Cybersecurity Trends

Edizione italiana, N. 4 / 2021

INTERVISTE VIP:

LUCIANO FLORIDI
PIERAUGUSTO POZZI
AGNESE SCAPPINI

Folder Centrale: Vulnerability Management

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

Gestire le priorità in scenari complessi.

Autore: Nicola Sotira

La digitalizzazione fa continui progressi nell'innovazione di prodotti e servizi, e nell'era COVID ha visto un'improvvisa accelerazione. Tutto si sta spostando velocemente online, creando una nuova fase economica legata alla rivoluzione digitale che rischia di fare vittime anche a livello sociale. Questa transizione sempre più veloce e sempre più caldeggiata anche dal legislatore che, dovendo affrontare lo stato di crisi pandemica, ha visto nel digitale un alleato nella gestione della crisi, piattaforme di vaccinazione, green pass, gestione intelligente dell'anagrafe, utilizzo di App per la mobilità e prenotazione dei sistemi sanitari solo per fare alcuni esempi. In questo contesto, il settore della sicurezza informatica sembra arrancare, essendo ancora legato a vecchi schemi che a volte non corrispondono all'agilità richiesta dalla trasformazione digitale, oltre al problema cronico di essere percepito solo come un costo. Spesso, bisogna ammettere che l'inadeguatezza nella valutazione del rischio informatico ha come conseguenza il riversamento di attività e risultati degli scanner sui dipartimenti IT che non fanno altro che sovraccaricare il personale che difficilmente può gestire questo numero di attività. Uno degli argomenti, nel vasto catalogo dell'enciclopedia della sicurezza, è la gestione delle vulnerabilità dove si cerca ancora di dare priorità all'enorme numero di segnalazioni euristiche, spesso limitate, con il risultato che queste rimangono residenti nei sistemi per mesi o anni. Solo per contestualizzare alcuni numeri, usiamo il rapporto del National Institute of Standards (NIST) che nel 2020 ci dice che sono state registrate oltre 18.000 vulnerabilità dove il 57% è stato classificato ALTO/CRITICO.

Un approccio potrebbe essere quello di trovare metodologie per correggere e rimediare a tutte le vulnerabilità garantendo la massima copertura. Questa opzione, però, consumerebbe certamente risorse in modo inefficiente, fissando anche problemi a basso rischio. D'altra parte, correggere solo le vulnerabilità ad alto rischio ci lascerebbe esposti ad altre vulnerabilità. La sfida è trovare la giusta combinazione di queste opzioni esposte e ridurre il numero di segnalazioni ai dipartimenti IT aziendali. Questa sarà una delle sfide che dovremo affrontare per aumentare l'efficacia e il valore della sicurezza delle informazioni nel nuovo ecosistema digitale.

Diverse ricerche ci mostrano uno scenario in cui quando viene rilasciata una nuova vulnerabilità di sicurezza, gli aggressori iniziano una corsa frenetica per scansionare la rete alla ricerca di sistemi vulnerabili, mentre chi si difende deve attuare delle contromisure per proteggere le proprie infrastrutture. Sempre da questa ricerca sappiamo che in media gli aggressori iniziano la scansione entro i primi 15 minuti dal rilascio dei CVE, parlando di vulnerabilità pubbliche e non di zero day. Purtroppo, il numero di queste CVE, anche solo considerando quelli critiche, è in continuo aumento e senza un'adeguata prioritizzazione le azioni di mitigazione rischiano di mettere in difficoltà anche i migliori reparti IT.

La scansione dell'infrastruttura pubblica, l'inventario aggiornato delle risorse, l'utilizzo dell'intelligence insieme a una comprensione avanzata degli exploit è sicuramente una delle basi per un'efficace prioritizzazione delle vulnerabilità.

Inoltre, i progressi dell'intelligenza artificiale possono offrire diverse opportunità per ridurre la manualità e quindi aumentare l'efficienza nella gestione delle vulnerabilità. La crescente complessità delle reti e applicazioni, insieme al numero e alla sofisticazione delle minacce, rende l›uso dell›AI rilevante nel lavoro di prioritizzazione delle criticità. ■

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.

Che cos'è la Vulnerability Management Prioritization?

Autore: Ed Bellis

La Vulnerability management prioritization è uno degli aspetti più importanti di un moderno programma di vulnerability management. La prioritizzazione è fondamentale perché l'azienda media presenta milioni di vulnerabilità informatiche, ma anche i team più dotati di risorse possono risolvere solo il 10% circa di esse.

Perché la vulnerability management prioritization è fondamentale?

La Vulnerability management prioritization è un elemento critico di un programma di vulnerability management. Infatti, un'azienda tipica può presentare milioni di vulnerabilità informatiche su laptop, server e dispositivi connessi a Internet come stampanti e router, ed è impossibile anche per il team più dotato di risorse rimediare ad ogni vulnerabilità.

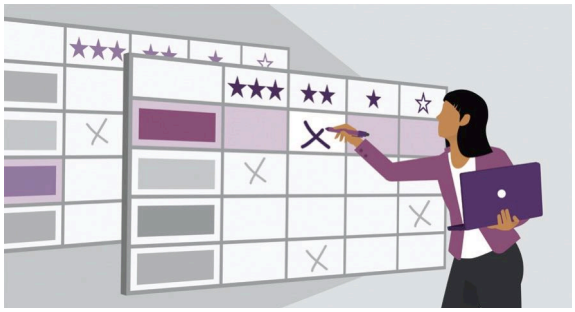
In effetti, l'organizzazione media può aspettarsi di correggere solo 1 su 10 di tutte le vulnerabilità all'interno del proprio ambiente. Questo è ciò che rende il vulnerability management così essenziale.

La prioritizzazione è la chiave

L'efficacia di un programma di vulnerability management è direttamente legata alla sua capacità di concentrarsi sulle vulnerabilità che rappresentano il rischio maggiore per una specifica organizzazione. Un approccio diverso potrebbe non essere di aiuto ai team di remediation IT e AppDev oberati di lavoro, i quali rischierebbero di sprecare il loro tempo per correggere vulnerabilità a basso rischio.

BIO

Ed Bellis, Chief Technology Officer e cofondatore di Kenna Security, ora parte di Cisco, è un veterano ed esperto del settore della sicurezza ed è conosciuto negli ambienti della sicurezza come "il padre della gestione delle vulnerabilità basata sul rischio". Ha fondato Kenna Security per fornire un approccio alla risoluzione dei rischi basato sui dati e aiutare i team IT a stabilire le priorità e contrastare le potenziali minacce alla sicurezza. Ed è l'ex CISO di Orbitz ed ex vicepresidente, Corporate Information Security presso Bank of America. È consulente di Dharma ed ex consulente di SecurityScoreboard.com e Society of Payment Security Professionals. Ed è uno degli autori del libro Beautiful Security (Oram, Andy & Viega, John, O'Reilly Media, 2009). Ed è un relatore frequente a conferenze del settore, tra cui RSA e Black Hat e un collaboratore di cybersecurity per Forbes, Dark Reading, SC Magazine e altre pubblicazioni.

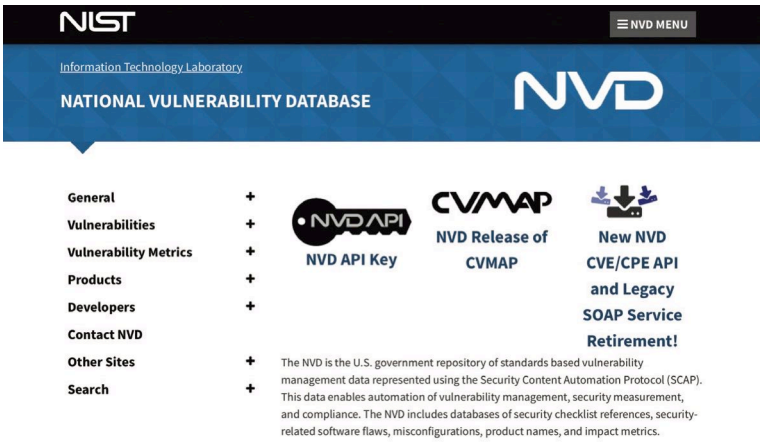


La maggior parte delle organizzazioni oggi prioritizzano le vulnerabilità in base a due approcci: si affidano al Common Vulnerability Scoring System (CVSS) per determinare quali vulnerabilità correggere prima, oppure si basano sulla priorità fornita dalla loro soluzione di scansione delle vulnerabilità. I due approcci spesso si sovrappongono perché molti scanner si basano principalmente sui punteggi CVSS per determinare la priorità.

Pregi, punti di forza e carenze del CVSS

La maggior parte delle organizzazioni prioritizzano le vulnerabilità in base ai punteggi CVSS, utilizzando spreadsheet, tool scelto per la gestione delle correzione delle vulnerabilità. I punteggi CVSS, che classificano la gravità delle vulnerabilità informatiche su una scala da 1 a 10 (dove 10 è il più grave), sono molto utilizzati perché sono molto intuitivi. La maggior parte dei team di sicurezza e IT si concentra sulle vulnerabilità con punteggi CVSS di 7 o superiori. Le vulnerabilità valutate con quel livello finiscono nello spreadsheet della remediation, di solito con priorità in base al punteggio, quelle vicine a 10 sono in cima alla lista.

Sebbene il CVSS sia semplice, presenta diversi svantaggi. Innanzitutto, basandosi su sistemi di punteggio, il CVSS è statico. Una volta che le vulnerabilità sono catalogate e assegnate a un numero CVE (Common Vulnerabilities and Exposures), in genere ricevono un punteggio CVSS nel National Vulnerability Database entro poche settimane, prima che vengono scritti eventuali exploit in gradi di sfruttarle.



Ciò significa che vengono valutati in base alla valutazione iniziale del loro potenziale da sfruttare per poi essere aggiornati raramente, se non mai. Ma le vulnerabilità sono dinamiche e il loro profilo di rischio cambia spesso nel tempo man mano che vengono pubblicati exploit in grado di sfruttarle e tali exploit vengono utilizzati in natura. I punteggi statici non tengono conto di tali modifiche.

Inoltre, i punteggi CVSS mancano di un contesto. In altre parole, non riflettono fattori come la prevalenza della vulnerabilità negli ambienti di rete reali, il volume degli exploit, l'importanza dell'asset interessati o qualsiasi altra informazione contestuale necessaria al security analyst per comprendere veramente il livello di rischio.

Punti di forza e di debolezza del punteggio dello scanner

Gli strumenti di scansione che offrono un punteggio e una prioritizzazione si basano sulla convenienza: producono sia i risultati della scansione che la prioritizzazione delle vulnerabilità in un'unica soluzione. Ma molte soluzioni di scansione riconfezionano semplicemente il punteggio CVSS, applicando una loro scala (ad esempio, 1-5 invece di 1-10).

Questi punteggi dello scanner, e la loro conseguente prioritizzazione, sono statici e privi di contesto rispetto ai punteggi CVSS.

Il contesto è vitale per la vulnerability management prioritization

Per un'efficace vulnerability management prioritization, è importante che gli strumenti di gestione delle vulnerabilità tengano conto di più del semplice fatto che un CVE sia stato sfruttato o della rapidità con cui si verificano tali exploit. Un processo moderno di vulnerability management tiene conto anche del contesto nel quale si inquadra ogni vulnerabilità e il suo posto unico all'interno di un ambiente IT. Ad esempio, risponde a una serie di domande, tra cui:

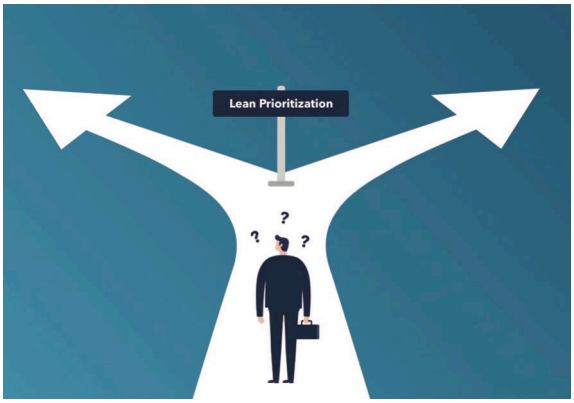
- Quanto è importante nel tuo ambiente l'asset (server, dispositivo o rete) in cui è presente la vulnerabilità? È rivolto a Internet o al cliente?
- L'asset contiene informazioni finanziarie o altre informazioni sensibili?
- La vulnerabilità esiste all'interno di un ambiente regolamentato?
- Quanti utenti potrebbe avere un impatto per un exploit eseguito con successo?
- Gli exploit prendono di mira attivamente la tua azienda?

Senza l'aiuto di una moderna soluzione di vulnerability management prioritization, sarebbe impossibile rispondere a tutte queste domande per valutare correttamente il rischio che ogni vulnerabilità rappresenta per il tuo ambiente unico. La giusta piattaforma, tuttavia, gestisce automaticamente tutte queste attività. Infatti, le più moderne soluzioni di vulnerability management integrano informazioni complete sulla vulnerabilità con un'ampia intelligence sulle minacce del mondo reale, applicano una *data science* avanzata guidata da algoritmi di machine learning e una risk analysis automatica, metriche di rischio personalizzate che aiutano a tracciare e segnalare i progressi nella riduzione del rischio e anche remediation service level agreements (SLAs) basati sul rischio che una vulnerabilità rappresenta per il tuo ambiente, confrontato con la propensione al rischio della tua organizzazione.

Vulnerability management prioritization: Perchè "abbastanza buono" non lo è

Quando si tratta di vulnerability management prioritization, soluzioni "abbastanza buone" come CVSS e prioritizzazione basata su scanner rischieranno di farvi andare alla ricerca di vulnerabilità che non rappresentano un rischio per il tuo ambiente, impedendo ai team di sicurezza e IT di dedicare tempo a iniziative più preziose.

Sia il CVSS che la prioritizzazione basata su scanner producono così tanto rumore - vulnerabilità elencate come "critiche" che in realtà non comportano



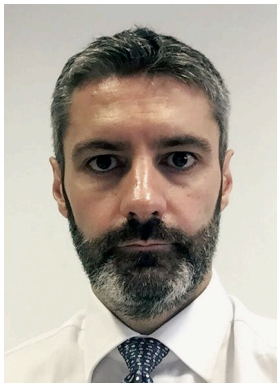
alcun rischio misurabile - che il costo reale dell'utilizzo di tali approcci può superare di gran lunga le spese di investimento in una soluzione che dà la priorità alle vulnerabilità in base al rischio.

In un test nel mondo reale su tre approcci di prioritizzazione che lavorano dallo stesso set di dati, CVSS2 ha determinato che l'organizzazione aveva bisogno di correggere 17.279 vulnerabilità per ottenere una copertura di remediation del 50%. Una nota soluzione di scansione ha dato la priorità a 15.214 vulnerabilità come "critiche". Infine, una soluzione di gestione delle vulnerabilità basata sul rischio ha determinato che era necessario correggere solo 627 vulnerabilità per ottenere una copertura di remediation del 50% e affrontare comunque ogni vulnerabilità ad alto rischio. Da quale elenco di priorità per la gestione delle vulnerabilità preferiresti lavorare?

La verità è che, risk-based vulnerability management prioritization allinea i team di sicurezza e di bonifica attorno a un obiettivo comune, la riduzione del rischio, e a sua volta elimina l'attrito che si verifica così spesso quando la sicurezza consegna all'IT un elenco di migliaia di cosiddette vulnerabilità "critiche" a patch con poca o nessuna comprensione sul motivo per cui devono essere patchate.

Dai un'occhiata al podcast Why Vulnerability Scores Can't Be Looked At In A Vaccum, per ulteriori informazioni su come funziona la definizione delle priorità della gestione delle vulnerabilità e su come si sta evolvendo. ■

Gestione delle vulnerabilità.



Autore: Massimo Cappelli

Quando si tratta l'argomento vulnerabilità non bisogna tralasciare il contesto in cui la vulnerabilità viene inserita. Il contesto di riferimento è la funzione del rischio. Il rischio lo intendo come funzione dipendente dal prodotto della minaccia per la vulnerabilità per l'impatto. La vulnerabilità ovviamente viene associata a un bene, inteso in questo caso come un asset informatico (hardware o software). Quindi il rischio è dato dalla probabilità che una minaccia sfrutti una vulnerabilità, presente su un asset, e provochi quindi un impatto.

BIO

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

Primo passo per gestire le vulnerabilità è raccogliere informazioni sugli asset. La gestione delle vulnerabilità è una tematica che affligge tutte le aziende, soprattutto le aziende complesse e di grandi dimensioni che nel corso degli anni hanno stratificato le proprie infrastrutture IT. Molte realtà si sono strutturate con propri datacenter per poi passare a sistemi ibridi, con la convivenza di datacenter interni e cloud; oppure si sono affidate a soluzioni completamente in cloud.

Queste stratificazioni hanno aumentato la complessità delle infrastrutture stesse su cui poggiano i servizi aziendali. Spesso le architetture non vengono aggiornate e si rischia di avere fotografato un'architettura in un tempo T0 che nel corso degli anni ha subito modifiche. Nelle aziende multi-servizi, dove, a volte, per ogni business unit esiste un referente IT, la gestione degli asset può essere ancor più critica se manca un coordinamento centrale fra tutti i referenti.

Per non parlare dell'espansione del cloud, in cui gli asset sono gestiti da fornitori esterni, dell'avvento della tecnologia workload e della diffusione degli IoT. La tecnologia è in continua evoluzione ed è difficile stare al passo. Questo è determinato anche da un approccio a silos.

Un problema annoso, che se ne dica, non è mai stato pienamente risorto. Per usare una metafora pubblicitaria: ogni mattina un manager si alza e sa che dovrà correre per raggiungere i propri obiettivi di business; ogni mattina un CISO si alza e sa che dovrà rincorrere un manager per mettere al sicuro il business.

La creazione di un gestionale centralizzato che raccolga e normalizzi le informazioni su tutti gli asset è una soluzione che potrebbe agevolare la gestione delle vulnerabilità ma non è da considerarsi sufficiente. La piattaforma dovrebbe essere mantenuta e aggiornata e soprattutto

dovrebbe essere arricchita da informazioni che permettano di contestualizzare l'asset. L'informazione principe è relativa al servizio a cui afferisce quell'asset. Solo con la contestualizzazione di quale servizio poggia su quell'asset, si può veramente comprendere quale ruolo abbia e quale criticità possa rappresentare una sua esposizione. Ci saranno asset che supportano processi di business e asset che supportano processi interni, oppure entrambi i processi. Il mantra è simile a quello della Polizia: segui i soldi. Identificare i servizi che generano i ricavi e la catena tecnologica che li supporta è un primo passo per garantire che i servizi a maggiore valore aggiunto possano essere protetti.

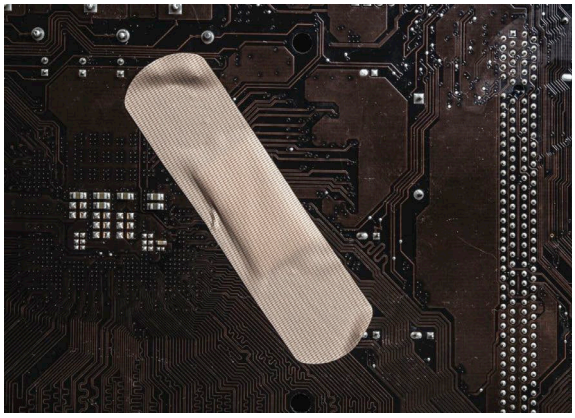
A seconda del servizio supportato è necessario stabilire quale sia la rilevanza dell'asset stesso. Quindi è necessario effettuare una pesatura. La pesatura è dettata dalla tipologia di informazioni che tratta e dalla rilevanza che ha nel processo di creazione del valore. Questo è fondamentale per determinare l'impatto, nel caso in cui la vulnerabilità venga sfruttata.

Una volta raccolte le informazioni sugli asset e sui servizi a cui afferiscono, è necessario verificare che questi asset non siano affetti da vulnerabilità, perlomeno conosciute. E qui che entrano in gioco informazioni esterne all'azienda. Esistono database pubblici e a pagamento che mettono a disposizione informazioni sulle nuove vulnerabilità. L'acronimo utilizzato per identificare nuove vulnerabilità è CVE (Common Vulnerabilities and Exposures).

Sono queste informazioni che devono essere correlate con le informazioni degli asset presenti in azienda. Le vulnerabilità solitamente vengono pubblicate con un livello di gravità, calcolato considerando più parametri: possibilità di accesso, di sfruttamento, complessità nello sfruttamento, l'impatto che può provocare in caso di sfruttamento e così via. La presenza di una vulnerabilità su un asset fa scattare tutta una serie di considerazioni di cui abbiamo accennato sopra e che considerano sia la rilevanza dell'asset contestualizzata sia la criticità della vulnerabilità.

Oltre a ciò, sarebbe opportuno considerare anche chi possa essere in grado di sfruttare questa vulnerabilità. Qui si entra nella sfera della minaccia. L'esistenza o meno del cosiddetto exploit, l'accessibilità a questo exploit, il prezzo stesso dell'exploit sono ulteriori fattori da considerare nell'attribuzione del livello di criticità. Inoltre, considerazioni devono essere fatte anche su chi eventualmente abbia capacità di sfruttare quell'exploit. Queste considerazioni servono a comprendere le tempistiche necessarie per il processo di patching.

Il patching non è un processo immediato perché richiede un'analisi per comprendere quali possano essere le conseguenze dell'installazione della patch sul sistema. Inoltre, soprattutto in realtà complesse, il sistema di patching prevede delle pianificazioni con archi temporali più o meno lunghi. Una patch può richiedere a volte anche mesi prima di essere installata. Le informazioni sulla minaccia servono a determinare

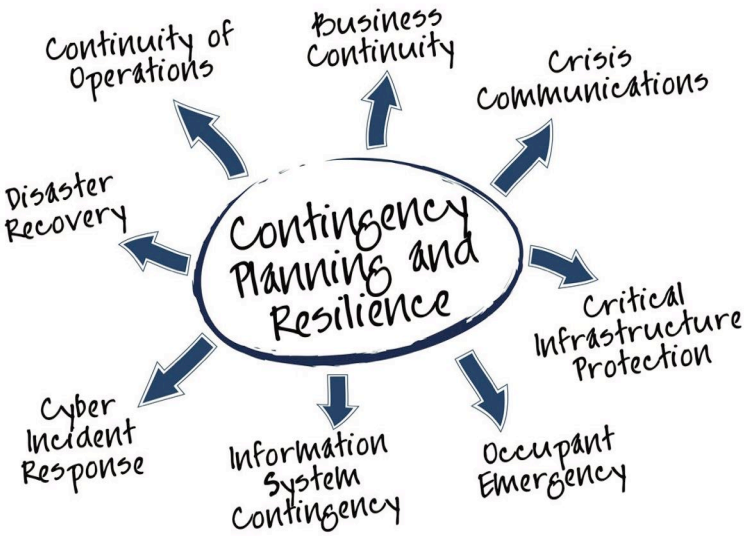


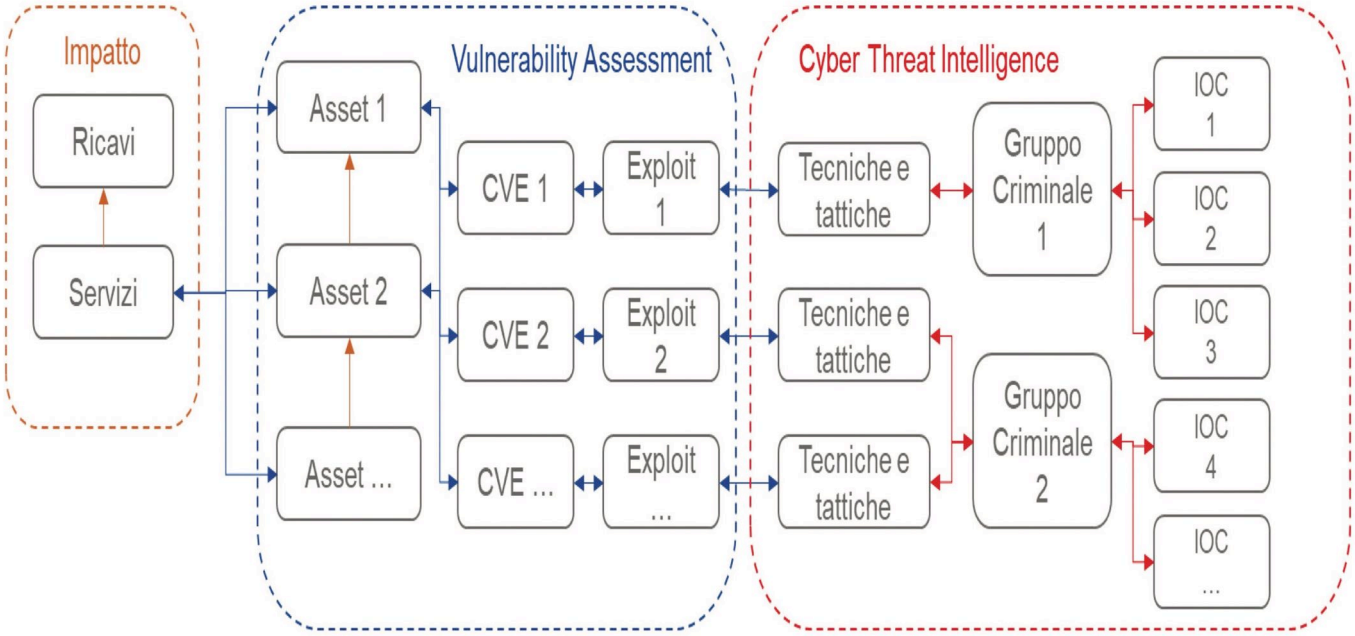
se quel processo debba essere accorciato oppure no. Se si hanno indicatori che la propria azienda sia sotto attacco da gruppi specifici e questi gruppi siano in grado o abbiano già sfruttato una determinata vulnerabilità, allora sarebbe il caso di accorciare i tempi e chiedere il rilascio della patch quanto prima. Gli indicatori possono derivare da campagne di phishing subite, da alert scattati sul perimetro esterno e così via.

