



Maggiore sicurezza in soli due giorni: gli enti locali italiani si affidano alla sicurezza delle reti tedesche

Trani è – una cittadina dell'Italia meridionale con una popolazione di circa 60.000 persone. Si trova in Puglia, nella provincia di Barletta-Andria-Trani. L'ottima reputazione dell'azienda tedesca macmon secure GmbH è giunta anche in Italia, dove l'ingegnere e CIO Valerio Catino, che sovrintende al settore informatico -di 250 dipendenti comunali, ha contattato Bludis, distributore esclusivo di macmon in Italia.

La sfida: proteggere la rete informatica da attacchi interni ed esterni e rendere più efficienti i processi amministrativi legati alla gestione delle VLAN nel reparto IT.

macmon Network Access Control: soluzione perfetta per le Pubbliche Amministrazioni

Nell'ambito della selezione di una soluzione affidabile per il controllo dell'accesso alle reti (NAC, Network Access Control), macmon secure GmbH si è classificata tra le migliori aziende grazie alla vasta esperienza acquisita nel settore della pubblica amministrazione. Uno dei principali obiettivi del *Comune di Trani* è creare un sistema di difesa efficace contro gli attacchi non autorizzati alla rete governativa.

La pubblica amministrazione di Trani gestisce dati altamente sensibili dei propri cittadini, un obiettivo redditizio per i **cyber criminali**. Gestisce, inoltre, informazioni su **infrastrutture critiche**, compresi i dati sui fornitori di energia e sul sistema di trasporto pubblico, nonché documenti di gara e pianificazione.

Dopo aver scelto di affidarsi agli esperti di sicurezza informatica di macmon secure, il comune è riuscito a integrare la soluzione NAC in soli due giorni. All'inaugurazione, Valerio Catino, responsabile del reparto IT del *Comune di Trani*, ha dichiarato: „La soluzione NAC di macmon permette ai nostri amministratori di sistema di monitorare efficacemente i dispositivi collegati alla rete e il numero approssimativo di PC, stampanti, computer portatili e dispositivi tecnici in uso in qualsiasi momento. Il sistema NAC di macmon rileva, segnala e impedisce il funzionamento di sistemi di terzi nella rete interna del nostro ente pubblico. In questo modo possiamo proteggere il nostro sistema informatico da attacchi aiuti personali sensibili.“

Il sistema NAC di macmon permette di visualizzare in tempo reale la topologia dell'intera rete e di eseguire la mappatura di tutte le connessioni tra i dispositivi in rete presenti nell'infrastruttura. Questa preziosa panoramica è stata messa a disposizione del team IT di Trani subito dopo l'integrazione, consentendogli di individuare, ad esempio, configurazioni errate, dispositivi sconosciuti e vulnerabilità, garantendo così la massima stabilità e sicurezza della rete.



La città portuale di Trani che si trova sulla costa pugliese, il tacco dello "stivale" italiano, conta 60.000 abitanti.



„Grazie al sistema NAC di macmon, possiamo garantire l'integrità della rete consentendo l'accesso esclusivamente a dispositivi già definiti e autorizzati.“

Catino Valerio, Chief Information Officer *Comune di Trani*



Il Comune di Trani è la prima città in Italia ad aver affidato completamente la sicurezza dell'infrastruttura comunale a macmon secure.

Come soluzione di sicurezza **indipendente dal produttore**, macmon garantisce un monitoraggio affidabile anche per reti con diversi componenti. Poiché le modifiche alle strutture di gestione e alle procedure di gara possono creare sistemi e infrastrutture informatiche eterogenee nella pubblica amministrazione, l'indipendenza

produttori e server VMware virtuali) può continuare a essere utilizzata nella sua forma attuale senza problemi. In caso di modifiche, l'insieme di regole, le funzioni automatizzate e i processi in background fanno in modo che non sia necessario adottare misure supplementari nel sistema NAC di macmon. Questo rappresenta un grande vantaggio soprattutto nel campo della pubblica amministrazione, dal momento che i distretti amministrativi e le strutture organizzative spesso cambiano con la fine della legislatura.

L'approvazione rapida e mirata degli endpoint riduce notevolmente i costi amministrativi

Il secondo obiettivo del *Comune di Trani* è quello di prevenire l'uso di dispositivi non autorizzati. Adesso è possibile autorizzare i dispositivi degli ospiti e dei dipendenti (BYOD, Bring Your Own Device) in modo semplice e sicuro tramite il portale guest grazie a una gestione dinamica dei segmenti di rete.

QUALI OBIETTIVI HA RAGGIUNTO IL COMUNE DI TRANI UTILIZZANDO IL NAC DI MACMON?

- ✓ Protezione della rete da accessi indesiderati da parte di dispositivi non autorizzati
- ✓ Gestione intelligente e dinamica dei dispositivi guest esterni e dei dispositivi dei dipendenti (BYOD)
- ✓ Affidabilità ottimizzata della rete
- ✓ Bassi costi amministrativi
- ✓ Gestione centralizzata di tutti gli switch di rete
- ✓ Monitoraggio semplice della rete
- ✓ Visibilità e controllo su tutti i dispositivi della rete
- ✓ Gestione in tempo reale dell'inventario IT
- ✓ Elevata flessibilità e affidabilità
- ✓ Implementazione e gestione di concetti VLAN dinamici e statici
- ✓ Relazioni efficaci, orientate all'utente ed efficienti per l'audit
- ✓ Analisi forense degli eventi legati alla sicurezza
- ✓ Controllo dell'accesso alla rete semplice e veloce
- ✓ Applicazione delle politiche di conformità
- ✓ Integrazione con altre soluzioni di sicurezza esistenti
- ✓ Supporto in loco da parte del partner italiano Bludis
- ✓ Concessione di licenza semplificata
- ✓ Buon rapporto qualità-prezzo



dal produttore e la possibilità di **integrare facilmente** soluzioni di sicurezza già esistenti, in questo caso WatchGuard, ha rappresentato un fattore decisivo nella scelta da parte delle autorità comunali.

