

BUSINESS SOTTO CYBER- ATTACCO

**Cybersecurity per l'Impresa: Difendi la
Tua Azienda dalle Forze Oscure della Rete**

Massimiliano Corradini

con il contributo di Mohammed Bellala

Prima edizione: Maggio 2025

© Tutti i diritti sono riservati.

Ogni riproduzione anche parziale e con qualsiasi mezzo, deve essere preventivamente autorizzata da Massimiliano Corradini.

Edita da: Safebreach Academy



Indice

INTRODUZIONE	1
Perché questo libro?	1
A chi è rivolto il libro?.....	2
Perché ci concentriamo in particolar modo sulle PMI?.....	3
CAPITOLO 1: IL PROBLEMA DELLA CYBERSECURITY COINVOLGE TUTTI	9
1.1 Cybersecurity per la gestione degli affari – i criminali informatici... 12	
1.2 Cybersecurity per i privati - i dati sensibili che vengono usati contro gli utenti.....	17
1.3 Cybersecurity per Stati, organizzazioni e aziende - frodi, ricatti, blocchi	21
1.4 Criminologia del cybercriminale.....	22
CAPITOLO 2: LO SCENARIO DEL DIGITALE ITALIANO.....	27
2.1 L'Italia fanalino di coda del digitale	29
2.2 La classificazione delle aziende Italiane	30
2.3 Houston abbiamo un problema per le PMI	34
2.4 E-commerce indispensabile.....	40
2.5 È il peggior anno di sempre	43
CAPITOLO 3: SE VUOI COMBATTERLI E LIMITARLI DEVI CONOSCKERLI: CHI SONO I CYBERCRIMINALI	53
3.1 Il modello di affiliazione	68

3.2 Gli Initial Access Broker	72
3.3 I RaaS	76
3.4 I RaaS Operator, chi effettua il colpo	82
3.5 I Gruppi più importanti a livello mondiale: i casi più clamorosi	83
3.6 Le nuove truffe e le Scam city	85
3.7 Un caso italiano recente	87
3.8 TLC: il “butterfly effect” del mercato delle telecomunicazioni italiano e le conseguenze in campo cybersecurity	90
CAPITOLO 4: VETTORI E TECNICHE DI ATTACCO	95
4.1 Social engineering come funziona e sue caratteristiche	96
4.2 Phishing e sue varianti	99
4.3 Phishing mirato- spear phishing, whaling e BEC	101
4.4 Phone phishing-vishing-smishing- quishing	102
4.5 Web phishing- watering hole- cybersquatting e typosquatting ...	104
4.6 Una delle conseguenze: Social non sicuri	108
CAPITOLO 5: COSA FACCIAMO	111
5.1 L'azienda come modello digitale	114
5.2 L'effetto farfalle nere e (blu).....	117
5.3 Quanti sono i cybercriminali?	123
5.4 17.000 società informatiche: quante con competenze cyber?	128
5.5 Quanto costa un intervento post attacco?	137
5.6 Principali aree tecnologiche di investimento 2023-2024	146
5.8 ROI della cybersecurity “certificata”	150
5.9 La cultura della PMI inconsapevole.....	155
5.10 Leggi vigenti e normative standard per l'intervento.....	157
CAPITOLO 6: IL MODELLO A 5 LIVELLI PER SOPRAVVIVERE	161
6.1 Un approccio «originale» per l'offerta cyber per le aziende	161
6.2 La teoria dei vincoli (fin dove applicarla)	166
6.3 Le basi del modello	170
6.4 I principi	182
6.4.1 Initial reactive	186

6.4.2 Essential reactive	189
6.4.3 Cyber Proactive	195
6.4.4 Cyber Adaptative	207
6.4.5 Cyber Protect	211
CAPITOLO 7: UNO SGUARDO AL FUTURO	217
GLI AUTORI	223
Note Biografiche di Massimiliano Corradini	223
Ringraziamenti di Massimiliano Corradini	224
Note e ringraziamenti di Mohammed Bellala.....	225

Introduzione

Perché questo libro?

Si parte sempre dal *perché*, come ci insegna il brillante Simon Sinek: il *perché* di un progetto imprenditoriale, di un'azienda, o persino di un libro. Una vecchia canzone di Frank Sinatra (cantata magistralmente nel film "Pal Joy" del '57 diretto da George Sidney con Kim Novack e Rita Hayworth) aveva una parte che faceva «If they ask me I could write a book...»

E così, anche io mi sono chiesto: "perché non scrivere un libro sullo stato dell'arte della cybersecurity" pensando a chi, come voi, può testimoniare lo stato in cui versano le PMI italiane e che patiscono i molteplici problemi che emergono da questa immagine.

La "challenge" che mi sono prefissato è sicuramente importante ma lo scopo a cui ambisco è superiore allo sforzo richiesto: dimostrare che nel nostro paese non siamo ancora capaci di difendere i nostri interessi a partire dalla messa in sicurezza delle nostre reti informatiche.

