

BUSINESS CASE

Osservatorio Cybersecurity & Data Protection

IL MONITORAGGIO DEI DATI AZIENDALI E L'ANALISI DELLE POSSIBILI MINACCE IN GRUPPO LUBE



Ricerca 2021
Business Case

IL SETTORE

Manufacturing

L'AZIENDA

Gruppo Lube è un'azienda italiana che produce cucine componibili e complementi di arredo, oltre che un'importante società di volley maschile, militante nel campionato di Superlega.

L'ESIGENZA

Tutela del patrimonio tecnologico, informativo e intellettuale dell'azienda e riduzione dell'impatto causato da eventuali disservizi del sistema informativo aziendale.

IL PROGETTO IMPLEMENTATO

Implementazione di un servizio di monitoraggio e gestione eventi erogato dal SOC, composto da una soluzione SIEM affiancata da un team di specialisti, focalizzati sull'analisi delle potenziali minacce.

I BENEFICI

- Spostamento del focus del personale aziendale da attività secondarie verso attività centrali per il core business.
- Aumento della consapevolezza delle problematiche di sicurezza tra i dipendenti aziendali.
- Visione a 360 gradi delle componenti del sistema informativo aziendale a diversi livelli di granularità.

Il monitoraggio dei dati aziendali e l'analisi delle possibili minacce in Gruppo LUBE

L'AZIENDA

Gruppo Lube è un'azienda italiana che produce cucine componibili e complementi di arredo, oltre che un'importante società di volley maschile, militante nel campionato di Superlega.

Nata nel 1967 come impresa artigianale di due famiglie a Treia, in provincia di Macerata, negli anni ha registrato un'importante crescita, che l'ha portata ad essere oggi una realtà di 650 dipendenti con un fatturato annuo di circa 200 milioni di euro e diverse certificazioni del settore all'attivo.

L'azienda gode di notevole rilievo all'interno del territorio nazionale, tanto da essere considerata leader di mercato, sia per la riconoscibilità del suo marchio sia per la grande attenzione posta nei confronti dei suoi rivenditori, considerati partner commerciali, e dei suoi clienti.

L'ESIGENZA

Il focus aziendale in materia di sicurezza all'interno dell'organizzazione ha radici molto profonde e ha iniziato a manifestarsi dapprima con l'attenzione riservata al tema della sicurezza nel luogo di lavoro.

L'organizzazione ha poi iniziato a considerare le implicazioni legate alla parte informatica, focalizzando l'attenzione

sull'impatto derivante da un possibile fermo della produzione a seguito di un disservizio del sistema informativo aziendale, oltre che sulle eventuali conseguenze che avrebbero potuto verificarsi sulle singole componenti dei sistemi.

È stata quindi avviata una valutazione sulle azioni da implementare al fine di tutelare adeguatamente il patrimonio tecnologico, informativo e intellettuale dell'azienda, monitorando e analizzando in modo intelligente i vari flussi di dati e la loro integrità, con la consapevolezza che il dato stesso rappresenta un elemento fondamentale per l'organizzazione.

IL PROGETTO IMPLEMENTATO

Gruppo Lube ha pertanto iniziato un processo di selezione del fornitore insieme al quale mettere in campo un progetto per il monitoraggio e l'analisi dei dati aziendali, con l'obiettivo di avere maggiore visibilità di tutto ciò che accade in azienda: dal singolo click del dipendente fino al funzionamento, a un più alto livello, delle varie applicazioni del sistema informativo.

La scelta è ricaduta su Yarix, divisione di Var Group che si occupa di cybersecurity, viste anche le collaborazioni già in essere con il Gruppo su altri fronti.

IL SETTORE

Manufacturing

L'AZIENDA

Gruppo Lube è un'azienda italiana che produce cucine componibili e complementi di arredo, oltre che un'importante società di volley maschile, militante nel campionato di Superlega.

L'ESIGENZA

Tutela del patrimonio tecnologico, informativo e intellettuale dell'azienda e riduzione dell'impatto causato da eventuali disservizi del sistema informativo aziendale.

IL PROGETTO IMPLEMENTATO

Implementazione di un servizio di monitoraggio e gestione eventi erogato dal SOC, composto da una soluzione SIEM affiancata da un team di specialisti, focalizzati sull'analisi delle potenziali minacce.

I BENEFICI

- Spostamento del focus del personale aziendale da attività secondarie verso attività centrali per il core business.
- Aumento della consapevolezza delle problematiche di sicurezza tra i dipendenti aziendali.
- Visione a 360 gradi delle componenti del sistema informativo aziendale a diversi livelli di granularità.

Il monitoraggio dei dati aziendali e l'analisi delle possibili minacce in Gruppo LUBE

La parte più importante del progetto è rappresentata dal servizio di monitoraggio e gestione eventi erogato dal Security Operation Center (SOC) di Yarix. Da un punto di vista tecnologico, il servizio è composto da una soluzione di Security Information and Event Management (SIEM), che permette di monitorare le attività, il flusso di rete e i log delle applicazioni in modo previsionale e proattivo. Lo strumento è poi affiancato da un team di specialisti che, grazie alla loro expertise, rafforzano la possibilità di individuare e analizzare le potenziali minacce. Grazie alle avanzate capacità di Analytics, il sistema è in grado di identificare in tempo reale i segnali di rischio, prevenendo anche le minacce ancora sconosciute.

Nello svolgimento delle attività di monitoraggio e analisi è previsto anche il coinvolgimento delle figure aziendali dedicate alla gestione della sicurezza aziendale nelle diverse aree dell'organizzazione, in modo da evitare un'eccessiva rigidità dal punto di vista organizzativo e riuscire a diffondere la consapevolezza sulle problematiche di sicurezza informatica all'interno di tutta l'azienda.

I BENEFICI

Da un punto di vista organizzativo, l'implementazione del progetto ha permesso a Gruppo Lube di strutturarsi in

maniera molto solida ed efficiente: il personale aziendale è oggi decisamente meno impegnato da attività secondarie e sempre più focalizzato su attività centrali per il core business. Allo stesso tempo, è aumentata in modo significativo la consapevolezza delle problematiche di sicurezza tra tutti i dipendenti aziendali coinvolti nelle diverse funzioni e attività.

Da un punto di vista tecnologico, invece, le attività di monitoraggio stanno portando Gruppo Lube ad avere una visione a 360 gradi delle varie componenti del suo sistema informativo a diversi livelli di granularità, dal più alto livello fino al singolo dato circolante tra le applicazioni.