Intervista a Marco Castaldo, Amministratore Delegato di CSE-Cybsec

Due chiacchiere un'azienda italiana di eccellenza 'nel campo della cybersecurity.

In questo Blog, sempre più spesso affrontiamo temi legati all'evoluzione del "cyberspazio", e nel mio penultimo libro "Il sex appeal dei corpi digitali" pongo l'accento sui pericoli – anche per la salute del nostro organismo – di un abuso degli strumenti digitali nella nostra vita quotidiana. Di pari passo con lo sviluppo del digitale, cresce sempre di più la portata delle minacce cibernetiche, alla sicurezza di dati e infrastrutture tecnologiche, militari e statuali, ma anche aziendali e private. Nel 2017 si è costituita – fusione di precedenti esperienze professionali di eccellenza – un'azienda al 100% italiana nel campo della cyber security: Cybsec S.p.A, che inaugurerà mercoledì 24 a Roma la sua nuova sede. Ho intervistato in anteprima Marco Castaldo, Amministratore Delegato di Cybsec.

Dott. Castaldo innanzitutto, cos’è la Cyber Security, nella vostra visione?

Grazie per questa domanda solo apparentemente scontata. L’innovazione e la digitalizzazione sono elementi sempre più indispensabili per l’esistenza stessa di un’impresa: ricerche di grandi società di consulenza, come The Boston Consulting Group, mostrano numeri alla mano che le aziende più innovative e più digitalizzate sono quelle che hanno annualmente maggiori incrementi di produttività, di profitti e di quote di mercato, quelle meno innovative sono a rischio di espulsione dal mercato.
Ma, c’è un ma: il web è stato costruito pensando alla connessione e non alla sicurezza; assicura dunque i vantaggi imprescindibili dell’immediatezza e orizzontalità, che qualche anno fa erano impossibile anche soltanto immaginare, ma comporta anche dei rischi che vanno affrontati e ridotti ad un livello accettabile, dotandosi di strumenti efficaci di difesa cibernetica ed implementando “una cultura della sicurezza” all’interno delle organizzazioni e delle aziende.
Per usare una metafora: è come se grazie allo sviluppo della tecnologia digitale avessimo costruito negli ultimi dieci anni automobili che rispetto alle precedenti vanno dieci volte più veloci e consumano dieci volte di meno, dimenticando però di dotarle di un airbag speciale e di freni al titanio, che a certe velocità fanno la differenza tra il salvarsi la vita oppure no in caso di incidenti.

Non stiamo quindi parlando di ambiti squisitamente tecnologici, “cose da ingegneri e programmatori”, insomma…

Esatto: ***la cyber security ha un ineludibile aspetto tecnologico; ma non si esaurisce in esso.*** *In Cybsec riteniamo infatti che per difendere i propri sistemi digitali – ma meglio sarebbe dire i propri asset patrimoniali più*

strategici – e incrementare i vantaggi della digitalizzazione si debba adottare, implementare ed aggiornare in continuazione soluzioni e strumenti capaci di prevenire e/o resistere efficacemente ad attacchi informatici. IL focus è proprio su questo: sulla protezione degli asset e dei "valori" delle aziende.

Questo è un elemento distintivo rispetto alla concorrenza. Ve ne sono altri?

Possiamo dire che il nostro approccio – conformemente al pensiero del nostro CTO, Pier Luigi Paganini: uno dei massimi esperti in campo internazionale nel settore – è quello di una strategia *di security che parte da due poli: il punto di vista del vertice operativo del cliente sugli asset critici da proteggere e sugli obiettivi di sviluppo dell'organizzazione, e il punto di vista dell'attaccante, che mira ad abbattere le difese per motivi legati al profitto criminale, ad interessi politici – sempre più spesso geo-politici – o a visioni ideologiche estreme ed anti-sistema. Ci caratterizziamo quindi* ***per*** *un servizio "chiavi in mano" – di tipo tecnologico, ma anche legale, assicurativo e di formazione – che non è mai modellato su "soluzioni standard".*

La società in questi primi mesi ha stipulato "alleanze"?