"So why not": quindi perché no. Oggi sembra che chiunque possa scrivere un libro, ma *Business Sotto*

Cyber-Attacco nasce da un percorso ben diverso: anni di studio, un master, esperienza sul campo e la trasformazione di un System Integrator in un vero MSSP. Non è solo un libro, è il risultato di un viaggio nella cybersecurity dedicato alle piccole e medie imprese italiane. Ci sono migliaia di libri ormai in cui gli autori (o le intelligenze artificiali che li hanno aiutati a scrivere) consigliano qualsiasi tipo di miglioramento per l'azienda, dallo yoga agli eventi di team-building... trascurando un "lievissimo" dettaglio: le PMI italiane sono completamente esposte a un pericolo di cui nessuno si sta occupando seriamente.

A volte sembra di assistere a uno spettacolo surreale in cui il manager si preoccupa del clima aziendale organizzando eventi mondani, mentre lascia la cassaforte aperta in un locale che dà sulla strada.

Il fine che si prefigge questo testo è alto, ambizioso ma necessario: fornire un contributo nel mare Magnum dell'universo cyber ai cittadini, ai giovani, agli imprenditori e anche a chi è del mestiere. L'espressione "cybersecurity" è diventata familiare a chiunque, e ne siamo pervasi in molti momenti della nostra giornata soprattutto perché sempre più connessi con l'universo digital.

A chi è rivolto il libro?

In primis a chi ha la responsabilità di condurre aziende piccole e medie, il tessuto produttivo ed imprenditoriale del nostro bel paese, poi agli IT manager, a chi opera nelle reti, ai C.I.S.O. (Chief Information Security Officer) di aziende più strutturate, e poi in fondo anche a

chiunque abbia un lavoro per cui debba connettersi ad una rete (esiste qualcuno che ne sia immune?) perché il tema rilevante che vorrei suggerire è che la formazione deve partire dall'anello debole di questa catena, dal singolo individuo, da chi oggi con un click può far affondare la barca, il canotto o la nave da crociera su cui è imbarcato. E “last but not least” per i padri e per le madri di ragazzine e ragazzini che da nativi digitali dovrebbero avere un'educazione informatica consapevole, con un occhio di riguardo alle insidie della rete. Deve far riflettere che i figli di Bill Gates, uno tra i pionieri dello sviluppo digitale nel mondo, non hanno avuto lo smartphone prima dei 15 anni proprio su esplicito divieto del padre, il quale è ben consapevole dei danni che questo oggetto può fare nelle mani sbagliate.

Perché ci concentriamo in particolar modo sulle PMI?

Perché le aziende grandi, le corporate hanno le “spalle larghe”, nel senso che hanno persone ben formate che si dedicano a questo aspetto: hanno procedimenti, processi e procedure per cui risulta per loro usuale delineare il perimetro del rischio cyber. Lo affidano a mani esperte, acquistano servizi S.O.C (Security Operation Center) e rispondono con una procedura di gestione della crisi ad eventuali data breach.

Spesso le grandi corporation e multinazionali sono seguite dalle “TOP 45” della consulenza americane, anche nel nostro bel paese ci sono aziende che si sono dotate di Business Unit, di società di assistenza specializzate

nel mondo cyber e di Security Operation Center che offrono servizi ai loro clienti.

Il peso della responsabilità di alcune scelte del management italiano appare decisamente più leggero quando a fornire l'opportuna "consulenza" intervengono realtà come Accenture, Ernst & Young, Deloitte o PricewaterhouseCoopers. E nessuno potrebbe loro nulla obiettare.

Mettiamoci però dalla parte di chi:

- ✓ Risorse ne ha poche
- ✓ Competenze ancora meno
- ✓ È ignorante nell'accezione socratica per cui non ne capisce neppure l'utilità
- ✓ In fondo pensa "perché dovrebbe capitare a me"?

E in fondo verrebbe da credergli, nella sua totale ingenuità, se non fosse che è proprio a lui che, il rischio di cyberattacchi, può far più male:

- ✓ Proprio perché non ha risorse
- ✓ Non ha competenze
- ✓ Non sa che pesci prendere se dovesse succedere
- ✓ E quando avviene va nel panico più totale

Questo testo è stato scritto a quattro mani da due persone con un background diverso ma convergente.

Mi chiamo Massimiliano Corradini e nel 2021 ho svolto il Master in cybersecurity alla Bologna Business School col Prof. Michele Colajanni, Master che si prefiggeva

lo scopo di introdurre i partecipanti alla carriera di C.I.S.O. (Chief Information Security Officer).

È una figura che viene dalle realtà anglosassoni che per prime l'hanno introdotta e che ormai si inserisce anche nel nostro panorama lavorativo. Questo ruolo è di solito inquadrato come quello di un manager ben pagato che ha come obiettivo quello di pensare giorno notte e festività alla cybersecurity per aziende che “se lo possono permettere”. Non è puramente un informatico, “a volte” è più un avvocato appassionato di IT; comunque deve conoscere processi e procedure da introdurre nelle aziende.

Per quanto mi riguarda, ho deciso di cogliere il guanto della sfida sulla cybersecurity all'indomani di un evento che mi ha molto colpito. A distanza di un anno da uno degli eventi dedicati al tema: “Cybersecurity una gara da vincere”, svolto a Imola e promosso dall'Università di Bologna e da esperti della materia, più di una figura eminente del settore lanciava un “grido di dolore”: siamo indifesi e siamo sotto attacco. Poteva mai cadere nel vuoto quel grido di dolore e lasciare solo o inascoltato quell'allarme lanciato nell'aria?

