essere rilevati automaticamente, limitando le probabilità che abbiano ripercussioni sui servizi in un secondo tempo.

Grazie all'automazione, la sicurezza smette di essere un ostacolo al lavoro degli sviluppatori. Inoltre, l'automazione permette di eliminare le complessità nascoste, accelera l'implementazione delle soluzioni e offre completa visibilità alle aziende mantenendole sempre protette.



Soluzioni di sicurezza integrate e scalabili

Quando si decide di rinnovare la strategia di sicurezza dell'azienda, è importante considerare che non può funzionare in un contesto isolato, soprattutto rispetto al lavoro dei team DevOps. L'integrazione permette alle pratiche di sicurezza di essere applicate senza attriti su qualsiasi applicazione, istanza cloud e workload cloud.

È l'integrazione l'elemento in grado di trasformare una strategia di sicurezza mediocre in una soluzione davvero efficace. Basta una sola occhiata per capire che gli strumenti che non sono stati progettati specificamente per il cloud non sono adatti a proteggere ambienti cloud dinamici, non sono ottimizzati per le applicazioni cloud-native e rendono complicato il monitoraggio. In più, richiedono un intervento manuale da parte dell'utente. Al contrario, le soluzioni nate per il cloud garantiscono coerenza in tutta l'infrastruttura cloud e anche oltre. La presenza di strumenti integrati permette ai responsabili della sicurezza di tirare un sospiro di sollievo: le soluzioni cloud-native mantengono sicurezza e conformità senza generare il carico di lavoro delle soluzioni on-premise che finora erano la norma.

BIO

Stefano è Solution Architecture Manager, Europe Channel & MSSP; entra in CrowdStrike nel Febbraio 2017 con l'obiettivo di stabilirne la presenza tecnica nelle nazioni sud Europa e, dopo aver guidato il gruppo di prevendita nella regione, oggi è a capo del team Europeo dei Solution Architect a supporto del business dei Channel partner e degli MSSP.
Il suo viaggio nella Cyber Security Stefano lo inizia nei primi anni '90 con lo studio di diversi linguaggi di programmazione, di architetture di rete complesse e di diversi sistemi operativi, per poi spostarsi velocemente verso l'Ethical Hacking, gli Assessment di sicurezza, la Forensic e l'Incident Response. Nel corso degli ultimi 15 anni ha lavorato ogni giorno aiutando le aziende nel fortificare la loro postura di sicurezza e migliorare le loro capacità di rispondere alle minacce.
Grazie all'innovativa piattaforma ed ai servizi di CrowdStrike, Stefano è in grado di abilitare i propri clienti nell'ottenere il più importante risultato nell'odierno panorama delle minacce: lo "STOP THE BREACHES".

Comporre un pacchetto completo

Combinando insieme i tre elementi di cui abbiamo parlato è possibile implementare una strategia di sicurezza cloud-native in grado di evolvere insieme al business. Le piattaforme di sicurezza nate per il cloud garantiscono visibilità e controllo su qualsiasi ambiente pubblico, privato, ibrido e multi-cloud. L'automazione consente ai responsabili della sicurezza di abbandonare la ricerca degli errori di configurazione che i cybercriminali possono sfruttare, per dedicarsi ad attività più strategiche. La capacità di un'azienda di risolvere molti problemi più velocemente va di pari passo con il suo successo. ■

Le nuove strategie di cyber-security saranno data-driven

splunk>

Autore: Antonio Forzieri

Il 2020 è stato un anno sfidante per chiunque si occupi di Cybersecurity. Il quadro pandemico dovuto al virus Sars-Cov-2, l'attacco a Solarwind e l'introduzione di nuovi modelli di business per i player del mondo Ransomware ha creato una miscela esplosiva difficile da mitigare o da disinnescare.

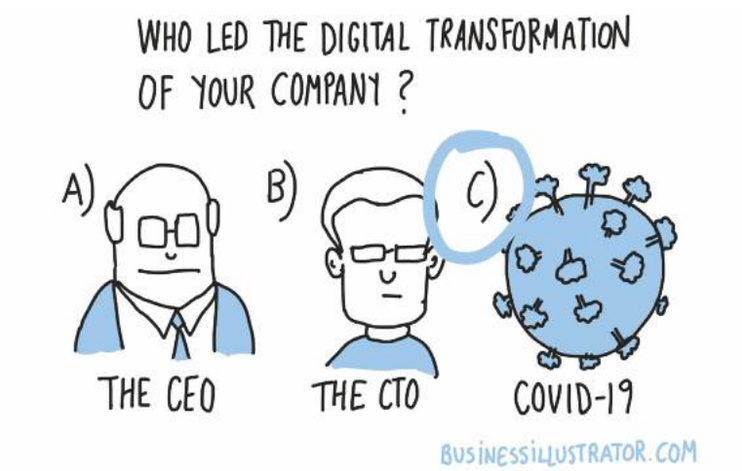
Da un giorno all'altro, la pandemia ha costretto il rapido passaggio al lavoro a distanza, con una transizione verso il Cloud tutt'altro che morbida. Alcune aziende hanno dovuto implementare progetti di trasformazione nel giro di una o due settimane (e no, non sto esagerando).

Tutti noi abbiamo sicuramente visto un MEME o una vignetta molto simile a quello che trovate di seguito, e credo che rappresenti molto bene la situazione che moltissime realtà si sono trovate a sperimentare.

Il passaggio repentino al Cloud, sia esso in forma di SaaS, PaaS o IaaS, congiuntamente al massiccio uso di soluzioni di lavoro remoto (e.g.: VPN) e all'uso di postazioni personali per scopi professionali ha ovviamente comportato un'espansione della superficie d'attacco che non si è potuta tenere sotto controllo.

Ricordo un carissimo amico, CIO di un'organizzazione medio grande dirmi "Antonio, avevo in ballo il refresh delle workstation, ho dovuto convertirlo in un ordine di laptop e token (per MFA). E il tutto ho dovuto farlo con l'ordine delle workstation praticamente in transito."

E se da un lato la superficie d'attacco è diventata improvvisamente molto più ampia, dall'altro gli attaccanti non hanno smesso di ricordarci come ci siano ancora



molti aspetti a cui guardiamo poco e che sono tremendamente fragili: Solarwind è stato l'ennesimo esempio di un attacco alla Supply Chain. Non si tratta di nulla di nuovo, sono tutte cose già viste (basti ricordare NotPetya nel Giugno 2017). Altro esempio recente è l'attacco verso CodeCove.

