voices

CrowdStrike Customer Case Study

europe energy

Europe Energy protegge clienti, dati e transazioni commerciali da milioni di euro con le soluzioni CrowdStrike

Se anche solo una delle sue transazioni nell'ambito del trading di energia da svariati milioni di euro dovesse fallire a causa di un cyberattacco, Europe Energy non solo perderebbe entrate, ma potrebbe non avere abbastanza tempo per acquistare tutta l'energia necessaria a rifornire i propri clienti prima della chiusura del mercato, e potrebbe anche affrontare problemi di conformità normativa, con il rischio di vedersi sospendere il proprio account. Non sorprende quindi che la sicurezza sia in cima alla lista dei motivi di preoccupazione di Stefano Libriani, Chief Information Officer di Europe Energy.

Europe Energy è un'organizzazione multinazionale specializzata nella negoziazione e nella distribuzione di energia in Europa. L'azienda fornisce anche servizi di telecomunicazione e internet, con l'obiettivo di fornire ai clienti un unico fornitore per tutte le esigenze. Europe Energy è stata fondata nel 2007 e conta 150 dipendenti.

Proteggere transazioni da 10 milioni di euro

Oltre alle proprie operazioni di trading di alto valore, Europe Energy deve proteggere i dati dei suoi 100.000 clienti per tutelare loro e la reputazione del proprio marchio ed evitare loro di incorrere nel rischio di pagare multe, come verificatosi ad esempio in seguito a violazioni del Regolamento Generale sulla Protezione dei Dati (GDPR). "Alcune delle nostre operazioni, che hanno un valore fino a 10 milioni di euro, possono richiedere ore per essere completate e temiamo che anche una sola di queste transazioni possa venire compromessa," ha dichiarato Libriani. "Quando acquistiamo energia da una region, dobbiamo venderla a un altro cliente lo stesso giorno, poiché non è possibile immagazzinarla. Avviare una transazione e non essere in grado di chiuderla si traduce in un'enorme perdita per l'azienda e per la nostra reputazione".

Sebbene il rischio per Europe Energy non sia diverso da quello di altri settori, i suoi alti ricavi, che si avvicinano al miliardo di euro, possono farla apparire come un 'honeypot' per i criminali e gli attori di attacchi ransomware. Avendo questa particolare attività, tra l'altro, margini particolarmente ridotti, ogni potenziale perdita può rappresentare un grosso problema per l'azienda.

In uno scenario in cui fronteggiare la minaccia di attacchi si fa sempre più prioritario, Europe Energy ha cercato di migliorare e rafforzare la propria sicurezza. L'azienda stava gestendo autonomamente tutte le proprie esigenze di sicurezza, un approccio che stava diventando sempre più difficile, lento, costoso e laborioso gestire. Ma quando una violazione della sicurezza di tipo zero-day ha colpito l'azienda, l'ha scossa e spinta ad agire. "L'attacco zero-day ci ha spinto a pensare a una soluzione di servizio che potesse offrire un controllo migliore del nostro perimetro di sicurezza" ha affermato Libriani. Fortunatamente l'attacco non ha provocato danni, ma l'azienda ha impiegato tre giorni per individuare e risolvere i problemi correlati.

SETTORE

Energia

LOCATION/HQ

Milano, Italia

SFIDE

- Proteggere i dati di 100.000 clienti
- Minaccia di perdere ricavi da trading di energia per milioni di euro
- Mitigare il rischio di ingenti sanzioni normative
- La gestione della sicurezza era complessa, lenta e laboriosa

LA SOLUZIONE

Società italiana attiva nel mercato dell'energia, Europe Energy ha utilizzato CrowdStrike Falcon Complete™ per proteggere e mettere al sicuro i dati dei clienti, ridurre al minimo il rischio di perdere ricavi da trading per milioni di euro e per rafforzare la reputazione del marchio

"La reazione di CrowdStrike OverWatch è stata sorprendente e da quel momento abbiamo capito che potevamo fidarci di CrowdStrike per proteggere i nostri clienti e la nostra attività".