In sintesi, per avere un sistema efficiente ed efficace di gestione delle vulnerabilità, è necessario avere tutta una serie di altre informazioni: un database con tutti gli asset presenti in azienda; i servizi supportati dai singoli asset e il valore che questi servizi creano; almeno una fonte informativa sulle vulnerabilità pubblicate ed eventuali exploit ad esse associate; dove possibile anche informazioni sui modelli di attacco in cui potrebbero essere utilizzate e relativi gruppi criminali. In questo modo, fintanto che la vulnerabilità non è sanata, sarebbe possibile comunque monitorare altri indicatori per proteggere i servizi.

Questo solo per pesare la vulnerabilità e poterla comunicare con il giusto dettaglio informativo ai gestori del patching. Avere una correlazione di tutte queste informazioni potrebbe portare l'azienda a passare da un concetto di rischio statico a rischio dinamico. La valutazione del rischio cyber non si limiterebbe più a una semplice fotografia nel tempo ma a un flusso continuo. I decisori potrebbero avere la possibilità, in ogni istante di verificare il livello del rischio cyber associato al servizio. Ne gioverebbero anche i processi di crisis management, incident handling e business continuity.

Il tutto però richiede sia un forte commitment da parte dei business owner, sia una forte collaborazione fra tutte le anime dell'azienda che dovrebbero fare sistema. È il business owner che deve imporre questa filosofia di pensiero sia alle funzioni IT sia alle funzioni di sicurezza. ■





Le 4 fasi del Vulnerability Management: Un processo per la mitigazione del rischio.

Autore: Paolo Cecchi

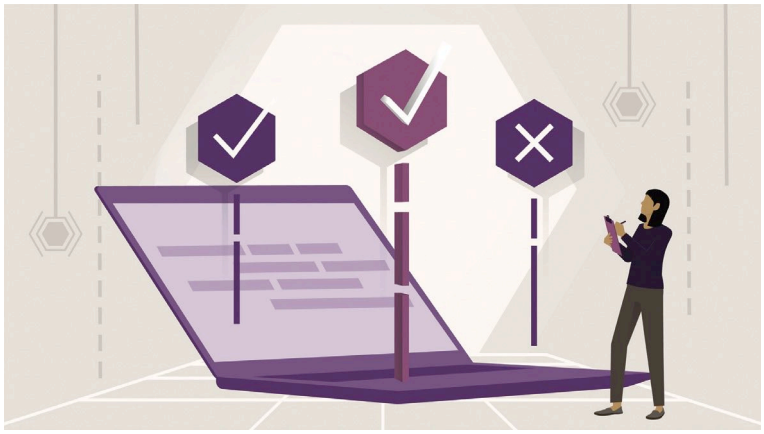
Le strategie e gli strumenti di gestione delle vulnerabilità consentono alle organizzazioni di valutare e mitigare rapidamente le vulnerabilità di sicurezza nella loro infrastruttura IT. Un processo di gestione delle vulnerabilità può variare da organizzazione ad organizzazione, ma la maggior parte dovrebbe seguire quattro fasi principali: identificazione delle vulnerabilità, valutazione delle vulnerabilità, trattamento delle vulnerabilità e infine segnalazione delle vulnerabilità. Tipicamente, una combinazione di strumenti e risorse umane esegue questi processi.

In questo articolo tratteremo le seguenti tematiche:

- Che cos'è la gestione delle vulnerabilità
- L'importanza della gestione delle vulnerabilità
- Le 4 fasi del processo di gestione delle vulnerabilità
- Creazione di programmi di gestione delle vulnerabilità efficaci

Che cos'è la gestione delle vulnerabilità?

La gestione delle vulnerabilità è una strategia che le organizzazioni possono utilizzare per monitorare, ridurre al minimo ed eliminare le vulnerabilità nei loro sistemi. Implica l'identificazione e la classificazione delle vulnerabilità in modo che possano essere applicate protezioni appropriate o adottate misure correttive.



Spesso, i processi di gestione delle vulnerabilità impiegano l'uso di scanner di vulnerabilità, database di vulnerabilità, test di vulnerabilità manuali o automatizzati e una varietà di altri strumenti. Questa combinazione di strumenti e processi aiuta i team di sicurezza a garantire che tutte le minacce vengano prese in considerazione.

BIO

Paolo Cecchi è Regional Sales Director di Exabeam per Italia, Malta e Iberia. Nel gennaio 2021 apre la filiale italiana di Exabeam, con il compito di posizionarla sul mercato, creare nuove opportunità di business e sviluppare il canale di vendita nella regione. In precedenza ha lavorato in importanti System Integrator operanti a livello nazionale e in multinazionali del settore (Telindus, Juniper, FireEye, Carbon Black poi acquisita da VMware), ricoprendo nel tempo ruoli di vendita con maggiore responsabilità. Negli oltre 20 anni di esperienza sul campo ha maturato significative competenze nella vendita di soluzioni a valore aggiunto in ambito cyber security e ICT.

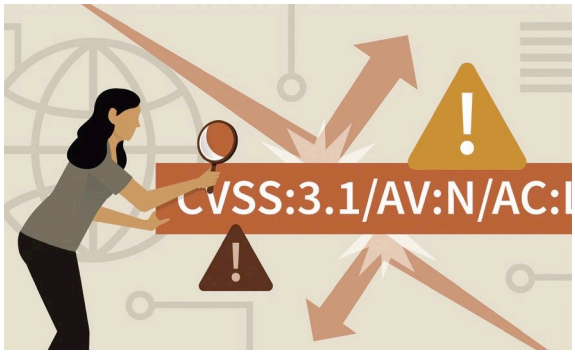
Ciò comprende:

- Vulnerabilità nel codice, come SQL injection o opportunità di cross-site scripting (XSS)
- Meccanismi di autenticazione e autorizzazione insufficienti
- Impostazioni non sicure o mal configurate, come controlli di accesso deboli o password

L'importanza della gestione delle vulnerabilità

Le vulnerabilità offrono opportunità agli aggressori di entrare nei sistemi aziendali. Una volta all'interno, gli attaccanti possono abusare delle risorse aziendali, rubare dati o negare l'accesso ai servizi.

Un programma di gestione delle vulnerabilità fornisce linee guida strutturate per aiutare le organizzazioni a valutare e proteggere la propria Infrastruttura. Piuttosto che ignorare le vulnerabilità o rischiare che le vulnerabilità vengano trascurate, questo processo può aiutare i team di sicurezza a condurre una ricerca approfondita.



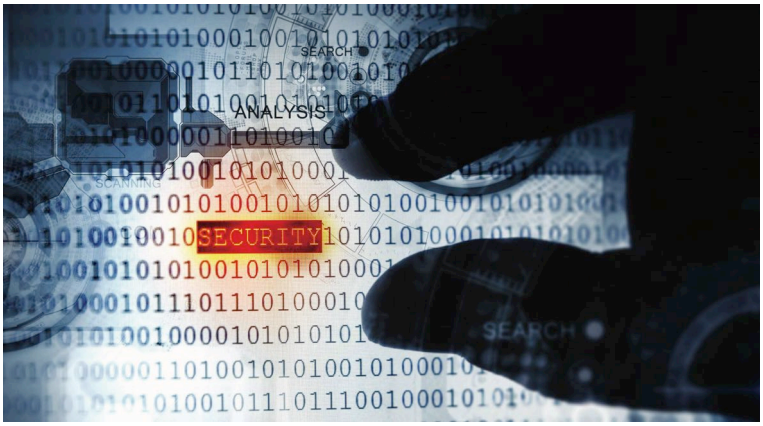
Le strategie di gestione delle vulnerabilità permettono di ridurre il tempo di esposizione dell'azienda a possibili attacchi e anche fornire una prova di due diligence nel caso in cui l'organizzazione sia compromessa nonostante gli investimenti in programmi cyber.

Le 4 fasi del processo di gestione delle vulnerabilità

Quando si crea un programma di gestione delle vulnerabilità, è necessario tenere conto di diverse fasi, che se implementate correttamente permettono di garantire che nessuna vulnerabilità venga trascurata.

1. Identificare le vulnerabilità

La prima fase del processo di gestione richiede l'identificazione delle vulnerabilità che potrebbero interessare i sistemi presenti all'interno dell'organizzazione. Una volta note le vulnerabilità che potrebbero avere un impatto sui sistemi aziendali è possibile identificare quali di queste sono effettivamente presenti.



Questa fase utilizza informazioni di intelligence sulle minacce e database di vulnerabilità per guidare la ricerca. Spesso include anche l'uso di scanner di vulnerabilità per identificare i componenti interessati e creare un inventario da utilizzare nella gestione delle patch.

L'obiettivo di questa fase dovrebbe essere quello di creare una mappa completa dell'infrastruttura IT che specifichi dove si trovano le risorse, come è possibile accedere a tali risorse e quali sistemi sono attualmente utilizzati per la protezione. Questa mappa può quindi essere utilizzata per guidare l'analisi delle vulnerabilità e facilitare la loro risoluzione.

2. Valutare le vulnerabilità

Dopo aver identificato tutte le possibili vulnerabilità nel sistema, è possibile iniziare a valutare la gravità delle minacce. Questa valutazione aiuta a determinare quali debbano essere le priorità dei programmi di sicurezza e può aiutare a ridurre i rischi più velocemente.

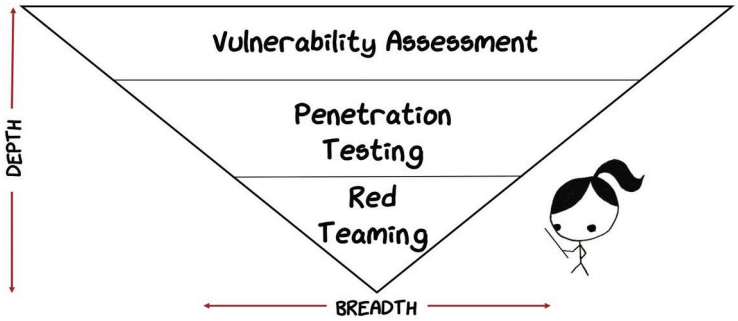
CVSS 3.0 Metric Categories

Correggendo prima le vulnerabilità più gravi si riduce la possibilità che si verifichi un attacco e contestualmente si migliora la capacità di protezione degli altri componenti dell'infrastruttura IT. Esistono diversi sistemi che è possibile utilizzare per stabilire il rischio che una vulnerabilità venga sfruttata.

Un sistema è il Common Vulnerability Scoring System (CVSS), un sistema standardizzato utilizzato da molti database e ricercatori di vulnerabilità. Il CVSS valuta il livello di vulnerabilità in base alle caratteristiche intrinseche, ai tratti temporali e all'effetto specifico della vulnerabilità sui diversi sistemi. Il problema con CVSS è che una volta assegnato un livello di rischio, questo non cambia; quindi, è importante includere nella valutazione del rischio altri fattori, come ad esempio informazioni di intelligence sulle minacce e informazioni specifiche sui rischi aziendali per determinare la corretta priorità.

3. Risoluzione delle vulnerabilità

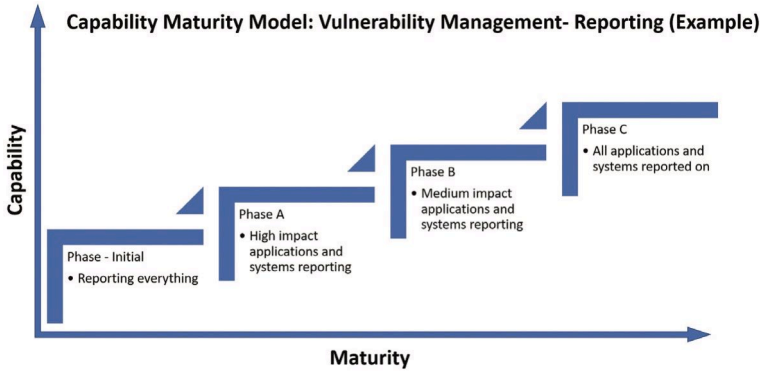
Con un piano di gestione delle vulnerabilità prioritario in atto, è possibile iniziare le attività di risoluzione. Durante questa fase, potrebbe essere necessario aumentare il monitoraggio o ridurre l'accesso alle aree identificate come a rischio. Ciò può aiutare a prevenire lo sfruttamento efficace delle vulnerabilità finché non è possibile applicare patch o aumentare in modo permanente le protezioni.



Dopo che le vulnerabilità sono state risolte, è necessario verificare l'esito positivo della correzione. I Penetration Test sono utili in questo caso per valutare opportunamente l'efficacia delle attività di correzione eseguite. Sono inoltre utili per garantire che non siano state create nuove vulnerabilità durante le attività di risoluzione.

4. Segnalazione delle vulnerabilità

La segnalazione delle vulnerabilità dopo la risoluzione delle stesse può sembrare superflua, ma in realtà aiuta a migliorare la sicurezza e le risposte agli attacchi futuri. Avere un registro delle vulnerabilità e informazioni in



merito a quando tali problemi sono stati risolti mostra la responsabilità dell'organizzazione in merito a tematiche di sicurezza ed è richiesto da molti standard di conformità.

Avere registrazioni delle vulnerabilità può essere utile anche quando si indaga su eventi futuri. Ad esempio, partendo dalle lezioni apprese nella gestione delle vulnerabilità, può evitare l'inclusione di nuove vulnerabilità in progetti di ampliamento dell'infrastruttura IT e ridurre così la superficie d'attacco.

Creazione di programmi di gestione delle vulnerabilità efficaci

Lo sviluppo di un efficace programma di gestione delle vulnerabilità può richiedere del tempo ed è un processo in continua evoluzione. Le seguenti best practice per la gestione delle vulnerabilità possono aiutare a creare un

programma solido fin dall'inizio e a ridurre il numero di perfezionamenti necessari per renderlo efficace.

Eseguire regolarmente Penetration Test

Uno dei modi migliori per garantire che nuove vulnerabilità non vengano incluse nei sistemi IT è eseguire regolarmente dei Penetration Test. Questi test, a condizione di utilizzare tecniche e strumenti aggiornati, garantiscono che le vulnerabilità scoperte di recente vengano identificate e risolte rapidamente.

I Penetration Test possono anche aiutare i team di sicurezza a comprendere meglio come operano gli aggressori e fornire una visione obiettiva della posture di sicurezza dell'organizzazione. Ciò fornisce ai team di sicurezza una base realistica per identificare dove è necessario dedicare maggiori risorse e può aiutarli a rispondere agli attacchi in modo più efficace.

Avere visibilità delle risorse e dei sistemi IT

Durante la fase di identificazione e test, è fondamentale avere visibilità di tutti gli asset e componenti IT dell'infrastruttura aziendale. In caso contrario, è molto probabile che alcune vulnerabilità non vengano identificate e opportunamente gestite.

La disponibilità di un inventario completo degli asset IT aiuta anche a "pulire casa". Quando si crea questo tipo di inventario, è probabile che si scoprano applicazioni e dati legacy che non sono più necessari e l'eliminazione delle stesse migliora la gestione della sicurezza e probabilmente anche le prestazioni dei sistemi.

La creazione di un inventario IT può essere difficile da ottenere attraverso l'esecuzione di semplici scansioni di rete, poiché ad esempio risorse come laptop e dispositivi mobili spesso risiedono fuori rete, specialmente a seguito della pandemia Covid 19. Assicurarsi di disporre degli strumenti corretti per individuare e valutare queste risorse è fondamentale per ridurre il rischio di vulnerabilità.

Utilizzare l'intelligence sulle minacce

Sapere quali vulnerabilità esistono, come vengono sfruttate tali vulnerabilità e quali opzioni di rimedio sono disponibili è fondamentale. Per ottenere tale risultato l'opzione migliore è utilizzare l'intelligence già esistente nelle comunità di sicurezza.

I forum e i database di feed di intelligence sulle minacce possono fornire una vasta gamma di informazioni e best practice. Queste fonti sono particolarmente utili per fornire competenze specifiche che altrimenti potrebbero mancare nei piccoli team di sicurezza.

Visualizzare i dati di vulnerabilità per l'awareness

Non è possibile eliminare tutte le vulnerabilità dei diversi sistemi aziendali, ma è possibile ridurre al minimo i rischi. Ad esempio, per le vulnerabilità create dagli utenti non è possibile eliminare semplicemente le autorizzazioni utente, ma è possibile educare gli utenti a identificare, ridurre e segnalare i rischi.

Un metodo per farlo è creare visualizzazioni dei dati di vulnerabilità. Questo può aiutare gli utenti a capire da dove provengono le vulnerabilità e come evitare questi rischi. Può anche aiutare a stabilire l'importanza della mitigazione dei rischi e la posta in gioco in caso di violazione dei sistemi.

La gestione delle vulnerabilità non è sempre facile come scansionare, applicare patch e convalidare. L'applicazione di patch ai sistemi critici può influire sui tempi di attività del sistema, soprattutto se è necessario un riavvio. Inoltre, alcuni tipi di dispositivi connessi possono funzionare solo con software in esecuzione su sistemi operativi obsoleti per i quali le patch non sono più disponibili. Dovranno essere messe in atto misure di sicurezza secondarie per proteggere tali sistemi dagli exploit se le patch non possono essere applicate in modo tempestivo a causa dell'impatto aziendale o della necessità.

Utilizzo dei dati di gestione delle vulnerabilità con un SIEM di nuova generazione

I dati dei log di gestione delle vulnerabilità hanno un grande valore se combinati con i log di sicurezza e di rete e analizzati in un SIEM di nuova generazione, come Exabeam Security Management Platform:

- Le risorse critiche che sono vulnerabili ma attualmente non possono essere riparate possono essere aggiunte a un elenco di controllo (watchlist), fornendo ai team di sicurezza una visione chiara di eventuali attività rischiose che si verificano su quei sistemi.
- I dati delle scansioni di vulnerabilità possono essere inclusi in Exabeam Smart Timelines, fornendo in maniera automatizzata agli analisti una vista end-to-end degli eventi.
- Le informazioni sui dispositivi possono essere arricchite con i dati di intelligence sulle minacce di Exabeam, consentendo ai team di sicurezza di comprendere indicatori di minacce esterne specifici relativi al loro ambiente.

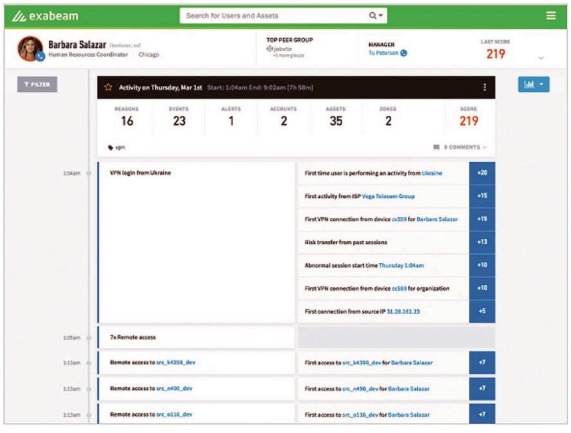
I seguenti moduli e funzionalità Exabeam possono essere utilizzati per analizzare e arricchire i dati raccolti dagli strumenti di gestione delle vulnerabilità:

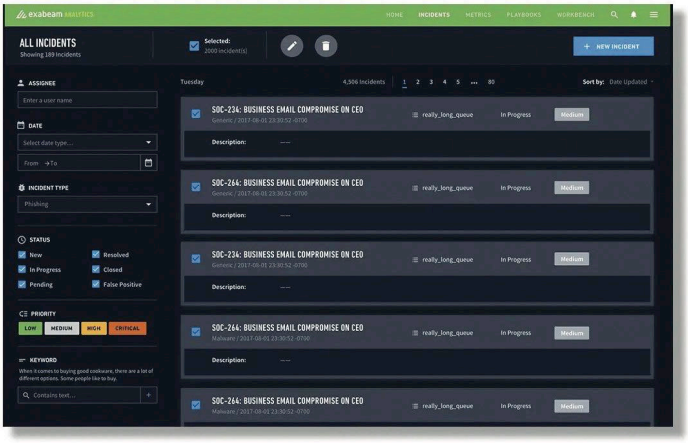
- **Advanced Analytics:** utilizzo dell'analisi comportamentale per identificare comportamenti anomali che potrebbero indicare un attacco e correlazione con i dati dell'analisi delle minacce per identificare il tipo e l'origine dell'attacco.
- **Cloud Connectors:** possono essere utilizzati per raccogliere facilmente dati da una serie di popolari soluzioni di gestione delle vulnerabilità basate su cloud.
- **Smart Forensic Analysis:** raccolta di tutte le informazioni rilevanti su un incidente di sicurezza, tra più utenti, indirizzi IP e sistemi IT, combinandole con i dati di intelligence sulle minacce e disponendole su una sequenza temporale associata all'incidente.
- **Incident Response Automation:** raccolta di dati da centinaia di strumenti, identificazione automatica degli incidenti, correlazione con dati di intelligence sulle minacce e orchestrazione automatica delle fasi di contenimento e mitigazione.
- **Threat Hunting:** utilizzo dei dati di intelligence sulle minacce, in combinazione con l'analisi dei dati sulla sicurezza interna, per identificare minacce nuove e sconosciute che potrebbero interessare l'organizzazione.

Oltre a questi strumenti, Exabeam offre anche un servizio di Threat Intelligence che, con tecnologia proprietaria, raccoglie e analizza gli indicatori di compromissione da più feed.

Il servizio di Threat Intelligence è gratuito per i clienti Exabeam essendo parte integrante della Security Management Platform di Exabeam e può anche integrarsi con feed di threat intelligence di terze parti per una più ampia copertura di IOC.

Ulteriori informazioni sulla piattaforma di gestione della sicurezza Exabeam: Exabeam Security Management Platform. ■





Un approccio Open Source alla gestione delle vulnerabilità.

