alperia

Reti elettriche sicure e senza interruzioni

2020

kaspersky BRING ON THE FUTURE

Kaspersky Industrial CyberSecurity

Alperia ha adottato la soluzione Kaspersky KICS for Nodes per proteggere i sistemi di telecontrollo dedicati alle centrali di produzione ed alla rete di distribuzione preposta all'erogazione di energia elettrica a 280 mila utenti nell'Alto Adige. La scelta è stata dettata dall'esigenza di avere una soluzione dedicata all'ambiente OT, che offrisse la massima protezione senza rischiare di interrompere il funzionamento di macchine fondamentali per la fornitura dei servizi.

"L'idea di avere una task force con i tecnici di Kaspersky a disposizione in azienda ci ha permesso di customizzare il prodotto cucendolo a misura sulla nostra realtà".

Sandro Moretti
Division Manager Teleconduction & Telecommunication

L'aumento dei dispositivi connessi e la crescente digitalizzazione delle infrastrutture delle reti di pubblica utilità porta con sé tante opportunità, ma anche un aumento esponenziale dei rischi.

Secondo il Global Risks Report 2020, realizzato dal World Economic Forum, la combinazione tra attacchi informatici su vasta scala e la possibile interruzione di infrastrutture critiche e reti di informazione è al secondo posto della classifica dei rischi più temuti.

Un dato evidenziato anche dall'Allianz Risk Barometer 2020, secondo il quale gli incidenti informatici rappresentano il rischio aziendale maggiormente percepito a livello globale, mentre al secondo posto c'è l'interruzione di attività.

Non è quindi una sorpresa che le aziende che erogano servizi essenziali (dall'acqua all'energia, dai trasporti alle telecomunicazioni) stiano prestando sempre più attenzione alla protezione delle infrastrutture che sono chiamate a gestire. È questo anche il caso delle aziende che operano nel settore della generazione e della distribuzione di energia elettrica.

Energia e gas per 280 mila Altoatesini

Alperia è la realtà altoatesina che fornisce energia elettrica e gas a 280 mila utenti gestendo 34 centrali idroelettriche, 6 centrali di teleriscaldamento, oltre 8.600 km di rete elettrica e 700 punti di ricarica elettrica.

L'azienda nasce nel 2016 dalla fusione tra le due più importanti società energetiche locali: AEW, le cui radici affondano alla fine del XIX secolo, quando la sua antenata Etschwerke realizzò le prime centrali per utilizzare la forza dell'acqua al fine di dotare il territorio di energia elettrica; e SEL - Società energetica altoatesina, che nell'ultimo decennio ha preso in mano la gestione delle grandi centrali idroelettriche e della rete elettrica dell'Alto Adige.

A capo della funzione Telecomunications e Teleconduction di Alperia Group c'è l'ingegner Sandro Moretti: una figura esperta che, riportando direttamente al direttore generale del gruppo, guida oggi un team di 13 persone con il compito di gestire i sistemi di trasmissione dei dati di produzione e le telecomunicazioni. In pratica si tratta della squadra che gestisce le RTU, i datacenter, l'operatività delle sale di controllo e la rete di collegamento verso le due realtà del gruppo che si occupano di produzione (Alperia Greenpower) e distribuzione (Edyna) di energia elettrica.

Le specificità del mondo OT

Pensare di affrontare la questione della security dei sistemi industriali con lo stesso approccio finora impiegato nelle soluzioni "business" sarebbe un errore, e Moretti ne è convinto. Se in ambito IT i principi base della Cyber security definiscono un dato sicuro quando sono rispettati, nell'ordine: riservatezza, integrità e disponibilità, in ambiente OT l'ordine di questi tre fattori va letto al contrario. Le caratteristiche irrinunciabili sono infatti disponibilità, in primis, e poi integrità e riservatezza. Un paradigma, questo, particolarmente valido nel caso delle infrastrutture critiche, dove i sistemi devono essere sempre attivi (ed è proprio questo anche il motivo per cui tutti i sistemi sono gestiti da macchine ridondate).

Una logica conseguenza di questi principi è che in ambito industriale vanno utilizzate soluzioni espressamente pensate per questo scopo: porte, protocolli e regole sono infatti diverse e tipiche dei dispositivi collegati alla rete di impianto e dei sistemi di controllo e telecontrollo. Inoltre spesso sono presenti macchine dotate di sistemi operativi che, per poter essere sempre disponibili, non sempre sono aggiornati in tempo reale all'ultima patch di sicurezza.

