Axitea: la sicurezza da fisica a digitale in un mondo che cambia

https://www.hwupgrade.it/i/n/axitea.logo.720.jpg,

Abbiamo intervistato Marco Bavazzano, amministratore delegato di Axitea, realtà italiana che offre servizi di sicurezza sia fisica che digitale: una prospettiva unica nel panorama europeo

di Riccardo Robecchi pubblicata il **27 Giugno 2022**, alle **17:01** nel canale Security

axiteaCloud Security

Axitea è una realtà unica non solo nel panorama italiano, ma anche in quello europeo: si occupa infatti sia della sicurezza fisica, sia di quella digitale delle aziende sue clienti. Un approccio che le dà una prospettiva incomparabile sullo stato della sicurezza, in senso generale, e di come il mondo stia cambiando e stia diventando sempre più strettamente legato alla componente digitale. Abbiamo parlato di questo e altro con **Marco Bavazzano**, amministratore delegato di Axitea e principale promotore del cambiamento aziendale che l'ha portata a occuparsi anche di sicurezza cyber.

Axitea: dalla difesa della sicurezza fisica a quella digitale

"Nel DNA della nostra azienda c'era la capacità di gestire il rischio delle intrusioni fisiche, quindi per noi è stata quasi

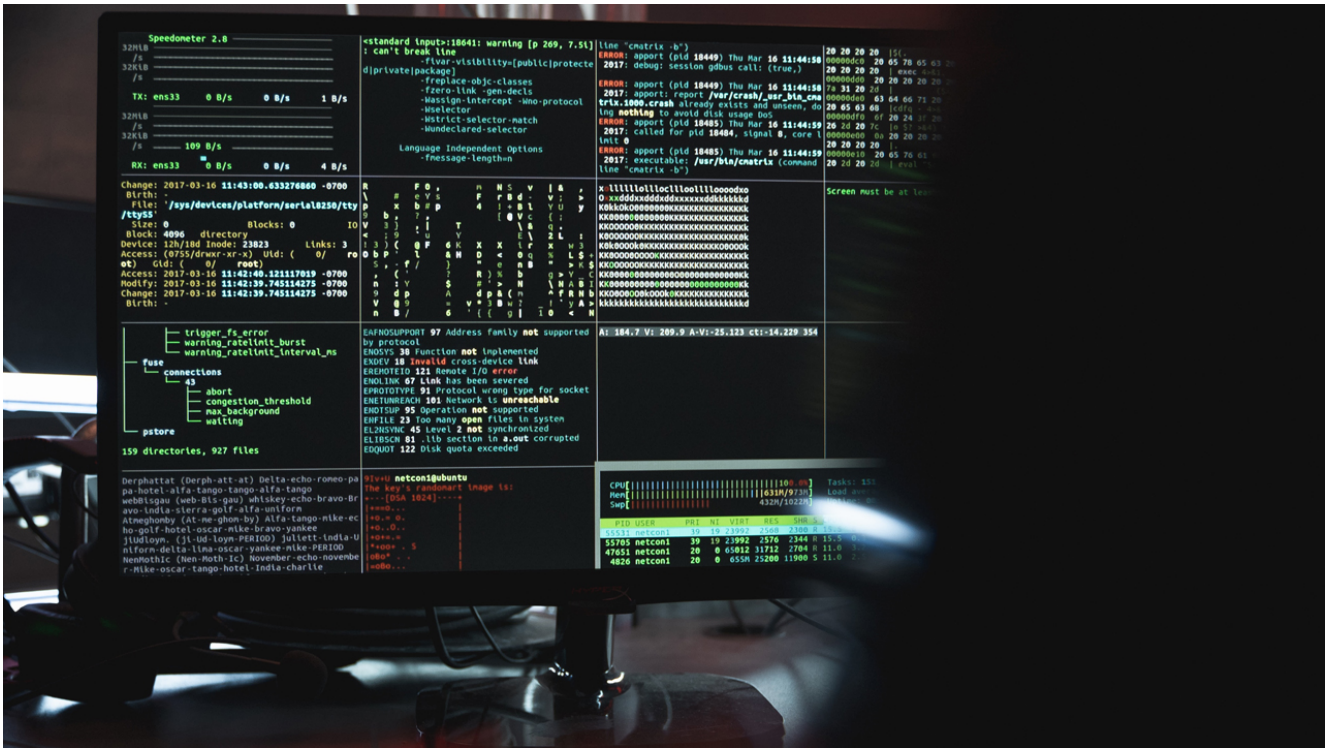
una naturale evoluzione quella di seguire l'evoluzione del rischio delle aziende nostre clienti che, a seguito del processo di trasformazione digitale, si esponevano sempre più anche a rischi di intrusione digitale, oltre che fisica", ci dice Bavazzano (in foto). *"In questo senso abbiamo trovato naturale sviluppare le competenze necessarie per continuare a supportare le aziende nella gestione del rischio che man mano andava ad assumere sfumature e connotazioni diverse e più ampie rispetto alla situazione storica."*

