mimecast®

INTERNAL THREATS PERSONIFIED: How Employees Can Jeopardize Your Cybersecurity

Understanding the Risk

Hidden Threats: What You Don't See Can Hurt You
When it comes to securing email and protecting against cyberattacks, most organizations focus their attention and resources on inbound emails. They invest in strong email security gateway solutions designed to thwart incoming phishing attempts, malware, impersonation attacks, malicious URLs and attachments and other content generally categorized as spam.

This is a great start …

However, based on aggregate data of Mimecast customers, ***only 40% of email originates through inbound system traffic.*** The other 60% of email traffic is introduced via internal-to-internal (40%) or outbound (20%) email communications.

In other words, most companies are not inspecting and securing up to 60% of their email traffic.

Emails sent between users or from internal users to third parties such as customers and suppliers represent the majority of most organizations' email traffic; however, they are often left under-protected.

And as we've seen from past news events, it only takes one successful attack to infiltrate an organization's email environment, leak sensitive information and cause long-term reputational damage.

Your Employees Can Be Your Greatest Asset, or Your Weakest Link When it Comes to Email Security

According to Mimecast's **2018 State of Email Security Report**, developed in conjunction with Vanson Bourne:

Employees frequently become unwitting participants in attacks, aiding the lateral movement of threats through the distribution of malicious URLS and attachments or the exposure of sensitive data.

In this E-book, we'll take a closer look into several email-related activities that employees often engage in that contribute to the spread of these insider ("hidden") threats and then discuss what measures your organization can take to protect itself from these "hidden" threats.

USE CASE #1

Credential Harvesting

My Account is now Your Account, Mr. Attacker?

Rima receives an email saying that there is an issue with her Microsoft Office 365™ account and she needs to login to her account to verify and update her information. The email was sent to her work email and Rima clicks on the link provided and proceeds to login with her Microsoft account credentials (typically Active Directory credentials). Unknown to Rima, the site she is on, while looking legitimate, is actually a phishing site set up to harvest her credentials as she attempts to "login" to Office 365. Not only do the attackers now have her login information, but they then quickly use it to gain access to her Office 365 account and read her email correspondence and archives. They then use their access to her account to send emails, containing malicious links, malicious attachments and/or malware, to distribute an attack to all her contacts. These include internal colleagues as well as partners, many of whom consider Rima a trusted contact and click on the malicious link or open the attachment in the email. The threat continues to spread like wildfire both within Rima's organization and within her partners' organizations.

Minimize Damage to Corporate Brand

Clearly, once Rima's partners realize that the email they received from her was indeed malicious, they may feel violated. No one wants to be connected to malicious activity, especially at a corporate level. There is a level of trust between partners, vendors and other third parties that sensitive data will be protected, and appropriate security measures will be taken to safeguard against compromises. Having such an event take place can leave a bad taste in a partner or vendor's mouth and leave a long-lasting negative brand impression on the offending organization.

The Mimecast Difference

Mimecast can help provide reputational protection for your organization. Internal Email Protect scans all internal and outbound email traffic to help prevent the spread of attacks between internal users and to third parties like customers and suppliers, while also protecting against the unintentional or malicious exposure of sensitive information.

80%

of surveyed companies had encountered threats caused by attackers infiltrating and compromising users' email accounts.*

*Mimecast's **2018 State of Email Security Report**

USE CASE #2

Downloading and Distributing Content with Colleagues

Good Intentions Gone Wrong

Maria has a friend who is interested in an open position at her company. Her friend sends his resume to Maria using Dropbox. Maria accesses the resume via Dropbox and saves it onto her work computer. She then attaches the file to an email that she then sends, using her work email account, to the HR recruitment lead for the position.

The HR recruiter opens the attachment, sees that there is a link to the applicant's LinkedIn profile and clicks on it. Unfortunately, the resume Maria attached contains malicious code and by clicking on the link, has unleashed a virus on the recruiter's computer that then infiltrates the organization's network.

Scan Internally Distributed Attachments and Links

There is no guarantee that any file or link shared online, even if it is shared by a 'trusted source' through file sharing mediums such as Dropbox or Slack, are safe. If Maria's friend had sent his resume to her work account directly, it would have passed through her organization's email gateway and most likely been scanned, deemed suspicious and blocked before ever reaching her inbox. In this scenario however, the threat was introduced via email internally, thus bypassing most secure email gateways.

The Mimecast Difference

Mimecast Internal Email Protect can help reduce the time required to identify the source of attacks from days or weeks to seconds and can prevent the lateral movement of attacks (either between users or from users to third parties). It does so by inspecting internally generated email emails and flagging potentially compromised accounts based on the use of malicious URL, attachments, or the movement of sensitive information. In addition, Internal Email Protect continuously checks inbound files to identify malware post-delivery, as well as files sent internally via email, and can automatically reach back into a user's inbox to remove infected or undesirable emails.