"Sin da subito la direzione ha capito che non si potevano utilizzare nel mondo OT (Operational Technologies) gli stessi paradigmi che valgono nel mondo IT", spiega

990ca.
dipendenti

€1.3mld
miliardi di euro
di fatturato

1.056.717 euro
di investimenti
in ricerca

Moretti. "Per questo Alperia ha provveduto a separare il perimetro della rete OT da quello della rete IT e a impostare delle strategie di gestione diversificate".

Il gruppo di lavoro capitanato da Moretti si è messo allora in cerca di una soluzione che consentisse di inserire, all'interno del perimetro della gestione dei sistemi di telecontrollo, un sistema di sicurezza contro gli attacchi informatici più evoluto del classico endpoint in uso nel dipartimento IT e, soprattutto, dedicato all'ambito OT.

Dopo un'attenta analisi delle (poche) soluzioni disponibili sul mercato specificamente dedicate agli ambienti industriali Moretti decide di puntare su KICS – Kaspersky Industrial CyberSecurity.

Installare una soluzione di sicurezza su sistemi che devono essere sempre attivi non è però così semplice. E allora Alperia e Kaspersky decidono di mettere in piedi un gruppo di lavoro congiunto per realizzare il miglior set-up possibile della soluzione.

La collaborazione si rivela la strada giusta da seguire, anche perché in Alperia non era disponibile un ambiente di test e occorreva lavorare direttamente sulle macchine in produzione.

"L'idea di avere una task force con i tecnici di Kaspersky a disposizione in azienda ci ha permesso di customizzare il prodotto cucendolo a misura sulla nostra realtà", spiega Moretti.

Implementazione su misura

Si parte quindi, a fine 2018, con un Proof of Concept: la soluzione KICS for Nodes viene messa in funzione su alcune macchine per diverse settimane.

"Per noi era fondamentale affinare la soluzione sul campo, verificare gli effetti sull'operatività delle macchine e capire quali esclusioni impostare e quali ottimizzazioni fare", racconta Moretti.

"In Alperia tutti i sistemi sono ridondati. Abbiamo quindi installato la soluzione solo su una delle due macchine ridondate – quella principale - per poter avere un backup solido in caso di problemi, senza rischiare impatti sulla produzione in caso di problemi. Abbiamo così potuto fare diversi stress test, che sono stati tutti superati brillantemente".

All'inizio il KICS è stato impostato in modalità monitoraggio. "Volevamo verificare se il nuovo sistema rilevasse eventuali falsi positivi e avesse delle interazioni che potessero rallentare gli applicativi che girano, rischiando di bloccare certi servizi fondamentali. Una volta avuta la sicurezza che il sistema era perfettamente a punto, siamo passati alla piena operatività, consentendo al KICS anche di bloccare automaticamente eventuali servizi sospetti".

"Durante questa fase i nostri tecnici hanno abilitato un logging dell'agente più

Sicurezza
Protezione dei dati industriali
Protezione degli impianti per assicurarne la continuità operativa

Controllo
Tutela delle attività di monitoraggio degli impianti

Prestazioni
Abilitazione delle attività di manutenzione predittiva

approfondito per capire come si comportasse e che interazioni avesse con lo SCADA. Dopo un'attenta analisi dei LOG abbiamo offerto ulteriori informazioni ad Alperia per la configurazione", spiega Diego Magni Pre-Sales Manager di Kaspersky.

Dopo il primo deplyment, la task force ha provveduto a estendere gradualmente la copertura del sistema alle altre macchine e agli altri ambienti (fisici e virtuali). "Oggi abbiamo una quarantina di server protetti dalla soluzione Kaspersky", racconta Moretti. "In meno di sei mesi siamo andati a regime e lo abbiamo fatto per gradi e in tutta sicurezza".

Oltre il rapporto cliente – fornitore

Moretti è visibilmente soddisfatto dei risultati ottenuti e del supporto ricevuto: "Sono convinto che in casi come questo si debba andare oltre il classico rapporto cliente - fornitore e puntare a un rapporto di partnership più esteso. Per questo stiamo prendendo in considerazione l'idea di fare un contratto di service con Kaspersky che vada oltre l'assistenza sul prodotto e si configuri come una fornitura di consulenza su tutto il perimetro della rete", conclude Moretti.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
www.kaspersky.it/enterprise-security/industrial

www.kaspersky.com

kaspersky BRING ON THE FUTURE

2020 AO KASPERSKY. ALL RIGHTS RESERVED. REGISTERED TRADEMARKS AND SERVICE MARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.