Le infrastrutture critiche nazionali stanno cambiando, sono sempre più privatizzate: una protezione Zero trust è fondamentale

Nathan Howe, Global Vice President of Innovation, Zscaler

Le infrastrutture critiche in tutto il mondo sono sempre più privatizzate. Ad esempio, i servizi di comunicazione per i consumatori e quelli satellitari (di cui più della metà sono già privati), i servizi ferroviari o i settori più nuovi ed ecologici come la ricarica dei veicoli elettrici e l'energia solare per uso domestico. Questa situazione accresce la preoccupazione per la sicurezza di questo ecosistema e capire come proteggerlo al meglio è una priorità per i team della sicurezza.

Mentre questi settori industriali continuano a crescere e ad evolversi in modi inaspettati, una cosa è certa: per proteggerli, devono prima essere identificati e definiti. È urgente comprendere meglio l'ampiezza e la profondità delle infrastrutture critiche nazionali di un Paese, delineare la loro definizione e decidere quali nuove infrastrutture richiedono una "protezione prioritaria".

Cosa si intende per infrastrutture prioritarie?

Nell'aprile 2023, il governo britannico ha aggiornato la definizione e la categorizzazione dell'infrastruttura critica nazionale, riportandola come *"l'insieme di quegli elementi critici dell'infrastruttura - vale a dire risorse materiali, i servizi, i sistemi di tecnologia dell'informazione, le reti e i beni infrastrutturali o processi e i lavoratori essenziali che li gestiscono - che, se danneggiati o distrutti, causerebbero gravi ripercussioni alle funzioni cruciali della società, tra cui: un forte impatto negativo sulla disponibilità, l'integrità o l'erogazione di servizi essenziali - compresi quei servizi la cui integrità, se compromessa, potrebbe portare a una significativa perdita di vite umane o vittime - tenendo conto di conseguenze economiche o sociali significative; e/o un impatto significativo sulla sicurezza nazionale, sul sistema di difesa nazionale o sul funzionamento dello Stato*". Attualmente, i settori delle infrastrutture nazionali sono tredici e comprendono le comunicazioni, l'energia, i trasporti e l'acqua, solo per citarne alcuni.

In modo simile, in Germania, un'infrastruttura viene considerata "critica" *ogni qualvolta sia di "grande importanza per il funzionamento delle società moderne e qualora un guasto o degrado comporterebbe interruzioni durature del sistema nel suo complesso".* È importante notare che nel 2015 il Ministero federale tedesco dell'interno, dei lavori pubblici e della patria ha espresso preoccupazione per la crescente importanza della dimensione informatica delle infrastrutture critiche e per la crescente necessità di protezione dagli attacchi contro le tecnologie dell'informazione. Lo stesso anno è stato approvato l'IT security Act, che ha posto le basi per tale protezione. Nell'ambito di questa legge, gli operatori delle infrastrutture critiche a cui si applica *"devono dimostrare all'Ufficio federale per la sicurezza delle informazioni (BSI) di soddisfare gli standard di sicurezza informatica e devono inoltre segnalare a tale ufficio gli incidenti di sicurezza informatica".*

Requisiti di questo tipo, con una focalizzazione particolare sull'aspetto informatico, sono applicati anche nella maggior parte delle nazioni europee. Tuttavia, mentre molti Paesi si sono concentrati sull'identificazione dei settori critici per proteggerli meglio dal panorama delle minacce informatiche in costante evoluzione, altri non hanno ancora seguito l'esempio. L'assenza di una standardizzazione globale comporta una mancanza di protezione e di unificazione coerente e, di conseguenza, maggiori opportunità per gli hacker di approfittarne e di scatenare il caos in modo esponenziale.

Un aspetto di questa conversazione, oggi più importante che mai, è il rischio che deriva dall'espansione dell'innovazione. Le infrastrutture critiche più obsolete e tradizionali, come l'industria chimica e il settore dell'energia nucleare ad uso civile, sono fortemente protette da difese fisiche per

tenere lontani gli intrusi. Tuttavia, i settori più nuovi, come quello della ricarica dei veicoli elettrici e dell'energia solare, non possono permettersi lo stesso lusso, e la loro protezione viene in un secondo momento. Poiché molte di queste nuove tecnologie vengono sviluppate per essere utilizzate direttamente dal pubblico, le soluzioni di cybersecurity sono l'unica alternativa ai muri fisici e alle serrature che possono impedirne la compromissione.

Il pericolo potenziale dell'innovazione

Analizzando più da vicino i sistemi di ricarica per veicoli elettrici, la tecnologia stessa è accessibile e si trova nei piazzali delle stazioni di servizio o in aree meno protette, dove il pubblico può facilmente accedere e mettere a rischio la sicurezza. In questo caso, i rischi di violazione vanno da persone che semplicemente ne approfittano e sono alla ricerca di un accesso Internet, a coloro che cercano di violare i sistemi di pagamento. Poiché le stazioni di ricarica per veicoli elettrici possono fisicamente manipolate e aperte con facilità, rappresentano un rischio significativo per le più ampie infrastrutture critiche nazionali a cui sono collegate e con cui interagiscono, come le reti elettriche, i sistemi finanziari e internet.