Abbiamo lanciato un progetto di ricerca congiunto con l'Università del Sannio, considerata un'eccellenza nel campo della cyber security e focalizzato sull'uso del machine learning e dell'intelligenza artificiale per l'implementazione di strumenti di difesa cibernetica; abbiamo sottoscritto un contratto di partnership con uno dei più affermati Studi legali dello Stato di Israele, consociato con una primaria società di Venture Capital specializzata in particolare sul finanziamento di start up nel settore della

Cyber Security. Oggetto del mandato, è lo scouting di start-up d'eccellenza, in particolare con focus sulle soluzioni per la GDPR (General Data Protection Regulation), Threat Intelligence e soluzioni per i SOC – Security Operation Center, per poi lanciare partnership finalizzate a veicolare sul mercato italiano le specifiche soluzioni, con marchio CSE. Inoltre, abbiamo promosso e contrattualizzato sin dalla partenza alleanze operative con tre brand internazionali: Orrick Legal, Grant Thorton Consulting, e NTT Data. Abbiamo inoltre costituito un ***Malware Analys Lab – dal nome "Zlab" –*** *per la scoperta e l'analisi dei malware di nuova generazione, con analisti di altissima specializzazione, che sta rapidamente imponendosi all'attenzione della comunità internazionale della cyber security. É a firma dello ZIab la pubblicazione di una immediata analisi preliminare del malware BAD RABBIT che ha creato scompiglio a livello internazionale, uscendo, primi al mondo, in contemporanea con il colosso internazionale Kaspersky, analisi che è stata subito ripresa e rimbalzata sui social come Twitter e sui siti specializzati a livello internazionale.*

In qualche misura, voi specialisti in Cyber Security "prevedete il futuro": una costante pratica di simulazione di scenario per mitigare i rischi. Partendo da questa metafora, cosa vede in prospettiva, nel prossimo periodo, nello scenario degli attacchi cyber a livello internazionale?

Le rispondo così: tentare di "prevedere scenari futuri" è parte intrinseca della natura umana, anzi, forse ne è la principale caratteristica distintiva. Ma quella che stiamo vivendo in questo appassionante dominio è una condizione del tutto "innaturale": ci sforziamo di fare previsioni ma siamo smentiti dai fatti in tempo reale. Tutto l'impegno profuso dalle migliori "menti tecnologiche" nello sviluppare il mondo digitale che ci circonda – in qualsiasi campo, dalla scienza al marketing, dalla medicina all'istruzione, dalla produzione

al risparmio energetico, dalla riduzione dell'analfabetismo alla diffusione della democrazia – ha il suo opposto nello sviluppo di nuove capacità di attacco da parte dei "cattivi", i quali– ricordiamolo – hanno dalla loro due enormi vantaggi strategici: da un lato una superficie attaccabile che si allarga a dismisura – mentre scrivo ci sono lanci di agenzia che parlano della minaccia alla rete mondiale del malware Okiru di cui il nostro Chief Technology Officer Pierluigi Paganini è stato il primo al mondo a dare l'allarme, insieme ad un'altra figura di riferimento mondiale dell'arena degli hacker etici, Odisseus – e dall'altro la possibilità di scegliere in totale autonomia il momento in cui attaccare. Senza dimenticare il bassissimo livello di rischio personale, stante la difficoltà da parte delle vittime di un attacco di poter riconoscere con precisione e senza dubbio i responsabili dell'attacco.
La strada maestra per difendersi è quindi "fare sistema": occorre un cambiamento culturale radicale che ci convinca a mettere il problema della sicurezza cibernetica ai primi posti delle nostre priorità, con la conseguente necessaria spinta verso un processo urgente di innovazione tecnologico, organizzativo, legislativo, finanche militare, a un livello sicuramente sovranazionale.
Noi nel nostro quotidiano come ho detto mettiamo in campo competenze eccellenti, facciamo progetti di ricerca, importiamo tecnologie all'avanguardia dai paesi più avanzati in cyber security; mettiamo tutto il nostro impegno nella difesa del paese, delle sue strutture critiche e degli asset patrimoniali delle imprese pubbliche e private.