Come se non bastasse anche il mondo Ransomware ha visto enormi evoluzioni, il modello as a service è stato abbracciato pienamente con l'introduzione del servizio RaaS per l'appunto (Ransomware as a Service) e l'introduzione di quello che è stato battezzato come quadruple extortion model:

- Single: ransom per riprendere il controllo sui propri sistemi decifrando i dati;
- Double: ransom per evitare che i dati cifrati vengano rilasciati pubblicamente e che la notizia diventi pubblica;
- Triple: la minaccia o l'esecuzione di un DDoS, generalmente in fase di negoziazione per influenzare la vittima a pagare;
- Quadruple: mail verso i clienti dell'azienda compromessa o utilizzo di call center per contattare la vittima durante la fase di negoziazione.

Il 2020 ha visto gruppi come Avaddon, che recentemente ha chiuso i battenti dopo molti attacchi condotti con successo, o come Darkside, responsabile del recente attacco a Colonial Pipeline.

Una nuova ricerca, sponsorizzata da Splunk e pubblicata recentemente in The State of Security 2021, fornisce un primo sguardo al panorama post-SolarWinds. C'è ancora molto da fare, ma ci sono ragioni per cui provare ad essere ottimisti.

I ricercatori dell'Enterprise Strategy Group (ESG), in collaborazione con Splunk, hanno intervistato più di 500 leader della sicurezza e IT in tutto il mondo solo due mesi dopo la scoperta degli attacchi SolarWinds. I dati sembrano mostrare come le organizzazioni non hanno ancora capito il rischio di uno degli attacchi alla supply chain visti fino ad oggi. In particolare, la nostra ricerca ha rilevato che:

Solo il 47% dei CISO aveva informato la leadership o il board circa le implicazioni degli attacchi SolarWinds nei due mesi successivi alla loro divulgazione, il che implica che le tematiche di Cybersecurity della Supply Chain non sono ancora un problema all'attenzione del board, e questo nonostante siano ormai abbastanza all'ordine del giorno.

Il 78% delle aziende si aspetta un altro attacco alla Supply Chain in stile SolarWinds.

Il report sottolinea come gli attacchi alla Supply Chain non siano l'unica sfida per i CISO. La grossa spinta fornita dalla pandemia, sia all'utilizzo del cloud sia al lavoro remoto ha reso temi come la sicurezza di ambienti ibridi e multi-cloud e dell'accesso remoto ai dati centrali nella strategia di moltissime realtà.

La ricerca offre anche segnali incoraggianti, segno che il cambiamento sta già avvenendo. Da evidenziare è il rapporto tra i team di sicurezza e IT: l'83% degli intervistati ha convenuto che la collaborazione è migliorata durante la pandemia. Quasi il 90% delle organizzazioni ha anche affermato di aver incrementato il budget per la sicurezza e il 35% ha dichiarato di averlo fatto «in modo significativo».

BIO

In Splunk, Antonio Forzieri (Cyber Security Specialization and Advisory, EMEA) ricopre il ruolo di leader per l'offerta Cyber Security. In precedenza, Antonio ha lavorato per Symantec dove ha ricoperto il ruolo di leader per l'offerta Cyber Security a livello EMEA inizialmente e a livello Global successivamente supportando clienti nella realizzazione di complesse iniziative in ambito Cyber Security che vanno dalla costruzione/evoluzione di Cyber Defense Center fino all'implementazione di Programmi di Cyber Intelligence per clienti pubblici e privati. Prima dell'esperienza in Symantec Forzieri ha lavorato per altre aziende italiane con incarichi svolti in tutta EMEA dove si è occupato di diverse tematiche tra le quali Compliance, Endpoint Security, Data Loss Prevention, Encryption, Ethical Hacking, Analisi Frodi, oltre ad attività di formazione in ambito Security. Tra le attività svolte, Forzieri supporta organizzazioni pubbliche e private in caso di attacchi informatici e frodi.
Antonio Forzieri è laureato in Ingegneria delle Telecomunicazioni al Politecnico di Milano, dove è docente nel corso "Mobilità e Sicurezza delle reti".

Ecco altre metriche interessanti emerse dalla ricerca:

- Il 75% delle infrastrutture dei clienti che utilizzano cloud è in realtà già oggi multicloud.
- L'87% prevede di utilizzare più fornitori di servizi cloud tra due anni.
- Il 76% degli intervistati afferma che i lavoratori remoti sono più difficili da proteggere.
- Il 53% conferma che gli attacchi sono aumentati durante la pandemia e il 12% lo definisce un aumento significativo.

Da dove possiamo cominciare per cambiare le cose?

Un buon spunto è stato fornito da Doug Merrit, CEO di Splunk, durante la RSA Security Conference: "Data is essential to an effective cybersecurity program". I dati sono fondamentali per identificare e rispondere a qualsiasi minaccia alla sicurezza e per evolvere la propria strategia di Cybersecurity.

Viviamo nella cosiddetta Data Age, in cui la spina dorsale di qualsiasi strategia di sicurezza efficace, soprattutto dopo COVID e SolarWinds, deve incentrarsi sui dati. La strategia di Cybersecurity deve essere data-driven.

I dati non sono solo ciò che proteggiamo, sono ciò che ci consente di ottimizzare i nostri investimenti e comunicare efficacemente rischi e mitigazioni. È ciò che ci dice quando gli attori delle minacce bussano alla porta o quando sono già all'interno del nostro perimetro.

Per utilizzare i dati in modo efficace, dobbiamo iniziare abbracciando la strategia zero trust, che si basa sulla limitazione dell'accesso a dati e risorse fino a quando una connessione non si dimostra sicura. Dobbiamo valutare continuamente le minacce esistenti ed emergenti e le tecniche, le tattiche e le procedure (TTPs) sfruttate dai threat actors, in modo da poter rimediare a eventuali punti deboli. Inoltre, dobbiamo implementare un Security Operation Center moderno (SOC) costruito su una piattaforma scalabile con funzionalità di automazione complete per rilevare le minacce, identificare le anomalie e abbreviare i cicli di risposta. Il tutto utilizzando framework di riferimento quali il MITRE ATT&CK.

Infine, dobbiamo anche utilizzare i dati per migliorare le comunicazioni, la condivisione delle informazioni sulle minacce e la fiducia dei fornitori.