Queste porte di ricarica per veicoli elettrici, a livello di base spesso offrono agli utenti la possibilità di navigare sul web grazie a una connessione Wi-Fi. Questo significa, in teoria, che gli utenti potrebbero manipolare i terminali di pagamento o accedere a siti pericolosi che comportano rischi specifici. Quando si perdono i controlli fisici, le basi della sicurezza informatica sono fondamentali per limitare il vettore d'attacco. Riprendere il controllo informatico una volta perso è una delle lotte più difficili per il settore informatico.

Un altro esempio attuale è rappresentato dai pannelli solari. Nonostante la sua importanza per la società moderna, il settore dell'energia si è adattato più lentamente di altri alla tecnologia digitale a causa delle sue dimensioni complessive e della necessità di un'elevata disponibilità del sistema. Questo aspetto si riflette nella legislazione di tutto il mondo, dove le reti elettriche sono classificate come uno degli elementi più critici.

La crescente popolarità delle alternative più ecologiche all'energia tradizionale ha portato a un aumento delle energie rinnovabili, dai parchi eolici off-shore alla creazione di energia solare da parte di una singola abitazione. Questo crescente utilizzo della tecnologia digitale richiede maggiori funzionalità di rete e, soprattutto, collega componenti precedentemente isolati a reti di comunicazione più ampie. Ciò li rende sempre più esposti a reti esterne come Internet, con un conseguente ampliamento della superficie di attacco.

Naturalmente, con queste nuove soluzioni, come i sistemi fotovoltaici domestici, i loro sistemi non sono controllati così strettamente come quelli delle aziende di energia nazionali. Di conseguenza, l'hardware e il software possono essere identificati dai criminali informatici che possono prendere il controllo dell'energia reimmessa nella rete e causare danni considerevoli anche quando controllano una quantità di energia relativamente piccola, sfruttando l'effetto a cascata. In definitiva, sfruttando questo meccanismo, un criminale informatico potrebbe causare blackout a livello di sistema, con un impatto sulla distribuzione e sulla trasmissione dell'energia elettrica su scala nazionale.

Chi ha il compito di proteggere l'infrastruttura nazionale?

A causa della crescente posta in gioco, ci si interroga sempre di più su chi abbia la responsabilità di proteggere il panorama infrastrutturale in continua evoluzione e crescita. Che si tratti di governi, aziende o singoli individui, è importante che la parte o le parti responsabili trovino il giusto equilibrio tra innovazione e normative. In Germania e in altri Paesi europei, la protezione delle infrastrutture

critiche nazionali è definita come un compito che deve essere svolto congiuntamente da governo, aziende, operatori e anche dalla società civile. Tuttavia, su scala globale, per evitare potenziali catastrofi in futuro, i Paesi devono impegnarsi ad agire ora per creare basi sicure su cui la società moderna possa prosperare, senza il rischio incombente di minacce informatiche.

Una soluzione Zero Trust

Per proteggere le infrastrutture critiche nazionali dai pericoli informatici legati alla privatizzazione e all'innovazione rapida senza regolamentazione ci sono tre fasi fondamentali da seguire e il modello Zero Trust è stato progettato per gestirle tutte e tre. In primo luogo, la visibilità dei rischi, in secondo luogo, l'identificazione dei dati critici che devono essere protetti e, infine, l'implementazione della protezione per tali dati. Come soluzione, Zero Trust può offrire a Paesi, governi e aziende una visione del panorama dei rischi che si trovano ad affrontare, oltre a creare i giusti percorsi per proteggersi.

Più granulare può essere la protezione informatica, meglio è. Probabilmente, la lezione più importante per i responsabili della protezione delle infrastrutture critiche nazionali è l'importanza di implementare la giusta strategia infrastrutturale fin dall'inizio. Essere sicuri fin dall'inizio, prima che si verifichi la violazione, è il modo più sicuro per salvaguardare l'infrastruttura, soprattutto perché il mondo ha bisogno di una regolamentazione globale o nazionale sulla sicurezza di questi settori nuovi e sempre più privatizzati.

A proposito di Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange protegge migliaia di clienti da attacchi informatici e dalla perdita di dati collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata su SSE, è la più grande piattaforma di sicurezza cloud in line del mondo.

Per ulteriori informazioni:

Tania Acerbi e Monica Fecchio

Prima Pagina

Piazza Giuseppe Grandi 19 - 20129 Milano

e-mail: tania@primapagina.it

e-mail: monica@primapagina.it