# Cybersecurity Trends

Edizione italiana, N. 2 / 2022

INTERVISTE VIP:

NIR ZUK
GIOVANNI MARIA FLICK
MARCO RAMILLI
LUCIANO FLORIDI

ISSN 2559 - 1797
ISSN-L 2559 - 1797

## Folder Centrale: Automazione

# 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

# Automazione chiave nei processi cyber.

Autore: Nicola Sotira

In un dominio sempre più digitale nel quale uno dei temi rilevanti è la l'esperienza utente, molti aspetti della gestione e dell'assistenza informatica sono ancora molto poco digitali e spesso altamente manuali, e l'area afferente alla cybersecurity non fa eccezione. In molti casi l'attività umana è sempre necessaria; occorre un essere umano flessibile e pensante per poter prendere delle decisioni e chiudere il task.

## 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.**

Tuttavia, quando possiamo automatizzare le attività di sicurezza e far sì che siano le macchine a svolgere il lavoro, scopriamo una pletora di vantaggi rispetto ad una serie di processi guidati dall'uomo. Uno dei vantaggi nell'utilizzo dell'automazione è che, una volta che gli script e il software di automazione sono stati testati, la probabilità di errore è notevolmente inferiore rispetto a un approccio manuale.

Questo vale anche per gli approcci manuali che utilizzano un doppio controllo: l'autocompiacimento è comune, generalmente in proporzione a quanto è noioso il lavoro, e anche revisioni ragionevolmente coscienziose possono subire errori, in particolare durante i periodi di lavoro sotto pressione o nell'emergenza.

Inoltre, tutti noi ci siamo resi conto che il digitale non è che apre alle ore 9 e chiude alle 17. Il digitale è funzionante h24 per 365 giorni all'anno. Uno dei vantaggi dell'automazione e che può funzionare ogni volta che lo si desidera, senza bisogno di pagare gli straordinari e senza richiedere orari impossibili.

Come abbiamo anticipato, a prescindere dall'automazione, ci sarà sempre bisogno di *"un essere umano e della sua intelligenza"*. Tutti noi preferiamo svolgere un lavoro interessante e coinvolgente piuttosto che un lavoro noioso e banale; quindi, possiamo usare l'automazione non solo come mezzo per smettere di fare il secondo, ma come opportunità per svolgere del lavoro più stimolante.

Le competenze necessarie per introdurre l'automazione nei processi di cybersecurity si sono evolute in modo significativo e continueranno a farlo. Se fino a pochi anni fa le competenze fondamentali dell'automazione erano la progettazione di algoritmi e lo sviluppo di software, oggi il compito è molto più complesso e richiede una comprensione della scienza dei dati e dell'analisi statistica, per non parlare della conoscenza e dell'esperienza specifica degli strumenti e delle piattaforme di Machine Learning (ML) che vengono utilizzate per implementare le automazioni stesse. L'automazione moderna, e quella del prossimo futuro, si discosta quindi in modo significativo dall'automazione tradizionale, offrendo un'interessante opportunità a chiunque sia in grado di addestrarsi o di apprendere autonomamente gli strumenti e le tecniche necessarie per implementare l'automazione basata su Intelligenza Artificiale e Machine Learning.

Queste nuove metodologie, se applicate in aggiunta agli onnipresenti strumenti di automazione tradizionali, ci offrono l'opportunità di far lavorare le macchine in modo efficace, mentre i cervelli umani si concentrano sui compiti difficili o impossibili da svolgere per le macchine. ■

# Senza automazione non ci potrà essere sicurezza.

## Intervista VIP con Nir Zuk.

Autore: Nicola Sotira

***"Zero trust" è uno dei temi oggi maggiormente dibattuti nelle conferenze che si svolgono in tutto il mondo. Qual è il suo punto di vista in merito?***

Zero Trust non è una tecnologia. È un concetto. I fornitori di sicurezza degli endpoint ti diranno che Zero Trust riguarda la sicurezza degli endpoint. Non puoi fidarti dell'endpoint senza la sicurezza dell'endpoint e i fornitori di gestione dell'identità ti diranno che è tutta una questione di identità che devi verificare. La mia visione è molto diversa in materia.


***In che senso, può spiegarlo in modo più dettagliato a Cybersecurity Trends?***

Applicare Zero Trust vuol dire attivare i medesimi controlli di sicurezza indipendentemente dalla situazione e dal caso d'uso.

Tradizionalmente adottiamo approcci diversi in base alle situazioni. Quando l'utente si trova in sede e tenta di connettersi a un'applicazione che si trova nel data center, facciamo operazioni molto diverse rispetto a quando l'utente è lontano dall'ufficio e l'applicazione si trova in un *cloud* pubblico. Qualora l'utente si trova lontano dall'ufficio e l'applicazione è collocata in un data center tradizionale, utilizziamo un collegamento in VPN. Se l'applicazione è in SAS, utilizziamo CASB. Questo vuol dire che eseguiamo controlli di sicurezza diversi con livelli di complessità differenti rispetto a parametri di affidabilità variabili che dipendono di volta in volta dall'utente e dall'applicazione.

Zero Trust riguarda la normalizzazione. Non importa quale sia l'utente, né dove si trovi, non importa come si connetta, che si tratti di SD-WAN o IPsec


### BIO

**Nir Zuk è il fondatore e Chief Technology Officer di Palo Alto Networks, il più grande fornitore di cybersecurity al mondo. L'idea alla base di questo prestigioso brand è quella di consolidare nel tempo sempre più funzioni di cybersecurity attorno a un'unica piattaforma, al fine di facilitare i clienti e di evitare loro di dover installare molti prodotti forniti da molti provider. In una unica piattaforma hanno a disposizione tutte le funzionalità necessarie. Zuk ha rilasciato a Cybersecurity Trends questa intervista in esclusiva.**

o MPLS o VPN client e così via, tramite proxy e qualunque sia l'applicazione, SAS cloud pubblico o privato, data center tradizionale.

***Quali sono i vantaggi connessi all'utilizzo di queste soluzioni?***

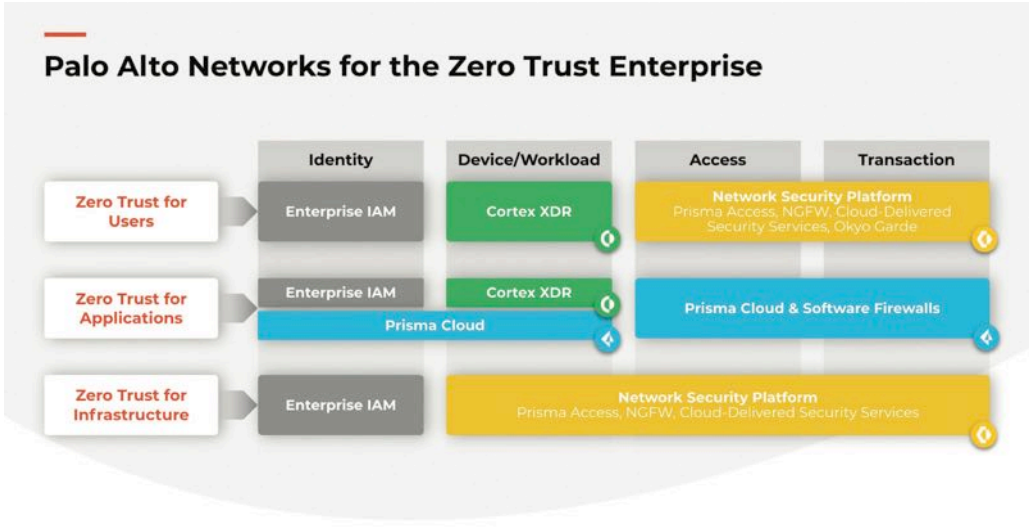
È una soluzione che innalza i livelli di sicurezza organizzativa e aziendale, rendendo anche più "semplice" e immediata la tutela degli asset, in quanto non prevede un firewall per gestire determinate situazioni, una VPN di accesso remoto per il CASB, il proxy etc. etc.

Ci troviamo per altro di fronte a un sistema integrato e quindi più economico. Mi riferisco a un qualcosa che chiamiamo accesso PRISMA, che in sostanza, è il nostro intero stack di sicurezza di rete distribuito nei data center in tutto il mondo. Siamo presenti in più di centoventi luoghi in tutto il mondo, tutti collegati con la rete privata.

Altro aspetto importante è stato determinato dal passaggio alla sicurezza applicata ai "margini" del *cloud*. Si chiama anche SASE, Secure Access Services Edge, e quindi non importa chi sia l'utente, né dove si trovi.

Non importa se si connette con SD-WAN all'Edge, o con IP sec, o con VPN client o con un elenco di client VPN o proxy o qualsiasi altro metodo una volta acquisito il loro regime di traffico all'Edge, viene elaborato allo stesso modo.

Questo ci fa capire che non importa quale sia l'utente, né i percorsi che intende seguire. Quello che noi tendiamo a utilizzare è in particolare il *peering* diretto per governare il traffico su applicazioni SAS, cloud pubblico, cloud privato, e sui data center tradizionali.




***Altra questione, di cui si discute molto in questo momento, sono le tematiche collegate agli autonomous SOC in stretta correlazione con l'avanzamento dell'automazione. Occorrono investimenti importanti, con rientri che sono tutti da valutare. Qual è il suo giudizio su questo che rappresenta un salto in avanti molto forte rispetto al passato?***

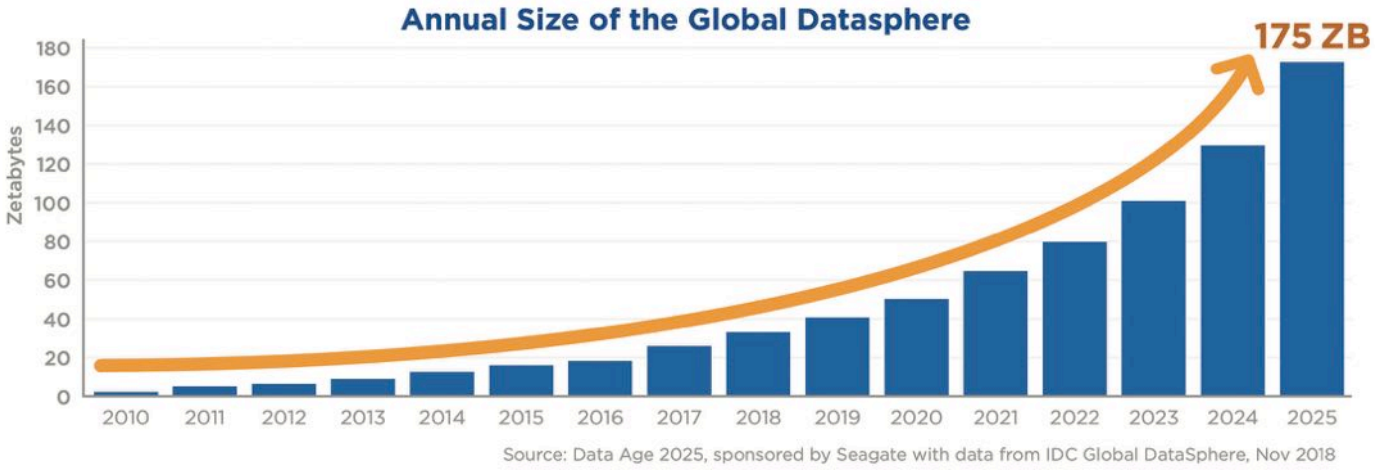
Prima cercherei di capire perché abbiamo bisogno di automatizzare i SOC. I SOC non riescono a esaminare tutti gli alert, cosa impossibile utilizzando le sole capacità umane di governo, misura e controllo. Pertanto, la maggior parte dei SOC filtra gli alert e gestisce solo quelli che è in grado di gestire. Applicando regole di correlazione, spesso sbagliate o insufficienti, un SOC tipicamente gestisce circa 50 alert a settimana a fronte di decine di migliaia di avvisi ricevuti. Ciò significa che potrebbe scartare e non analizzare gli alert realmente necessari per individuare i problemi prima che si verifichino.

***Le macchine intelligenti saranno sempre più al centro della cyber security, con quali conseguenze?***

Il trend è inevitabile, le prospettive incoraggianti. Abbiamo bisogno di macchine per fare sempre meglio il nostro lavoro. Se generiamo un avviso per qualsiasi motivo nella rete, sugli endpoint, nel cloud, nei server delle applicazioni, qualsiasi avviso che riguardi la gestione dell'identità e degli accessi, la scansione del codice, dobbiamo indagare a fondo le conseguenze che genera questo tipo di informazione. Quindi questo è il primo obiettivo dell'automazione del SOC. Così ogni qual volta che si verifica un problema ed è necessario eseguire una risposta agli incidenti, oppure se si verifica una violazione dei dati, il team di sicurezza è in grado di dire cosa è successo. Sono, anche, in grado di individuare le aree vulnerabili e i comportamenti degli "attaccanti"; quello che serve è poterli prevedere, come dicevo prima. L'automazione ci aiuterà molto in questo senso.

***Non si può però negare che esiste anche un problema di qualità, non solo di quantità dei dati. Non crede?***

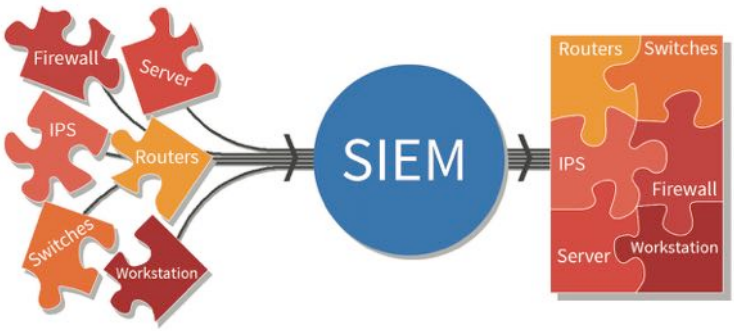
Assolutamente sì. Tutti vorremmo vivere in un mondo in cui possiamo raccogliere i dati di rete da un fornitore e i dati degli endpoint di cui abbiamo bisogno da un altro fornitore e quindi i dati del carico di lavoro cloud da




un terzo fornitore. Questo però non accade, perciò dobbiamo agire con consapevolezza e competenza. Teniamo presente che molti dati devono essere generati in base a ciò che si desidera fare di queste informazioni; perciò, occorre visione e strategia per governare i processi di automazione.

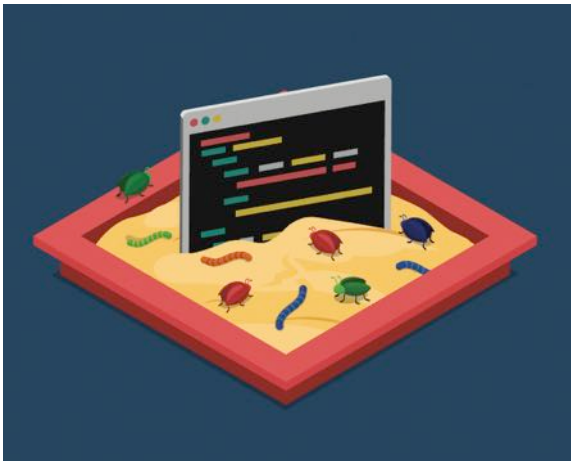
***Facile a dirsi ma difficile da attuare in ambienti multi-vendor. La difformità delle fonti richiede una gestione oculata, perché si ha bisogno di dati di altissima qualità, dati con dettagli diversi, diversi da quelli che vengono gestiti oggi dai SIEM. Spesso i dati non sono orientati alle macchine. Come si risolve questo problema?***

Sono d'accordo, difficile gestire in azienda problematiche come quelle che lei prospetta. Se poi guardiamo al mercato, altri interrogativi emergono. In Italia le piccole e medie imprese oggi sono la maggior parte. Anche io vivo in un piccolo paese in Israele, che dista circa tre ore di volo da Roma, che per dimensionamento delle imprese presenta caratteristiche simili. Non ci sono aziende molto grandi. L'automazione in questi contesti è l'unico modo in cui un'azienda di medie dimensioni, che non può permettersi di avere un SOC proprio, può fare sicurezza. L'esternalizzazione non funziona, l'esternalizzazione della sicurezza sposta i problemi su qualcun altro. Bene. Quindi, se sei una piccola impresa, hai ancora bisogno di cinque persone che esaminino le tue informazioni e gestiscano la tua sicurezza. Spostare su un outsourcer non aiuterà, sostituirlo con un software aiuterà. Posso fare un esempio perché sia più chiaro quello che dico.




***La ascolto…***

Circa 10 anni fa, siamo usciti sul mercato con la nostra sandbox, spiego meglio a cosa serve. Se si prende un file, per esempio un PDF che non si è mai visto prima, che una volta eseguito apre una "strana" connessione con un paese straniero è evidente che esiste qualche criticità. In prima battura la sandbox consente di inviare un avviso al SOC, un alert, che deve preludere a un'attività di *reverse engineering,* al fine di capire quali indirizzi IP devono essere bloccati, quali URL di dominio e via via con le altre procedure. Poche centinaia di clienti utilizzavano questo servizio fino a poco tempo fa. Abbiamo perciò deciso di automatizzarlo, con l'intento di prendere sotto osservazione qualunque "fenomenologia" sospetta si potesse verificare. Abbiamo così applicato il reverse engineering per capire automaticamente cosa doveva essere bloccato e di conseguenza quali informazioni inviare all'infrastruttura. Oggi abbiamo qualcosa come 50 o 60.000 clienti che lo utilizzano, i clienti sono motivati a utilizzare la sandbox perché è sicura e automatizzata, sarà questo il binomio vincente.



***Sono numeri eloquenti che parlano da soli. Quali scenari si aprono alla luce di queste importanti esperienze che state maturando?***

Se fino a venti anni fa mi avessero chiesto quanto tempo sarebbe occorso per creare un sistema sicuro, avrei detto un'eternità. Quando infatti pensi di aver implementato tutte le soluzioni scopri che prodotti e servizi utilizzati sono già vecchi, al momento in cui li si mette in opera. La complessità entro cui oggi ci

muoviamo non mi ha reso più ottimista, ma va detto che è cambiato il paradigma e la logica con cui si concepisce e si attua la sicurezza informatica, che viene attuata in larga parte con un SAS Software As Service, per cui non è necessario implementare. È evidente che questo assetto modifica molte cose. La sfida che abbiamo di fronte è la *governance* della *cybersecurity* nelle piccole e medie imprese, cosa attuabile solo attraverso l'automazione delle operazioni di sicurezza. Altra sfida nella sfida la bravura delle persone. Non si può prescindere dal fattore umano se si vogliono raggiungere livelli di performance adeguati degli apparati e sistemi di tutela aziendale.

***Prima di chiudere questa interessante chiacchierata non posso esimermi dal chiederLe: Come cambierà la sicurezza nell'immediato futuro?***

Non credo sia possibile prevedere come si comporteranno i "cattivi", non voglio nemmeno tentarlo. Quello che penso è che dobbiamo essere preparati a qualsiasi evenienza, come la più stretta attualità ci ha insegnato. Il futuro, e non dico nulla di nuovo, sarà basato sui dati, il che significa, che dobbiamo trattare con firme nei firewall, sull'endpoint e così via. Il rilevamento degli attacchi più sofisticati, come quelli alla catena di approvvigionamento, mirati a ciò che chiamiamo APT mette in gioco una grande capacità di elaborazione dei dati, che è l'unico antidoto che abbiamo per affrontare un cyber crimine sempre più organizzato e perciò temibile. Altro fattore cruciale è l'automazione dei SOC. Non credo che saremo in grado di fare nulla nella cybersecurity senza la realizzazione di un SOC autonomo, questo deve essere fatto nel giro di tre anni. Stiamo arrivando al punto in cui molti degli attacchi sono automatizzati, gli stessi avversari utilizzano il *cloud* per automatizzare gli attacchi. Spesso utilizzano il machine learning per conoscere gli obiettivi su Linkedin e sui social media e sferrare un'offensiva sui clienti, in modo completamente automatizzato.

***Potremmo dunque concludere dicendo che il* Cloud *è l'ultima frontiera?***

Non utilizzerei affermazioni categoriche, una cosa è certa: nel giro di pochi anni le persone non saranno in grado di affrontare queste tipologie di attacchi. Non mi stanco di ripetere che bisogna automatizzare reti e sistemi parlando di *zero trust*, abbiamo sottolineato i motivi per cui la sicurezza va spostata ai "margini" del cloud. Direi di più: in poco tempo gran parte della sicurezza di Internet verrà fornita dal cloud. Nessuna attrezzatura sarà allocata in sede. Come spesso accade abbiamo prima pensato alle applicazioni e all'infrastruttura, e poi alla sicurezza, con il risultato che anche nell'orizzonte del cloud, la sicurezza è in ritardo. Ma il nostro sguardo deve andare anche oltre.

***A cosa si riferisce?***

Al fatto che dovremmo iniziare a pensare al più presto alla *home security*. Ho passato la giornata in ufficio, fino alle 16:00 in Israele, poi ho continuato con i vari applicativi, a lavorare da casa in costante contatto con l'Europa, ma soprattutto con gli Stati Uniti. Se qualcuno volesse conoscere il mio indirizzo IP, ci metterebbe circa dieci minuti. Dal mio indirizzo al collegamento con il dark web, il passo è breve. Sono, infatti, certo che ci sono applicazioni non così sicure sull'XBox di mio figlio, la mia TV è potenzialmente una porta di accesso che ti porta a casa mia e poi sul mio pc. Quello che sto dicendo non è un esercizio accademico, ma descrive la quotidianità che ormai fa parte di noi. Lo Smart working è infatti un'ulteriore sfida che dovrà impegnarci, sarà la casa la prima e l'ultima frontiera da difendere. Anche su questo terreno il Cloud potrà aiutarci, perché oggi con i servizi SAS è possibile garantire la sicurezza, perché *l'home office*, e su questo credo che possiamo veramente chiudere, rappresenta ormai "il problema" per le aziende che intendono affrontare il futuro con buone *chances* di successo. ■

**CYBERSECURITY DIALOGUES**

- ROMANIA -

**8th Edition - September 21-22, 2022**

**Organized by:**

web for your business
swiss webacademy

NTT DATA

**Hosted by:**

CONSILIUL JUDEȚEAN
SIBIU

# A WAR-TORN POST-PANDEMIC WORLD: ATTACKS AT 360°.
# SOLUTIONS FOR SECURING YOUR BUSINESS.


**www.cybersecurity-dialogues.org**

**Under the aegis of:**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Embassy of Switzerland in Romania**

**In partnership with:**

1949.2019 COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Gendarmerie nationale

Centre de recherche de l'EOGN

POLICE GENEVE

CYBERINT

IGPR POLIȚIA ROMÂNĂ

GUVERNUL ROMÂNIEI

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

**Media partner:**

BURSA
ZIARUL OAMENILOR DE AFACERI

**Simultaneous translations:**

ACSB events

CMCS INTERNATIONAL

FIC Forum International de la Cybersécurité

ULBS
Universitatea "Lucian Blaga" din Sibiu

**Location:** Sibiu County Council - Parliament Hall, Str. Gen. Magheru, Nr. 14

**Live streaming upon inscription: www.bursa.ro**

# La nostra sicurezza è forte quanto la nostra capacità di gestirla: la necessità di Attack Path Management per il Cloud Ibrido.

Autore: Karl Buffin

Ora non è un segreto che le aziende siano cresciute e abbiano favorito l'adozione del cloud più velocemente di qualsiasi altro periodo precedente. Uno degli attori chiave nel guidare la missione delle aziende di tutto il mondo di digitalizzare è il COVID-19. La necessità di operazioni per tenere il passo con l'elevata domanda di accesso ha spinto le aziende ad accelerare i loro piani da pochi anni a mesi. Inoltre, il lavoro a distanza è ormai divenuta una pratica aziendale comune che complica

ulteriormente i problemi delle organizzazioni che proteggono le proprie risorse più critiche. Ciò è dovuto in parte al fatto che il nostro perimetro si è drammaticamente ampliato e, con un lato positivo, è quasi scomparso allo stesso tempo. Non è più sufficiente proteggere tutto ciò che si trova all'interno. Le aziende stanno sollevando e spostando i carichi di lavoro e le risorse critiche dall'on-premise al cloud e viceversa per soddisfare le esigenze degli utenti e dei servizi che li richiedono.

Nuovi gap di sicurezza vengono costantemente creati a causa di nuovi modi di lavorare in un ambiente ibrido. Gli aggressori informatici sfruttano questa modifica per ottenere il punto d'ingresso iniziale e violare

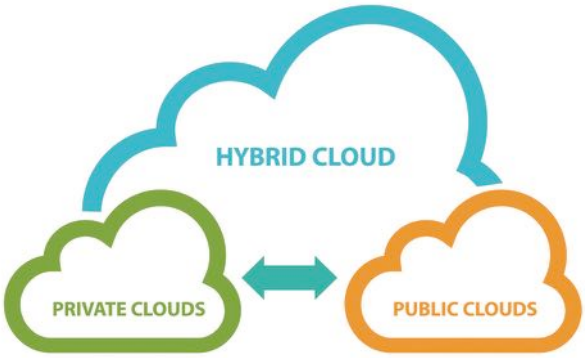
## BIO

**Attualmente Sales Director di XM CYBER, Karl Buffin ha iniziato la sua carriera in Gemalto come responsabile delle vendite, diventando presto responsabile delle regioni dell'Europa meridionale e del Medio Oriente. Ha lavorato per alcuni dei maggiori operatori di cybersecurity come SafeNet, Verisign e Symantec. Con oltre 20 anni di esperienza nel settore della sicurezza informatica, delle vendite e della distribuzione nella regione EMEA, Karl Buffin è stato Direttore Vendite per il Sud Europa di Skybox Security, prima di raggiungere XM CYBER.**

un'organizzazione sfruttando configurazioni errate, identità eccessivamente permissive, vulnerabilità ed errori umani.


Ma è chiaro il motivo per cui tutti si stanno spostando sul cloud. Offre maggiore agilità, migliore capacità di collaborare, un'infrastruttura IT minima da gestire, servizi evergreen (in particolare SaaS), prezzi prevedibili e ha il potenziale per una maggiore automazione. La ricerca mostra che il 90% delle organizzazioni utilizzerà effettivamente il multi-cloud o avrà un qualche tipo di strategia ibrida entro il 2022. È probabile che tu stia già utilizzando il cloud e, in caso contrario, sei sulla buona strada.

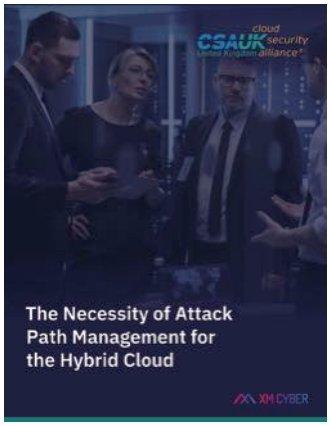
Indipendentemente da come gestisci la tua organizzazione, puoi sfruttare le informazioni dettagliate sul percorso di attacco per avere una visione chiara del tuo approccio alla sicurezza del cloud ibrido. Concentrare gli sforzi di sicurezza durante la fase di propagazione della rete per interrompere gli attacchi in corso prima che si verifichino produrrà il massimo ritorno sugli investimenti.




Per colmare il divario, XM Cyber ha pubblicato, in collaborazione con UK Chapter of the Cloud Security Alliance, un white paper pratico che esplora la necessità della gestione del percorso di attacco per il cloud ibrido di oggi.

Parliamo dell'importanza di comprendere i percorsi di attacco che un utente malintenzionato motivato può utilizzare per provare a compromettere i tuoi ambienti on-premise, multi-cloud e ibridi. La comprensione del percorso di attacco consente alle organizzazioni di identificare potenziali *choke points*, monitorare i requisiti e le debolezze dell'architettura per migliorare la propria postura di sicurezza generale.

Il cambiamento più influente che aiuterà a migliorare la tua postura di sicurezza del cloud ibrido è utilizzare la prospettiva dell'attaccante per vedere l'attacco prima che si verifichi mappando tutti i possibili percorsi di attacco e ottenendo una visione chiara dello stato di sicurezza nel tuo ecosistema di cloud ibrido. Concentrarsi sulle intersezioni chiave dove più percorsi di attacco convergono per sfruttare un asset critico, è molto più utile rispetto alla ricezione di un semplice alert su un singolo componente con un punteggio CVSS elevato valutato utilizzando il Common Vulnerability Scoring System (CVSS). Senza le informazioni sui percorsi di attacco seguiti dai threat actors e su come possono compromettere le tue risorse critiche, è difficile mantenere una postura di sicurezza elevata e avere il sopravvento sui tuoi avversari.