Autore: Francesco Corona

Generalità. Ora più che mai è tempo di sdoganare infrastrutture tecnologiche e SW per la cyber security attraverso ambienti volte a proteggere la piccola e media utenza internet. Tali ambienti dovranno andare oltre le più tradizionali contromisure rappresentate da SW anti-malware. Da questo punto di vista sensori IDS/IPS/Ibridi, (IDS=Intrusion Detection; IPS=Intrusion Prevention) agenti intelligenti on-board e ambienti di monitoraggio SIEM (Security Information and Event Management) di tipo open source, quindi più flessibili ed adattivi, nonché più economici, possono essere integrati nelle reti domestiche e in quelle di piccole e medie imprese con le tradizionali misure di homeland security (allarmistica sensoriale e telecamere), quindi alla portata di tutti. Un nuovo approccio integrato in linea con le regole dell'IoT e delle Smart City. La crisi Covid-19 ha evidenziato infatti un aumento degli attacchi individuali e a piccole e medie imprese meno protette e dunque più vulnerabili delle grandi corporation. Essendo la piccola utenze sottoposta alla normativa sulla privacy GDPR oltre alle eventuali certificazioni di qualità ISO27001, nasce una immediata necessità di risolvere queste vulnerabilità con utilizzo di approcci standardizzati efficienti ed efficaci. Sarebbe auspicabile trovare la maniera di inserire i report dei vari vulnerability assessment all'interno del sistema di log management, per automatizzare il più possibile il processo di identificazione di attacchi. In effetti l'implementazione di NIST-800-53 e NIST-800-41 MITRE offrononо questa possibilità.

ID	Recommendation Description		
FBP-1	Deny *"Inbound or Outbound traffic from a system using a source address that falls within the address ranges set aside in RFC1918 as being reserved for private networks"* [67].		
	Threat	**Vulnerability**	**Countermeasure**
	$threat_{Inbound192.168.0.0/16SrcIPPkt}$	$Vul_{UnAuthenInbound192.168.0.0/16PktToFW}$	$iptr_{DropIn192.168.0.0/16SrcIPPktInputChain}$
	$threat_{Outbound192.168.0.0/16SrcIPPkt}$	$Vul_{UnAuthenOutbound192.168.0.0/16PktFromFW}$	$iptr_{DropOut192.168.0.0/16SrcIPPktOutputChain}$
	$threat_{Inbound192.168.0.0/16SrcIPPkt}$	$Vul_{UnAuthenInbound192.168.0.0/16PktToHost}$	$iptr_{DropIn192.168.0.0/16SrcIPPktForwardChain}$
	$threat_{Outbound192.168.0.0/16SrcIPPkt}$	$Vul_{UnAuthenOutbound192.168.0.0/16PktFromHost}$	$iptr_{DropOut192.168.0.0/16SrcIPPktForwardChain}$
	$threat_{Inbound10.0.0.0/8SrcIPPkt}$	$Vul_{UnAuthenInbound10.0.0.0/8PktToFW}$	$iptr_{DropIn10.0.0.0/8SrcIPPktInputChain}$
	$threat_{Outbound10.0.0.0/8SrcIPPkt}$	$Vul_{UnAuthenOutbound10.0.0.0/8PktFromFW}$	$iptr_{DropOut10.0.0.0/8SrcIPPktOutputChain}$
	$threat_{Inbound10.0.0.0/8SrcIPPkt}$	$Vul_{UnAuthenInbound10.0.0.0/8PktToHost}$	$iptr_{DropIn10.0.0.0/8SrcIPPktForwardChain}$
	$threat_{Outbound10.0.0.0/8SrcIPPkt}$	$Vul_{UnAuthenOutbound10.0.0.0/8PktFromHost}$	$iptr_{DropOut10.0.0.0/8SrcIPPktForwardChain}$
	$threat_{Inbound172.16.0.0/12SrcIPPkt}$	$Vul_{UnAuthenInbound172.16.0.0/12PktToFW}$	$iptr_{DropIn172.16.0.0/12SrcIPPktInputChain}$
	$threat_{Outbound172.16.0.0/12SrcIPPkt}$	$Vul_{UnAuthenOutbound172.16.0.0/12PktFromFW}$	$iptr_{DropOut172.16.0.0/12SrcIPPktOutputChain}$
	$threat_{Inbound172.16.0.0/12SrcIPPkt}$	$Vul_{UnAuthenInbound172.16.0.0/12PktToHost}$	$iptr_{DropIn172.16.0.0/12SrcIPPktForwardChain}$
	$threat_{Outbound172.16.0.0/12SrcIPPkt}$	$Vul_{UnAuthenOutbound172.16.0.0/12PktFromHost}$	$iptr_{DropOut172.16.0.0/12SrcIPPktForwardChain}$
ID	**Recommendation Description**		
FBP-2	Deny *"Inbound traffic containing ICMP (Internet Control Message Protocol) traffic"* [67].		
	Threat	**Vulnerability**	**Countermeasure**
	$threat_{ICMPNetworkScan}$	$Vul_{InfoDisclosureICMPReplyPktFromFW}$	$iptr_{DropInICMPPktInputChain}$
	$threat_{ICMPNetworkScan}$	$Vul_{InfoDisclosureICMPReplyPktFromHost}$	$iptr_{DropInICMPPktForwardChain}$

Table 1: Semantic Threat Graphs Extract for NIST-800-41: Guidelines on Firewalls and Firewall Policy.

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

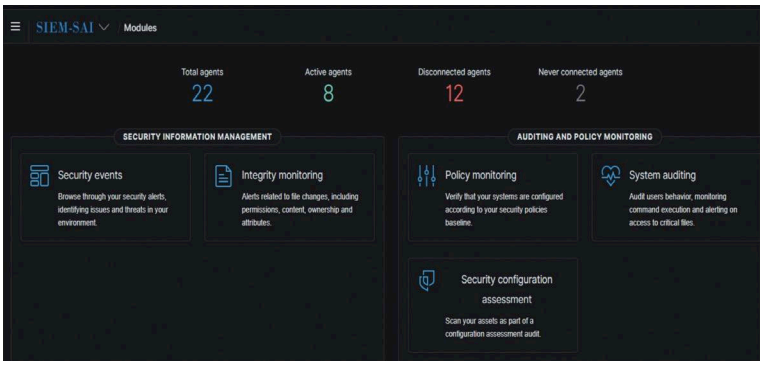
Le parti fondamentali di questa architettura che potrebbe anche afferire a un SOC (Security Operational Center) prevedono:

- **Un Event Manager**
- **Un Correlation Manager con eventuali sistemi interni di E-learning per allertamento preventivo**
- **Un ambiente di Datafusion , Data Analysis**
- **Un CMDB** – (Configuration Management Data Base)
- **Un Ticketing System**
- **Un Workflow Manager and OPSs** – ovvero un Incident Manager dotato di un Sistema di allertamento rapido con un Operational Procedure Steps (OPSs)
- **Un cruscotto con grafica avanzata e reportistica.**

Normalmente i SIEM hanno metodi predefiniti per il collezionamento, il filtraggio, l'aggregazione e la normalizzazione di log di particolari sistemi o applicazioni (per esempio, server web, database relazionali, mail server, ecc.). In tali casi il SIEM sa come interpretare i vari campi presenti nel log originario (per esempio il campo numero 12 rappresenta l'IP sorgente) o determinati valori presenti nel log originario (per esempio l'evento con codice 680 in un sistema Windows rappresenta un'autenticazione fallita). Per sistemi o applicazioni che non dispongono di metodi predefiniti, i SIEM forniscono normalmente strumenti che permettono di costruirsi gli schemi più appropriati, rendendo il sistema molto più flessibile ed adattivo rispetto agli asset da proteggere. La generazione degli eventi avviene all'interno dei sistemi e delle applicazioni di cui si vogliono raccogliere i log da far pervenire al SIEM. Possono essere considerate due diverse famiglie di eventi generati:

1. I generatori di dati basati su eventi (sensori) che generano eventi corrispondenti a specifiche operazioni svolte da sistemi operativi, applicazioni, dispositivi di sicurezza e così via sulla rete.
2. I generatori di dati basati sullo stato (polling), generano eventi basati sulla reazione a stimoli esterni ad esempio dati relativi a check di integrità o demons che hanno il compito di verificare lo stato di un certo servizio.

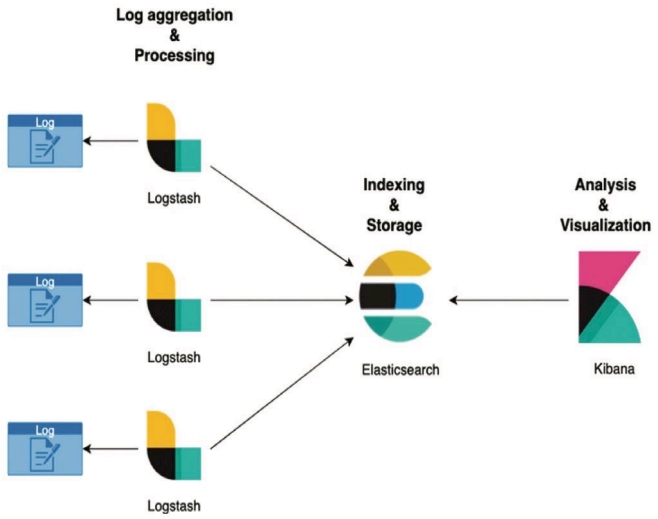
Strategia di gestione dei Log. Il server SIEM può anche riceve i log dagli asset senza bisogno di installare un software particolare (agentless). Alcuni SIEM hanno la possibilità di iniziare la connessione con il sistema sorgente, utilizzando opportuni meccanismi di autenticazione per andare a reperire ad intervalli regolari i log presenti, per esempio disponibili in un database o in un file di testo; si parla in tal caso di metodi pull. In altri casi i sistemi sorgente inviano loro stessi i log al SIEM, dove è presente un opportuno receiver in tal caso si parla di metodo push. Esempio di questo tipo di metodo è il Syslog. In una infrastruttura di log management basata sul modello Syslog, ogni sorgente produce log dello stesso formato (con lo stesso orario sincronizzato tramite orologio atomico) ed utilizza lo stesso meccanismo per trasferire i log a un server Syslog remoto. Syslog fornisce un semplice framework per la generazione, lo storage e il trasferimento dei log, che ogni asset sia esso sistema operativo, software di sicurezza o applicazione può utilizzare. Molte sorgenti di log usano Syslog come formato nativo oppure offrono la possibilità di convertire i log dal loro formato nativo a Syslog. Lo standard Syslog consente di operare una classificazione del messaggio, al fine di stabilirne la tipologia e la priorità, basandosi su due attributi: la facility e la severity. La facility rappresenta la tipologia del messaggio, per esempio messaggio del kernel, messaggio di autorizzazione, di sicurezza, applicativo. La severity può assumere un valore compreso fra 0 (emergency) e 7 (debug).



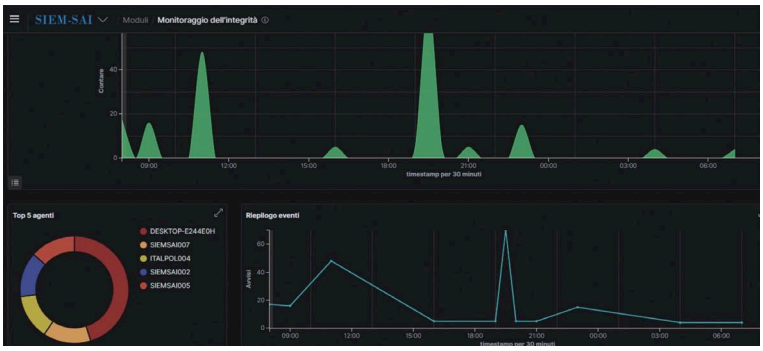
Dash Board di un generico SIEM Open Source.

Una corretta strategia di Log Management prevederà i seguenti 4 punti:

1. **Centralizzare nel sistema di log management tutti gli eventi rilevanti.** Una volta definiti gli eventi rilevanti per la propria organizzazione, occorre far sì che tali eventi siano registrati all'interno di un sistema centralizzato, dopo averli sottoposti a filtraggio, aggregazione e normalizzazione. Solo gli eventi provenienti dai sistemi giudicati rilevanti debbono essere raccolti.
2. **Definire l'ambito di applicazione.** Occorre documentare quali sono i sistemi rilevanti ai fini del monitoraggio della sicurezza o del rispetto alle normative. Occorre definire quali sono le reti e gli asset interni che fanno parte di una rete protetta. Occorre, infine, produrre un documento che definisca dove sono registrati gli eventi e il periodo di conservazione per ogni tipologia di log.
3. **Revisione tempestiva dei log.** È necessario definire quali sono gli eventi di interesse ovvero gli eventi che possono costituire una minaccia, tenendo conto che, dei centinaia di migliaia di log prodotti giornalmente, meno dell'1% rappresenta una minaccia. Occorre definire dei Service Level Agreement (SLA) e delle Standard Operating Procedures (SOPs) per ogni tipo di evento di interesse, stabilendo l'intervallo di tempo affinché l'evento venga evidenziato con una procedura da seguire per ogni evento di interesse. Occorre infine schedulare la produzione di report degli eventi chiave dei dispositivi di sicurezza.
4. **Creare un percorso di audit degli eventi di interesse.** Occorre mantenere un percorso di audit sicuro per provare come gli eventi di interesse siano stati gestiti e risolti. Documentare poi come ogni evento di interesse sia stato gestito attraverso le SOPs rispettando gli SLA.



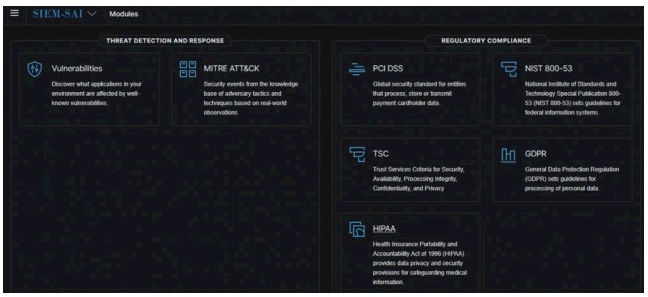
Reporting avanzato. Attraverso strumenti quali Kibana ed Elastic Search è possibile correlare ed interpetare i dati rilevati dai sensori in modo semplice ed efficace. Kibana è un'applicazione frontend gratuita e aperta che si trova sopra lo stack Elastic Stack, fornendo funzionalità di ricerca e visualizzazione dei dati per dati indicizzati. Comunemente noto come strumento di creazione di grafici (già denominato ELK=Elasticsearch - Logstash - Kibana), Kibana funge da interfaccia utente per il monitoraggio, la gestione e la protezione di un cluster Elastic Stack, nonché da hub centralizzato per soluzioni integrate sviluppate per lo Stack. Pensato nel 2013 all'interno della community Elasticsearch, Kibana è cresciuto fino a diventare l'interfaccia dello Stack stesso, offrendo un portale per utenti ed applicazioni di grande potenza rappresentativa e velocità.



Esempio di grafici Kibana per l'Integrity Monitoring di un generico SIEM

Analisi del rischi. Tutti gli standard di riferimento implementati in un SIEM afferiscono ad una analoga strategia di Risk Management anche se con differenti approcci dipendenti dalle differenti metodologie e standard di riferimento(ISO31000,ISO27001,COBIT, ITIL, COSO ecc.). Indicativamente una gestione ed analisi dei rischi può essere assimilata alle seguenti 4 fasi fondamentali:

- identificazione o classificazione degli asset da proteggere;
- identificazione delle minacce a cui sono soggetti gli asset;
- identificazione delle vulnerabilità;
- stima delle probabilità di sfruttamento;
- valutazione del rischio.



Moduli di un generico SIEM open source.

Regulatory Compliance. Un SIEM orientato al mercato e alla piccola utenza dovrà soddisfare delle complience ad ampio spettro verso NIST 800-53, PCI DSS, TSC, HIPAA, GDPR, che andremo ad esplicitare di seguito.

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

TSC. In ottica SOC-SIEM (SOC=Security Operational Center), nei così detti Trust Services Criteria (TSC) dell'AICPA. I SOC Response Team devono disporre di tutti i controlli applicabili ed essere in grado di fornire tempestivamente prove dell'efficacia di tali controlli. I criteri per i servizi fiduciari (TSC) necessari ad ottenere la certificazione SOC 2 e quindi soddisfare i più recenti standard del framework, sono relativi a controlli che le

organizzazioni devono implementare nell'infrastruttura IT. Le cinque categorie di criteri di controllo sono riportate in figura. Va da sè che uno strumento come il SIEM, in grado di supportare tali controlli, faciliterà l'approccio ad un SOC certificato anche e soprattutto in ottica CLOUD.

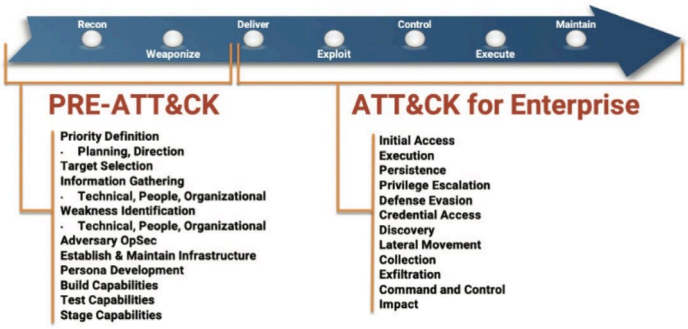
HIPAA. L'Health Insurance Portability and Accountability Act (HIPAA) è una legge federale degli Stati Uniti che definisce i requisiti per il trattamento dei dati sanitari protetti dei privati. La compliance HIPAA è regolamentata dall'HHS (Department of Health and Human Services) e l'OCR (Office for Civil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

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

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

MITRE FRAMEWORK

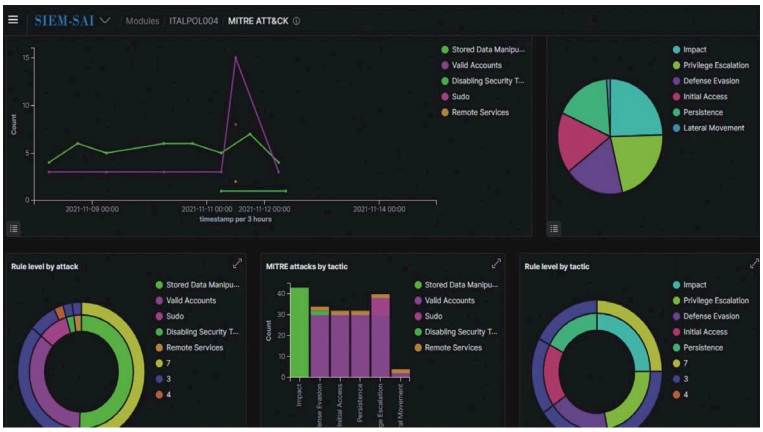
Considerata una tipica Cybersecurity Kill Chain il framework MITRE, originariamente pensato con due ambienti fondamentali: PRE-ATT&CK e ATT&CK come mostrato in figura, ha recentemente subito alcune modifiche.



PRE-ATT&CK offriva inizialmente ai difensori la possibilità di rispondere a domande come: Ci sono segni di cosa un attaccante potrebbe prendere di mira? Quali tecniche comunemente usate usa l'attaccante contro di te? In che modo dovresti dare la priorità alle acquisizioni e all'analisi dei dati di intelligence sulle minacce cyber per ottenere ulteriori informazioni per «percepire» l'attaccante prima che si verifichi l'exploit?

Il 27 ottobre 2020, MITRE ha pubblicato ATT&CK v8. Questa versione rimuove il dominio PRE-ATT&CK dalla chain ATT&CK, sostituendo il suo ambito con due nuove tattiche in Enterprise ATT&CK Reconnaissance e Resource Development (vedi figura MITRE Tecniche e Tattiche). È stata inoltre aggiunta una nuova piattaforma in cui si testano queste tecniche.

ATT&CK MITRE ha suddiviso infatti ATT&CK in diverse matrici: enterprise, mobile e PRE-ATT&CK che viene evidenziato internamente appunto come matrice. Ogni matrice include strategie e tattiche diverse pertinenti all'argomento della matrice. La matrice ATT&CK for Enterprises ad esempio descrive cosa fa normalmente un utente malintenzionato quando si infiltra in una rete aziendale. Le informazioni raccolte durante un attacco sono presentate sotto forma matriciali alle quali si accede ad informazioni estese sulle **Tattiche, Tecniche** e **Procedure** dell'attaccante. La struttura di ATT&CK consiste in 14 tattiche che delineano il **"perché"** dell'approccio di un attaccante e quindi rappresentano l'obiettivo del suo attacco. Le tecniche ATT&CK sono del tipo **"come"** un avversario raggiunge un determinato obiettivo. Le procedure sono i passaggi specifici che un avversario compie per eseguire e implementare una tecnica. Queste tecniche rappresentano i vari modi in cui un cyber-attack può raggiungere obiettivi target. Questo approccio, implementato in un SIEM open source fornisce una soluzione completa e molto economica per prevenire e mitigare minacce alla sicurezza informatica.



Dash board delle minacce rispetto alle TTP MITRE registrate da un generico SIEM open source.

Combinando queste due soluzioni, le difese di un'organizzazione possono essere migliorate contrastando le azioni nemiche in tutte le fasi del ciclo di vita dell'attacco. Per ciascuna tecnica elencata nel MITRE ATT&CK, vengono fornite le seguenti informazioni:

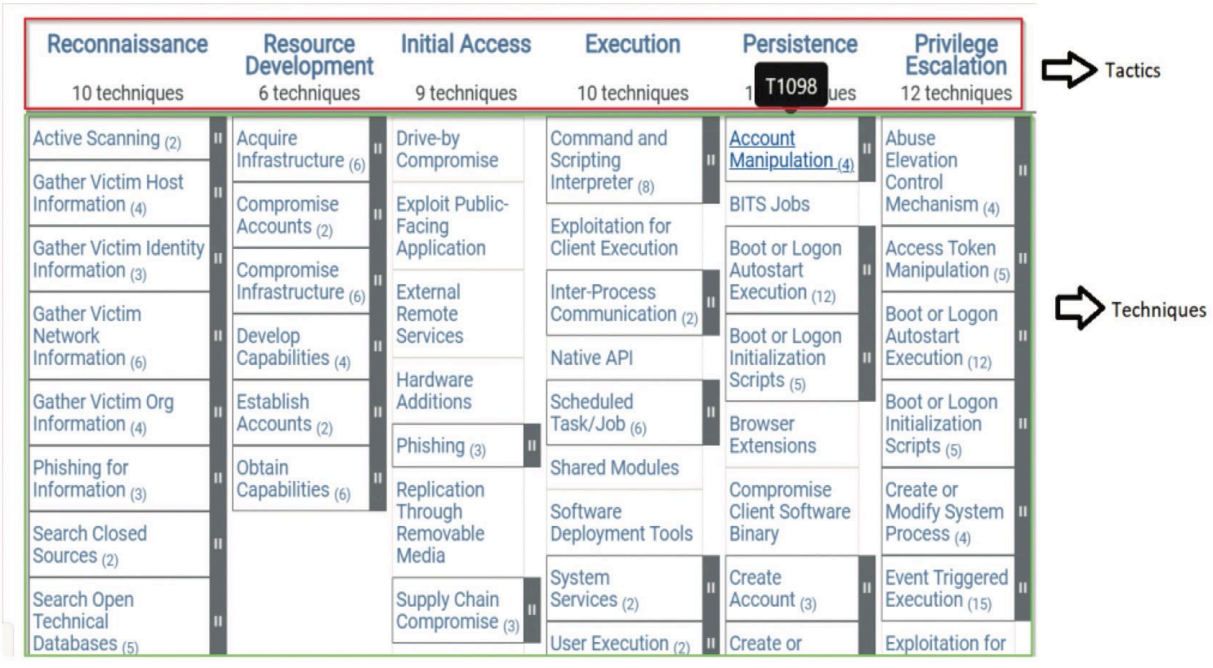
- Un identificatore e la tattica a cui è associato.
- Le fonti di dati che identificano l'uso della tecnica.
- Le mitigazioni e i metodi di rilevamento.

Le informazioni presenti nella matrice ATT&CK fanno parte di una raccolta di dati continuamente aggiornata. MITRE ha unificato le energie per includere informazioni sui crimini informatici che utilizzano determinate tecniche di attacco. Lo sviluppo delle contromisure sarà di tipo adattivo rispetto agli attacchi real time. Le informazioni fornite dal framework ATT&CK possono essere utilizzate dai team SOC per stabilire le priorità e per individuare le vulnerabilità nelle misure strategiche. Le tecniche, le tattiche e le procedure ATT&CK possono quindi essere utilizzate per dare priorità alla mitigazione delle minacce e scoprire le lacune nella sicurezza di una organizzazione.