Il Prof. Colajanni, dal palco, rifletteva sul fatto di aver insegnato per svariati anni a ingegneri, a tecnici, a “nerd” di vario tipo, a manager in scuole di business per ruoli direzionali e a C.I.S.O. Rivolgendosi indirettamente a sì e no il 3% delle aziende italiane, aziende che tra l'altro hanno tutte le risorse per pagarsi corsi, tecnici e altro...

È decisamente arrivato il momento di prestare attenzione a quel 97% di realtà imprenditoriali non formate, chiamandoli ad accogliere il guanto di sfida.

Noi l'abbiamo fatto strutturando un'offerta "cyber oriented" pensata per le tasche di piccole medie imprese italiane.

Rimaneva l'onere di lasciare un contributo ad un pubblico più esteso e da qui l'idea di un libro a uso e consumo di una platea più ampia, con poche conoscenze tecniche e con tanto da scoprire.

È così che è nata la necessità di mettere nero su bianco le nostre conoscenze, senza sensazionalismi: questo libro non aprirà Matrix al novello Neo con la pillolina rossa... ma almeno permetterà di capire come Matrix è parte del nostro mondo anche se non lo vediamo.

Dico "le nostre conoscenze" perché insieme a me c'è il mio compagno di viaggio, Mohammed Bellala, a cui ho affidato la stesura di alcuni punti particolarmente importanti e complessi. Non avrei mai pensato ad un libro sulla cybersecurity senza Mohammed perché è a lui e al Team di Safebreach e di Cyber Syntegra che si deve passione, focus e forte coinvolgimento di tutta l'azienda sul tema.

Mohammed è un tecnico super-professionista e iper-appassionato, un grande formatore i cui corsi sono sempre sold out e a cui devo dire molte volte grazie:

- Perché malgrado le innumerevoli certificazioni tecniche dirà socraticamente che non ne sa abbastanza

- Perché la componente etica per chi eroga soprattutto servizi offensivi e insegna corsi di tecniche offensive è il must e il biglietto da visita imprescindibile.
- Perché è un fantastico compagno di libro anche perché ha adottato tutte le tecniche per sconsigliarmi dal farlo.
- Perché il messaggio di fondo viene fuori da un dualismo: da chi l'azienda deve condurla e ne ha la responsabilità e chi sull'argomento passa ai fatti e ne è esperto.

Poiché la cybersecurity è ormai un tema che coinvolge tutti i reparti, i processi e il personale, e che richiede un'analisi da diverse prospettive e competenze trasversali, l'approccio che proponiamo in questo libro è il seguente:

- Ψ Non è un manuale tecnico
- Ψ Non rappresenta la Summa Theologica
- Ψ Non è rivolto agli iper-appassionati di cybersecurity... anche se forse saranno quelli che più lo leggeranno (questa è una scommessa con Mohammed)
- Ψ Per forza di cose e per la natura della materia trattata, quando uscirà questo testo ci saranno nuove evoluzioni da considerare e nuovi elementi da aggiungere (per questo motivo, nel retro copertina troverai un Qr Code che rimanda al nostro blog per rimanere sempre aggiornato)
- Ψ Si tratta di una maratona senza un traguardo

Dal dualismo tra chi l'azienda la guida e ne ha la responsabilità e chi non deve farla affondare per un click nasce l'approccio concreto che proponiamo, per cui questo libro:

- Ψ Vuol far arrivare i concetti nel modo più semplice possibile
- Ψ Vuol tuttavia fornire un altro punto di vista perché questo argomento in fondo riguarda tutti noi
- Ψ Vuole contribuire allo sviluppo della cultura sulla cybersecurity nel paese maggiormente colpito dagli attacchi mondiali
- Ψ Vuole fornire utili strumenti di orientamento per le piccole e medie realtà aziendali
- Ψ Vuole mettere a disposizione dell'azienda digitale di oggi, un modello organizzativo, tecnologico e funzionale per la misurazione della postura cyber

Forti di questa consapevolezza e di questa necessità che siamo sicuri sia anche la tua, ora, caro lettore, ti auguriamo una buona lettura!

CAPITOLO 1

Il problema della cybersecurity coinvolge tutti

Ognuno di noi ha diverse identità digitali tra il mondo personale, quello lavorativo e come privato cittadino: un account di posta personale (Gmail, Aruba, Libero etc...) un account aziendale in cui sono definiti dominio, privilegi ed autorizzazioni per accedere a server aziendali, a servizi in Cloud. Ognuno di noi è registrato e ha accesso a diversi servizi e viene identificato da un codice fiscale per lo Stato fisco, una patente per la motorizzazione civile e dal 2015 ha accesso al registro elettronico con lo SPID, il sistema di autenticazione riservato ai cittadini per l'accesso ai servizi della pubblica amministrazione con un'identità digitale unica. Sistema che verrà sostituito per tutti dall'IT wallet, un'unica

piattaforma in cui saranno raggruppati e accessibili diversi documenti come la carta d'identità elettronica, la tessera sanitaria, i documenti di disabilità, la patente di guida e varie carte o documenti di aziende private con cui abbiamo rapporti. Per ognuno di questi servizi c'è un'identità digitale.

