REEVO | GRUPPO SOGEGROSS

CASE STUDY

Sogegross e la partnership con ReeVo al servizio della GDO

SUMMARY

- Un gruppo della GDO dove l'IT non può fermarsi mai
- La cybersecurity come leva di continuità operativa
- Una partnership costruita nel tempo
- Quando il SOC fa davvero la differenza
- Guardare avanti insieme

CASE STUDY

Sogegross e la partnership con ReeVo al servizio della GDO

GDO significa Grande Distribuzione Organizzata, un settore chiave in cui la continuità operativa non rappresenta un semplice requisito tecnologico, ma il presupposto stesso del business.
Non è una iperbole e nemmeno una esagerazione. È nei numeri e nella quotidianità di tutti i protagonisti di questo mercato.
In un ecosistema così interconnesso, ogni singola interruzione può tradursi istantaneamente in punti vendita paralizzati, catene logistiche bloccate, gravi impatti sulla customer experience e ingenti perdite economiche immediate. In un simile scenario, **Cloud e Cyber Security** non sono più ambiti distinti, ma **diventano i pilastri indispensabili di un'unica strategia di resilienza digitale**.
È proprio in questo contesto, al centro di questo panorama così delicato e critico che si inserisce la collaborazione tra **Sogegross e ReeVo**, una solida partnership costruita nel tempo che oggi rappresenta un modello concreto di come innovazione tecnologica, competenze specialistiche e fiducia reciproca possano trasformare la sicurezza informatica in un vero vantaggio competitivo.

CASE STUDY

REEVO | GRUPPO SOGEGROSS

Un gruppo della GDO dove l'IT non può fermarsi mai

Con oltre 1,25 miliardi di euro di fatturato, circa 3.300 dipendenti e una presenza capillare nel Nord Italia attraverso i marchi Basko, Gros Market, Ekom e Doro, il Gruppo Sogegross opera in uno dei **mercati più complessi e sfidanti** sotto il profilo operativo.
La distribuzione moderna vive infatti secondo una **logica di continuità assoluta**: punti vendita, magazzini, sistemi logistici, casse, piattaforme digitali e supply chain devono essere disponibili senza interruzioni.

Come racconta Marco Staiti, IT Manager di Sogegross, il ruolo dell'IT va ben oltre la gestione dell'infrastruttura.
"Sogegross ha sempre investito molto sul digitale e siamo convinti che il digitale porti innovazione e valore all'azienda. Dalla mia funzione ci si aspetta, naturalmente, che tutto funzioni H24, 365 giorni all'anno. Ma soprattutto ci si aspetta innovazione, proattività e la capacità di portare sul mercato soluzioni che possano essere adottate in azienda nel miglior modo possibile." Garantire la costante disponibilità dei servizi è quindi soltanto il punto di partenza. La vera sfida per Sogegross è **costruire un'infrastruttura agile e sicura**, capace di evolvere continuamente, anticipando i bisogni del business e l'inevitabile evoluzione delle minacce informatiche.

CASE STUDY

REEVO | GRUPPO SOGEGROSS

La cybersecurity come leva di continuità operativa

Negli ultimi anni il settore retail e la GDO sono diventati uno dei principali bersagli della criminalità informatica. La crescente digitalizzazione delle operations, l'integrazione tra sistemi logistici e punti vendita e l'enorme quantità di dati gestiti hanno ampliato notevolmente la superficie d'attacco.

A confermarlo sono anche i dati del **Rapporto Clusit,** che evidenziano come gli attacchi cyber continuino a crescere sia per numerosità sia per sofisticazione. Minacce come ransomware, compromissioni delle identità digitali e attacchi mirati alle infrastrutture critiche sono diventati un rischio reale. Per le aziende della GDO la disponibilità dei sistemi è diventata una variabile direttamente collegata alla continuità del business: un'interruzione può avere effetti immediati sulla logistica, sulle vendite e sul servizio al cliente.
Per un'azienda d'eccellenza come Sogegross, che opera senza interruzioni durante tutto l'anno, questo significa **affrontare la sicurezza come un processo continuo**, in costante evoluzione.