Mappatura di intelligence delle minacce. L'elenco organizzato ed accessibile dei TTP registrate degli attaccanti è una guida preziosissima per studiare le minacce da parte dei team SOC all'interno di un SIEM. Nell'ipotesi che l'attività potenziale di un aggressore sia predittiva sulla base di TTP precedentemente sperimentate, è utile per tutti i team di difesa ed analisi delle minacce registrare queste informazioni in modo strutturato (compresi i dettagli di supporto). Oltre alle informazioni su come identificare, rilevare e mitigare la tecnica, viene anche fornita una descrizione esaustiva di ciascuna tecnica rilevata. È inoltre possibile illustrare le lacune di esposizione rimuovendo a livello di codice le informazioni dal database per tecniche di interesse forense. ATT&CK aiuta de facto ad avere una visione più approfondita della capacità difensiva dell'organizzazione. Le procedure e le tattiche di ATT&CK osservate o rilevate possono essere utilizzate dal Security Operations Center (SOC) e dall'unità di Incident Response. Ciò consente di spiegare dove si trovano le capacità di difesa e gli errori rilevati e fornisce inoltre una convalida dei controlli per la prevenzione e l'identificazione della minaccia.

Quando si fa riferimento alle tecniche ATT&CK, i controlli difensivi possono avere un significato ben noto. La mappatura delle difese ATT&CK offre una roadmap delle vulnerabilità difensive in riferimento a tipologie di attacco precedentemente registrate. Diversi strumenti e risorse standardizzano le tattiche e le tecniche per una sicurezza coesa ed inclusiva. I difensori potranno quindi mantenere una maggiore consapevolezza condivisa durante il processo di Information Sharing associato.

Sonde IDS/IPS. Concludiamo questo articolo facendo notare che sonde molto economiche di tipo open source basate su Raspberry PI OS carrozzate con tecnologia IDS/IPS (ad esempio Suricata) sono molto efficienti per la risoluzione di vulnerabilità in reti domestiche e reti afferenti a piccole e medie imprese. Possono quindi assumere differenti configurazioni di rete e trasmettere attraverso API con il SIEM open source per il rispetto delle normative sulla protezione dei dati e sulle certificazioni di qualità e gestione di rischi. ■



MITRE Tecniche e Tattiche in ciascun step della kill chain.

Contromisure e controlli per contrastare le vulnerabilità.

Autore: Giancarlo Butti

Nella gestione dei rischi per contrastare le vulnerabilità è necessario individuare opportuni controlli di sicurezza la cui selezione e gestione richiede un'attenta valutazione per ottimizzare il rapporto costi/benefici[1].

Nell'ambito della gestione dei rischi una vulnerabilità non può essere intesa solo come una caratteristica intrinseca di un componente informatico.

Nel senso più ampio del termine[2] può essere rappresentato da molteplici fattori, ad esempio l'assenza di qualcosa (si vedano al riguardo le tabb. 1, 2 e la fig. 3).

La correlazione fra vulnerabilità e rischio è ben espressa dalle immagini che seguono tratte dall'Australian Standard Handbook of Information Security Management e dall' ISO/IEC 15408-1 Common Criteria.

Dalle immagini appare evidente come il rischio sia legato alla possibilità che una minaccia, sfruttando una vulnerabilità, produca un danno. Sempre dalle immagini si evidenzia che per contrastare le minacce e le vulnerabilità e ridurre quindi i rischi si interviene adottando apposite contromisure (o security control).

È interessante notare il diverso approccio utilizzato nei due documenti:

- nella norma ISO la contromisura ha effetti sulla vulnerabilità
- nell'altro documento i controlli di sicurezza hanno effetti sulla minaccia.

In effetti la classificazione dei controlli/contromisure può avvenire secondo logiche e approcci diversi.

Ad esempio per finalità:

- riduzione delle probabilità di accadimento
- limitazione dell'impatto.

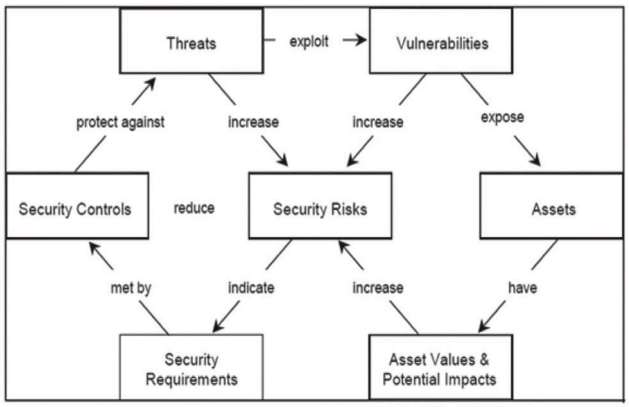


Fig. 1 - Relazione dei componenti del rischio secondo la **Australian Standard Handbook of Information Security Management**

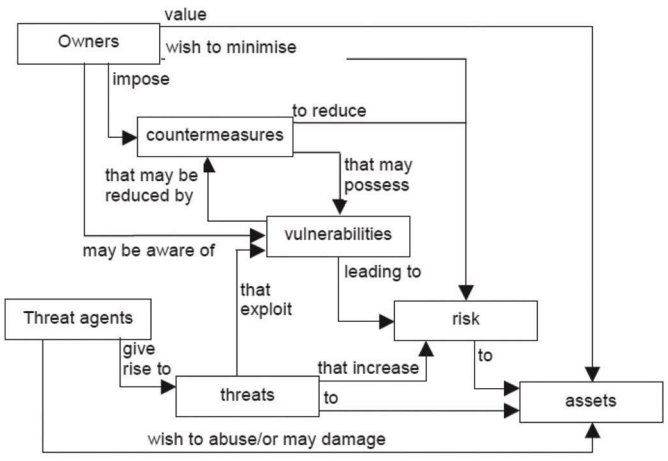


Fig. 3 – Relazione dei componenti del rischio secondo la **ISO/IEC 15408-1 Common Criteria**

Nel primo caso la misura di sicurezza rende meno frequente la possibilità che l'evento accada (o che accadendo provochi un danno[3]), mentre nel secondo caso consente di limitare l'impatto (parliamo genericamente di impatto, ma in realtà gli impatti sono molteplici, diretti, indiretti, consequenziali…):

- se si utilizzano dischi in RAID si riducono le probabilità del blocco di un server
- se si dispone di copie aggiornate di dati, di immagini dei dischi, di un contratto di assistenza con intervento immediato si riduce l'impatto.

Per momento di attuazione:

- preventive (evitare / prevenire)
- successive (ripristinare / recuperare)

in funzione del fatto che siano applicate per prevenire l'accadimento di un evento, oppure per porvi rimedio:

- come azione preventiva; se ad esempio si utilizzano dischi in RAID o componenti ridondati in un server, si riduce la possibilità di perdita di dati o di interruzione di un servizio in seguito alla rottura o guasto di un componente
- come azione successiva di recupero o ripristino della disponibilità; grazie all'utilizzo di copie aggiornate di dati, di immagini dei dischi, di un contratto di assistenza con intervento immediato, si riduce l'impatto derivante dalla perdita di dati o dal fermo di un servizio, permettendone il ripristino in tempi rapidi e senza perdita di informazioni (permangono ovviamente le perdite derivanti dai costi di ripristino e dal fermo del servizio).

La scelta di quali controlli[4] implementare è condizionata da numerosi fattori; l'analisi del rischio consente di avere una stima della priorità degli interventi e dell'importanza degli stessi.

CARENZE ORGANIZZATIVE
Mancata regolamentazione a vari livelli
Mancata definizione dei ruoli
Mancanza di procedure, policy…
Mancata identificazione del valore delle risorse
Mancata identificazione dei rischi
Mancata identificazione ed implementazione di adeguate contromisure
Mancata definizione dei controlli e del processo di gestione degli stessi
Mancata definizione della responsabilità dei controlli

Tabella 1: Stralcio della tabella delle vulnerabilità tratto da: **SICUREZZA TOTALE 4.0 - L'ABC sulla physical cyber security per i DPO (e non solo)**

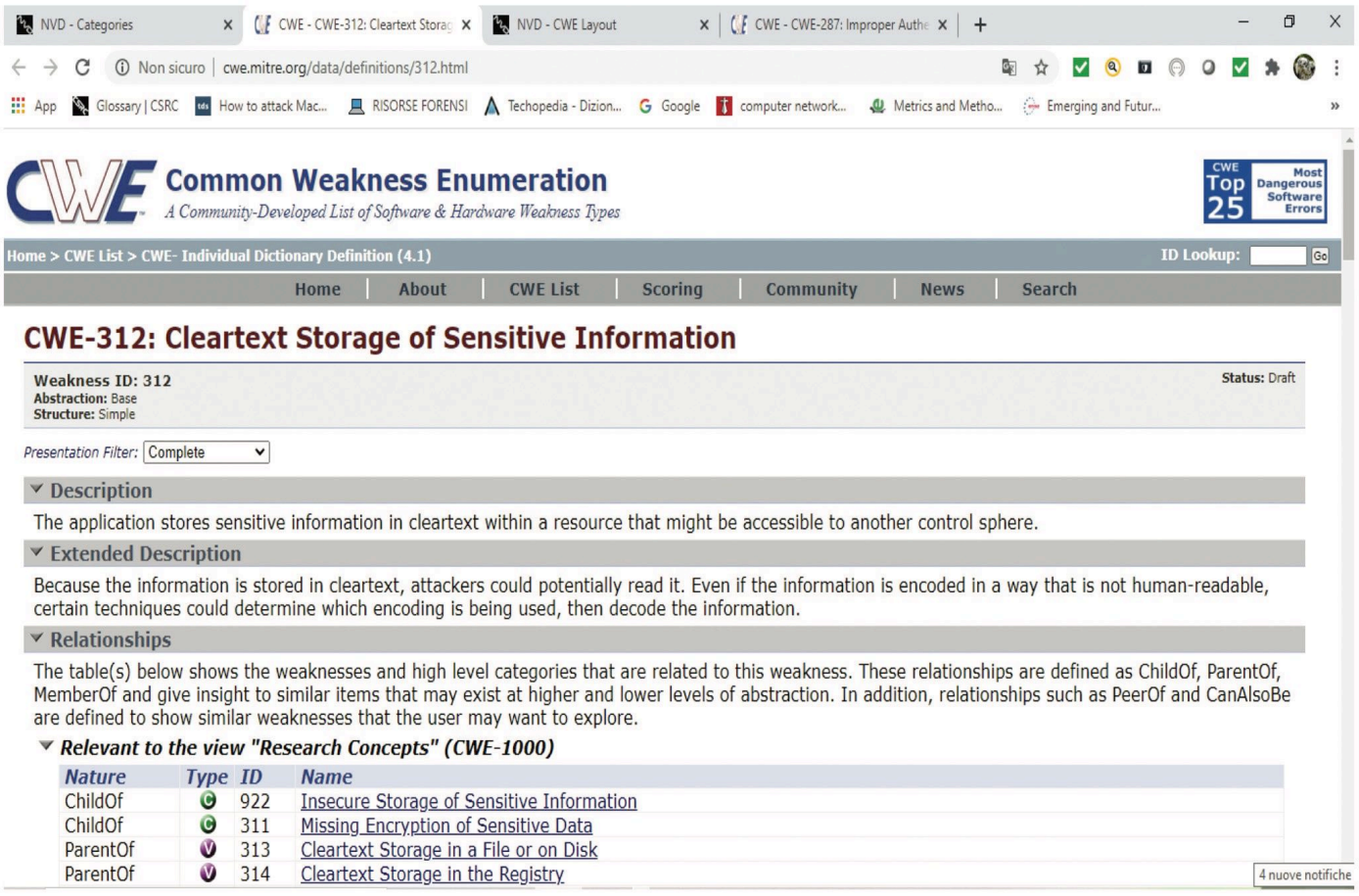


Fig. 3 - Uno dei numerosi database di vulnerabilità disponibili on line

Vulnerability	Threat	Asset Type
Lack of policies in respect of dial up access, modem use, and software use	Unauthorised Dial-in Access	Data
Lack of policy requiring all enquires for information to be withheld until the identity of the requestor can be verified	Social Engineering	Software Data
Lack of policy restricting staff to use of licensed software	Use of Pirated Software	Software
Lack of policy restricting the provision of information by staff over the phone	Social Engineering	Software Data
Lack of proof of receiving a message	Misrouting/re-routing of messages	Data
Lack of proof of sending or receiving a message	Repudiation	Data
Lack of redundancy and back-ups	Failure of communications services	Data
Lack of regular update of Anti virus software	Malicious Code	Software Data
Lack of software auditing	Use of Pirated Software	Software
Lack of Software Change Management policies and procedures	Unauthorised Software Changes	Software Data

Tab 2 – Stralcio della tabella dedicate alle vulnerabilità tratta da **Information Security Guideline for NSW Government - Part 2 Examples of Threats and Vulnerabilities**

Considerando che i budget sono limitati sarà necessario concentrare la propria attenzione:

- dove il rischio è maggiore
- dove interventi dal costo contenuto possano risolvere situazioni di minore entità.

Per far questo è necessario valutare:

- il costo di una contromisura
- il rapporto costo/benefici
- il rischio residuo, considerando la contromisura in essere
- come gestire il rischio residuo.

Nella valutazione di una contromisura vanno considerati i costi di:

- acquisizione
- implementazione
- gestione
- formazione
- revisione periodica
- ….

Non vanno tuttavia dimenticati altri aspetti altrettanto importanti, solitamente trascurati almeno dal punto di vista economico, ma che possono tradursi in ulteriori costi.

Una contromisura potrebbe infatti avere degli impatti negativi su altri parametri di funzionamento, ad esempio, di un sistema informativo; potrebbe infatti comportare, ad esempio, dei rallentamenti o dei malfunzionamenti di un'applicazione.

Questi aspetti vanno quindi considerati e valorizzati.

Se ad esempio una contromisura genera dei rallentamenti in quanto consuma risorse del sistema, si dovranno accettare un degrado dei servizi (e sarebbe opportuno valutarne il costo in termini di riduzione di produttività) o sarà necessario aumentare le prestazioni del sistema tramite opportuni interventi tecnici, che ovviamente hanno un costo.

L'esempio effettuato non è casuale.

Quando si parla di analisi del rischio del punto informatico e delle relative vulnerabilità si tende a pensare solo agli aspetti di sicurezza (e di fatto viene effettuata dalle strutture che si occupano di sicurezza informatica).

In realtà sarebbe più corretto parlare di rischio informatico in generale; una minaccia sfruttando una vulnerabilità potrebbe infatti portare, come nell'esempio precedente, al rallentamento del sistema, senza avere impatti sulla sicurezza.

Il tema degli impatti operativi e non solo di sicurezza del resto ha portato l'UE a inserire nella PSD2[5] l'obbligo di notifica sia degli incidenti di sicurezza sia di quelli operativi[6].

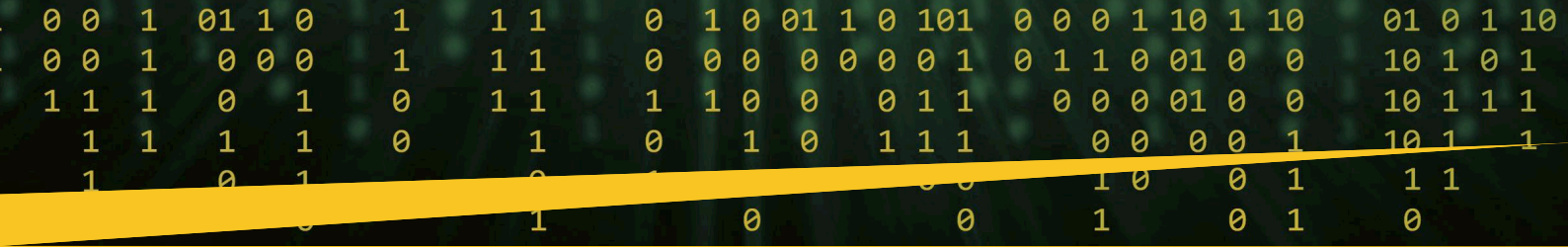
Per valutare quali controlli implementare un'analisi puntuale asset per asset può non essere una buona idea; è infatti probabile che la stessa tipologia di asset sia soggetta alle stesse minacce e vulnerabilità e che anche gli impatti indiretti e consequenziali siano i medesimi. È quindi possibile raggrupparli per classe salvo che la correlazione fra asset non suggerisca un approccio diverso.

Analogamente una stessa misura di sicurezza può avere effetti su numerosi asset; la sua valutazione in termini di costi/benefici deve quindi tener conto anche di questi aspetti.

Ad esempio, se si applicano ad uno specifico locale misure di sicurezza per limitare il rischio di furto di un asset critico in esso contenuto, tale intervento preserverà anche tutti gli altri asset contenuti nel locale.

Per ottimizzare i costi preventivati si potranno collocare tutti gli asset critici nel locale protetto; in questo modo un rapporto costi/benefici negativo nel caso di un solo asset, potrebbe diventare positivo.

Nell'effettuare tale operazione è però necessario valutare anche possibili aspetti negativi; se si raccolgono in un unico locale tutti gli asset critici dell'azienda per proteggerli dal furto, ma non si valutano altri rischi, quali ad esempio quello di distruzione in seguito ad un incendio, si è commesso un grave errore.



A chi non è mai capitato di vedere ordinatamente allineate flotte di mezzi pesanti sul parcheggio di un'azienda?

Il loro raggruppamento consente sicuramente una più facile sorveglianza, ma nel caso in cui un mezzo prenda fuoco sarà difficile che anche gli altri automezzi non siano coinvolti nell'incendio.

La valutazione dell'adeguatezza di una contromisura è quindi un processo complesso che deve prendere in considerazione numerosi fattori e correlazioni e che richiede:

- a priori una valutazione di quale sarà l'effettiva riduzione del rischio
- a posteriori, una verifica della sua efficacia.

Per quanto riguarda il primo aspetto i parametri da considerare sono molteplici, in funzione della complessità della metodologia di analisi del rischio adottata.

L'effetto di un controllo viene misurato solitamente effettuando una nuova analisi dei rischi considerando implementato il controllo stesso, attraverso stime che considerando di quanto possa ridurre la probabilità (le probabilità) o l'impatto (gli impatti).

Va anche considerato che la decisione di implementare una misura di sicurezza non si limita alla sua implementazione, ma richiede la definizione di un processo di gestione. Tutti elementi che introducono elementi di incertezza che possono vanificare l'iniziale efficacia valutata per il controllo stesso.

Consideriamo ad esempio il caso di un antifurto.

La decisione della sua implementazione deriva da un'analisi dei rischi (non necessariamente formalizzata) che ha evidenziato come sia opportuno attivare questa misura di sicurezza a tutela di uno o più asset aziendali.

La scelta del tipo di soluzione può essere vincolata da aspetti tecnici (posizionamento, interazione con altre misure di sicurezza già in essere…), economici (favorevole rapporto costi/benefici), normativi; è inoltre opportuno valutare eventuali controindicazioni.

Per l'adeguata gestione delle misure di sicurezza devono essere definite una serie di regole, in quanto le misure tecniche devono essere SEMPRE accompagnate da procedure di gestione nei vari momenti del loro ciclo di vita:

- l'attivazione dell'antifurto può essere automatica, basata ad esempio su una programmazione oraria, oppure manuale; in questo caso va definito chi deve inserire l'antifurto (ad esempio l'ultimo ad uscire dall'ufficio)
- è necessario verificare con dei controlli a campione che effettivamente tale policy aziendale sia nota ed applicata, che l'antifurto venga effettivamente inserito, che effettivamente l'antifurto funzioni
- deve essere definito quale comportamento adottare in caso di allarme, chi deve essere avvisato, come intervenire.

Tali regole si sommano a quelle di carattere più generale che rappresentano le misure di sicurezza organizzativa.

Parte delle attività manuali descritte nell'esempio potrebbe essere eliminata, riducendo il rischio di errore e la necessità di controlli, se:

- l'antifurto entra in funzione ad una certa ora e solo in caso di variazione di orario è necessario attivarlo manualmente
- il sistema è dotato di strumenti diagnostici che segnalano malfunzionamenti, eventualmente con chiamata automatica al servizio di manutenzione.

L'esempio anticipa il tema dei controlli post implementazione.

Non è sufficiente verificare che il controllo sia attivo; va verificato anche come viene gestito.

È inoltre utile definire dei parametri che possano permettere di misurare in forma oggettiva quelli che siano i risultati ottenuti tramite l'individuazione di appositi lead e lag indicator[7]; al riguardo esistono numerosi framework di riferimento, quali COBIT, Mitre (Cyber Resiliency Metric…), CIS (Controls Measures and Metrics…).

Sub-Objective: Restore functionality	
Representative Activity and Corresponding Approaches	**Possible Representative Metrics and Measures**
RE-S2-A1: Execute recovery procedures in accordance with contingency or continuity of operations plans *[Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore]*	Time between initiation of recovery procedures and completion of documented milestones in the recovery, contingency, or continuity of operations plan [MT-37] Time between event or detected circumstances which motivated recovery procedures and achievement of [minimum acceptable, target] mission MOPs [MT-20] Percentage of mission capabilities for which [minimum acceptable, target] MOPs are achieved within [minimum threshold, target] period of time since initiating event [RE-S2-A1-1] Percentage of mission-critical cyber resources which are recovered from a backup [RE-S2-A1-2] Size of gap between lost and recovered mission-critical resources (time service or connection was unavailable, number of records not recovered) [RE-S2-A1-3] Percentage of mission-essential processes and interfaces restored to predisruption state [MT-89] Length of time to reconstitute a key information asset from a backup data store [MT-184]

Tab. 3 – Stralcio della tabella dedicate agli indicatori tratta da **Mitre: Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring**

Ma come deve essere effettuata tale attività e a chi compete tale compito?

Come evidenziato in un precedente articolo[8] per avere qualche suggerimento possiamo rivolgerci ad uno dei settori più regolamentati: quello finanziario.

La Circolare 285 di Banca d'Italia dedica infatti uno specifico capitolo al sistema dei Controlli interni, fra i cui compiti vi è appunto quello di verificare l'efficacia dei controlli.

Ovviamente non si tratta esclusivamente dei controlli legati alla sicurezza del sistema informativo, in quanto la normativa presidia qualunque tipo di rischio al quale è esposto un istituto finanziario.

Tuttavia costituisce un ottimo esempio per costruire un articolato sistema di controllo che, opportunamente semplificato, può essere adattato alle varie situazioni.

Partiamo con le definizioni che la Circolare 285 da del rischio informatico[9]:

- *"rischio informatico (o ICT)": il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT). Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici;*

e delle funzioni dei controlli interni:

- *"funzioni aziendali di controllo": la funzione di conformità alle norme (compliance), la funzione di controllo dei rischi (risk management function) e la funzione di revisione interna (internal audit)*

La definizione di rischio informatico è significativa da diversi punti di vista.

Il primo è che si parla di rischio informatico e non solo, come troppo spesso accade, di sicurezza informatica.

Un'organizzazione può subire moltissimi danni in seguito a incidenti operativi o malfunzionamenti che nulla hanno a che fare sulla sicurezza e l'enfasi data solo a questo aspetto ed ai soli parametri RID (Riservatezza, Integrità, Disponibilità) nelle analisi dei rischi non solo è molto riduttivo, ma da una falsa percezione della rischiosità aziendale che si somma a tutti gli altri rischi tipici dell'analisi dei rischi[10].

Altro aspetto interessante è il considerare il rischio informatico dai vari punti di vista e quindi operativo, reputazionale e strategico.

Per quanto attiene le funzioni di controllo queste sono articolate per specializzazioni: legate ai rischi, alla conformità ed alla verifica dell'operato dei controlli (audit).

Questi ultimi sono articolati su 3 livelli:

- *controlli di linea (c.d. "controlli di primo livello"), diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture operative (ad es., controlli di tipo gerarchico, sistematici e a campione), anche attraverso unità dedicate esclusivamente a compiti di controllo che riportano ai responsabili delle strutture operative, ovvero eseguiti nell'ambito del back office; per quanto possibile, essi sono incorporati nelle procedure informatiche. Le strutture operative sono le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi; esse devono rispettare i limiti operativi loro assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi;*
- *controlli sui rischi e sulla conformità (c.d. "controlli di secondo livello"), che hanno l'obiettivo di assicurare, tra l'altro:*
  a. la corretta attuazione del processo di gestione dei rischi;
  b. il rispetto dei limiti operativi assegnati alle varie funzioni;
  c. la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione.