Prendiamo come esempio gli attacchi alla Supply Chain: i fornitori di tecnologia, come Splunk, hanno il dovere di aggiornare regolarmente i propri fornitori e spiegare loro come mitigare il rischio di minacce emergenti. Dobbiamo quindi comunicarlo ai nostri clienti, come abbiamo fatto dopo l'operazione SolarWinds. È necessaria una piattaforma solida e flessibile per controllare e condividere questi dati su larga scala con i nostri clienti e la comunità nel suo insieme.

L'anno passato ha presentato sfide per i professionisti della sicurezza, ma ha anche aperto opportunità, sbloccato budget e galvanizzato il supporto a tutti i livelli organizzativi per costruire pratiche di sicurezza più solide.

Confido che i CIO/CIO stiano sfruttando lo slancio attuale per accelerare i miglioramenti e stare al passo con l'intensificarsi delle sfide alla sicurezza.

Per ulteriori informazioni, inclusi consigli per migliorare la tua security posture, consulta The State of Security 2021.

https://www.splunk.com/en_us/blog/leadership/state-of-security-research-zeroes-in-on-data-strategies.html ■

Quando il cittadino diventa un semplice oggetto usa e getta...

Odiando lo Stato eletto, e con pesanti conseguenze, anche gli Enti di ordine pubblico

Autore: Laurent Chrzanovski

Rileggere tutti gli articoli degli ultimi numeri della nostra rivista ci lascia un sapore amaro. Ci sembra di vivere in un circolo vizioso senza fine. In sintesi, tutti i punti estremamente importanti menzionati dai massimi esperti... sono esattamente gli stessi con cui abbiamo a che fare da quindici anni.

Le minacce sono ogni giorno sempre più pericolose; mentre, paradossalmente, la sfida per aumentare la consapevolezza della sicurezza informatica e dell'igiene digitale, così come l'applicazione di nuove leggi e regole, da molto difficile ormai è diventata quasi impossibile.

Così facendo, da cittadini gli europei diventeranno molto rapidamente dei semplici e modificabili oggetti, nemmeno soggetti, di proprietà dei giganti della Big Tech. Tale condizione potrebbe essere ben rappresentata dal dialogo tra Morpheus e Neo in Matrix - una sceneggiatura scritta venti anni fa...

Morpheus: "Matrix è ovunque, è intorno a noi, anche adesso nella stanza in cui siamo. È quello che vedi quando ti affacci alla finestra o quando accendi il televisore. L'avverti quando vai al lavoro, quando vai in chiesa, quando paghi le tasse. È il mondo che ti è stato messo dinanzi agli occhi, per nasconderti la verità."

Neo: "Quale verità?"

Morpheus: "Che tu sei uno schiavo. Come tutti gli altri sei nato in catene, sei nato in una prigione che non ha sbarre, che non ha mura, che non ha odore, una prigione per la tua mente".

Gli anni della pandemia digitale stanno arrivando ora...

L'effetto principale dei blocchi e delle misure prese in tempi di pandemia è che la maggior parte delle persone sono, molto più che prima del COVID-19, completamente perse e confuse nel loro rapporto con il mondo reale, lo Stato e il mondo digitale.

Gli allarmi "bandiera rossa" provengono da tutte le discipline, tutti gli ambiti, tutti i paesi. Ma per i giganti della tecnologia, i giorni sono solo *"business as usual"*, senza limiti, senza regole, senza leggi per contenere i loro eccessi... Proprio ora, quando, grazie all'implementazione del 5G, si sta realizzando la quarta rivoluzione industriale.

Cercheremo, in questo breve testo, di presentare sinteticamente le minacce più importanti che stiamo affrontando, da un punto di vista sociale, umanistico e democratico. Per questo esercizio, prenderemo come base il rapporto annuale delle pietre miliari dell'IE Center for the Governance of Change (CGC), *"European Tech Insights 2021"*.

Pubblicato eccezionalmente in due volumi separati a causa del momento molto speciale che viviamo *(Parte I. Come la pandemia ha alterato il nostro rapporto con la tecnologia & Parte II. Embracing and Governing Technological Disruption)*. Il rapporto si concentra sul fatto che una vasta maggioranza dei cittadini europei ha ora reazioni, approcci e comprensioni bipolari in ciò che si aspetta dal mondo digitale.

La più grande minaccia per il nostro sistema democratico è che se confrontiamo i risultati su uno stesso tema, arriviamo sempre allo stesso dilemma. Da un lato, una grande maggioranza vuole leggi per tassare l'alta tecnologia, leggi per salvare i posti del lavoro umano contro l'automatizzazione e regole per un maggiore controllo sui social media e le fake news. D'altra parte, la maggior parte dei cittadini non si fida affatto delle istituzioni che avrebbero il compito di promulgare queste leggi, tasse e regole. Questo è ciò che rileva il sondaggio del rapporto sui parlamentari europei: *"più del 50% degli europei sostiene la sostituzione dei loro parlamentari con algoritmi. Le generazioni più giovani sono particolarmente favorevoli, con il 60% dei 25-34enni a favore".*

Possiamo osservare la stessa situazione sui temi più cruciali di quest'anno:

- **Sanità:** mentre *"la maggioranza degli europei sostiene la costruzione di un'Unione Europea della Salute per migliorare la cooperazione nel campo della sanità pubblica"* (65%), gli stessi intervistati *"sono completamente divisi quando si tratta di lasciare che i loro governi condividano le loro cartelle cliniche con aziende private"* (45% a favore, 47% contro). Peggio ancora *"la maggioranza dei giovani europei sotto i 25 anni è disposta a lasciare che i loro assicuratori raccolgano dati personali sulla salute e sull'esercizio fisico attraverso l'uso di wearables per la salute"* (46%).

- **La censura dei social media e la diffusione delle fake news:** *"La percezione di Google, Amazon, Facebook e Apple è peggiorata notevolmente nell'ultimo anno: solo la Germania sosteneva la loro rottura l'anno scorso. Oggi tutti i paesi europei, tranne l'Italia e la Polonia, sono favorevoli a limitare il potere dei giganti della tecnologia"* con l'aggiunta che *"gli europei sono in stragrande maggioranza contrari a che Facebook diventi un colosso della messaggistica privata"* e che c'è un *"ampio consenso tra gli europei sul fatto che i social network abbiano avuto un impatto negativo e aumentato la polarizzazione politica"* (56%). Ma per gli stessi cittadini, *"le fake news sui social network dovrebbero essere controllate dalle piattaforme e non dai governi"* (55% vs 27%).

