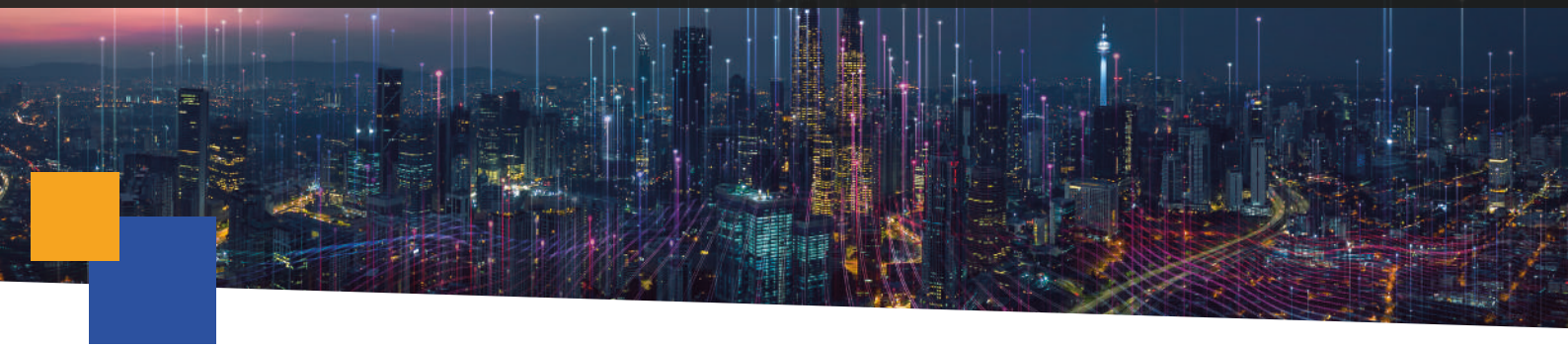
ALFAGROUP



CORPORATE NETWORK AIRSPACE

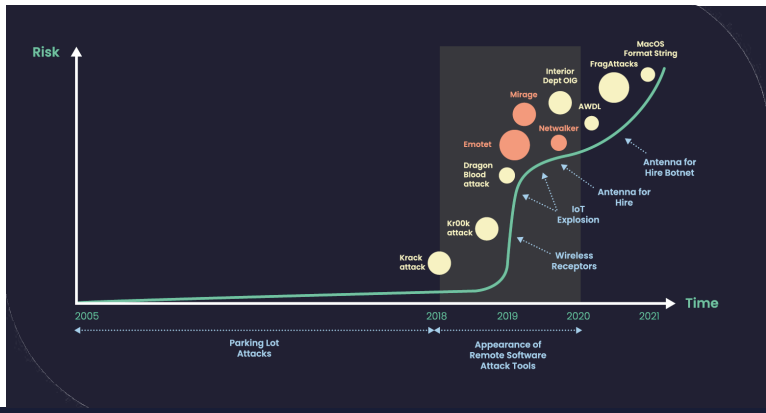
LA PIU' AMPIA SUPERFICIE DI ATTACCO NON PROTETTA E NON CONTROLLATA DELLA TUA RETE

La rete aziendale può essere, intenzionalmente o meno, compromessa da Antenna for Hire™ - qualsiasi dispositivo wireless non sotto il controllo dell'azienda, ma posto nelle sue vicinanze - con conseguente accesso non autorizzato alla rete, dirottamento del dispositivo o perdita di dati. AirEye assicura il rispetto della politica di sicurezza wireless e previene gli attacchi che sfruttano l'Antenna for Hire™ che sta trasmettendo nello spazio aereo della rete aziendale.

LE SFIDE DEL "NETWORK AIRSPACE":

Il numero di attacchi effettuati sfruttando le reti wireless è in forte e costante crescita dal 2019. Il rischio non riguarda solo le tradizionali reti Wi-Fi: il crescente utilizzo di dispositivi IoT, la possibilità di connettere alla rete i dispositivi più disparati (stampanti, TV, webcam, ...) hanno ampliato esponenzialmente la superficie di attacco.

Le vulnerabilità possono nascondersi anche al di fuori del perimetro IT; la vicinanza ad apparecchiature di terze parti, inevitabile soprattutto nei contesti urbani, ovunque ci sia una forte concentrazione di aziende o semplicemente nei luoghi pubblici, ha reso possibile l'emergere di fenomeni come l'Antenna for Hire, attraverso cui un attaccante mette a disposizione un Access Point malevolo con l'intento di prendere il controllo di un endpoint aziendale. L'adozione dello smart working, a cui la pandemia ha dato una spinta da cui difficilmente si tornerà indietro negli anni a venire, ha reso necessario dotare molti più dipendenti di laptop, tablet o smartphone con capacità di connessione wireless; questi vengono utilizzati a casa ma anche in luoghi aperti al pubblico, interagendo con reti wi-fi sconosciute ed eventualmente costituendo un pericolo una volta riportati in azienda.