Stefano Libriani
Chief Information Officer
Europe Energy

voices

CrowdStrike Customer Case Study

Esperienza unica di pre-vendita

Europe Energy ha iniziato a sondare il mercato alla ricerca di una nuova soluzione e, dopo aver valutato otto aziende, ha scelto CrowdStrike. “Europe Energy ha apprezzato CrowdStrike per le capacità tecniche e la gamma di servizi offerti” ha commentato Libriani. “Ad esempio, il tool di extended detection and response di CrowdStrike è il migliore sul mercato. Ma l’intera esperienza con CrowdStrike è stata fantastica. CrowdStrike ha dedicato molto tempo e sforzi per illustrare i prodotti e i servizi e ci ha persino permesso di "testarli" in un ambiente di laboratorio prima di impegnarci nell'acquisto. Ci ha mostrato come avviene un attacco e come fermarlo. Abbiamo imparato molto, non solo su CrowdStrike, ma anche sull'intero settore della sicurezza. Fornire una visione così approfondita e completa della portata e delle capacità delle soluzioni CrowdStrike fin dalle prime fasi del processo di vendita è stato unico. Nessun altro fornitore ha offerto tutto questo”.

Uno degli altri fattori chiave della decisione è stata la gamma di moduli e strumenti aggiuntivi che altri fornitori fanno pagare a parte e che sono inclusi invece nella soluzione CrowdStrike. “Con CrowdStrike tutto è integrato in un'unica piattaforma e questo è un enorme vantaggio. Significa che dobbiamo imparare, monitorare e mantenere un'unica soluzione basata sul cloud, il che riduce sia il tempo che le spese generali”, ha dichiarato Libriani.

Europe Energy ha implementato una suite di soluzioni CrowdStrike Falcon Complete per monitorare e proteggere 300 endpoint, tra cui laptop, PC e server. La maggior parte dei dipendenti utilizza computer portatili, il che ha permesso loro di lavorare a casa durante la pandemia COVID-19. L'implementazione, che ha richiesto solo due giorni, è stata semplice e facile anche tra sistemi operativi diversi.

“All'inizio abbiamo usato CrowdStrike per controllare cosa succedeva nel nostro ambiente”, ha commentato Libriani. “Ma da allora, e questo è il punto chiave di CrowdStrike, non abbiamo più bisogno di guardare la console ogni giorno perché funziona automaticamente in background, riducendo in modo significativo la quantità di tempo che prima impiegavamo”.

L'azienda dispone di un'infrastruttura IT ibrida tra cloud e on-premise. On-premises è una server farm Linux iperconvergente per le operazioni aziendali interne. I sistemi rivolti ai clienti sono in cloud e comprendono principalmente portali online per la visualizzazione e la gestione dei servizi da parte dei clienti, oltre ad applicazioni mobili e per i partner.

CrowdStrike Falcon OverWatch è "straordinario"

Per sottolineare l'efficacia di CrowdStrike, Libriani ha spiegato che una postazione di lavoro appartenente a un ex dipendente era stata bloccata. Non appena il team ha iniziato ad accedere al dispositivo, a causa del comportamento anomalo della workstation, è stato emesso un allarme da Falcon OverWatch e il team Falcon Complete è entrato in azione per contenere ed eliminare la minaccia. “La risposta è stata sorprendente e da quel momento abbiamo capito che potevamo fidarci di CrowdStrike per proteggere i nostri clienti e la nostra azienda” ha affermato Libriani.

Per Europe Energy, uno dei vantaggi principali di CrowdStrike è la sicurezza acquisita grazie alla possibilità di rafforzare e migliorare l'efficacia della sicurezza degli endpoint. “La presenza di CrowdStrike è per noi fonte di tranquillità”, ha dichiarato Libriani. “Oltre a una solida sicurezza, ciò significa anche che possiamo concentrarci su attività più importanti, come dedicare più tempo alla fornitura di servizi pratici e efficaci per i nostri clienti”.