Ottieni subito il white paper *"La necessità di Attack Path Management for the Hybrid Cloud"* e ottieni le best practice per proteggere la tua organizzazione dagli attacchi informatici e aumentare la postura di sicurezza.

Scarica il white paper: https://info.xmcyber.com/whitepaper-csa-attack-path-management-for-the-hybrid-cloud ■

| | WITHOUT Attack Path Management | WITH Attack Path Management |
|---|---|---|
| Visibiity | Manually define Environment [VMs,devices, DB, criticak assets, etc.] | Easily defined and mapped with fast deployment [VMs, devices, DB, critical assets, etc.] |
| Analysis | Constantly and manually monitor environment according to least-priviliges, without any knowledge of best practices | Continuosly and automatically monitor environment against latest attack techniques [aligned with MITRE] |
| Action | First- hand knoweledge of risk remediation | Prioritized and guided remediation steps for highest risks. |

*© XM CYBER, The Necessity of Attack Path Management for the Hybrid Cloud, p. 17*

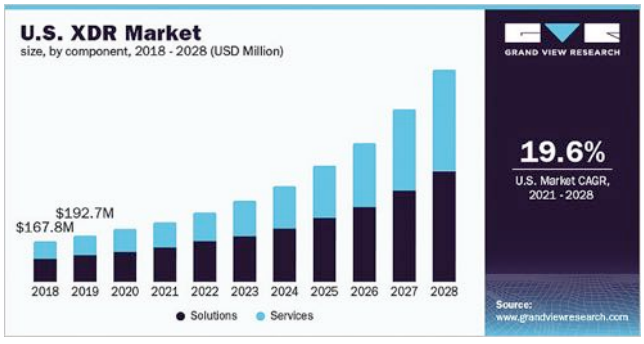
# Automatizza la "Response" nella tua strategia XDR.

Autore: William Udovich

L'Extended Detection and Response (XDR) offre un netto vantaggio contro gli attacchi avanzati, ma molti dei cosiddetti "approcci XDR" oggi disponibili sono in realtà poco più che estensioni delle attuali soluzioni EDR (Endpoint Detection and Response), che si basano su noti indicatori di compromissione (Indicators of Compromise, IOC) per trovare e bloccare le minacce già conosciute. Sebbene possano offrire maggiore visibilità sulle risorse di rete, non forniscono però la correlazione necessaria per eliminare i nuovi attacchi, per i quali non sono disponibili IOC noti.


Al contrario, l'Advanced XDR sfrutta l'Intelligenza Artificiale (AI) e il Machine Learning (ML) per correlare automaticamente i dati di telemetria provenienti dai vari asset di rete al fine di rilevare attacchi mai visti prima. Advanced XDR rileva in anticipo comportamenti potenzialmente malevoli per consentire ai Defender di rimediare più velocemente.

Advanced XDR incorpora i due elementi principali di EDR - monitoraggio e rilevamento continui e risposta automatizzata alle minacce - su tutti gli endpoint, ma XDR monitora anche le minacce nell'intera infrastruttura di un'organizzazione, inclusi i profili utente, le applicazioni di collaborazione e produttività aziendale, i workload cloud e molto altro ancora. Tali funzionalità critiche spiegano perché XDR viene spesso definito il futuro della sicurezza informatica.




## BIO

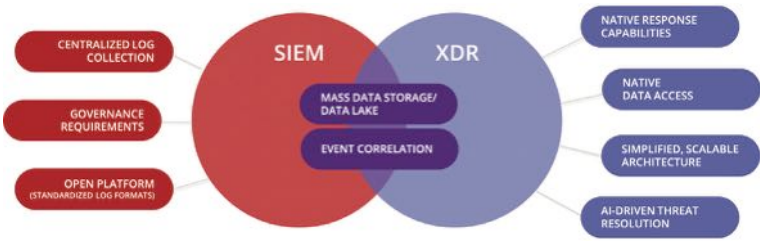
**William Udovich è Vice President Southern Europe and Africa di Cybereason. William ha maturato una esperienza ventennale in ambito cyber security sia nel campo della consulenza e che nelle divisioni marketing e vendite presso multinazionali. E' laureato in Ingegneria Elettronica presso il Politecnico di Milano e ha conseguito un MBA presso la SDA Bocconi School of Management. Attualmente lavora in Cybereason come Regional Vice President per il Sud Europa, Africa e Israele con focus sulla prevenzione di minacce cyber e EDR (Endpoint Detection and Response). Dal 2011 al 2019 ha ricoperto diverse posizioni di leadership EMEA in CyberArk contribuendo alla crescita dalla fase di startup fino alla posizione di leader di mercato in ambito PAM (Privileged Access Management) in Italia, Iberia, Nord Europa, Africa e Middle East. Dal 2004 al 2010 ha lavorato in CA Technologies Divisione Sicurezza, dapprima focalizzandosi sul territorio italiano per poi ricoprire ruoli di leadership a livello europeo.**

La società di ricerca e analisi ESG ha stimato che più di due terzi delle organizzazioni investiranno in XDR entro la metà del 2022. Questa spesa influirà sul tasso di crescita annuale composto (CAGR) del 19,9% che secondo Grand View Research[1] caratterizzerà il mercato globale di XDR da qui al 2028.

## L'automazione è la chiave

Secondo la Computing Technology Industry Association (CompTIA), uno dei vantaggi più importanti che sta aiutando a guidare la crescita di XDR è la capacità di automatizzare le operazioni di sicurezza al fine di abbattere i silos di dati e accelerare le risposte alle minacce.

Advanced XDR fornisce la visibilità necessaria su un'intera catena di attacco, ovunque esso accada, per rivelare esattamente come è progredito e quali risorse e utenti sono stati colpiti. Offre, inoltre, opzioni di risposta automatizzata e/o guidata che le soluzioni SIEM (Security Information and Event Management) non possono fornire e le soluzioni SOAR (Security Orchestration, Automation and Response) faticano a fornire su larga scala, senza un importante sforzo in termini di interventi manuali da parte degli analisti di sicurezza e dei team di incident response.




Uno dei principali punti di forza di una soluzione Advanced XDR è la possibilità di liberare i team di sicurezza dalla necessità di indagare individualmente su grandi quantità di alert, attraverso una varietà di soluzioni puntuali, per rispondere rapidamente alla domanda "siamo sotto attacco?"

Advanced XDR lo fa automaticamente, correlando i dati di telemetria per rivelare le tempistiche di attacco dalla *root cause* e consentire così ai team di sicurezza di rispondere in modo più rapido ed efficiente.

## Abbattere i silos di dati

L'infrastruttura IT di molte organizzazioni è oggi più complessa che mai, con reti decentralizzate che tradizionalmente sono affidate a strumenti di sicurezza specifici. Il problema è che gli attacchi si sono evoluti per attraversare questi ambienti, consentendo agli attaccanti di nascondersi nei meandri della rete, perché gli strumenti di sicurezza tradizionali non possono correlare la telemetria attraverso tutti gli elementi di una rete moderna. E nemmeno possono identificare gli attacchi che sfruttano questi diversi elementi in un'unica progressione di attacco, limitando quindi la visibilità di un team di sicurezza nella catena di attacchi in corso e complicando quindi il compito di analizzare un incidente nella sua interezza.

Advanced XDR non si basa su una moltitudine di alert di minacce non contestuali provenienti da risorse disparate, ma fornisce in modo automatizzato un contesto e correlazioni approfondite tra queste risorse, risparmiando agli analisti di sicurezza il noioso compito di un triage costante e di investigare manualmente gli alert non comprovati.

Advanced XDR abbatte i silos di informazioni che altrimenti impedirebbero ai team di sicurezza di ottenere una visione unificata dello stato di sicurezza della propria organizzazione. Lo fa integrando nel suo approccio di rilevamento e risposta funzionalità di firewall, soluzioni antivirus, EDR, Identity and Access Management (IAM), Cloud Workload Protection (CWPP) e altre tecnologie di sicurezza.

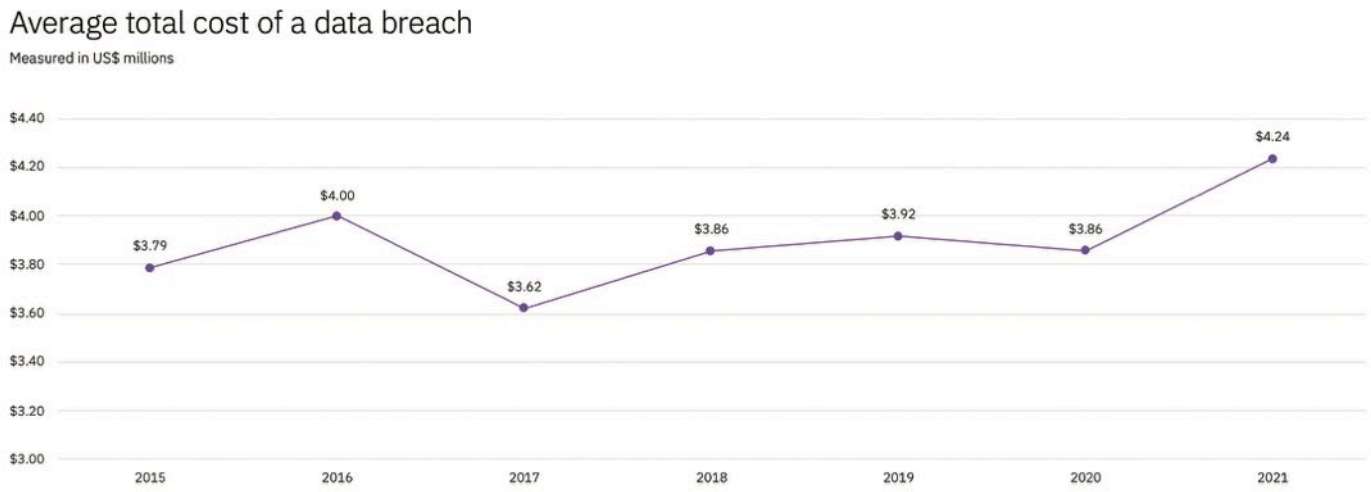
## L'automazione velocizza i tempi di risposta

I team di sicurezza possono ricorrere a strumenti SIEM, piattaforme SOAR e altre soluzioni incomplete nel tentativo di aumentare la propria visibilità, ma in assenza di correlazioni automatizzate dovranno comunque esaminare manualmente gli alert uno alla volta, quindi tentare di correlarli tra loro per identificare una catena di attacco.

Questo processo manuale implica che i team di sicurezza possono (e spesso lo fanno) perdere facilmente qualche elemento nel processo, il che li porta a restare scoperti anche quando credono di aver già posto rimedio a un incidente. E anche se riuscissero a identificare tutte le diverse componenti di un'operazione d'attacco, i team di sicurezza avrebbero dedicato così tanto tempo alle loro indagini da non riuscire a lanciare una risposta anticipata per arrestare l'attività.

Nel suo *Cost of a Data Breach Report 2021*, ad esempio, IBM ha rilevato che un'organizzazione impiega in media 287 giorni per identificare e contenere una violazione. Questo tempo di permanenza offre agli attori delle minacce quasi un anno per nascondersi nei sistemi di una vittima, condurre ricognizioni, spostarsi lateralmente in diverse parti della rete ed esfiltrare informazioni sensibili.

Non sorprende, quindi, che le violazioni dei dati con un tempo di permanenza nelle reti di oltre 200 giorni costino alle organizzazioni una media di 4,87 milioni di dollari, mentre quelle con un tempo di permanenza inferiore a 200 giorni costino 3,61 milioni di dollari. È anche importante sottolineare che il prezzo di 4,87 milioni di




*© IBM Cost of a Data Breach Report 2021, p. 12*

dollari ha superato il costo medio di una violazione dei dati che si attesta sui 4,24 milioni di dollari, danni che sono già del 10% superiori a quelli del 2020 e con il costo più alto mai registrato nella storia del rapporto di IBM.

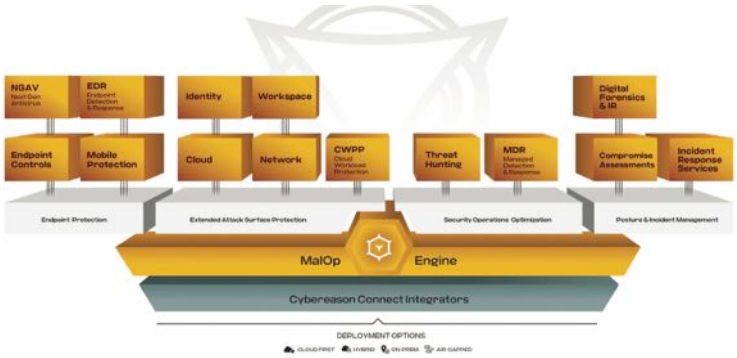
Advanced XDR riduce drasticamente il tempo di permanenza dell'attaccante attraverso un approccio operation-centric, che si concentra sugli indicatori di comportamento (Indicators of Behavior, IOB). Questi IOB rimediano a un'intera sequenza di attacco, consentendo ai team di sicurezza di terminare l'attacco nel suo insieme invece di rimediare a elementi isolati. Ad esempio, il rilevamento e la rimozione di un malware su un endpoint fa ben poco per impedire che le credenziali dell'utente compromesse vengano nuovamente utilizzate in modo improprio e non risolve la persistenza dell'attaccante su una rete target.

## Vantaggi dell'XDR avanzato

Laddove altre soluzioni limitano i dati critici raccolti in quanto non possono elaborarli o archiviarli, una piattaforma come Cybereason Advanced XDR è progettata per raccogliere e analizzare il 100% dei dati degli eventi in tempo reale.


Altri strumenti XDR non hanno la capacità di acquisire tutta la telemetria disponibile a livello di endpoint. Ricorrono allo "smart filtering", in cui la telemetria viene eliminata anche se potrebbe essere utile per il rilevamento (non è quindi così "smart"). Lo fanno perché devono inviare tutti i dati al cloud per l'analisi prima di poter restituire un rilevamento.

Le organizzazioni oggi possono sfruttare i vantaggi di una piattaforma come Cybereason XDR basata su Chronicle, che combina la piattaforma di difesa Cybereason con il suo motore brevettato MalOp™, in grado di analizzare oltre 23 trilioni di eventi relativi alla sicurezza a settimana, con il motore di analisi della sicurezza informatica di Google Cloud, che acquisisce e normalizza petabyte di dati di telemetria dall'intero ambiente IT. La combinazione delle funzionalità di Cybereason e di Google fanno sì che la telemetria non venga assolutamente filtrata, il che consente al motore di analisi predittiva AI/ML di identificare prima l'attività di attacco e porre rimedio alle minacce più velocemente.




L'applicazione dell'intelligenza artificiale non è una panacea e per il prossimo futuro sarà senza dubbio necessario un mix di risorse umane e soluzioni basate sull'intelligenza artificiale che lavorino insieme. Tuttavia, l'AI migliorerà l'efficienza di ogni membro del team di sicurezza e amplificherà l'efficacia dell'intero stack di sicurezza.

Per approfondimenti leggi anche:

https://www.cybereason.com/blog/how-ai-driven-xdr-defeats-ransomware ■

1 Grand View Research | Extended Detection And Response Market Size, Share & Trends Analysis Report By Component (Solutions, Services), By Deployment Type, By Application, By Region, And Segment Forecasts, 2021 - 2028

# L'automazione dei processi: rischi e opportunità.

Autore: Giancarlo Butti

**Quando si parla di automazione si pensa immediatamente al mondo dell'industria, ai processi industriali, alle fabbriche, ai robot. In questo articolo parleremo invece degli strumenti per automatizzare i processi e i relativi rischi e opportunità.**

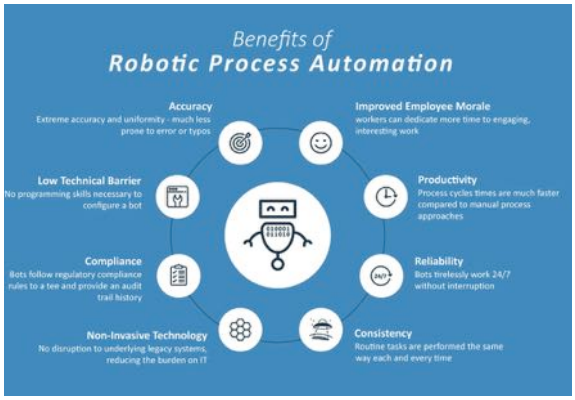
Con il termine RAP *(Robotic Process Automation)*, si intendono le tecnologie e gli strumenti che permettono di automatizzare i processi ripetitivi, realizzati utilizzando applicazioni software governate da operatori umani; la finalità di tali strumenti è quella di permettere l'automazione di tali processi con facilità.

Per certi versi si tratta un'evoluzione, in molti casi molto spinta, di quelle che sono le macro disponibili già da molti anni nelle applicazioni di produttività individuale quali Excel o Word. Le macro possono essere usate molto semplicemente registrando e riproducendo l'attività dell'utente, ovvero possono essere integrate con ulteriori funzionalità grazie alla disponibilità di uno specifico linguaggio di programmazione.

Personalmente, grazie alla macro, ho creato applicazioni molto complesse senza usare una sola riga di codice.

Fra queste la trascodifica di un bilancio, dal formato previsto da un software di contabilità italiano, ad un modello standard di una società turca, con relativa traduzione in inglese.

Gli strumenti RAP consentono di ampliare tali capacità automatizzando in modo intelligente i processi; per tale motivo la loro trattazione avviene solitamente nell'ambito delle applicazioni dell'IA.



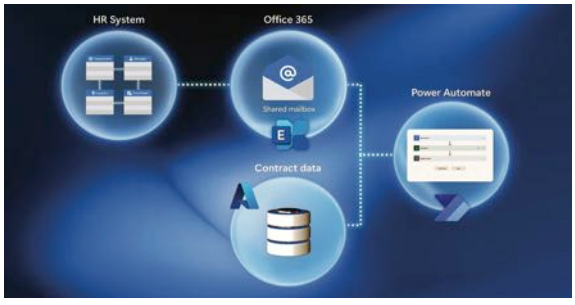

Se alcuni anni fa era soprattutto il mondo della finanza a presentare le proprie applicazioni pilota (nel 2017 durante un convegno organizzato dall' ABI sono stati presentati alcuni casi in tal senso, quali ad esempio la chiusura in modalità completamente automatizzata di un rapporto dopo aver analizzato tutte le posizioni di un cliente), oggi tali strumenti sono parte integrante, ad esempio, del nuovo sistema operativo di Microsoft, che incorpora in Windows 11 Power Automate per desktop[1].

Un'evoluzione molto rapida che rende disponibile a tutti gli utenti del nuovo sistema operativo strumenti (e decine di modelli) per automatizzare in autonomia i propri processi operativi.

I vantaggi che ne possono derivare sono abbastanza evidenti, automatizzando i processi ripetitivi:

- si liberano gli operatori dalle attività meno significative, affinché possano occuparsi di quelle a maggior valore aggiunto
- si limitano gli errori operativi causati dall'operatore umano
- si velocizzano le operazioni
- è possibile impostare meccanismi di controllo più efficaci
- è possibile automatizzare i controlli.

Inoltre, in molte situazioni l'automazione non richiede l'uso di figure tecniche specializzate per l'implementazione ma, come nel nuovo sistema operativo di Microsoft, può essere impostata direttamente dall'utente finale.



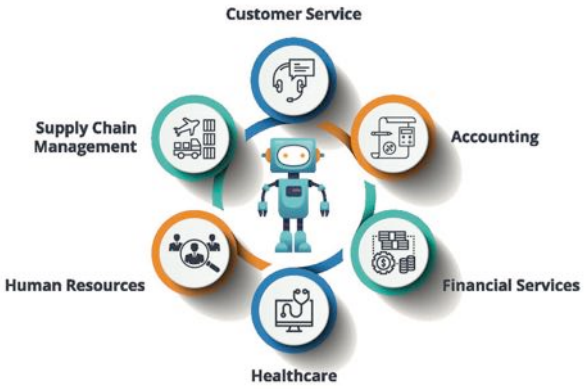

Tali strumenti, tuttavia, non risolvono una serie di rischi legati alla operatività degli utenti, che in realtà potrebbero essere aggravati dal loro uso e dal conseguente aumento della produttività.

Vanno infatti distinte le situazioni nelle quali ciò che viene automatizzato è un processo che utilizza per il proprio svolgimento applicazioni centralizzate e adeguatamente presidiate, da quelle nelle quali i processi si svolgono in tutto o in parte mediante l'uso di prodotti di produttività individuale (quali programmi di elaborazione testo e fogli elettronici) e loro appendici (ad esempio cartelle condivise sul cloud…).

La disponibilità di tali strumenti ha da tempo permesso agli utenti più evoluti di sviluppare in autonomia applicazioni per lo svolgimento di operazioni complesse, in particolare laddove l'azienda non renda disponibili specifiche soluzioni per la loro gestione (per problemi di costo, di flessibilità, di tempo o semplicemente perché gli utenti vogliono mantenere la propria autonomia senza dipendere dai tempi e dalle risorse dell'ICT).

Oggi, la disponibilità di strumenti come Power Automate direttamente da sistema operativo, consentirà un ulteriore livello di libertà ed autonomia per gli utenti, in particolare a quegli utenti evoluti abituati da tempo a operare al di fuori del sistema informativo ufficiale dell'azienda, delle relative policy e vincoli e dei relativi controlli.

Va anche ricordato che questa tipologia di utenti spesso si occupa di argomenti rilevanti per l'azienda, quali ad esempio il bilancio o il controllo di gestione o, nel mondo bancario, della finanza.




Se da un lato quindi la disponibilità di strumenti di automazione può agevolare il lavoro degli utenti, dall'altro si introducono una serie di rischi significativi, come ha ben compreso Banca d'Italia, che nella Circolare 285 già da parecchi anni ha introdotto sul tema uno specifico paragrafo:

> *4. La sicurezza delle applicazioni sviluppate dalle unità operative e di controllo*
>
> *Lo sviluppo di applicazioni direttamente in carico alle unità operative e di controllo è sottoposto a misure di natura organizzativa e metodologica, tese a garantire un livello di sicurezza comparabile con le applicazioni sviluppate dalla funzione ICT.*
>
> *Un periodico monitoraggio censisce le applicazioni sviluppate con strumenti di informatica d'utente e ne verifica la rispondenza alla policy di sicurezza, in particolare se utilizzate in attività rilevanti quali la predisposizione dei dati di bilancio, del risk management, della finanza e del reporting direzionale, al fine di contenere il rischio operativo.*

La richiesta che Banca d'Italia esprime nella propria circolare (che è vincolante per le banche italiane, le quali rischiano sanzioni fino al 10% del proprio fatturato[2] in caso di mancato rispetto delle prescrizioni previste) è molto onerosa.

Tali applicazioni, essendo di fatto irrinunciabili, devono garantire lo stesso livello di sicurezza presente nel resto del sistema informativo.

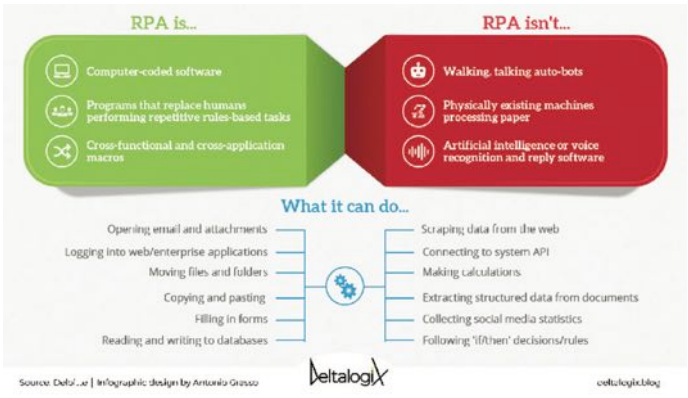
Una sfida non banale, considerando che tali strumenti non dispongono di funzionalità base di sicurezza quali ad esempio la gestione di profili di accesso differenziati o il tracking delle modifiche apportate…

Ma non sono solo questi i rischi legati alle applicazioni sviluppate direttamente dagli utenti; ne cito alcuni:

- manca solitamente la documentazione che dettagli le regole che sono state implementate
- chi le ha realizzate ne detiene spesso in modo assoluto il know how; al riguardo, per quanto possa essere relativamente semplice ricostruire algoritmi e formule utilizzati in un foglio elettronico, può essere difficile ricostruire le motivazioni che hanno portato a tali scelte, in particolare allorquando non si tratti di un solo foglio elettronico, ma di un insieme di fogli fra loro interconnessi
- spesso sono conservate solo sul pc di chi le ha sviluppate, e quindi inaccessibili per il resto dell'azienda
- non esiste una reale gestione delle versioni
- sono facilmente modificabili (questa, del resto, è la loro forza) e sono quindi soggette a variazioni accidentali derivanti da errori operativi dell'utilizzatore
- non sono soggette a backup, salvo che il loro sviluppatore non provveda al riguardo
- sono utilizzate di solito in produzione senza seguire un iter di validazione e test
- possono contenere degli errori nelle formule, nel codice, nelle query, che difficilmente sono evidenti in assenza di test esaustivi
- etc.

La disponibilità di soluzioni RAP, aumentando il livello di autonomia degli utenti (ovviamente se si permette agli utenti di sviluppare autonomamente l'automazione dei loro processi) o comunque facilitando notevolmente la possibilità di automatizzare processi che fanno uso di prodotti di produttività individuale, può aumentare, se non vengono adottate le opportune contromisure, il livello di questi rischi.

Se infatti per un'azienda l'alternativa all'automazione di un processo tramite tali strumenti è lo sviluppo di un'applicazione ad hoc, ben difficilmente sarà percorsa questa seconda (e onerosa) soluzione.




## 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.**

È quindi di fondamentale importanza che la disponibilità e l'uso di tali strumenti siano accompagnati da una valutazione complessiva dei costi e benefici per l'azienda da tutti i punti di vista e non solo, come troppo spesso accade, dalla semplice valutazione della riduzione dei costi derivante dal minor uso di "mano d'opera".

Anche per quanto attiene i rischi va considerato che, se da un lato è innegabile che l'automazione permetta di ridurre i rischi legati alla operatività, dall'altro l'eventuale presenza nei processi automatizzati di applicazione sviluppate dagli utenti o più in generale di prodotti di produttività individuale può aumentare i rischi legati al

loro uso in conseguenza dell'aumento dei volumi di dati ed operazioni processabili.

In sintesi, quindi, vanno adeguatamente distinte le varie situazioni:

- da un lato si avranno i casi in cui la tecnologia RPA consente di automatizzare processi che vengono svolti utilizzando essenzialmente applicazioni ben consolidate, presidiate e con un adeguato livello di sicurezza; per tali situazioni il bilancio fra costi/rischi e benefici sarà di norma positivo.
- dall'altro si avranno casi nei quali tale tecnologia è applicata a processi anche solo parzialmente effettuati con strumenti di produttività individuale; in questi casi la riduzione dei rischi legata alla operatività manuale deve essere comparata con l'eventuale aumento di rischio legato al numero di operazioni trattate in un ambiente non sicuro.

Per questa seconda situazione devono essere eventualmente impostate le opportune contromisure, che si possono agevolare proprio dall'uso dell'automazione dei processi.

