CASE STUDY

Do Not Disturb! Blocking Email Threats at the Door

The hotel sector is rapidly emerging as a key target for cyber criminals. It's little wonder, given the rich array of guests' personal and financial information. And with email being a prime attack vector, the hotel sector – from major hotel chains to budget accommodation providers – face the daunting task of keeping their networks and their guests' personal and financial data safe.

Trustwave®

Client Spotlight

This iconic budget accommodation network has over 30 locations across New Zealand, nearly 250 staff and hosts over 250,000 guests annually.

The Challenge

With more than 280 billion business and consumer emails sent and received daily, email remains the most ubiquitous, inexpensive and effective form of business communication. But as a prime channel for cyber attacks, email also is challenging to secure. This budget accommodation provider needed a robust email security solution to protect it from an increasing number of malicious email-borne threats. With booking inquiries streaming in from across the globe, front desk staff dealt with a daily deluge of emails that potentially contained malicious links or attachments. In particular, the organization noticed a marked increase in phishing scams and ransomware. But it was a malware infection that took operations offline for a half-a-day and affected nearly 150 staff that crystalized their need to beef up their email security.

> *"We use a lot of Trustwave security products. Not only has Trustwave always provided good solid advice but they've also taken the time to understand us. We really value that partnership."*
>
> Business Systems Manager

The Solution

The client implemented Trustwave Secure Email Gateway (SEG). Incorporating threat intelligence from the Trustwave SpiderLabs® research team, SEG provides them with advanced real-time protection against the latest email-borne threats. And to help the client meet regulatory and industry requirements, the solution provides powerful data loss protection to manage confidential data. SEG also enables the client to build highly customized message handling rules through a flexible policy configuration engine.

The client also implemented the Trustwave Blended Threat Module (BTM) which provides protection against comprised URLs embedded in emails by scanning these links each and every time a user clicks on it.

Industry Threat

The consequences of a data breach to the hotel sector are considerable – from reputational damage, lost revenue and steep fines due to data breach notification laws in a number of countries and Europe's General Data Protection Regulation (GDPR). One common attack vector used to target the hospitality industry, according to the 2018 Trustwave Global Security Report, was telephone-initiated spear phishing. The caller would complain about being unable to make a reservation on the victim's website and ask to email his details to the staff member. The attacker then emailed a message with a malicious file attached, waited until the victim confirmed they opened the attachment and then hung up the phone.

> *"We now have peace of mind. With more robust email security in place, our risk is reduced. Plus we don't have to invest in multiple applications – we have one application that covers all the bases."*
>
> Business Systems Manager

Trustwave®

CSDND-0319