Per poter controllare le reti moderne in modo totale, una soluzione NAC deve essere in grado di supportare tutte le **tecnologie di autenticazione**: non tutti i provider offrono la possibilità di usufruire di questa funzionalità o di un funzionamento misto con tecnologie come 802.1X e SNMP. Il sistema NAC di macmon non solo supporta queste funzioni, ma offre anche la scalabilità con la rete. L'infrastruttura esistente (l'amministrazione comunale gestisce il proprio centro dati con endpoint di diversi

La molteplicità di endpoint diversi, come notebook o tablet di vari produttori, non rappresenta un problema per il NAC di macmon anche quando si tratta di gestire dispositivi guest, poiché l'autenticazione avviene tramite il server **macmon RADIUS** basato sull'indirizzo MAC univoco.

Il *Comune di Trani* integra il sistema di controllo dell'accesso alla rete con un **portale guest** che consente l'accesso temporaneo e limitato anche da parte di endpoint di terzi, mentre finora i dispositivi guest dovevano essere gestiti dal reparto informatico. Ora le identità guest appropriate possono essere preparate da altri membri del personale tramite il portale guest e i dipendenti possono registrare i propri dispositivi in maniera autonoma



Il "Castello svevo normanno" è una fortezza fatta costruire nel secolo XIII da Federico II di Svevia. Il compito della fortezza era quella di proteggere la città dai nemici. Oggi, la tecnologia NAC dell'azienda di Berlino protegge la rete comunale dagli attacchi dei "nemici".

in base a criteri specifici. Delegare la gestione dei dispositivi degli ospiti e dei dipendenti in questo modo riduce notevolmente il carico di lavoro del reparto informatico.

Valerio Catino aggiunge: „Fornire un accesso a internet dedicato e limitato nel tempo ai visitatori senza bisogno di creare infrastrutture separate per dipendenti e ospiti ci permette di risparmiare risorse e di ridurre il carico di lavoro per i nostri dipendenti. Grazie al sistema NAC di macmon, possiamo garantire **l'integrità della rete** consentendo l'accesso esclusivamente a dispositivi già definiti e autorizzati.“

IL NOSTRO DISTRIBUTORE TECNOLOGICO IN ITALIA



BLUDIS VALUE
ADDED
DISTRIBUTOR

Il distributore italiano a valore aggiunto Bludis

vanta oltre 20 anni di esperienza nella vendita di soluzioni informatiche e di telecomunicazione e offre un'ampia gamma di servizi a valore aggiunto per rivenditori, integratori di sistemi, fornitori di servizi internet e clienti finali. L'azienda, che collabora da anni con macmon secure GmbH, è leader nella distribuzione di soluzioni tecnologiche in Italia e offre soluzioni nei settori della comunicazione, della sicurezza informatica, della gestione IT, del cloud computing e dell'IoT.

Maggiori informazioni: www.bludis.it



FOCUS SUGLI ATTACCHI INFORMATICI IN ITALIA NEL 2018

Pubblicato dal Dipartimento di ricerca statistica il 13 marzo 2020:

Nel 2018, le aree più vulnerabili delle imprese colpite sono state quelle legate all'identificazione, all'autenticazione e al **controllo degli accessi**, mentre il 41% degli attacchi ha riguardato l'accesso non autorizzato ai sistemi TIC.

VMware Carbon Black ha condotto uno studio sulla sicurezza informatica nell'aprile 2020, intervistando 255 fra CIO, STO e CISO italiani. Secondo quanto emerge dallo studio, il 99% delle aziende intervistate ha dichiarato di aver subito attacchi informatici negli ultimi 12 mesi, e il 68% ha ammesso di avere subito una violazione due o più volte l'anno. Lo studio rivela che gli attacchi informatici sono diventati molto più sofisticati, mentre il 99% degli interpellati afferma di voler aumentare la spesa per le difese informatiche. Altre importanti ricerche condotte da Exprivia rivelano

che il numero degli attacchi informatici in Italia è cresciuto enormemente durante l'emergenza coronavirus, con un aumento del 59% della violazione dei dati. In base ai risultati della ricerca, il numero di attacchi informatici è raddoppiato tra gennaio e aprile 2020. Un'analisi di oltre 30 fonti pubbliche di informazione evidenzia che il 50% degli attacchi hanno avuto luogo nel mese di aprile. Education, Finanza e Sanità i settori più colpiti sull'onda del coronavirus e della crescita dello smart working, della didattica digitale e della connettività.

FONTE: <https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-in-italia-picco-di-attacchi-hacker-durante-il-lockdown/> (disponibile solo in italiano)

Contatto macmon secure GmbH | Alte Jakobstraße 79 - 80 | 10179 Berlin | Germania | Tel.: +49 30 23 25 777-0 | nac@macmon.eu | www.macmon.eu