Come anticipato infatti, sarà possibile automatizzare anche i processi di controllo, anche se tale misura da sola non può bastare e deve essere affiancata da misure sia di carattere generale quali:

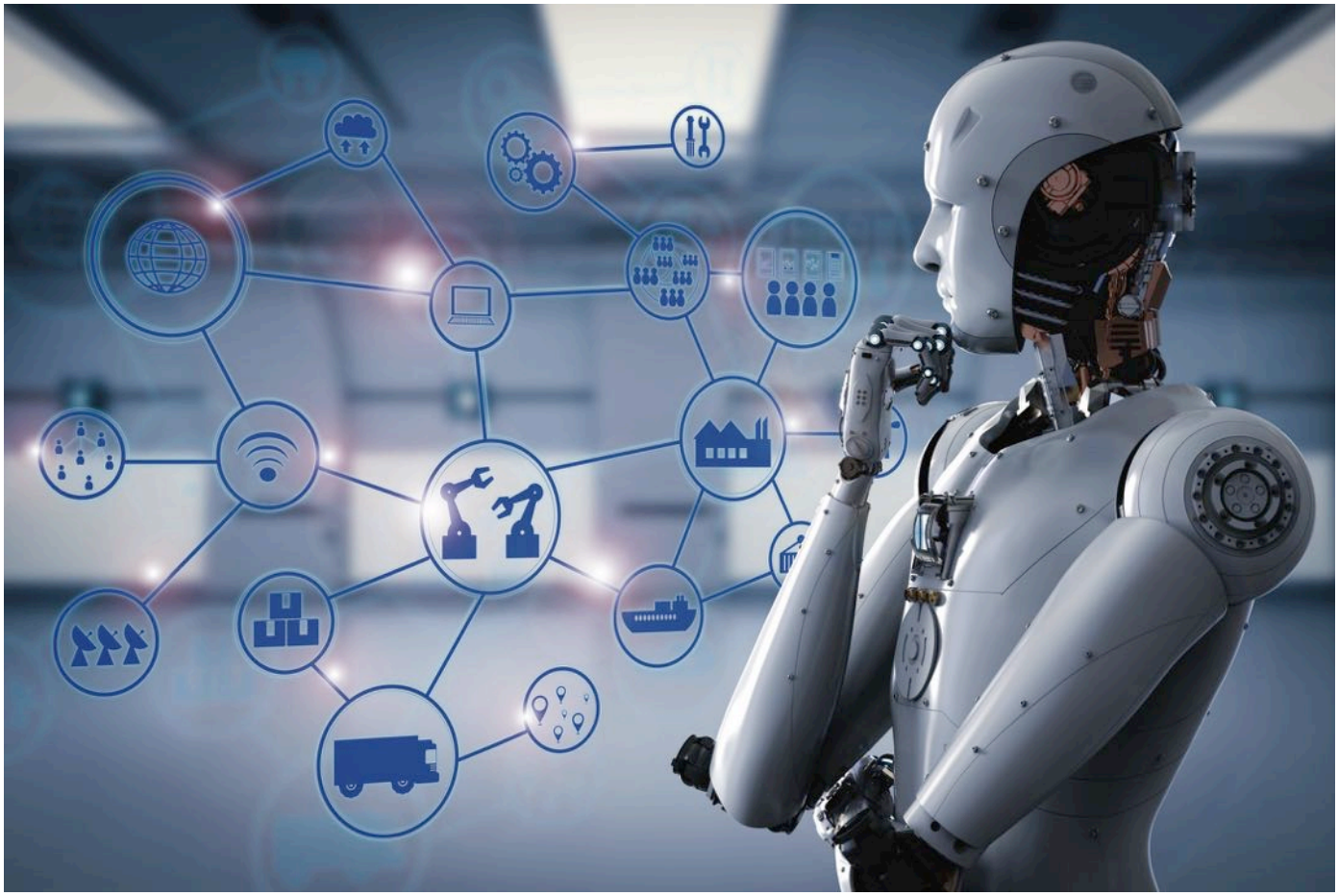
- la definizione di una policy sull'uso degli strumenti di produttività individuale e sullo sviluppo delle applicazioni da parte degli utenti
- il censimento e classificazione delle applicazioni
- il monitoraggio dei controlli impostati
- la revisione periodica delle esigenze degli utenti al fine di valutare, laddove i rischi siano troppo elevati, lo sviluppo di applicazioni ad hoc
- l'uso di piattaforme (ne esiste più di una) per il presidio delle applicazioni sviluppate dagli utenti, sia specifiche, legate alla singola situazione.

## Conclusioni

Come per tutte le tecnologie l'utilizzo delle soluzioni RAP può portare notevoli vantaggi, ma se non correttamente indirizzato, in alcuni ambiti può portare ad un aumento dei rischi per l'azienda.

Come sempre quindi il corretto approccio deve comprendere un'analisi a 360 gradi, al fine di saper cogliere le opportunità che la tecnologia rende disponibili ed a guidarla, in particolare se questa sarà resa disponibile di default agli utenti come componente del sistema operativo installato sulle loro postazioni.

1 https://powerautomate.microsoft.com/it-it/robotic-process-automation/
2 A titolo esemplificativo le pesanti sanzioni introdotte dal GDPR arrivano al massimo al 4% del fatturato



# L'algoritmo rischia di diventare il nuovo vitello d'oro. Se scienza, virtù e cultura del diritto non camminano insieme.

## Intervista VIP a Giovanni Maria Flick.

Autore: **Massimiliano Cannata**

"Il primo aspetto cruciale che dobbiamo tenere bene a mente è la necessità di acquisire una consapevolezza adeguata del rapporto che esiste tra rischi e opportunità in una società in cui l'automazione risulta ormai componente dominante della vita quotidiana. La consapevolezza può infatti permetterci di evitare errori di percezione, euforia o sottovalutazione, che non possiamo permetterci in questa fase delicata della storia dell'umanità".

***Presidente Flick, il suo ultimo saggio "*L'algoritmo d'oro e la torre di Babele *(ed. Baldini + Castoldi) offre un'interessante panoramica della contemporaneità. In particolare, insieme alla coautrice Caterina Flick, lei si sofferma sulle opportunità e i rischi della società tecnologica, dominata dal digitale e dall'automazione. A quali scenari dobbiamo prepararci?***

Mi capita spesso di citare la metafora dei porcospini, tratta da uno scritto di Schopenhauer: i due animali incontrandosi di notte in inverno, non riescono a trovare la giusta distanza. Se stanno lontani sentono freddo, se si avvicinano troppo finiscono col pungersi; provando e riprovando, riescono a trovare la giusta o quanto meno una accettabile distanza. Quello della distanza o meglio

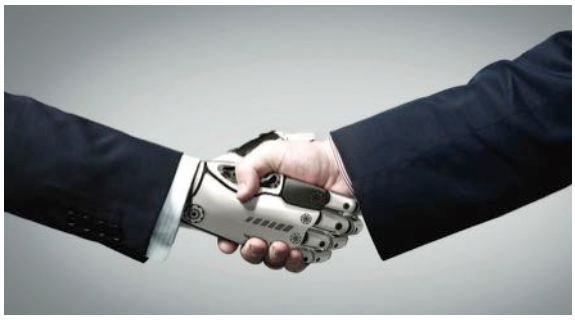
della cautela da tenere rispetto all'eccezionale progresso della tecnica è il grande tema del nostro tempo. Con molte difficoltà stiamo cercando di studiare il rapporto tra uomo e ambiente, in questa epoca che molti studiosi definiscono dell'antropocene, proprio per il fitto intreccio che lega l'individuo, la società e il contesto naturale che ci circonda. Ecologia e giustizia, natura e società hanno un comune destino. La paura del diluvio

universale, che i disastri naturali hanno prepotentemente riproposto, sta giustamente condizionando l'agenda dei governi e facendo alzare la soglia dell'attenzione. Lo stesso percorso, credo, occorre fare per comprendere le implicazioni relative allo sviluppo dell'information society e dell'automazione. Conoscere bene il binomio tra uomo e conoscenza risulterà decisivo, per focalizzare gli scenari che si aprono nell'immediato futuro e per cogliere l'equilibrio tra vantaggi (irrinunziabili) e rischi (inevitabili), nell'entusiasmo ma anche nella preoccupazione per il futuro e per le regole con cui affrontarlo.

## Sicurezza e automazione

***Intelligenza umana, sicurezza e sistemi automatici, una triangolarità destinata a diventare dominante nel mondo di oggi. È possibile trovare un giusto equilibrio tra uomini e civiltà delle macchine?***

Non credo che sia corretta questa contrapposizione. La civiltà è un modo di organizzare la convivenza tra le persone, per rendere possibile il progresso e la crescita collettiva. L'art. 9 della Costituzione ricorda proprio la "missione culturale" della Repubblica, aspetto su cui tornerò più avanti. Quella delle macchine non è dunque una civiltà, come non c'è stata nel passato a mio giudizio una civiltà del legno o del ferro; sono modi impropri per definire alcune tappe del progresso umano nella storia. Strumenti e valori vanno sempre distinti per avere chiaro l'orizzonte problematico di cui ci stiamo occupando.



***In uno scritto recente ha tessuto l'elogio della foresta (G. M. Flick, M. Flick,* Elogio della foresta, dalla selva oscura alla tutela costituzionale, ed. Il Mulino, n.d.r.*) cui fa da contraltare la città. Questo dualismo è molto presente nella sua riflessione. Quale messaggio dobbiamo trarre?***

La foresta e la città evocano due modelli contrapposti che sono, contrariamente a quanto si pensa, entrambi complessi. Nella città prevale la logica del profitto nell'organizzazione della convivenza, nella foresta prevale l'ambiente, anche se minacciato, in quest'ultima dovrebbe rimanere dominante. L'uomo ha sempre cercato di organizzarsi in società per ragioni di scambio e per il bisogno di sicurezza o per ragioni di potere,


per questo ha creato delle infrastrutture adatte al suo insediamento. La crescita a dismisura di megalopoli non risponde però all'ideale originario della città giusta, che risale a Sant'Agostino, ma anche alla tradizione biblica. Tornando al tema centrale della nostra conversazione – il rapporto tra sicurezza e automazione – le città vivono l'attualità di questa dicotomia. La tecnologia sta cambiando strutture e organizzazione urbana; pensiamo alle *brain city* o alle *smart city*. Tutte prospettive affascinanti a patto di non tradire un principio fondante della nostra Costituzione, su cui si regge la convivenza e il patto sociale che ci tiene uniti: quello della solidarietà e della giustizia sostanziale. Se questo non accade la città tecnologica rischia di creare dei nuovi ghetti, con aree povere che si fronteggiano con isole dorate.

## L'identità tra spazio, tempo e relazione

***Come ha ricordato in occasione dell'evento dedicato ai 25 anni della privacy esiste il rischio che sistemi guidati da algoritmi sostituiscano l'uomo in funzioni connaturate alla sua identità. Che contromisure vanno adottate?***

La privacy ha a che fare con la nostra identità, che è segnata da tre coordinate: spazio, tempo e relazioni, come si evince molto bene dal dettato costituzionale. Pensiamo al diritto all'oblio e al "presente virtuale" che spesso condanna l'individuo senza appello. Questo accade perché vi sono "trappole della memoria" alimentate dalla rete che vanno regolamentate. La riscrittura dell'art.9 della Costituzione è significativa in tal senso, perché guarda al paesaggio non tanto nella fissità di un valore estetico, quanto nella dinamica di un bene comune che deve impegnare la politica, le istituzioni, le organizzazioni internazionali a scelte decisive per l'avvenire delle generazioni future, soprattutto alla luce di una recentissima modifica che rende più esplicita e vincolante in termini di eguaglianza l'indicazione costituzionale. L'art. 41 e l'art. 42 rafforzano questa visione (mi scuseranno i lettori per i continui riferimenti alla nostra Carta Costituzionale, ma sono un giurista non un tecnologo) perché sottolineano come l'iniziativa economica non può svilupparsi a danno dell'ambiente e neppure in contrasto con gli interessi generali e i diritti delle generazioni future. Come vede la riflessione sul dominio sempre più diffuso dell'automazione – oltre a imporre un'analisi attenta sulla "gestione predittiva" nell'amministrazione della giustizia (pensiamo al connubio tra processo, sentenza e nuove tecnologie) – suggerisce di mantenere una visione molto ampia nella lettura di tutte le fenomenologie del cambiamento che investono l'uomo nella triplice dimensione del passato, del presente e del futuro.

***L'Algoritmo d'oro è dunque il nuovo vitello d'oro, per tornare al titolo molto evocativo del suo scritto. L'immagine biblica può tornare di attualità, con quali conseguenze?***

L'algoritmo in sé non è buono né cattivo; come tutti gli strumenti dipende dalla sua programmazione e dall'uso che se ne fa. Se facciamo prevalere la

logica del profitto, dati e informazioni diventano merci di scambio, non servono a cercare la verità ma a confondere e a condizionare l'opinione pubblica. Si tende sempre più a profilare gli utenti, a scavare nelle loro abitudini anche più segrete per indurre bisogni artificiali da sfruttare commercialmente o politicamente o ideologicamente e culturalmente. Lo vediamo con quello che sta avvenendo con la guerra in Ucraina, e lo abbiamo visto prima con la pandemia. Una "babele di voci" non sempre competenti e realmente interessate a scandagliare i fatti con la massima obiettività possibile. Da qui l'immagine biblica che evoca il "vitello d'oro" il miraggio dell'arricchimento, cui tutto deve essere sacrificato. Le lingue si confondono e confluiscono in un "linguaggio unico" (tra uomo e uomo, tra uomo e macchina, tra macchina e macchina) come quello della piana di Ur dove si iniziò a costruire la torre di Babele ma l'interesse è uno: il potere e il profitto.

L'informazione non correttamente utilizzata genera queste grandi contraddizioni. L'art. 21 ci viene in soccorso definendo il diritto alla manifestazione libera del pensiero, un diritto che può paradossalmente prevedere l'espressione di falsità. Anche in questo caso bisognerà bilanciare il diritto all'informazione con il diritto a essere informati, nel rispetto della riservatezza e segretezza. Ricordo che abbiamo lavorato con Stefano Rodotà sulla definizione di questi principi, arrivando alla normativa di Schengen, premessa alla definizione della legge istitutiva dell'autorità Garante. Quella intuizione e il percorso che ha guidato il nostro operato rimane valido: alla tutela del corpo fisico, si è aggiunta la tutela di quello che Rodotà ha definito "corpo elettronico" con un'immagine rimasta insuperata.

## La torre di babele e il rischio del "folle volo"

***La "quarta rivoluzione" che stiamo attraversando avrà una rilevanza più profonda delle precedenti anche sul piano dell'evoluzione del diritto?***

Siamo oltre l'Habeas corpus; con la diffusione dell'automazione e dell'algoritmo abbiamo a che fare con una nuova generazione di diritti l'Habeas data e con la sfera dei neuro diritti, mentre nuove discipline prenderanno campo. Primo fra tutte il *brain reading*, che introdurrà forse strumenti in grado di leggere il pensiero. Credevamo che si trattasse di una superficie insondabile, quella delle motivazioni che albergano nel foro intimo della coscienza, invece, siamo di fronte ad ambiti tutti ancora da indagare, per i giuristi e non solo loro. Una cosa mi rende cautamente ottimista, che vorrei esplicitare a conclusione della nostra conversazione: la scienza si sta rendendo conto che l'accumulo della conoscenza senza virtù, può avere risvolti molto problematici. *"…fatti non foste a viver come bruti, ma per seguir virtute e canoscenza"* (Inferno, XXVI, 119/120) ci ricorda il sommo poeta. La sete di sapere se non alimentata da valori si può trasformare sempre in un "folle volo" con effetti distruttivi per tutta l'umanità.

A maggior ragione ciò deve dirsi rispetto all'ultimo stress test in corso per l'umanità, nel primo ventennio del nuovo millennio: la guerra con la sua novità di globalizzazione; di coinvolgimento dei civili; di utilizzo della cibernetica e delle *fake news*; di paura nucleare della mutua distruzione. Dopo il terrorismo globale nel 2001, la crisi economica nel 2007, la pandemia nel 2019 e ora anche la carestia come conseguenza della guerra, oltre alla carestia provocata sino ad ora dal saccheggio della natura.

Cosa pensiamo sia più giusto fare: continuare a cambiare l'ambiente per adattarlo all'uomo, o cambiare l'uomo per adattarlo all'ambiente? ■

## BIO

**Dopo aver conseguito nel 1962 la laurea in Giurisprudenza, viene chiamato a dirigere la Città dei ragazzi di Roma. A 24 anni vince il concorso in magistratura qualificandosi primo a livello nazionale. Nel 1976 lascia la magistratura per intraprendere la carriera di avvocato penalista e di professore ordinario di Diritto penale che interrompe nel 1996 con la nomina a Ministro della Giustizia nel governo Prodi I. Nel febbraio del 2000 viene nominato giudice della Corte costituzionale dal presidente della Repubblica Ciampi. Cinque anni dopo assume la carica di vicepresidente e nel 2008 ne diventa presidente. Attualmente ne è Presidente emerito. È professore emerito di Diritto penale all'Università Luiss di Roma, dove ha insegnato fino alla nomina a giudice costituzionale. È stato inoltre presidente onorario della Fondazione Museo della Shoah di Roma ed è stato consigliere e poi presidente della Fondazione San Raffaele del Monte Tabor e Presidente emerito della Corte costituzionale. È stato delegato del Commissario straordinario del governo per l'Expo 2015 di Milano. Ha rappresentato il Governo italiano nella convenzione per la redazione della Carta dei Diritti Fondamentali dell'Unione Europea sino alla sua nomina di Giudice costituzionale. È inoltre membro della Commissione di studio per l'Etica della Ricerca e la Bioetica del C.N.R.**

# La miglior risposta a un incidente informatico non è la piu' veloce, ma la più ragionata.

## Intervista VIP a Marco Ramilli.

Autore: Massimiliano Cannata

*Cybersecurity Trends* affronta in questa intervista realizzata con Marco Ramilli, Chief Executive Officer di Yoroi srl, azienda del gruppo Tinexa polo italiano di eccellenza che gestisce sistemi integrati per la difesa cibernetica, l'intreccio sempre più fitto che lega sicurezza informatica e IA.

### BIO

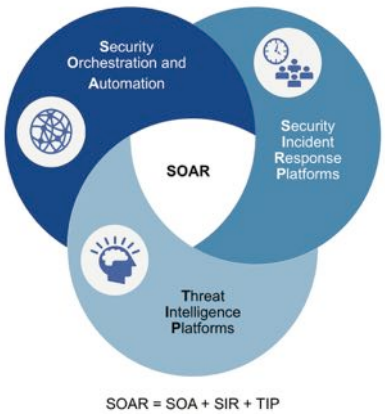
**Esperto di sicurezza Informatica, specializzato in Malware Analysis e sistemi di evasione, Marco Ramilli ha ottenuto un PhD presso l'Università degli studi di Bologna in collaborazione con l'Università della California, Davis, dove ha realizzato alcune delle principali tecniche per individuare nuove famiglie di Malware ed alla messa in sicurezza di noti sistemi di voto elettronico. Ha lavorato per il Governo degli Stati Uniti d' America, dove ha contribuito alla realizzazione dell OEVT. CyberSecurity blogger dal 2007, autore di due libri sulla sicurezza informatica e sulle metodologie di penetrazione di sistemi informatici, autore di innumerevoli articoli scientifici pubblicati su note riviste quali IEEE ed ACM. CEO e fondatore di Yoroi, una delle aziende più innovative di Cybersecurity, appartenente al Gruppo Tinexta S.p.A. dal 2020.**

***Ingegner Ramilli in che rapporto stanno sicurezza e automazione?***

La domanda offre uno spunto più generale che vorrei cercare di argomentare, perché offre l'opportunità di inquadrare il grado di evoluzione scientifica e tecnologica che caratterizza la complessità dei sistemi IT nel contesto della rivoluzione digitale in atto. Partirei se permette dall'esperienza che vivo quotidianamente operando in azienda.

***Prego, la ascolto…***

Ho sentito in più occasioni frasi del tipo: "Quando siamo di fronte ad un attacco informatico, è necessario essere velocissimi altrimenti ci ritroviamo in poco tempo i dischi cifrati". Questo "claim" approssima due scenari molto differenti tra loro lasciando intendere che una risposta immediata ad un incidente informatico sia la soluzione migliore, ovvero la migliore risposta che si possa avere. Da questa linea di pensiero nasce l'imminente necessità di installare tecnologie di orchestrazione automatica come le SOAR *(Security Orchestration, Automation and Response n.d.r)*. Non credo che sia corretto operare in tal senso, perché la logica che sottende questa scelta associa alla velocità di cifratura di un ransomware la velocità di attacco, che sono due dimensioni profondamente differenti.



SOAR = SOA + SIR + TIP

***Si tratta di un aspetto molto delicato, possiamo spiegarlo in termini semplici?***

Non è corretto definire un attacco moderno "veloce", perché siamo comunque di fronte ad azioni lente, premeditate e molto studiate. Ricordiamoci che un attaccante deve compiere

numerosi passi prima di arrivare all'avvio del *Ransomware*, che è l'ultimo *step* di una catena molto complessa, che comporta di fatto passaggi molto lenti. Pensiamo per esempio all'aumento del footprint interno, operazione che ha il fine di garantirsi una persistenza aziendale e non di sistema. Per effettuare questo "passo" l'attaccante deve per prima cosa effettuare scansioni "sotto-traccia", identificare possibili e ulteriori punti di accesso, per poi sfruttare i punti individuati o exploitare le vulnerabilità rilevate nella rete interna attraverso un processo che si definisce *"trial and error"*. Tali passaggi dipendono fortemente dalla complessità della rete oggetto di attacco e dalla sua dimensione reale. Stiamo parlando di attività che occupano da giorni a mesi.


***Quella della velocità è dunque una falsa percezione?***

Una falsa percezione dovuta a un modo sbagliato di guardare i trend evolutivi in atto. Penso a un esempio eclatante come il "rapimento dei dati", operazione con cui un ipotetico attaccante si applica per *esfiltrare* le informazioni della vittima, che devono essere estratte "pochi byte alla volta" per evitare che sistemi volumetrici possano identificare pattern di traffico malevolo. Considerando in particolare l'enorme quantità di dati sottratti nel corso di attacchi della tipologia *"double extrortion/ransomware moderno"* occorrono giorni se non settimane per portare a termine. Per questo motivo invece di parlare genericamente di velocità, credo che sia più corretto e più aderente alla realtà dei fatti ritenere che una volta avviato il ransomware, la migliore difesa da mettere in atto possa essere quella più rapida, a patto di ricordarsi che stiamo parlando solo dell'ultimo atto della catena.


## Il paradigma della complessità

***Dal paradigma del controllo al paradigma della* governance*, gli studiosi della complessità da Edgar Morin a Mauro Ceruti, al Nobel Giorgio Parisi tendono a inserire le problematiche legate alla sicurezza in un orizzonte filosofico ed epistemologico che presenta forti discontinuità rispetto al passato. Le sue riflessioni sono molto vicine a questo indirizzo di pensiero che tende a capovolgere le convinzioni della fisica di stampo newtoniano e galileiano che ha dominato per secoli. Quali scenari si prospettano?***

In un contesto mutato, sempre più dominato dalle leggi del caos, che governano sistemi lontani dall'equilibrio anche per chi si occupa della tutela di reti e sistemi, gli indirizzi strategici hanno cambiato profondamente profilo. Quando dico che bisogna comprendere che la migliore difesa delle infrastrutture critiche e delle organizzazioni aziendali non è semplicemente quella più veloce, sottintendo la matrice complessa su cui poggiano le architetture informatiche nelle organizzazioni produttive. Questo non vuol dire che la velocità di intervento non giochi un ruolo fondamentale, non a caso *Yoroi* ha investito molto nei team che operano senza soluzione di continuità nelle 24 ore, a patto di ricordarsi che non è l'unico parametro. Altra dimensione importante è l'esperienza, che si intreccia con un'adeguata conoscenza delle tipologie di attacco, delle strategie di difesa, e infine la flessibilità degli artefatti che gli analisti detengono, affinando tecniche specifiche in risposta agli attacchi/minacce che si verificano.

## Elogio della "lentezza" e della qualità del fattore umano

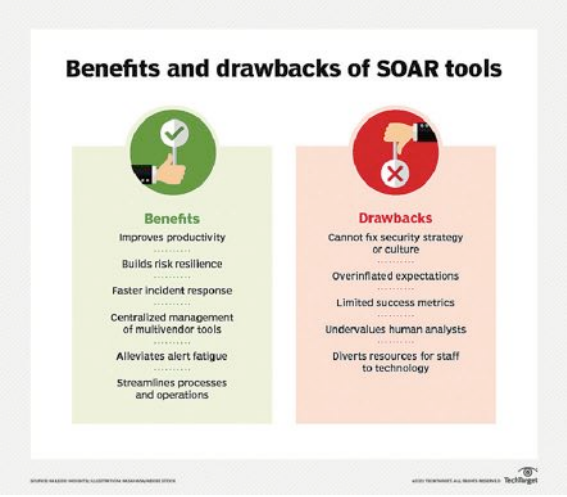
***La tecnologia SOAR, cui faceva prima riferimento, quali livelli di protezione garantisce?***

Per rispondere alla domanda dobbiamo considerare un paradosso. Maggiore è il numero di strumenti che orchestra un SOAR, più alta sarà la precisione di intervento, ma anche il tempo di reazione. Se misuriamo la qualità degli interventi sull'unico terreno della velocità, cadiamo ancora una volta in un'evidente contraddizione. In effetti la spiegazione deve essere un'altra: nel momento in cui un *ransomware*


viene lanciato da un attaccante su una macchina vittima, essendo un processo di cifratura automatica la cui velocità dipende unicamente dalla forza computazionale e dalla velocità di lettura/scrittura del disco della macchina ostaggio, neanche un processo di automazione come un SOAR riuscirà a intervenire in tempo essendo un'automazione dipendente da vari componenti che presentano differenti latenze e relativi errori. Questo vuol dire che tutte le volte che sentiamo i clienti tracciare la facile equazione: Cyber Attack=Velocità di intervento = SOAR siamo di fronte ad un approccio riduzionista, non più accettabile per quanto ho cercato di spiegare fin d'ora. Questo dimostra come la migliore risposta ad un incidente informatico non sia quella più rapida, ma la più ragionata.

***Possiamo illustrare in termini semplici le modalità operative del SOAR?***

Un SOAR lavora per playbook, ovvero per passaggi successivi basati su indicatori statici. Il ragionamento statico, non è un ragionamento intelligente, perché non considera il cambio di contesto e non cerca di adattarsi ad esso. L'incapacità di adattamento è di fatto un deficit di intelligenza. Un SOAR non ha infatti grande capacità di adattamento. Un'email oggi può essere benevola e domani può non esserlo, un dominio oggi è innocuo domani diventa propagatore di Malware, un login localizzato da una certa zona del mondo oggi può risultare autentico, domani destare forti sospetti.




Una strategia di difesa basata solo su una piattaforma come SOAR è una difesa basata su un livello di ragionamento ridotto, soprattutto su una scarsa capacità di astrazione, con la conseguenza che la variabilità del reale sfugge ad ogni capacità di analisi. Questo ci fa capire, se ancora non fosse chiaro a sufficienza, che è sempre l'essere umano "aiutato/aumentato" da una buona tecnologia che fa la differenza.

Ricordarlo non è mai superfluo, per evitare di cedere a troppi facili e superficiali entusiasmi. ■

# Minacce interne: profiling e rilevamento.

Autore: **Battista Cagnoni**

*"È tutta una questione di fiducia"*, si potrebbe dire. La maggior parte delle attività e delle interazioni umane si basa sulla fiducia.

Ci fidiamo di coloro che hanno realizzato e messo in opera il sistema di segnalazione stradale. Non possiamo controllare che quando vediamo il verde del semaforo sulla nostra strada a 80 km/h, gli altri abbiano il rosso e non si muovano. Allo stesso modo, ci fidiamo del cuoco del ristorante che prepara il nostro pasto con ingredienti buoni e non dannosi per la nostra salute. Non possiamo entrare in cucina e controllare personalmente cosa succede.

Allo stesso modo in cui ci fidiamo delle persone con cui lavoriamo, ci fidiamo di coloro che assumiamo e che hanno accesso a informazioni riservate e alla proprietà intellettuale che è così vitale per l'azienda.

Questo rappresenta un rischio aziendale e le organizzazioni che hanno raggiunto un elevato livello di maturità sanno bene dove si trova il punto critico, ma allo stesso tempo sono consapevoli che si tratta di uno dei problemi più difficili da risolvere.

Le operazioni di sicurezza si basano su persone, processi e tecnologie, e se un buon equilibrio tra queste tre componenti è ragionevole, efficace e necessario in relazione alle minacce esterne, è ancora più necessario e deve essere portato al limite in relazione al rilevamento delle minacce interne.

