CASE STUDY

L'Università degli Studi di Napoli Federico II Mette in Sicurezza la Propria Rete con il Supporto di Fortinet

L'Università degli Studi di Napoli Federico II, fondata nel 1224, è la più antica università pubblica del mondo e la terza in Italia per numero di iscritti. È, difatti, un mega-Ateneo ed è considerata una delle migliori Università in Italia, tra l'altro nota nel mondo per la rilevante attività di ricerca. Vanta uno staff accademico di oltre 2.600 docenti, uno staff amministrativo di oltre 3.000 dipendenti e un numero di studenti iscritti che supera i 70.000. L'Università è composta da quattro scuole, ventisei dipartimenti, numerose strutture di varia natura e 56 centri di Ateneo, tra cui il CSI, il Centro di Ateneo per i Servizi Informativi, che eroga servizi e fornisce le infrastrutture informatiche e telematiche a supporto delle attività amministrative, didattiche e di ricerca dell'Ateneo e garantisce l'implementazione, la manutenzione e il presidio delle tecnologie informatiche e telematiche dell'Ateneo, quale punto di raccordo trasversale alla pluralità di strutture e servizi.

La Federico II conta, attualmente, oltre 30 sedi distribuite tra la città metropolitana di Napoli e le altre province campane (Avellino, Bellizzi, etc.). Nel corso dell'anno 2022, inoltre, è stata inaugurata una nuova sede nel quartiere di Scampia, laddove prima sorgeva la "Vela H", sede del CdL in Infermieristica, ampliando così la copertura sul territorio anche in zone solitamente definite come periferiche.

In tale contesto viene gestita la rete tematica della Federico II, che consta di cinque nodi principali collegati su fibra dark (IRU): Monte Sant'Angelo (MSA), Centro Storico (CS), Ingegneria (ING), Policlinico (Poli) e infine il Polo San Giovanni a Teduccio (SGAT). L'Ateneo è, inoltre, membro fondante della comunità GARR (Gruppo per l'Armonizzazione delle Reti per la Ricerca) ed è, pertanto, in carico al CSI anche la gestione del POP GARR, il punto di accesso alla rete nazionale della ricerca che garantisce alle strutture collegate e agli utenti un servizio di connettività all'avanguardia per l'ampiezza di banda disponibile, per la qualità del portafoglio servizi e per un efficace supporto alle attività di ricerca e formazione su tutto il territorio nazionale.

Il traffico generato è chiaramente elevatissimo (basti pensare che gli utenti giornalieri sono circa 20.000/25.000 e le sessioni al secondo superano il milione e mezzo) e la necessità di proteggere efficacemente il network dal rischio di attacchi informatici è, nel corso del tempo, diventata sempre più stringente.

Proteggere la rete: un'esigenza imprescindibile

Le sfide a cui l'Università Federico II intendeva rispondere erano sostanzialmente due: la mancanza di visibilità che portava all'incapacità di proteggere adeguatamente la rete, e la sostanziale complessità dell'infrastruttura, nello specifico riguardo l'installato.

"Fortinet è stata scelta dopo aver preso in esame diverse soluzioni proposte da brand concorrenti, in virtù dell'ampia gamma di funzionalità a disposizione, così come della convenienza dell'offerta esposta. Di grande importanza è stato anche il rapporto di fiducia creatosi con il referente che ha seguito l'operazione

Università degli Studi di Napoli Federico II

Rete metropolitana e Servizi innovativi di rete

"Fortinet è stata scelta dopo aver preso in esame diverse soluzioni proposte da brand concorrenti, in virtù dell'ampia gamma di funzionalità a disposizione, così come della convenienza dell'offerta esposta. Di grande importanza è stato anche il rapporto di fiducia creatosi con il referente che ha seguito l'operazione e la successiva implementazione."

Carmine Piccolo,
Responsabile della Rete di Ateneo
Università degli Studi di Napoli Federico II

Dettagli

Cliente: Università degli Studi di Napoli Federico II

Settore: Istruzione

Paese: Italia

e la successiva implementazione", Carmine Piccolo, Responsabile della Rete di Ateneo, Università degli Studi di Napoli Federico II.

