IMQ INTUITY VERIFICA LA REALE PROTEZIONE DEI PROGETTI E DEL KNOW HOW DI ASKOLL

Askoll

Askoll è un'azienda che, da oltre, quarant'anni, è leader nella tecnologia dei motori elettrici sincroni ad alta efficienza energetica. Progetta e produce pompe, motori e circolatori per il settore dell'elettrodomestico e dell'acquariologia.

Dal 2015, dopo 3 anni di ricerca, Askoll ha deciso di utilizzare la sua esperienza e le sue competenze per intraprendere una nuova sfida ed entrare nel settore della mobilità sostenibile, progettando biciclette a pedalata assistita e scooter elettrici. Questi ultimi sono i più venduti in Italia.

Oggi Askoll Group è un gruppo internazionale con sede a Dueville, che comprende 11 società tra Italia, Slovacchia, Romania, Brasile, Messico, Cina ed è titolare di numerosi brevetti e marchi nazionali, comunitari o internazionali.

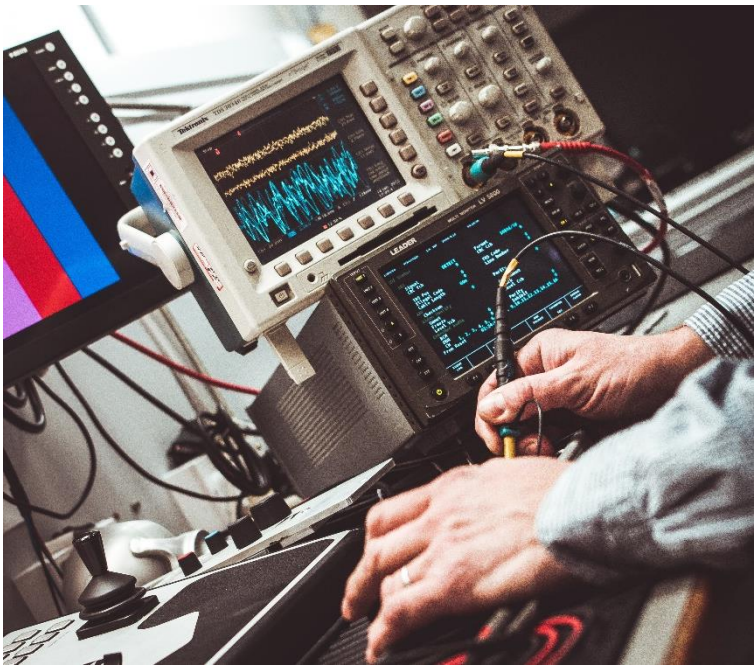
Il suo obiettivo è quello di progettare prodotti sempre più all'avanguardia, mirando all'efficienza energetica, ai bassi consumi ed al risparmio delle materie prime nel rispetto dell'ambiente.

(*http://www.askoll.com/it/index.aspx*)

NECESSITÀ DI ASKOLL

La necessità di un'azienda come Askoll, che fonda il suo business sulla continua ricerca e innovazione, è di custodire e di salvaguardare il proprio know-how, sul quale l'azienda investe ogni anno moltissimo in termini di tempo e risorse, sia economiche che umane.

In tale contesto è essenziale tutelare in ogni modo possibile il know-how acquisito, consapevoli che quest'ultimo rappresenta il vero valore aggiunto per il futuro dell'azienda.



"VISTA L'IMPORTANZA STRATEGICA PER ASKOLL DEI SUOI PROGETTI, VOLEVAMO ESSERE CERTI CHE QUANTO FINORA IMPLEMENTATO, IN TERMINI DI PROTEZIONE DELLE INFORMAZIONI, FOSSE REALMENTE EFFICACIE NEL DIFENDERE IL BUSINESS DELL'AZIENDA DA UN POTENZIALE ATTACCO INFORMATICO ED EVENTUALMENTE IDENTIFICARE I PUNTI PIÙ CRITICI.

CI SIAMO AFFIDATI AD INTUITY IN QUANTO IL SUO APPROCCIO ALLA CYBERSECURITY, DIVERSO RISPETTO A QUELLO PROPOSTO DA ALTRE AZIENDE DEL SETTORE, BEN RISPONDEVA AL NOSTRO OBIETTIVO".

MORENO PANETTO,
IT SYSTEMS MANAGER DI ASKOLL

LA SOLUZIONE: INTUITY RED TEAM

Il servizio di Red Team proposto ad Askoll da IMQ Intuity simula a tutti gli effetti un attacco informatico, permettendo di capire come un potenziale furto industriale potrebbe avere esito positivo e attraverso quali vettori: vulnerabilità tecnologiche e/o imputabili al fattore umano.

Il servizio IMQ Intuity Red Team combina attività di Infrastructure Attack con altre di Social Engineering e di Physical Attack, al fine di conoscere come l'azienda sia in grado di reagire di fronte ad uno scenario di attacco che simula la realtà.