- **Lavoro:** *"una maggioranza schiacciante di europei (61%) è disposta a pagare più tasse in cambio dell'aumento dei salari dei lavoratori essenziali"; "una vasta maggioranza di europei vuole leggi e tasse per salvare i posti di lavoro umani contro i compiti automatizzati"* e *"C'è un forte e ampio sostegno per l'introduzione di una "tassa tecnologica" con il 65% dei cittadini a favore e il 15% contro".* Ma nello stesso tempo, *"un terzo degli europei preferirebbe avere un'IA piuttosto che un funzionario pubblico che prende una decisione sui loro pagamenti di assistenza sociale o sull'approvazione del loro visto. Un quarto*

degli europei si fida anche dell'IA più degli umani quando si tratta di negoziare e concedere prestiti ipotecari".

Lo shopping online: L'incomprensione su ciò che è desiderato raggiunge il suo apice con il caso Amazon: *"la maggioranza degli europei (50%) crede che Amazon danneggi le piccole imprese e i negozi locali".* Ma *"fino al 64% degli intervistati britannici, il 48% dei tedeschi e il 47% degli italiani preferiscono comprare i loro libri attraverso la loro piattaforma invece di andare in un negozio fisico".* Inoltre, *"più di un terzo degli europei (35%) preferisce farsi consegnare un pacco da un robot piuttosto che da un umano"...*

Pericoli del mondo online: *"la stragrande maggioranza degli europei (86%) ritiene che la dipendenza digitale sia un problema"* ma *"una vasta maggioranza di europei vuole che la democrazia diventi digitale: il 72% preferirebbe votare tramite il proprio smartphone piuttosto che fisicamente, e solo il 17% è contrario" e "il 42% degli europei sostiene l'uso della tecnologia facciale nella vita quotidiana se la rende più conveniente".*

In sintesi, c'è una totale mancanza di fiducia nello Stato eletto, che viene gravemente danneggiata da una sbagliata unione di tutte le istituzioni statali incaricate dell'ordine pubblico, per non parlare del diffuso fenomeno di totale sfiducia nel cosiddetto *"Deep State"* (servizi segreti). L'incompetenza, le amministrazioni sovraccariche e la burocrazia (pubblica e privata) non sono un problema, anche il benessere viene dopo la lotta contro la corruzione - o meglio ciò che è percepito come corrotto in ogni Stato - che è secondo i cittadini il problema principale da risolvere per ripristinare la fiducia nella democrazia (opinione condivisa sia dagli europei che dagli americani)...

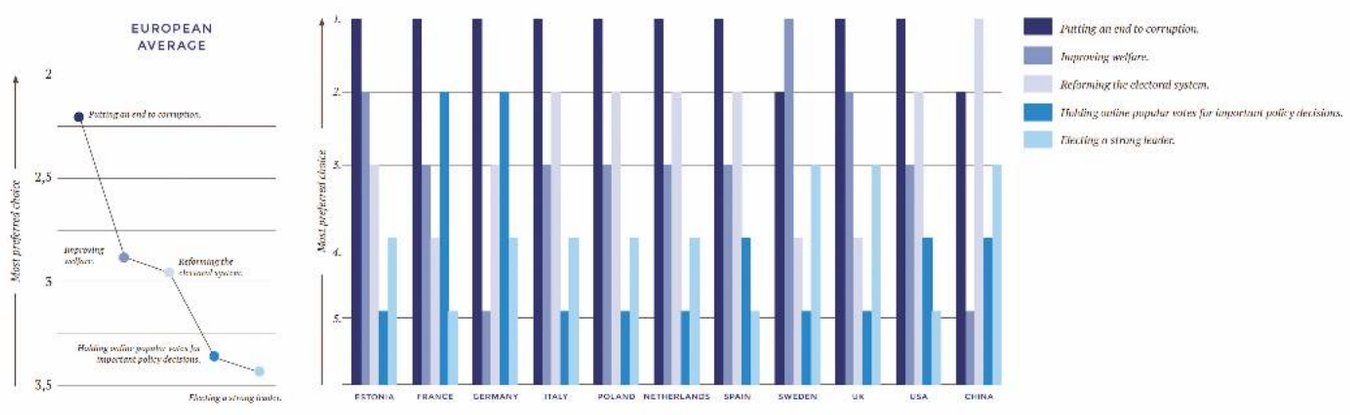
BIO

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

Autorità in allarme... senza conseguenze

Nel frattempo, le autorità accademiche e specializzate sventolano quotidianamente bandiere rosse. Abbiamo scelto tre argomenti all'interno dell'ultimo, il più importante tra l'enorme panopticon di sfide culturali e di sicurezza che dobbiamo affrontare.

Il primo problema è certamente quello del riconoscimento facciale dal vivo. I cittadini britannici sanno meglio di tutti quello che scriviamo, visto che l'argomento ha occupato i titoli di tutte le testate delle loro mainstream news. Il 18 giugno, il commissario per l'informazione del Regno Unito, Elizabeth Denham, ha

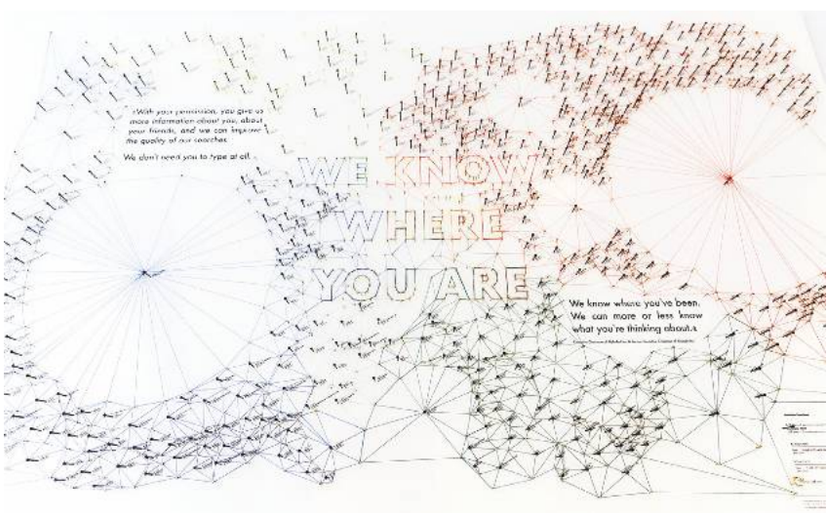


pubblicato sul suo blog istituzionale un articolo per il grande pubblico che rende accessibile e chiarissima la sua profonda preoccupazione di imporre urgenti e necessarie limitazioni per contrastare il riconoscimento facciale dal vivo (LFR) da parte delle Tech Giant[1] e, allo stesso tempo, per permettere alle forze dell'ordine di utilizzare al meglio questa tecnologia[2]. Riportiamo qui la frase più significativa del suo testo, a nostro avviso: *"Dovremmo essere in grado di portare i nostri figli in un complesso ricreativo, visitare un centro commerciale o girare una città per vedere le attrazioni senza avere i nostri dati biometrici raccolti e analizzati ad ogni passo che facciamo".*

