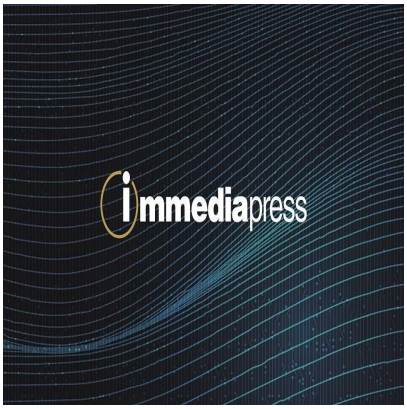

Il â??big bang digitaleâ?? del settore energetico: il 75% si digitalizzerÃ in due anni, ma a quale costo?

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Un recente studio congiunto di Kaspersky e VDC ha rivelato che oltre la metÃ delle aziende del settore energetico ha giÃ subito incidenti informatici con costi superiori a 1 milione di dollari. Questo dato mette in luce i crescenti rischi finanziari e operativi che minacciano le infrastrutture critiche. Con lâ??accelerazione della trasformazione digitale nel settore, la protezione degli ambienti OT sempre piÃ¹ connessi Ã¨ diventata una prioritÃ strategica.

Chiamato a garantire energia affidabile, efficiente e sostenibile, il settore energetico sta intraprendendo la trasformazione piÃ¹ rapida e profonda della sua storia. La destinazione Ã¨ un modello operativo â??completamente digitaleâ?•, ma la velocitÃ di questo percorso presenta un paradosso: le stesse tecnologie che rendono la rete piÃ¹ intelligente e pulita ne ampliano simultaneamente la vulnerabilitÃ alle minacce informatiche.

Lâ??accelerazione digitale dellâ??energia

La portata della trasformazione nel settore Ã¨ straordinaria. Secondo il report congiunto di Kaspersky e VDC, â??Powering Cyber Resilience in the Energy Sectorâ??, meno del 5% delle aziende energetiche puÃ² oggi considerarsi completamente digitale. Eppure, nel giro di soli due anni, questa cifra Ã¨ destinata a esplodere: quasi tre quarti (75%) delle aziende prevede di raggiungere la piena digitalizzazione. Questo â??big bang digitaleâ?? sta ridisegnando generazione, trasmissione e distribuzione, promettendo guadagni senza precedenti in termini di efficienza, affidabilitÃ e sostenibilitÃ .

Tuttavia, la stessa connettivitÃ che consente lâ??ottimizzazione della rete in tempo reale apre nuove porte ai criminali informatici. Le conseguenze si fanno giÃ sentire. La ricerca rivela che oltre la metÃ delle aziende energetiche ha subito incidenti informatici con costi superiori a 1 milione di dollari. Non si tratta semplicemente di una violazione dei dati, ma di una minaccia diretta alla continuitÃ operativa e alla stabilitÃ della rete elettrica.

Cosa guida la digitalizzazione energetica?

Le aziende del settore stanno sfruttando tecnologie avanzate per far fronte allâ??instabilitÃ dei mercati, rispettare le normative e integrare nuove fonti di energia. Gli obiettivi principali, identificati nel report, sono focalizzati sui risultati di business fondamentali:

Per raggiungere questi obiettivi, le aziende del settore energetico stanno adottando tecnologie avanzate come lâ??analisi basata sullâ??IA, i digital twins e gli strumenti di manutenzione predittiva per ottimizzare domanda e offerta, anticipare guasti alle apparecchiature e ridurre le interruzioni non pianificate. Droni automatizzati e robotica migliorano ulteriormente la sicurezza e lâ??efficienza delle ispezioni presso gli impianti di trasmissione e generazione, aiutando gli operatori a migliorare i parametri di affidabilitÃ come SAIDI e SAIFI[1] favorendo al contempo la gestione dinamica della rete e una piÃ¹ agevole integrazione delle risorse energetiche distribuite.

