www.giovannicerrato.it

APPUNTI DI UN CYBERSECURITY MANAGER

Considerazioni sul mondo della Cybersecurity riassunte in 10 frasi

Scritto da Giovanni Cerrato

Abbiamo fatto sempre così

E fino ad ora non è mai successo niente è la conclusione sottintesa di questa frase. Quante volte abbiamo sentito pronunciare queste parole?

In un mondo dove gli attacchi Cyber sono in continuo aumento e dove essi sono diventati più profittevoli del mercato della droga continuare a "**fare così**" vuol dire trascurare un rischio importante.

La Cybersecurity potrebbe essere paragonata al tema **dell'innovazione**. Nelle pubbliche amministrazioni, startup, PMI e grandi aziende al pari dell'innovazione è necessario capire che la Cybersecurity non può essere trascurata.

Senza innovazione molte aziende sono fallite e allo stesso tempo molte aziende a seguito di **data breach** o attacchi **ransomware** sono state costrette a chiudere.

Anche essere compliant alle normative Gdpr, Nis, Dora, Iso 27001 diventa un vantaggio competitivo come allo stesso tempo evitare multe importanti.

Bisogna sdoganare definitivamente il concetto di "abbiamo sempre fatto così" e "innovare".

Non è una questione di “se” ma di “quando”

In un mondo sempre più interconnesso e digitalizzato, affrontare un **Cyberattacco** non è una possibilità remota, ma una certezza.

I criminali sanno bene che un attacco cyber è molto meno rischioso di una rapina. In una rapina, l’aggressore deve essere fisicamente presente, con il rischio di essere catturato. Oltretutto ci sono serie evidenze del reato e prove certe.

Nel **Cyberspazio**, invece, l’attaccante può operare dall'altra parte del mondo, cancellando ogni traccia del suo operato. Scoprirlo non è affatto garantito e, quando accade, spesso è troppo tardi. Basta pensare che secondo il report Mandiant “M-Trends 2024”, il tempo medio di permanenza di un attaccante all’interno di un sistema (il cosiddetto “**dwell time**”) è di circa 10 giorni nel 2023.

Nella sfida tra attaccanti e difensori, questi ultimi sono sempre in una posizione di svantaggio, un concetto noto nel cyberspazio come "asymmetric." Questo significa che le risorse e i costi necessari per lanciare un attacco sono minimi rispetto enormi danni che possono essere inflitti.

Anche i conflitti moderni vedono un ruolo sempre più centrale della cybersecurity. Non a caso, già dal 2016, la **NATO** ha riconosciuto il cyberspazio come il **quinto dominio** di guerra, al pari di aria, terra, mare e spazio. Un attacco informatico potrebbe quindi essere considerato un atto di aggressione, giustificando una risposta difensiva.

È cruciale quindi spostare l'attenzione sul concetto di **post breach**, come già fanno le aziende più blasonate e chiedersi:

- Cosa farò quando accadrà?
- Ho un piano di continuità?
- Il mio piano di backup è efficace?
- Come gestisco gli incidenti?
- Sono preparato a gestire una crisi?

Avere una risposta a queste domande fa la differenza tra chi è in grado di fronteggiare un attacco Cyber e chi sarà destinato al collasso dei sistemi.

Un computer sicuro è un computer non collegato a Internet e chiuso a chiave in una cassaforte

Spesso è difficile far comprendere che **il rischio zero non esiste**. Qualsiasi dispositivo informatico acceso e connesso in rete è esposto a minacce, ed è impensabile chiudere tutte le porte o non esporre alcun servizio.

Una strategia di Cybersecurity efficace deve concentrarsi su tre pilastri:

- Calcolare il rischio
- Gestire il rischio
- Esporre solo lo stretto necessario

Il calcolo del rischio avviene attraverso un **risk assessment**, che funge da base per le decisioni successive.

Le opzioni per la gestione del rischio sono:

- **Eliminazione**: rimuovere il rischio alla radice, come disinstallare un software vulnerabile. Questa strategia, sebbene efficace, può richiedere un grande sforzo o non essere sempre applicabile.