Inutile dire che se questa frase è in linea con l'opinione pubblica che abbiamo appena analizzato, l'uso del LFR da parte delle istituzioni di polizia e, "peggio", dei servizi di intelligence è totalmente in contrasto con i risultati del sondaggio che abbiamo sopracitato. Per una questione di comodità, i cittadini preferiscono che la loro intimità personale sia in gestita dalle app piuttosto che custodita dallo Stato, il cui dovere primordiale, oltre ad assicurare sanità e educazione, è quello di proprio quello garantire la nostra sicurezza, fisica e digitale.

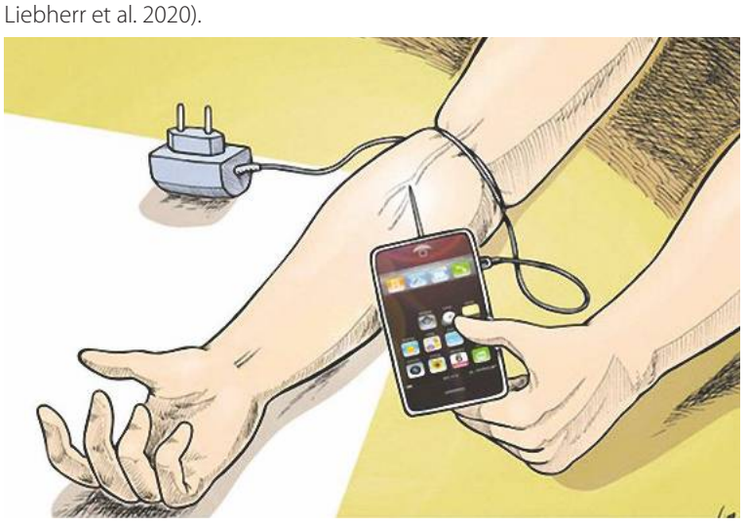
Il secondo dilemma è che non sarà più accettata alcuna sensibilizzazione all'igiene digitale o alla sicurezza informatica se tutto ciò sarà considerato come un ostacolo alle comodità di ognuno. E visto che la maggioranza delle persone vuole che lo smartphone sia usato sempre di più, per il lavoro, la vita privata, le operazioni bancarie, e ora anche... il voto, le porte dell'inferno sono ormai spalancate.

Perché non c'è niente di meno sicuro di uno smartphone. Peggio ancora, nella riedizione migliorata del suo fondamentale *"The Shallows: What the Internet Is Doing to Our Brains"*, Nicholas Carr segnala un fenomeno studiato a fondo da molti scienziati in occasione dei traumatismi post-localizzazione: l'abuso di smartphone, oltre a infettare facilmente il cloud con tutti i virus possibili, sta riducendo drasticamente la membrana esterna del nostro cervello, la parte sensibile la cui regola



The Alphabet City, opera d'arte di Tactical Tech e La Loma, realizzata con open data estratti dalle GAFAM.

è proprio quella di permettere alle informazioni di entrare nella nostra memoria. Prima - bambini, ma anche adulti - iniziano gli eccessi di utilizzo dello smartphone, e peggiore sarà, mese dopo mese, la loro capacità di memoria, dato che questa membrana si rigenera molto lentamente e smette di rigenerarsi una volta compiuti 50 anni (vedi Tanil, Yong 2020 & Liebherr et al. 2020).



L'ultimo allarme, non meno importante, è che l'equazione UMANO + SMARTPHONE non è solo l'ultimo anello debole della sicurezza, ma è anche la via diretta verso la morte della sofisticazione delle nostre lingue.

Le continue riforme per adottare in ogni lingua europea espressioni «e-slang» sono la risposta sbagliata al completo impoverimento della capacità linguistica degli studenti, che possiamo osservare nelle università in cui insegniamo, in tutto il continente. Con non più di 200 parole necessarie per leggere un tabloid o una notizia mobile dei MSM, inutile dire che i tesori dell'umanità costituiti dalla grammatica e dalla semantica propria ad ogni lingua o dialetto saranno fra poco studiati come il greco antico o il latino.

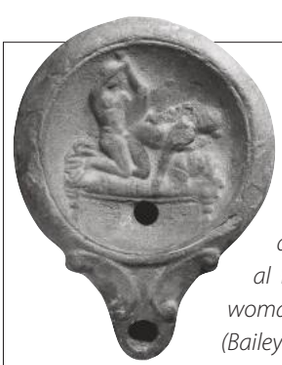
L'inglese (per meglio dire, il Globish) può permetterselo mantenendo la sua versione accademica per gli accademici, dato che questa particolare lingua non ha una ente unico che ne definisce i vocaboli e la grammatica, come accade per la maggioranza delle lingue neolatine, tra le quali citeremo come esempio l'Académie Française.

Ed è così che non è possibile trasporre nelle nostre lingue l'esempio statunitense di accettazione di e-neologismi a scopi utili, come spiega Gretchen McCulloch nel suo saggio promosso dal Times come *"una replica ben studiata ai grammatici scontrosi che pensano che la tecnologia stia trasformando i ragazzi in pigri, inarticolati bavosi"*. Il francese, l'italiano, lo spagnolo e tante altre lingue non possono permettersi questo lusso, o allora dovremo accettare di passare da una lingua sofisticata, elaborata e precisa a una sorta di "latino medievale" post-moderno.

