Studio Filippini & Associati
CONSULENZA FISCALE E SOCIETARIA

Studio Filippini & Associati
Piazza Annibaliano 18
00198 Roma

Tel +39.06.88812201
Fax +39.06.88812199
studiofilippini@studiofilippini.it

P.I. 04818971006

Dottori Commercialisti
Aldo Filippini
Alessandra Razzi

ROMA, 25 NOVEMBRE 2024

CIRCOLARE INFORMATIVA 15/2024

(A CURA DI ALDO FILIPPINI)

CYBERSECURITY E GOVERNANCE

Premessa

Alzi la mano chi non ha mai avuto esperienza di qualche tipo di attacco informatico; per qualcuno, magari più attento nell'impostazione e gestione dei propri presìdi, potrebbe essersi trattato di un maldestro tentativo di ottenere dati sensibili; altri potrebbero aver subito un blocco temporaneo sul funzionamento del proprio PC con la distruzione di qualche documento personale, con evidente disagio e perdita di tempo ma pochi danni veri e propri; altri ancora, spero non molti, potrebbero aver sperimentato la brutta esperienza di un blocco prolungato delle proprie attività commerciali con gli imponenti

costi conseguenti e le importanti responsabilità connesse ad una esfiltrazione dei dati sensibili di altri soggetti, laddove non fossero state poste in essere misure di protezione adeguate.

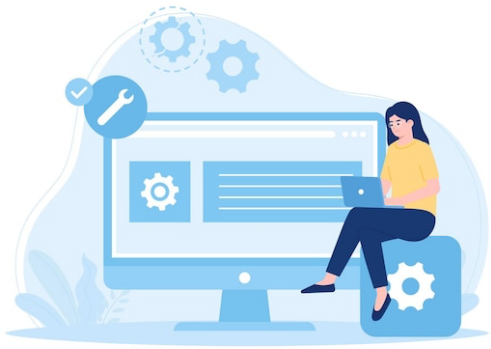
Se le conseguenze di un attacco informatico possono essere “molto fastidiose” per un privato, esse potrebbero diventare devastanti in capo ad una società, con profili di responsabilità non banali per gli amministratori e i responsabili della sicurezza informatica.

Ora, che l’utilizzo delle nuove tecnologie nelle aziende negli ultimi decenni abbia avuto uno sviluppo via via crescente è cosa conosciuta.

Che esso sia diventato esponenziale negli ultimi anni è anch’esso un fatto.

A ciò, tuttavia, non ha corrisposto un parallelo sviluppo nella nostra cultura sull’utilizzo degli strumenti informatici.

Anzi.



Paradossalmente, è successo il contrario. Chi incominciava a smanettare su un pc qualche decennio fa doveva combattere con interfacce non semplici, applicativi per i quali era necessario ragionare (!), database che dovevano essere configurati in parte dagli utenti, etc. Le soluzioni ai problemi quotidiani erano cercate sui forum di discussione, che erano dei veri e propri think tank, una ricchezza a disposizione di tutti per la propria cultura informatica, dove si acquisivano, oltre alle conoscenze tecniche, anche consapevolezza e sensibilità sul nuovo meta-ambiente che si andava creando.

Ma poi tutto è diventato più “facile”.

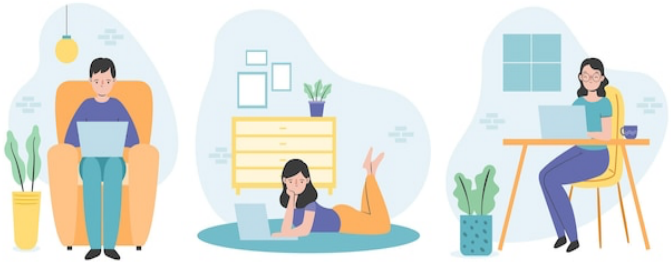
I grandi player hanno (giustamente) offerto soluzioni sempre più semplici per l’utente (e conseguentemente enormemente più complesse “dietro l’interfaccia”), l’utente si è (giustamente, forse… ma forse no…) concentrato maggiormente sulla propria attività principale (avvocato, contabile, medico, etc.), lasciando agli esperti il compito di gestire tutto ciò che avesse a che fare con l’IT.

Questo fenomeno non è una caratteristica solo dell’informatica: quando mio padre andava in motocicletta, lui, o chiunque dei suoi compagni, era in grado di smontarla e rimontarla tutta da capo e l’unico motivo di recarsi in officina era per la disponibilità delle attrezzature; oggi io monto sullo scooter, spingo un bottone e parto e se mi si ferma a mala pena so metterlo sul cavalletto.

