电子邮件更需要零信任

笔者先罗列几个重要的统计数据：

- 全世界有超过 50 亿个活跃的电子邮件账户，每月发送的电子邮件超过 40 亿封；
- 90%的网络攻击从网络钓鱼邮件开始，这些网络钓鱼邮件由于没有包含可能被邮件服务提供商拦截的恶意附件而顺利进入用户收件箱；
- 97%的人无法准确识别网络钓鱼邮件诈骗，30%的网络钓鱼邮件被用户打开阅读，甚至点击了其中的链接；
- Gmail 每天阻止超过 1 亿封网络钓鱼电子邮件。

从这些统计数据可以看出：电子邮件安全问题已经不再是传统的防垃圾邮件和防恶意附件等安全问题，而是要解决钓鱼邮件攻击问题。

随着绝大数用户都已经完成了邮件服务迁移到云上，并且许多云邮件服务提供商不限邮箱容量，使得电子邮件已经从消息通信转变为各种内容的存储库。个人邮箱变成了从过去到现在数字生活的博物馆，容纳一切从银行对账单、话费清单、网购确认单、快递通知单、电子发票、健康体检记录到税务文件等等。而对于企业单位邮箱，电子邮件每天收集同同事、外部供应商和客户的往来通信，还有内部备忘录、财务数据、合同、员工记录、客户数据、研发资料、销售文档等大量其他敏感机密内容。也就是说，今天的电子邮箱不再是收件箱，更像是一个文件柜。这就要解决如何保证文件柜中保存的文件的安全问题，如何保证这些含有机密信息的文件在云中的安全问题。

电子邮件应用的这两个新变化使得邮件安全解决方案必须与时俱进，重点是要如何防范电子邮件内容欺诈和保障电子邮件在云端的全生命周期安全，最可靠的解决方案就是对明文电子邮件的零信任，采用密码技术实现电子邮件数字签名和加密！

1. 对没有数字签名的明文电子邮件零信任，只有数字签名才能解决身份欺诈难题

之所以假冒身份邮件猖獗，是因为电子邮件发件人邮箱地址是可以随意假冒的，所以，即使收到邮件时显示的是公司 CEO 的邮箱，也不能相信这是真的，曾经发生过假冒 CEO 邮件要求财务支付十几万美元的欺诈案例。

如何解决这个问题，唯一的方案是数字签名，最基础的密码应用，用电子邮件证书实现的电子邮件数字签名是无法假冒的，因为用户在申请邮件证书时需要验证邮箱控制权，而数字签名绑定电子邮件地址是假冒电子邮件无法实现的。所以，邮件安全的零信任原则之一就是不信任明文电子邮件，只信任有数字签名的电子邮件。

零信浏览器集成邮件客户端，对明文邮件零信任，自动用邮件证书数字签名每一封邮件，彻底杜绝邮件欺诈。

2. 对没有加密的明文电子邮件零信任，只有加密才能解决邮件内容泄密难题

明文邮件的第二个安全问题是邮件内容非常容易被非法篡改，典型的攻击就是邮件的确是公司 CEO 发来的，但是 CEO 要求转账给 A 公司被篡改为转账给 B 公司，这也是曾经发生的邮件安全事件。但是，如果邮件加密了，那就无法篡改邮件内容了。而如果邮件同时有数字签名，则一旦邮件被篡改，则数字签名无效，邮件客户端会有警示，也就不会上当受骗了。

由于现在的邮箱已经变成了文件柜，所以，也只有邮件加密了才会是以密文方式保存在云端邮件服务器中，只有这样才能确保邮箱保存的个人机密信息和商业秘密不会被非法窃取和泄密。所以，邮件安全的零信任原则之二就是不信任明文电子邮件，只信任加密电子邮件。

零信浏览器集成邮件客户端，对明文邮件零信任，自动用邮件证书加密每一封邮件，彻底杜绝邮件泄密。

电子邮件安全是一个永恒的话题，正因为电子邮件在日常生活和工作中起到了非常重要的作用，所以，我们必须有零信任安全理念才不会遭遇钓鱼邮件攻击，必须采用密码技术来实现电子邮件数字签名和加密，只有这样才能真正保障电子邮件安全。

而如何实现电子邮件加密和数字签名？传统的电子邮件加密方案是要求用户自己向 CA 申请电子邮件证书，并事先同收件人交换公钥，非常难用而难以推广普及应用，即将上线的零

信邮件加密自动化解决方案将完美地解决了这个难题，只需使用零信浏览器登录邮箱就可以实现无感无痛的自动化邮件加密和数字签名，只有这样才能真正普及邮件加密和数字签名，从而真正保障电子邮件在途和在云的全生命周期安全。

有诗为证：

邮件安全很重要，
明文邮件零信任。
零信技术有高招，
自动加密保安全。

王高华

2024 年 10 月 9 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 181 篇(共 51 万 8 千多字)和英文 70 篇(8 万 7 千多单词)。。