Tornando a Matrix, il pensiero di Morpheus si adatta perfettamente ai nostri tempi: *"Nel corso della storia umana, siamo stati dipendenti dalle macchine per sopravvivere. Il destino, a quanto pare, non è privo di senso dell'ironia".*

E per concludere con ironia, proprio le lingue usate accademicamente potrebbero diventare l'ultimo strumento per evitarci qualsiasi censura del Gafam: con i colleghi e, in primis, con l'accordo del nostro omologo citato nel nostro testo, abbiamo parafrasato una descrizione a noi nota grazie a quello che è considerato un caposaldo per gli studiosi: i quattro volumi del compianto Donald Michael Bailey di *A Catalogue of the Lamps in the British Museum* (Londra, 1975-2004).

Abbiamo usato Twitter, Linkedin, Messenger, Facebook e abbiamo postato: *"our colleague XXX is known to be in congress with selected students"* allegando una foto di lui con i suoi studenti di dottorato, il 99% dei quali sono donne. Considerato dagli algoritmi come un errore di inglese scritto da qualcuno di un paese dell'Europa Orientale, il nostro testo non è stato censurato né mentre lo scrivevamo né dopo averlo postato, su nessuna delle reti sociali accennate! Naturalmente, abbiamo cancellato tutti i post immediatamente così come gli account falsi creati per questo esercizio...



Lampada romana in argilla.
Realizzata a matrice da un'officina cipriota, poi importata in Egitto.
Datazione : 30-70 D.C.
Sul suo disco, la stessa scena raffigurata su quattro lampade realizzate in Italia e conservate al British Museum, descritta dal Bailey come «a woman in congress with a man on a bed" (Bailey 1980, pp. 67-68).

Scherzi da ateneo a parte, consideriamo necessarie, indispensabili ed immediate la lettura e la consecutiva implementazione dei consigli che ci offre Cal Newport, docente di Informatica all'Università di Georgetown, nel suo ultimo saggio, tradotto immediatamente in 18 lingue tra le quali anche l'italiano - del quale riproduciamo il titolo originale, che rende meglio il contenuto: *"Digital Minimalism: Choosing a Focused Life in a Noisy World"*. Vi sono talmente tante app e gadget che, minimamente, non mancheranno per niente nemmeno a chi le usa freneticamente... pur di rilanciare il profondo lato umano, appassionato, interessato, disponibile verso le cose realmente importanti che esiste in ognuno ed ognuna di noi.

Bibliografia:

- Nicholas Carr, *The Shallows: What the Internet Is Doing to Our Brains* (updated ed.), Atlantic Books, London 2020
- Cal Newport, *Digital Minimalism: Choosing a Focused Life in a Noisy World,* Penguin Business, London 2019 (versione italiana: *Minimalismo digitale. Rimetti a fuoco la tua vita in un mondo pieno di distrazioni.* Edizioni ROI, Milano 2019)
- Clarissa Theodora Tanil, Min Hooi Yong, *Mobile phones: The effect of its presence on learning and memory,* PLoS ONE 15(8): e0219233.
  (https://doi. org/10.1371/journal.pone.0219233)
- Magnus Liebherr, Patric Schubert, Stephanie Antons, Christian Montag, Matthias Brand, *Smartphones and attention, curse or blessing? - A review on the effects of smartphone usage on attention, inhibition, and working memory,* Computers in Human Behavior Reports 1, 2020 (https://doi.org/10.1016/j.chbr.2020.100005)
- Gretchen McCulloch, *Because Internet: Understanding the New Rules of Language*, Randomhouse, London 2019 ■

1 https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf
2 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

Frank Pasquale
Le Nuove leggi della robotica
Luiss University Press

Nell'era dei Robot è sempre la competenza umana il motore dello sviluppo

di Giovanni Lo Storto* e Daniele Manca*

Frank Pasquale, esperto del rapporto tra tecnologia e legge, da anni lavora sulle profonde asimmetrie informative che caratterizzano l'era degli algoritmi. Lo studioso si è ritagliato negli ultimi anni – con merito – un ruolo da vero precursore della materia. Trae spunto, in questo suo nuovo lavoro, da una semplice constatazione: l'abilità di una macchina o di qualsiasi sistema di automazione, in grado di mostrare capacità umane, non va confuso con l'effettivo possesso di quelle capacità. La parola chiave è simulazione, una parola-bussola che, seguendo il ragionamento di Pasquale, deve guidarci nell'articolare quella "difesa delle competenze umane" che, a detta dello studioso statunitense, rappresenta il cuore della missione fondamentale della nostra specie – mantenere l'innovazione saldamente dalla nostra parte. Possiamo, secondo l'autore, evitare le "conseguenze peggiori della rivoluzione dell'intelligenza artificiale e allo stesso tempo sfruttare il suo potenziale": una posizione non dissimile da quelle espresse da pensatori come Roy Kurzweil, che ha fissato il 2045 l'anno in cui dovrebbe avvenire la singolarità tecnologica, immaginando un mondo in cui esseri umani e macchine saranno ibridate; o o Hannah Fry, la matematica che ha suggerito come neutralizzare una "tecnologia cattiva" favorendo quella "buona".

In *Homo Deus*, Yuval Noah Harari ha sostenuto che entro un secolo le tecnologie trasformeranno nel profondo la razza umana in creature simili a divinità, alimentate dall'intelligenza artificiale e da una miriade di tecnologie che emergeranno da una rivoluzione che egli chiama chiama *datismo*. Harari riconosce che una visione del genere può essere trasformata fin troppo facilmente in una sorta di "religione della tecnologia". Egli, tuttavia, abbraccia pienamente il nucleo vitale che sta alla base delle sue preoccupazioni. Alla domanda se le persone debbano resistere a un futuro di progresso tecnologico apparentemente inevitabile, risponde subito: "È impossibile fermare il progresso tecnologico".

