Accenture. Blackout e hacker, i timori delle utilities per smart grid e reti elettriche

Nel settore delle Utilities il 63 per cento degli executive ritiene che nei prossimi cinque anni il proprio paese possa essere, a vari gradi, esposto al rischio di interruzione dell'erogazione di elettricità a causa di un attacco cibernetico alle reti di distribuzione. Questo dato – che emerge da un nuovo rapporto di Accenture, Outsmarting Grid Security Threats, realizzato nell'ambito del programma di ricerca Digitally Enabled Grid – sale al 76 per cento in Nord America.

L'indagine, svolta su un campione di più di 100 dirigenti di aziende del settore in oltre 20 paesi, evidenzia inoltre che la maggiore preoccupazione a fronte di un attacco informatico sia l'interruzione dell'erogazione di elettricità (il 57 per cento si ritiene molto preoccupato a tale proposito), seguito dalla sicurezza per dipendenti e/o clienti (53 per cento) e dai danni agli asset fisici della rete (43 per cento).

"Il rapido sviluppo di malware sempre più sofisticati e facilmente utilizzabili da cyber criminali costituiscono una chiara minaccia per i sistemi di distribuzione dell'energia elettrica" afferma **Mauro Marchiaro**, Responsabile Settore Energia di Accenture in Italia, Europa Centrale e Grecia. *"In assenza di un'efficace protezione, i ricchi flussi di informazioni trasportati dalle reti digitali potrebbero essere manipolati per causare malfunzionamenti ed interruzioni dell'erogazione di energia elettrica causando disagi, danni economici e commutandosi in una reale minaccia per il paese e l'intera comunità".*

Se da un lato la maggiore connettività dei sistemi di controllo abilitati dalla rete intelligente porterà notevoli benefici in termini di sicurezza, produttività, qualità dei servizi e efficienza operativa, dall'altro l'88 per cento degli intervistati ritiene che la cyber security sia una forte fonte di preoccupazione nello sviluppo delle smart grid.

Inoltre, le utilities sono sempre più esposte alla crescita di dispositivi domestici connessi all'Internet of Things (IoT), quali centraline domestiche e elettrodomestici intelligenti. L'esposizione al rischio introdotto da tali dispositivi in questo settore è difficile da quantificare, tuttavia il 77 per cento degli interpellati ritiene che l'IoT veicoli nuovi potenziali minacce di natura cyber.

In Asia ed in Europa, circa un terzo degli interpellati vede il rischio principale per le attività di distribuzione nelle azioni da parte di cyber criminali. Per il Nord America invece il pericolo maggiore è rappresentato dagli attacchi da parte dei governi (32 per cento).

"Lo sviluppo della rete intelligente e dell'IoT potrebbe aprire nuove vie d'attacco se la Cyber Security non è parte integrante della sua progettazione", aggiunge Marchiaro. "Le reti intelligenti devono essere dotate di meccanismi di protezione molto sofisticati e complessi in grado di evolvere rapidamente nel tempo ed in grado pertanto di adeguarsi al continuo sviluppo di malware; ciò al fine di garantire un miglior controllo ed al contempo una maggior capacità / velocità di risposta nel ripristino della rete in caso di attacchi cibernetici".

Le Utilities devono rafforzare i propri modelli operativi di cyber security e sviluppare un sistema di distribuzione

resiliente

Sono tante le utilities che devono recuperare terreno per sviluppare un sistema robusto di sicurezza informatica, dato che più di 4 interpellati su 10 hanno affermato che i rischi per la cyber security non erano o erano solo parzialmente integrati nei processi di gestione del rischio.

Inoltre, la crescente convergenza fra minacce fisiche e informatiche richiede lo sviluppo di presidi che vanno ben oltre i semplici requisiti nazionali di conformità alla sicurezza. Le utilities devono investire per rendere la loro rete intelligente più resiliente e per sviluppare capacità di reazione e recupero più efficaci.

Data la complessità delle reti di distribuzione elettrica e il numero crescente di hacker sempre più preparati e con grandi risorse finanziarie, molte utilities non sono adeguatamente protette e preparate. Se si guarda alla capacità di riportare alla normalità le attività della rete dopo un cyber attacco, solo il 6 per cento ha affermato di sentirsi assolutamente preparato e il 48 per cento adeguatamente preparato.

"La cyber security deve diventare una competenza distintiva nel settore, proteggendo l'intera catena del valore e l'ecosistema esteso end-to-end. Le utilities, già esperte nel distribuire in modo affidabile l'elettricità e nelle operazioni di ripristino, necessitano di agilità e rapidità nel creare un'adeguata consapevolezza di fronte a un attacco informatico e far leva sulla stessa per intervenire prontamente e proteggere la rete", afferma **Paolo Dal Cin, Responsabile di Accenture Security per Italia, Europa Centrale e Grecia**. *"Lo sviluppo di questa nuova capacità richiederà innovazione costante, oltre a un approccio pratico alla scalabilità e alla collaborazione con i partner per realizzare valore".*

Interventi per costruire e scalare la difesa informatica

Anche se non c’è una sola strada per procedere, ci sono alcuni interventi che ogni utility dovrebbe considerare per rafforzare la resilienza e il responso ai cyber attacchi, fra cui:

- Integrazione della resilienza nella progettazione delle risorse e dei processi, con l’inclusione della sicurezza fisica e informatica;
- Condivisione di dati e informazioni come attività indispensabile per aiutare a creare consapevolezza sul panorama delle minacce informatiche e su come prepararsi di conseguenza
- Sviluppo di modelli di governance della gestione della sicurezza e delle emergenze.

Il programma di ricerca annuale Digitally Enabled Grid di Accenture valuta le implicazioni e le opportunità di una rete sempre più digitale. Lo studio del 2017 contiene interviste con più di 100 dirigenti di utility di oltre 20 paesi. I dirigenti intervistati sono coinvolti nel processo decisionale per le questioni relative alle reti intelligenti. I paesi rappresentati sono Arabia Saudita, Australia, Belgio, Brasile, Canada, Cina, Emirati Arabi Uniti, Filippine, Germania, Giappone, Italia, Malesia, Norvegia, Olanda, Portogallo, Regno Unito, Spagna, Stati Uniti, Sudafrica, Svizzera, Tailandia.

Accenture. Blackout e hacker, i timori delle utilities per smart grid e reti elettriche