"Quello che abbiamo fatto di importante è che non abbiamo semplicemente stretto una partnership con aziende del settore informatico, andando a realizzare un'offerta commerciale integrata, ma abbiamo sviluppato internamente le competenze necessarie per supportare le aziende anche nella gestione del rischio informatico. Abbiamo ampliato l'organico con nuove assunzioni, perché chiaramente queste competenze specializzate erano e sono molto distinte rispetto a quelle che avevamo già all'interno dell'azienda. Su alcune figure professionali abbiamo inoltre erogato formazione ad hoc per implare e sviluppare le conoscenze di questo nuovo settore: i nostri venditori hanno da sempre avuto un'alta capacità consulenziale orientata al rischio fisico, ma con l'introduzione di nuovi servizi di sicurezza informatica, era necessario insegnare loro un approccio di tipo consulenziale nella gestione del rischio digitale. Abbiamo inoltre creato una struttura di pre-sales *che, con competenze specialistiche, supporta i venditori nella presentazione e proposizione dell'offerta a clienti e* prospect*."*

"Questo nostro posizionamento è unico non soltanto in Italia, ma anche in Europa, perché [quella dal fisico al digitale] è una transizione difficile; questa evoluzione è abbastanza complessa perché, come tutti i programmi di trasformazione, necessita di un impegno fortissimo dall'alto, ma è un problema anche di cultura. Le aziende che provengono dal mondo della

sicurezza fisica non hanno, in linea di massima, la cultura necessaria ad affrontare i temi del digitale; noi ci siamo riusciti perché, nell'immissione di questo nuovo capitale umano, abbiamo curato anche l'ingresso di molte persone provenienti dal mondo ICT e, quindi, l'azienda ha vissuto una trasformazione molto profonda perché la sua cultura è stata pervasa da competenze digitali. Axitea è diventata essa stessa un'azienda digitale con processi resi molto efficienti dall'utilizzo delle tecnologie digitali. Questa trasformazione interna è stata molto importante per effettuare la trasformazione del nostro modello di business e della nostra offerta, e quindi avere successo; siamo unici perché è un percorso molto più difficile e forse è questo che ci dà un vantaggio competitivo. Altri ci seguiranno magari, ma ci stanno mettendo del tempo per arrivare [al nostro punto].”

Quanta consapevolezza c'è dei rischi legati al digitale?



La sicurezza fisica appare, almeno dall'esterno, come un ambito ben noto e ben compreso alle aziende, mentre quella cyber è ancora un campo in cui mancano consapevolezza e competenze. Ma dal punto di vista di Axitea è davvero così?