Marco Staiti lo sintetizza con grande chiarezza:
"**La cybersecurity per l'azienda è fondamentale**, ancora di più per una realtà che lavora H24, 365 giorni all'anno. Per questo abbiamo sempre investito molto nella sicurezza e siamo stati tra le prime aziende italiane a dotarsi di un SOC operativo 24 ore su 24."

CASE STUDY

REEVO | GRUPPO SOGEGROSS

Una partnership costruita nel tempo

Il legame tra il gruppo Sogegross e ReeVo nasce oltre dieci anni fa.
Quella che all'inizio era una **collaborazione** focalizzata sulla risposta a un'esigenza tattica di sicurezza è **cresciuta progressivamente** fino a diventare una relazione strategica che oggi coinvolge l'intero ecosistema di sicurezza aziendale.

Secondo Staiti, **il vero valore della partnership** non **risiede** esclusivamente nelle tecnologie adottate, bensì **nella qualità del fattore umano.**
"Abbiamo iniziato con un piccolo firewall. Oggi ReeVo è un **partner fondamentale per lo sviluppo della cybersecurity** in azienda. Siamo riusciti a implementare soluzioni che non pensavamo fosse possibile realizzare. Questo è stato possibile grazie alle persone di ReeVo, alla fiducia costruita negli anni e a una collaborazione trasparente tra i nostri team."

Una relazione che si fonda su un elemento spesso sottovalutato nei progetti tecnologici: la **condivisione delle competenze**.
Per Sogegross il confronto continuo con specialisti che operano in contesti industriali differenti consente infatti di anticipare nuove minacce, confrontare approcci diversi e accelerare l'adozione delle migliori pratiche di sicurezza.

CASE STUDY

REEVO | GRUPPO SOGEGROSS

Quando il SOC fa davvero la differenza

Per anni la cybersecurity è stata percepita principalmente come un insieme di tecnologie di protezione: firewall, antivirus, sistemi di autenticazione. Oggi questo approccio non è più sufficiente. Le organizzazioni moderne devono assumere come quasi inevitabile il tentativo di compromissione spostando il focus della propria strategia sulla capacità di individuare tempestivamente le anomalie e intervenire prima che si trasformino in un incidente.
È questo il principio che sta alla base del **Security Operations Center** (SOC), oggi considerato uno dei pilastri delle moderne strategie di cyber resilience. Il SOC è una struttura operativa che monitora in modo continuativo infrastrutture, reti, endpoint, identità digitali e applicazioni, raccogliendo e correlando milioni di eventi di sicurezza provenienti dall'intero ecosistema IT. Attraverso piattaforme avanzate di monitoraggio, sistemi di analisi e il lavoro di analisti specializzati, il SOC distingue comportamenti anomali da falsi positivi, individua rapidamente un attacco in corso e attiva le procedure di risposta più efficaci.

Il valore di questo modello non **risiede** soltanto nella tecnologia, ma **nella perfetta sinergia** tra automazione avanzata, competenze umane verticali e capacità di intervento continuo. Per organizzazioni come Sogegross, che operano senza interruzioni durante tutto l'anno, poter contare su un presidio specializzato 24 ore su 24 significa ridurre drasticamente i tempi di rilevazione e di risposta agli incidenti, neutralizzando gli impatti prima di divengano critici.