**Ma cos'è una minaccia interna?**

Se si consulta uno dei migliori libri finora pubblicati, il Libro Bianco di Eric D. Shaw e Harley V. Stock[1] , i risultati più interessanti di questo studio sono evidenziati qui:

## BIO

**Battista Cagnoni, Senior Consultant, Advisory Services, EMEA di Vectra, è un esperto di sicurezza con una vasta esperienza in diverse aree del settore, dove ha ricoperto posizioni come Security Engineer, Security Analyst o SOC Lead. È appassionato di cultura della sicurezza informatica, consapevolezza e comprensione delle metodologie per affrontare i problemi di sicurezza. Condivide costantemente le sue conoscenze, offrendo consigli e processi al massimo livello, aiutando i CISO che stanno pensando a come rafforzare e raggiungere un elevato grado di maturità nelle operazioni di sicurezza. Battista è in possesso delle certificazioni GIAC Forensic Analyst e Incident Handler, nonché dei certificati CISSP, GCFA, GCIH Expert.**

**A livello interno, è più probabile che i furti di proprietà intellettuale vengono commessi da quelli che ricoprono ruoli tecnici.**

La maggior parte dei furti di proprietà intellettuale è commessa da dipendenti maschi, con un'età media di 37 anni, che occupano principalmente ruoli tecnici, tra cui ingegneri o scienziati, manager, venditori e programmatori. La maggior parte dei ladri di proprietà intellettuale ha firmato accordi sulla proprietà intellettuale, il che indica che le regole da sole, senza la comprensione e l'applicazione da parte dei dipendenti, sono inefficaci.

**A livello interno, quelli che commettono furti di proprietà intellettuale di solito hanno già trovato un nuovo lavoro.**

Circa il 65% dei dipendenti che commettono furti di proprietà intellettuale o insider trading ha già accettato un lavoro presso un'azienda concorrente o ha avviato una propria azienda al momento del furto. Circa il 25% è stato reclutato da un estraneo che aveva preso di mira i dati che voleva ottenere da loro e circa il 20% dei furti prevede la collaborazione con un altro "nemico interno".

**A livello interno, quelli che commettono i furti di proprietà intellettuale rubano più spesso ciò a cui hanno l'autorizzazione, ad accedere.**

I soggetti prendono i dati che conoscono, con cui lavorano e a cui spesso hanno il permesso di accedere. Infatti, il 75% di loro ha rubato materiale a cui aveva accesso debitamente autorizzato. Questo complica la capacità di un'organizzazione di proteggere la propria proprietà intellettuale attraverso controlli tecnici e conferma la necessità di accordi vincolanti con i dipendenti, come ad esempio quelli che stabiliscono quali parti della "proprietà intellettuale" tornino o meno di loro proprietà una volta lasciato il loro incarico.

**A livello interno, tra il furto di proprietà intellettuale quello dei segreti commerciali è il più frequente.**

I segreti commerciali costituiscono il 52% dei casi di furto. Nel 30% dei casi si tratta di informazioni commerciali come dati di fatturazione, listini prezzi e altri dati amministrativi; nel 20% dei casi di *source code;* nel 14% dei casi di software di proprietà della ditta;


nel 12% dei casi di informazioni sui clienti; nel 6% dei casi di strategie aziendali.

**A livello interno, i furti di proprietà intellettuale sono commessi da dipendenti di reparti tecnici, ma vengono scoperti da dipendenti non tecnici.**

La maggior parte dei ladri (54%) ha utilizzato una e-mail della rete aziendale, un canale di accesso remoto alla rete o un trasferimento di file in

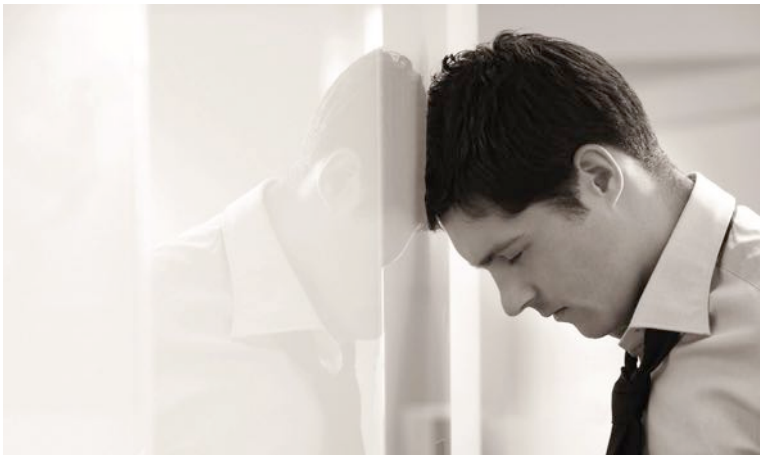

rete per estrarre i dati rubati. Tuttavia, la maggior parte dei furti di proprietà intellettuale da parte dei dipendenti è stata scoperta da colleghi di reparti non tecnici piuttosto che da quelli che lavorano nell'area IT dell'azienda.

**I fallimenti aziendali possono indurre gli addetti ai lavori a pensare di rubare la proprietà intellettuale dell'azienda.**

Nel caso del furto interno, si assiste ad un aumento di questo reato quando il dipendente è stanco di "pensarci" e decide di agire o sono altri a chiederglielo. Questo accade spesso dopo un avvenimento percepito come un fallimento professionale o nel caso di aspettative non soddisfatte. Questa demarcazione tra intenzione e azione spiega perché alcuni furti di insider sembrano essere spontanei, mentre in realtà non lo sono.

Dopo aver tracciato il profilo della tipica minaccia insider, vediamo come affrontare questo rischio e le possibili misure di mitigazione. L'ICAR offre un approccio interessante. Nella sezione del sito web dedicata alla sicurezza delle infrastrutture[2] , viene descritto il concetto di *"Persone come sensori".*

*"La componente umana del rilevamento e dell'identificazione di una minaccia interna è rappresentata dal personale di un'organizzazione. Collaboratori, coetanei, amici, vicini, familiari o osservatori casuali sono spesso in grado di*



*comprendere e conoscere le predisposizioni, i fattori di stress e i comportamenti di un dipendente che potrebbe meditare di compiere atti dolosi. Quando si osserva il comportamento umano, si devono tenere presenti due capacità importanti:*

*Saper ascoltare l'altra persona attraverso i suoi criteri, non i vostri. Non date per scontato che qualcuno chieda aiuto o chieda di essere fermato, o che parli delle sue intenzioni nello stesso modo in cui potreste farlo voi.*

*Ascoltate l'altra persona con gli occhi. Le persone spesso rivelano le loro intenzioni attraverso la comunicazione non verbale. "*

Esiste anche una serie di indicatori che vale la pena menzionare, in quanto forniscono un contesto più profondo e dettagli preziosi per identificare i segnali di una minaccia interna.

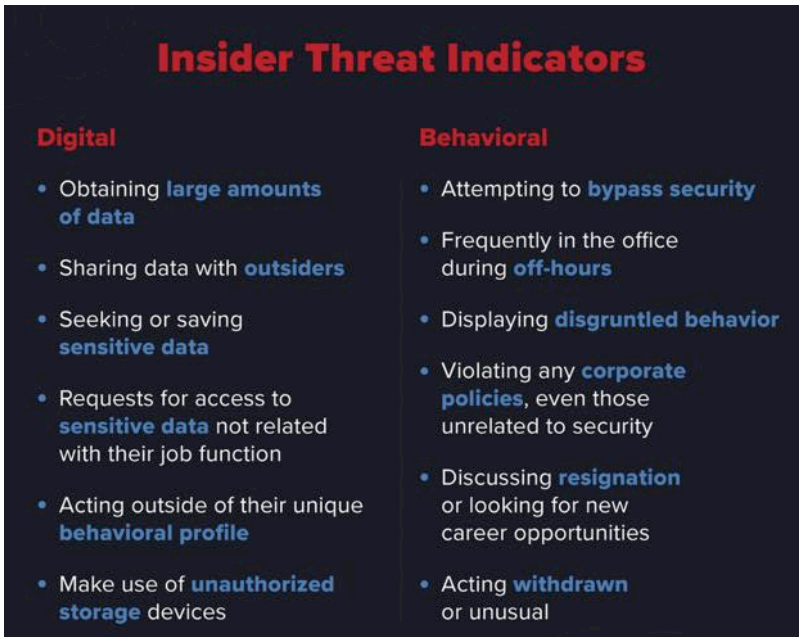
- **Gli indicatori personali** sono una combinazione di predisposizioni e fattori di stress personali che colpiscono un dipendente in un particolare momento e che possono trasformarlo in una minaccia o spingerlo ad agire.
- **Gli indicatori del percorso di carriera** sono eventi che si sono verificati prima che una persona fosse assunta da un'organizzazione o prima che avesse accesso alla rete dell'organizzazione.
- **Gli indicatori comportamentali** sono azioni che possono essere osservate direttamente da colleghi, personale delle risorse umane, manager di linea e tecnologia. Nel corso del tempo, i comportamenti formano un filo conduttore di attività da cui si possono evincere alcuni cambiamenti come indicatore di minaccia.
- **Gli indicatori tecnici** riguardano l'attività della rete e degli utenti e richiedono l'applicazione diretta di sistemi e strumenti informatici per essere rilevati.
- **Indicatori organizzativi/ambientali:**
  - Le politiche e le pratiche culturali aziendali possono svolgere un ruolo importante nella creazione o nella gestione di una minaccia interna.
  - I fattori ambientali possono intensificare o attenuare i fattori di stress che possono contribuire ai cambiamenti comportamentali e alla progressione di un individuo da dipendente fidato a minaccia interna. Questi fattori sono spesso legati alle politiche organizzative e alle pratiche culturali.
- **Gli indicatori di violenza** sono comportamenti specifici o insiemi di comportamenti che possono causare paura o preoccupazione che una persona possa agire; questi comportamenti includono, ma non sono limitati a, intimidazioni, molestie e bullismo.

Infine, è importante ricordare che con l'evoluzione delle tecnologie di intelligenza artificiale, come l'*apprendimento automatico,* è possibile combinare l'approccio comportamentale con strumenti tecnici come i metadati della rete o dell'utente. Questo accelera il processo di rilevamento di diversi ordini di grandezza.

Che si tratti di comportamenti *"Smash and Grab"* o *"Slow bleeding"*, l'intelligenza artificiale sarà in grado di generare indicatori utili a partire dal «noise" (insieme di dati) del flusso di rete dell'azienda.

La combinazione di diversi tipi di indicatori può anche creare un valore aggiunto e quindi migliorare la preparazione di un'azienda contro le minacce interne.

Un esempio che abbiamo visto di recente è quello di un dipendente che si dimette e durante il periodo di preavviso inizia a raccogliere ed estrarre dati. In questo scenario specifico, la combinazione di indicatori non tecnici - le dimissioni - con un approccio di threat hunting - la ricerca di anomalie nei metadati di rete - può essere molto vantaggiosa. ■

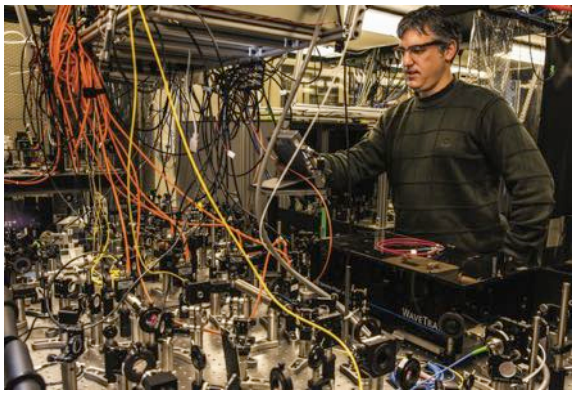



1 Eric D. Shaw, Harley V. Stock, Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall, Symantec 2011 (https://static1.squarespace.com/static/596a623ba5790afcec9c024e/t/59c9e063a803bb62117213c0/1506402404657/Symantec+Malicious+Insider+Whitepaper+FINAL2.pdf)
2 https://www.cisa.gov/detecting-and-identifying-insider-threats

# Automazione e crittografia avanzata: idee brillanti dal passato per migliorare la sicurezza futura?

Autore: Laurent Chrzanovski*

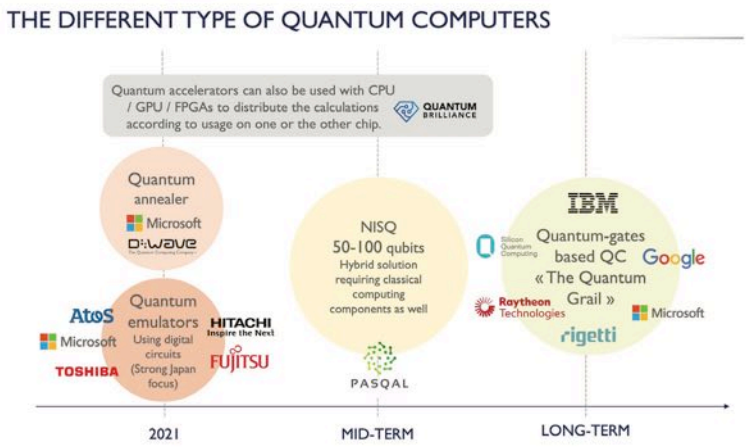
Non abbiamo dubbi sul fatto che il futuro dell'automazione, ma anche dell'AI e della sicurezza sarà quantico. Tuttavia, i server quantici e l'informatica quantica sono (e saranno per molto tempo) estremamente costosi e richiedono specialisti di altissimo livello per il loro funzionamento.



*Uno specialista imposta un computer quantico al Duke Quantum Center © Duke University*

Pertanto, se non si è una grande azienda (ad esempio, una top 200 di Forbes), investire in server e arruolare programmatori quantici è semplicemente impossibile.

Di conseguenza, i servizi quantici di alto livello sono e saranno forniti come *"pay per service"* da pochissime aziende informatiche *"above the top"*, cioè principalmente dalle GAFAM e dai loro concorrenti cinesi - indipendentemente da chi sia il produttore del hardware quantico -, a cui si possono aggiungere alcune decine di aziende statunitensi, britanniche, europee, russe e israeliane.




*Lo sviluppo dei produttori di server quantici*
*© Yole Quantum Technologies 2021. Market and Technology Report.*

Il problema con le GAFAM e i loro concorrenti asiatici rimarrà per ogni tipo di piccola, media o grande impresa e può essere riassunto nella semplice domanda *"ci si può fidare di loro anche se si pagano i loro prodotti? "*.

Le enormi preoccupazioni sollevate in tutta l'UE dopo la pubblicazione del rapporto ufficiale del governo olandese lo scorso febbraio, e dei consecutivi rapporti del mese di marzo, sulle carenze in materia di privacy in Teams, OneDrive Sharepoint e Azure AD di Microsoft, seguiti a giugno dal rapporto

svizzero dell'Incaricato Federale della protezione dei dati e della trasparenza (1), confermano ancora una volta atteggiamenti e comportamenti scorretti dei GAFAM (e delle loro controparti asiatiche). Queste pratiche corrispondono esattamente a quanto studiato tecnicamente da Shoshana Zhuboff (2) e, filosoficamente, da Slavoj Zizek (3).

**Privacy test on Microsoft Teams: be careful with the exchange and storage of confidential personal data**

3 March 2022

The Dutch higher education sector and the Dutch government were recently advised not to discuss any (highly) sensitive information through the Microsoft Teams communication platform. This follows from a privacy test conducted by Privacy Company, commissioned by SURF and the Ministry of Justice and Security. If you work with (special categories of) personal data, read on to find out what this means for your work or studies.

*La pagina per studenti e ricercatori dell'Università di Amsterdam dettagliando come e quando utilizzare Teams.*

## Crittografia avanzata come alternativa

L'ultimo rapporto del NIST, redatto da N. Moha (4), che esamina le attuali fasi di sviluppo delle tecniche di crittografia avanzata nell'ottica di una futura standardizzazione - una nuova versione dell'Advanced Encryption Standard (NIST-AES) del 2001 - dimostra che ci vorrà ancora tempo, perché sono stati rilevati non pochi problemi di sicurezza in ciascuno dei nuovi prodotti di ricerca sottoposti a un'analisi avanzata da parte di oltre 80 aziende statunitensi. Dal rapporto emergono livelli deboli di resilience soprattutto nelle fasi di *parametrazione ed implementazione* dei prodotti.

Nel frattempo, i più grandi gruppi di criminalità informatica (e non solo quelli state-sponsored) non aspettano e quasi tutti i prodotti disponibili sul mercato possono essere decifrati, come è stato recentemente dimostrato (5). Tutto dipende soltanto da quanto un'azienda vuole investire per sapere tutto sul suo concorrente, secondo la serie di offerte (illegali) di *"pay-per-service"*, allineate in funzione del livello di crittografia e degli strumenti di sicurezza utilizzati dalla società target.

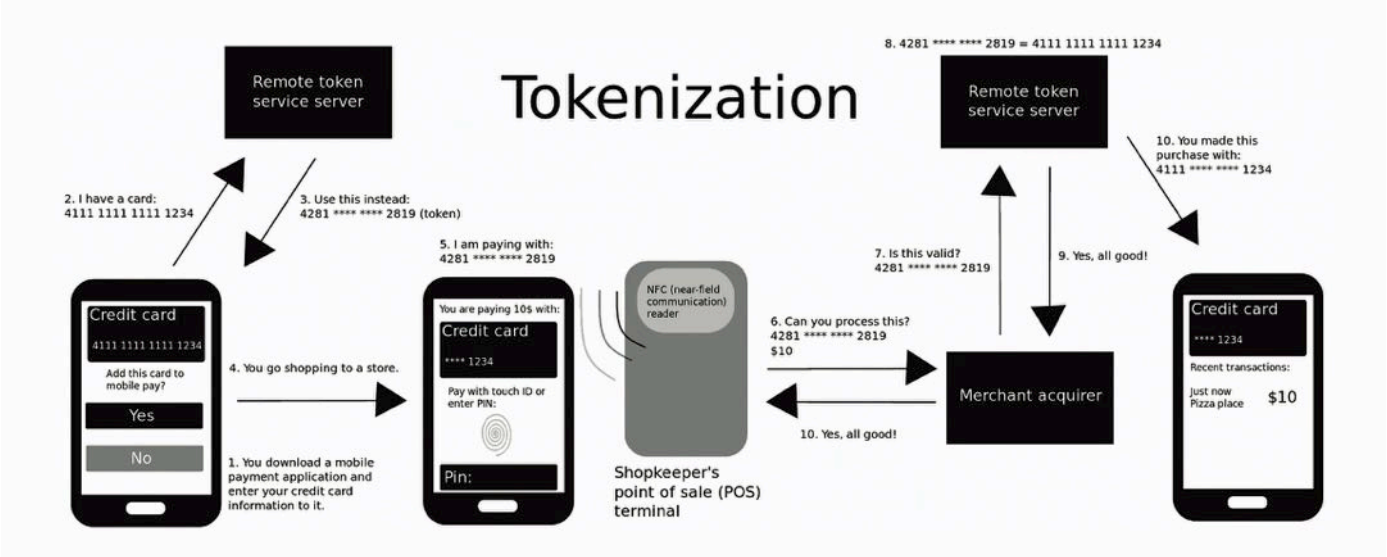

*Principali tipi di attacchi contro sistemi di crittografia, esclusi quelli legati al fattore umano © Krademy*

## BIO

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

Anche la *tokenizzazione* dei dati cifrati, che fornisce sicuramente una delle migliori alternative, è recentemente diventata oggetto di molte ricerche che ne hanno rivelato i "contro" (6) : i token vanno affidati ai migliori specialisti tecnici e non bisogna mai dimenticare che ogni tecnica di *tokenizzazione* ha una vita molto breve prima di diventare "attaccabile".

Quindi... quali saranno le possibili nuove strade della crittografia e quindi dell'automazione avanzata? La ruota non deve essere reinventata ogni anno, e le migliori aziende di sicurezza lo hanno capito da decenni. Il diventare sempre più transdisciplinari le ha portate, a volte con grande successo, ad applicare concetti già presenti nella filosofia greca nelle conquiste tecniche fatte ad uso di altre scienze durante il *"siècle des lumières"*, cioè l'Ottocento.




Fu proprio in quel periodo che Max Karl Ernst Ludwig Planck inventò il termine *quanta* per spiegare il mistero delle unità discrete scambiate da una radiazione elettromagnetica quando interagisce con la materia, dando vita alla costante di proporzionalità *h*, denominata "costante di Planck", base stessa della *vecchia teoria quantica*.

Tra la ricchezza delle scoperte dell'Ottocento, due di esse forniscono oggi capacità applicative molto interessanti per i sistemi di crittografia di nuova generazione o semplicemente per aumentare drasticamente la resilienza dei sistemi di crittografia avanzati disponibili oggi e nel prossimo futuro.

## Teoria dell'entropia applicata alla crittografia

L'entropia, vocabolo creato nel 1867 dal fisico tedesco Rudolf Julius Emanuel Clausius a partire dal termine greco antico τροπή, che significa *"trasformazione"*, costituisce il punto centrale della seconda legge della termodinamica dello stesso Clausius. Esso afferma che l'entropia dei sistemi isolati lasciati all'evoluzione spontanea non può diminuire con il tempo, poiché essi arrivano sempre a uno stato di equilibrio termodinamico in cui l'entropia è massima (7).

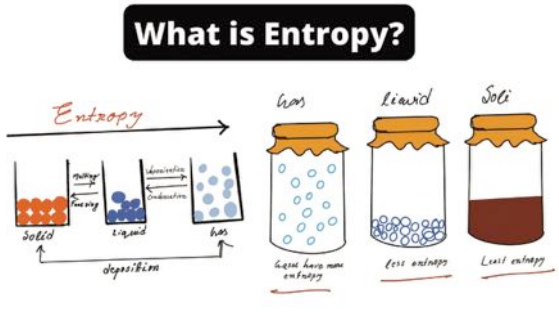
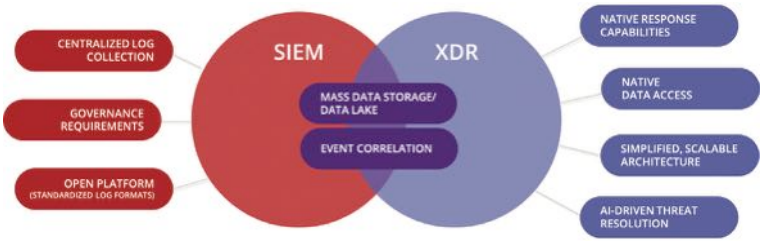
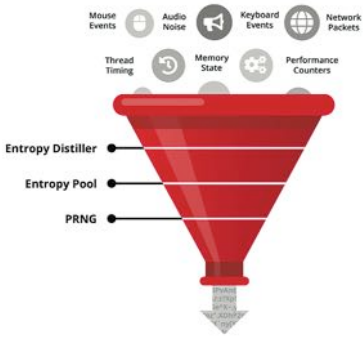



*Immagine © microbiologynote.com*

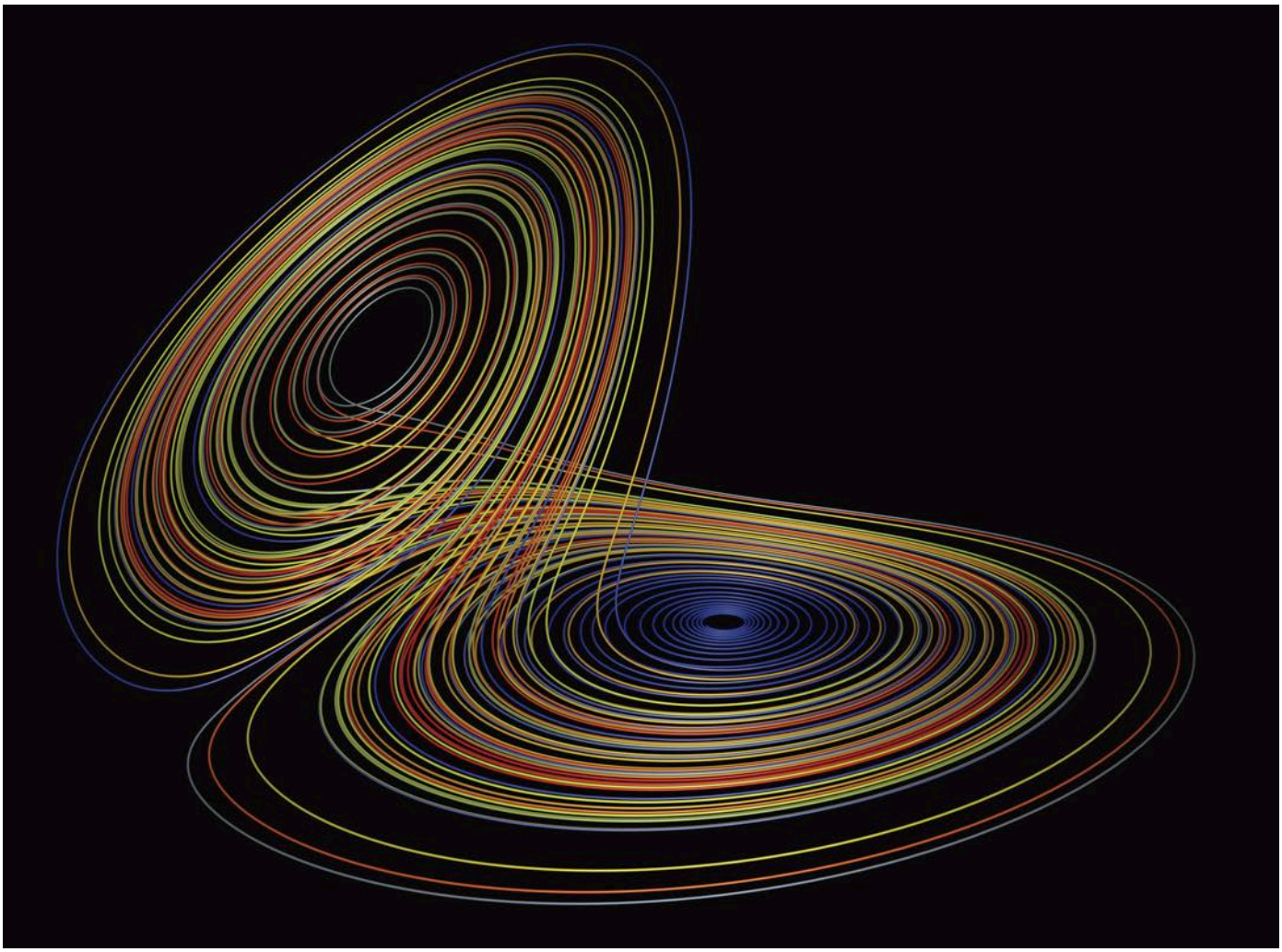
Senza che gli utenti lo sappiano, la teoria dell'entropia è uno dei concetti fondamentali utilizzati per costruire i più recenti sistemi di difesa automatizzati noti come XDR *(Extended Detection and Response)*, che aggiungono agli strumenti difensivi di un'azienda una tecnologia che al momento viene definita come *"the ultimate tool"* per proteggere un'azienda e la sua strategia di automazione. Come tale, l'XDR è ormai proposto come prodotto da tutte le major dell'IT e della cyber-security.




Ma l'entropia è anche una delle basi stesse della crittografia, come perfettamente ripreso da Edgar e Manz (8): *"L'entropia è la base su cui operano tutte le funzioni crittografiche. L'entropia, nella sicurezza informatica, è una misura della casualità o della diversità di una funzione che genera dati. I dati con un'entropia completa sono completamente casuali (random) e non possono essere trovati matrici significative"* (traduzione: autore). Quasi ogni mese vengono pubblicati nuovi sviluppi sull'uso dell'entropia nel campo del random, alcuni dei quali spiegano perfettamente il meccanismo, come ad esempio il rapporto sintetico di PKWare (9) o la recente pagina del blog di Crypto4A (10).