  Le funzioni preposte a tali controlli sono distinte da quelle produttive; esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi;
- *revisione interna (c.d. "controlli di terzo livello"), volta a individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni e del sistema informativo (ICT audit), con cadenza prefissata in relazione alla natura e all'intensità dei rischi.*

Più dettagliatamente per quanto di interesse per questo articolo, la funzione di controllo dei rischi (risk management function):

- *sviluppa e applica indicatori in grado di evidenziare situazioni di anomalia e di inefficienza dei sistemi di misurazione e controllo dei rischi;*

e nell'ambito del controllo del rischio informatico:

…sono chiaramente assegnate responsabilità in merito allo svolgimento dei seguenti compiti di controllo di secondo livello:

- *il controllo dei rischi, basato su flussi informativi continui in merito all'evoluzione del rischio informatico e sul monitoraggio dell'efficacia delle misure di protezione delle risorse ICT.*

Per quanto attiene la funzione di revisione interna i suoi compiti sono così declinati:

- *… è volta, da un lato, a controllare, in un'ottica di controlli di terzo livello, anche con verifiche in loco, il regolare andamento dell'operatività e l'evoluzione dei rischi, e, dall'altro, a valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del sistema dei controlli interni, portando all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento al RAF, al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi. Sulla base dei risultati dei propri controlli formula raccomandazioni agli organi aziendali.*
- *valuta la completezza, l'adeguatezza, la funzionalità, l'affidabilità delle altre componenti del sistema dei controlli interni, del processo di gestione dei rischi e degli altri processi aziendali, avendo riguardo anche alla capacità di*

individuare errori ed irregolarità. In tale contesto, sottopone, tra l'altro, a verifica le funzioni aziendali di controllo dei rischi e di conformità alle norme;

Inoltre:

- *verifica, anche attraverso accertamenti di natura ispettiva:*

…

g. la rimozione delle anomalie riscontrate nell'operatività e nel funzionamento dei controlli (attività di "follow-up");

…

- *effettua test periodici sul funzionamento delle procedure operative e di controllo interno;*

Esistono quindi in letteratura e sono facilmente accessibili strumenti e modelli che aiutano un'organizzazione a valutare l'efficacia dei controlli e a definire la propria struttura di controlli interni.

Uno stimolo quindi a superare un approccio un po' troppo semplicistico al problema e strumenti per poter rappresentare al management dati più oggettivi sull'efficacia dei controlli previsti e/o implementati.

Interessanti evoluzioni in questo senso sono rappresentate inoltre da FAIR Controls Analytics Model e dalle tecniche di rappresentazione delle informazioni analizzate quali la metodologia Bowtie. ■

1. Parte del testo è tratta dal libro: **G.Butti - SICUREZZA TOTALE 4.0 - L'ABC sulla physical cyber security per i DPO e le PMI (e non solo) – 2019 – ITER** https://www.iter.it/prodotto/sicurezza-totale-4-0/
2. Si veda: **G.Butti - Cyber exposure: dalle vulnerabilità alla valutazione dei rischi**, in CyberSecurity Trends N.3/2021
3. Si veda: NIST Special Publication 800-30 Rev 1
4. Nel testo sarà utilizzato il termine controlli o contromisure indifferentemente
5. Direttiva europea sui sistemi di pagamento digitale
6. Si veda al riguardo l'articolo: G.Butti - **Incidenti di sicurezza, ecco come affrontarli secondo la normativa PSD2** https://www.cybersecurity360.it/soluzioni-aziendali/incidenti-di-sicurezza-ecco-come-affrontarli-secondo-la-normativa-psd2/
7. Per un approfondimento sul tema si rimanda all'articolo: G. Butti, A. Piamonte Misurare la physical cyber security, https://atc.mise.gov.it/images/documenti/Rivista/2016/6_misurare_la_sicurezzaiscom.pdf
8. Si veda in proposito l'articolo: G.Butti - Cybersecurity e mondo finanziario, in CyberSecurity Trends N.1/2020
9. Un'altra definizione riportata dalla Circolare 285 è la seguente: *rischio informatico (IT): il rischio di perdite corrente o potenziale dovuto all'inadeguatezza o al guasto di hardware e software di infrastrutture tecniche suscettibile di compromettere la disponibilità, l'integrità, l'accessibilità e la sicurezza di tali infrastrutture e dei dati;*
10. Si veda in proposito: **G.Butti - I rischi nell'analisi dei rischi: gli errori da evitare per rendere fruibile e ripetibile l'analisi effettuata** https://www.cybersecurity360.it/legal/privacy-dati-personali/i-rischi-nellanalisi-dei-rischi-gli-errori-da-evitare-per-rendere-fruibile-e-ripetibile-lanalisi-effettuata/

BIO

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

L'umanità, il digitale e i "futuri possibili".

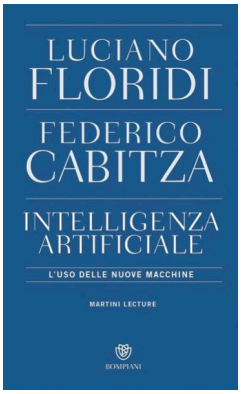
Intervista VIP con Luciano Floridi, Università di Oxford - Bologna.

Autore: Massimiliano Cannata

Luciano Floridi (Oxford-Bologna) e Federico Cabitza si sono confrontati su uno dei grandi temi del nostro tempo: l'intelligenza artificiale (IA), uso, sviluppo, limiti. Bompiani ha pubblicato i tratti salienti di una riflessione multidisciplinare che investe il destino dell'uomo e il futuro prossimo venuto del pianeta che abitiamo, tra paure, speranze, progetti. Abbiamo chiesto a Luciano Floridi di toccare i nodi problematici di questa delicata fase della contemporaneità.

Professore comincerei con una citazione:* "Sono affascinato dai futuri possibili a patto che sia sempre l'uomo a guidare la macchina". *Nel suo saggio si fa riferimento a questa celebre affermazione del Cardinale Martini. Lo sviluppo dell'IA va letto nella chiave interpretativa proposta dal gesuita?

Il saggio riprende i temi principali della mia "Martini Lecture", parte del ciclo che si ispira al magistero del grande Cardinale e teologo. Quando Martini



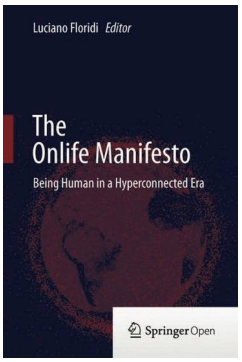
usa la frase "futuri possibili" cui lei si riferisce nella domanda, non intende certo alimentare la fantascienza, né alcuna speculazione fantasiosa, intende piuttosto sottolineare l'apertura razionale che bisogna avere rispetto al cambiamento. L'umanità deve saper esercitare responsabilità e visione quando lavora sulla ricerca e l'innovazione. Ricordiamoci che il futuro non avviene casualmente, non è una pietra che rotola dall'alto, è fatto di miliardi di progetti e di idee che trovano punti di convergenza e equilibri. Mi viene in

BIO

Luciano Floridi è professore ordinario di Filosofia ed Etica dell'Informazione e Direttore del Digital Ethics Lab dell'Oxford Internet Institute, all'Università di Oxford, e Turing Fellow presso l'Alan Turing Institute. Tra i molti riconoscimenti e incarichi, è stato titolare della Cattedra UNESCO in Information and Computer Ethics, Francis Yates Fellow presso il Warburg Institute di Londra, e Gauss Professor della Akademie der Wissenschaften di Göttingen. Si è impegnato in numerose iniziative di policy col Parlamento e il Governo britannici, col Parlamento Europeo, la Commissione Europea, il Consiglio d'Europa, l'UNESCO, la Camera dei Deputati italiana, nonché con molte aziende quali Capgemini, Cisco, DeepMind, Deloitte, EY, Facebook, Fujitsu, Google, IBM, Leonardo, Microsoft, Sogeti, Tencent, Vodafone e Volkswagen.
Il professor Floridi è anche un seguitissimo divulgatore e inventore di neologismi ormai divenuti iconici a livello globale, come 'infosfera', 'quarta rivoluzione', 'iperstoria', e 'onlife', neologismo quest'ultimo per intendere la nuova esistenza nella quale la barriera fra reale e virtuale è caduta, e non c'è più differenza fra "online" e "offline".

mente l'immagine delle gocce d'acqua in un bicchiere pensando ai grandi movimenti di popolo che hanno mutato la faccia della storia nei secoli. Assumiamoci dunque le nostre responsabilità, questo l'insegnamento di Martini che mi sento di condividere, anche dalla mia prospettiva che è quella di un laico agnostico. La vita è la nostra, non dimentichiamolo mai.

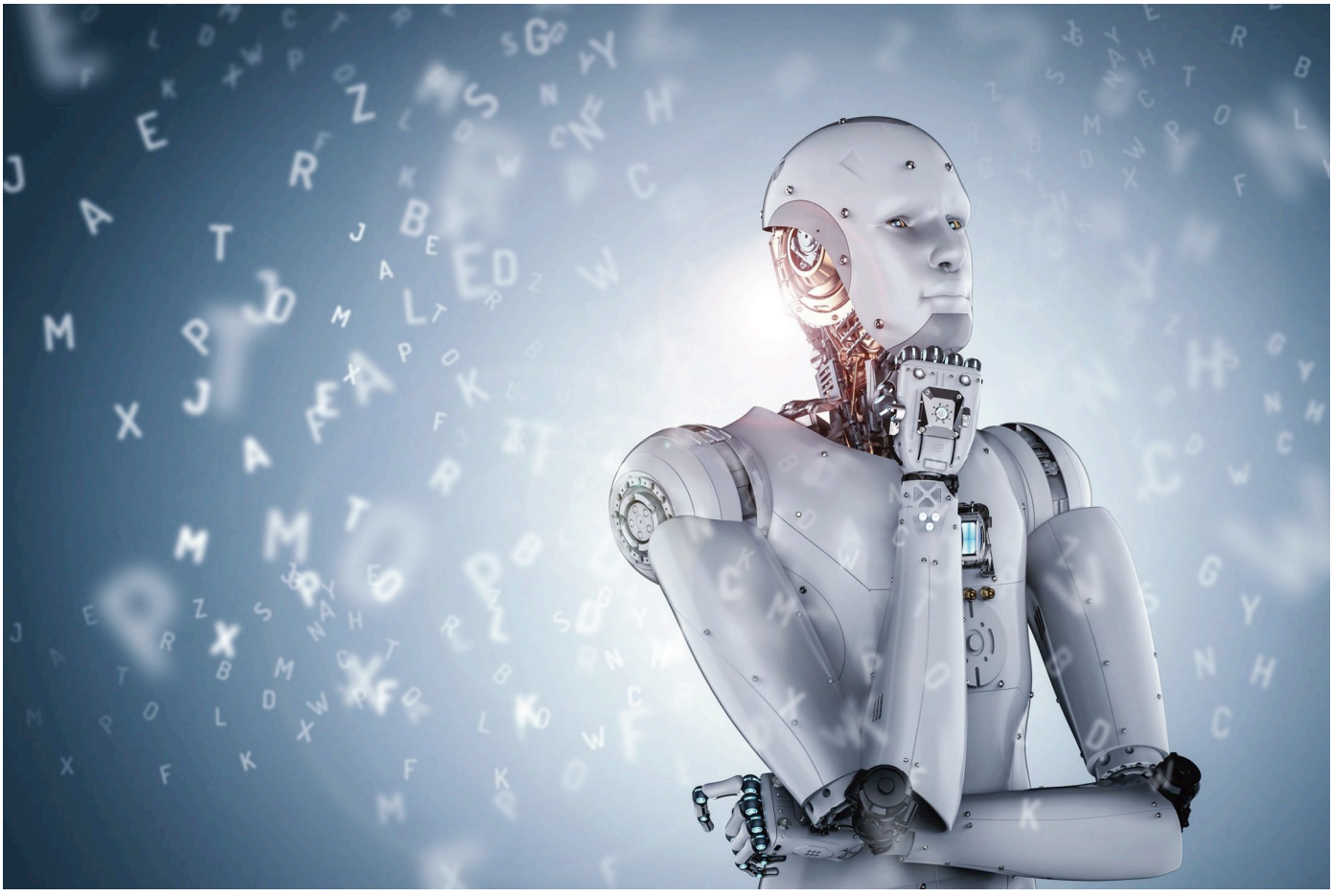
"Onlife", come ci ha già spiegato in una precedente intervista pubblicata da* Cybersecurity Trends*, è la nuova categoria dell'essere entro cui ci muoviamo. Quale deve essere la "distanza" che dobbiamo mantenere dai dispositivi elettronici per usarli con intelligenza, sicurezza e adeguata consapevolezza?



Quella della distanza è una riflessione importante. Soggetto e oggetto sono categorie che appaiono oggi radicalmente mutate. Di conseguenza anche la distanza tra queste componenti non è quella che siamo abituati a considerare. Persino la relazione che intratteniamo con il mondo risulta modificata, la simpatia e l'antipatia, per dirla con i termini che usavano i filosofi della classicità, ha subito delle varianti molto importanti. La distanza che misuravamo per raggiungere, per esempio una città, non ha più un riferimento preciso che consente di misurarla, perché il digitale sta modificando il paesaggio urbano, attraverso percorsi differenziati in momenti differenti, a seconda del traffico. Gli oggetti sono interattivi, li possiamo toccare, come un'icona che si accende sullo schermo del mio pc, ma non la potrò fisicamente spostare, come si fa con un sopramobile, una pentola, un paio di occhiali, eppure rimane pur sempre qualcosa con cui interagisco. Anche il soggetto si sta modificando, socializza il suo essere nella rete e con gli strumenti connessi, riconsiderando continuamente la sua identità. La distanza è diventata dunque un rapporto tra interattività e socializzazione. L'individuo manifesta una molteplicità di volti nell'universo tecnologico, la sua identità si articola di conseguenza, la sfida è quella di non frammentarla in mille rivoli, perdendosi tra un *tik tok*, un social e un *twitter*.

L'intelligenza artificiale è un'ulteriore manifestazione di quella che Emanuele Severino definiva "cieca volontà di potenza della tecnica". Come si fa a sgombrare il campo da tante false "letture" che generano paure e che di fatto sono un freno all'innovazione?

La ricetta è quella di sempre, la dovremmo conoscere: serve più conoscenza. La paura è fomentata dall'ignoranza, paura sociale, quindi dell'altro ma anche della tecnologia. La tecnologia esercita una domanda di conoscenza molto precisa. La responsabilità rimane la nostra, quando utilizziamo mezzi e strumenti sofisticati



e potenti. Attenzione però: credo che sia pericoloso parlare di umanità in generale, come se fosse un unico blocco. Da un lato abbiamo una parte del mondo che produce, utilizza, si serve della tecnologia, per controllare e dominare, dall'altra parte miliardi di persone che non conoscono il linguaggio della tecnica, non la producono e non la controllano e perciò rischiano di subirla. Non c'è un'umanità e una tecnologia prese in universale, ci sono tante tecnologie e tante umanità, il tema è come si rapportano tra di loro. Questo apre la riflessione sulla diseguaglianza, sulla dinamica che contrappone, per usare un termine gramsciano, ceti egemoni e ceti subalterni, nazioni forti e nazioni deboli.

È evidente che serve una sensibilità etica per bilanciare il percorso dello sviluppo della scienza e della tecnologia insieme a quello della società e dell'ambiente. Oggi comandano, non tanto i produttori di informazione, ma chi controlla l'ambiente digitale che rende possibile la circolazione delle informazioni e la formulazione delle domande essenziali da cui dipende l'evoluzione economica, politica e sociale della contemporaneità. Per dirla con una frase a effetto la nuova morfologia del potere è la morfologia dell'incertezza.

L'IA nella quarta rivoluzione

Nell'economia della quarta rivoluzione, descritta con compiutezza di analisi da un suo precedente saggio, l'IA che posto occupa?

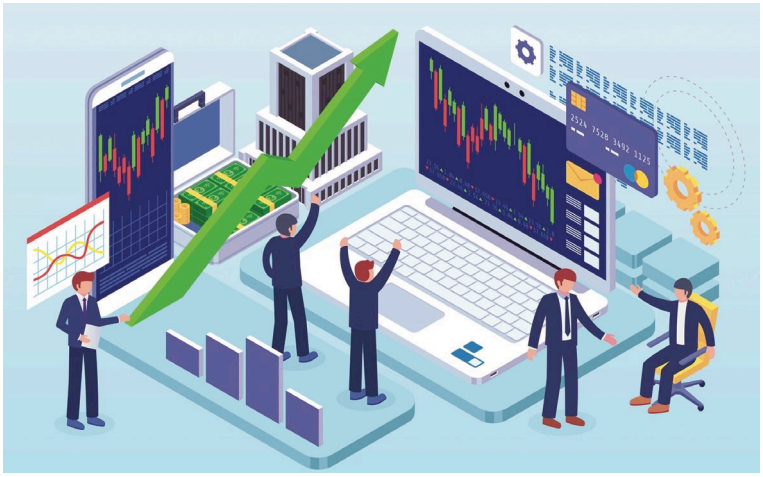
Immaginiamo di aver costruito un ambiente e di avere allo stesso tempo progettato le forze che lo fanno funzionare. Siamo nella condizione di chi ha costruito un'isola, ed è anche in grado di controllare i movimenti e le azioni degli animali che si muovono in quell'isola. A questo punto c'è da chiedersi: l'ambiente e le forze che agiscono autonomamente in questo ambiente chi le controlla? La mia ricerca attuale si sta concentrando sul fatto che l'IA non è una nuova forma di INTELLIGENZA, MA UNA NUOVA FORMA DI CAPACITA' DI AZIONE, una nuova *agency*, per usare un termine inglese che non trova corrispettivo nel nostro vocabolario. Forme di agency nel mondo ne abbiamo conosciute tante. La agency della natura: terremoti, vulcani, il vento, "cose che fanno cose", per usare un gioco di parole. La agency biologica: il cavallo, il cane pastore… quella umana, degli individui che si muovono nell'universo, ma che sono anche in grado di creare il motore, aprendo la strada per la creazione della agency meccanica. E ora ne abbiamo una quinta…

A cosa si riferisce?

A una agency autonoma che ha una capacità di agire che assomiglia al motore a scoppio in quanto ingegnerizzata, ma anche un po' a un animale. Pensiamo all'algoritmo che ha una sua indipendenza, ma qualcuno lo deve pur guidare per raggiungere un risultato, come un cavallo che corre da solo, ma va guidato nella direzione giusta. Torniamo ancora alla riflessione inziale di Martini e la nostra nuova isola. In un ambiente sempre più digitale controllare queste cinque forme di capacità di agire: naturale, animale, umana, meccanica e digitale vorrà dire essere i "nuovi padroni" dell'universo. Si stanno di fatto sovrapponendo, in modo pericoloso, i controllori dell'ambiente e i controllori di questa nuova capacità di agire. Siamo oltre il vecchio dominio delle élite, fondato sulla differenza di classe e di censo, entriamo in una forma di controllo molto più pervasiva, quella che riguarda l'ecosistema e le forze che si muovono in esso.

Che cosa comporta tutto questo?

Nuovi scenari di intervento e di responsabilità per le classi dirigenti innanzi tutto. È possibile che fra pochi anni arriverà il *quantum computing*, ultima frontiera dell'evoluzione computazionale. Se le stesse persone avranno il dominio anche su questo nuovo strumento i pericoli aumenteranno. Chi



controllerà i controllori? Non stiamo parlando di fantasie astratte, perché questo futuro è già presente. La sovrapposizione lineare tra egemonia ambientale, egemonia in termini di *agency* e di capacità di prevedere il futuro deve fare alzare l'asticella dell'attenzione. Non vedo altra via di uscita: i controllati devono controllare i controllori, la società deve maturare questa capacità, aggiornando quanto scritto nella costituzione, che assegna al popolo la sovranità. Il circolo virtuoso di ogni democrazia che funzioni è questo, controllare chi comanda, avendo la possibilità di rimuoverlo nel momento in cui perde di vista il bene comune. Anche il business deve sottostare a questo controllo "popolare", senza una *governance* illuminata le nostre democrazie saranno destinate ad ammalarsi con le conseguenze del caso.

I nuovi profili di rischio

Lo sviluppo delle tecnologie impone nuovi profili di rischio. Cosa dice un filosofo ai suoi studenti se come abbiamo appurato in questa conversazione lo stesso vocabolario della conoscenza ha mutato statuto: soggetto, oggetto, spazio, tempo, relazioni causali, non sono definibili in maniera univoca, come orientarsi allora?

È importante mettersi insieme, confrontarsi e tentare di socializzare la conoscenza. Nessuno può pretendere di avere una visione complessiva esaustiva, ma tutti possiamo portare un tassello, un contributo per capire e disegnare meglio la realtà. Anche se il mondo cambia mentre credi di averlo studiato e capito bisogna ricordarsi che i fondamenti, la natura umana restano invariati. Per questo vale la pena leggere Platone o Aristotele che ci dicono cose eternamente valide. Con un piccolo esempio biografico, sto leggendo "La ricerca del tempo perduto". Probabilmente ci vorrà un anno, ma mi servirà molto nel mio lavoro quotidiano, per la capacità introspettiva, lo scandaglio dell'animo umano, la lettura della società nelle sue gioie, paure, speranze, pregiudizi o aspettative che fa Proust e che rimane valida anche ai nostri giorni.

Rimane poi importante abbracciare l'innovazione. Prendere sul serio l'"altro", la diversità con spirito inclusivo. Vuol dire comprendere che anche nella diversità, la comune umanità è il fattore che ci lega e che può legare anche il dialogo intergenerazionale. Wittgenstein diceva che devi arrivare dove tocchi il letto del fiume, per intuire la sostanza delle cose per raccontarla senza tempo, senza però illuderti che il tuo sia l'unico discorso. Parlare di quella temporalità che ci diversifica, senza però generare conflitti può aiutarci. Contemperare la costanza delle invarianti e l'accelerazione della temporalità, può infatti rappresentare la chiave che porta al domani. Questa è la sfida, che comincia dai primi anni della scolarizzazione, che parte dalle nostre prime e indimenticate maestre e docenti (e parlo al femminile per ragioni sia personali sia sociologiche). Nel mio caso, cinque insegnanti alle quali devo la mia formazione, me le lasci menzionare, per uno come me che non ha memoria e non si ricorda neppure che cosa ha fatto ieri sono nomi importanti: Mattei (elementari), Geromel (medie), Viterbo (ginnasio), Migliorini (liceo), Haack (università).

Per concludere, sono convinto che è anche su questi fattori – tolleranza, socializzazione, solidarietà, e poi intelligenza, conoscenza e innovazione – che misureremo il grado di progresso che saremo capaci di raggiungere nel futuro che ci appartiene. ■

Il digitale dalla A alla Z. Un dizionario per comprendere la rivoluzione in corso.

Intervista VIP con Pieraugusto Pozzi.

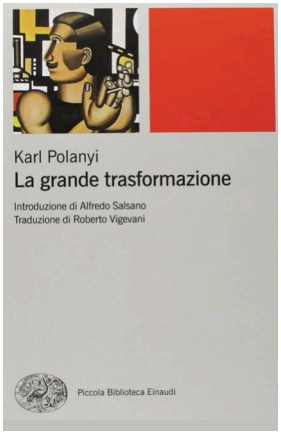
Autore: Massimiliano Cannata

Il "piccolo dizionario della grande trasformazione digitale", edito da Aras", è un'iniziativa costruita attraverso la collaborazione di esperti ed accademici di diversa estrazione ed esperienza che fa tornare alla mette una celebre affermazione del *Tractatus* di Wittgenstein *"i limiti del mio linguaggio sono i limiti del mio mondo"*.

Prof. Pozzi Lei ha curato questa originale operazione, con quali finalità?

Con gli autori che mi hanno affiancato nella ricerca abbiamo pensato che il modo migliore per capire questo universo digitale in espansione, e anche per intravedere la materia ed energia oscura che contiene, fosse scrivere un dizionario che parlasse dei nuovi mondi, galassie e protagonisti che lo formano. Lo studio serve a riflettere intorno alle parole e ai concetti chiave del nuovo universo digitale, che ha avuto origine con il Bit Bang che ha segnato la convergenza digitale, unificando ambiti, mercati, culture prima nettamente separati, quali: informazione, editoria, media, pubblicità, istruzione, cultura di massa.

