mimecast

SOLUTION BRIEF

Minimize Ransomware's Impact

with Cloud-based Prevention, Continuity, and Recovery

Ransomware poses a large and growing threat to organizations of all sizes, from enterprises to small businesses and government agencies. What is ransomware? It's a type of cyber-extortion scheme involving malware that encrypts data and files on victims' PCs, servers or other systems, thus making them unusable. Once deployed, the attacker demands the payment of a ransom in exchange for a decryption key, which unlocks the files to make them usable again.

The *2017 Data Breach Investigations Report, 10th Edition*, Verizon Enterprise Solutions found that ransomware incidents climbed from the 22nd most common malware attack in 2014 to the 5th most common in 2017.[1] The report also found that email surpassed web drive-by downloads as the top malware vector in 2017. Global ransomware damage costs are predicted to exceed $5 billion in 2017, up from $325 million in 2015.

FBI statistics show that ransomware attacks can be costly[3] and lead to:

- Productivity loss
- Permanent data loss
- IT personnel time to perform recoveries (and related opportunity costs)
- Outside forensics services to contain and remediate infections
- Disrupted business activities with customers and partners
- Damage to the brand caused by negative publicity

Current Approaches Fall Short

Many organizations mistakenly believe that their antivirus and other prevention-oriented security products protect adequately against ransomware. They also often overlook ransomware scenarios when formulating their continuity or disaster recovery plans. Yet according to IT analyst firm Gartner, Inc., ransomware perpetrators change their tactics and the ransomware code itself constantly to evade antivirus defenses.[2] The fast-evolving nature of these crimes makes ransomware-centric risk management a matter of what to do when, rather than if, your organization is attacked.

The Need for a Multifaceted Strategy

Faced with the constant escalation of ransomware threats, as well as the pain and cost of restoring operations after an attack, an effective strategy for managing email-borne ransomware risk needs to be multifaceted, and include measures to :

mimecast®

SOLUTION BRIEF

- Prevent ransomware from reaching the organization,
- Maintain email continuity in the event that ransomware breaks through, and
- Recover email services and data quickly and with minimal disruption to business operations.

Mimecast enables this layered ransomware defense strategy by providing prevention, continuity, and recovery functionality from a single multiservice cloud grid computing architecture powered by the Mime|OS operating system.

Strategic Components

This layered approach to ransomware protection disarms and neutralizes the majority of ransomware attacks, simplifies recovery, and maintains mailbox continuity using technologies developed for our security, continuity, and archiving services.

Mimecast Targeted Threat Protection (TTP) defends against email-borne malicious links, weaponized attachments and malware-less social-engineering (e.g., "phishing") attacks – the three most common attack methods – using real-time scanning, blocking of suspect websites, and file sandboxing capabilities. TTP protects against a wide range of attack techniques commonly used in ransomware campaigns.

Mimecast Mailbox Continuity delivers simple, cost-effective protection against email downtime events associated with ransomware attacks and recovery and restoration operations. During such events, the Mailbox Continuity service continues to manage both inbound and outbound mail through in the Mimecast Platform and makes available 58 days of retained mail (or up to 99 years with the Archiving Service option). This capability also gives users and administrators "email as usual" access to their folders, calendar items, and contacts, to help organizations maximize uptime for the impacted users, or for the entire email service, in cases where the email server itself has been hit by ransomware.

Mimecast Sync & Recover repurposes email archive data and monitors, captures, and preserves outlook calendar items, and contact lists for use in restoring Exchange Server and Exchange Online data after an attack by ransomware or other malware. Administrators can use Sync & Recover to replicate user Outlook configurations quickly and easily, to bring impacted systems back to full production.

Whether email servers are maintained on premises or in the cloud, the risks of human error, technical failure and malicious intent still loom. Every organization has employees and administrators who are prone to making mistakes. This extends to the Office 365 engineers responsible for keeping the service running as smoothly as possible. The Office 365 cloud is created using real data centers and staffed with real people. While measures can be taken to minimize mistakes, with technology something always can (and usually will) go wrong. Having the ability to restore Office 365 data to a known good point in time is important should something mistakenly get deleted or corrupted. It's critical to recognize that Office 365 Service Level Agreements (SLAs) apply to service availability, not to data recovery or resilience.

Benefits

Mimecast enables organizations to secure, recover, and maintain availability of email services, content, and data via a single, purpose-built cloud archiving platform. The Mime|OS operating system is continually enhanced to deliver the best possible email security, archiving and continuity service experiences. The unified management of these diverse services gives administrators an easy, intuitive administration experience that they cannot achieve with discrete security and backup products from other vendors. In short, Mimecast's single-vendor, single-platform solution provides for the protection of corporate information assets through the duration of a ransomware threat.

Conclusion

As ransomware attacks continue to run rampant, organizations will face growing pressure to protect sensitive digital resources. However, neither preventive nor remedial approaches alone offer complete protection. Organizations can easily deploy and manage a layered defense against ransomware by taking advantage of Mimecast's unique approach to cyber resilience, made possible by our Mime|OS and cloud grid computing architecture. An approach enabled by Mimecast layers TTP, Mailbox Continuity, and Sync & Recover technologies to prevent the majority of attacks, quickly recover from attacks that get through, and continue email operations during recovery and restoration.

1. Trend Micro, Incorporated, TrendLabsSM 2016 1H Security Roundup.
2. Gartner, *Use These Five Backup and Recovery Best Practices to Protect Against Ransomware,* June 8, 2016.
3. 2016 Internet Crime Report, Cyber Division, Federal Bureau of Investigation