Veritas sceglie Trend Micro e si mette al sicuro dagli attacchi ransomware.

Sito Web
www.gruppoveritas.it

Regione
Veneto, Italia

Settore
Utilities

Dipendenti
2.250

Partner
Personal Data

Competitor utilizzati in precedenza
Kaspersky, McAfee

Prodotti
- Deep Security, Deep Discovery, OfficeScan

Ambiente IT
VMware, Citrix, NetApp, Windows XP, Windows 2003

Benefici
- Protezione completa dei server e degli endpoint
- Protezione dei sistemi legacy
- Protezione dai ransomware e dagli attacchi mirati
- Gestione centralizzata della sicurezza

INTRODUZIONE

Veritas (Veneziana Energia Risorse Idriche Territorio Ambiente Servizi) è una multiutility interamente pubblica, la prima del Veneto per dimensioni e fatturato e una delle più grandi d'Italia. È ottava per i servizi idrici integrati e sesta per quelli ambientali. Veritas gestisce l'igiene ambientale, il servizio idrico integrato, alcuni servizi urbani collettivi e la produzione di energia da fonti rinnovabili e biomasse. Veritas fornisce servizi ambientali ai cittadini e alle imprese in un territorio di oltre 2.650 kmq e 930.000 abitanti.

LA SFIDA

Veritas, nel 2016, decide di aggiornare la propria infrastruttura di sicurezza. Questa decisione è data dall'esigenza di patching dei sistemi, dalla necessità di avere delle prestazioni migliori sulla parte endpoint, gateway e posta elettronica e infine dall'urgenza di doversi difendere da minacce e attacchi sempre più evoluti. Tutte queste necessità non erano rese possibili dalle soluzioni precedenti in uso. Stefano Nironi, Responsabile Sistemi Informativi Veritas, ricorda "I prodotti precedenti che utilizzavamo non ci soddisfacevano. Lato endpoint avevano mostrato parecchie lacune e avevamo paura di trovare virus. Inoltre trovavamo molte macchine sconnesse e non protette". Da qui nasce la richiesta al partner informatico Personal Data, per farsi consigliare una nuova soluzione.

PERCHÉ TREND MICRO

Personal Data, storico e autorevole System Integrator con sede a Brescia, identifica Trend Micro come vendor adatto a risolvere le necessità di Veritas e segue attentamente e con scrupolo tutte le fasi di trasformazione dell'infrastruttura di security dell'azienda.

"Ci è stato proposto Trend Micro, abbiamo analizzato il prodotto e ci è piaciuto per come affronta e risolve le minacce ma soprattutto per il fatto che va alla ricerca delle minacce non conosciute e non solo di quelle conosciute. Questa caratteristica mi ha molto colpito e interessato". Afferma Stefano Nironi. Grazie a Trend Micro, l'azienda risolveva non solo le esigenze in ambito endpoint e reti, ma anche lato server. "Avevamo molti server che non potevano essere dismessi e che utilizzano sistemi non più supportati come Windows 2003. L'unica soluzione che poteva

“Avevamo molti server che non potevano essere dismessi e che utilizzano sistemi non più supportati come Windows 2003. L’unica soluzione che poteva garantirci la sicurezza era Deep Security, grazie alla sua capacità di patching virtuale e intrusion prevention.”

Stefano Nironi,
Responsabile Sistemi Informativi, Veritas

“In questa zona ci son molte aziende che hanno subito un attacco ransomware. Fino ad oggi noi siamo riusciti a bloccare tutti i tentativi di attacco e non abbiamo avuto nessun caso di ransomware. Questo mi ha fatto fare anche bella figura con la direzione e ha confermato che Trend Micro è stata una buona scelta. Posso dire che Trend Micro è un servizio completo che riesce a coprire tutta l’azienda.”

Stefano Nironi,
Responsabile Sistemi Informativi, Veritas

garantirci la sicurezza era Deep Security, grazie alla sua capacità di patching virtuale e intrusion prevention”.

SOLUZIONI

L’infrastruttura IT di Veritas è costituita da un data center interno basato su storage NetApp e farm VMware, che gestisce circa 200 macchine virtuali ed eroga i servizi per tutte le sedi remote.