Insomma, e tornando all’IT, la maggior parte di noi è rimasta ignorante, non ha avuto né tempo né voglia di conoscere e informarsi, mentre la complessità della tecnologia e l’utilizzo che se ne faceva evolveva di ora in ora.

E poiché le aziende sono organismi molto complessi, la mancanza se non di una preparazione perlomeno di una consapevolezza dell’importanza della Cybersecurity, nell’intero personale, aumenta il rischio di penetrazione da parte di soggetti male intenzionati anche in aziende che hanno disposto procedure di sicurezza apparentemente adeguate.

A ciò, peraltro, si aggiunge il fatto che, soprattutto a seguito della pandemia, è molto diffusa a tutti i livelli aziendali, forse con la sola eccezione dei blue collars, la pratica di lavorare da



una propria postazione (soprattutto, ma non solo, la propria abitazione), il che ovviamente aumenta ulteriormente i rischi e richiede che ulteriori procedure di sicurezza siano implementate.

Cosa può succedere? Principali rischi

La European Union Agency for Cybersecurity (ENISA), nella sua pubblicazione ENISA Threat Landscape 2023[1] ha individuato le seguenti principali minacce per la sicurezza informatica[2]:

DDoS Attack	Attraverso il Distributed Denial of Service Attack il server è invaso da una quantità di traffico tale da renderlo non accessibile agli utenti
Ransomware	Il Ransomware è un tipo di Malware che impedisce all'utente di accedere ai propri dati, che vengono inoltre criptati. Il nome (*ransom*, riscatto) deriva dalla richiesta di denaro che segue l'attacco al fine di rendere nuovamente accessibili i dati.
Malware	Con il termine Malware si identifica qualsiasi software per danneggiare o sfruttare (senza autorizzazione) un dispositivo
Social engineering	Per Ingegneria Sociale si intendono le attività che sfruttano il comportamento umano per ottenere l'accesso al dispositivo: gli utenti possono essere indotti ad aprire documenti, file o e-mail, a visitare siti Web o a concedere

[1]Per chi fosse interessato la pubblicazione è liberamente scaricabile al seguente link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 .
[2]L'elenco e le relative descrizioni non hanno una definizione assoluta: per esempio il Malware comprende anche il Ransomware; un'attività di Social Engineering può essere propedeutica ad un DDos Attack o a un Ransomware, e così via.

	l'accesso a sistemi o servizi. E' molto importante considerare che, sebbene le modalità utilizzate per indurre la vittima in errore possano avere aspetti tecnologici, **esse si basano principalmente sul comportamento umano;** e, soprattutto, che le **attività** di Ingegneria Sociale sono spesso propedeutiche ad attacchi Ransomware, **non di rado mesi o addirittura anni prima dell'attacco vero e proprio.**
Threats against data	Le minacce ai dati includono Data Breach (Violazione di Dati) e Data Leaks (Perdita di Dati). Secondo la definizione della ENISA: - La Violazione di Dati è un attacco informatico intenzionale con l'obiettivo di ottenere un accesso non autorizzato e rilasciare dati riservati - Le Perdita di Dati è un evento anche accidentale causato da configurazioni errate o errori umani che può causare la perdita o l'esposizione involontaria di dati riservati
Internet threats	In notevole crescita negli ultimi periodi, comprendono le interruzioni dei servizi di Internet o delle comunicazioni elettroniche, blackout, arresti o censure. Il pericolo può arrivare non solo da criminali: le interruzioni di Internet possono essere dovute anche ad operazioni governative, disastri ambientali, tagli di cavi, problemi tecnici e azioni militari.
Information manipulation and	La fattispecie interessa meno il settore degli operatori economici, ma viene qui riportata sia per completezza sia

interference	per l'enorme crescita (e pericolo che rappresenta) che essa ha avuto negli ultimi anni. Si tratta di un modello di comportamento, intenzionale e coordinato, che ha il potenziale di avere un impatto negativo su valori, procedure e processi politici.
Supply chain attacks	Un attacco alla catena di approvvigionamento prende di mira la relazione tra le organizzazioni e i loro fornitori, ed è costituito da una combinazione di almeno due attacchi. Le conseguenze possono essere devastanti per la possibilità di attaccare una platea molto vasta di operatori sfruttando un ingresso che potrebbe anche rimanere "nascosto" per diverso tempo.[3]

Cosa si dovrebbe fare? La Governance

Che gli organi di governo debbano dedicare massima attenzione e risorse agli aspetti della Cybersecurity è ovvio[4]. Peraltro, la novità della materia, gli aspetti tecnici particolarmente complessi, la diffusa mancanza di sensibilità sui pericoli di origine tecnologica rispetto a quelli tradizionali, non aiutano né gli amministratori né i responsabili IT e della sicurezza.

[3] Emblematico è stato il caso SolarWind, nel 2020, con il quale furono attaccati dati e le reti interne di migliaia di clienti della nota società di Software.