Ci troviamo allora forse nella stessa posizione di Jehuda Löw, capaci di costruire esseri possenti al nostro servizio, ma sempre correndo il rischio che una nostra distrazione, omettere di inserire la tavoletta di legno nella bocca del golem o, fuor di metafora, consentire che l'AI si sviluppi in un contesto di leggi e policy deboli, faccia sì che sfuggano al nostro controllo, diventando una minaccia per noi stessi? Dov'è finito il "sublime digitale" che teorizzava Vincent Mosco, quella qualità della tecnologia e del cyberspazio che ci faceva pensare a un nuovo futuro di apertura e libertà guidato proprio dallo sviluppo delle tecnologie digitali? Forse, e non sarebbe un esito negativo, il nostro rapporto con il mondo digitale sta solo vivendo i dolori della crescita. L'innovazione (e il nostro adattamento), del resto, è un processo di crescita non tanto differente da quello che riguarda i nostri corpi: procede per piccoli strappi e adattamenti successivi, a volte repentini, a volte persino un po' dolorosi. L'esplosione davanti ai nostri occhi dell'era digitale, qualche anno fa, ci ha riempito di entusiasmo. Andando avanti, abbiamo iniziato a percepire qualche turbamento, e poi ci siamo spaventati. Come è possibile che il sogno si sia trasformato in un incubo? Forse non è successo: forse era il nostro sguardo ad essere naturalmente immaturo, e così forse oggi eccediamo nella misura del nostro spavento. È questo il senso del libro di Frank Pasquale: lo sviluppo tecnologico non è il golem, ma un entusiasmante percorso che non sappiamo dove ci porterà, e proprio questo è il bello. Nei prossimi dieci anni vivremo più cambiamenti che nei precedenti due secoli e mezzo, ha osservato Peter Fisk rischiamo di non goderci lo spettacolo perché, forse, abbiamo lasciato che per certi aspetti lo sviluppo procedesse in modo sregolato. Ecco cosa sono le nuove leggi di Pasquale: le regole che consentiranno al gioco di svolgersi correttamente. Frank Pasquale non è il solo ad essersi espresso in questo senso. Il "teorico del tutto" Stephen Hawking e il creatore di SpaceX e Tesla, Elon Musk, sono stati, tra i tanti, forse i più notevoli sostenitori dell'urgente necessità di regolamentare l'AI per evitare che l'umanità paghi un prezzo troppo salato, e ai loro nomi così eclatanti si aggiunge una lunga lista di pensatori, intellettuali, filosofi, policy-makers… È proprio sull'urgenza e la natura di questa regolamentazione che è costruita la profonda riflessione di Frank Pasquale, che ricorda come le leggi di Asimov (uno: un robot non può recar danno a un essere umano né permettere che, a causa di un suo mancato intervento, un essere umano riceva danno; due: un robot deve obbedire agli ordini impartiti dagli esser umani, purché non vadano in contrasto con la prima legge; tre: un robot deve proteggere la propria esistenza purché non vada in contrasto con la prima o la seconda legge), non bastino più. Oggi l'umanità si trova a fronteggiare rischi molto più insidiosi di quelli immaginati dal filosofo e scienziato di origine sovietica. Le leggi di Pasquale sono le linee guida lungo le quali organizzare la nostra difesa: l'AI deve essere complementare alla competenza umana, diventare una intelligenza *aumentata* più che artificiale, strumento al fianco di professionisti e lavoratori e non loro sostituto; non bisogna consentire a nessuno, big tech incluse, di contraffare l'umanità – di dare cioè ai sistemi di AI voci e fattezze umane, di istruirli a simulare emozioni e comportamenti di uomini e donne; è necessario combattere la corsa agli armamenti che le nuove tecnologie rischiano di innescare; infine, la trasparenza deve essere un requisito irrinunciabile dei sistemi intelligenti, che devono recare i nomi di chi li ha creati e li controlla. Sullo sfondo, rimane un principio che Pasquale lascia implicito e che noi proviamo a chiarire, prendendo in prestito le parole di Gerd Leonhard: il futuro – inteso anche nel senso materiale delle nuove tecnologie – non

è qualcosa in cui inciampiamo, non è un'ombra che ci sovrasta, un accadimento ineluttabile che siamo costretti a subire.

Il futuro è quello che facciamo noi ogni giorno: siamo noi nella cabina di comando. *Le nuove leggi della robotica* è un libro che potrebbe benissimo essere usato dai legislatori per scrivere le leggi e i regolamenti che governeranno lo sviluppo dell'AI nei prossimi anni, anzi, è auspicabile che venga letto e discusso ampiamente. L'ambito del lavoro e della difesa della competenza umana, benché di estrema importanza e vastissimo, è tuttavia addirittura limitato se paragonato alla reale portata della sfida che secondo Frank Pasquale ci stiamo giocando: secondo lui infatti – ed è difficile dargli torto – limitare la competenza al contesto delle professioni è tanto fuorviante quanto pericoloso. Sono i valori umani la vera competenza da preservare: e così, nell'era della tecnologia esponenziale, viene da concludere che al cuore del vero sviluppo c'è la trasmissione di quei saperi che, da sempre, rendono gli esseri umani quello che siamo. Ma la regolamentazione, le leggi, l'apprendimento di discipline e materie *inutili* o magari addirittura umanistiche, tutto questo parlare di etica, insomma – non rischia di frenare l'innovazione? Forse: ma tutto dipende dal senso e dal valore che diamo alla parola innovazione. Perseguire uno sviluppo tecnologico e una crescita economica senza limiti e senza badare alle conseguenze somiglia davvero a una strada che sale? Ricordare che si è inseriti in un sistema – una società, una comunità, un ecosistema… - che è anche nostra responsabilità curare, a volte anche prima di un interesse individuale, è davvero un segnale di decrescita? Sul terreno dello sviluppo tecnologico si gioca oggi una partita di cruciale importanza per il genere umano, e siamo così fortunati da essere noi a poterla giocare. Dimostriamo di esserne all'altezza.

---

*Gionanni Lo Storto direttore generale Università Luiss Guido Carli e Daniele Manca vicedirettore del Corriere della Sera sono autori della prefazione del saggio di Frank Pasquale. Ne pubblichiamo un estratto ringraziando la Luiss University Press per la gentile concessione. ■

Fareed Zakaria
Il mercato non basta: dieci lezioni per il mondo dopo la pandemia
Ed. Feltrinelli

Per cambiare dobbiamo prima di tutto capire il mondo

di Massimiliano Cannata

La metamorfosi è la legge della vita. La pandemia ci ha sbattuto in faccia questa evidenza, ora sta a noi reagire con razionalità e intelligenza. Ne saremo capaci? Fared Zakaria analista indoamericano della Cnn tra i massimi esperti di geopolitica

nell'era della globalizzazione è disposto a fare professione di ottimismo a una condizione però: che l'umanità sappia modificare in fretta convinzioni e atteggiamenti. In questo suo ultimo saggio lo studioso offre uno spaccato interessante dello stato del pianeta. È bene ricordarsi, questo il primo suggerimento che la tempesta non è ancora finita, abbiamo lasciato le mascherine ma non certo la paura. Il mostro si chiama ora variante Delta, la partita non è vinta. "Per cambiare bisogna prima di tutto capire il mondo", questo il primo grave deficit conoscitivo che ci ha caratterizzato. Dobbiamo ritornare al pensiero critico, per rimetterci in cammino alla svelta, senza spazio per la riflessione non riusciremo a mettere in campo quelle strategie necessarie a contrastare la risacca della globalizzazione.