Le sfide umane e tecniche nella sicurezza delle operazioni energetiche

Proteggere la trasformazione digitale del settore energetico Ã¨ una sfida tanto umana quanto tecnologica. Secondo Kaspersky, oltre il 45% delle aziende indica la carenza di personale specializzato in cybersecurity industriale come principale ostacolo. Questa lacuna di competenze lascia i team dei sistemi di controllo sovraccarichi e limita la loro capacitÃ di implementare difese proattive o coordinare una risposta efficace agli incidenti, mentre il pensionamento di ingegneri esperti erode ulteriormente il patrimonio di conoscenze operative critiche.

Allo stesso tempo, una persistente divisione tra IT e operations complica la governance. Mentre i dipartimenti IT gestiscono spesso le politiche di cybersecurity, i team di operations e ingegneria che supervisionano gli ambienti SCADA[2] e i team di operations e ingegneria che supervisionano gli ambienti SCADA e lâ??automazione delle sottostazioni danno prioritÃ alla sicurezza e alla continuitÃ operativa. Quasi tre quarti delle aziende riferisce che la cybersecurity dei sistemi di controllo Ã¨ gestita principalmente dallâ??IT, con meno del 10% che indica una leadership operativa â?? una frammentazione che puÃ² tradursi in prioritÃ disallineate e strategie di protezione incoerenti.

Le conseguenze di una protezione inadeguata delle infrastrutture energetiche

Trascurare la cybersecurity OT nel settore energetico va ben oltre le perdite finanziarie. Un attacco riuscito puÃ² avere conseguenze fisiche e sistemiche immediate, mettendo a rischio lâ??affidabilitÃ della rete, la sicurezza pubblica e la resilienza nazionale.

Lâ??impatto finanziario Ã¨ grave e multidimensionale. Kaspersky conferma che oltre il 50% delle aziende ha subito perdite superiori a 1 milione di dollari per incidente. Questi costi vanno oltre la gestione dellâ??incidente e gli eventuali pagamenti di riscatto. Un attacco ransomware che impedisce agli operatori lâ??accesso ai sistemi potrebbe bloccare la generazione per ore, causando perdite ingenti in termini di produzione energetica e ricavi. Lâ??accesso non autorizzato ai PLC[3] puÃ² causare danni fisici a turbine o trasformatori, innescando costosi cicli di riparazione e prolungati fermi operativi, con una media di 19 ore per violazione.

La risposta strategica: rafforzare la cybersecurity OT nel settore energetico

Per affrontare in sicurezza questo punto di svolta digitale, i leader del settore energetico devono adottare un approccio fondamentalmente diverso alla cybersecurity, che ponga gli ambienti OT al centro del business. Non Ã¨ piÃ¹ sufficiente applicare una sicurezza di livello IT ai sistemi di controllo industriale. La risposta strategica deve invece fondarsi su tre pilastri essenziali:

La trasformazione digitale del settore energetico Ã¨ inevitabile, ma il suo successo dipende dal rendere la cybersecurity OT un abilitatore strategico di affidabilitÃ e resilienza. Con le competenze giuste, i leader del settore energetico possono digitalizzare con fiducia, salvaguardando al contempo le infrastrutture critiche.

Per saperne di piÃ¹ sulle soluzioni Kaspersky per il settore energetico, Ã¨ possibile consultare la pagina dedicata.

[1] Nel settore energetico, il SAIDI (indice di durata media delle interruzioni di rete) e il SAIFI (indice di frequenza media delle interruzioni di rete) sono gli indicatori standard di affidabilitÃ utilizzati dalle aziende di servizi pubblici per misurare le proprie performance.

[2] Il sistema SCADA (Supervisory Control and Data Acquisition) Ã¨ unâ??architettura di controllo che comprende computer, comunicazioni di dati in rete e interfacce grafiche utente per la supervisione di alto livello di macchinari e processi.

[3] Programmable Logic Controllers (PLCs) sono computer industriali rinforzati.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Marzo 16, 2026
Autore
redazione