实施零信任安全，该从何入手？

Gartner 分析师 John Watts 和 Neil MacDonald 认为：零信任”是一个被许多单位过度使用、被广泛误解的术语。大多数对零信任感兴趣的单位都处于规划或战略阶段。希望转向实际实施的单位应关注两个主要项目：用户到应用程序分段(基于零信任架构)和工作负载到工作负载分段(基于身份的分段)。

笔者在同许多朋友聊起零信任时也有同感，大家都认为零信任很重要，但的确不知道如何下手，毕竟这是一个要放弃传统安全防护的“城堡和护城河“方案的痛苦过程。同时，《密码法》的生效实施，也使得许多政府单位不知道如何下手，如果克服经费短缺难题，但又能在《密码法》合规上有所前进。这两件事可能有读者认为互不相干，其实可以结合起来一起统筹规划，它们其实是一件事！因为《密码法》对关键信息基础实施的保护要求其实就是零信任原则，必须采用密码来实现信息加密和安全认证。

那么，该如何入手？如何才能做一件事能到达满足两个安全应用需求？笔者在这里分享三点见解：

(1) 树立零信任理念，零信任是一个旅程，不是一蹴而就的事情。

首先需要说明的是，零信任是一个安全理念，不特指某个技术或某个方案。我们必须首先树立零信任理念，充分认识到这是一个趋势和必须要实施的。但是，零信任是一个旅程，而不是大规模更换基础设施或业务流程。单位应寻求逐步实施零信任原则、流程变更和技

术解决方案，以保护其最高价值的数据资产。大多数政府机构和企业将无限期地继续以零信任和基于边界的混合模式运营，同时继续投资于正在进行的 IT 现代化计划。

(2) 实施零信任安全，从基础安全开始。

要实施零信任安全，网络基础设施可以先不动，先从基础安全做起。什么是基础安全？首先就是网站系统 https 加密，这是最基础的基础，无论是内网还是外网系统，都必须全部实施 https 加密，因为 http 明文传输无法保障机密信息的安全，内网明文流量也是不安全的，据统计安全事件的 70%都是从内网开始的。也就是说：所有 http 流量无论是浏览器访问、手机 App 访问还是系统软件 API 访问都必须改造成 https 加密流量，服务器端都必须部署 SSL 证书。这个改造的成本低至几百元/年/网站，不仅满足了零信任安全改造的要求，而且满足了《密码法》合规改造的要求。

第二个基础安全就是邮件加密，明文邮件都是不可信的，无法保证邮件发送者身份可信，无法保证邮件内容不会被非法篡改，无法保证邮件内容不会被泄密。零信任安全的第二个网络流量安全就是加密电子邮件流量，用电子邮件证书实现端到端加密，保证邮件从用户端加密发出、传输和存储在云端，确保电子邮件的全生命周期安全。这个改造的成本也非常低，每个邮箱每年仅需几十元！不仅能满足零信任安全改造的要求，而且能满足《密码法》合规改造的要求。

第三个基础安全就是代码签名，不仅仅是各种电脑软件的代码签名，更重要的是数字签名各种远程升级的代码，各种设备系统的 OTA 空中升级系统必须改造为只信任有特定 CA 签发的代码签名证书数字签名的代码软件，只有这样，才能有效防止各种设备系统的恶意攻击。

第四个基础安全就是文档签名，不信任所有无数字签名的电子文档，政府单位发布的任何文档都应该有可信数字签名，一网通办的办事结果文件都必须有发布单位的数字签名，只有这样，老百姓才不会上当受骗，各种防范电信诈骗的努力才会真正能达到事半功倍的效果。

以上四个基础安全改造第一个最重要，这是重中之重，因为各种政务服务和商业活动都已经搬到网上了，如果不采用全站 https 加密，则根本无法保障个人机密信息和企业商业秘密不会被非法窃取和非法篡改，这些安全问题仅仅依靠法律是不够的，必须有相应的技术防范措施来保障。

(3) 基于身份证书实现强身份认证改造，数据加密改造，网络分段改造等。

在完成了基础安全改造后，就能保障网络流量是加密的，应用和文档是安全可信的。接下来就应该着手身份认证系统改造，彻底关闭不安全的用户名和口令的认证方式，采用身份证书来实现强身份认证。给每个用户颁发身份证书，用户访问任何资源都必须出示相应级别的身份证书并通过认证。所有设备也都必须有身份证书，这个身份证书可以是 SSL 证书，因为 SSL 证书也有身份认证属性，可以证明自己的服务器身份。

完成身份认证系统改造后就要着手用证书加密重要数据的改造，机密数据用证书加密后存数据库，用户通过身份认证后获取此数据，则解密后用用户的公钥加密返回给用户，用户用自己的私钥解密获得数据明文。同时，在生成数据时必须调用时间戳服务获取时间戳签名数据与数据一起存库，这样就可以证明数据的生成时间可信和数据并没有篡改。

当然，网络细化分段当然也可以同步进行，让不同的应用位于不同的网段，以便通过认证的用户能更高效快捷地获取数据。但是，网络的分段的前提还是必须先完成基础安全改造，满足零信任的基础安全要求。

总之，零信任是一个没有终点的旅程，需要从基础安全做起，需要采用密码技术来实现零信任基础安全，需要我们一步一个脚印脚踏实地的往这个方向前进，只有这样才能最终达到零信任的最高安全境界。

王高华

2021 年 12 月 22 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。