

SOC 4.0: la cyber security al centro dell'innovazione

Le aziende si trovano oggi di fronte a una nuova era: solo gli imprenditori che sapranno cogliere le opportunità della Digital Transformation, potranno rendere più competitivo il loro business. Questo nuovo scenario vede, accanto a minacce informatiche che già conosciamo, la l'emergere di nuove tecniche di attacco alla sicurezza. Esempari sono stati gli attacchi DDoS che hanno utilizzato il malware Mirai, sfruttando la vulnerabilità di webcam prodotte da un'azienda cinese; questo evento ha aperto scenari inattesi, rendendo necessari parametri di sicurezza nettamente superiori per dimensioni e portata.

Protagonisti di questi attacchi i dispositivi IoT, device che realizzano la prospettiva di un mondo interconnesso, spesso protetti solo da semplici password predefinite, offrendo ai criminali informatici un facile accesso alle reti hardware e software di pubblici uffici, fabbriche e altre infrastrutture potenzialmente sensibili. La trasformazione digitale dei sistemi produttivi e di comunicazione, di cui siamo oggi al big bang con 6 miliardi di dispositivi connessi e una prospettiva per il 2020 di 25 miliardi, presta il fianco alla criminalità informatica, che cerca di coglierne gli aspetti di vulnerabilità. I ransomware, che hanno caratterizzato il 2016 per incidenza e continua evoluzione, prenderanno di mira nel corso del nuovo anno anche l'IoT.

Tra gli obiettivi dei cyber criminali ci sono i dati delle aziende e delle istituzioni, oltre che delle persone, perché si possono rivendere o perché forniscono accesso a ulteriori informazioni.

Gli attacchi sono sempre più pervasivi, pronti a sfruttare qualsiasi dispositivo, tanto che la necessità per le aziende di studiare la propria difesa è divenuta un imperativo.



LA SICUREZZA È UN ASPETTO FONDAMENTALE DELL'INNOVATION JOURNEY CHE VAR GROUP PROPONE ALLE AZIENDE

Per maggiori informazioni: www.vargroup.it/cybersecurity

Cyber security: non solo questione di tecnologia, ma di scelte strategiche

L'apertura verso la connessione alle reti di un numero sempre crescente di persone, cose e dispositivi e l'introduzione nelle reti aziendali di un numero sempre maggiore di dati provenienti da diversi dispositivi, favorisce l'emergere di sempre nuove vulnerabilità per far fronte alle quali è richiesto un approccio alla sicurezza sempre più sofisticato.

“Siamo di fronte ad un momento evolutivo importante, fatto di innovazione nei modelli di business, che richiede capacità di rivedere il modo di presentarsi sul mercato” spiega Francesca Moriani, Amministratore delegato di Var Group, partner per l'innovazione delle imprese da oltre 40 anni. “Per questo la sicurezza è un aspetto fondamentale dell'Innovation Journey che noi proponiamo alle aziende con le quali lavoriamo quotidianamente”.



Var Group ha ripensando in ottica completamente nuova la propria offerta per le aziende dei settori Automotive, Retail, Fashion, Furniture, Mechanics, Food, Wine e Paper, rendendo più efficienti i processi anche grazie all'integrazione progetti di Internet of things, realtà virtuale, realtà aumentata, visual sharing, wearable device, 3D printing, big data e predictive, smart working e droni, solo per citarne alcuni. In questo approccio solo una corretta strategia di security può essere funzionale: ecco perché dal 2014 Var Group è entrata nella compagine sociale di Yarix, azienda leader nel settore della sicurezza informatica. Insieme hanno sviluppato *Var Shield*, un'offerta unica in Italia, un unico servizio che riunisce soluzioni, consulenza, le tecnologie e le infrastrutture più evolute, per offrire alle aziende la gestione della security in completo outsourcing. Erogato in modalità hybrid cloud, *Var Shield* permette agli imprenditori di affidarsi ad un partner competente, concentrandosi così sul proprio core business.

Rientra nel servizio anche il SOC (Security Operation Center), basato su tecnologia IBM QRadar, che già alla fine del 2014 Var Group ha avviato insieme a Yarix. Un centro all'avanguardia, presidiato h24x365, per fornire un approccio olistico ed esaustivo in tema di sicurezza informatica, business continuity e disaster recovery. Centro di competenza per la security, Var Group, grazie alle competenze sviluppate dal team Yarix, è l'unica azienda privata in Italia ad essere membro del FIRST, prestigioso organismo internazionale che riunisce i CERT (Computer Emergency Response Team) più importanti al mondo, come quelli di Apple, di Google e della Nasa, per la risposta agli incidenti informatici e la condivisione in tempo reale di informazioni.

Una partnership internazionale per un SOC 4.0

Esperienza pluriennale, competenza e ricerca sono alla base dell'innovativo e pionieristico progetto di SOC 4.0 e di una partnership italo-israeliana che mette in campo l'impegno di Var Group con ricercatori delle università italiane ed esperti delle aziende israeliane più innovative. "Si tratta di una task force internazionale che consentirà di realizzare il primo SOC 4.0, una struttura capace di monitorare, rilevare e rispondere agli attacchi informatici di nuova generazione, quelli che transitano per i dispositivi IoT (Internet of Things) e i sistemi informatici SCADA, sempre più usati per il controllo dei sistemi fisici di produzione nelle fabbriche e nelle infrastrutture strategiche", racconta Mirko Gatto, Direttore Divisione Cyber Var Group.

Strategie altamente innovative a cui si è giunti attraverso un percorso evolutivo fondato sulla security intelligence, ovvero soluzioni capaci di collezionare e analizzare in tempo reale enormi quantità di flussi informativi in ingresso e in uscita dal perimetro di rete, individuando prontamente la minacce ad alto rischio provenienti sia dall'esterno che dall'interno, per una sempre più efficace strategia di difesa. Precursori in questo campo sono le soluzioni di IBM, di cui Var Group è Premier Business Partner. La soluzione IBM QRadar SIEM si basa sulle competenze all'avanguardia e sull'intelligence fornita dal team di ricerca IBM X-Force per fornire un approccio preventivo alla sicurezza. IBM X-Force Exchange, completa-



mente integrata nella soluzione IBM QRadar SIEM è la piattaforma di collaborazione di IBM Security, il cui contenuto è costantemente e tempestivamente aggiornato dai ricercatori di IBM sulle più recenti ed evolute minacce alla sicurezza, ed è fruibile dalle aziende per proteggersi in modo tempestivo dai cyber attacchi.

La costante ricerca è alla base dell'evoluzione e delle potenzialità straordinarie di IBM Watson, il sistema cognitivo che offre soluzioni applicabili in diversi ambiti, come l'analisi del traffico stradale o l'utilizzo nel settore medico-sanitario, incluso l'importantissimo apporto nel monitoraggio della sicurezza informatica. Watson che agisce a supporto dell'operatore di sicurezza analizza il traffico di dati in tempo reale e identifica potenziali situazioni anomale, andando a eseguire ricerche massive su web e deepweb. Un supporto dunque che risulta di grande efficacia nella fase di riconoscimento degli attacchi, abbattendo in modo consistente il tempo necessario ad operatori umani per eseguire le stesse ricerche. Il valore cognitivo di IBM Watson può supportare l'operatività degli analisti di sicurezza, rendendo loro disponibili in poco tempo informazioni. E, si sa, quando c'è un attacco in corso ogni secondo è prezioso.