RISULTATI

L'automazione ha sostituito il full-time security role

Allarmi sulle minacce in tempo reale e migliore visibilità sull'intera infrastruttura di sicurezza

Un'unica soluzione integrata di gestione e controllo

ENDPOINTS

300

PRODOTTI CROWDSTRIKE

- Falcon Complete™ managed detection and response (MDR)
- Falcon Device Control™ for cloud-delivered device control
- Falcon Discover™ IT hygiene
- Falcon Insight XDR™ endpoint detection and response (EDR)
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus (NGAV)
- Falcon Spotlight™ vulnerability management

voices

CrowdStrike Customer Case Study

La portata delle funzionalità del portafoglio di CrowdStrike ha permesso a Europe Energy di gestire un'ampia gamma di attività di sicurezza, come l'evidenziazione e la mitigazione delle vulnerabilità e la fornitura all'azienda di una visione chiara, dettagliata e completa del proprio ambiente. Falcon Spotlight, ad esempio, aiuta l'azienda a implementare in modo efficiente gli aggiornamenti di sicurezza. Insieme ad altre soluzioni CrowdStrike e a misure aggiuntive come l'autenticazione multifattoriale, la chiusura delle porte del firewall e lo spostamento dei servizi rivolti all'esterno nel cloud, tutto ciò ha portato a un'infrastruttura di sicurezza più solida e affidabile.

Fornire fiducia e sicurezza

"CrowdStrike ci ha fornito i mezzi per difenderci dagli attacchi", ha affermato Libriani. "Possiamo monitorare l'ambiente in modo accurato e in tempo reale tramite un'unica dashboard, che evidenzia le vulnerabilità e le azioni da intraprendere per proteggerle. Un tempo la paura era doppia: quella di essere attaccati e quella di non sapere quali vulnerabilità avessimo".

Prima di CrowdStrike, Europe Energy dedicava una persona a tempo pieno al monitoraggio e alla mitigazione delle vulnerabilità di sicurezza. I processi automatizzati delle soluzioni CrowdStrike hanno permesso di reindirizzare una parte significativa del tempo verso attività più preziose e produttive.

Libriani ha aggiunto che uno degli aspetti importanti del rapporto con CrowdStrike è il suo impatto sulla reputazione del marchio. "Uno dei maggiori vantaggi della partnership è stato l'utilizzo del marchio CrowdStrike per rafforzare il nostro" ha dichiarato. "Ora possiamo dimostrare ai nostri clienti e agli altri stakeholder che, grazie all'impiego di CrowdStrike, fornitore di una delle migliori e più note soluzioni di sicurezza sul mercato, stiamo proteggendo loro e i loro dati più efficacemente e in modo più solido che mai".

INFORMAZIONI SU CROWDSTRIKE

CrowdStrike® (Nasdaq: CRWD), leader nella sicurezza informatica a livello globale, ha ridefinito la sicurezza con la piattaforma cloud-native più avanzata al mondo per proteggere le aree più critiche del rischio aziendale - endpoint e workload cloud, identità e dati. Grazie alla tecnologia CrowdStrike Security Cloud e a un'intelligenza artificiale di livello mondiale, la piattaforma CrowdStrike Falcon® sfrutta gli indicatori di attacco in tempo reale, le informazioni sulle minacce, lo spionaggio degli avversari in evoluzione e la telemetria arricchita proveniente da tutta l'azienda per fornire rilevamenti estremamente accurati, protezione e ripristino automatici, threat hunting d'élite e osservabilità prioritaria delle vulnerabilità. Costruita appositamente nel cloud con una singola architettura di agenti leggeri, la piattaforma Falcon permette di beneficiare di una scalabilità senza pari, di una protezione e di prestazioni superiori, di una complessità ridotta e di un time-to-value immediato.

CrowdStrike: **We stop breaches.**

Per maggiori informazioni:
https://www.crowdstrike.com/
Seguici su: Blog | Twitter | LinkedIn | Facebook | Instagram
Prova una demo gratuita oggi:
https://www.crowdstrike.com/free-trial-guide/