RISCHI E LIMITAZIONI DELLA TECNOLOGIA ATTUALE:

I firewall, gli IDS/IPS e le soluzioni di Network Access Control sono essenziali per monitorare l'accesso alle reti aziendali. Pur essendo in grado di controllare e bloccare i tentativi di accesso alla rete interna, non riescono a intercettare quei dispositivi interni che possono connettersi a reti estranee, aggirando efficacemente le regole di sicurezza aziendali.

Gli endpoint o i dispositivi che si connettono a punti di accesso malevoli e sono contemporaneamente connessi alla rete cablata aziendale costituiscono porte d'ingresso attraverso le quali un attaccante può muoversi liberamente all'interno della rete aziendale.

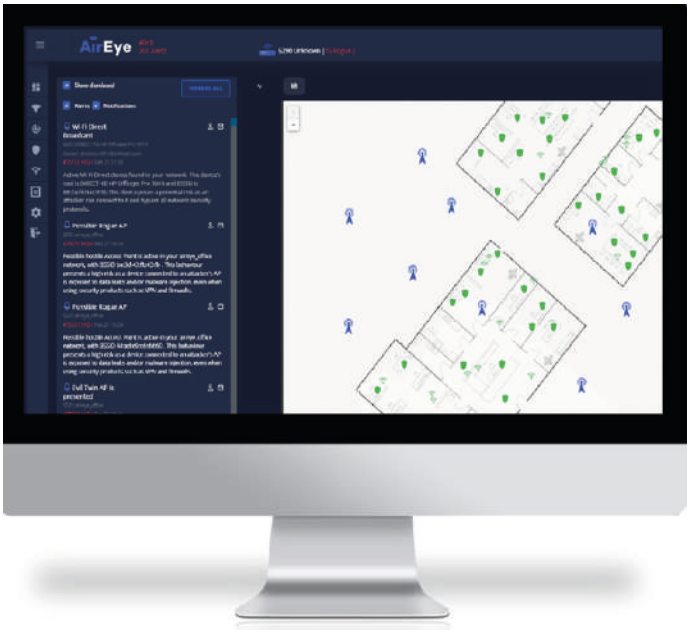
Le organizzazioni sono esposte ad un rischio concreto di esfiltrazione di informazioni strategiche, brevetti e proprietà intellettuale, non intercettata dai sistemi di sicurezza implementati (es. DLP). Inoltre, nel caso dell'industria manifatturiera, l'accesso alla rete da parte di un attaccante esterno gli consentirebbe di agire sui dispositivi IoT che regolano i processi produttivi, danneggiandoli e bloccandoli. Allo stesso modo, per i dispositivi dotati di funzioni di connessione P2P (es. stampanti con protocolli WiFi Direct, TV, ecc.) esistono policy e procedure operative, ma mancano efficaci strumenti di controllo continuo.

LA SOLUZIONE **ALFA GROUP:** **AIREYE DOME**

AirEye, leader nel Network Airspace Control and Protection (NACP), ha sviluppato una soluzione che aiuta le organizzazioni ad ottenere visibilità, controllo e protezione del loro Network Airspace, garantendo un livello di resilienza con la stessa affidabilità, garanzia e sicurezza che esiste per le reti cablate.

La soluzione SaaS è zero-touch, non intrusiva e necessita del dispiegamento di antenne, dalla lunghezza totale di 25 cm in corrispondenza degli Access Point aziendali, che richiedono solo l'alimentazione e l'accesso a internet per essere immediatamente operative. Attraverso la console cloud è possibile visualizzare la situazione in tempo reale e gestire le policy e gli eventi rilevati.

COME FUNZIONA:



1.MONITORAGGIO

Monitora costantemente e analizza tutti i canali di comunicazione wireless che trasmettono nel tuo spazio aereo aziendale, in tempo reale.

2. IDENTIFICAZIONE

Identifica le risorse aziendali e i canali di comunicazione, e classifica i diversi tipi di dispositivi e reti intorno al canale.

3. CONTROLLO

Rileva le violazioni della politica di sicurezza wireless aziendale e termina automaticamente qualsiasi potenziale connessione tra i dispositivi coinvolti.

4. PREVENZIONE

Rileva le interazioni maligne e termina l'attacco.

5. REPORTING

Comunica ai vertici aziendali e all'area Operations le violazioni di policy prevenute e gli attacchi digitali bloccati per via aerea.

