Email security essential for enterprise security

The year 2017 witnessed major security breaches worldwide. For the first time ever, we saw several "cryptoworm" like WannaCry and Petya, variants self-propagate across vulnerable workstations around the world. We also witnessed more traditional ransomware families cause remarkable damage to victimized organizations as well as strains that embraced novel tools and techniques.

Large scale breaches were reported at Yahoo, HBO and Equifax to name a few, which led to data loss, leaking of private email conversations and intellectual property theft. Even political campaigns like Democratic National Convention (DNC) suffered from such email attacks. Hackers also targeted offshore law firms (Panama Papers) and stole information about potentially shady financial practices of the super-rich. When a target of that size and consequence falls prey to hackers, and all under the guise of "doing social good," it's clear just how expansive cyber-threats and the motives behind them have become. Indeed, the 'ransomware' that took the world by storm was not distributed via an email mail-spam campaign.

Trends from 2017

The disturbing trend which can be assessed is that the frequency of the attacks and their sophistication is progressive in nature and is getting further complicated to avoid detection. On an average a data breach now costs companies more than USD 3.6 million, which doesn't account for bolstering security protocols or managing reputation fallout. The larger and more long-term cost that's measured in consumer confidence is perhaps most damaging — one that can lead to millions in lost revenue.

Cybersecurity is one of the biggest concerns for most enterprises, and the email security should be a major point of attention as it is the most vulnerable point of attack for any organisation. Hackers regularly target inbox because they're an easy point of access and offer a treasure trove of valuable information.

Email security essential for enterprise security

New Security Architecture

Companies are getting serious about cybersecurity and they are focusing on ways to secure the email systems in the organisation. Best practices for a comprehensive and easy-to-use email security strategy are being adopted.

Use of Blockchain based email system

As part of the solution, it is being recommended by cyber-security experts that email systems should be based on 'blockchain' technology which is becoming increasingly important, as current email services are cumbersome and are no longer secure. Indeed, email service providers are using obsolete technology that has become too vulnerable to ever-more sophisticated hackers.

Cyberattacks have been the norm for a long time. Now, however, the frequency, magnitude, and implications of email hackings and other malicious acts are increasing dramatically. As a result, it is now urgent to innovate and move toward more secure email technologies, such as those that integrate the security that blockchain technology provides.

Filtering Aided by Machine Learning

Companies often use dozens of security products aimed at protection and detection. These systems funnel an ever-growing number of alerts and incident notifications to security teams. If a security organization can't keep up with the volume of work, the typical solution is to add manpower. This approach simply cannot scale fast enough because the needed growth in manpower simply can't keep pace with the growing volume of alerts. As a result, enterprises are slow to triage and mitigate security issues. They also run the risk of a critical alert or response task getting overlooked or lost in the noise.

Comparing incoming emails against a database of known threats and analyzing the content for malicious phrases and patterns helps to filter out bad traffic. With the aid of machine learning and live threat analysts, these filters can better detect and deflect newer and more advanced threats. When security teams take advantage of automation, they can rapidly triage alerts, investigate incidents, contain threats, and protect their companies and customers faster than ever before.

User Education and Best Practices

Technical tools are invaluable, but implementing these tools without making any changes on the ground floor i.e. employee training and education can still keep the organisation vulnerable. Employees should be educated and trained as to how to identify suspicious emails and, equally important, encourage them to report any suspicious messages to their respective IT teams. While often associated as one of your weakest links, employees can become one of the most effective lines of defense to combat cyberthreats with consistent training and reinforcement.

Predictions for cyber security landscape for the year 2018 are debatable. But by incorporating security tools and educating users, companies can ensure that their sensitive information — from intellectual property to login credentials to private conversations — is secure.

For Security Solutions:
Call: +919717495402
Email: contact.us@securitas-india.com

For Background Verification:
Call: +91 9978990585
Email: ev.screen@securitas-india.com

National Command Centre:
18001038797
www.securitas.in