Email Needs Zero Trust

The author lists some important statistics here:

- 5 billion active email accounts worldwide, and over 4 billion emails are sent each month.
- 90% of cyberattacks start with phishing emails that it enters user inboxes because they do not contain malicious attachments that might be blocked by email service providers.
- 97% of people cannot accurately identify phishing email scams, and 30% of phishing emails are opened and read by users, or even the links in them are clicked.
- Gmail blocks over 100 million phishing emails every day.

It can be seen from these statistics that email security issues are no longer traditional security issues such as anti-spam and anti-malicious attachments, but rather addressing phishing email attacks. As most email users have completed the migration of email services to the cloud, and many cloud email service providers provide no limit on mailbox capacity, email has transformed from message communication to a repository of various contents. Personal mailboxes have become a museum of digital life from the past to the present, accommodating everything from bank statements, phone bills, online shopping confirmations, express delivery notices, electronic invoices, health examination records to tax documents, etc. As for corporate mailboxes, emails collect daily correspondence with colleagues, external suppliers and customers, as well as internal memos, financial data, contracts, employee records, customer data, R&D materials, sales documents and many other sensitive and confidential contents. In other words, today's email is no longer an inbox, but more like a file cabinet. This requires solving the problem of how to ensure the security of files stored in the file cabinet and how to ensure the security of these files containing confidential information in the cloud.

The changes in email applications require email security solutions to keep pace with the times. The key is how to prevent email content fraud and ensure the security of emails throughout their life cycle in the cloud. The most reliable solution is zero trust in plaintext emails and uses cryptographic technology to achieve email digital signature and encryption.

1. **Zero trust in plain text emails without digital signatures, only digital signatures can solve the problem of identity fraud.**

The reason why fake identity emails are rampant is that the sender's email address can be forged at will. Therefore, even if the email received shows the email address of the CEO, you cannot believe it is real. There have been fraud cases in which fake CEO emails demanded the finance department to pay hundreds of thousands of dollars.

How to solve this problem? The only solution is digital signature, the most basic cryptographic application. The digital signature of an email implemented with an email certificate cannot be forged, because the user needs to verify the control of the mailbox when applying for an email certificate, and the digital signature is bound to the user's email address, which cannot be achieved by forging an email. Therefore, one of the zero trust principles of email security is to not trust plain text emails, but only trust emails with digital signatures.

ZT Browser integrates an email client, zero trust in plain text emails, and automatically digitally signs each email with an email certificate, completely eliminating email fraud.

2. **Zero trust in unencrypted plaintext emails. Only encryption can solve the problem of email content leakage.**

The second security issue with plain text emails is that the email content can be easily tampered with illegally. A typical attack is that the email is indeed sent by the CEO, but the CEO's request to transfer money to Company A is tampered with to transfer money to Company B. This is also an email security incident that has occurred before. However, if the email is encrypted, the email content cannot be tampered with. If the email is also digitally signed, once the email is tampered with, the digital

signature will be invalid, and the email client will have a warning, and will not be deceived.
Since mailboxes have become file cabinets, only encrypted emails can be stored in ciphertext on cloud email servers. Only in this way can it ensure that personal confidential information and business secrets stored in mailboxes will not be illegally stolen or leaked. Therefore, the second zero trust principle of email security is to not trust plaintext emails, but only encrypted emails.

ZT Browser integrates an email client, zero trust in plain text emails, and automatically encrypts each email with an email certificate, completely eliminating email leaks.

Email security is an eternal topic. Because email plays a very important role in daily life and work, we must have a zero trust security concept to avoid phishing email attacks. We must use cryptographic technology to implement email digital signatures and encryption. Only in this way can we truly ensure email security.

How to implement email encryption and digital signature? Traditional email encryption solutions require users to apply for email certificates from CA and exchange public keys with recipients in advance. This is very difficult to use and difficult to popularize. The upcoming ZoTrus Email Encryption Automation Solution will perfectly solve this problem. Users only need to use ZT Browser to log into mailbox to achieve painless and automatic email encryption and digital signature. Only in this way can email encryption and digital signature be truly popularized, thereby truly ensuring the security of emails throughout their life cycle in transit and in the cloud.

Richard Wang

October 9, 2024
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 70 articles in English (more than 87,000 words) and 181 articles in Chinese (more than 518,000 characters in total).