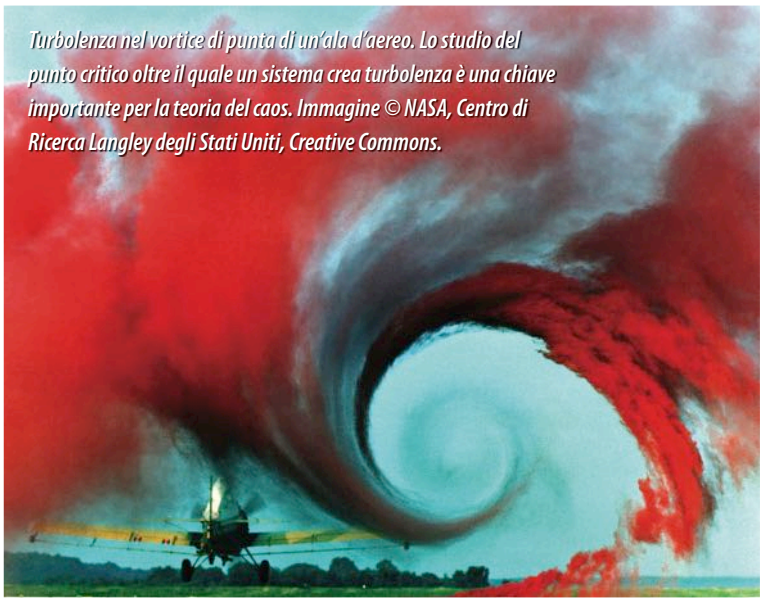



*Flusso di uscita random basato su una «vera» chiave random*
*© Cypto4A blog*



## La teoria del caos applicata alla crittografia

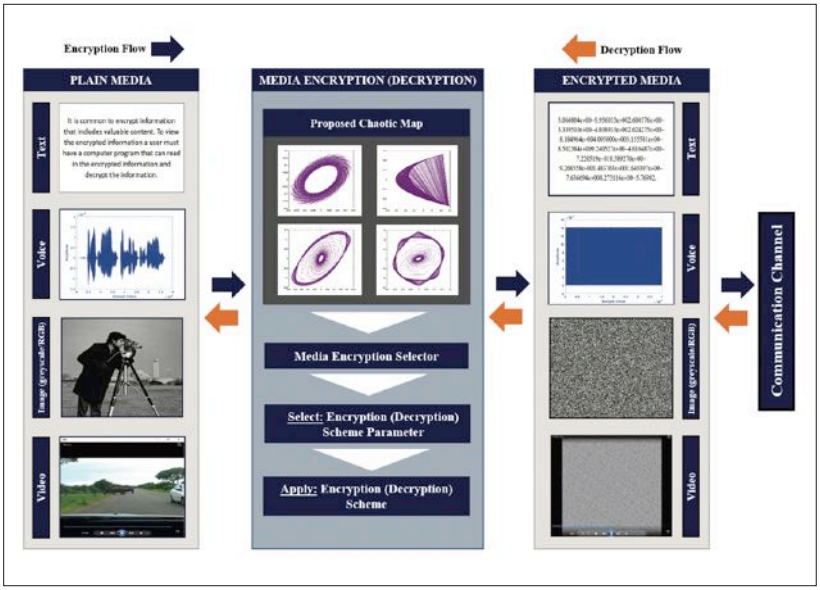
Uno dei "padri" della teoria del caos è Henri Poincaré. Negli anni ottanta dell'ottocento, studiando il problema dei tre corpi, scoprì che possono esistere orbite non periodiche, ma non sempre crescenti né prossime a un punto fisso (11).



*Turbolenza nel vortice di punta di un'ala d'aereo. Lo studio del punto critico oltre il quale un sistema crea turbolenza è una chiave importante per la teoria del caos. Immagine © NASA, Centro di Ricerca Langley degli Stati Uniti, Creative Commons.*

Tuttavia, gli studiosi hanno discusso fino agli anni '70 per definire meglio una teoria completa e la sua applicazione, soprattutto nei campi dell'elettronica, dei primi modelli di calcolo, della meteorologia, della geologia e dell'economia.

Da un punto di vista delle scienze informatiche vi è la necessità di feedback e di controllo (e quindi da qui la nascita del *command and control*) per evitare un elevato livello di caos e di turbolenze. Negli ultimi decenni però, la teoria del caos è stata utilizzata anche in crittografia, spesso con risultati deludenti perché i *pattern* scelti erano troppo facili da indovinare - binari oppure ispirati all'ADN umano (12). Negli ultimi cinque anni, però, la tecnica è tornata prepotentemente in ascesa, grazie al gran numero di ricercatori informatici che hanno proposto nuovi approcci e schemi estremamente promettenti sia per i loro aspetti innovativi che per la loro affidabilità, almeno nelle fasi di sperimentazione (13) (14), in special modo per rendere illeggibili contenuti testuali, vocali e multimediali (15).




*Struttura schematica dei processi di cifratura e decifratura di una pipeline «a chaos»*
*© Yasser et al. 2020, fig. 1, p. 4*

## Cosa dobbiamo fare?

Non importa quale sistema di automazione e di crittografia decidiate di utilizzare, perché il vero problema rimane, anche con le tecnologie più avanzate, una scarsa capacità di gestione di questi ultimi tools e il fattore umano. Ricorderemo in conclusione uno dei leitmotiv ribadito nei ricchi dibattiti tenutisi durante la prima edizione annuale del *"Cyber Espionage Awareness Day for Business"* (Bucarest, 14 giugno). In quell'occasione, tutti gli specialisti dei settori pubblici e privati hanno ripetuto quattro regole essenziali e semplici:

1. *ridurre la quantità di dati generati dalla vostra azienda* (recenti rapporti hanno verificato, negli ultimi 5 anni, una moltiplicazione con esponenziale 10 dei dati prodotti quotidianamente dalle aziende, mentre la maggioranza delle organizzazioni non ha registrato una crescita del numero di clienti, di fornitori, di dipendenti, di benefici o di segmento di mercato).
2. *ridurre la quantità di dati condivisi o inviati.*
3. *prevenire il fattore umano:* i vostri dati possono essere salvati dopo la crittografia, ma prima e, soprattutto, dopo la decifrazione da parte del destinatario, sono estremamente vulnerabili, mentre il fattore umano è stato la chiave del successo di oltre l'80% degli attacchi, conformemente al rapporto cyber 2022 del WEF.
4. *conoscere i programmi di spionaggio esistenti sul mercato:* da qualche anno, per i criminali informatici e quindi i loro clienti, è molto più facile spiare i dipendenti di un'azienda piuttosto che usare tecniche avanzate di *"brute force"* sui sistemi IT. La moltiplicazione di spyware zero-click per la voce, di archiviazione dei dati, di trasmissioni è enorme e la gamma delle loro capacità è ben spiegata a seconda del loro prezzo: da 2,5 milioni di dollari (di livello militare, zero-click, quasi inosservabile) a 100.000 dollari (un solo click necessario) o molto meno (rilevabile se si dispone degli strumenti appropriati). ■

* Ringraziamo Mauro Vignati, docente presso l'Università della Svizzera Italiana nonché ex capo della sezione Cyber della Polizia Federale Svizzera, per i preziosi consigli e l'attenta rilettura del nostro testo.

(1) Cfr. Dutch Government (2022), DPIA on Microsoft Teams, OneDrive Sharepoint and Azure AD (June 2021) Data protection impact assessment on the processing of Diagnostic Data Version 1.1., Public Version, 16 February 2022, Dutch Ministry of Justice and Security, Strategic Vendor Management Microsoft, Google and AWS (SLM Rijk) and SURF, The Hague
(https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad)
Si vedano i recenti aggiornamenti sul sito dell'Università di Amsterdam: "Privacy test on Microsoft Teams: be careful with the exchange and storage of confidential personal data"
(https://student.uva.nl/en/content/news/2022/03/privacy-test-on-microsoft-teams-be-careful-with-the-exchange-and-storage-of-confidential-personal-data.html?cb)
Per la Svizzera, vedasi : "Esternalizzazione di dati personali in un cloud di Microsoft da parte della Suva (il Fondo nazionale svizzero di assicurazione contro gli infortuni, n.d.r.) – A causa di concezioni del diritto in parte contrastanti, l'IFPDT consiglia alla Suva di rivalutare la esternalizzazione di dati personali in un cloud gestito dal gruppo statunitense Microsoft." https://www.edoeb.admin.ch/edoeb/it/home/attualita/aktuell_news.html
(2) Shoshana Zhuboff (2019), The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power, Profile Books Ltd, London / Public Affairs, New York
(3) Slavoj Zizek (2019), Like a thief in broad daylight. Power in the Era of Post-Humanity, London, Penguin
(4) Mouha N. (2021), Review of the Advanced Encryption Standard (NISTIR 8319), NIST 2021 (https://doi.org/10.6028/NIST.IR.8319)
(5) Hazhirpasand M., Ghafari M. (2021), Cryptography Vulnerabilities on HackerOne, in : The 21st IEEE International Conference on Software Quality, Reliability and Security (QRS), pp. 18-27 (doi: 10.1109/QRS54544.2021.00013)
(6) see the synthesis of the problematic in Malviya G. (2021), What is a Token? What are its Pros and Cons?, Loginradius Blog, 21.08.2021 (https://www.loginradius.com/blog/identity/pros-cons-token-authentication/)
(7) Clausius, R. (1867), The Mechanical Theory of Heat – with its Applications to the Steam Engine and to Physical Properties of Bodies. London: John van Voorst.
(8) Edgar T.W., Manz D.O. (2017), Chapter 2 - Science and Cyber Security, in Edgar T.W., Manz D.O. (eds.) Research Methods for Cyber Security, Syngress, pp. 33-62 (doi.org/10.1016/B978-0-12-805349-2.00002-9)
(9) PKWare (2018), The Entropy Problem. Random Data and Secure Cryptography, PKWare White Paper
(10) Crypto4A (2021) Why We Need Entropy in Cybersecurity, Crypto4A blog, May 10, 2021 (https://crypto4a.com/blog/why-we-need-entropy-in-cybersecurity/)
(11) Poincaré J.H. (2017), The three-body problem and the equations of dynamics : Poincaré's foundational work on dynamical systems theory. Popp Bruce D. (Translator). Cham: Springer International Publishing, 2017
(12) Kocarev L. (2001), Chaos-based cryptography: A brief overview, in IEEE Circuits and Systems Magazine, vol. 1, no. 3, pp. 6-21, 2001 ( doi: 10.1109/7384.963463)
(13) Amer Sharif et al. (2021), Chaos-based Cryptography: A Brief Look Into An Alternate Approach to Data Security, in: Journal of Physics: Conference Series 1566, 2020 (doi:10.1088/1742-6596/1566/1/012110)
14) Qiao Z. (2021), Nonlinear dynamics, applications to chaos-based encryption, Cryptography and Security, École centrale de Nantes, 188 p. (https://hal.archives-ouvertes.fr/tel-03200707)
15) Yasser et al. (2020), A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications, in Entropy 2020:22, 1253 (https://doi.org/10.3390/e22111253)


**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

# L'infosfera ha bisogno dell'intelligenza dell'uomo e di un'etica pratica per scandire il progresso della civiltà.

## Intervista VIP a Luciano Floridi.

Autore: Massimiliano Cannata

Con la pubblicazione del saggio *Etica dell'intelligenza artificiale* (ed. Raffaello Cortina) Luciano Floridi, professore ordinario di Filosofia e Etica dell'Informazione all'Università di Oxford e di Sociologia della Cultura e della Comunicazione *all'Alma Mater Studiorum Università di Bologna,* aggiunge un importante tassello per la costruzione di un sistema filosofico finalizzato a spiegare il profondo cambiamento d'epoca determinato dall'eccezionale sviluppo delle tecnologie digitali, che segnano la contemporaneità. Teorico della *"Quarta rivoluzione",* la ricerca dello studioso conduce all'analisi di quel "salto ontologico" che ha proiettato l'individuo ad "abitare" la dimensione dell'infosfera, in cui reale e virtuale sono due facce inscindibili della stessa realtà con tutte le conseguenze che sul piano epistemologico ed esistenziale questo comporta.

***Prof Floridi questo ultimo lavoro è orientato alla sistematizzazione dell'etica. I grandi del pensiero in epoca anche molto remota, da Aristotele a Kant per citare figure poste a fondamento di tutta la cultura del mondo occidentale lo hanno fatto lasciando un'impronta indelebile. Al di là di questi paragoni di certo ingombranti e venendo all'attualità del suo interessante saggio Lei scrive nella parte introduttiva che l'IA ha bisogno di una cornice concettuale più che di una spiegazione storico tecnologica, per essere compresa. Possiamo partire da questa sua precisazione, che appare importante in quanto possiede le sembianze di un pronunciamento di metodo?***


Ci tengo a precisare subito che impegnarsi a ricostruire il percorso cronologico dello sviluppo delle tecnologie, lavoro per altro meritevole, è insufficiente a fornire un contributo efficace alla loro comprensione. Il saggio è centrato sull'etica, come lei accennava nella domanda, ma questo non vuol dire necessariamente occuparsi degli aspetti cognitivi e intellettuali in modo sganciato dalla realtà. Al contrario, il mio intento è quello di indagare l'impatto concreto dello sviluppo tecnologico nella nostra vita quotidiana. Lo studio si concentra su alcune questioni procedurali, senza fare nessun processo alle intenzioni, soprattutto senza etichettare con "pregiudizi" di valore l'impetuoso sviluppo del digitale, che è un dato oggettivo incontrovertibile. Non c'è nessuna oscura "macchinazione" dietro le quinte, fortunatamente il progresso della scienza e delle tecnologie va avanti a dispetto delle false convinzioni e dei pregiudizi, che spesso si alimentano sui mass media e i social.

***Essenziale appare nella trattazione il divorzio tra la capacità di risolvere problemi e l'intelligenza nel farlo. La differenziazione tra mezzo***

***e strumento rimane essenziale per mantenere lucidità nell'indagine scientifica, ma rimane un principio difficile da attuare, tanto da sollevare le preoccupazioni di tanti studiosi, il caso più eclatante è quello del filosofo Emanuele Severino, che negli ultimi scritti paventava un'irriducibile "una cieca volontà di potenza della tecnica, divenuta fine a sé stessa". Preoccupazioni mal poste?***

Purtroppo, confesso la mia ignoranza nei confronti del lavoro di Severino e non vorrei pronunciarmi su cose che non conosco. Per rimanere al nostro ambito di riflessione credo che vada fatta una distinzione tra la capacità di agire con successo e la necessità di esercitare l'intelligenza nel farlo. Nei nostri comportamenti, essere intelligenti è vitale, ma l'IA opera con notevole successo senza alcun uso dell'intelligenza e questo è straordinario. Vi sono automobili con guida largamente autonoma che fanno i loro percorsi nelle città, ma questo non vuol dire che non serve l'intelligenza se guidiamo noi. L'automobile senza un uomo al volante ha la stessa intelligenza del frigorifero, non dimentichiamolo. Quello che va osservato è che il delta tra capacità di azione e intelligenza aumenterà sempre di più. Non per questo il nostro apporto di esseri razionali diventa superfluo, perché saremo sempre più chiamati a governare i sistemi complessi, e a fare delle scelte con un numero crescente di variabili. Il mio robot può tagliare l'erba meglio di me, ma è il momento giusto di farlo? E dovrà tagliare prima quella del giardino davanti casa o quella dietro la cucina? L'IA risolve un problema e paradossalmente lo rende "stupido". Pensiamo al gioco degli scacchi, che un computer può condurre con padronanza e meglio di qualsiasi giocatore. Se dovessimo farlo noi dovremmo esercitare tutta la nostra intelligenza.

***L'individuo che ormai abita l'*infosfera*, come si colloca tra quella che lei definisce* "riserva di capacità di agire" *e potenza crescente dell'IA?***

L'uomo fa parte di un sistema che ha bisogno dell'intelligenza per funzionare. Siamo dei mammiferi particolarmente evoluti, che processano dati e informazioni mediati dall'intelligenza. L'ambiente entro cui ci muoviamo sollecita le nostre facoltà "superiori". Le reti neurali e il machine learning non sono in sé una novità, li avevamo già da decenni, quello che nel passato mancava erano i dati e la potenza computazionale di cui oggi disponiamo. Pensiamo all'elicottero di Leonardo, interessante sul piano della concezione ideale, ma impossibile da far volare senza un motore, con le sole conoscenze e tecnologie in possesso in epoca rinascimentale. Con l'IA è stata segnata un'escalation, siamo entrati nella società dei big data, con tutte le conseguenze del caso. Il metaverso, realtà che si sta facendo strada, apre ulteriori fronti di riflessione, sarà molto importante capire e regolamentare questa nuova realtà, anche sul terreno della privacy e della tutela della riservatezza, elementi di rischio che, come le cronache ci fanno vedere ogni giorno, risultano fatalmente amplificati.

***Soffermiamoci su quest'ultimo aspetto, centrale per la nostra rivista. Lo sviluppo dell'IA e dei processi di automazione che cosa comportano sul piano della* cyber security*?***

La lettura del progresso è sempre biunivoca, per questo a mio giudizio non si deve essere né apocalittici né integrati, per usare una celebre dicotomia. Pensiamo ai sistemi assicurativi che oggi si fondano su previsioni elaborate con l'IA, oppure alle proiezioni sull'emergenza climatica, si basano sulla grande potenza di calcolo di cui disponiamo che ci consente di colmare tanti gap, di individuare gravi vulnerabilità, anticipando il verificarsi di molte minacce. Amplificazione del rischio e responsabilizzazione di chi opera nella cyber security è evidente che camminano insieme. Lo si sta vedendo anche in questa fase delicata, in cui sull'Europa spirano venti di guerra. Si paventano da più direzioni attacchi informatici, per sventarli occorrono azioni di sistema concertate, oltre all'esercizio di elevati livelli di competenza. Non mi stanco di ribadire in questo scenario difficile da leggere che rimane centrale il fattore umano. Lo studio delle azioni e dei comportamenti sono oggetto dell'etica che assume, ritorno a quanto ho affermato all'inizio, una valenza pragmatica essenziale per muoversi nel contesto attuale.

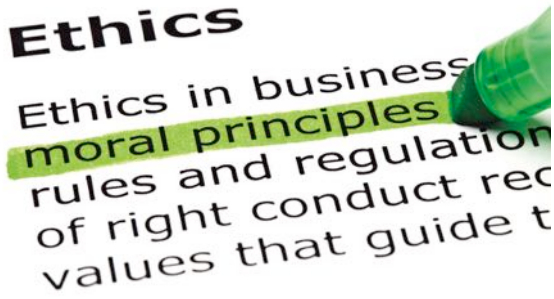
***L' "etica soft", cui è dedicato un capitolo del saggio, in che rapporto sta con l'etica tradizionalmente intesa?***

La definirei un'etica *"post compliance"*. Intendo dire che non ci troviamo di fronte all'etica classica, di stampo rigorista, come quella kantiana, per esempio, assoluta, indifferente rispetto alla legalità perché viene prima delle norme. La morale che a volte dobbiamo applicare si muove dentro il perimetro di leggi eticamente corrette. Faccio un esempio concreto: il minimo salariale risponde a dei criteri tabellari molto precisi, questo non vuol dire

## BIO

**Luciano Floridi è professore ordinario di Filosofia ed Etica dell'Informazione all'Università di Oxford, dove dirige il Digital Ethics Lab dell'Oxford Internet Institute, il Data Ethics Research Group dell'Istituto Alan Turing e il comitato consultivo sull'etica dell'European Medical Information Framework. Esperto di filosofia dell'informazione – disciplina di cui è considerato il fondatore -, di computer ethics, data ethics, di etica dell'informazione e di filosofia della tecnologia, è anche membro del comitato consultivo di Google sul "diritto all'oblio"; è professore ordinario di Sociologia della Cultura e della Comunicazione all'Università Alma Mater di Bologna, dove dirige il *Centre for Digital Ethics*.**

che non si possa riconoscere uno stipendio superiore ai lavoratori se lo si ritiene giusto. Allo stesso modo in una partita di calcio se qualcuno si fa male fortuitamente l'arbitro non è obbligato a fermare il gioco se non ravvisa irregolarità, questo non vuol dire che i giocatori non possano decidere di fermarsi ugualmente per prestare i soccorsi del caso. È questa "esigenza etica" che vive dentro norme che a loro volta rispettano i principi morali, l'oggetto principale dell'indagine che svolgo nel mio saggio.




***Esiste un'ulteriore declinazione dell'etica, quella che chiama in causa gli "algoritmi". Può chiarirci le idee anche in questo particolare ambito?***

Gli algoritmi che utilizziamo di solito non presentano delle criticità specifiche. Quasi sempre i problemi insorgono dall'utilizzo dei dati sui quali addestriamo gli algoritmi. Per esempio, le discriminazioni nascono perché sono già presenti nei dati che usiamo. Bisogna considerare che è l'alto livello di complessità interna di queste tecnologie che le rende poco trasparenti. L'esempio del traffico in città può far comprendere bene quello che intendo. È facile spiegare perché c'è traffico in una zona della città: per esempio piove, è l'orario di chiusura degli uffici e c'è lo sciopero dei mezzi di trasporto pubblico. Ma sarebbe impossibile determinare perché ogni guidatore è esattamente dove si trova, e quale tragitto e esigenze hanno causato il suo contributo al traffico. L'opacità è una componente quasi ineliminabile in sistemi così ramificati. La categoria della causalità, come la abbiamo appresa dalla fisica classica di stampo newtoniano, non regge più in sistemi lontani da equilibri elementari. Le scienze sociali lo sanno molto bene, e per questo perseguono letture macroscopiche dei loro fenomeni senza pretendere di entrare nel dettaglio e neppure nei micro elementi molecolari. La storia come disciplina di studio può insegnarci molto in questo senso. Rispetto ad eventi come la seconda guerra mondiali, sappiamo spiegare a grandi linee le cause, ma se dovessimo focalizzare momento per momento tutte le implicazioni di ogni singola azione e reazione, il problema della spiegazione risulterebbe incomprensibile. È evidente che bisogna adeguare il modello. La categoria di causa effetto nella logica lineare del determinismo classico non regge di fronte alle mutazioni di una società così dinamica, complessa e tecnologizzata. Lo stesso vale per le reti neurali. Va cambiato il metodo di indagine e l'ermeneutica dei dati e dei fenomeni, per trovare la giusta lettura del cambiamento d'epoca entro cui siamo immersi.

***Il "gambettò" e il cambiamento climatico. Un "neologismo" che incuriosisce. Di che cosa si tratta?***

Chi gioca a scacchi lo sa bene. Si tratta del sacrificio di un pedone, quindi di uno svantaggio, che però porta strategicamente alla vittoria della partita. È quello che dobbiamo fare se vogliamo osservare le leggi della sostenibilità. Il digitale consuma molta energia è vero, ma senza il digitale non potremmo avere tutti i servizi e le soluzioni che ci servono per salvare l'ambiente. In altre parole, alcuni sacrifici sono a volte necessari in vista di un fine superiore. Questo dovrebbero capirlo, su un altro piano, anche le classi dirigenti, spesso miopi, legate all'ultimo sondaggio. In vista di un progetto superiore, a volte vanno fatte scelte impopolari. Il progresso si genera anche così.

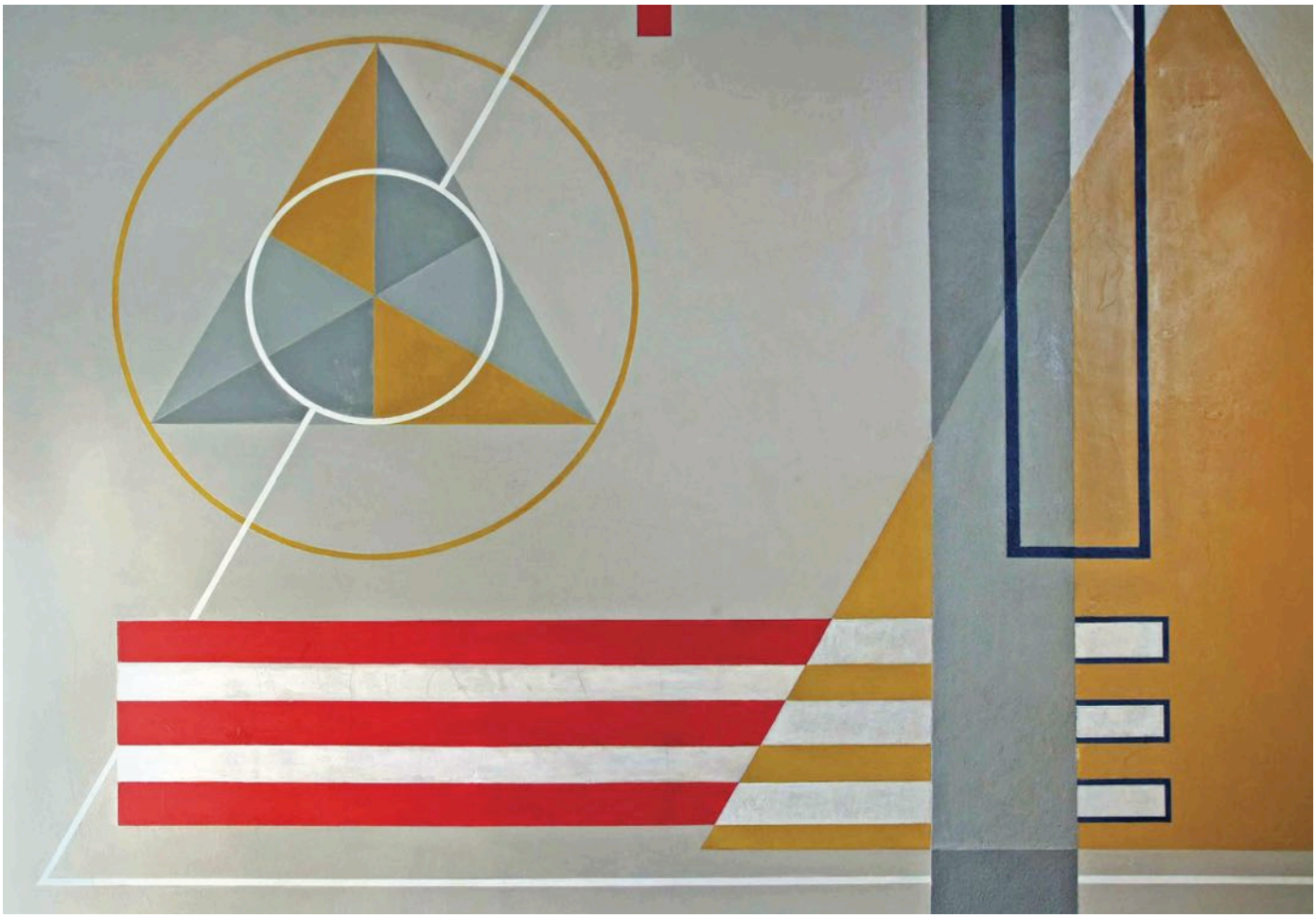
***Siamo un bellissimo "errore di natura", malgrado tutto, si legge nell'ultimo paragrafo del libro. Non le pare una conclusione troppo "sibillina"?***

Mantengo una posizione molto laica rispetto ai grandi interrogativi che riguardano l'origine dell'uomo e dell'universo. Noi esseri umani siamo un mistero, altamente improbabile dal punto di vista statistico. Abbiamo capacità uniche, meravigliose, possediamo una vita mentale straordinaria che non ha paragoni nel creato. Non so se ci sia un destino a monte e a valle, un architetto che abbia voluto tutto questo. So però che è andata così, abbiamo vinto il biglietto della lotteria di Madre natura. Dobbiamo sentire

tutto il peso e la responsabilità di questa condizione unica nel creato. Siamo gli unici esseri ad avere non solo diritti (anche gli animali ne hanno) ma anche doveri. Ecco perché mi piace definire l'umanità un magnifico errore di natura, un "beautiful glitch".

***Un'ultima sollecitazione sulla disciplina che con tanta passione lei insegna: la filosofia, che sembra oggi aver recuperato un fascino che sembrava appannato. Imprenditori, manager, consulenti, uomini delle istituzioni non esitano, infatti, a chiamare in causa quel sapere filosofico che sembrava destinato a finire nella cassetta dei vecchi arnesi, belli ma inutili. A che cosa è dovuta questa rivalutazione?***

Questa che lei chiama rivalutazione di quella che per molti aspetti è la regina delle discipline non deve stupirci. La filosofia è *design concettuale*, è il nutrimento di quella vita mentale che fa dell'umanità una "specie speciale". La saggezza di Socrate, la sua "dotta ignoranza" che spesso chiamiamo in causa è l'effetto di questo design concettuale che la filosofia compie fin dalle sue origini. La Repubblica di Platone è un ottimo esempio. La *Bauhaus* come scuola di design, si iscrive nella stessa logica. Quante lampade abbiamo, quante poltrone tutte esteticamente e funzionalmente affascinanti, a dimostrazione dell'infinita capacità che hanno le idee di rigenerarsi e di mescolarsi con il divenire del reale e delle nostre esigenze. Lo stesso avviene per le nostre creazioni concettuali. Una cosa che vorrei sottolineare infine: la filosofia deve avere comprensione e rispetto per tutte le attività umane, nessuna supponenza post-crociana è oggi ammissibile. Identificare, analizzare e capire i problemi pressanti con cui abbiamo a che fare e sviluppare buon design concettuale per risolverli questa è la filosofia di cui abbiamo bisogno, per essere all'altezza del nostro tempo. Il messaggio di fondo del libro è proprio questo. ■



# I nemici informatici monetizzano il ransomware: il punto di vista di CrowdStrike.

CROWDSTRIKE

Autore: Luca Nilo Livrieri

I dettagli delle transazioni e gli schemi di monetizzazione degli avversari informatici moderni rivelano insight fondamentali che contribuiscono ad aumentare il livello di difesa delle organizzazioni contro gli attacchi ransomware.