- **Mitigazione**: implementare contromisure appropriate, come l'acquisto di un firewall, l'installazione di patch o la formazione del personale.

- **Accettazione**: in alcuni casi, accettare il rischio è una scelta possibile, ma solo se si è pienamente consapevoli e preparati.

- **Trasferimento**: affidare il rischio a terzi, ad esempio attraverso un'assicurazione Cyber.

La gestione dei rischi richiede una chiara definizione delle priorità. Un errore comune è considerare tutto prioritario, ma **quando tutto è una priorità, nulla lo è davvero**.

La chiave è saper distinguere e focalizzarsi su ciò che conta davvero.

Una cosa l'hai capita se la sai spiegare a tua nonna

Come diceva un mio professore all'Università, **un bravo ingegnere deve rendere facili i concetti difficili**, non il contrario.

In un ruolo **manageriale**, è cruciale saper dialogare con il board e il management per richiedere budget e illustrare strategie e roadmap degli interventi.

Tuttavia, uno degli **errori** più comuni che vedo tra i professionisti della **Cybersecurity** è l'**uso di un linguaggio troppo tecnico**, inadatto a un pubblico manageriale. Parlare di vulnerabilità e tecnicismi invece di concentrarsi sugli impatti economici e sui rischi, temi che interessano maggiormente il board, è un errore frequente.

Adattare il linguaggio e le argomentazioni al proprio pubblico è una delle **soft skill** più apprezzate negli esperti di **cybersecurity**, oltre che nel **public speaking**.

Una comunicazione efficace permette di trasmettere l'importanza della Cybersecurity anche a chi non è del settore, aumentando la consapevolezza e il supporto all'interno dell'azienda.

La sicurezza non è un prodotto ma un processo

Molte aziende pensano che l'acquisto dei migliori firewall, EDR, XDR e delle ultime novità del mercato rappresenti la **strategia di Cybersecurity** ideale, senza rendersi conto di quanto sia essenziale saperle effettivamente utilizzare.

Ho visto **CISO** acquisire i migliori prodotti sul mercato, ma senza dedicare un team all'analisi degli alert di sicurezza.

Strategie e processi di cybersecurity inefficaci non solo sprecano **budget** preziosi, ma rischiano anche di esporci, dopo un **breach**, a difficili confronti con il board. Infatti certamente sarà necessario giustificare scelte inadeguate nonostante l'importante investimento fatto.

Adottare soluzioni senza sapere come usarle o configurarle può risultare persino pericoloso, creando una **falsa sensazione di sicurezza**.

Spesso ho assistito ad aziende con firewall di brand rinomati ma con poche regole di firewalling e controllo del traffico.

Ho visto CISO affascinati dall'intelligenza artificiale senza avere procedure di gestione degli incidenti o un SOC dotato di playbook efficienti.
Ricordiamoci: **concentrarsi sul processo è l'arma vincente**.

Non puoi proteggere ciò che non sai di avere

In tutti gli standard di Cybersecurity, l'**asset inventory** è un pilastro fondamentale. Senza un inventario preciso degli asset, definire una strategia di protezione efficace diventa una sfida insormontabile.

Non basta sapere quali asset possiedi è altrettanto essenziale comprendere come questi siano interconnessi. Prima o poi un attacco si verificherà (ricordiamo: non è una questione di "se", ma di "quando"), e il Business Continuity manager deve conoscere i **processi aziendali critici** e gli asset che li supportano.

Il team di Cybersecurity deve avere una visione chiara degli asset più importanti per poter applicare ad essi una politica di difesa avanzata.

La **mappatura delle comunicazioni** deve rendere possibile intercettare prontamente un sistema che comunica per la prima volta con una nuova macchina: questo è un segnale di allarme importante.

Il Business Continuity manager e il team Cyber devono capire l'impatto che produce l'isolamento di un sistema infetto su tutto il contesto.

L'**asset inventory** deve essere **aggiornato e dinamico**, non statico. Utilizzare fogli Excel non è sufficiente per tenere traccia degli asset in modo efficace.