COME AFFRONTARE I RISCHI DI SICUREZZA DEL CORPORATE NETWORK AIRSPACE:

ACCESSO NON AUTORIZZATO ALLA RETE AZIENDALE

Dispositivi con doppia connettività si connettono sia a reti non monitorate e non autorizzate, sia alla rete aziendale.

- Impedisci qualsiasi accesso wireless non autorizzato a un dispositivo con doppia connessione
- Ricevi visibilità sui dispositivi che stanno trasmettendo Wi-Fi Direct, Mobile Hotspot e AWDL, individuando tutti i dispositivi connessi tramite queste tecnologie
- Ricevi visibilità sui dispositivi che stanno utilizzando la condivisione di file, AirDrop, Feem e lo streaming multimediale, individuando tutti i loro dispositivi simili
- Identifica le reti wireless con configurazioni non sicure
- Individua le reti abilitate WPS
- Rileva gli hotspot wireless gestiti da utenti autorizzati e non autorizzati
- Proteggi la tua rete da FragAttacks
- Previeni gli attacchi malware di diffusione wireless come Emotet

FURTO DI RETE O DEVICE

L'attaccante utilizza un Antenna for Hire™ nelle vicinanze dell'azienda e lo trasforma in un Access Point (AP) sotto il suo controllo

- Rileva i rogue e gli AP "Evil Twin".
- Rileva l'SSID-Squatting
- Impedisci ai dispositivi aziendali di connettersi agli AP malevoli o agli Evil Twin
- Previeni gli attacchi captive portal/ AP splash screen/ Pineapple evil portal
- Proteggi da attacchi FragAttacks
- Previeni lo sfruttamento wireless dei dispositivi tramite attacchi come Ripple20 o Amnesia33

DATA LEAKAGE

Dati aziendali che lasciano la rete aziendale sicura attraverso un canale di rete non supervisionato

- Rileva i dispositivi aziendali che si collegano a reti non monitorate (Guest o qualsiasi rete esterna)
- Rileva i dispositivi aziendali che si collegano a reti non autorizzate
- Previeni le violazioni involontarie dei criteri wireless da parte di dipendenti legittimi
- Previeni l'esfiltrazione malevola di dati
- Proteggi da FragAttacks

IL VALORE DELLA SOLUZIONE

Da un punto di vista strategico, la soluzione consente di:

Migliorare la progettazione e la sicurezza della Corporate Network Airspace.

Supportare il team di incident Response attraverso l'arricchimento dei playbook SOAR/SIEM.

Sviluppare una visibilità analitica di tutte le connessioni Wireless che consenta di identificare, analizzare, investigare e gestire le nuove minacce che colpiscono dipendenti, sistemi aziendali e partner dell'organizzazione.

Sopperire alla mancanza introdotta dalle attuali tecnologie di sicurezza, che non consentono di adottare l'approccio Cyber Kill-Chain per le reti wireless, così come avviene per le reti wired, attraverso le automazioni dei controlli e delle funzioni di prevenzione.

Supportare le attività di Data Breach Investigation attraverso l'utilizzo di dati reali e storici necessari al team di Incident Response per garantire l'efficace capacità di risposta agli incidenti cyber.

PERCHÈ ALFA GROUP

- **ATTENZIONE ALL'INNOVAZIONE**
  Il nostro team mantiene uno sguardo costante sull'evoluzione tecnologica, non solo per individuare le migliori soluzioni dei grandi vendor, ma anche per scoprire approcci nuovi ed innovativi con cui rispondere alle necessità dei nostri clienti.
- **PARTNERSHIP ESCLUSIVE**
  La soluzione Network Airspace Security del nostro partner AirEye è attualmente l'unica sul mercato a garantire la protezione dagli attacchi aerei effettuati catturando gli endpoint aziendali.
- **APPROCCIO CUSTOMER-CENTRIC**
  Lavoriamo al fianco dei nostri Clienti, comprendendo a fondo le necessità della loro organizzazione ed individuando la soluzione più efficace per soddisfarle.
- **SOLUZIONI END-TO-END**
  Combiniamo competenze tecnologiche e consulenziali altamente specializzate con una conoscenza trasversale sui diversi ambiti di Rischio Digitale. Questo ci permette di offrire ai nostri clienti soluzioni end-to-end puntuali e complete, e di seguirli in tutte le fasi del progetto, dall'ideazione alla delivery.

VUOI SAPERNE DI PIÙ?

SCOPRI LA SOLUZIONE CON UNA PROOF OF VALUE GRATUITA DI DUE SETTIMANE

CONTATTI:

info@alfagroup.it
www.alfagroup.it