Le identità digitali sono oggi il principale obiettivo dei criminali informatici per cui occorre una maggior consapevolezza su cosa rilasciamo, come lo facciamo, come registriamo e salviamo credenziali e accessi. In particolare, cosa cercano i criminali:

- Carte di credito e dati finanziari
- Dati personali e sanitari
- Credenziali di accesso
- Documenti di identità, foto e video

In generale qualsiasi informazione utile sia come singolo individuo sia per la struttura dove lavora.

Come siamo arrivati a questo? L'attenzione crescente verso il tema della cybersecurity riflette l'evoluzione della nostra società digitale, che sta trasformando ogni aspetto della nostra vita: modelli di produzione e di consumo, modelli di business e di comunicazione, leggi, commercio, criminalità. La pandemia del 2020 ha agito come un acceleratore, consentendo all'Italia di ridurre in parte il divario tecnologico e digitale rispetto al resto del mondo industrializzato. Questo tema ha contribuito a generare l'urgenza discussa in questo testo: il significativo ritardo nell'adozione delle tecnologie digitali e

delle misure di sicurezza. L'accelerazione è stata spesso determinata da fattori esterni, come le normative europee con relative sanzioni, o la necessità di ottenere certificazioni per partecipare a filiere produttive sempre più esigenti.

La crescita esponenziale dell'Internet of Things e degli oggetti "smart", sempre connessi alle reti in ogni momento e luogo, sta trasformando radicalmente il panorama tecnologico. Parallelamente, l'apertura delle reti aziendali alla produzione e la crescente importanza dell'Operational Technology (OT) richiedono una nuova attenzione. In questo contesto, emerge e si sviluppa con un'accelerazione sorprendente, persino per i suoi stessi creatori, un fenomeno che potrebbe rappresentare un evento dirompente, o, parafrasando i filosofi del Novecento, una "burrasca creativa" in stile schumpeteriano: l'Intelligenza Artificiale.

A ciò si aggiungono eventi drammatici che segnano la storia contemporanea. La guerra tra Russia e Ucraina, ad esempio, ha visto un'esplosione di attacchi cyber, condotti da gruppi attivisti schierati a favore o contro gli Stati dei due blocchi. Lo shortage di materiali causato dal Covid, l'impennata dei prezzi, i conflitti come quello tra Israele e Palestina, e gli attacchi nello stretto di Bab-el-Mandeb da parte degli Houthi, sono tutti fattori che, in modi diversi, hanno favorito, intensificato e alimentato le attività delle organizzazioni criminali nel mondo del cybercrime.

Pensiamo poi che, come utenti, non potremmo mai pensare di vivere senza connessione per qualche secondo

e diamo per scontato che i servizi siano sempre attivi, disponibili e funzionanti 24 ore su 24. Tirando le somme: ci sono sempre più oggetti connessi alle reti, sempre più devices smart in una società iperconnessa, il che equivale a mandare a nozze chi di mestiere vuol fare il criminale informatico. Un tempo, per tenere lontani questi soggetti pericolosi, chi amministrava le reti delle aziende erigeva attorno al proprio castello digitale l'equivalente di un fossato ricoperto d'acqua e abitato da feroci coccodrilli, ovvero: bastava un firewall e degli antivirus basati su firme. Un lontano ricordo. Oggi la difesa non ha confini e non ha limiti perché siamo connessi da qualsiasi luogo sempre e comunque e con sempre più devices e applicazioni disponibili in real time. Ognuno di noi e ogni oggetto che possediamo ci espone a vulnerabilità maggiori. Una vera manna per chi attacca e molti pensieri in più per chi difende.

La minaccia cyber colpisce indiscriminatamente: commercio, privati cittadini, organizzazioni, aziende e Stati. Nessuno è immune, e credere di non essere un bersaglio interessante è l'errore che espone maggiormente agli attacchi dei cybercriminali.

1.1 CYBERSECURITY PER LA GESTIONE DEGLI AFFARI – I CRIMINALI INFORMATICI

È un dato di fatto che si è passati dall'idea romantica dell'hacker col cappuccio in uno scantinato ad un vero e proprio mercato del crimine informatico i cui attori

principali possono essere assimilati ad organizzazioni, Holding o multinazionali a tutti gli effetti. Vedremo successivamente il modello di affiliazione che utilizzano e chi sono i protagonisti di questo mondo sotterraneo.

Senza andare molto indietro nel tempo, questa immagine “cinematografica” del cybercriminale si fa più forte con la serie del 2015 *Mr. Robot*, con un giovane Rami Malek nei panni dell'ingegnere Elliot Alderson, racconta la storia di un hacker vigilante che, di giorno, lavora per una società di sicurezza informatica. Nei suoi momenti liberi, Elliot si trasforma in un giustiziere digitale, lottando contro il sistema, mentre si lascia sedurre da un movimento di hacktivist, la *fsociety*, il cui obiettivo è distruggere una multinazionale accusata di aver insabbiato rifiuti tossici, responsabili della morte di numerose persone, tra cui suo padre, a causa della leucemia. La serie, composta da quattro stagioni, tiene il fiato sospeso e si distingue per la sua indiscutibile capacità di intrattenere gli amanti della suspense e del genere.