Ma proviamo a enucleare in sintesi le dieci lezioni, tratteggiate nello studio.

La prima lezione riguarda il nostro rapporto con il tempo, che deve legarsi alla responsabilità, costituendo un binomio che non potremo più separare. Gli errori fatti nel recente passato ci hanno presentato il conto. I margini di manovra sono ormai sottilissimi, non avremo una seconda chance, o ci si salva insieme o periremo tutti. La seconda lezione si sofferma sul dramma della diseguaglianza, destinata a diventare una delle grandi questioni della contemporaneità. Vi sono paesi più avanzati e paesi fatalmente indietro. La campagna di vaccinazione lo ha fatto vedere in maniera molto chiara. L'Europa è rimasta indietro rispetto agli USA, mentre paesi come India, Brasile, interi continenti come l'Africa, aspettano ancora interventi efficaci e risposte. Se non ci occuperemo di loro ogni sforzo sarà vano, è bene ricordarselo.

Terza lezione: *"Il tetto va aggiustato mentre c'è il sole"*, il motto preso a prestito dal grande presidente americano Kennedy è quanto mai cogente in questa fase storica. Le occasioni non devono essere sprecate, perché potremmo trovarci di fronte a un'emergenza ancora più grave nel prossimo futuro. Ora o mai più… Bisogna intervenire sugli errori fatti per correggerli a tutti i livelli. Quarto punto di attenzione: le azioni individuali non bastano, lo si può facilmente constatare sul difficile terreno della politica. Populismi e nazionalismi hanno le ore contate, serve un piano per la cooperazione globale per superare l'impasse in cui ci siamo cacciati. Sul terreno della geopolitica gli effetti del nuovo corso si stanno già registrando. Le tensioni con la Cina sono una componente preoccupante, cui però fa fortunatamente da contraltare il diverso indirizzo che Biden sta cercando di dare alla politica estera americana. Alt all'"*American First*" vessillo di Trump, maggiore equilibrio e consapevolezza della complessità saranno i punti di riferimento di un mutato indirizzo, che riavvicinerà gli USA al tradizionale rapporto privilegiato con il vecchio Continente. Altro aspetto incoraggiante la collaborazione tra Francia e Germania che coincide con quella che Draghi ha definito la fine della stagione del

debito, per enfatizzare la necessità di adottare investimenti finalizzati allo sviluppo di cui l'economia, stremata dal *lockdown*, ha bisogno.

Quinta lezione: individuazione corretta delle priorità. Consumo di energia da ridurre, gas serra da limitare, deforestazione selvaggia, città intensive, tutti fenomeni che vanno tenuti sotto controllo e che dovranno trovare una classe dirigente pronta a farsi carico di una corretta *governance* dell'innovazione non facile da praticare. Alle tradizionali categorie *dell'essere e del tempo* enunciate da Heidegger nel celebre saggio che rappresenta una delle pietre miliari della filosofia del '900, occorrerà aggiungere l'oikos degli antichi greci, ossia l'ambiente entro cui ci muoviamo, una nutrice che si prende cura di noi fin dalla nascita, che però l'umanità, alle più diverse latitudini, ha tradito, ignorando le leggi dell'ecosistema.

La sesta raccomandazione riguarda alcuni comportamenti scorretti. AIDS, SARS, EBOLA, febbre Suina, COVID 19 si sono diffuse a causa di un connubio troppo stretto uomo animale. Bisognerà in questo caso ritrovare le "giuste distanze", osservando canoni di maggiore rispetto della salute e dell'integrità fisica, se non vorremo avere a che fare, nel prossimo futuro con altre anche più terribili epidemie.

Il percorso di Zakaria non si ferma ai fattori ambientali, per spingersi a considerare l'universo della politica, che deve modificare contenuti e linguaggi. L'esempio che viene portato dallo studioso riguarda il *"millenarismo apocalittico"* in cui una grande democrazia come l'America vive purtroppo ancora avvolta. Da un recente sondaggio è emerso che per il 50 % della popolazione non è tanto importante fare buone leggi e adeguate riforme per migliorare la macchina dello stato, quanto attivare dei meccanismi di difesa contro chi (sarebbero in tanti secondo questa percezione) vorrebbe la distruzione della nazione a "stelle e a strisce". Aspetto strettamente legato al rinnovamento della politica, la necessità di superare la polarizzazione del mondo e la "dittatura" delle *fake news*. L'esercizio della "bugia" in una società fragile in balìa delle menzogne che proliferano in rete va insomma arrestato, per poter ritrovare quella cognizione della realtà necessaria a inquadrare i fenomeni che attraversano la società in questo cambiamento d'epoca.

Rafforzare gli strumenti della conoscenza vuol dire affinare rigore di metodo. Non sarebbe una cattiva abitudine tornare a verificare le fonti da cui attingere elementi di analisi, il più possibile oggettiva su quello che avviene e sui fatti che segnano la nostra vita. Di capitale importanza, in questa dinamica, non farsi distrarre dai "rumori" di fondo. Questa la decima e ultima "lezione", che fa intravedere il monito di chi vuole sgombrare il campo dall'*"entropia"* informativa, che disorienta, annebbiando la coscienza dei cittadini, costretti ad annaspare nel mare di incertezze, create ad arte. Non abbiamo certo bisogno di falsi manovratori, per uscire dal tunnel della crisi, che ci attanaglia da troppo tempo. In questo si innesta il ruolo degli intellettuali: "La scrittura non servirà a trasformare i bruchi in farfalle, non servirà a farci sentire meglio, ma a renderci più umani", ha ragione Paul Aster che ha usato queste parole esprimendo il suo parere su questo *annus horribilis*. Crediamo che lo spirito che ha animato Zakaria non sia molto distante da questa posizione. *"Nulla è già scritto"* il titolo dell'ultimo capitolo del libro apre, infatti, un regno inedito di possibilità, che sta all'uomo saper volgere a proprio favore, senza cercare alibi superficiali, destinati a liquefarsi alla prima prova della storia. ■

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