[4] *"Il Consiglio di Amministrazione è quindi direttamente coinvolto nei processi decisionali, strategici e organizzativi che riguardano l'utilizzo della tecnologia digitale a supporto della trasformazione dei modelli di business. Una non adeguata gestione di tali aspetti potrebbe concorrere a configurare una responsabilità degli amministratori".* (Assirevi, Monografia n. 4 – maggio 2023)

La riflessione in materia potrebbe iniziare da alcuni dei concetti espressi nella già citata Monografia di Assirevie nell'ENISA Threat Landscape 2023[5] :

- Il framework di cybersecurity dovrebbe comprendere in modo olistico e trasversale linee guida e best practice per gestire i rischi del mondo digitale e, indipendentemente dal settore in cui si opera e della percezione del rischio che ne hanno gli organi direzionali, dovrebbe essere finalizzato ad ottenere una posizione di sicurezza forte

- Tutte le funzioni devono essere coinvolte

- E' opportuno il coinvolgimento anche degli stakeholder per una miglior definizione dei rischi e allocazione delle risorse

- L'ottenimento di certificazioni, ancorché non sufficienti, può contribuire, anche tramite il processo stesso di ottenimento, alla diffusione di una miglior consapevolezza del rischio e conseguente attenzione

- E' necessario allocare adeguate risorse economiche

- L'adozione di un framework richiede comunque la decisione di investire tempo e risorse da parte del management e, potenzialmente, di sottoporre l'organizzazione ad uno sforzo congiunto non indifferente

- E' necessario comunicare in modo chiaro i propri obiettivi e le priorità

- Il framework dovrebbe comprendere attività di coordinamento e scambi di informazioni con altri operatori del settore e con le istituzioni, anche, ma non

[5] Per approfondimenti si veda Assirevi, cit. Capitolo II, e ENISA Threat Landscape 2023, cit., Annex B

solo, tramite i canali associativi esistenti, le attività convegnistiche e di formazione, incontri finalizzati etc.

In altre parole, oltre alla (ovvia) implementazione e manutenzione di adeguate procedure di sicurezza, sta diventando sempre più evidente la necessità di creare una ***cultura*** e una ***consapevolezza*** sulla cybersecurity, diffusa a tutti i livelli dell'operatore economico, nessuno escluso.

Un criminale può infatti entrare in una rete aziendale in due modi[6]:

- Sfruttando la debolezza delle procedure di sicurezza esistenti (che dovrebbero anche essere strutturate in modo da bloccare danni rivenienti da ingenuità da parte degli utenti, quali l'apertura di un allegato infetto)
- Sfruttando, in un ambiente potenzialmente ben protetto, un unico, apparentemente banale, momento di disattenzione da parte di un utente con permessi di accesso elevati[7]

Inoltre, e questo è un aspetto particolarmente delicato e potenzialmente devastante per il soggetto colpito, in alcuni casi il criminale che è riuscito ad entrare nei sistemi della vittima non procede subito a bloccare gli

[6] La realtà è più complessa, ma ai fini di queste brevi note ci si perdonerà questa semplificazione.
[7] Quando Anonymous dichiarò guerra ai terroristi dell'Isis (#OpISIS) nel 2015, gli hacker del famoso network passavano settimane a monitorare le attività quasi impenetrabili dei terroristi, dandosi il cambio giorno e notte, con l'obiettivo di sfruttare pochi secondi di disattenzione nell'osservanza dei rigidissimi protocolli di utilizzo delle reti e strumenti informatici, per entrare e sferrare il loro attacco. Raramente questo tipo di attenzione viene riservata agli operatori economici, a meno che non siano particolarmente importanti o strategici per fini politici.

stessi e a chiedere il riscatto. Esso invece rimane silente per molto tempo, anche diversi mesi, studiando meglio l'ambiente, se ci riesce anche prendendo possesso e infettando i sistemi di back-up, per poi colpire dopo aver preparato bene il terreno e azzerato le possibilità di risposta e recupero dati da parte del soggetto aggredito.

Per questi motivi, e molti altri che non andiamo a trattare per amor di sintesi, mai come nel caso della sicurezza informatica sono necessarie, oltre a procedure robuste, anche la diffusione di una adeguata cultura e sensibilità in materia e una consapevolezza dei rischi reali.

Entrambi i documenti che abbiamo citato in nota contengono elementi utili e spunti di riflessione interessanti per valutare l'adeguatezza dei propri protocolli di sicurezza per la prevenzione di cyberattacchi e per gli eventuali miglioramenti da apportare.

§ § § § § §

Non esitate a contattarci per qualsiasi approfondimento.

Cordiali saluti,

Aldo Filippini