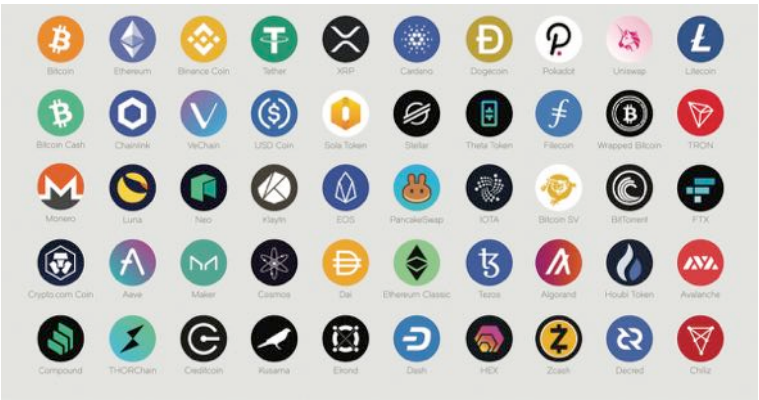
Negli ultimi anni, il crimine informatico si è evoluto notevolmente, trasformandosi da semplici attacchi *spray-and-pray* in un sofisticato ecosistema criminale incentrato su tecniche di monetizzazione altamente efficaci, che consentono agli avversari di massimizzare il loro successo e la loro profittabilità.

La monetizzazione è il passo compiuto dagli avversari per ricevere un pagamento al termine di un'operazione. Per evitare di essere scoperti, gli autori delle minacce evolvono costantemente i loro metodi attraverso prove ed errori. Una buona conoscenza del funzionamento di tale processo, inclusi i dettagli delle transazioni, il valore delle recenti compromissioni e gli avversari partecipanti, può aiutare le organizzazioni a combattere i moderni autori delle minacce e a difendersi da essi.

La caccia alle minacce di CrowdStrike offre ai decision-makers dell'area IT e della sicurezza spunti fondamentali riguardanti la monetizzazione dell'eCrime. A seguire, un'analisi dettagliata delle più recenti osservazioni e alcuni elementi utili per un elevato livello di difesa.

## Il ruolo primario delle criptovalute

Bitcoin è la criptovaluta preferita nelle campagne ransomware per diverse ragioni: è più facile da ottenere ed è disponibile su larga scala. I portafogli



### 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.**

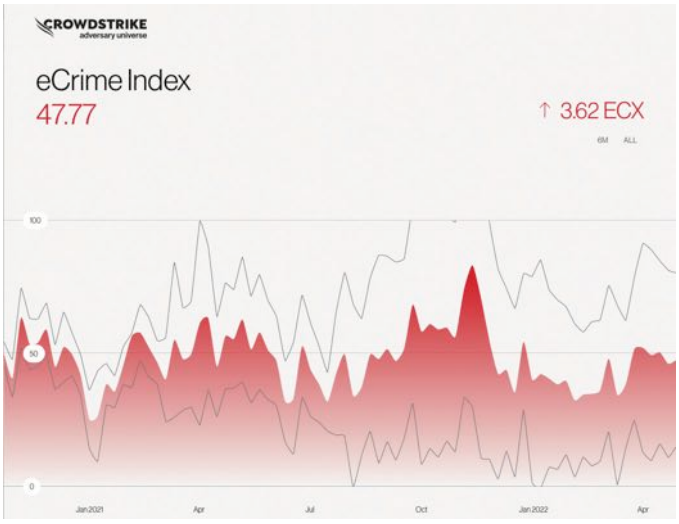
Bitcoin non richiedono informazioni personali identificabili, dunque chiedere un riscatto in Bitcoin facilita il pagamento da parte delle vittime e permette agli avversari di rimanere anonimi.

Tuttavia, non tutti i dettagli dei Bitcoin sono nascosti. Il valore di ogni transazione e il portafoglio Bitcoin sono visibili pubblicamente, consentendo agli attaccanti e alle forze dell'ordine di seguire i pagamenti fino alla loro destinazione finale. Mentre l'identità del titolare del portafoglio è nascosta, i Bitcoin possono essere scambiati con valute fiat in un numero qualsiasi di borse di criptovalute, dove l'identità degli avversari informatici può essere esposta.

Per aumentare l'anonimità, gli attaccanti utilizzano spesso i servizi di miscelazione, che ridistribuiscono i Bitcoin da varie fonti su diversi indirizzi per nascondere la fonte originale dei fondi e ostacolare l'analisi della transazione. Un altro metodo usato per garantire l'anonimato e impedire la tracciabilità dei fondi è il «salto di catena», in cui i criminali informatici convertono la valuta in un altro formato, come Monero (XMR), una forma di criptovaluta che molti aggressori preferiscono per tutelare l'anonimato.

## La variabilità delle richieste di riscatto

Secondo i dati del Financial Crimes Enforcement Network (FinCen) del Dipartimento del Tesoro degli Stati Uniti, il valore delle attività sospette legate al ransomware e segnalate nei Suspicious Activity Reports durante i primi sei mesi del 2021 era di 590 milioni di dollari USD, rispetto ai 416 milioni di dollari USD relativi a tutto il 2020. L'Intelligence di CrowdStrike ha inoltre rilevato un aumento del 36% della richiesta media di riscatto rispetto al 2020, per un totale di 6.1 milioni di dollari nel 2021.




## I broker di accesso creano i propri listini prezzi

I broker di accesso violano le infrastrutture delle vittime per poi vendere le credenziali (ottenute illecitamente o con altri metodi di accesso) nelle comunità clandestine. Gli operatori di malware o gli affiliati acquistano tali informazioni di accesso, evitando così di introdursi nella rete in modo indipendente, per eseguire attacchi più rapidi e mirati.

Il costo di questi accessi è variabile. L'Intelligence di CrowdStrike ha rilevato prezzi dai 100 dollari USD ai 64 mila dollari USD (il più alto identificato sino ad ora). I fattori che determinano tale costo includono il livello di privilegio concesso, il fatturato annuo stimato dell'azienda presa di mira, il numero di endpoint, quantità potenziale di dati disponibili per l'esfiltrazione e la reputazione del broker.

## Gli aggressori non pagati possono mettere all'asta i vostri dati

Qualora la vittima dell'attacco ransomware rifiutasse di soddisfare le richieste degli avversari, i dati esfiltrati potrebbero essere messi all'asta sul dark web o su siti di leak dedicati. Questa tattica consente agli autori delle minacce di guadagnare anche qualora il primo tentativo di monetizzazione non andasse a buon fine, oppure di


aumentare il loro profitto anche se la vittima dovesse pagare. Talvolta i dati vengono venduti ad altri avversari informatici, che potrebbero usarli per trovare nuove vittime o ottenere informazioni personali sull'identità per commettere frodi o pianificare ulteriori attacchi.

## L'ecosistema eCrime continua a prosperare

Il ransomware è probabilmente la fonte di reddito più popolare per i criminali informatici. Tuttavia, molti avversari fanno ancora affidamento su altre forme di monetizzazione. L'Intelligence di CrowdStrike ha scoperto che gli avversari utilizzano ancora diversi metodi tradizionali per generare fondi: ad esempio, offrono vari servizi per sostenere la più ampia economia sommersa, tra cui spambot, servizi di monetizzazione, pay-per-install e kit di exploit. Tra questi, EcoPanel è un pannello web personalizzabile che consente agli utenti di gestire le varie fasi della frode di rifornimento come modo per monetizzare l'eCrime. Come parte di questo processo, i criminali informatici usano dati rubati per comprare beni di elevato valore, per poi spedirli ad intermediari con sede negli Stati Uniti o in Europa. A loro volta, questi li rispediscono agli attori dell'eCrime, che li vendono sui mercati locali per ottenere fondi.

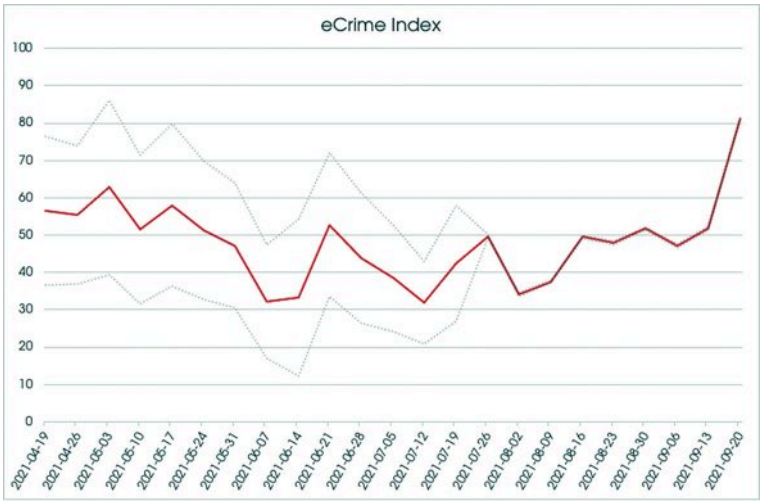

## I principali elementi di difesa

Comprendere come i cyber-criminali monetizzano le campagne ransomware è fondamentale per consentire alle aziende di implementare un'adeguata strategia di difesa. Ecco di seguito alcuni elementi utili:

1 **I dati aiutano a definire la strategia.** Gli avversari sono alla ricerca dei dati aziendali sensibili che, se ottenuti, potrebbero esporre l'azienda ad estorsioni o altre minacce. È necessario determinare il valore dei dati e dove questi risiedono per costruire una strategia di sicurezza a più livelli che dia priorità ai dati, intesa come risorsa più preziosa, affinchè possano essere protetti facendo leva su una gestione efficiente delle identità e dei principi di Zero Trust. La capacità di creare una difesa a più livelli e di pianificare gli imprevisti legati al potenziale fallimento dei suoi componenti è essenziale per proteggere i dati sensibili.

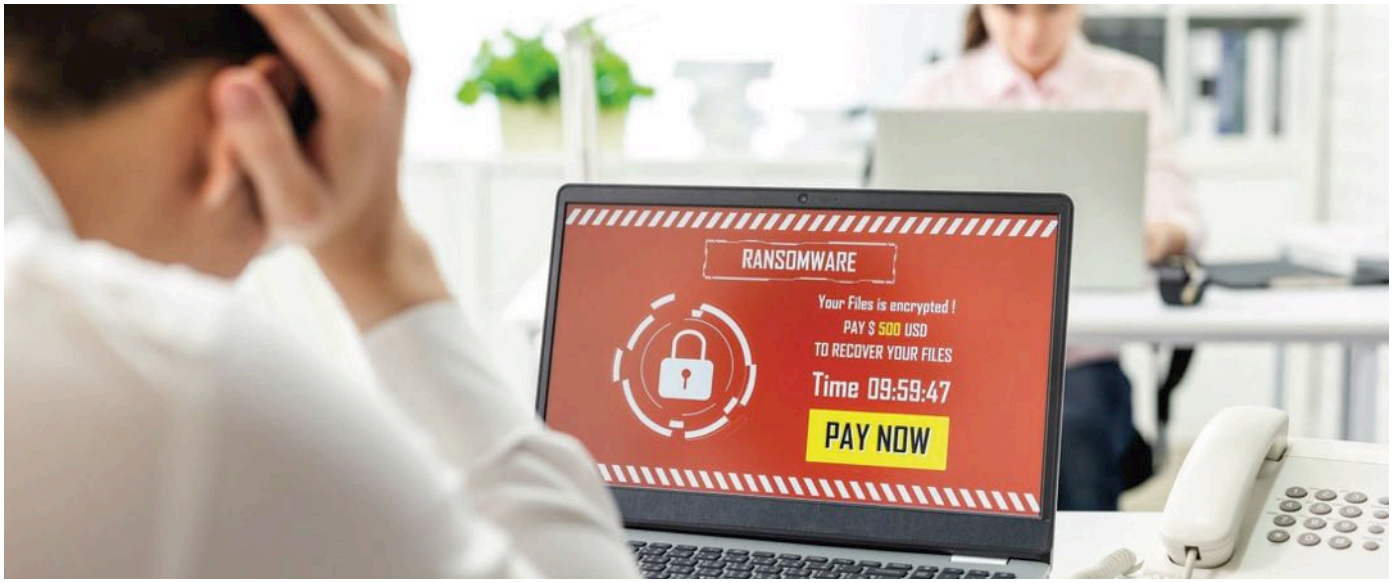
2 **La caccia alle minacce è fondamentale per tracciare la monetizzazione dell'eCrime.** il processo di monitoraggio continuo richiede un'attività di intelligence sulle minacce che consenta di comprendere chi potrebbe prendere di mira i dati, come potrebbero essere attaccati e il valore di tali dati all'interno dell'ecosistema della criminalità informatica, in modo da poter determinare come investire al meglio nelle soluzioni di monitoraggio.

3 **L'eCrime Index (ECX) di CrowdStrike aiuta a tracciare la monetizzazione del crimine informatico.** L'ECX si basa su una serie di dati relativi alla criminalità informatica, come le vittime di ransomware, le fughe di dati della caccia grossa, le attività di attacco e i tassi di criptovaluta, tutti ponderati in base all'impatto. L'ECX è utile per comprendere meglio le tendenze più ampie dell'ecosistema eCrime, che possono essere un fattore di determinazione dell'attività delle minacce.

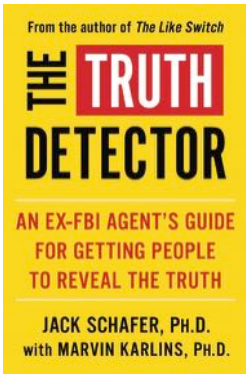



*Valori settimanali dell'ECX (in milioni di USD) iniziando con la data dell'incidente che ha colpito la the Colonial Pipeline (a destra) © Crowdstrike*

Il modello di business del cyber-crimine si evolve costantemente per fare spazio a nuove tattiche. Imparare a conoscere tali tecniche può aiutare gli addetti all'IT e alla sicurezza a comprendere meglio gli avversari e, di conseguenza, a rafforzare il livello di difesa della propria organizzazione. ■



# Fatti a bit e a pezzetti. Cosa possiamo imparare da un esempio di spionaggio aziendale?





Questo articolo è riprodotto e tradotto per gentile concessione degli autori. La sua versione originale è stata pubblicata per la prima volta come breve esempio in Schafer, J. e Karlins, M. (2020) ,The Truth Detector. An *Ex-FBI Agent's Guide for getting people to reveal the truth,* Simon & Schuster, New York, 144-150 (versione epub) e poi come articolo completo: Schafer, J. and Karlins, M. (2021), Hacked by Bits and Pieces: What Can We Learn from an Example of Corporate Espionage? *Journal of Information Security,* 12:3, 224-231. (https://doi.org/10.4236/jis.2021.123012 )

Autori: Jack Schafer, Marvin Karlins

## 1. Introduzione

Poiché l'archiviazione di informazioni proprietarie e riservate su computer estremizzati diventa una pratica aziendale comune, la necessità di sicurezza informatica diventa sempre più importante [1] [2].

Questa necessità è stata evidenziata dalle numerose violazioni della sicurezza che hanno coinvolto note multinazionali, tra cui Adobe, eBay, Equifax, LinkedIn e Yahoo [3] [4].


Quando i casi di spionaggio industriale nelle grandi aziende statunitensi vengono portati all'attenzione del pubblico, la maggior parte delle persone evoca immagini ispirate ai film hollywoodiani: super tecnologi della darknet con decine di computer e dispositivi di hacking in stile «James Bond» che utilizzano le loro conoscenze superiori e le loro invenzioni all'avanguardia per violare i firewall ed estrarre i dati desiderati.

Sebbene esistano questi mezzi di spionaggio altamente sofisticati, come nel caso del recente attacco ransomware a Colonial Pipeline (il più


grande oleodotto degli Stati Uniti), gli stessi risultati possono spesso essere ottenuti con mezzi molto più semplici.

In effetti, basta una persona, un telefono cellulare, un software facilmente reperibile e un piano d'azione per superare le più avanzate barriere di sicurezza aziendali e ottenere informazioni aziendali proprietarie.

L'obiettivo di questo articolo è quello di evidenziare, attraverso un esempio concreto, quanto segue:

1. l'importanza di rendersi conto e riconoscere che ogni individuo in un'organizzazione può essere un portale per un'intrusione informatica;
2. la necessità di formare adeguatamente le persone a essere vigili contro le truffe informatiche e a diffidare di qualsiasi richiesta di accesso a un computer.

## 2. Procedura

Per dimostrare quanto sia facile per un hacker intelligente accedere alle informazioni digitali, anche quando i dati sono protetti da misure di sicurezza informatica avanzate, forniamo qui un esempio di violazione dei dati. Ringraziamo l'esperto di cybersicurezza Nathan House per averci fornito questo esempio illuminante di spionaggio aziendale. La sua sfida, in qualità di aspirante hacker, consisteva nell'introdursi in una rete informatica protetta utilizzando solo il suo ingegno e un telefono cellulare.

## 3. Risultati

L'obiettivo di Nathan è quello di accedere al computer di una specifica azienda per estrarre informazioni a cui non avrebbe altrimenti accesso. Di seguito spiega, passo dopo passo, cosa sta facendo e perché lo sta facendo (quali informazioni sta cercando di ottenere).

**Chiamata n. 1: al centralino della società**

NATHAN: Buongiorno, ho un problema con il telefono dell'ufficio. Potete mettermi in contatto con qualcuno che possa aiutarmi?

OPERATORE: La metto in contatto.

SERVIZI TELEFONICI: Salve.

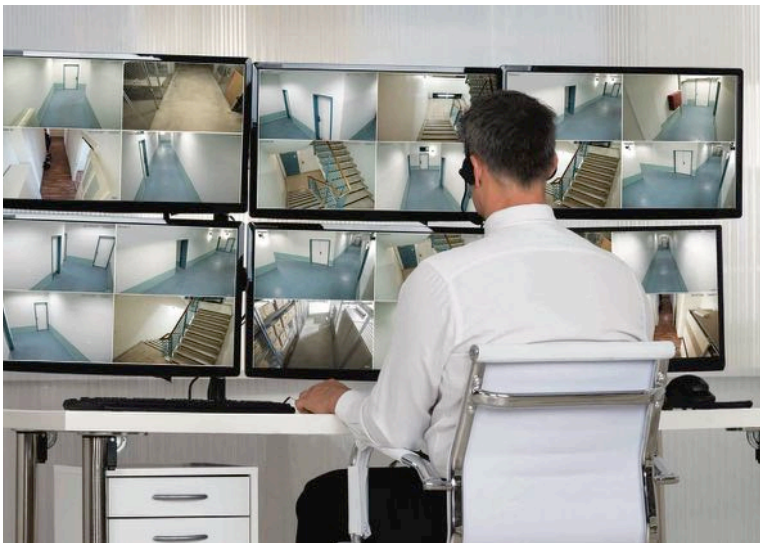
NATHAN: Buongiorno. Ho un problema con il telefono dell'ufficio. Scusate, ma sono nuovo qui. C'è un modo per

scoprire chi mi sta chiamando quando suona il mio telefono dell'ufficio? C'è l'identificazione del chiamante?

SERVIZI TELEFONICI: Non proprio, perché qui usiamo gli hot desk [Un hot desk è un ufficio condiviso da più persone, a volte da più persone durante i tre turni giornalieri.]. Visto che le persone usano abitualmente il cellulare, l'ID del chiamante non è spesso collegato a un nome. È un problema per voi?

NATHAN: No, ora va tutto bene. Capisco. Grazie. Arrivederci.

***Ora so che l'azienda utilizza gli hot desk e che l'ID del chiamante non è sempre richiesto. Pertanto, non è un problema se chiamo dall'esterno dell'azienda. Se fosse richiesta l'identificazione, potrei comunque evitarla.***



**Chiamata 2: al centralino dell'azienda**

NATHAN: Buongiorno, può passarmi la sicurezza dell'edificio?

OPERATORE: Ok.

SICUREZZA DELL'EDIFICIO: Buongiorno, come posso aiutarla?

NATHAN: Salve, non so se le interessa, ma ho trovato una carta d'accesso fuori dall'edificio che deve essere caduta a qualcuno.

SICUREZZA DELL'EDIFICIO: Basta restituircela. Siamo nell'edificio 3.

NATHAN: OK. Nessun problema. Posso chiedere con chi sto parlando?

SICUREZZA DELL' EDIFICIO: Mi chiamo Eric Wood. Se non sono qui, datelo a Neil.

NATHAN : Ok, è fantastico. Lo farò io stesso. Lei è il responsabile della sicurezza dell'edificio?

SICUREZZA DELL'EDIFICIO: Si tratta di fatto della Sicurezza delle strutture, il cui responsabile è Peter Reed.

NATHAN: Grazie mille. Arrivederci.

***Questo scambio mi ha permesso di conoscere i nomi di alcune persone del servizio di sicurezza, il nome esatto del dipartimento e del capo della sicurezza, e di sapere che sono loro a occuparsi delle tessere di accesso fisico.***

**Chiamata 3: al centralino dell'azienda**

NATHAN: Salve, chiamo da Agency Group Associates e mi chiedo se potete aiutarmi. Circa un mese fa ho avuto una riunione con alcuni impiegati delle vostre risorse umane, ma purtroppo il mio computer si è bloccato e ho perso i loro nomi.

OPERATORE: Certo, nessun problema. Lasciatemi dare un'occhiata a quel reparto. Ha idea dei loro nomi?

NATHAN: So che uno di loro era il capo delle risorse umane. All'incontro, tuttavia, erano presenti diverse persone.

OPERATORE (PAUSA): Ok, ci siamo. Il responsabile delle risorse umane è Mary Killmister. Il suo numero di telefono è XXX-XXXX.

NATHAN: Sì, mi suona familiare. Quali sono gli altri nomi dell'HR?.

OPERATORE: In HR, Jane Ross, Emma Jones...

NATHAN: Sì, sicuramente Jane ed Emma. Potrei avere i loro numeri, per favore.

OPERATORE: Certamente. Quello di Jane Ross è XXX-XXXX e quello di Emma Jones è XXX- XXXX. Vuole che gliene passi uno?

NATHAN: Sì. Puo' passarmi Emma, per favore?

***Ora conosco i nomi dei tre addetti alle risorse umane, compreso il capo dipartimento.***


**Chiamata 4: all'ufficio risorse umane dell'azienda**

RISORSE UMANE: Buongiorno, Emma Jones.

NATHAN: Salve, Emma. Sono Eric della Sicurezza delle Strutture nell'Edificio 3. Mi chiedevo se poteste aiutarmi. Abbiamo avuto un problema con il computer del database delle carte di accesso. Ieri sera si è bloccato e alcuni dati dei nuovi dipendenti sono andati persi. Sapete chi può dirci chi sono i nuovi dipendenti delle ultime due settimane, dato che le loro tessere di accesso non funzionano più? Dobbiamo contattarli e informarli il prima possibile.

EMMA: La posso aiutare in questo. Cercherò i nomi e glieli manderò via e-mail, se le va bene. Ha detto nelle ultime due settimane?

NATHAN: Nelle ultime due settimane, sì. È fantastico, grazie, ma sarebbe possibile inviarlo via fax perché condividiamo un computer per la posta elettronica e anche questo ha risentito del guasto al server.

EMMA : Sì, va bene. Qual è il vostro numero di fax? Oh, e come che si chiama lei?

NATHAN: Prenda nota che è per Eric. Dovrò trovare il numero di fax e richiamarla.

EMMA : Ok.

NATHAN: Sa quanto tempo ci vorrà per trovare le informazioni?

EMMA: Non dovrei impiegare più di trenta minuti.

NATHAN: Potrebbe iniziare a lavorarci subito? È piuttosto urgente.

EMMA: Ho alcune cose da fare questa mattina, ma dovrei avere i nomi entro questo pomeriggio.

NATHAN: È fantastico, Emma. Grazie. Quando ha finito, potrebbe chiamarmi subito per iniziare a riattivare le loro carte?

EMMA: Sì, certo. Qual è il suo numero?

NATHAN: Le darò il mio numero di cellulare. In questo modo sarà sicura di raggiungermi. Eccolo : XXX-XXX-XXXX.

EMMA: Ok, certo. Chiamerò quando avrò l'elenco.

NATHAN: Eccellente. Grazie, lo apprezzo veramente molto.

**Chiamata 5: al centralino dell'azienda**

NATHAN: Buongiorno. Può passarmi il supporto informatico?

OPERATORE: La collego subito... [Lunga attesa].

SUPPORTO IT: Salve, posso avere il suo numero di identificazione o il riferimento della sua pratica?

NATHAN: Ho solo una domanda veloce. Va bene così?

SUPPORTO IT: Di che cosa si tratta?

NATHAN: Un tizio della Reuters cerca di inviarmi una

presentazione e mi chiede qual è la dimensione massima dell'allegato.

SUPPORTO IT: Sono 5 megabyte, signore.

NATHAN: È fantastico, grazie. Oh, un'altra cosa. Ha detto che si trattava di un file .exe e che a volte si bloccano o qualcosa del genere.

SUPPORTO IT: Non sarà in grado di inviare un file eseguibile, perché gli scanner antivirus lo bloccheranno. Perché deve essere un file .exe?

NATHAN: Non lo so. Come può inviarmelo, allora? Potrebbe chiudere la zip o qualcosa del genere?

SUPPORTO IT: I file zip sono consentiti, signore.

NATHAN: Oh, un'ultima cosa: non riesco a vedere l'icona di Norton Antivirus nella barra delle applicazioni. Nell'ultimo posto in cui ho lavorato, c'era una piccola icona.

SUPPORTO IT: Qui utilizziamo McAfee. È solo un'icona diversa, quella blu.

NATHAN: Questo chiarisce tutto, allora. Grazie. Arrivederci.

***Ora so che per inviare un eseguibile via e-mail, deve essere prima zippato e pesare meno di 5 MB. So anche che utilizzano l'antivirus McAfee.***


**Chiamata 6: qualche ora dopo, una telefonata di Emma alle Risorse Umane.**

EMMA: Salve, sei Eric?

NATHAN : Sì, Salve.

EMMA: Ho l'elenco dei nuovi dipendenti per lei. Vuole che glielo mandi via fax?

NATHAN : Sì, per favore. Sarebbe fantastico. Quanti sono?

EMMA: Circa dieci persone.

NATHAN: Non sono sicuro che il fax funzioni correttamente qui. Potrebbe leggermeli ad alta voce? Penso che sarebbe più veloce.

EMMA: Ok. Ha una penna?

NATHAN : Sì, vada avanti.

EMMA: Sarah Jones, reparto vendite. Il regista è Roger Weaks... [legge il resto dell'elenco].

NATHAN: Ok, grazie. È stata di grande aiuto. Arrivederci.

***Ora ho un elenco dei nuovi dipendenti delle ultime due settimane. Ho anche i reparti a cui appartengono e i nomi dei loro responsabili. I nuovi dipendenti sono molto più suscettibili all'ingegneria sociale (influenza o controllo da parte di una fonte esterna) rispetto ai dipendenti di lunga data.***

**Chiamata 7: al centralino dell'azienda**

NATHAN: Salve, sto cercando di inviare un'e-mail a Sarah Jones ma non sono sicuro del formato dei vostri indirizzi e-mail. Lei lo sa?

OPERATORE: Sì, sarebbe sarah.jones@targetcompany.com.

NATHAN: Grazie.

**Email di ingegneria sociale**

Pochi minuti dopo, viene inviata un'email con indirizzo del mandante che sembra quasi alla perfezione l'indirizzo reale della security [messaggio di posta elettronica con un falso indirizzo del mittente].

**Da:** itsecurity@targetcompany.com.
**TO:** sar.jones@targetcompany.com.
**Oggetto:** Sicurezza informatica.

Cara Sarah,

In qualità di nuovi dipendenti dell'azienda, dovrete essere a conoscenza delle politiche e delle procedure di sicurezza informatica dell'azienda e, in particolare, della «Politica di utilizzo ragionevole» che tutti i dipendenti devono applicare.

Lo scopo di questa politica è quello di definire l'uso ragionevole delle apparecchiature informatiche [dell'azienda target]. Queste regole sono in vigore per proteggere il dipendente e [l'azienda target]. L'uso inappropriato presenta rischi, tra cui attacchi di virus, compromissione dei sistemi e dei servizi di rete e problemi legali.