"Sull'ambito della sicurezza fisica c'è una consapevolezza abbastanza diffusa di quelli che possono essere i rischi; c'è però una sempre maggiore attenzione a preferire soluzioni di tipo tecnologico. Le aziende hanno capito che le soluzioni tecnologiche in molti contesti sono più efficaci rispetto a quello che può essere l'intervento umano e, quindi, troviamo sempre più aziende che magari cercano Axitea per la capacità di fornire loro, in sostituzione di un servizio di 'guardiania' con personale armato, un servizio di videosorveglianza basato su algoritmi di videoanalisi con l'intelligenza artificiale, che rendono i sistemi di allarme molto efficaci perché arrivano quasi a eliminare qualsiasi falso positivo. I clienti di solito sono già a conoscenza dei rischi in ambito fisico e capiscono il valore delle tecnologie avanzate", ci conferma Bavazzano.

"Nell'ambito della sicurezza informatica la situazione è un po' diversa. La consapevolezza sta crescendo, ma non è ancora sviluppata in modo adeguato; questo è però un tema sociale, non riguarda soltanto le aziende ma, in generale, un po' tutta la nostra società. Una delle attività su cui ci siamo impegnati fin dall'inizio è rendere più consapevoli le aziende rispetto ai rischi derivanti da un'esposizione digitale, dal fatto dunque di avere degli asset *digitali esposti a minacce provenienti da Internet e non solo. Si assiste a un momento di consapevolezza in questo ambito a seguito del fatto che il numero di attacchi è diventato così cospicuo, e la pubblicazione sui media di notizie relative a questa situazione è diventata così frequente, che le aziende si sono rese conto del problema."*

“Permane l’atteggiamento di molte aziende secondo cui i problemi riguardano solo le grandi aziende o specifici settori; resta dunque molta ignoranza da questo punto di vista, perché tutti siamo esposti alle minacce informatiche. Banalmente, il fatto che il conflitto tra Russia e Ucraina si sia aperto a questa componente cyber, sebbene tale componente non sia stata utilizzata in modo massiccio fino a questo momento, con attacchi da parte della Russia nei confronti dell’Ucraina e viceversa, in realtà ha aumentato il livello di rischio di tutte le aziende nel mondo. Entrambe le nazioni hanno operato per indebolire l’altra fazione, hanno usato armi cyber che non hanno una limitazione territoriale e hanno dunque iniziato a diffondersi in tutto il mondo aumentando il livello di rischio di tutte le aziende.”

Qual è la relazione tra il mondo della sicurezza fisica e della sicurezza informatica?

“Nel momento in cui assistiamo alla digitalizzazione delle imprese, ad esempio con il programma Industria 4.0 che ha avuto molto successo nell’introdurre sistemi informativi in ambienti che erano magari gestiti soltanto con sistemi elettronici di vecchia generazione, il fisico ha cominciato a essere invaso dall’informatica e sta cominciando a rendersi conto, a seguito della diffusione delle minacce cyber, del fatto che questa contaminazione, che è stata ed è augurabile per moltissimi motivi, a partire dall’aumento dell’efficienza e dell’efficacia produttiva di tutte le aziende, pone comunque le aziende di fronte a nuovi rischi. La consapevolezza sta maturando, ma non è ancora sufficientemente elevata. Basti pensare che il Paese sta ancora facendo i suoi primi passi nella definizione e implementazione di una strategia per la gestione della cybersicurezza. Abbiamo visto proprio di recente la pubblicazione di un decreto che contiene i principi e le linee guida della strategia per la gestione della cybersicurezza nel nostro Paese, quindi le aziende devono

acquisirli e farli propri.”

Qual è la situazione italiana sulla cybersicurezza?

La Francia ha stabilito la sua agenzia per la cybersicurezza nel 2009. La fondazione di quella italiana e lo stanziamento di ingenti fondi tramite il PNRR cambieranno la situazione verso il meglio per il nostro Paese o dovranno esserci ancora cambiamenti significativi?

