Thomas Berndorfer, CEO, Connecting Software
July 9, 2019

Share

What can financial institutions do to improve email security?

Financial institutions are in a fully-fledged war against data breaches. And rightly so – the finance sector is a frequent target of ransomware, phishing, and other malicious attacks. Sensitive communications are particularly vulnerable, with thousands getting leaked every year.

Yet at the same time, championing email security in the finance sector may seem like a Sisyphean task. Despite trying to reach for the beacon in far-off distances, security providers get stuck with repetitive problems and security holes; they never really get to implement a reliable, comprehensive preventive architecture.

With mass scandals circling the finance sector like a plague, how can companies enhance their security where it matters the most?

Don't underestimate emails

While IT professionals nowadays deal with a myriad of difficult issues, emails often get overlooked. Digital communications may be the cornerstone of our work – but they are forgotten by companies spending vast amounts of money on malware detectors and firewalls. Added to that, there is a general belief that providers are the ones responsible for our email security. However – be it Microsoft or others – that's not the case. In finance more than anywhere, organizations can lose customers overnight after just one instance of being hacked, and these overlooked systems present popular entry points for hackers.

Being proactive is crucial. It's necessary to go beyond general blacklisting of known spam and malware. IT professionals can look into end-to-end solutions such as content censors with custom settings and filters that match their security needs. Sending an email outside the network can automatically hide attachments or limit characters in the email body, with the potential to flag specific terms, such as the word loan or interest rate.

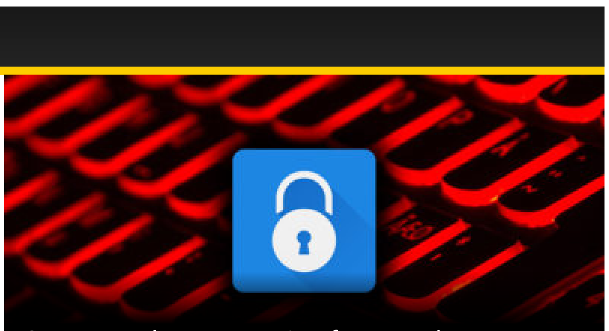
These Exchange Server tools for Office 365 bring clarity to complex settings that run on a variety of servers or domains. Protecting sensitive communications, they can do wonders for optimization of operations, while bringing benefits to workers at the same time. Employees are able to work more flexibly, assessing their calendars and inboxes even from their personal devices without putting their companies at risk.

Emails contain a lot of information, links, and information trails. Phishing scams, such as fake "lost passwords" or "reset your account" pleas are only a few of the potential threats. Emails require robust protection on different levels, be it authentication processes, content, sender identity or the functionality of the setup itself. By focusing on all these, organizations can approach email security as a whole, developing a clear, preventive game plan.

Preach decentralization

Decentralization should pervade every aspect of email security. Whether physically – with different databases and tools, or conceptually – with limited access rights, it can radically decrease the risk of leaks. Centralized points are the most tempting targets for hackers, and financial institutions often commit basic errors, such as storing passwords and usernames at the same location.

High security environments normally operate on multi-structural levels; therefore, one vulnerable knot shouldn't affect the overall security. This is because they control what information is stored where and who can access it. While decentralization doesn't need to visibly alter the IT architecture, it can still be a gamechanger.



Secure enclave protection for AI and ML

How to make DevSecOps stick with developers

Three signs your SOC is ready for XDR

Hackers breached U.S. government agencies via compromised SolarWinds Orion software

CISSP
Certified Information Systems Security Professional
An (ISC)² Certification
STRONG
Stronger Cybersecurity Starts with CISSP
LEARN MORE

What's new

More than half of organizations don't have an insider risk response plan

Countries that retaliate too much against cyberattacks make things worse for themselves

Secure enclave protection for AI and ML

42% of security leaders said the pandemic has changed their cybersecurity priorities

Mind the human factor

There's something that's out of the hands of even the most skilled IT experts: the human factor. As each worker interacts with the systems daily, they can heavily impact the security milieu. For this reason, IT literacy and security habits of employees working in the financial sector should be cultivated as much as possible.

In the financial sector, it's particularly important that the employees understand. This includes training on the specific threats common in finance, mastering crisis management, and creating knowledge exchange channels both within the organization and other institutions. Likewise, it's crucial that high security environment conduct vetting of both employees and third parties handling their data.

The preventive censor solution, implemented even by Microsoft on the Office 365 level, can help determine what data is suitable for internal networks. While an employee's mischievous attempt can't be absolutely prevented per se, organizations can limit their access to sensitive information, preventing problems even before they arise.

Likewise, there's an urgent need to train end-users, helping them to understand the basics of cybersecurity. With Microsoft now enabling 256-character passwords, we can see that the potential for hacking is enormous. But apparently, the most commonly used passwords on breached accounts is "123456", used by 23.2 million accounts all around the world, together with those as "1111111" or "password". It's beneficial for companies to have an established password policy, encouraging a change on a regular basis or promoting a password manager and multilevel authentication.

Financial institutions can have hundreds of different locations with thousands of employees using their email accounts daily. Be it through passwords or powerful exchange solutions, email security solutions can't, under any circumstance, be side-lined or underestimated.

More about

CISO | Connecting Software | cybersecurity | email security | opinion | phishing | scams | strategy

Share this

Featured news

- More than half of organizations don't have an insider risk response plan
- Countries that retaliate too much against cyberattacks make things worse for themselves
- 42% of security leaders said the pandemic has changed their cybersecurity priorities
- High-risk vulnerabilities discovery increased 65% in 2020
- Hackers breached U.S. government agencies via compromised SolarWinds Orion software

Don't miss

lock
Secure enclave protection for AI and ML

Internet
Countries that retaliate too much against cyberattacks make things worse for themselves

USA flag
Hackers breached U.S. government agencies via compromised SolarWinds Orion software

Cisco Jabber
Cisco re-patches wormable Jabber RCE flaw

DevSecOps
How to mak
stick with de

Help Net Security - Daily information security news with a focus on enterprise security.

Follow us

- Features

IN CASE YOU'VE MISSED IT

(IN)SECURE Magazine
ISSUE 67 (November 2020)