Anche i primi hacker degli anni 80 e 90 hanno da sempre suscitato un misto di curiosità e simpatia perché a volte accostati a cavalieri del bene contro i Poteri Forti, le multinazionali dello sfruttamento e perché in fondo, per alcuni, le opere sono state sul crinale tra l'etico (hacker nel senso vero) e il crimine. Come non ricordare Kevin Mitnik (il Condor) l'hacker forse più famoso della storia, ricercato negli anni 90 per aver violato oltre 40 importanti organizzazioni criminali tra cui i computer della Pacific Bell e “dopo 4 anni di carcere scontati fino

al 2000” pian piano è diventato una delle voci più forti nell’insegnamento delle tecniche (lecite) di hacking, autore del celebre “The art of deception” (2003) e consulente e conferenziere di grido. Si è spento nel 2023 in attesa del primo figlio dopo un anno di lotta contro un cancro al pancreas.

Come non citare Gary McKinnon, un ragazzo scozzese appassionato di UFO con la sindrome di Asperger che nel 2002 compì il più grande attacco informatico militare di tutti i tempi contro migliaia di PC dell’Esercito, della Marina, dell’Aeronautica, della NASA e del Dipartimento della Difesa. Grazie alla diagnosi di sindrome di Asperger e ai successivi studi effettuati su McKinnon da parte di Simon Baron-Cohen, direttore del Centro di ricerca sull’autismo dell’Università di Cambridge, l’avvocato dell’hacker riuscì a negare l’estradizione richiesta nel 2012 dagli Stati Uniti da parte di Theresa May Sottosegretario di Stato per gli Affari Interni del Regno Unito. Nel corso della sua ricerca sull’autismo, Baron-Cohen è poi diventato un’autorità sulla connessione emergente tra Asperger e ingegneria. “Ha senso che qualcuno con la sindrome di Asperger possa diventare abile nell’hacking”, disse “semplicemente perché una delle cose che condividono è la comprensione dei sistemi, compresi i sistemi informatici”. Vi sono stati altri grandi hacker/criminali informatici affetti dalla sindrome di Asperger come Andrian Lamo e Albert Gonzales. Nel mio piccolo posso testimoniare di un episodio avvenuto nella città dove sono nato e cresciuto fino a 20 anni, L’Aquila, in cui uno studente del Dipartimento di

matematica pura e applicata, corso di laurea in informatica, prossimo alla tesi, aveva ‘bucato’ i sistemi del Pentagono ed era entrato dentro ai segreti più segreti d’America arrivando perfino all’archivio contenente i dati personali dell’ex presidente degli Stati Uniti, Bill Clinton.

Erano gli anni '90, si diceva e “l’America era pur sempre l’America”, come a dire che in fatto di tecnologia sarebbero sempre stati inarrivabili e avanti rispetto al “vecchio continente”. Eppure, dall’Aquila un laureando, col solo intento di dimostrare a sé stesso cosa potesse fare divertendosi, rivelò a tutti che le sue competenze e capacità erano superiori a quelle della superpotenza e riuscì a mettere in crisi la sicurezza del quartier generale del Dipartimento della difesa degli Stati Uniti d’America. Dell’episodio ne parlarono televisioni, giornali e ci si trovò all’Aquila il Dipartimento della Difesa americano. Il Rettore di allora il Prof. Giovanni Schippa affermava (era il 95) “Avrà fatto anche un danno ma avete visto quanto sono bravi i nostri studenti?”. Difatti l’anno dopo le iscrizioni al dipartimento di informatica triplicarono ma il clamore e la presenza degli americani fecero passare anche momenti di panico al mio amico che da quel momento non volle più tornare sull’argomento malgrado l’interesse suscitato e le richieste di multinazionali per mirabolanti carriere prospettate.

Ebbene quel mondo lì, che raccontiamo con un velo di divertimento e malinconia, è solo un ricordo. Oggi si parla per la cybersecurity di un Megatrend dove scorrono fiumi di investimenti e oceani di costi legati agli

attacchi. Secondo il report IBM “Cost of Data Breach” nel 2023, il costo degli attacchi informatici rilevati ha raggiunto i 8 trilioni di dollari, cifra che è arrivata a 9,5 trilioni di dollari nel 2024 e supererà i 10,5 trilioni di dollari nel 2025 (fonte IBM). Per fare un confronto, nel 2015 il valore degli attacchi informatici era di 3 mila miliardi di dollari. Per quanto riguarda la violazione dei dati, un attacco medio negli Stati Uniti provoca perdite pari a 4,45 milioni di dollari.

Se questo flusso di denaro fosse misurato come quello di uno Stato, il crimine informatico potrebbe essere la terza economia mondiale dopo Stati Uniti e Cina (stando alla fonte “Cybersecurity Ventures”).

