ARP GUARD by ISL

WHITEPAPER

ZERO-TRUST
Network Access

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

FIDARSI È BENE, ZERO-TRUST È MEGLIO

UN CONCETTO DI SICUREZZA INFORMATICA RESILIENTE

I modelli di sicurezza tradizionali localizzano i potenziali aggressori solitamente al di fuori dai confini della propria rete, trascurando così le vulnerabilità causate da componenti o diritti di accesso che agiscono all'interno della rete stessa.
Le strategie di sicurezza che proteggono le aziende dalle minacce provenienti principalmente dall'esterno non possono più far fronte in maniera adeguata alle attuali sfide del cybercrimine come il Social Engineering ed il Phishing.
L'aumento degli attacchi originati dall'interno della rete richiede l'adozione di ulteriori livelli di sicurezza, ovvero contromisure olistiche e resilienti che possano reagire in modo mirato a queste minacce.

ZERO-TRUST NETWORK ACCESS

La soluzione Network Access Control ARP-GUARD di ISL GmbH dal 2003 contribuisce a perseguire un approccio di sicurezza fondamentale, che oggi ricopre un ruolo di rinnovata importanza.
La soluzione ARP-GUARD NAC controlla costantemente tutti gli accessi e identifica in modo univoco ogni dispositivo prima che acceda alla rete e alle risorse aziendali. Tale approccio è ora ampiamente conosciuto come „Zero-Trust Network Access (ZTNA)".

MAI FIDARSI - CONTROLLARE SEMPRE

Secondo questo principio fondamentale di sicurezza nessun dispositivo è per principio sicuro, anche se si trova all'interno della rete. Di conseguenza, ogni tentativo di accesso viene costantemente controllato e protocollato - l'accesso è concesso solo dopo l'avvenuta autenticazione.
ARP-GUARD contribuisce alla realizzazione del concetto Zero Trust resiliente incidendo su due elementi costitutivi fondamentali, ovvero i Device e il Network.

ARP-GUARD rende visibili tutti gli asset che si trovano in rete in maniera istantanea, garantendo la totale trasparenza e di conseguenza la massima protezione dalle minacce.

ARP-GUARD offre un pacchetto completo di regole attraverso le quali è possibile definire le linee guida che regolano il network. Le regole sono definite dall'amministratore e applicate integralmente in tutta l'infrastruttura aziendale. È così possibile controllare chi ha accesso e a quali risorse, rendendo così molto più facile proteggere i dati e le risorse sensibili da accessi non autorizzati.

Monitorando continuamente l'attività di rete, ARP-GUARD fornisce una panoramica di tutto ciò che nella rete accade in tempo reale. Gli accessi indesiderati e le anomalie rilevanti possono essere identificati in modo immediato, incrementando così il livello di sicurezza della rete.

La micro-segmentazione della rete limita la libertà di movimento di un potenziale attaccante. La diffusione e i conseguenti danni causati da una minaccia risultano pertanto drasticamente ridotti e controllabili. L'assegnazione ad una VLAN viene eseguita in maniera dinamica dal VLAN Management di ARP-GUARD; inoltre è possibile definire specifiche regole di sicurezza per ogni specifico segmento in maniera altamente granulare.

Prima di consentire l'accesso alla rete ad un dispositivo, ARP-GUARD Endpoint controlla se esso soddisfa i requisiti predefiniti, come conformità o requisiti di sicurezza.

ARP-GUARD identifica in modo univoco ogni dispositivo prima che acceda alla rete. L'autenticazione attraverso la procedura del Fingerprinting protegge da manipolazioni quali MAC-Spoofing e ARP-Poisoning.

COME PUÒ ESSERE DEFINITO IL CONCETTO ZERO TRUST?

Zero Trust può essere definito come la costruzione di una architettura nella quale le connessioni non avvengono mai in virtù della fiducia ma al contrario a seguito di una verifica. In questo contesto si presuppone che un attore malevolo sia sempre attivo.
Questo punto di vista conduce a realizzare ambienti di sistema altamente flessibili e dotati di elevata affidabilità, che meglio rispondono alle esigenze delle moderne postazioni di lavoro.

Fonte: www.gartner.com