61%

of organizations were hit by an attack where malicious activity was spread from one infected user to other employees via email.*

*Mimecast's **2018 State of Email Security Report**

USE CASE #3

Sharing Confidential Data with the Wrong Person

A "My Bad" Turns Disastrous

Bob, a finance manager is in a rush to finish fiscal planning for 2019. He is using two Excel spreadsheets to communicate with the sales leadership team around proposed targets for next year. One sheet includes employee names as well as current and proposed sales targets. The other sheet has the same information but also includes salary and bonus information for the entire sales organization. In a hurry, Bob accidentally forwards the more sensitive version of the file to the entire leadership team via a distribution list. He notices his mistake right away but has no means to pull the email from the various users' inboxes. Instead he calls all of them and begs them to delete the file. Unfortunately, Emily, the director of sales operations, is away from the office and opens the file. Emily notices she makes less money than those in her peer group. She is livid and HR and Emily's boss, the SVP of sales, need to have multiple meetings with her to diffuse the situation.

Take Back Control with Remediation

Needless to say, if Bob could have had IT pull back this email right after it was sent, hours of lost productivity and damaged employee trust could have been avoided. Also, now that the file containing sensitive information has been distributed to a wider audience, how can IT ensure that one of the recipients won't forward the email to yet another person?

Bob's mistake becomes IT's problem. Careless insiders don't intend to cause harm to their organization, but often make mistakes like forwarding sensitive data internally or externally or unknowingly sending an email with a malicious attachment or URL to colleagues, customers or partners. While these actions are not done with malicious intent, a careless insider does increase an organization's security risk or potential for a data leak.

The Mimecast Difference

Mimecast can help IT take back control by providing organizations with advanced message and threat remediation capabilities. Internal Email Protect can automatically reach back into a user's inbox to remove infected or undesirable emails. Administrators can also manually monitor, search for and remediate emails via the Threat Remediation Dashboard.

88%

of firms were exposed by the actions of careless users who had inappropriately shared sensitive data or violated company security policies.*

*Mimecast's **2018 State of Email Security Report**

USE CASE #4

Profanity in the Workplace

If You Don't Have Anything Nice to Say ...

Jonathan just found out from his boss that he will be let go from his organization. He has worked at his company for over seven years, pouring his blood, sweat and tears into numerous projects that have proven to be very successful and driven strong revenue growth over the years. The news of his imminent layoff has left him very angry, confused and hurt. He is so upset, he rushes back to his computer, and without thinking twice, he sends out an email with inappropriate language that is negative about the leadership of the organization to all of his contacts. He also talks about the roadmap of the product he is working on and delivers a long rant about key features that he does not agree are a good idea but that the leadership team is insisting should be incorporated in the product. In addition to his work colleagues, some of the recipients of this email are partners, vendors and customers he has worked with over the years.

DLP to the Rescue

Jonathan has not only aired his own 'dirty laundry' about his organization to external recipients, including partners, vendors and customers, but he has also sent out sensitive information about the product roadmap that is considered confidential. Clearly, his behavior will be seen as both shocking and completely unprofessional by whomever reads his email. His use of profanity and negative comments about his organization will certainly not sit well with customers and 3rd parties may consider re-evaluating the business they do with this organization.

The Mimecast Difference

Mimecast Internal Email Protect can help prevent accidental or intentional exposure of profanity, abusive language and/or confidential information by applying data leak prevention policies to internal and outbound emails. Internal Email Protect can also help to mitigate damage through automatic or manual removal of internal-to-internal emails.

59%

of organizations will suffer a negative business impact from an email-borne attack caused by malicious intent, human error or technical failure*

*Mimecast's **2018 State of Email Security Report**

THE SOLUTION

Threat protection, visibility and remediation for internal and outbound email

Mimecast Internal Email Protect applies best-practice security inspections to internal and outbound email traffic, allowing organizations to monitor, detect and remediate security threats that originate from within their email systems. A 100% cloud-based service, it includes scanning of attachments and URLs, as well as inspections for violations of data leak prevention policies and the remediation of emails and malicious files detected.

Internal Email Protect is a component of Mimecast's Targeted Threat Protection service and integrates seamlessly with Mimecast's full suite of security solutions.

Arm Your IT Team with the Visibility it Needs to Protect Your Organization

Internal Email Protect provides IT administrators with full visibility of internal and outbound email traffic and threats across the entire organization, enabling them to quickly detect and identify the source of these email-based attacks that can, otherwise, take weeks or months to isolate the root cause and address.

Remediate Threats

Internal Email Protect continuously rechecks inbound files to identify malware post-delivery, as well as files moving internally via email, and can automatically reach back into users' inboxes to remove malicious or undesirable emails. Administrators can also manually monitor, search for and remediate emails via the solution's Threat Remediation Dashboard.

Protect the Integrity of Your Organization

Internal Email Protect (IEP) prevents the spread of attacks between internal users and to third parties like customers and suppliers, while also protecting against the unintentional or malicious exposure of sensitive information.

Mimecast IEP is a single, integrated 100% cloud-based solution that enables IT to:

- Increase visibility and control
- Automatically or manually remediate threats
- Quickly isolate the source of an attack and shut it down
- Monitor email traffic for inappropriate or policy-prohibited content
- Protect against reputational damage
- Implement data leak prevention policies across all internal and outbound communications
- And more!

It's Time to Take Threats on the Inside Seriously

LEARN MORE