“Stiamo sicuramente andando nella direzione giusta, ma come fate notare ci stiamo muovendo in forte ritardo rispetto ad altri Paesi. Anche il Regno Unito si era mosso con largo anticipo, nel 2005 o 2006 aveva già annunciato stanziamenti nell’ordine dei 650 milioni di sterline, mentre noi stiamo ancora implementando i dettami che sono arrivati dall’Europa nel 2013. Ci vorrà molto tempo: poco fa è stato rilasciato il piano strategico e, come dice il nome stesso, è un qualcosa di

alto livello. Il percorso per arrivare ad avere un'implementazione efficace delle linee guida fondamentali per la sicurezza informatica delle nostre aziende e dei servizi essenziali per il Paese è, quindi, ancora lungo. C'è anche un tema di cultura digitale dei cittadini, quindi bisognerà promuovere iniziative per aumentare tale livello. Siamo un Paese che ha bisogno di crescere su un tema di fondamentale importanza per il futuro, ma oggi siamo ancora immaturi. La strada è segnata e sicuramente è quella giusta, quindi speriamo di poterla percorrere nei tempi più rapidi possibili. Le risorse che si è deciso di destinare a questo tema sono significative, ma solo adesso si è preso questa decisione; speriamo che non ci siano ripensamenti, ma non credo ciò succederà mai perché sarebbe troppo grave."

Parlando dell'offerta di Axitea, com'è strutturata e come si differenzia per quanto riguarda la cybersicurezza?

"Crediamo che, a differenza della grande molteplicità di realtà sul mercato, il ruolo di un fornitore di soluzioni di sicurezza non è quello di suggerire a un'azienda l'acquisto di un prodotto al posto di un altro, perché non è un prodotto che permette di affrontare al meglio il tema della cybersicurezza. È un tema molto complesso da gestire e richiede che ciascuna azienda metta in piedi processi, organizzazioni e tecnologie per averne una gestione adeguata. Chiaramente, a seconda della dimensione dell'azienda, questi processi e queste organizzazioni avranno un modello più o meno articolato o snello, ma di certo non esiste un prodotto che è migliore di tutti e che si risolve tutti i problemi che si possono avere su questo frangente. Anche se c'è una moltitudine di produttori che cercano di far credere esattamente questo alle aziende, con attività di marketing ben organizzate: con questo prodotto metti in salvo i tuoi dati, annulli la tua esposizione al rischio, sei in salvo dai ransomware eccetera. Non è assolutamente così."

“L’approccio di Axitea è di tipo consulenziale e cerca di costruire in modo sartoriale la soluzione giusta per ciascuna azienda. Non andiamo a reinventare la ruota ogni volta, perché le aziende si assomigliano tutte e hanno molte esigenze similari, ma ogni volta andiamo a “fare il vestito su misura”. Costruiamo quindi un servizio che è quello più adeguato per la gestione del rischio di quell’azienda, considerando l’estensione del sistema informativo, e il tipo di servizi che vengono utilizzati sia nei confronti dei clienti sia internamente. Si fa quindi una valutazione a 360 gradi di quella che in gergo è definita la security posture *dell’azienda e andiamo a supportare l’azienda con i nostri servizi nella definizione e implementazione di quei processi, di quei modelli organizzativi che sono necessari per gestire al meglio questo rischio.”*

A chi si rivolge Axitea nello specifico?

“Ci rivolgiamo a tutto il mercato aziendale, focalizzandoci in modo prevalente sulle piccole e medie aziende, ma seguiamo anche alcune grandi aziende. C’è da dire che molto spesso i security manager *di una grande azienda si rivolgono ai grandi attori del mercato non perché possano offrire un servizio o una consulenza migliori dei nostri, ma perché questo li tutela nei confronti dei propri stakeholder. Anche questo fa parte di una cultura che è necessario cambiare, perché è poi la cultura che ha portato alle situazioni gravissime che conosciamo del blocco dei sistemi informativi della Regione Lazio, di molti ospedali della Regione Lombardia e così via. Le cose erano state fatte bene? No, però era stato chiesto di farle a quell’azienda che è il* top *nel panorama mondiale. È una cultura sbagliata in cui non c’è la capacità di assumersi delle responsabilità e si dimostra più la capacità di trovare da subito una via d’uscita a quelli che potrebbero essere i propri problemi, anziché risolvere i problemi dell’azienda.”*

Read More