È proprio questo il modello con cui ReeVo affianca Sogegross. Attraverso una **strategia che integra Cloud, servizi gestiti di cybersecurity, Managed Detection & Response (MDR) e un SOC operativo H24,** il monitoraggio continuo dell'infrastruttura consente di intercettare comportamenti sospetti nelle fasi iniziali della cosiddetta kill chain dell'attacco, quando è ancora possibile contenere l'intrusione prima che gli aggressori riescano a compromettere sistemi critici o sottrarre dati. **L'obiettivo** non **è** semplicemente generare alert, ma **offrire una reale capacità di analisi, correlazione degli eventi, threat intelligence e supporto operativo durante l'intero ciclo di gestione dell'incidente.**

Questo approccio riflette una tendenza ormai consolidata del mercato. Secondo il **Rapporto Clusit** la crescente velocità e sofisticazione degli attacchi rende sempre più strategiche le capacità di monitoraggio continuo, threat detection e incident response. Oggi **la resilienza di un'organizzazione dipende** sempre meno dalla sola prevenzione e **sempre più dalla rapidità con cui riesce a individuare, contenere e neutralizzare un attacco.**

L'efficacia di questo modello si è manifestata concretamente durante un tentativo di compromissione subito da Sogegross nel giorno di Pasqua.
Sfruttando il periodo festivo, gli attaccanti avevano tentato l'intrusione, ma il SOC di ReeVo ha rilevato tempestivamente alcune attività anomale all'interno dell'Active Directory: erano state infatti create delle utenze sospette e i cybercriminali avevano già avviato i primi movimenti laterali all'interno della rete. La segnalazione immediata ha consentito al team IT di Sogegross e agli specialisti ReeVo di attivare rapidamente le procedure di contenimento.
"Ricordo perfettamente quella chiamata: era il giorno di Pasqua. Il SOC ci ha avvisato che erano state create delle utenze sulla nostra Active Directory e che erano iniziati movimenti laterali. Nell'arco di circa un'ora e mezza siamo riusciti a espellere gli attaccanti dall'infrastruttura. Non hanno provocato danni e non sono riusciti a sottrarre dati. È stato in quel momento che ho avuto la conferma concreta dell'efficacia delle soluzioni implementate insieme a ReeVo."

L'episodio ha confermato una convinzione maturata negli anni da Marco Staiti: la sicurezza informatica non consiste nel credere che nessuno riuscirà mai a entrare nei sistemi aziendali, ma nella capacità di riconoscere rapidamente ogni anomalia e reagire con tempestività.
"**Quello che fa davvero la differenza è il tempo di risposta**: bisogna individuare gli attacchi rapidamente e risolverli il prima possibile. Per riuscirci servono tecnologie sempre aggiornate, processi consolidati e persone con cui costruire un rapporto di grande fiducia e professionalità."

CASE STUDY

REEVO | GRUPPO SOGEGROSS

Guardare avanti insieme

L'**accelerazione impressa dall'intelligenza artificiale** sta modificando rapidamente anche il panorama della sicurezza informatica.
Le stesse tecnologie di AI che consentono di migliorare automazione, analisi predittiva e rilevazione delle minacce vengono oggi sfruttate anche dagli attaccanti per rendere campagne di phishing, social engineering e malware sempre più sofisticati e rapidi.
Di conseguenza, la capacità di aggiornare continuamente strumenti, competenze e modelli operativi diventa un elemento imprescindibile per ogni organizzazione.
Marco Staiti guarda a questo scenario con realismo e con la consapevolezza che nessuna azienda per quanto strutturata, possa affrontare in totale autonomia un'evoluzione tanto rapida.

"L'intelligenza artificiale sta cambiando completamente i paradigmi del nostro lavoro. Se fino a qualche anno fa riuscivo a immaginare come sarebbe stata la cybersecurity nei successivi quattro o cinque anni, oggi è molto più difficile. Per questo mi aspetto tanto dal nostro partner ReeVo: confronto continuo, nuovi punti di vista e la capacità di affrontare insieme un'evoluzione che riguarda tutto il settore."
È una visione che sintetizza il significato della partnership tra Sogegross e ReeVo: non un semplice rapporto cliente-fornitore, ma un percorso condiviso in cui Cloud, cybersecurity, competenze e fiducia reciproca diventano gli elementi chiave per costruire un'organizzazione resiliente. Un **modello di collaborazione capace di garantire continuità operativa oggi e di accompagnare l'innovazione digitale del business anche di fronte alle sfide che caratterizzeranno il futuro della GDO.**

REEVO

#ReeVolutionaryStory