"Il digitale è un nuovo ordine, non semplicemente un passaggio evolutivo", così si legge nell'introduzione. Alla luce di questa affermazione, quali scenari si aprono per il prossimo futuro?



Molti autori parlano giustamente di rivoluzione e di trasformazione digitale. In questo lavoro abbiamo piuttosto voluto riprendere l'intuizione di Karl Polanyi, che a metà del Novecento aveva evidenziato come la grande trasformazione industriale fosse stata generata dalla capitalizzazione di terra, denaro e lavoro. La trasformazione digitale, di converso secondo noi, si sta compiendo nella capitalizzazione di dati, informazioni e conoscenze, che stanno di fatto segnando una nuova categoria ontologica. Stiamo sperimentando una profonda trasformazione dell'economia, della politica, della scienza, che sono gli asset di riferimento che avevano caratterizzato la modernità, e che oggi ridefiniamo come: tecnoeconomia, tecnopolitica, tecnoscienza.

Un diverso orizzonte si sta dunque facendo strada, siamo preparati ad affrontarlo?

Parlerei piuttosto di un nuovo ordine iper-moderno dell'universo digitale, amplificato e accelerato dall'emergenza pandemica che ci ha costretto ad adottare gli strumenti del digitale per continuare, in remoto, ad avere relazioni e a svolgere tutte le nostre attività di lavoro, di studio, di relazione. Per dirla con Edgar Morin sono tutte tracce di quella *"metamorfosi digitale"* con cui dobbiamo imparare a fare i conti.

Essere digitale come nuova categoria ontologica

Da algoritmo a Generazione Z si snoda il vocabolario della quarta rivoluzione. Qual è il fil rouge di questo affascinante percorso?

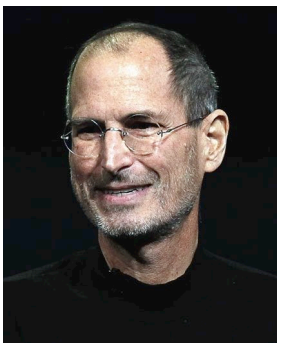
Per avere un obiettivo praticabile in tempi ragionevoli, abbiamo pensato di lavorare su ventisei parole chiave, una per ciascuna lettera dell'alfabeto internazionale. Il primo avvincente lavoro fatto con la squadra interdisciplinare degli autori (una linguista, uno storico, un filosofo, tre ingegneri) è stata la scelta delle parole, dei lemmi da compilare. Chiaro il *fil rouge:* il digitale è il motore di una trasformazione in fieri, che non è limitatamente tecnologica ma profondamente culturale. Questo richiede la comprensione di parole molto usate nella quotidianità e importate dall'inglese come *policy* e *key*, redatte da Silvia Boero, linguista che vanta una lunga esperienza accademica negli Stati Uniti, accanto alle voci più tecnologiche curate da colleghi con un profilo ingegneristico, Riccardo Poggi e José Cerruto.

Non solo concetti, ma anche personaggi, come Steve Jobs e Xi Jinping. Viene da chiedersi: cosa avranno in comune?

Potremmo dire che è il fattore "D", come digitale, che li accomuna, nel senso che in ogni voce del dizionario e, in particolare nell'illustrare i personaggi che lei ha menzionato nella domanda, abbiamo cercato di far capire quale sia stato il contributo che hanno offerto alla trasformazione digitale e come la loro stessa esperienza di vita sia stata, come per molti di noi, modificata dal digitale.

BIO

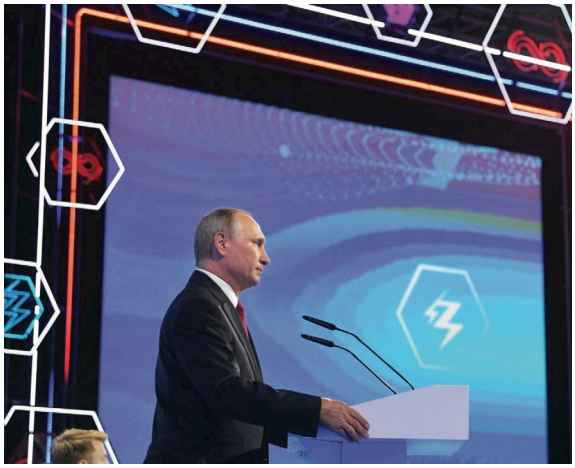
Pieraugusto Pozzi è segretario generale Associazione Infocivica, ingegnere, autore di ricerche, saggi e rapporti sul mondo digitale. Ingegnere elettronico, dagli anni Ottanta lavora nell'industria e nella ricerca nei settori della telematica e delle reti di calcolatori. Dagli anni Novanta, in qualità di Direttore FTI (Forum per la Tecnologia dell'Informazione), coordina e realizza studi e rapporti sugli aspetti politici, economici, normativi, sociali e culturali del digitale e delle tecnologie dell'informazione e della comunicazione (commercio elettronico, sistemi digitali di pagamento, sicurezza dell'informazione, PA digitale, società digitale). Dal 1996 condirettore della Collana Società dell'Informazione e della Comunicazione pubblicata da Franco Angeli, ha avuto incarichi di docenza universitaria. Tra le pubblicazioni: Polis Internet (Franco Angeli, 2000); Crimine virtuale, minaccia reale. ICT Security (Franco Angeli, 2004); Moneyonline.eu. The future of digital payment systems (Franco Angeli, 2007); eGovernance and public communication for an inclusive eSociety (Franco Angeli, 2008), La macchina è antiquata, in Le Maschere del male. Una sociologia (Franco Angeli, 2015); Immagini del digitale. Dopo il Bit Bang (Nemapress, 2019); Connettività, conoscenza e società nell'universo digitale in Pubblicare l'architettura: dalla tradizione all'era digitale, (CNBA-Casalini Libri, 2020) e Piccolo dizionario della grande trasformazione digitale (Aras Edizioni, 2021).



Intelligenza artificiale e impatti geopolitici, un nesso spesso trascurato. Cosa c'è da capire su questo delicato terreno?

In questi ultimi mesi, molti scienziati della politica e molti esperti di geopolitica cominciano ad occuparsene seriamente. Se Bremmer parla di momento tecnopolare,

nel quale sono i poteri digitali a ridisegnare l'ordine mondiale, Kissinger, Schmidt e Huttenlocher parlano di epoca dell'intelligenza artificiale. Concretamente, mi pare che il caso Cambridge Analytica e i fatti di Capitol Hill abbiano dimostrato l'importanza della tecnopolitica digitale. Del resto, diversi leader politici, con accenti diversi, lo avevano compreso da tempo: Merkel (2016): "la trasparenza e la negoziabilità degli algoritmi afferisce ormai alla natura e alla sicurezza della democrazia"; Putin (2017): "chi controllerà la migliore intelligenza artificiale, governerà il mondo"; Xi Jinping (2017): "l'intelligenza artificiale cambierà profondamente il mondo e la vita umana e sociale... questo strumento consentirà un governo più efficiente e sarà indispensabile per mantenere la stabilità sociale".



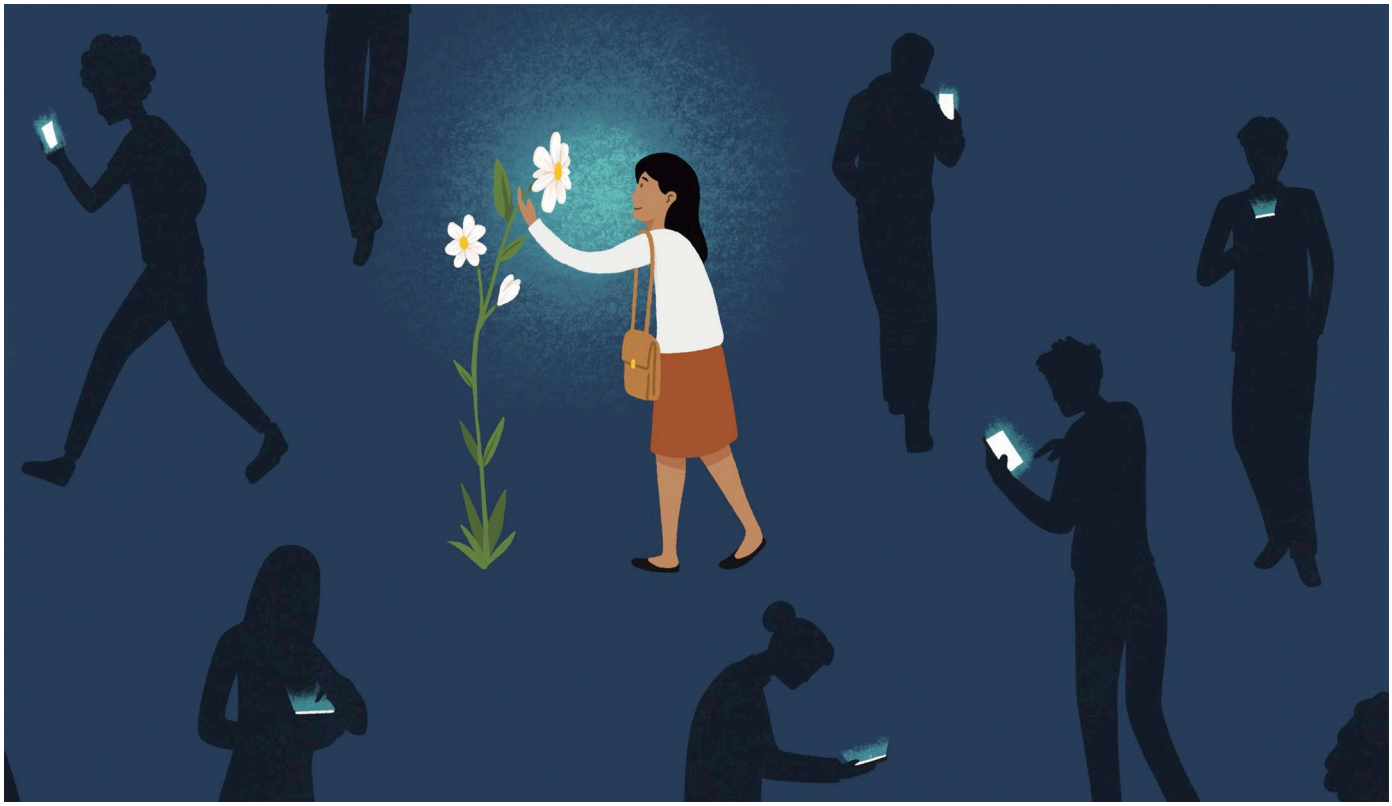
La stessa opinione pubblica ha mutato il suo profilo con la rivoluzione digitale. Abbiamo una opinione di sciame condivisa in varie bolle. Cosa vuol dire in concreto?

Significa che lo spazio pubblico della comunicazione, discussione e del confronto ideale e culturale che abbiamo conosciuto, con tutti i suoi limiti e l'orientamento al mainstream, è sempre più minoritario rispetto allo spazio privato e personalizzato delle piattaforme. In modo che il dibattito delle idee che si svolgeva nella sfera pubblica analogica regolamentata è diventato il mercato delle verità alternative, profittevoli e ingannevoli della sfera privata digitale deregolamentata. La risultante è data da una società che ha picchi virali di attenzione su singoli (importanti) aspetti di discriminazione, diseguaglianza, privilegio e spreco, sui quali però non opera una macchina ideale della ragione, dei sentimenti condivisi, dell'empatia, ma quasi sempre una macchina digitale del fango, che produce irrazionalità, emozioni negative, risentimento, attivando processi di individualizzazione e tribalizzazione che spezzano il legame sociale. Sono tutti fenomeni che la pandemia ha certamente acuito.

Storia e memoria in una società schiacciata sul presente

Il tema della memoria e il valore della storia hanno mosso l'ASC (Associazione di Storia Contemporanea) che ha promosso la ricerca. Quanto pesano questi fattori in una società superficiale che sembra voler rimuovere il passato, schiacciata come appare sul presente?

È stato determinante il ruolo di ASC e del suo presidente Marco Severini, che ha partecipato alla stesura del dizionario anche in qualità di autore (tra le altre, da ricordare le voci *contemporaneità* ed *etica*, n.d.r.), creando i presupposti necessari a perseguire l'obiettivo di interdisciplinarietà che



volevamo connotasse la ricerca e che ne aveva ispirato l'idea iniziale, elaborata con Roberto Cresti, filosofo e autore delle voci *memoria* e *umanesimo,* e, come Severini, docente all'Università di Macerata. Siamo preoccupati del fatto che, in luogo di una vera conoscenza storica, fondata su una visione complessiva e prospettica, si faccia strada un approccio cumulativo e informativo, schiacciato sul presente, superficiale, incapace di usare a dovere gli immensi giacimenti documentali disponibili. A queste condizioni la storia, che non è una scienza esatta, ma una disciplina di rigore scientifico, finisce col lasciare spazio al negazionismo (cioè al rifiuto ideologico di ammettere alcuni fatti del passato) o a comode interpretazioni, che si manifestano nelle sembianze delle cosiddette *"verità alternative"*, che possono diventare, sovente con il discutibile sostegno di atti legislativi, verità assolute.

Umanesimo digitale è una etichetta oggi spesso abusata. Qual è il giusto valore che va dato al rapporto tra etica, scienza e filosofia?

Il dizionario è stato pensato come strumento di un'autentica società della conoscenza, capace di esprimere consapevolezza e coscienza del presente e del futuro di un'umanità finalmente libera dal peso di apparati cognitivi artificiali sempre più perfezionati e pervasivi. Con gli altri autori abbiamo cercato di produrre un lavoro improntato all'umanesimo digitale, in linea con il programma proposto intelligentemente da Julian Nida-Rümelin e Nathalie Weidenfeld in *"Umanesimo digitale. Un'etica per l'epoca dell'Intelligenza Artificiale"*.

Il binomio sicurezza e libertà, come stiamo vedendo in questi tempi di emergenza, è una dicotomia chiave della contemporaneità. Sistemi pubblici e privati sono preparati alle sfide che abbiamo di fronte?

Senza dubbio, il digitale impatta il principio e l'esercizio di sovranità nei settori che sono stati il cardine degli Stati moderni: moneta, difesa, istruzione, sanità, fiscalità e giustizia. Settori tutti sfidati dalla trasformazione digitale, che ne muta gli assetti organizzativi e la missione essenziale. Basti pensare alla statistica (disciplina che definisce i sistemi e i metodi di raccolta, ordinamento ed elaborazione dei dati) che, come ricorda il suo etimo, si sviluppa storicamente per rafforzare la capacità di governo degli Stati nazionali attraverso la raccolta e l'elaborazione di dati demografici, sanitari, scolastici, amministrativi. Negli ultimi decenni, prima la digitalizzazione e soprattutto la datificazione, hanno portando un volume costantemente crescente di dati di interesse pubblico verso le grandi piattaforme private globali.

Un esempio molto chiaro lo abbiamo avuto dall'accidentato sviluppo delle applicazioni di tracciamento nella crisi pandemica che ha richiesto, almeno nei paesi occidentali, l'accordo con Apple e Google, detentori della tecnologia operativa degli smartphone. Vanno anche segnalate le minacce portate alla giurisdizione, alla sovranità e alla sicurezza degli stati nazionali. Gruppi criminali e terroristici, imprese ed "agenzie private", usando mezzi digitali,

possono portare alle infrastrutture, alle istituzioni e alle comunità attacchi sempre più rapidi e sofisticati, con gravi conseguenze sul pano economico, ma anche geopolitico. Per queste ragioni appare davvero fondamentale che la sicurezza digitale possa disporre di un presidio professionale, qualitativamente alto in grado di ridurre le vulnerabilità dei tanti colleghi che ci leggono e che svolgono ogni giorno con passione e dedizione il loro lavoro. ■

L'uomo e i valori devono essere al centro della rivoluzione tecnologica.

Intervista VIP con Agnese Scappini.

Autore: Massimiliano Cannata

Psicologa del lavoro, psicoterapeuta, esperta di comunicazione, scrittrice, Agnese Scappini è un'attenta osservatrice dei fenomeni di trasformazione della società. In questa intervista analizza gli impatti della rivoluzione tecnologica, soffermandosi su due aspetti cruciali: l'evoluzione dei cambiamenti organizzative e delle dinamiche relazionali legate allo sviluppo dello Smart Working e il delicato binomio: internet e minori, connubio ricco di opportunità, ma anche denso di pericoli e insidie.

Professoressa Scappini, la pandemia è stata un catalizzatore di molti processi economici e sociali. Il primo effetto visibile è stato determinato dall'adozione, prima marginale e oggi significativa, dello* Smart Working. *Quale scenario si apre sulla spinta di questo "strappo" radicale, fino a un anno fa assolutamente imprevedibile?

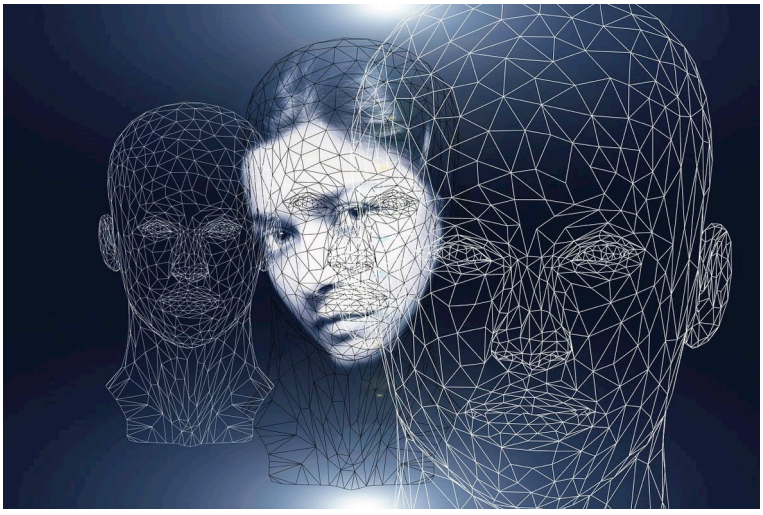
La Pandemia come tutte le grandi crisi sociali ha provocato più che uno strappo, un'accelerazione drastica di un processo intrapreso nell'ultimo ventennio, con l'avvento di Internet, incredibile e potentissimo strumento. Le potenzialità della rete sono tali da esigere la costruzione di una nuova categoria di valori sociali e civili capace di supportarne la portata e l'utilizzo. Credo che gli scenari futuri saranno sempre più legati alla creazione di un substrato valoriale, per farlo è necessario cominciare a recuperare un po' del passato che ci appartiene.

Quali rischi e quali opportunità possono arrivare dalla "rivoluzione intelligente" generata dall'uso di massa delle info* – appliances, *che deve essere accompagnata da consapevolezza, formazione, attitudine al cambiamento da parte del maggior numero di persone possibile, tutti, per dare i frutti sperati?

La "rivoluzione è intelligente" se non si riduce ad essere semplicemente performativa; lo smart working, sebbene sia capace di potenziare i fattori di produzione, porta con sé il grave rischio di ridurre drasticamente le relazioni sociali, a causa del venir meno dello scambio interpersonale e interprofessionale, non mi riferisco solo all'ambito lavorativo. L'attitudine al cambiamento, cui lei si riferisce nella domanda può rafforzarsi solo a condizione di rafforzare la socialità, il confronto costante di storie, competenze, esperienze.

Reale e virtuale hanno aperto il fronte di una "nuova ontologia". Questa categoria dell'esistente, fondata su una condizione "ibrida", come va vissuta e interpretata?

Il virtuale si può a mio avviso definire una nuova dimensione dell'essere, "ibrida" sì certamente, comprende la persona e nello stesso momento la ridimensiona o addirittura la supera (in base all'uso che se ne fa appunto). Va precisato che la dimensione virtuale oggi non è più un'alternativa al reale ma ne diviene un prolungamento, questo comporta che l'identità dell'individuo esige una costruzione, oggi molto più accurata che in passato.



"Diario di un pesce in quarantena" è un'interessante metafora, che definisce una condizione. Lei racconta nel suo ultimo libro con efficacia espressiva e capacità immaginifica, questo* hannus orribilis *dalla prospettiva di un "pesciolino", per lanciare quale messaggio all'opinione pubblica?

L'immagine di un pesciolino rosso, che si muove dentro un piccolo recipiente d'acqua, esprime la condizione più stringente a cui si possa pensare. Il piccolo animale non sa, però, di essere costretto da pareti, osserva le persone della famiglia con cui vive, che sono a loro volta confinate in casa, improvvisamente privi della libertà di agire. Il paradosso sta in questo: le condizioni del pesciolino e della famiglia che lo ospita diventano simili. Entrambi in apnea, ma il pesciolino vive nell'acqua, a noi non basta vivere immersi nell'elemento originario, perché è essenziale la comunicazione tra i vari esseri viventi. Siamo esseri in connessione, la nostra linfa vitale viene da questo continuo contatto, dovremmo cercare di non dimenticarlo mai.

Vivere da reclusi ha cambiato il nostro modo di essere, ma anche il profilo delle città che abitiamo. Molte cose fanno pensare che non torneremo più quelli di prima, quale futuro ci aspetta? La memoria, tema trattato nel suo "Diario", che peso potrà avere in un mondo che sembra schiacciato sul presente?

La memoria è un tema che mi sta a cuore, a cui dedico un capitolo dell'ultimo saggio su cui sto lavorando. Ogni ipotesi e avanzamento verso il futuro esige il recupero della memoria, che deve darci la consapevolezza di quello che siamo stati, di chi eravamo. "Siamo nani sulle

BIO

Psicologa ad indirizzo lavoro e contesti, Psicoterapueta fenomenologiaca, esperta in comunicazione e scrittrice. Svolge la libera professione di Psicologa clinica, Psicologa del Lavoro e dello sport, si occupa di terapia individuale e di coppia, di adolescenza e infanzia. La sua formazione è strettamente legata alla psicologia clinica, alla psicologia sociale e del lavoro, alla psicologia giuridica, alle metodologie inclusive, al team building, al miglioramento della propria performance e di quella collettiva, alla prevenzione e gestione delle problematiche inerenti a stress lavoro/ correlato e traumi. Ha partecipato come relatrice a webinar formativi per l'associazione Ondif (Osservatorio Nazionale sul Diritto di Famiglia) e Aiga, sulla violenza di genere e assistita. È responsabile Comunicazione e Media per l'Ordine degli Psicologi dell'Umbria e in quanto esperta di comunicazione ha eseguito docenze in giornate di formazione sia per aziende che per privati, riguardo l'uso dei social a scopo lavorativo e non, e stilato policy aziendali collaborando con i legali rappresentanti. Nel settembre 2017 presenta il suo primo romanzo "Una Rosa per un Santo", a maggio 2020 pubblica la sua seconda opera "Diario di un pesce... in Quarantena". Ha scritto diversi articoli di ordine psicologico. Prima ancora ha perseguito la laurea in Lettere e Filosofia con specializzazione in 'Etica delle relazioni umane'.

spalle dei giganti", gli umanisti che avevano rispolverato questo detto che aveva origini più antiche lo sapevano bene, per questo condannavano la dimenticanza, male che caratterizza la nostra epoca. Siamo oggi come predisposti alla condizione ansiogena, nell'attesa di un futuro, privo di quelle certezze acquisite dall'esperienza del passato, questo ci espone alla paura. Schiacciati sul presente, siamo bloccati da una miopia che limita la capacità di progetto e di conseguenza la nostra stessa proiezione verso il domani.

La "luce", altro elemento da lei trattato. Luce come energia e motore del racconto… Siamo, però, immersi nel "buio" del tunnel del contagio, angosciati da nuove "varianti" che ci tolgono il sonno. Ne usciremo?

Siamo noi la luce, quindi è nostro dovere e responsabilità illuminare, guidare la storia. Il covid più che un momento buio, è un sintomo di un malessere del corpo sociale, come tutti i sintomi deve essere compreso e interpretato, se vogliamo attuare quel salto di paradigma, necessario a cambiare passo.

Difesa dei minori e uso consapevole delle tecnologie. Come va affrontato questo che è destinato a diventare uno dei grandi temi del nostro tempo?