Come abbiamo visto, i criminali informatici si sono trasformati in vere e proprie organizzazioni conglomerate del crimine, spesso operanti in paesi dove, in alcuni casi, collaborano strettamente con gli Stati. Tra questi troviamo nazioni come la Cina, la Russia, l'Iran e la Corea del Nord, che, secondo la definizione data dall'amministrazione Clinton negli anni '90, sono considerati 'paesi canaglia' per il loro sostegno al terrorismo internazionale

Da notizie di stampa in cui si apprende che, per creare un clima distensivo con la Russia e giungere alla pace con l'Ucraina, gli Stati Uniti sono stati disponibili a fermare la Cyber War in corso (dichiarazioni del 3 marzo 2025 di Pete Hegseth, segretario alla difesa americano).

1.2 CYBERSECURITY PER I PRIVATI - I DATI SENSIBILI CHE VENGO NO USATI CONTRO GLI UTENTI

La nostra “vita digital”, sempre connessa, lascia evidenti tracce sul web dove criminali informatici, skript kiddens e altri attori hanno facilità a reperire informazioni, identità digitali, carte d’identità, codici fiscali, foto, accessi a portali, carte di credito. Il dark web è il luogo dove si riescono a reperire con relativa facilità tutte queste informazioni con pochi dollari.

È indicativo il fatto di come sia nato l’“Onion routing”, il principio fondamentale che consente a Tor (il browser usato per evitare di essere tracciati) di mantenere l’anonimato dei suoi utenti grazie ad un programma sviluppato e finanziato a metà degli anni 90 dal governo federale degli Stati Uniti d’America. Lo scopo era quello di proteggere le persone nella comunità dell’Intelligence, gli informatori, cittadini e giornalisti che vivevano sotto regimi oppressivi, permettendo loro di comunicare e interagire nel completo anonimato. La Marina degli Stati Uniti brevettò lo sviluppo della rete Onion nel 1998 e concede nel 2006 il codice TOR in licenza gratuita. E sempre nel 2006 molti scienziati creano il Tor Project, un’associazione senza scopo di lucro in Massachusetts ricevendo notevoli fondi per un progetto a beneficio dell’umanità. Nel 2009 avviene la prima transazione sulla blockchain di bitcoin che costituisce la pietra miliare dell’intero sistema di trading. Si erano magicamente creati gli ingredienti perfetti perché il

crimine organizzato avesse a disposizione un sistema di anonimato, una moneta anonima e la rete Onion per perpetrare i suoi scopi.

Oggi bastano pochi click per scaricare TOR e navigare con alcuni motori di ricerca quali DuckDuckgo nei meandri del dark web e ricercare credenziali email, numeri di telefono, carte d'identità, carte di credito e quanto può bastare per effettuare truffe con phishing o smishing ai malcapitati o aprire con quei documenti un conto all'estero e operarci in modo da far sembrare tutto lecito. Se lo può fare un comune cittadino neppure troppo esperto si può immaginare come utilizzino questi dati chi ne fa una professione criminale.

In un bel servizio delle Iene del 28 maggio 2024 Luigi Pelazza intervista "Lupo", un giovane "criminale" informatico che aveva accettato di spiegare come operava nel rubare informazioni, poi utilizzate per i suoi scopi malevoli. Questo a pochi giorni dall'arresto dell'allora più ricercato criminale informatico d'Europa, Julius Kivimaki, per aver hackerato migliaia di pazienti che poi ricattava. Lupo è specializzato in database e nel servizio fa vedere come riesce a carpire le credenziali di una giovane. Appostandosi dentro un furgone, vicino al palazzo di residenza della ragazza, prima disturba il segnale wifi e contemporaneamente offre un clone del wifi originale, inducendo facilmente gli utenti, che non si accorgono delle differenze, ad inserire le proprie credenziali. Con un semplice scan vede chi è connesso, ne individua le vulnerabilità e tira fuori un database di foto compromettenti di un utente (che poi potrebbe essere

ricattato) così come individua le vulnerabilità di un sito e lancia un malware che permette di scoprire gli utenti registrati con credenziali criptate. In pochi istanti, con un semplice programma, riesce a decifrarle. Tra le innumerevoli credenziali, seleziona quelle di una ragazza e trova le carte d'identità di sua figlia, madre e padre, complete di foto, che potrebbero essere utilizzate per il selfie richiesto dagli istituti di credito per aprire un conto online. Successivamente, analizzando il database con circa 40.000 email e password, utilizza un altro programma per identificare quante di queste persone avevano aperto un conto online con le stesse credenziali. Ne seleziona una decina e mostra come, chiamando uno degli assegnatari e presentandosi come PayPal, riesca a eludere il sistema di doppia autenticazione. Si fa passare per l'utente e, chiedendo informazioni su un acquisto sospetto effettuato dal suo conto, convince l'interlocutore a fornirgli il codice OTP. In questo modo, il malcapitato, ignaro, finisce per consegnargli il codice che permette di completare le transazioni online.