La topologia evolve da routed legacy a Spine-Leaf

Dopo una prima fase di analisi e pianificazione, in cui sono stati evidenziati i principali punti di debolezza e sofferenza dell'architettura 'legacy', si è deciso di passare da un modello Routed a un modello Spine-Leaf e in ogni punto di connessione dei nodi 'leaf' è stata installata una coppia di firewall adatti a gestire il traffico generato dallo specifico nodo.

Grazie a questo progetto, l'intera rete si aggrega ora, prima di uscire su Internet, sui nodi di un FortiGate 3400E "Stretched Cluster", situati presso un nodo nella sede di Monte Sant'Angelo e un nodo nella sede del Centro Storico. Le sedi secondarie sono dotate di un Firewall FortiGate 1800F ciascuna, mentre le due sedi principali (MSA e CS) sono dotate di attestazione Spine-Leaf su due VDOM (Virtual Domain) dedicati sul Cluster 3400. Il passaggio da una topologia Routed legacy a una Spine-Leaf ha moltiplicato la velocità della rete.

Un'ulteriore sfida nella creazione di questa architettura è stata quella di razionalizzare e analizzare, e dove possibile filtrare, l'enorme quantità di traffico internet/intranet generato. Attraverso l'uso di FortiAnalyzer, una soluzione che raccoglie, archivia e analizza automaticamente i registri provenienti da tutti i dispositivi di sicurezza Fortinet, è stato possibile ottenere visibilità sulla postura di sicurezza dell'intera università e dei suoi utenti. Una volta raccolte le informazioni, è diventato naturale gestire il processo di qualsiasi incidente di sicurezza rilevato nel log grazie a FortiSIEM, il sistema di gestione delle informazioni e degli eventi di sicurezza di Fortinet, che offre capacità che vanno dalla creazione automatica dell'inventario delle risorse all'applicazione di analisi comportamentali all'avanguardia, per rilevare e rispondere rapidamente alle minacce. Non da ultimo, grazie a FortiMail è stato possibile potenziare il livello di antispam offerto dal produttore del servizio di posta. Il risultato raggiunto in termini di volume di email di spam processate è drasticamente aumentato così come il tasso di falsi positivi e falsi negativi riscontrati.

Impatto sul business

- Conseguito un miglioramento della stabilità generale della rete
- Gestito in modo razionale ciascuno dei segmenti di rete che richiedono la connessione a Internet, garantendo il percorso più breve ai molteplici breakout
- Protetto efficacemente il network dal rischio di subire attacchi informatici

Soluzioni

- FortiGate Next-Generation Firewall
- FortiAnalyzer
- FortiAuthenticator
- FortiMail
- FortiSIEM

Miglioramento della stabilità e della sicurezza dell'infrastruttura

L'implementazione delle soluzioni Fortinet, che ha incontrato il favore del management dell'Ateneo, ha comportato un miglioramento della stabilità e della sicurezza generale della rete.

In particolare, i principali benefici ottenuti riguardano la gestibilità dell'intera struttura e la possibilità di applicare sicurezza avanzata per proteggersi da minacce complesse. Avere a disposizione la soluzione Next Generation Firewall in un'architettura come quella realizzata presso l'Università degli Studi di Napoli Federico II consente di applicare i controlli di sicurezza, di filtraggio e di protezione nel punto più prossimo alla generazione del traffico; questa scelta ottimizza anche il carico in termini di banda di tutta la rete e distribuisce in più punti il lavoro necessario ad ispezionare il traffico generato dalle migliaia di utenti che quotidianamente frequentano i vari campus. Il tutto gestito in maniera omogenea, coerente e con le medesime politiche di sicurezza.

Il progetto, iniziato nell'ambito dell'Azienda Ospedaliera, è stato successivamente ampliato nei vari campus, e a breve tutti e 5 i Point of Presence (POP) saranno dotati della medesima configurazione Spine-Leaf e vi sarà un'omogenizzazione dell'intera infrastruttura.

Per quanto riguarda il futuro, il desiderio è quello di efficientare ulteriormente la rete, implementando due livelli di sicurezza al suo interno e ottenendo una maggior profondità e puntualità nell'isolare le minacce informatiche direttamente sul nascere.

April 18, 2024 3:27 PM
2599481-0-1-EN