Innanzitutto, affrontiamo sul serio la questione. Non lo stiamo ancora facendo sufficientemente. Quella che diviene necessaria è la disciplina. Nel corso dei parent training che tengo presso il mio studio cerco di guidare i genitori a strutturare una regolamentazione nell'utilizzazione dei diversi dispositivi elettronici. Non ci rendiamo conto che diamo nostri figli in mano un incredibile potere senza che noi per primi disponiamo delle competenze necessarie. Per la prima volta nella storia i genitori conoscono gli strumenti, meno dei figli, questo fa perdere loro quell'autorevolezza necessaria per chi deve fare da guida. Torno, in chiusura, alla prima domanda: dobbiamo strutturare e consolidare un sistema di valori, in assenza del quale il genere umano non potrà sviluppare al meglio le eccezionali potenzialità di cui dispone. ■

I dati un tesoro prezioso da difendere nella società delle reti.

Autore: Massimiliano Cannata

La protezione dei dati personali è la nuova vera frontiera da difendere, il tesoro prezioso che fa gola alla criminalità che opera nella piazza virtuale, spinta da interessi di business e dalla volontà di limitare le libertà democratiche. Il messaggio è stato lanciato da una giornata di studi organizzata dal Policlinico *"Paolo Giaccone"* di Palermo. Lo stato maggiore della sanità regionale, i vertici della guardia di Finanza, il Garante della Privacy, nell'occasione rappresentato dall'avvocato Guido Scorza, membro del Collegio, tra i massimi esperti di diritto e tecnologie, si sono confrontati sul tema: *"Privacy: ruoli di responsabilità e controllo".*

"Un evento – ha detto in apertura il Commissario Straordinario **Alessandro Caltagirone** - che vuole mettere a confronto più punti di vista. La complessità del tema richiede interdisciplinarietà, perché senza esercitare uno sguardo obliquo le aziende sanitarie e le imprese non potranno ottemperare tutto quello che il regolamento entrato in vigore nel 2018 richiede in materia di trattamento dei dati". "Quello che abbiamo voluto mettere sul tavolo – commenta Boris La Corte responsabile del Gruppo Aziendale Privacy – è la dimensione della responsabilità sociale della pubblica amministrazione che gestisce la sanità. La sicurezza in questi ambiti rappresenta la punta avanzata di una sensibilità che coinvolge la dignità della persona, la sua condizione di benessere, esistenziale oltre che fisica. Consapevole di questo il Policlinico di Palermo ha voluto marcare la diversificazione fra le attività di controllo che competono al *Data Protection Officer* e il corpus più ampio di interventi cui l'Azienda è chiamata a rispondere nella quotidianità delle scelte politiche e organizzative.

BIO

Filosofo, giornalista professionista, e autore televisivo, Massimiliano Cannata svolge la sua attività come consulente di direzione nell'ambito della comunicazione d'impresa e della ricerca applicata allo sviluppo della cultura manageriale nel contesto organizzativo della social innovation.
Membro del Comitato scientifico della rivista di filosofia, architettura e cultura della città "Anfione e Zeto", tra i curatori dell'edizione italiana di Cybersecurity Trends, collabora con Il Mattino di Padova oltre a svolgere attività di divulgazione scientifica su alcune riviste di settore. E' autore di numerosi saggi sui temi del passaggio dall'industriale al digitale e di sociologia del cambiamento.

Un evento interdisciplinare

Tre i versanti di analisi affrontati dai relatori: ***Giuridico:*** il nuovo regolamento europeo ha previsto l'introduzione di una figura il DPO che ha come compito la tutela e il controllo dei dati personali. ***Filosofico:*** l'introduzione delle tecnologie nella pratica terapeutica apre un orizzonte di rischio per il "corpo elettronico", fatto di quelle informazioni che ci appartengono e che sono potenzialmente esposte al cyber-spionaggio. All'interrogativo etico, formulato dai pensatori dell'antichità: "cosa devo fare per essere uomo", si aggiunge "cosa dobbiamo fare per essere uomini nel cyberspazio" in un contesto in cui non bastano più gli assi cartesiani per orientarsi, spazio e tempo infatti si intrecciano, facendo saltare ogni ipotesi di prevedibilità in un vorticoso incrocio segnato da incertezza e instabilità crescenti.

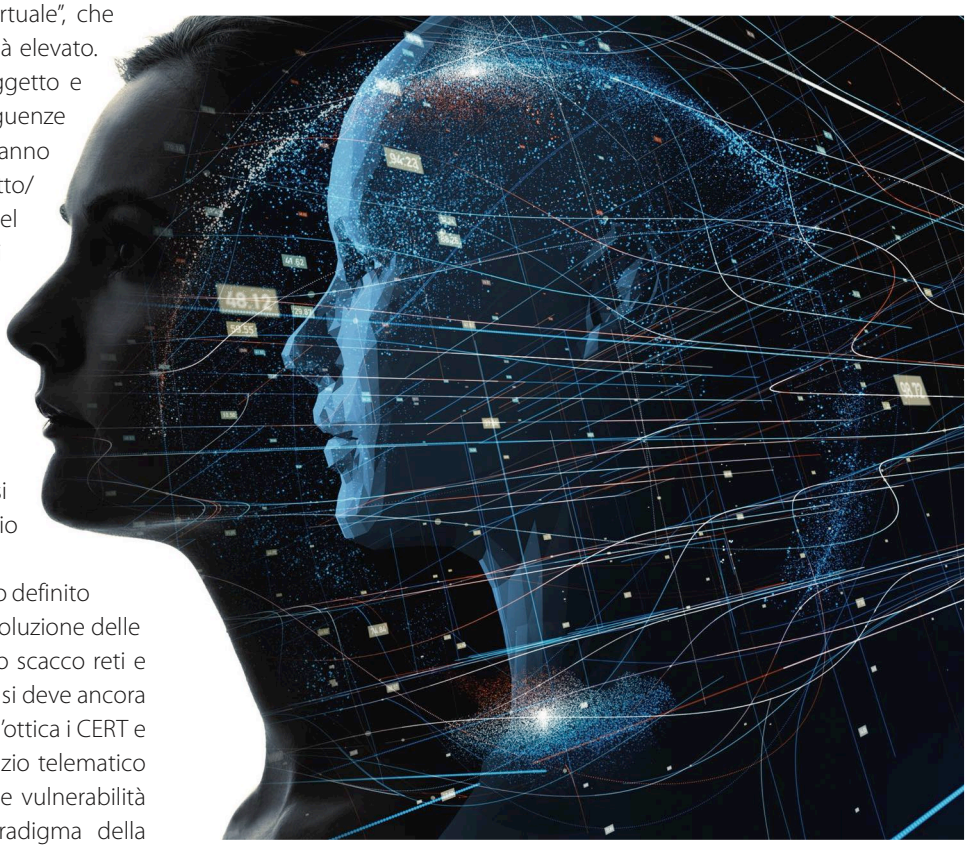
Alla liquidità ben delineata dagli studi di Bauman si è ormai sovrapposto un ulteriore tassello, la fragilità costitutiva *dell'homo technologicus,* sollecitato a governare reti e sistemi straordinariamente articolati. La dimensione dell'altro quando si parla di *Data Protection* diventa, infatti essenziale, quell'altro che, per richiamare le tesi di Bertrand Badie "è la circostanza che ci chiama all'essere". Il virtuale ha infatti imposto una "nuova ontologia", all'essere come "potenza" e come "atto" teorizzato nella "Metafisica" di Aristotele, si è aggiunta la categoria dell'essere "virtuale", che impone un livello ancora di responsabilità elevato. La tecnologia è dentro di noi, dove soggetto e oggetto si mescolano, con delle conseguenze epistemologiche e scientifiche che hanno delle ricadute sul destino del soggetto/paziente e più in generale sul destino del corpo collettivo. All'interrogativo dei primi filosofi ***"cosa devo fare per essere uomo",*** **si sovrappone** ***"cosa devo fare per essere uomo nel cyberspazio"*** in un contesto in cui non bastano gli assi cartesiani per orientarsi. Spazio e tempo si intrecciano come ci ha insegnato Einstein, facendo saltare ogni ipotesi di prevedibilità in un vorticoso incrocio segnato da fatto incertezza e instabilità.

Ed eccoci al terzo versante, che abbiamo definito *Strategico.* La complessità crescente e l'evoluzione delle minacce informatiche, che mettono sotto scacco reti e sistemi, possono dare la misura di quanto si deve ancora fare per proteggere reti e sistemi. In quest'ottica i CERT e le strutture preposte alla difesa dello spazio telematico stanno lavorando sull'individuazione delle vulnerabilità e dei segnali deboli, adottando il paradigma della *governance* del rischio, nella consapevolezza che la potenza tecnologica implica una fragilità intrinseca, che non può essere cancellata. In un tale contesto non dobbiamo stupirci se la sanità occupa una centralità nel discorso pubblico, che mai si era verificata nella storia recente. La "cronicizzazione delle emergenze impone una rivisitazione degli stereotipi e delle verità che abbiano creduto fino a ieri immodificabili" come ha scritto Antonio Scurati. Lo stesso archetipo dell'alternarsi vita morte è messo in discussione dalla pandemia che ci ha trascinato in un inverno della mente e del cuore, che sembra non ammettere il "tempo nuovo" della primavera. Risulta allora evidente che l'economia della cura e le dinamiche ad esse connesse incarnano l'orizzonte primario delle aspettative di un'umanità disorientata, prigioniera della paura.

Il DPO nell'orizzonte della complessità

La nuova figura del DPO non potrà certo limitarsi a *"controllare il traffico delle reti",* dovrà misurare gli impatti che strumenti sempre più sofisticati applicati alla medicina determineranno sui pazienti, favorendo l'emersione della responsabilità sociale, che nel caso dell'impresa sanitaria ha delle ricadute molto precise sulla salute di milioni di cittadini. "Non scordiamoci – ha commentato **Chiara Delaini** DPO, specializzata in *Data Protection, Information Security, Business Continuity* - che stiamo parlando prima di tutto di individui e delle informazioni che li riguardano. Il GDPR non è una questione di forma, ma di sostanza, non si tratta di accontentarsi di compilare dei documenti, ma di lavorare su contenuti e processi.

Le parole chiave che dobbiamo tenere a mente sono: prevenzione, diagnosi, terapia, assistenza e accoglienza. A questi concetti si legano: la ricerca, la formazione, senza di cui sarebbe impossibile orientarsi in realtà

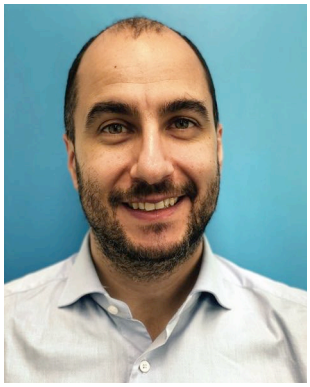


organizzative dense e articolate, potenti ma nello stesso tempo fragili". Si tratta dei "sette piani" di Dino Buzzati che aveva *ante litteram* raccontato il divenire della modernità e la metamorfosi dei contesti urbani, in una società in divenire. "Ampia la catena di implicazioni che la rivoluzione digitale implica, in tutte le fasi del momento produttivo, come hanno evidenziato il colonnello ***Marco Menegazzo***, responsabile comandante del nucleo speciale Privacy e tutela delle frodi tecnologiche della Guardia di Finanza, che ha curato un video intervento in cui ha illustrato il contesto tecnico - normativo entro cui si innesta l'intensa attività delle fiamme gialle. "Il protocollo di intesa che la guardia di Finanza ha siglato con l'autorità garante della protezione dei dati personali" gli ha fatto eco il generale **Antonio Quintavalle** - ha fatto seguito all'approvazione del GDPR, a testimonianza della rilevanza e dell'urgenza di una problematica che proietta la cyber security, applicata alla tutela dei dati personali, in cima all'agenda delle istituzioni e dei governi".

Una materia bollente

La materia è bollente e in continua evoluzione. Nuove discipline si fanno strada mente siamo proiettati nel territorio ancora inesplorato del *Brain-raiding*, che introduce strumenti in grado di leggere il pensiero, e di interpretare la superficie, che credevamo insondabile, delle motivazioni profonde che animano il soggetto, fino a toccare il foro intimo della coscienza, da cui sgorga la sorgente dell'agire autonomo. "Abbiamo accettato supinamente dopo l'11 settembre una compressione forte della nostra libertà di agire e di muoversi. Da quel momento anche se è cessato quel pericolo non siamo più tornati indietro, questo deve far riflettere sui percorsi da seguire in una società segnata da criticità ricorrenti. Quello che appare sempre più evidente - ha spiegato Guido Scorza – è la difficoltà a trovare un bilanciamento tra i diritti universali, la libertà e la sicurezza. Impresa ardua per ogni legislatore a qualsiasi latitudine si trovi ad operare, se pensiamo che sarà chiamato a ridisegnare il campo delle norme, entro cui si costruiscono quelle relazioni sociali, che fanno comunità e che sono alla base del nostro vivere civile. ■

Sfruttare i vantaggi del cloud nativo senza compromettere la sicurezza informatica aziendale.



CROWDSTRIKE

Autore: Luca Nilo Livrieri, Manager, Sales Engineering - Southern Europe

Il report IDG's Cloud Computing Study 2020 analizza l'impatto del cloud computing sull'IT aziendale e sottolinea come oltre il 90% delle imprese operi, almeno in parte, proprio sul cloud. Tuttavia, i vantaggi dell'accessibilità e dell'efficienza portano anche alcuni svantaggi in termini di sicurezza informatica. Oggi, gli utenti possono accedere ad ambienti in cloud da qualsiasi dispositivo e da qualsiasi luogo, con una conseguente riduzione del livello di protezione rispetto all'utilizzo di reti locali. La domanda che la maggior parte delle aziende si pone è: come possiamo sfruttare i vantaggi del cloud computing senza compromettere la sicurezza informatica?

Migrazione al cloud-native e rischi in materia di cybersecurity

Le applicazioni cloud-native rappresentano la "nuova normalità" della tecnologia e sono state progettate specificatamente per aumentare la velocità, l'efficienza e la scalabilità dei servizi in cloud che stanno trasformando il modo in cui lavoriamo. La pandemia da Covid-19 ha accelerato l'adozione del cloud e dato alle imprese di tutto il mondo la capacità di poter rispondere in modo flessibile a esigenze in continuo cambiamento, oltre alla possibilità di gestire la forza lavoro dislocata ovunque e in remoto avvalendosi di servizi in cloud, come il miglior cloud storage.

Comprendere la sfida

Sebbene il termine "cloud-native" debba ancora essere adottato universalmente, il suo significato appare chiaro. Invece di negare i vantaggi delle piattaforme cloud intuitive con una basilare integrazione dell'architettura tecnologica esistente, un approccio cloud-native promuove la costruzione di un'infrastruttura specifica per il cloud, progettata per sfruttare al massimo le sue capacità uniche.

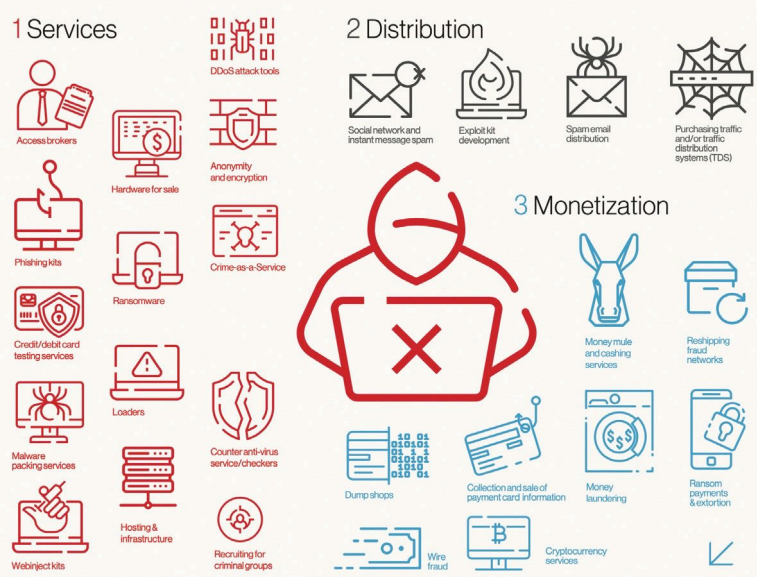
La sfida comune per coloro che adottano queste applicazioni cloud-native è quella di navigare in un modello di sicurezza a "responsabilità condivisa", dove la sicurezza viene determinata dallo sforzo congiunto tra fornitore e utente.

I fornitori di cloud computing sono responsabili del livello di sicurezza del cloud, nonché dell'infrastruttura e delle credenziali di accesso, mentre i clienti hanno anche la responsabilità di proteggere i dati all'interno del cloud. Le applicazioni cloud-native richiedono una propria strategia di sicurezza. Per questo motivo, i principali problemi si verificano quando i clienti adottano sul cloud lo stesso approccio di quando operano su tradizionali reti on-premise.

Altre problematiche riguardano le sfide IT più diffuse, come l'errore umano e lo Shadow IT, quando vengono effettuate modifiche e aggiornamenti o quando sono gli utenti ad aggiungere nuove risorse piuttosto che il dipartimento IT centrale, rappresentando una minaccia per l'ambiente cloud che rimane incustodito e vulnerabile agli attacchi.

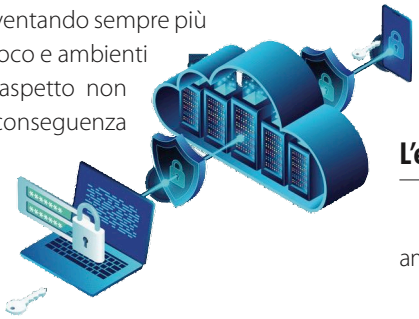
In questo scenario, oltre a dover affrontare minacce di tale portata, le aziende devono saper proteggere completamente il loro ambiente cloud-native e saper mitigare il rischio crescente, oltre che sempre più complesso, di attacchi mirati al cloud.

Secondo il Global Threat Report 2021 di CrowdStrike, gli autori delle minacce si avvalgono sempre più spesso di tattiche di estorsione dei dati, dove i dati vengono ceduti soltanto a seguito di un riscatto che, sempre più frequentemente, coincide con il pagamento di somme di denaro elevate. Nel 2020, i servizi di Intelligence di CrowdStrike hanno rilevato 1.430 attacchi che hanno usato proprio tecniche di estorsione dei dati.



Spostare la sicurezza alle fasi iniziali di sviluppo

Quando si configurano applicazioni cloud-native per condividere file in modo sicuro, la sicurezza viene tipicamente lasciata alla fine del processo. Gli sviluppatori si concentrano sull'esperienza utente e sul design e, una volta che l'applicazione è pronta, viene consegnata al team di sicurezza per applicare le patch. Un processo che sta diventando sempre più irrealizzabile. Con così tanti elementi in gioco e ambienti cloud moderni così complessi, questo aspetto non può essere messo in secondo piano. La conseguenza per coloro che lasciano la sicurezza alla fase finale del processo può determinare l'incompatibilità (l'applicazione rimarrà così senza protezione), costi aggiuntivi importanti e ritardi dovuti alla riconfigurazione dell'intero ambiente.



La soluzione è dunque quella di passare ad un approccio "shift left" alla sicurezza, collocandola il più possibile nelle fasi iniziali del processo di sviluppo, affinchè possa assumere un ruolo primario nello sviluppo dell'applicazione, anziché essere applicata a prodotto finito.

L'integrazione dei team di sicurezza dovrebbe essere prioritaria nella pipeline CI/CD. Lavorando al fianco degli sviluppatori, gli addetti alla sicurezza sarebbero in grado di incorporare i processi di sicurezza in qualsiasi fase dello sviluppo del prodotto, assicurandosi che le patch siano intuitive e rilevanti.

Oltre ai chiari benefici in termini di sicurezza, basarsi su un approccio "shit left" consente alle imprese di accelerare il roll-out e di ottenere una maggiore efficienza dei costi. Infatti, affrontare i problemi legati alla sicurezza nella fase di progettazione può essere sei volte più conveniente rispetto alla fase di implementazione e 15 volte rispetto a quella di test.

L'evoluzione della sicurezza in cloud

Quando le aziende scelgono di proteggere i loro ambienti cloud, l'approccio tradizionale si basa su tre livelli:

- Cloud Access Security Brokers (CASBs), agiscono come un checkpoint di sicurezza automatico tra le applicazioni cloud e gli utenti, monitorando il comportamento di questi ultimi e mitigando il rischio di furti di dati.

BIO

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

- Cloud Security Posture Management (CSPM), previene le configurazioni errate e supporta la conformità in tutte le infrastrutture cloud, registrando continuamente le violazioni di conformità e le risposte agli incidenti.
- Cloud Workload Protection (CWP) protegge la distribuzione e il funzionamento di tutte le applicazioni attraverso la rete cloud.

Tuttavia, mentre l'intento di proteggere la rete è positivo, la realtà è che questi prodotti separati, spesso rilasciati da vendor differenti, raramente si integrano

in modo efficiente o totale. Implementare soluzioni di questo tipo comporta una mancanza di visibilità end-to-end attraverso il cloud, nonché "punti ciechi" nella sicurezza della rete, che lasciano le aziende molto vulnerabili agli attacchi.

L'adozione di infastrutture cloud-native sta crescendo, così come la domanda di stack di sicurezza completi e integrati che includono vantaggi sia in termini di CSPM sia CWP. Tale tendenza ha portato allo sviluppo di Cloud-Native App Protection Platforms (CNAPPs).

Come suggerisce il nome stesso, le CNPPs forniscono il livello ottimale di protezione per l'infrastruttura cloud-native in ogni fase del ciclo di vita, dallo sviluppo al funzionamento. Questa protezione completa ha trasformato il modo in cui le imprese sono in grado di accedere, operare e proteggere il loro ambiente cloud.

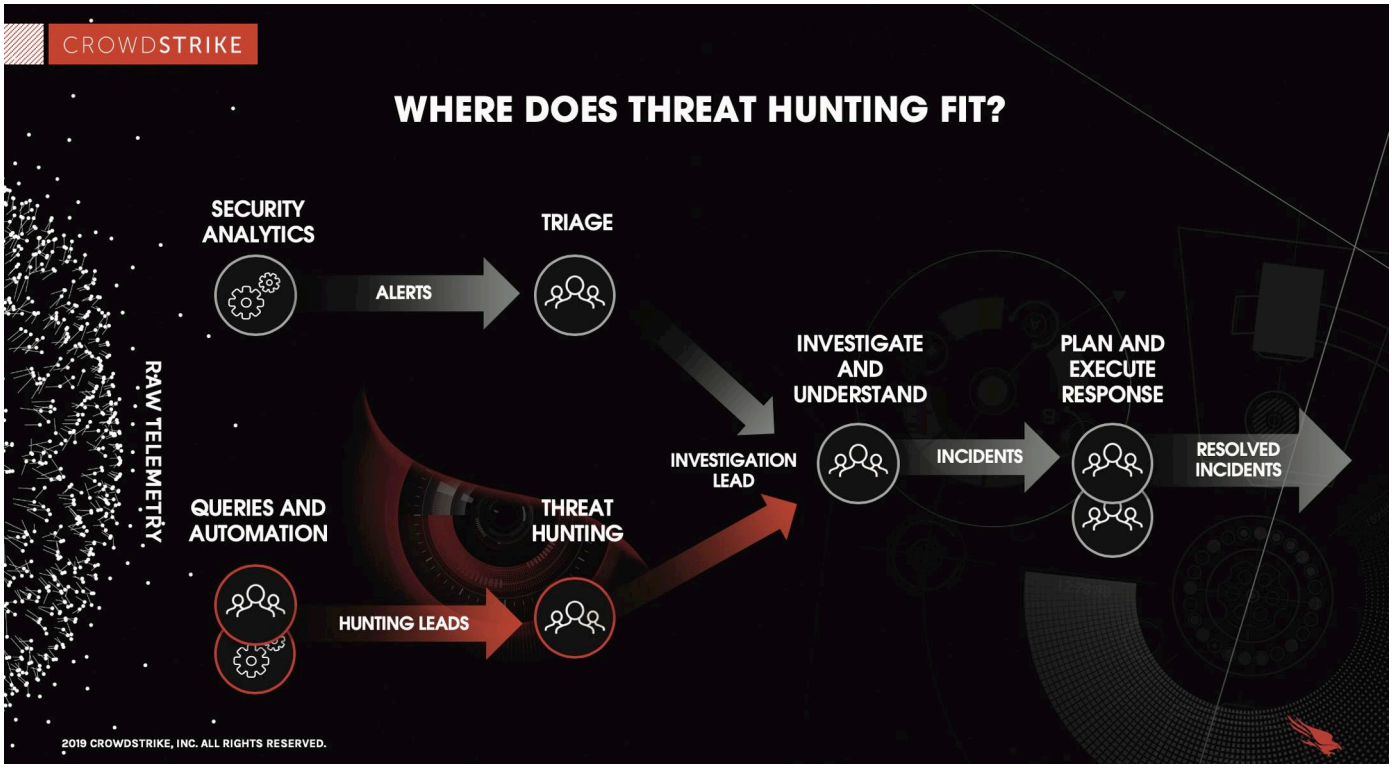
I dati analitici precedentemente raccolti sono ora comodamente accessibili in un unico ambiente e i team di sicurezza hanno una visione efficiente e a 360 gradi sull'attività, oltre ad essere in grado di fornire maggiori dati contestuali sulle potenziali minacce alla sicurezza.