Sul territorio sono dislocati anche una cinquantina di host fisici e le postazioni di lavoro sono all’incirca 2.000. Veritas utilizza Windows come sistema operativo e Citrix per la distribuzione delle applicazioni. Trend Micro e il partner Personal Data, per far fronte alle esigenze di protezione di Veritas hanno ideato una strategia di protezione su misura che ha messo in sicurezza la parte server con la soluzione Deep Security, la parte endpoint con la soluzione OfficeScan, che comprende ora caratteristiche di machine learning e behavioural monitoring e la parte di reti con Deep Discovery. In particolare Deep Discovery Inspector per la parte di rilevamento e Deep Discovery Analyzer per la parte di remediation. Tutte le soluzioni comunicano in tempo reale tra di loro e sono gestite a livello centrale dalla console Trend Micro Control Manager. La soluzione di punta di questo progetto è Trend Micro Deep Discovery, la soluzione più completa della propria categoria per contrastare la minaccia degli attacchi APT. Deep Discovery non solo mette a disposizione i tool adeguati a rilevare i malware zero-day e le attività di malintenzionati sull’intera rete e durante tutte le fasi che caratterizzano un attacco, ma è stata anche studiata per fornire strumenti di analisi approfondita grazie ai quali le imprese possono prevenire attacchi futuri. Le capacità di network detention e analisi della sandbox personalizzata di Deep Discovery permettono di rilevare le email di spear phishing spesso alla base dell’attacco, identificare il malware contenuto e scoprire i siti esterni di comando e controllo (C&C) utilizzati dai cybercriminali. Nello specifico, **Deep Discovery Inspector** è un dispositivo di rete che consente un controllo a 360 gradi su tutto il traffico della rete per rilevare qualsiasi aspetto di un attacco mirato. Deep Discovery Inspector monitora tutte le porte della rete e più di 100 protocolli, assicurando così la più ampia protezione disponibile. I motori di rilevamento specializzati e il sandboxing personalizzato identificano e analizzano malware, comunicazioni command-and-control e attività elusive degli aggressori che risultano invisibili alle soluzioni di sicurezza standard.

I BENEFICI

Le caratteristiche Trend Micro di una maggior leggerezza lato client, le capacità di individuare i movimenti laterali e le possibili intrusioni, oltre a proteggere i sistemi legacy grazie alla caratteristiche di virtual patching sono state molto apprezzate. Stefano Nironi ricorda “Le soluzioni Trend Micro ci hanno permesso di andare a proteggere anche i vecchi PC. Ad esempio, nei laboratori abbiamo ancora delle macchine con installato Windows XP. Questi computer sono associati a strumenti molto costosi e perfettamente funzionanti. Tecnicamente cambiare ogni singolo strumento ci sarebbe costato parecchie migliaia di euro, Trend Micro è riuscita a risolvere anche questa criticità, mettendo al sicuro le macchine Windows XP e facendoci risparmiare molti soldi sulla parte hardware”.

Nel complesso il responsabile IT è molto soddisfatto. Anche in relazione agli attacchi ransomware che stanno colpendo l’Italia[1], si dimostra tranquillo “In questa zona ci son molte aziende che hanno subito un attacco ransomware. Fino ad oggi noi siamo riusciti a bloccare tutti i tentativi di attacco e non abbiamo avuto nessun caso di ransomware. Questo mi ha fatto fare anche bella figura con la direzione e ha confermato che Trend Micro è stata una buona scelta. Posso dire che Trend Micro è un servizio completo che riesce a coprire tutta l’azienda”.

SVILUPPI FUTURI

Veritas sta valutando un aumento del controllo sui sistemi, attraverso la sostituzione dell’attuale firewall con uno Trend Micro. L’azienda ha inoltre attivato AirWatch e un altro passo sarà quello di installare una soluzione Trend Micro per proteggere i circa 250 device mobili che ormai fanno parte della realtà aziendale e si connettono alla rete tramite Wi-Fi. In futuro, un ulteriore progetto potrebbe essere legato alla protezione diretta dello storage.

MAGGIORI INFORMAZIONI

Per maggiori informazioni, per favore vai su
www.trendmicro.com

[1] Secondo i dati Trend Micro, l’Italia è il settimo Paese al mondo e il secondo in Europa più colpito dal fenomeno ransomware Trend Micro H1 2017 Threat Roundup

TREND MICRO™
Securing Your Connected World