Questa politica si applica a dipendenti, appaltatori, consulenti, personale temporaneo e altri lavoratori di [azienda target], compreso tutto il personale affiliato a terzi. Questa politica si applica a tutte le apparecchiature possedute o noleggiate dall'azienda target].

Qualcuno vi contatterà a breve per discuterne con voi.

Saluti, sicurezza informatica

**Chiamata 8: qualche ora dopo, una chiamata al centralino dell'azienda.**

NATAN: Salve. Potrebbe mettermi in contatto con Sarah Jones, per favore?

OPERATORE: La metto in contatto con lei.

SARAH: Buongiorno. Reparto vendite. Come posso aiutarvi?

NATHAN: Ciao, Sarah. Vi chiamo dalla sicurezza informatica per aggiornarvi sulle migliori pratiche di sicurezza informatica. Dovreste aver ricevuto un'e-mail al riguardo.

SARAH: Sì, oggi ho ricevuto un'e-mail al riguardo.

NATHAN : Ok, bene. È una procedura standard per tutti i nuovi dipendenti e richiede solo cinque minuti. Come ti trovi qui? Vi stanno aiutando tutti?

SARAH: Sì, grazie. È fantastico. Tuttavia, è un po' scoraggiante iniziare qualcosa di nuovo.

NATHAN: Sì, ed è sempre difficile ricordare i nomi di tutti. Roger ti ha presentato? [Le chiacchiere hanno lo scopo di stabilire un rapporto di fiducia tra i due]. Emma Jones è molto gentile con l'HR se avete bisogno di aiuto su questo fronte.

SARAH: Sì, Emma ha fatto il mio colloquio con le risorse umane per il lavoro.

NATHAN: Bene. Farei meglio di percorrere la presentazione della sicurezza con te. La tua posta elettronica è aperta? Ti invio subito la presentazione della sicurezza e potrò parlartene.

SARAH: Ok, vedo l'e-mail.

NATHAN: Ok, basta un doppio clic sull'allegato .zip della presentazione sulla sicurezza.

SARAH: Ok....

L'eseguibile che ha aperto è, in realtà, una serie di script e strumenti abilmente confezionati creati dal nostro programma di incapsulamento, che include RAT (malware per l'accesso remoto utilizzato per prendere il controllo di un computer), un rootkit (che consente l'accesso a un computer nascondendone l'esistenza), un keylogger (che registra i tasti premuti sulla tastiera del computer) e qualsiasi altra cosa che potrei voler aggiungere.

Quando Sarah fa clic sul file, la presentazione si avvia immediatamente. Si tratta solo di una serie di diapositive in PowerPoint che le dicono di non eseguire gli eseguibili che le vengono inviati, ecc. e altre buone pratiche di sicurezza.

La presentazione è contrassegnata da tutti i loghi dell'azienda che sono stati opportunamente copiati dal loro server web pubblico, solo per aggiungere un po' di sicurezza in più. Pochi secondi dopo, mentre segue la presentazione, gli script contenuti nel pacchetto iniziano a cercare di disabilitare McAfee e qualsiasi altro sistema di sicurezza informatica che possa proteggere l'utente. Quindi il rootkit si installa, nascondendo tutte le azioni future al sistema operativo o a chiunque conduca un'indagine forense.

Quindi il RAT viene nascosto e installato. Il RAT viene avviato a ogni riavvio del computer e queste azioni sono tutte nascoste dal rootkit.

Il RAT cerca quindi le impostazioni proxy e altre informazioni utili e tenta di uscire dalla rete e connettersi a Internet, pronto a ricevere i comandi dal suo master. Ovviamente, tutti i processi e le connessioni TCP (Transmission Control Protocol) sono nascosti e nemmeno l'esecuzione di operazioni come netstar (statistiche di rete) e il task manager (procedure che possono essere utilizzate per rilevare manipolazioni non autorizzate del computer) li rivelerà.

Il RAT si collega al master. Ora possiedo il PC ed è arrivato il momento di iniziare a guardarmi intorno e iniziare a fare hacking! Il lavoro è finito.

## 4. Discussione

Gli autori sperano che leggendo l'esempio appena fornito, che descrive l'acquisizione calcolata passo dopo passo del sistema informatico di un'azienda target, i dipendenti a tutti i livelli della gerarchia di un'organizzazione siano più consapevoli (e riconoscano) come:

1. Informazioni apparentemente innocue e facilmente ottenibili possono essere utilizzate per scopi malevoli;
2. Stabilire un rapporto di fiducia con una persona può renderla più propensa a diventare un complice inconsapevole in un'impresa di spionaggio;
3. È necessaria una costante vigilanza per garantire che le informazioni non vengano fornite senza un'attenta considerazione dell'autenticità e della giustificazione della fonte che le richiede.

Quando insegniamo ai nostri studenti, sia all'Accademia dell'FBI che alla School of Business, presentiamo sempre una citazione che ricorda

loro il ruolo che svolgono nella protezione delle informazioni nazionali e/o aziendali: *"Le informazioni riservate possono essere protette in caveau chiusi a chiave, dietro una serie di barriere fisiche ed elettroniche. L'anello più debole di ogni catena di sicurezza è l'uomo. Una volta che una serratura è chiusa, non si sblocca da sola... ma una lingua legata si scioglie facilmente".* A questo commento segue un'osservazione: *"Ogni volta che qualcuno vi coinvolge in una conversazione, soprattutto se sta cercando informazioni, non passate alla modalità di "risposta automatica"! Pensate a eventuali secondi fini dell'interlocutore mentre si svolge il dialogo. Fate attenzione quando fornite informazioni, soprattutto i tipi di dati che potrebbero essere utilizzati per il furto d'identità o lo spionaggio aziendale, e ricordate che l'informazione che fornite può sembrare insignificante, ma in combinazione con altre informazioni può essere il pezzo chiave che mette insieme l'intero puzzle" [5].*

## 5. Conclusione

Le informazioni presentate in questo articolo illustrano come le informazioni raccolte con cura e intelligenza possano portare a una grave violazione della sicurezza nella rete informatica di un'organizzazione. L'obiettivo è quello di fornire al lettore una comprensione preliminare del funzionamento di tale processo, al fine di ridurre il rischio che si verifichi in futuro.

## Riferimenti


[1] Brooks, C.J., Grow, C., Craig, P. and Short, D.D. (2018) Cybersecurity Essentials. Sybex, Hoboken. https://doi.org/10.1002/9781119369141

[2] Sai, H. (2019) Next Level Cyber Security. Leader's Press, Santa Barbara.

[3] Swinhoe, D. (2021) The 15 Biggest Data Breaches of the 21st Century. https://www.csoonline.com/

[4] Daswani, N. and Elbayadi, M. (2021) Big Breaches: Cybersecurity Lessons for Everyone. Apress, New York, USA. https://doi.org/10.1007/978-1-4842-6655-7

[5] Schafer, J. and Karlins, M. (2020) The Truth Detector. Simon & Schuster, New York, USA. ■


### BIO

**John R. «Jack» Schafer è un agente speciale dell'FBI in pensione, attualmente professore associato presso la Western Illinois University. Jack Schafer è stato un analista comportamentale, distaccato presso il National Security Behavioural Analysis Program dell'FBI, dove ha sviluppato molte delle idee presentate nel suo libro „The Truth Detector". Il dottor Schafer ha conseguito il dottorato in psicologia presso la Fielding Graduate University di Santa Barbara, California. Ha una propria società di consulenza e tiene conferenze e consulenze in America e all'estero. È autore di un libro intitolato Psychological Narrative Analysis: A Professional Method to Detect Deception in Written and Oral Communications. È inoltre coautore del volume Advanced Interviewing Techniques: Proven Strategies for Law Enforcement, Military, and Security Personnel. Ha pubblicato numerosi articoli su un'ampia gamma di argomenti, tra cui la psicopatologia dell'odio, l'etica nelle forze dell'ordine, la rilevazione degli inganni e i principi universali del comportamento criminale. L'ultimo libro di Schafer è il best seller The Like Switch: An Ex-FBI Agent's Guide to Influencing, Attracting, and Winning People Over.**

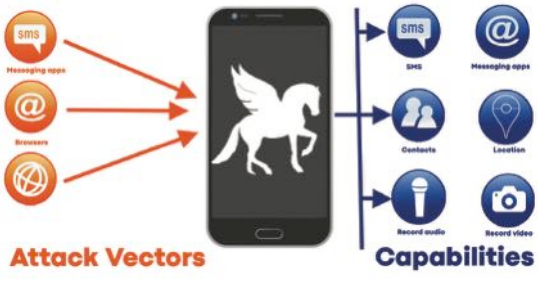
### BIO

**Marvin Karlins ha conseguito il dottorato di ricerca in psicologia sociale presso l'Università di Princeton. Attualmente è professore ordinario di management presso il Muma College of Business della University of South Florida. Il dottor Karlins svolge attività di consulenza in tutto il mondo e per vent'anni ha formato tutto il personale operativo della Singapore Airlines. Ha pubblicato 30 libri e oltre 150 articoli in riviste professionali, accademiche e divulgative. Molti dei suoi libri sono diventati bestseller internazionali, tra cui What Every BODY Is Saying: An Ex-FBI Agent's Guide to Speed-Reading People e The Like Switch: An Ex-FBI Agent's Guide to Influencing, Attracting, and Winning People Over. Il suo ultimo libro, scritto insieme a Tony March, è Paying It Backward: How a Childhood of Poverty and Abuse Fueled a Life of Gratitude and Philanthropy, pubblicato nel 2020. Karlins è membro della Authors Guild e della International Federation of Journalists.**

# "Pegasus", lo spyware per smartphone. Come funziona e come ci si può proteggere?

Autore: Costin G. Raiu

Uno degli eventi più importanti nel mondo cibernetico nel 2021 è rappresentato dai risultati di un'indagine condotta dal Guardian e da altre 16 organizzazioni mediatiche, che ha rilevato che più di 30.000 attivisti per i diritti umani, giornalisti e avvocati in tutto il mondo potrebbero essere stati presi di mira con lo spyware Pegasus (Pegasus è un cosiddetto *"software di sorveglianza legale"* sviluppato dalla società israeliana NSO).




Il rapporto pubblicato nel luglio 2021, intitolato "Pegasus Project" (1), sostiene che il malware è stato distribuito su larga scala attraverso vari exploit, tra cui diversi zero-days che hanno preso di mira i sistemi iOS. Sulla base di analisi forensi di numerosi dispositivi mobili, il laboratorio di sicurezza di Amnesty International ha effettivamente scoperto che il software è stato ripetutamente utilizzato in modo improprio per scopi di sorveglianza.

L'elenco delle persone prese di mira comprende 14 leader mondiali e un gran numero di attivisti, difensori dei diritti umani, dissidenti ed esponenti dell'opposizione. Più tardi nello stesso mese, quando è stato pubblicato il rapporto del Guardian e di Amnesty, funzionari del governo israeliano hanno visitato gli uffici della NSO nell'ambito di un'indagine sulle accuse (2).

Nell'ottobre 2021, la Corte Suprema indiana ha nominato un comitato tecnico per indagare sull'uso di Pegasus per spiare i cittadini (3). A novembre, Apple ha annunciato l'avvio di un'azione legale contro NSO Group per aver sviluppato un software che colpisce i suoi utenti con *"malware e spyware"*(4).

Infine, nel dicembre 2021, Reuters ha pubblicato che i telefoni del Dipartimento di Stato americano, allertati da Apple, sono stati violati con il malware Pegasus di NSO (5).


Nel 2022, le rivelazioni sono continuate: il 2 maggio 2022, il governo spagnolo ha annunciato che il primo ministro Pedro Sánchez e il ministro della Difesa Margarita Robles erano entrambi monitorati da Pegasus (6). In seguito a queste rivelazioni, il governo spagnolo ha immediatamente licenziato il capo dei servizi segreti del Paese, Paz Esteban.

Rilevare le tracce di Pegasus e di altre infezioni malware avanzate per dispositivi mobili è molto difficile ed è ulteriormente complicato dalle caratteristiche di sicurezza dei moderni sistemi operativi come iOS e Android.

Secondo le nostre osservazioni, la loro analisi è resa ancora più difficile dal fatto che si tratta di distribuzioni di malware non persistenti, che non lasciano quasi alcuna traccia dopo il riavvio del dispositivo infetto.

Poiché molti strumenti forensi richiedono un *jailbreak* (completo, in questo caso, di intrusione consenziente) del dispositivo, il malware viene rimosso dalla memoria durante il riavvio, necessario per questa operazione. Fortunatamente, ad oggi, è possibile utilizzare diversi metodi per rilevare Pegasus e altri malware mobili. Ad esempio, il *Mobile Verification Toolkit* (MVT) di Amnesty International è gratuito (7), open source e consente a tecnici e investigatori di ispezionare i telefoni cellulari alla ricerca di segni di infezione. L'MVT è supportato da un elenco di IoC *(indicatori di compromissione)* compilato da casi di alto profilo di abuso dei diritti umani, reso disponibile anche da Amnesty International.


In questi tempi di incertezza, molti utenti preoccupati in tutto il mondo si chiedono come proteggere i propri dispositivi mobili da Pegasus e da altri strumenti e malware simili.

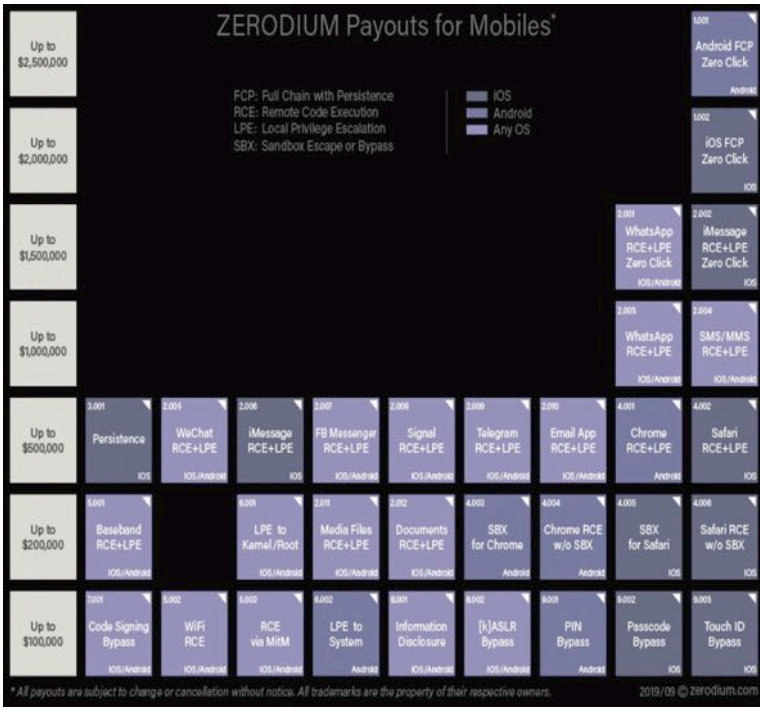
Allo stesso modo, i governi stanno cercando di valutare le proprie debolezze e di sviluppare strategie per identificare tali vulnerabilità, o almeno per evitare che si verifichino in futuro. In questo articolo esamineremo le più recenti tecniche di attacco utilizzate per distribuire malware sui telefoni cellulari e come difendersi da esse, tenendo presente che un elenco di tecniche di difesa non è esaustivo. Inoltre, poiché gli aggressori cambiano il loro modus operandi, anche le tecniche di difesa esistenti devono essere adattate molto frequentemente.

## BIO

**Direttore del Global Research and Analysis Team (GReAT) di Kaspersky, Costin è specializzato nell'analisi di minacce persistenti avanzate, exploit zero-day e malware complessi. È a capo del Global Research and Analysis Team (GReAT), famoso in tutto il mondo, che ha studiato il funzionamento interno di molti attacchi di alto profilo, tra cui RedOctober, WannaCry, ShadowPad e ShadowHammer e Moonlight Maze. Il suo lavoro attuale si concentra sullo sviluppo di tecnologie e sistemi di similitudine del codice per arricchire l'intelligence sulle minacce. Costin ha oltre 28 anni di esperienza nella tecnologia antivirus e nella ricerca sulla sicurezza. È membro del Virus Bulletin Technical Advisory Board, membro della Computer AntiVirus Researchers' Organization (CARO) e reporter della Wildlist Organization International. Prima di entrare in Kaspersky Lab, Costin ha lavorato per GeCad come ricercatore capo e come esperto di sicurezza dei dati nel gruppo di sviluppatori dell'antivirus RAV. Costin è cintura blu di Taekwondo. I suoi hobby sono gli scacchi, la fotografia e la letteratura di fantascienza.**

### Come si fa a stare al sicuro dalle minacce informatiche mobili più sofisticate?

Innanzitutto, va detto che Pegasus è un kit di strumenti dal prezzo relativamente alto. Il costo di un'implementazione completa può raggiungere facilmente i milioni di dollari. Allo stesso modo, altre minacce informatiche mobili possono essere distribuite attraverso exploit 0-click




0-day. Questi sono estremamente costosi: ad esempio, Zerodium, una società di intermediazione di *"exploit"*, richiede fino a 2,5 milioni di dollari per una catena di infezioni Android 0-click con persistenza avanzata:

Si può trarre subito una conclusione importante: lo spionaggio informatico sofisticato è un'attività che richiede molte risorse. Quando uno sponsor può permettersi di spendere milioni, o addirittura decine di milioni o centinaia di milioni di dollari USA in programmi offensivi, è altamente improbabile che un obiettivo possa evitare di essere infettato. In pratica, più prosaicamente, non si tratta di *"se si può essere infettati"*, ma quando e come: è, infatti, solo una questione di tempo e del prima che voi siate infettati, grazie alle risorse corrispondenti ai vostri strumenti e al loro livello di sicurezza.

La buona notizia è che lo sviluppo di exploit e la guerra informatica offensiva sono spesso più un'arte che una scienza esatta. Gli exploit devono essere adattati a versioni specifiche del sistema operativo e dell'hardware e possono essere facilmente vanificati da nuovi sistemi operativi, nuove tecniche di mitigazione o persino da piccole cose come eventi casuali.

Da questo punto di vista, l'infezione e il bersaglio sono anche una questione di costi e difficoltà per gli aggressori. Sebbene non sia sempre possibile impedire

lo sfruttamento e l'infezione di un dispositivo mobile, possiamo cercare di renderlo il più difficile possibile per gli aggressori.

Come lo facciamo nella pratica? Ecco una semplice lista di controllo:

**Su iOS :**

a) Riavviare ogni giorno.

Secondo le ricerche di Amnesty e CitizenLab, la catena di infezione di Pegasus si basa spesso su clic quotidiani senza persistenza, per cui un riavvio regolare ripulisce il dispositivo.

Se il dispositivo viene riavviato quotidianamente, gli aggressori dovranno reinfettarlo più volte. A lungo andare, questo aumenta le possibilità di rilevamento; potrebbe verificarsi un arresto anomalo o l'installazione di semplici app che rivelano un'infezione di natura stealth.

In realtà, non si tratta solo di teoria, ma di pratica: abbiamo analizzato un caso in cui un dispositivo mobile è stato preso di mira da un exploit 0-click (probabilmente FORCEDENTRY). Il proprietario del dispositivo lo ha riavviato regolarmente e lo ha fatto entro 24 ore dall'attacco. Gli aggressori hanno cercato di colpirlo più volte, ma alla fine hanno rinunciato dopo essere stati colpiti più volte durante i riavvii.

b) Disattivare iMessage.

iMessage è integrato in iOS ed è abilitato per impostazione predefinita, il che lo rende un interessante vettore di sfruttamento. Essendo abilitato per impostazione predefinita, è un meccanismo di consegna privilegiato per le stringhe da 0 clic.

Per molti anni gli exploit di iMessage sono stati molto richiesti, con guadagni significativi per le società di intermediazione di "exploit". *"Negli ultimi mesi abbiamo assistito a un aumento del numero di exploit per iOS, soprattutto per Safari e iMessage, sviluppati e venduti da hacker di tutto il mondo. Il mercato degli zero-day è talmente inondato di exploit per iOS che recentemente abbiamo iniziato a rifiutarne alcuni"*, ha scritto il fondatore di Zerodium Chaouki Bekrar nel 2019 a WIRED (8).

Ci rendiamo conto che questo potrebbe essere molto difficile per alcuni (in seguito), ma se Pegasus e altri malware APT mobili di fascia alta sono tra i modelli di minaccia che vi preoccupano, questo è un compromesso che vale la pena fare.

c) Disattivare Facetime.

Come sopra.

d) Mantenere aggiornato il dispositivo mobile; installare le ultime patch di iOS non appena disponibili.

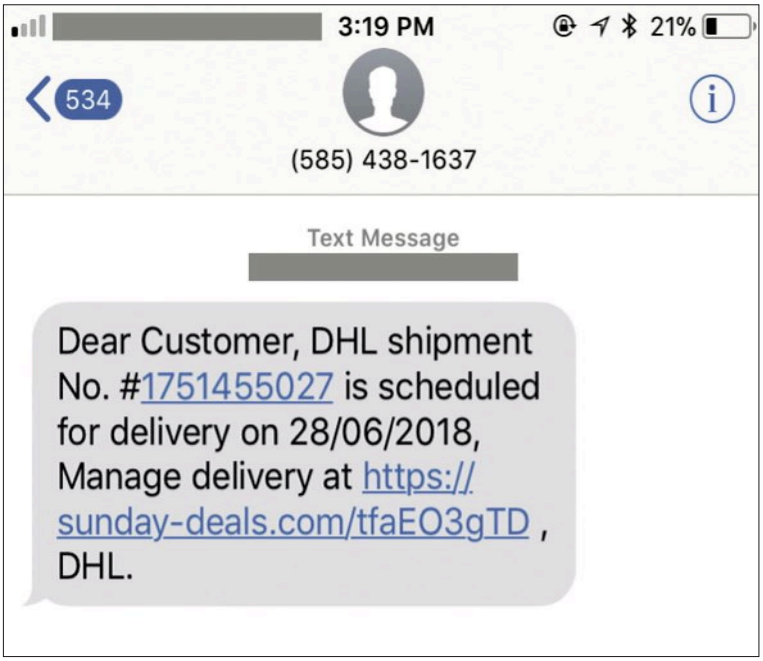
Non tutti possono permettersi di utilizzare le vulnerabilità 0-day. In effetti, la maggior parte dei kit di exploit per iOS di cui siamo a conoscenza mira a vulnerabilità che sono già state corrette. Tuttavia, molte persone utilizzano telefoni più vecchi e rimandano gli aggiornamenti per vari motivi.

Se volete stare al passo con (alcuni) hacker *sponsorizzati dallo Stato*, aggiornate il vostro sistema operativo il prima possibile e imparate a non avere bisogno di emoji per installare le patch (9).

e) *Non cliccate mai sui link ricevuti nei messaggi SMS.*

È un consiglio semplice ma efficace. Non tutti i clienti di Pegasus possono permettersi di acquistare catene di 0-day da milioni di dollari, quindi si affidano a exploit da 1 clic.

Queste arrivano sotto forma di messaggio, a volte via SMS, ma anche tramite altri servizi di messaggistica o persino via e-mail. Se ricevete un SMS interessante (o un messaggio tramite qualsiasi altro servizio di chat) con un link, apritelo su un computer desktop, preferibilmente utilizzando TOR Browser o un sistema operativo sicuro non persistente come Tails.




*SMS contenente un link malevolo usato per colpire un attivista politico - credit: Citizenlab*

f) *Navigare in Internet con un browser non nativo, come Firefox Focus, invece di Safari o Chrome.*

Sebbene tutti i browser su iOS utilizzino praticamente lo stesso motore di ricerca, Webkit, alcuni exploit non funzionano bene (vedi il caso APT LightRighter / TwoSailJunk (10)) su alcuni browser alternativi:

```
detect_os()

return {
        mobile: (typeof window.orientation !== "undefined") || (navigator.userAgent.indexOf('IEMobile') !== -1),
        webkit: parseFloat(/AppleWebKit\/([\d.]+)/.exec(navigator.userAgent)[1]) || 0,
        safari: window.navigator.userAgent.indexOf('Safari') > -1,
        version: function()
        {
                var match = (navigator.appVersion).match(/OS (\d+)_(\d+)_?(\d+)?/);
        if(match) {
                var version = [
                    parseInt(match[1], 10),
                    parseInt(match[2], 10),
                    parseInt(match[3] || 0, 10)
                        ];
                        return parseFloat(version[0]+'.'+version[1]+version[2]);
            } else {
                return "unknown";
```

*Il sistema operativo LightRiver verifica la presenza di "Safari" nella stringa dell'agente utente.*

**Stringhe dell'agente utente su iOS da Chrome (sinistra) /Firefox (destra):**

| Stringa dell'agente utente di Chrome su iOS | Firefox Focus User Agent Channel su iOS |
|---|---|
| Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 come Mac OS X) AppleWebKit/605.1.15 (KHTML, come Gecko) CriOS/96.0.4664.53 Mobile/15E148 Safari/604.1 | Mozilla/5.0 (iPhone; CPU iPhone OS 15_1 come Mac OS X) AppleWebKit/605.1.15 (KHTML, come Gecko) FxiOS/39 Mobile/15E148 Version/15.0 |

g) *Utilizzate sempre una VPN che mascheri il vostro indirizzo IP e il traffico dati.*

Alcuni exploit vengono trasmessi da attacchi MitM tramite l'operatore GSM, durante la navigazione di siti HTTP o tramite DNS hijacking. Utilizzando una VPN per mascherare il vostro indirizzo IP e il vostro traffico dati, è difficile per il vostro operatore di telefonia mobile individuarvi direttamente su Internet.

Complica inoltre il processo di targeting se gli aggressori hanno il controllo del flusso di dati, ad esempio durante il *roaming.*

Tenete presente che non tutte le VPN sono uguali e non tutte le VPN sono buone da usare. Senza individuare una VPN in particolare, ecco alcune cose da considerare quando si acquista un abbonamento VPN: Acquistare significa esattamente questo: niente VPN "gratuite".

- Cercate servizi che accettino pagamenti in criptovalute.
- Cercate servizi che non richiedano di fornire informazioni di registrazione.
- Cercate di evitare le applicazioni VPN: utilizzate invece strumenti open source come WireGuard e OpenVPN e profili VPN.
- Evitate i nuovi servizi VPN e cercate quelli ben noti che esistono da tempo.

h) Installare un'applicazione di sicurezza che controlli e avverta se il dispositivo è jailbroken.

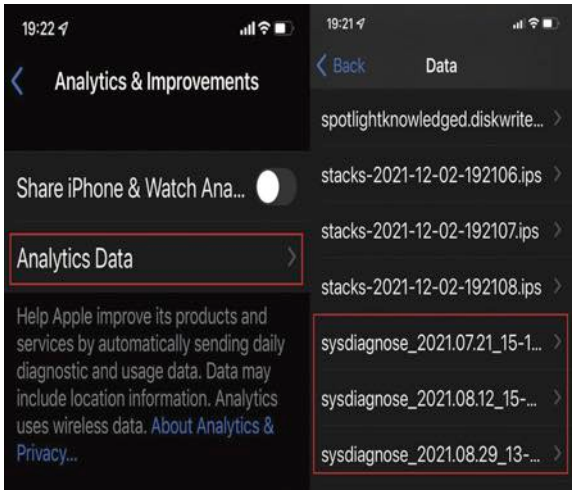
Frustrati dal fatto di essere presi a calci nel sedere più e più volte, gli aggressori finiranno per implementare un meccanismo di persistenza e "jailbreakare" il vostro dispositivo (accedere illegalmente a tutti i suoi contenuti). In questo caso le possibilità di catturare i malintenzionati si decuplicano e possiamo sfruttare il fatto che il dispositivo è stato jailbroken.

i) Eseguire il backup di iTunes una volta al mese.

Ciò consente di diagnosticare e individuare le infezioni in un secondo momento, utilizzando il meraviglioso pacchetto MVT di Amnesty.

j) Attivare spesso i *sysdiag* e salvarli in backup esterni.

Gli strumenti forensi possono aiutarvi a determinare in seguito se siete stati presi di mira. L'attivazione di un



*sysdiag* (un'applicazione che consente una diagnosi completa del sistema e dei contenuti) dipende dal modello di telefono.