Traiamo da questo semplice episodio alcune lezioni grazie all'opera di "Lupo" per noi utenti":

- Utilizzare Wi Fi pubblici o di alberghi o di altre strutture in cui siamo ospiti può essere molto pericoloso perché siamo poi facilmente intercettabili.
- Mai rilasciare documenti personali via email e se proprio necessario cancellarla subito
- Mai utilizzare le stesse credenziali per accedere a vari servizi

BUSINESS SOTTO CYBER-ATTACCO

- Mai comunicare codici via telefono ad operatori che si spacciano per il proprio Istituto o Operatori essenziali
- Assicurarasi di rilasciare credenziali su Portali che abbiano il bollino di sito sicuro

Da quest'attività Lupo, che non sarebbe altro che un "cracker" di profilo basso, asserisce di guadagnare circa 5.000 euro al mese con "colpi" che a volte fruttano qualcosa in più. La notizia spiacevole è che Lupo non è che un piccolo pesce nel Magnum di chi ne fa una professione criminale, ben altri sono i criminali pericolosi in rete.

L'iper-connettività, ormai parte integrante dei nostri strumenti di lavoro e svago, rende il compito di figure come Lupo e di chi opera nel cybercrime incredibilmente più semplice. Più tempo trascorriamo online, più aumentano le nostre vulnerabilità. Una vulnerabilità in origine mai risolta e quindi da sempre associata al sistema Spid e solo da poco deflagrata su scala nazionale ha mostrato quanto sia fragile il nostro ecosistema digitale: senza un registro centralizzato, ogni cittadino può avere fino a 12 identità attive, una per ogni provider. Questo apre la porta a furti d'identità digitali, con il rischio concreto che un criminale modifichi, ad esempio, l'IBAN associato, incassando così fondi destinati a ignari cittadini. Una falla silenziosa, ma devastante.

Nella "smartphone society", si stima che nel mondo siano in uso 7,5 miliardi di smartphone, quasi uno per ogni abitante del pianeta. Un quarto della popolazione,

circa 2 miliardi di persone, ne fa uso per almeno 7 ore al giorno. In Italia, 2 persone su 5 soffrono di “nomofobia” (No Mobile Phone Phobia), ovvero l’ansia di essere disconnessi o lontani dal proprio smartphone.

1.3 CYBERSECURITY PER STATI, ORGANIZZAZIONI E AZIENDE - FRODI, RICATTI, BLOCCHI

Dopo il dominio della terra, del mare, del cielo e dello spazio, lo spazio cibernetico è divenuto universalmente il quinto dominio o la quinta forza a disposizione degli Stati per esercitare pressioni e azioni nella scacchiera mondiale. Questo nuovo campo di battaglia digitale ha cambiato il modo in cui nazioni, organizzazioni e aziende si confrontano, con minacce che spaziano dalle frodi ai ricatti e ai blocchi informatici. Le frodi informatiche, come il noto caso del data breach subito da Yahoo nel 2013, che compromise miliardi di account, hanno evidenziato quanto sia vulnerabile la gestione delle informazioni personali e aziendali. Questo tipo di attacco può danneggiare irreparabilmente la fiducia dei consumatori e provocare perdite finanziarie significative.

Il ransomware, una forma di ricatto in cui gli aggressori cifrano i dati e richiedono un riscatto, ha preso di mira non solo imprese private ma anche infrastrutture critiche, come ospedali e sistemi di trasporto. Un esempio emblematico è l’attacco del ransomware WannaCry nel 2017, che colpì il Servizio Sanitario Nazionale del

Regno Unito, paralizzando decine di ospedali e mettendo a rischio la salute dei pazienti.

Gli attacchi di blocco informatico, noti come denial-of-service (DoS), sovraccaricano i server con richieste di accesso, simili a una folla che tenta di entrare in una piccola porta, bloccando così l'accesso legittimo. Questi attacchi possono essere utilizzati per estorsioni o come strumenti di protesta politica. Un'immagine efficace per descrivere un attacco DoS è quella di un ingorgo stradale, dove un flusso continuo di veicoli impedisce il normale scorrere del traffico, paralizzando l'intera rete stradale.

Mentre le minacce continuano a evolversi, le organizzazioni devono adattarsi rapidamente per proteggere le informazioni e garantire la continuità operativa. Questo richiede l'adozione di misure tecnologiche avanzate e una strategia di risposta pronta agli incidenti, essenziali per mantenere la sicurezza nel panorama digitale in costante cambiamento.

1.4 CRIMINOLOGIA DEL CYBERCRIMINALE

L'analisi criminologica dei cybercriminali evidenzia un problema fondamentale di percezione e definizione del reato digitale, che deriva sia dalla mancanza di consapevolezza delle vittime sia dall'autopercezione dei criminali stessi.

Da un lato, molte persone, inclusi manager e responsabili aziendali, faticano a riconoscere il potenziale

pericolo dei crimini informatici fino a quando non subiscono un danno concreto, come il furto di denaro o la compromissione di dati sensibili. Questa impreparazione si riflette nella percezione diffusa che i reati online siano meno gravi rispetto a quelli tradizionali: un problema di sicurezza secondario, simile a un fastidioso guasto meccanico o a un aggiornamento software da rimandare.