Inoltre, le CNAPPs eliminano l'errore umano che può verificarsi quando si integrano soluzioni di sicurezza separate. Questo tipo di configurazione errata rappresenta il 64% di tutti gli incidenti causati dall'errore umano: l'eliminazione di tali "punti ciechi" offre ai team di sicurezza maggiore vantaggio.

L'insieme di questi elementi porta ad una riduzione dei costi associati all'integrazione di più soluzioni da diversi fornitori, oltre ad una riduzione della richiesta di supporto sui team IT occupati. Coloro che desiderano godere dei vantaggi di una soluzione CNAPP dovrebbero cercare prodotti che soddisfino determinati criteri.

La piena integrazione di CSPM e CWP in una console di gestione cloud-native offre agli utenti una sicurezza completa e una visibilità totale sullo stato del loro ambiente. Inoltre, sfrutta la potenza del machine learning (ML), dell'intelligenza artificiale (AI), degli indicatori di attacco (IoA) e della tecnologia di rilevamento analitico e comportamentale.

In combinazione con il supporto da parte degli esperti in threat hunting, una strategia di questo tipo dà alle aziende una protezione continua in fase di esecuzione. Le aziende dovrebbero anche chiedere di avere una visibilità end-to-end sul ciclo di vita del prodotto e la protezione per i container on-premises e serverless, salvaguardando tutti gli aspetti dei loro flussi di lavoro in cloud. ■



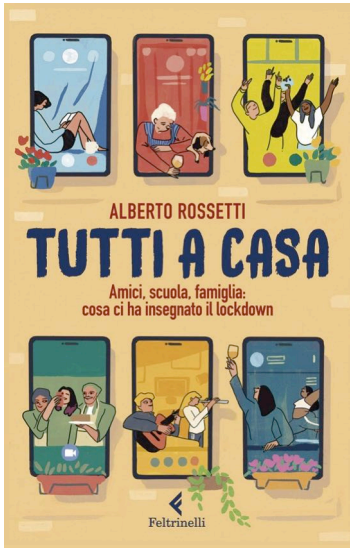
Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.

Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

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

www.itu.int/cop

Alberto Rossetti, *Tutti a casa. Amici, scuola, famiglia: cosa ci ha insegnato il lockdown,* Ed. Feltrinelli



Uno sguardo inedito sulla "generazione coronavirus"

La pandemia ha cambiato radicalmente le nostre vite. Una circostanza imprevedibile e drammatica, è entrata nella storia rappresentando uno spartiacque soprattutto per le generazioni più anziane, che avevano dimestichezza con un Pianeta diverso. Quali saranno le conseguenze di questo choc è presto per dirlo, così come difficile sarà anche per i più giovani riprendere "il filo del discorso". Le scuole hanno chiuso i battenti, sale giochi deserte, palestre abbandonate, luoghi di ritrovo "evaporati", è stato proibito dalla legge la frequentazione di amici e conoscenti. La discussione sulla opportunità e sulla durezza di questo stop ha visto impegnate le "teste d'uovo" più celebri, ma al di là del dibattito spesso accademico come hanno vissuto tutto questo o diretti interessati? Vivere un'esperienza complessa come la pandemia nelle diverse stagioni della vita che cosa comporta? Alberto Rossetti psicoterapeuta che si occupa di adolescenti e adulti e che cura da sempre progetti rivolti ai ragazzi, ha avviato un'indagine sul campo, intervistando i ragazzi. Sì proprio "i nostri figli" a cui di punto in bianco è stato proibito di andare a scuola (e persino a uscire di casa), di incontrare gli amici, di condurre insomma quella normale vita di relazione, che era la vita di tutti prima che arrivasse quel maledetto febbraio del 2020. Il risultato di questa indagine ha preso la forma del saggio: *Tutti a casa. Amici, scuola, famiglia: cosa ci ha insegnato il lockdown,* in cui vengono riassunte le risposte che i ragazzi hanno dato alle sollecitazioni dello studioso, che ne ha raccolto le testimonianze apparse su molteplici canali della giostra multimediale: social network, podcast, articoli a mezzo stampa. "Cronache della pandemia" è quello che emerge, in un contesto segnato dalla didattica a distanza, che ha reso discontinuo il confronto interpersonale, ha prosciugato ogni traccia di socialità, modificando nella sostanza il dialogo e i rapporti tra compagni di classe, amici, professori. educatori hanno molto da imparare dalle esperienze riannodate in queste pagine. Le confessioni a cuore aperto dei giovani, le manifestazioni di disagio, che si intrecciano con la volontà di ricominciare, le ansie, le speranze, l'esigenza forte di un ritorno alla normalità, che speriamo tutti sia ormai dietro l'angolo, sono momenti di un viaggio che apre il sipario su una giovanissima e ancora poco conosciuta "generazione coronavirus", il cui profilo dovrà essere **Le "cronache" non si rivolgono solo a ragazzi, anche se sono loro i protagonisti di un'esperienza complessa e per molti aspetti destinata a rimanere unica, perché anche genitori ed** compiutamente negli anni a venire. ■

Stefano Fratepietro, *Non è un libro per hacker,* Ed. Dario Flaccovio

La *digital forensics* nell'orizzonte del rischio informatico

Non è un libro per hacker attraversa la storia della digital forensics italiana, la scienza che si occupa di recuperare, ricostruire e repertare, nell'ambito delle indagini di polizia, il materiale presente nei dispositivi digitali legati a un crimine. Collocabile al culmine di quindici anni di esperienza dell'autore in materia di informatica forense e cyber security, il saggio riporta analiticamente e minuziosamente numerosi casi investigativi legati alle indagini di digital forensics, insieme ad alcune storie che illustrano con precisione quello che può accadere nei più oscuri meandri del web.

Pugliese di origine, Stefano Fratepietro ha affinato le competenze e svolto la sua professione in questo delicato ambito a Bologna, dove ha scoperto avventure "da film", che hanno per tre lustri attraversato la sua vita, intrecciandosi con la cronaca giudiziaria. Per quanto sovente sorprendenti, gli avvenimenti che si raccontano nel libro sono spiazzanti e al contempo autentici, con il risultato che il lettore è trascinato in un caleidoscopio di fatti incredibili, che si consumano tra un'indagine sul computer dell'ex dirigente di una multinazionale e un'investigazione su impensabili attacchi informatici. Il linguaggio adottato dall'autore si caratterizza per uno stile divulgativo, risultando comprensibile a una vasta platea di fruitori, ed è questo un pregio aggiuntivo di questa interessante iniziativa editoriale, che ha le carte in regola

per contribuire a diffondere una sempre maggiore consapevolezza circa i rischi connessi all'uso sempre più diffuso delle tecnologie digitali. Maturare una visione sul peso determinante che può rivestire la *computer forensics* oggi va di pari passo con l'esigenza crescente di affidare questa disciplina in mano a professionisti tecnicamente preparati ed eticamente responsabili, al fine di tutelare al meglio sia gli individui che le aziende, che rappresentano il target più diretto degli attacchi di *cybercriminali* sempre più rapidi, organizzati e senza scrupoli. ■

Adam Grant, *Essere originali. Come gli anticonformisti cambiano il mondo,* Ed. Hoepli

Il coraggio di quel "primo passo" che può cambiare l'esistenza

Questo lavoro di Adam Grant, tra i venticinque manager più influenti del mondo, autore da sempre molto attento ai cambiamenti, si caratterizza per originalità e anticonformismo. L'autore sollecita noi lettori a farci promotori delle migliori idee, seguendo gli esempi virtuosi in svariati campi, dalla politica allo sport, dall'imprenditoria alla tecnologia, di persone che hanno ottenuto grandi risultati capovolgendo il punto di vista dominante. Andare controcorrente, staccarsi dal *main stream*, superare di slancio visioni ormai obsolete, può essere decisivo. Esistono dei rischi quando si agisce staccandosi dalla massa per andarle addirittura contro, la reputazione o la carriera possono risentirne. L'autore si basa su sorprendenti studi scientifici e soprattutto su esempi individuali illuminanti, sfatando il mito secondo cui gli anticonformisti di successo sarebbero naturalmente portati a esercitare la leadership e ad affrontare il rischio. L'originalità può appartenere a chiunque, ognuno di noi può individuare opportunità di cambiamento, seguire una buona idea, sconfiggere la paura e i dubbi, non lasciarsi ridurre al silenzio da convenzioni e regole convenzionali e superate. Nel libro di Grant viene analizzato, in particolare, il successo di un imprenditore che promuove le sue startup elencando le ragioni degli investitori, si racconta anche di una dipendente di Apple che ha sfidato Steve Jobs pur trovandosi molto al di sotto nella gerarchia aziendale, di un'analista che ha ribaltato il dogma della segretezza nella CIA; di un miliardario e mago della finanza che decide di licenziare i dipendenti che non sono capaci di criticarlo abbastanza; di un produttore cinematografico che, con una sola domanda, ha permesso che venisse realizzato il primo film di animazione Disney basato su una storia originale. Una raccolta straordinaria di casi e fatti che fanno vedere come si può reagire al "gregge" e usare la propria testa. Alla fine della lettura si vede molto bene come anche le persone originali vivono le stesse insicurezze e le stesse paure di tutti noi, con la decisiva differenza che di fronte alle difficoltà la loro reazione non è la paralisi, perché sono capaci di trarre nuova forza dalle avversità e di superarle. *Essere originali* come suggerito dal titolo, vuol dire, in conclusione, affinare gli strumenti per realizzare i progetti, per mettere in campo idee vincenti e soprattutto per trovare il coraggio di fare il primo passo, che può cambiare l'esistenza. ■

Rapporto Censis

Vulnerabilità e irrazionalità. La società italiana in precario equilibrio

C'è una vulnerabilità che attraversa la società tecnologica, che non riguarda solo gli apparati digitali, come sarebbe facile dedurre, ma il corpo collettivo nel suo complesso che sta tentando di operare una strana fuga verso la magia e l'occultismo. La componente irrazionale si è infatti infiltrata in noi, assumendo le forme dello scetticismo e del rifiuto del dato scientifico. Questo singolare *"marcatore identitario"* dell'Italia di oggi, risulta dalla nitida fotografia scattata dal 55° Rapporto del Censis. "Accanto a una maggioranza che potremmo definire avvertita e saggia – spiega il direttore generale **Massimiliano Valerii** – una componente significativa della società italiana sta perseguendo una sorta di fuga dalla realtà, appigliandosi alla magia, al sortilegio, alla superstizione. Basti pensare che quasi il sei per cento degli italiani (circa tre milioni di persone) ritiene che il covid non esiste, uno su dieci che il vaccino sia inutile, mentre il trenta per cento che il vaccino sia un farmaco sperimentale. Siamo, insomma, tutti delle cavie quelli che ci sottoponiamo a questa discutibile pratica". Si tratta di numeri importanti che fanno comprendere come l'emergenza sanitaria, tra i tanti guasti causati, ha anche generato una sfiducia negli strumenti della ragione e nel metodo scientifico di ricerca della verità, che rischia di condannarci a una posizione di arretratezza. Le radici di tale atteggiamento oscurantista non sono nuove. Basti pensare che il 5,8% degli italiani è sicuro che la Terra sia piatta, uno su dieci continua a pensare che lo sbarco sulla luna sia stato solo frutto di un abile fotomontaggio televisivo, il 19% che lo standard di trasmissione 5G serva solo a controllare menti e persone, mentre quasi il quaranta per cento della popolazione ritiene che il crescente flusso migratorio, che sta scompaginando gli equilibri del pianeta, sia prodotto di un disegno di sostituzione etnica, coltivato da élite globaliste, animate da oscuri disegni di potere.

I "rendimenti decrescenti" degli investimenti sociali

Questa strana febbre dell'irrazionale non ha solo una matrice psicologia, vi sono ragioni storiche ed economiche profonde che la alimentano. Il rancore, tratto prevalente dell'Italia impoverita dalla crisi finanziaria che ha avuto origine dal crollo della Lehman Brothers è via via tramutato in quello che Giuseppe De Rita ha definito il *"Sovranismo psichico"*, preludio al gran rifiuto del discorso razionale, che è la nuova malattia con cui dobbiamo fare i conti. Una negazione così netta della modernità non era mai avvenuta. È probabile che il pensiero neo-scettico tragga la sua linfa dal rendimento decrescente degli investimenti sociali. Il sistema della formazione e dell'educazione è la spia più eloquente, come confermano i livelli di disoccupazione, l'amplissima fascia di NEET, fatta di tanti giovani che non lavorano e che non cercano occupazione. "Il rischio più grande – prosegue l'analisi di Valerii – è che si verifichi un rimbalzo di quelle fragilità e di quelle vulnerabilità che costituiscono un grave pericolo per il nostro sistema paese".

A preoccupare è lo scarso impiego del capitale umano che rischia di vanificare l'iniezione di denaro pubblico programmata dal PNRR. Se mancassimo questo appuntamento, parlare ancora di valore intrinseco delle scelte razionali sarebbe inutile, con tutte le tragiche conseguenze del caso. Bisogna fare in fretta e bene, le cose che ci vengo o chieste dall'Europa. La vulnerabilità di cui parla ***Cybersecurity Trends*** in questo numero non è poi così lontana da quella evidenziata dal Censis. La transizione digitale, che porta con sé la messa in sicurezza di reti e sistemi non può certo conciliarsi, con il rifiuto del metodo scientifico, né tanto meno con la scarsa propensione alla formazione che si registra in molti ambiti della nostra società. "La transizione per non essere un passivo "trascinamento" un lasciarsi portare da forze eteronome, ha spiegato in apertura della presentazione del rapporto il Presidente del CNEL Tiziano Treu, deve essere una transizione fondata su una progettualità trasversale, che ha bisogno di una consapevolezza diffusa per arrivare a un risultato tangibile". Non possiamo accontentarci del minimo sindacale, serve insomma un'idea paese rispetto a cui le classi dirigenti devono rispondere.

"Giù la maschera"

Per non "perdere il filo" e rimanere agganciati ai grandi processi di trasformazione in atto, lo studio del Censis prova a riassumere un crono programma che prende le mosse dalla transizione digitale, "simbolo – si legge nel Rapporto - della sfida tecnologica e dell'innovazione che attraversa le grandi società globali.

"L'adattamento continuato non regge più – è la riflessione di Giorgio De Rita segretaria generale del Censis - il nostro complessivo sistema istituzionale deve ripensare sé stesso. Siamo di fronte a una società che potrà riprendersi più per progetto che per spontanea evoluzione. La ripresa dello sviluppo è la prima strutturale richiesta che la società esprime in termini di progetto unitario. Basti guardare l'enfasi posta in questi mesi sul superamento delle più favorevoli ipotesi di crescita del PIL, la sopravvalutazione del ciclo di rimbalzo dei consumi interni, la fiducia posta nella capacità dei soggetti e dei fondi pubblici di annientare gli effetti della crisi. Tutti segnali che indicano un'aspirazione collettiva e condivisa di risalita, se non di ricostruzione".

La transizione demografica alle nostre latitudini si intreccia con il fronte della riflessione sul lavoro che rimane un'emergenza e un fronte caldo per la nostra economia e per il nostro futuro. "Il riposizionamento delle competenze in uno scenario produttivo e dei servizi radicalmente mutato, sfugge ancora alla sensibilità dell'opinione corrente. Il disallineamento tra domanda e offerta di lavoro, la dispersione di opportunità per mancanza o inadeguatezza delle competenze necessarie in questa nuova fase di ripartenza, non è un tema nuovo, ma oggi è al centro di un rinnovato bisogno collettivo". Sul terreno di questo bisogno dare risposte rappresenta la vera priorità. Non sono ammessi tatticismi, né ambiguità, risulterà più utile liberarsi della "maschera" che nasconde la tentazione, sempre presente, all'*"acquietamento del pensiero"* che, come ci ha insegnato Pirandello, assume spesso le sembianze di quella "corda civile", che si nutre solo di forme, che non modifica l'esistente, accontentandosi di subire passivamente fatti ed eventi. ■

Gian Luca Comandini

Da Zero alla Luna
Dario Flaccovio Editore

Una rivoluzione che sta cambiando il mondo

Blockchain è un termine critico con cui oggi devono misurarsi non solo gli addetti ai lavori e gli esperti della cybersecurity, ma la società nel complesso delle sue articolazioni. Siamo, infatti, di fronte a un'innovazione che sta cambiando radicalmente il mondo. Una tesi e un messaggio chiaro è quello che arriva da Gian Luca Comandini, giovane talento definito da Forbes tra gli under 30 più influenti del Paese. *"Da zero alla luna" (ed. Dario Flaccovio)* è un saggio/manuale, utile e brillante, che consente al lettore di entrare nell'universo della tecnologia, senza smarrirsi. Il titolo fa pensare alla conquista di una meta irraggiungibile, la luna è, da sempre, metafora del desiderio, della conquista, ma anche dell'ignoto, entità

impenetrabile che suscita interrogativi esistenziali radicali e profondi: *"che fai tu luna in ciel? Dimmi, che fai/ silenziosa luna?…"*, si chiedeva il pastore errante nell'Asia di Leopardi. Comandini non arretra mai di fronte a tali interrogativi, maneggia, infatti, la materia informatica con padronanza, senza però mai dimenticare di esercitare l'umiltà socratica nella trattazione. Per questo utilizza sempre una scrittura semplice e diretta. Con metodo si preoccupa di chiarire il vocabolario dell'innovazione, senza di cui non si potrebbe comprendere la natura del cambiamento in atto. *"Blockchain – spiega l'autore – non è altro che una sorta di libro mastro, distribuito e gestito da una rete di computer, ognuno dei quali ne possiede una copia"*. Il bitcoin è figlio di questa tecnologia, non si potrebbe spiegare senza far ricorso alla rete e al sistema degli algoritmi che governa gli scambi tra i nodi che la compongono.

Non c'è da stupirsi in merito. L'uomo ha sempre avuto bisogno di controllare le transazioni, di usare una moneta per praticarle, di escogitare sistemi per garantire la sicurezza di ogni passaggio economico. L'autore compie un salto nel 1400, spostando la narrazione su un'isola della Micronesia, dove nasce una prima forma di moneta. Fiducia, trasparenza, sicurezza, catena del controllo decentralizzata, gli abitanti di Yap (questa l'isola in questione n.d.r.) avevano già molto chiare in mente le connotazioni essenziali, che avrebbero poi rappresentato una costante nella storia economica.

Il rapporto tra l'uomo e il denaro è sempre identico a se stesso, fin dai primordi della civiltà ha mantenuto alcune precise connotazioni. Il filosofo Carlo Sini ha tratteggiato questo binomio con grande lucidità in occasione di una recente lectio magistralis tenuta all'Università di Milano: *"l'uomo è portato naturalmente allo scambio. Adam Smith si chiedeva da dove venisse questo forte impulso. Aristotele è stato probabilmente il primo pensatore a dirlo in maniera compiuta: lo strumento dello scambio è connaturato al linguaggio. E'*

Bibliografia - Cybersecurity Trends

con la specie umana che comincia infatti il segno linguistico e da quel momento cambia la storia del mondo… Il denaro non è un linguaggio, ma condivide con il linguaggio la profonda natura del segno, cioè di una cosa che sta al posto di un'altra, che la può rappresentare e vicariare nello scambio. Come non c'è cosa che non sia rappresentabile con la parola, allo stesso tempo non c'è cosa che non si possa comprare cioè scambiare col denaro. Il problema vero è decidere e comprendere al posto di che cosa sta il segno del denaro: risposta che, al di là di soluzioni "tecniche", resta tuttora problematica.".

Il sipario aperto dal filosofo si può proiettare negli ambienti più avanzati della tecnologia, costituiti da bitcoin, criptovalute, che si muovono nelle reti interconnesse. Registrare, criptare, rendere non replicabile, erano aspetti essenziali ieri, lo sono ancora di più nella contemporaneità, se si considera come si siano esasperati i profili di rischio nella dimensione virtuale dell'esistente. Anche le società arcaiche avevano deciso di "segnare il debito", perché rimanesse traccia. Probabilmente da quel momento l'uomo diventa irrimediabilmente "schiavo" di una scrittura cioè di un impegno a "saldare i conti" che bisognerà "onorare" indipendentemente dai casi della vita e del destino". A compensazione di questa visione negativa il filosofo sente il bisogno di precisare "bisogna aggiungere che il denaro è anche il fattore di massima liberazione del gruppo umano dal bisogno economico immediato e dalla miseria, ovviamente quando viene usato correttamente". Ed è proprio sull'utilizzazione corretta che possiamo recuperare il pensiero di Comandini, che dedica un capitolo al pericolo dell'ignoranza, che colmata e cancellata se vogliamo che il razzo ci porti sulla luna. Non ci sono altre possibilità: non possiamo fermare il vento con le mani, l'innovazione va praticata, ma dobbiamo comprendere con senso di responsabilità che quando parliamo di *blockchain* ci troviamo di fonte al trend tecnologico che sarà predominante nel secolo a venire, insieme all'IA, l'Internet delle cose, la corsa allo spazio la nanorobotica, i computer quantistici, e al biotech. "Chi come banche e aziende ricorda nella conclusione l'autore - avevano guardato con scetticismo a questa tecnologia emergente, oggi sta investendo 20 volte di più di quanto negli anni 90 era stato investito su Internet".

"Esci dal presente ed entra nel futuro ti aspetto, ci vediamo sulla Luna il razzo e in partenza!" Facciamo nostro l'auspicio finale, che si innesta nella cultura della collaborazione, che è più importante della competizione. La sfida sarà quella di tracciare un percorso verso il domani dove sarà ancora l'intelligenza umana a guidare la macchina, al fine di conferire il necessario orizzonte di senso al prepotente sviluppo della scienza e della tecnologia, che altrimenti finirebbe con l'annichilire la libera volontà dell'individuo. ■

Bibliografia a cura di Massimiliano Cannata

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

15 Dicembre 2021

XII Conferenza Nazionale sulla Cyber Warfare

CWC 2021 CYBER WARFARE CONFERENCE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE:

Funzione di Guida per la Resilienza Cyber ed Opportunità di Sviluppo Economico del Paese

ISCRIZIONE GRATUITA

WWW.EUCACS.ORG

evento riconosciuto

ICMQ CERSA

ICMQ S.p.a. – B.U. CERSA riconosce 3 crediti
per Professionista della security UNI 10459:2017
validi per il mantenimento della certificazione

promosso da:

EUCACS – European Center for Advanced Cyber Security

CSSII Centro universitario di Studi Strategici, Internazionali e Imprenditoriali

Cyber Academy

ideato d'intesa con:

inthecyber group

con la collaborazione di:

Net Consulting 3 – Empowering your Digital Business

aipsa

Clusit – Associazione Italiana per la Sicurezza Informatica

CERSA

sponsorizzato da:

accenture

Cisco

Capgemini

RSA

TINEXTA CYBER

TIM

Google Cloud

Il fattore umano nella cyber security

Valori e strategie da costruire insieme

A cura di Nicola Sotira

MANAGEMENT

TOOLS

GLOBAL CYBER SECURITY CENTER

FrancoAngeli