Ad esempio, su alcuni iPhone è sufficiente premere contemporaneamente i tasti VOL Su + Giù + Accensione. È possibile che si debba giocare più volte con questi tasti finché il telefono non emette un segnale acustico.

Una volta creato, il *sysdiag* apparirà nella diagnostica nella sezione "dati analitici":

**2. Su Android**


a) Riavviare ogni giorno.

La persistenza sulle ultime versioni di Android è difficile, molti APT e fornitori di exploit evitano la persistenza!

b) Mantenere il telefono aggiornato; installare le ultime patch.

c) Non cliccate mai sui link ricevuti nei messaggi SMS.

d) Navigare in Internet con un altro browser come Firefox Focus invece di Chrome.

e) Utilizzate sempre una VPN che mascheri il vostro indirizzo IT e il traffico dati.

Alcuni exploit si diffondono tramite attacchi MitM agli operatori GSM, durante la navigazione di siti HTTP o tramite DNS hijacking.

f) Installare una suite di sicurezza che esegua la scansione del malware e controlli e avvisi se il dispositivo è jailbroken.

A un livello più sofisticato, verificate sempre il traffico di rete utilizzando gli IOC dal vivo. Una buona configurazione potrebbe includere una VPN Wireguard sempre attiva verso un server sotto il vostro controllo, che utilizza *pihole* per filtrare le cose negative e registra tutto il traffico per una successiva ispezione (11).

## Una partita a punteggio zero?

Ryan Naraine, un noto commentatore di sicurezza, ha dichiarato: *"iMessage e FaceTime - questi sono i motivi per cui la gente usa gli iPhone!"* E ha ragione: iMessage e FaceTime sono due delle migliori aggiunte che Apple abbia fatto al suo ecosistema.

Fortunatamente, Apple ha migliorato notevolmente la *sandbox* di sicurezza che protegge iMessage con


BlastDoor in iOS 14 (12). Tuttavia, l'exploit FORCEDENTRY utilizzato da NSO per distribuire Pegasus ha aggirato BlastDoor e, naturalmente, nessuna funzione di sicurezza è mai a prova di hacker al 100% (13).

## Allora, cosa c'è di meglio in entrambi i mondi, vi chiederete?

Alcune persone, me compreso, hanno più telefoni: uno con iMessage disattivato e un iPhone *"honeypot"* con iMessage attivato. Entrambi sono ovviamente associati allo stesso ID Apple e allo stesso numero di telefono. Se qualcuno decide di prendermi di mira in questo modo, è probabile che finisca nel telefono *honeypot*.

## Non tacete se siete osservati...

Naturalmente, è possibile seguire alla lettera queste raccomandazioni ed essere comunque infettati. Purtroppo, questa è la realtà in cui viviamo oggi. Quando qualcuno ci dice di essere stato preso di mira da uno spyware mobile, gli diciamo di riflettere su queste domande:

- Chi vi ha preso di mira e perché?
- Cercate di capire cosa vi ha portato all'attenzione dei grandi. Potete evitarlo in futuro comportandovi in modo più discreto?
- Può parlarne?

Questo ha finito per far crollare molte società di sorveglianza, grazie alla cattiva pubblicità che tali casi hanno creato per loro, come quando molti reporter e giornalisti riportano gli abusi e smascherano le bugie e i misfatti generati da un operatore del settore.

Se siete stati presi di mira, cercate di trovare un giornalista e raccontate la vostra storia.

## Cambiare il dispositivo

Se si utilizzava iOS, provare a passare ad Android per un po'. Se eravate su Android, passate a iOS. Questo può confondere gli aggressori per un po'; ad

esempio, è noto che alcuni attori delle minacce acquistano sistemi operativi che funzionano solo su una determinata marca di telefono e di sistema operativo.

Acquistare un dispositivo secondario, preferibilmente con GrapheneOS, per comunicazioni sicure. Utilizzatelo con una carta prepagata o collegatevi solo tramite Wifi e TOR in modalità aereo.

Evitate i messaggi in cui dovete fornire il vostro numero di telefono ai vostri contatti. Una volta che un aggressore è in possesso del vostro numero di telefono, può facilmente prendervi di mira attraverso molti messenger diversi: iMessage, WhatsApp, Signal, Telegram, poiché sono tutti collegati al vostro numero di telefono.

Un'interessante novità è Session, che instrada automaticamente i messaggi attraverso una rete simile a Onion e non dipende dai numeri di telefono.

Cercate di entrare in contatto con un ricercatore di sicurezza della vostra zona e discutete costantemente delle migliori pratiche. Condividete con loro dati, messaggi sospetti o accessi non appena ritenete che ci sia qualcosa di strano.

La sicurezza non è mai un'unica soluzione istantanea che offra una garanzia al 100%; consideratela come un fiume, dove dovete adattare la vostra navigazione alla velocità, alle correnti e agli ostacoli.

Alla fine di tutto questo, vorrei lasciarvi con un pensiero. Se siete presi di mira da attori al servizio di Stati nazionali, significa che siete importanti.

Ricordate: è bello essere importanti, ma è più importante essere gentili.

Da soli siamo deboli, insieme siamo forti.

Il mondo può essere distrutto, ma credo che stiamo vivendo un momento in cui possiamo ancora fare la differenza.

Secondo un rapporto del Committee to Protect Journalists (CPJ), nel 2021 sono stati imprigionati 293 giornalisti, il numero più alto mai registrato dal CPJ da quando ha iniziato a registrarlo nel 1992 (14).

Sta a noi dare forma a quello che sarà il mondo per noi tra 10 anni, per i nostri figli e per i figli dei nostri figli.

## Riferimenti


(1) https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/
(2) https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-nso-group-offices-after-pegasus-revelations
(3) https://www.theregister.com/2021/10/29/india_nso_pegasus_probe/
(4) https://www.theguardian.com/technology/2021/nov/23/apple-sues-israeli-cyber-firm-nso-group
(5) https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/
(6) https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware
(7) https://github.com/mvt-project/mvt
(8) https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/
(9) https://twitter.com/ryanaraine/status/1324445133668974592
(10) https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/
(11) https://pi-hole.net
(12) https://googleprojectzero.blogspot.com/2021/01/a-look-at-imessage-in-ios-14.html
(13) https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
(14) https://edition.cnn.com/2021/12/09/media/journalists-imprisoned-cpj-census/index.html ■


Voi, il popolo, avete il potere: il potere di creare le macchine, il potere di creare la felicità. Voi, il popolo, avete il potere: il potere di rendere la vita bella e libera, il potere di rendere questa vita un'avventura meravigliosa.

Quindi, in nome della democrazia, usiamo questo potere. Dobbiamo unirci, dobbiamo lottare per un mondo nuovo, dignitoso e umano, che dia a tutti la possibilità di lavorare, che dia un futuro ai giovani e sicurezza alla vecchiaia.

Questi bulli vi hanno promesso tutte queste cose per farvi dare il potere - mentono. Non mantengono le loro promesse e non lo faranno mai. I dittatori si liberano prendendo il potere, ma schiavizzano il popolo.

Lottiamo dunque per mantenere questa promessa! Dobbiamo lottare per liberare il mondo, per abolire i confini e le barriere razziali, per porre fine all'avidità, all'odio e all'intolleranza.

Dobbiamo lottare per costruire un mondo di ragione, un mondo in cui la scienza e il progresso portino alla felicità di tutti. Soldati, in nome della democrazia, uniamoci! ■

**Discorso finale del film "Il grande dittatore" (Charlie Chaplin)**

Security Mind

# La Cyber Security incontra La Psicologia

*A cura di Veronica Patron Co-Founder di Security Mind*

Un programma di Cyber Security Awareness evoluto oltre a descrivere le varie tecniche di attacco, utilizzando una comunicazione efficace e comprensibile anche da persone inesperte in sicurezza informatica, dovrà analizzare il **fattore umano** nel contesto della Cyber Security, attingendo a contributi multidisciplinari per esempio le scienze sociali, la psicologia e la sociologia.

Nello specifico dovrà da un lato essere in grado di trasformare concretamente gli Atteggiamenti e i Comportamenti degli utenti di fronte alle crescenti minacce Cyber e dall'altro descrivere le dinamiche che intercorrono tra l'attaccante e la vittima, evidenziare quindi sia il modo di pensare della vittima sia quello di operare dell'attaccante.
Come dice Sun Tzu:

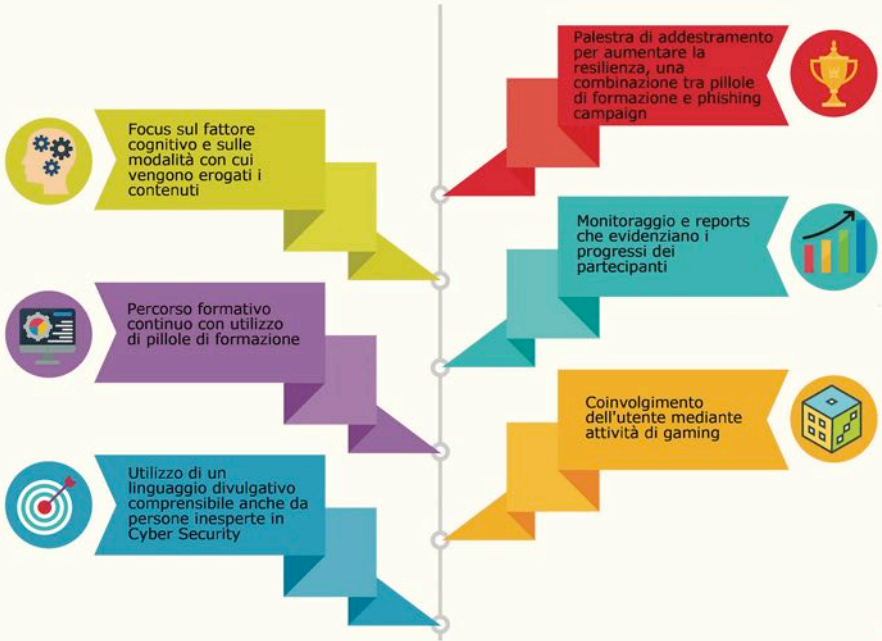
**"Se conosci il nemico e te stesso non dovrai temere il risultato di cento battaglie."**

Ma cosa significa analizzare un argomento di Cyber Security dal punto di vista psicologico?

Significa rendere l'utente consapevole che gli hacker, sfruttando le nostre emozioni, ci spingono ad agire d'istinto, senza utilizzare quella parte più razionale e logica del nostro cervello e creano dei meccanismi per ingannare il modo in cui il nostro cervello prende delle decisioni.

Inoltre gi hacker utilizzano momenti di disattenzione, come il lunedì mattina quando l'utente controlla l'email che ha ricevuto nel fine settimana, oppure 5 minuti prima della la pausa pranzo, oppure potrebbe utilizzare la fine della giornata lavorativa quando l'utente si sta preparando per terminare le attività lavorative.

## Le principali caratteristiche che dovrebbe avere un innovativo programma di Cyber Security Awareness per essere efficace e di successo:

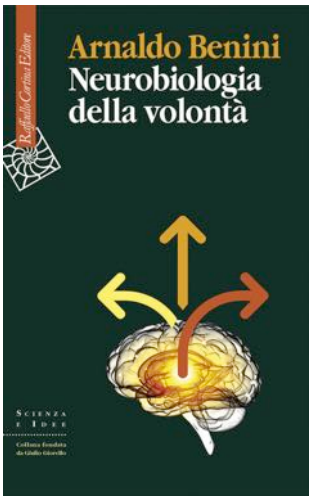



***La nostra Missone è passare dall'Informazione alla Trasformazione***

# Bibliografia

**Arnaldo Benini**
***Neurobiologia della volontà***
**Ed. Raffaello Cortina**
**Autore: Arnaldo Benini***

## Il libero arbitrio esiste realmente?




Il libero arbitrio è il problema centrale dell'etica, dei rapporti sociali e della responsabilità. Siamo liberi di scegliere idee e comportamenti e ne siamo responsabili? Per il filosofo materialista Paul Henri Thiry d'Holbach (1723-1789) l'illusione dell'uomo d'essere libero di decidere è pari a quella di una mosca, che, posatasi sul timone di un carro, è fiera di determinarne la direzione. L'uomo e la mosca immaginano di poter muovere l'universo. In realtà essi sono determinati. Da che cosa e come? Per riflettere sulla volontà, senza finire nelle tautologie e nelle astrattezze della letteratura filosofica e moraleggiante "sconvolgente nella sua inconcludenza" e per evitare il "polveroso nuvolone" del suo "filosofese", come lo chiamò Massimo Baldini trent'anni orsono, è necessaria la chiarezza concettuale che consenta analisi scientifiche e riflessioni concrete su uno dei problemi centrali dell'esistenza. Il dilemma dell'arbitrio, per sua natura, non è né filosofico né religioso. È scientifico.

Circa volontà e libero arbitrio, ci sono due possibilità, senza vie di mezzo: o si è, per scelta o spontaneamente, dualisti, come la stragrande maggioranza dell'umanità, che crede alla volontà libera e altro non può immaginarsi. Per i dualisti, la volontà è libera dai meccanismi cerebrali perché dipende da un ente immateriale individuale (anima o spirito, la *res cogitans* di Cartesio) che agisce senza condizionamenti fisici. Solo quando agiamo perché obbligati, avvertiamo che la volontà non è libera. Per il senso comune, facciamo quel che vogliamo, e pertanto ne siamo responsabili. Che il dualismo sia la spontanea convinzione di gran lunga più diffusa è la conferma di quanto poco il pensiero scientifico influenzi il senso comune. C'è chi ritiene che i dualisti attribuiscano le buone scelte all'anima e quelle infelici al corpo.

Oppure si ripone fiducia nella razionalità della scienza, per la quale la volontà, come tutti gli eventi della coscienza, è il prodotto di meccanismi nervosi. Essi non sono solo umani, perché di loro si rintraccia la storia evolutiva a partire da esseri remoti, anche se le loro scelte erano e sono più elementari di quelle dell'umanità e non sono condizionate dal senso morale. Che cosa deve essere "libero" e da quali vincoli ci si deve (o ci si può) liberare per agire in autonomia (in autonomia da che cosa?), e quindi con responsabilità? Se essere liberi significa volere e agire senza meccanismi cerebrali, che cosa è allora "libero" e dove si trova ciò che vuole e decide? È il problema che le neuroscienze cognitive, con dati raccolti da oltre un secolo, pongono alla ricerca e alla riflessione normativa, che di quei dati, fino a ora, con poche eccezioni, non ha saputo che farsene. Per la neuroscienza cognitiva la libera volontà nel senso dualista è un mito, tenace solo perché concorda col sentire comune.

Le neuroscienze propongono, con dati corroborati, anche se non definitivi (nella scienza, come nella vita, non ne esistono), che decisioni e azioni siano prodotti della macchina elettrochimica del cervello, il cui funzionamento potrebbe essere (almeno in parte, lo vedremo) casuale. La volontà, e quindi il comportamento, dipendono dai geni, dalla fisica e chimica del cervello, dagli ormoni, dagli organi di senso, dallo sviluppo prenatale, dall'esperienza, dallo sviluppo fisico e culturale, dall'ambiente. La visualizzazione del cervello con le tecniche della *brain imaging* mostra che i meccanismi nervosi della coscienza vengono attivati quando i centri della decisione sono già attivi da tempo.

L'uomo s'illude di decidere, mentre in realtà non fa ciò che vuole, ma vuole ciò che fa. La convinzione dualista della volontà indipendente dal cervello è talmente e tenacemente diffusa, anche fra gli atei, da porre il problema della sua origine evolutiva, che potrebbe essere analoga a quella delle religioni, cioè della credenza nell'aldilà e della sopravvivenza dopo la morte. Opinione diffusa fra i neuroscienziati, anche se non può essere corroborata sperimentalmente, è che l'illusoria libertà dell'arbitrio sia un espediente evolutivo della mente emerso e selezionato per conciliare l'uomo con la propria interiorità, alla quale attribuisce e riconosce la capacità di decidere. Il senso, anche se illusorio, d'esser liberi di decidere è sentito come valore essenziale, che rafforza la vita, e quindi la specie (…)

La biologia evolutiva spiega, meglio che qualsiasi altra concezione, non solo la duplicità della mente fra il bene e il male, ma anche la necessità materiale e psicologica che indusse l'uomo alla religione, alla convinzione della propria immortalità e al culto dei defunti.

Questi comportamenti hanno un'origine comune: le condizioni della vita delle quali l'uomo si rese conto quando i centri cognitivi dei lobi prefrontali l'arricchirono dei meccanismi nervosi dell'autocoscienza, cioè della capacità, solamente umana, di porre se stesso a oggetto della propria riflessione. Ciò avvenne a partire da circa un milione e trecentomila anni orsono (…)

Telmo Pievani riassume sostenendo che *"il primo motore dell'evoluzione è la variazione prodotta da mutazione e ricombinazione genetiche. Le mutazioni sono errori di duplicazione che alterano le sequenze di DNA… Le variazioni sono ereditabili e possono generare differenze nel fenotipo degli organismi. Mutazione e ricombinazione sono processi casuali nel senso che non hanno direzione…"* È proprio su questi effetti – positivi, negativi o neutri – che agisce la selezione naturale.

Nel libro si cerca di ordinare i dati delle neuroscienze circa la moralità e il male della natura umana nel contesto biologico dell'evoluzione. È uno dei più intricati meandri neurobiologici, psicologici e storici dell'autocoscienza.

**Il testo pubblicato è un estratto dell'introduzione del volume che pubblichiamo per gentile concessione dell'editore.* ■

## 25 anni Privacy in Italia, Ed. ANSA e Garante Privacy

Autore: Massimiliano Cannata

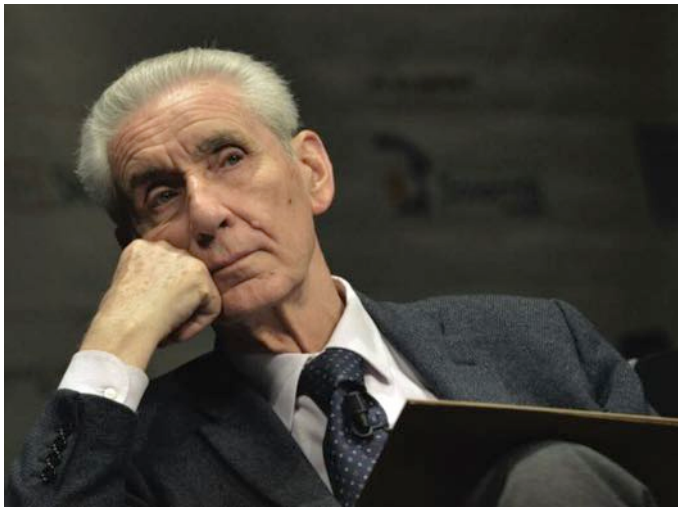
### Un anniversario cruciale per la cultura del diritto

"25 anni al servizio dell'uomo. l'Istituzione che ho l'onore di guidare è un presidio per i vulnerabili in funzione antidiscriminatoria". **Pasquale Stanzione**, presidente *dell'Autorità Garante per la protezione dei dati personali* con queste parole ha

aperto la presentazione del volume *"25 anni di privacy in Italia"* realizzato in collaborazione con l'Ansa dedicato a un anniversario che non può passare inosservato. "Un diritto – ha spiegato - che per non diventare tiranno deve trovare un costante bilanciamento tra pubblico e privato, legittimo bisogno di riservatezza e diritto di cronaca. In una prospettiva dell'innovazione aperta ai valori del neoumanesimo non è accettabile nessuna monetizzazione di un valore come la privacy che ha subito una profonda modificazione nel tempo". Libertà, uguaglianza e dignità costituiscono un trinomio delicato che sollecita la cultura del diritto, la speculazione filosofica, e i territori più avanzati della ricerca scientifica.

"I sistemi giuridici – mette in guardia **Guido Scorza**, avvocato, studioso di *diritto dell'Informatica e delle nuove tecnologie* componente del Collegio dell'Authority – andrebbero aumentati se vogliamo governare il prepotente sviluppo della **tecno-scienza**. Il rischio maggiore è quello di perdere la nostra libertà di autodeterminazione in relazione a una pluralità di scelte da quelle di consumo a quelle culturali sino ad arrivare a quelle relative alla nostra salute e alle cose della politica. Più soggetti terzi – sempre più spesso, peraltro, in maniera poco trasparente – raccolgono e trattano dati capaci di consegnare loro un enorme conoscenza sulle nostre inclinazioni, le nostre preferenze e le nostre debolezze, più tali soggetti, grazie agli algoritmi di intelligenza artificiale e ai big data – acquisiscono l'abilità di orientare, guidare, talvolta persino determinare ogni genere di nostra decisione". Meno privacy si traduce in meno libertà, cosa che dovremmo tenere bene a mente, in una società degli eccessi, spesso portata a varcare ogni limite.

### La lezione di Stefano Rodotà



Lo sapeva bene **Stefano Rodotà**, "padre" della privacy italiana, che aveva intuito per primo come la tutela della riservatezza fosse un aspetto cruciale della civiltà del diritto. "Vi sono beni – scriveva il grande giurista in Il *diritto di avere diritti* (ed. Laterza) che devono essere sottratti alla logica economica, che non possono essere

oggetto di proprietà. La privacy è uno di questi, basti pensare che il corpo e le sue parti non possono costituire oggetto di profitto". Rodotà aveva speso molte delle sue energie intellettuali nella definizione di una "Costituzione" per Internet, individuando nell'accesso al sapere, mediato dalle nuove tecnologie, un bene pubblico, al pari dell'aria e dell'acqua che respiriamo. La tutela di quello che definiva il "corpo elettronico", sostanziato dai dati sensibili e informazioni personali esposti ai cyber attacchi, è da ritenersi un diritto universale, sacro e inviolabile, da osservare con scrupolo. Mentre si fa strada lo scenario della cittadinanza globale, che si sovrappone fatale declino dello stato di Hobbes, consumato nell'orizzonte frastagliato di un mondo senza centro, diventa di importanza cruciale esercitare la sovranità rispettando i diritti di libertà proprietà e partecipazione di tutti gli uomini al dibattito pubblico, anche i più deboli. Tale diritto comincia dal rispetto per la sfera di autonomia e riservatezza entro cui si sviluppa la personalità e il progetto di crescita di ogni individuo che si muove nella complessità della storia.

## Opportunità e rischi

La torsione autoritaria imposta dai regimi autocratici (Cina e Russia sono solo i casi più eclatanti) che hanno calpestato il diritto di cronaca e "oscurato il Web", dimostra l'attualità di questa visione, nel contempo fanno riflettere decisioni, come il recente stop, imposto dai presidi, alle chat che intercorrono su whatsApp tra professori, studenti e genitori. È evidente, come si evince da tanti fatti di cronaca, che la tecnologia è entrata fino al midollo della nostra quotidianità, viviamo tutti nella condizione *onlife* teorizzata dal filosofo **Luciano Floridi** nel saggio *"La quarta rivoluzione"* (ed. Raffaello Cortina). Reale e virtuale sono contessuti e perciò non più separabili. "Dopo la rivoluzione eliocentrica, darwiniana, freudiana – spiega lo studioso docente alle Università di Oxford e di Bologna - quella dell'informatica ha stravolto più di tutte la nostra esistenza".

"La molteplicità degli interessi e dei diritti investiti nell'ambito della privacy è straordinariamente ampia" – ha ricordato **Giovanni Maria Flick** presidente emerito della Corte Costituzionale che da ministro della giustizia del primo governo Prodi si trovò a


collaborare proprio con Rodotà nella definizione della legge istitutiva dell'autorità Garante, proprio in un momento storico in cui la giustizia era travagliata da una molteplicità di problemi, riuscimmo a trovare una sintesi alta tra garanzia ed efficienza, destinata a lasciare un segno nel tempo. Dalla difesa dei big data fino alle rivelazioni biometriche, alla sicurezza dei dati che attengono al riconoscimento facciale di milioni di persone, quella della privacy - prosegue lo studioso che insieme a **Caterina Flick** ha da poco dato alle stampe: *"Il mito dell'informatica, L'algoritmo d'oro e la torre di babele" (Ed. Baldini+Castoldi)* - è una materia bollente".

I pericoli connessi al "volo di Icaro", lucidamente tratteggiati da Flick, toccano i più svariati ambiti. Dovremo fare i conti con la sfera dei neuro diritti, nuove discipline prendono campo. Prima fra tutte Il *brain reading,* che introduce gli strumenti in grado di leggere il pensiero. Credevamo che si trattasse di una superficie insondabile, quella delle motivazioni che albergano nel foro intimo della coscienza. È invece arrivato il tempo di occuparsi anche di questo. La sfida per il Garante continua, facendosi più ardua ogni giorno. ■

## Bruno Latour, *Dove sono? Lezioni di filosofia per un pianeta che cambia.* Ed. Einaudi

Autore: Massimiliano Cannata

### Il bisogno di una vera alleanza tra ecologia e giustizia

Il grido della terra e il grido dei poveri sono collegati. La questione sociale e la sofferenza degli ultimi fanno parte di stessa visione cosmologica che li contiene. Un indirizzo di pensiero si sta facendo strada che scompagina la tradizionale teoria della conoscenza. La crisi ecologica entro cui siamo proiettati, ha generato la grave malattia del pianeta, che è la stessa malattia dell'uomo, che ha perso quella sovranità sull'ambiente che aveva dalla modernità rivendicato come un trionfo. Bruno Latour, filosofo e antropologo dell'Università Science Po di Parigi, parla diffusamente di questa visione della contemporaneità con Antonio Spataro sull'ultimo numero della Civiltà Cattolica, sostenendo delle tesi destinate ad


aprire un ampio dibattito. La teologia con la sua preoccupazione per il destino dell'uomo e la cosmologia, scienza fatta di leggi immutabili, che la tradizione cartesiana ci aveva consegnato come fredda e lontana, non erano mai apparse così vicine. Una nuova alleanza sembra farsi strada tra questi saperi. "La meditazione sulla natura – spiega il pensatore francese – non può sganciarsi dall'attenzione per gli ultimi. Tra ecologia e giustizia esiste un nesso molto forte". Di questa intima connessione appare convinto per primo Papa Francesco: "La terra – si legge nell'enciclica *Laudato si* - si emoziona, può agire e soffrire proprio come l'uomo". Questo profondo salto di visione trova un riflesso importante nella scuola della complessità. "L'uomo biologico non può essere separato dall'uomo psicologico e culturale viviamo nella *terre- patrie,* che esprime la nostra origine e l'essenza delle nostre identità".

Le parole di Edgar Morin il grande sociologo francese che ha attraversato nella sua lunga vita tutto il Novecento, risuonano con la forza di un imperativo etico, straordinariamente attuale. Il senso più profondo di questa diversa prospettiva lo si ritrova negli scritti di Mauro Ceruti, insignito dal Premio Nonino proprio per l'attenzione a queste problematiche che ne fanno un "Maestro del nostro tempo". "L'attuale condizione umana è segnata da un inedito e simultaneo aumento di potenza tecnologica e di interdipendenza planetaria", scrive il filosofo in *una comunità di destino al tempo della complessità* (ed. Franco Angeli). "A questa condizione diamo il nome di Antropocene. Natura e società sono diventate una cosa sola, con il risultato che non è più possibile distinguere tra storia umana e storia naturale". Recuperare i punti di riferimento in un orizzonte dove anche le categorie kantiane dello spazio e del tempo risultano stravolte, appare dunque come la sfida più urgente per l'uomo del nostro tempo. *Dove sono?* il titolo dell'ultimo saggio di Latour tradotto in Italia da Einaudi, è la voce di uno spaesamento e l'espressione del bisogno di ritrovare al più presto il significato della relazione, in un mondo lacerato dalle emergenze.

Tornare a progettare una città per l'uomo, è l messaggio di fondo che si ricava dall'impegno intellettuali di studiosi che credono nella possibilità di ritrovare una equilibrata armonia tra l'individuo e il cosmo, tale da far pensare che la felicità non debba essere un astratto ideale della ragione, vagheggiato dagli ingenui, ma un progetto concreto, finalizzato al cambiamento della società. ■

Una pubblicazione

web for business
swiss webacademy



**Redazione:**

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

**ISSN 2559 - 1797**

**ISSN-L 2559 - 1797**

**Indirizzi:**

info@cybertrends.it

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

**www.swissacademy.eu**

**www.cybertrends.it**

CERT STAR

# Simulazione incidente cyber

## 13 luglio 2022
## #savethedate

info@cybertrends.it

Cybersecurity Trends


3
PROCESS
AUTOMATION