Dall'altro lato, anche gli stessi cracker, in particolare quelli che si muovono al di fuori dei grandi circuiti della criminalità organizzata, non si percepiscono come veri criminali. Questo è un punto fondamentale che genera però un equivoco psicologico capace di aumentare il divario tra una mentalità adattiva per la vita nella società civile e la devianza criminale che porta a considerare azioni illecite. La natura intangibile delle loro azioni - l'assenza di contatto fisico, la mancanza di violenza diretta o di danni visibili nell'immediato - crea una sorta di "cuscinetto morale" che permette ai perpetratori di mantenere una distanza emotiva dalle loro vittime. Per molti di questi individui, il cybercrimine appare quasi come un gioco di abilità o una prova di competenza tecnica, piuttosto che come un vero e proprio atto illegale che causa danni reali e duraturi. Questo fenomeno è stato esplorato da diverse ricerche in ambito psicologico e criminologico, che mostrano come gli hacker spesso giustificano le proprie azioni definendosi "ricercatori", "sfidanti del sistema", o addirittura "guardiani del web", creando un distacco semantico che attenua l'impatto psicologico del concetto di colpevolezza.

Ma la percezione errata della “non gravità” del crimine digitale ha conseguenze ben più profonde di quanto si possa pensare. Quando i cybercriminali non avvertono alcuna responsabilità morale o sociale, vengono a mancare quei freni psicologici e culturali che normalmente limitano la propensione a compiere reati. Questo scenario genera una sorta di effetto “punto cieco”, dove né i criminali né le vittime percepiscono fino in fondo l’impatto devastante del crimine. Si è così sviluppata una narrazione distorta: il cybercrimine come un fenomeno trascurabile o addirittura “gestibile”, una narrativa pericolosa che alimenta l’espansione di questo tipo di attività e favorisce la creazione di comunità clandestine sempre più articolate e pericolose.

La situazione è ulteriormente aggravata dall’esistenza di un mondo sommerso, il “dark web”, dove si muovono indisturbati non solo hacker indipendenti, ma anche organizzazioni criminali tradizionali, gruppi terroristici e persino reti di pedofili. Questi gruppi utilizzano piattaforme anonime e strumenti di crittografia avanzati per condurre operazioni illecite che vanno ben oltre il furto di identità o il sabotaggio informatico. Lo studio di McGuire (2012) ha mostrato come l’ecosistema del crimine informatico sia diventato il punto di convergenza tra criminalità tradizionale e nuove forme di illegalità. Le mafie italiane e russe, ad esempio, hanno imparato a sfruttare le criptovalute per il riciclaggio di denaro e la gestione di traffici illeciti, mentre gruppi terroristici come ISIS e Al-Qaeda utilizzano il web non solo per propaganda e reclutamento, ma anche per la

compravendita di armi e la pianificazione di attentati in modo discreto e coordinato.

Queste connessioni tra il crimine organizzato e il cybercrimine non sono ipotetiche, ma ben documentate: nel 2018, ad esempio, un'indagine dell'Europol ha rivelato come un noto gruppo mafioso italiano abbia utilizzato piattaforme di e-commerce false per facilitare il traffico di droga e la movimentazione di denaro illecito attraverso conti bancari offshore collegati a server in paesi con giurisdizioni deboli. Inoltre, uno studio dell'Università di Oxford (Hutchings & Holt, 2017) ha evidenziato come il ransomware sia diventato uno degli strumenti più redditizi per le organizzazioni criminali, generando guadagni di milioni di euro attraverso estorsioni digitali che sfruttano la mancanza di preparazione delle vittime e la difficoltà nel tracciare le transazioni.

La sottovalutazione dei danni reali del cybercrimine porta a una conseguenza paradossale: mentre i reati fisici, come il furto o l'aggressione, sono percepiti come immediatamente pericolosi e inaccettabili, i crimini online spesso passano inosservati o vengono ridimensionati come semplici "marachelle digitali". Eppure, le loro ripercussioni possono essere devastanti. Basti pensare al caso di Cambridge Analytica, in cui la raccolta illecita di dati ha avuto conseguenze geopolitiche di enorme portata, influenzando l'esito di elezioni e referendum in diversi paesi.

La sfida futura che già ci coinvolge, quindi, è creare una consapevolezza reale sia tra le vittime potenziali che tra i cybercriminali. Occorre innanzitutto abbattere il mito

del crimine informatico come reato “non dannoso”. I responsabili devono essere messi di fronte alla concretezza dei danni causati: furti d'identità che distruggono vite intere, violazioni di dati sensibili che portano al suicidio delle vittime di estorsioni, diffusione di materiale pedopornografico che genera traumi irreversibili nei minori. Parallelamente, è necessario formare le imprese e i singoli cittadini sull'importanza di un comportamento vigile e proattivo, insegnando che ogni azione compiuta online può avere conseguenze reali, e che trascurare la sicurezza non è solo un rischio, ma una pericolosa forma di complicità passiva.

Cambiare la percezione del cybercrimine richiede quindi un intervento a livello culturale: smettere di vedere l'attacco informatico come un fastidio temporaneo e iniziare a riconoscerlo per quello che è davvero: una minaccia concreta alla sicurezza personale, aziendale e sociale.