Nello specifico, le tecniche utilizzate nei confronti di Askoll sono state le seguenti:

OSINT (Open Source INTellingence): ricerca approfondita nel pubblico dominio (Internet, Deep & Dark Web) di informazioni relative ad Askoll ed al suo personale.

Attacco infrastrutturale ed applicativo: i sistemi ritenuti significativi sono stati sottoposti ad un attacco infrastrutturale ed applicativo per comprendere e sfruttare eventuali vulnerabilità esposte.

Social Engineering: attività volte ad ottenere delle informazioni utili per accedere a dati ed applicazioni, oltre che testare il livello di consapevolezza interna dell'azienda in ambito sicurezza.

Nella fattispecie, è stato utilizzato il **Phishing** come strumento di attacco da remoto, mentre l'accesso fisico è avvenuto con tecniche di *Impersonation* e *Piggybacking* (*Tailgating*).

"ERAVAMO PERFETTAMENTE CONSAPEVOLI CHE LA VULNERABILITÀ PIÙ CRITICA SAREBBE STATA RICONDUCIBILE AL FATTORE UMANO, SITUAZIONE COMPROVATA DALLE ATTIVITÀ DI SOCIAL ENGINEERING. CIÒ CHE CI HA MOLTO SORPRESI È LA PORTATA DI QUESTA VULNERABILITÀ, QUANTO INTUITY SIA RIUSCITA AD ADDENTRARSI NEL BUSINESS DELLA NOSTRA AZIENDA E DI CONSEGUENZA QUANTI DANNI AVREMMO POTUTO SUBIRE SE QUESTO FOSSE STATO UN ATTACCO REALE."".

MORENO PANETTO, *IT SYSTEMS MANAGER DI ASKOLL*

LA SOLUZIONE: INTUITY SECURITY AWARENESS

L'analisi empirica ottenuta attraverso la simulazione di reali attacchi informatici ha permesso di esporre al Board of Management di Askoll il rischio concreto legato alle vulnerabilità riscontrate e dimostrare la necessità di aumentare la consapevolezza interna sul tema della sicurezza informatica.

Lo scopo del servizio Hacking People di IMQ Intuity, erogato attraverso delle sessioni formative in aula, è stato quello di rendere gli utenti consapevoli dei pericoli derivanti dall'uso quotidiano degli strumenti informatici e fornire le necessarie informazioni per riconoscere e quindi eludere queste minacce.

LA SOLUZIONE: NETWRIX AUDITOR

"A conclusione delle attività effettuate da INTUITY, mi resi conto di avere una limitata visibilità in alcune aree della nostra infrastruttura, come ad esempio Active Directory, file e server. Abbiamo identificato in Netwrix Auditor la soluzione ideale per sopperire a questa carenza e soddisfare tutte le necessità di controllo dettate dal GDPR."

Moreno Panetto, IT Systems Manager di Askoll

La soluzione di Netwrix Auditor fornisce visibilità completa sia sulle configurazioni che sull'accesso ai dati all'interno dell'infrastruttura IT, rispondendo in maniera veloce e puntuale alle domande: chi ha fatto cosa, quando, dove e chi ha accesso a cosa.

Monitorare gli accessi e l'operatività degli utenti consente alle aziende di prevenire eventuali violazioni interne evitando così rischi di sicurezza di natura "*insider-caused*".

I VANTAGGI OTTENUTI

L'attività di Red Team ha consentito di quantificare, attraverso un metodo empirico, gli effetti di un eventuale attacco informatico, confermando i punti di forza delle scelte compiute da Askoll ed evidenziando le principali carenze.

Queste valutazioni sono state sottoposte successivamente all'attenzione del Board of Management per la definizione di un piano di investimenti in ambito cybersecurity.

"I SERVIZI DI INTUITY CI HANNO PERMESSO DI TESTARE QUANTO AVEVAMO IMPLEMENTATO A LIVELLO DI INFRASTRUTTURA DI SICUREZZA E DI CORREGGERNE ALCUNI ASPETTI, OLTRE CHE DI INTEGRARE UN SISTEMA DI AUDITING. IN MERITO ALLE ATTIVITÀ FORMATIVE SULLA CYBERSECURITY, I COLLEGHI SONO STATI MOLTO INTERESSATI E RICETTIVI."

MORENO PANETTO, *IT SYSTEMS MANAGER DI ASKOLL*

"Il mio feedback sul corso è senz'altro più che positivo. È servito per conoscere alcune tattiche di attacco ed è stato, almeno per me, molto formativo... ora guardo con un altro livello di attenzione mail, link, siti ecc.!"

"Interessanti le informazioni che ci sono state date per riuscire a distinguere i siti fasulli da quelli ufficiali e la parte della lezione dedicata a come costruire password articolate ma semplici da ricordare."

"Ora credo di aver acquisito degli strumenti utili sia a livello professionale che personale."

"Spero che in seguito ai continui aggiornamenti sulla sicurezza informatica, il corso possa essere ripetuto in futuro."

"il docente è stato chiaro nell'esposizione e comprensibile anche per le persone meno tecniche come me."