In sostanza, **non puoi gestire né proteggere ciò che non conosci.**

Se conosci il nemico e conosci te stesso, nemmeno in cento battaglie ti troverai in pericolo

"Se conosci te stesso, ma non il nemico, per ogni vittoria ottenuta subirai anche una sconfitta. Se non conosci te stesso né il nemico, soccomberai in ogni battaglia." – **Sun Tsu**.

Sono un grande fan di Sun Tsu e questa citazione racchiude perfettamente l'essenza della Cybersecurity.

Un bravo **CISO o Cybersecurity Manager** deve avere una profonda conoscenza delle minacce Cyber, ma il vero valore aggiunto per l'azienda viene dalla capacità di contestualizzarle in base all'ambiente, alla cultura, alla maturità e al settore merceologico specifico.

I rischi per una banca sono diversi da quelli per un'azienda nel retail, nel farmaceutico o nella produzione, così come la maturità e la preparazione del personale.

Le risorse economiche, le competenze e il grado di maturità variano notevolmente tra startup, PMI e grandi imprese.

La strategia cambia se i sistemi da proteggere sono prevalentemente in cloud, on-premises o in modalità ibrida

Proteggersi da tutti i rischi con risorse limitate è impossibile, la chiave è stabilire le giuste priorità.

La strategia vincente non consiste nell'adottare tutte le tecnologie più quotate nel Magic Quadrant di Gartner. **La vera sfida è creare un'armonia tra tecnologie, rischi, maturità, budget e competenze specifiche dell'ambiente che si deve proteggere.**

Simplicity is the key to security

Uno dei concetti più sottovalutati nella Cybersecurity è la semplicità. **Aggiungere complessità porta a carenze che lasciano spazio ai criminali informatici.**

Semplicità vuol dire adottare buone norme che riducono drasticamente i rischi.

- **Eliminare i servizi obsoleti** o dismessi per ridurre la superficie di attacco. Sembra ovvio, ma quando eseguivo i penetration test spesso trovavo vecchie versioni di API con bug di sicurezza ancora esposti e non più utilizzati.

- **Adottare il principio del "least-privilege"**: concedere agli utenti solo i privilegi necessari per svolgere i loro compiti. Non avete idea di quanti account amministrativi siano usati per compiti basilari.

- **Bloccare le utenze inutilizzate** da tempo.

La semplicità si applica anche alla scelta delle tecnologie. Avere alert e log su un'unica piattaforma o dotarsi di una soluzione unica per cercare vulnerabilità su tutti gli asset è fondamentale.

Un sistema complesso da gestire si traduce in maggiori possibilità di subire breach. Ogni elemento o permesso elevato dimenticato aumenta la superficie di attacco.

Ricordiamoci: **la semplicità è la chiave per una Cybersecurity efficace.**

Our key to success is knowing that network better than the people who set it up

Rob Joyce, dopo la sua esperienza alla **NSA** (National Security Agency), ha svelato particolari interessanti in una presentazione illuminante dal titolo NSA's six-phase plan for "targeted intrusions" (e.g. hacking a nation state's network).

Le frasi più incisive del suo discorso sono state: "**Our key to success is knowing that network better than the people who set it up" e "We need that first crack and we'll look to find it**."

Rob ha illustrato come l'NSA, per penetrare in un sistema target, si metta nelle condizioni di conoscerlo meglio di chi l'ha configurato, identificando servizi e vulnerabilità trascurate.

Ho sperimentato personalmente questo concetto in numerosi **vulnerability assessment**, durante i quali ho rivelato al committente l'esistenza di macchine e servizi vulnerabili di cui non erano a conoscenza o che pensavano fossero già dismessi.

Data la complessità dei sistemi attuali, un'accurata **verifica continua dei servizi**, degli asset e delle vulnerabilità diventa essenziale. Se non lo fai tu, lo farà un malintenzionato (e non sarà piacevole).

Conoscere a fondo la propria rete è la chiave per prevenire intrusioni e proteggere efficacemente l'azienda.