解析网络安全设计中的10大常见错误计算机等级考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E8_A7_A3_E6_9E_90_E7_BD_91_E7_c98_645138.htm 尽管我们都知道网络安全是关系到企业信息安全的最重要一环，但是我实际看到的情况却是，很多企业对于网络设计的安全性并不是非常重视。下面，我将介绍几种在网络安全设计时常见的错误，这些错误会对未来企业的网络安全构成严重影响。 1: 设置好就高枕无忧了 我要讲到的第一个错误更偏重于计划而不是网络设计。这种错误我一般将它称之为“ 设计好就高枕无忧 ”。犯这种错误的企业一般会下大力气去设计一个安全的网络，但是却忽略了后期对于这个设计的定期性的重新评估。因为网络风险是在不断变化的，因此企业的网络安全设计也应该不断进化。最好的办法就是定期对网络安全设计进行重新评估。 2: 在防火墙上开放过多的端口 我们都知道开放过多的端口没有好处，但是有时候又不得不多开放几个端口。就拿Microsoft Office Communications Server 2007 R2来说吧，如果你计划提供外部访问功能，那要多开十几个端口。另外， OCS 2007 R2还会随机开放大量的端口。这种情况下，网络安全管理员该怎么办呢？ 最好的解决方案之一是采用逆向代理（如微软的ForeFront Threat Management Gateway）。逆向代理的位置介于互联网和本地需要开放多个端口的服务器之间。这样设置后，服务器不需要再开放大量的端口，而外界对服务器的连接请求会先经过逆向代理进行拦截和过滤，并传递给服务器。这种设计不但能让服务器在外网前隐藏起来，还能帮助确保外部的恶意请求不会到达服务器。 3: 不同应用程序混

在一起 在经济危机下，企业很少会花钱添置新设备，因此尽可能压榨现有设备资源就成了唯一选择。在这种前提下，企业一般会在一台服务器上安装多个应用服务，让一台服务器扮演多个角色。虽然这么做并不是被禁止的，但是在计算机行业有一个规律，即代码越多，出现安全漏洞的机会就越多。 我并不是说每个服务器只能运行一种应用程序，或者扮演一种服务角色，但是至少我们应该仔细考虑应该把哪些应用程序或服务角色合并到一台服务器上。比如，在最小需求下，一个Exchange 2007需要三个服务器角色（hub transport, client access, 以及 mailbox server），你可以将这三个角色整合到一台服务器上。但是如果你要为外部客户提供Outlook Web Access服务就不要这样做了。因为Client Access Server服务器角色需要用到IIS来实现Outlook Web Access，也就是说，如果你将客户接入服务器角色和hub transport以及mailbox server 角色放在了一台服务器上，实际上就是把你的邮箱数据库开放给了互联网上的所有黑客。 4: 忽略了网络中的工作站 去年有个记者通过电话采访我，他问：您觉得对于网络安全威胁最大的是什么。我的回答是：网络里的工作站是网络安全的最大威胁。现在我仍持同样看法。我总是看到企业在不但的加强网络服务器的安全性，但同时却忽视了网络内的每一台工作站。除非工作站的安全防护措施非常好，否则使用它的员工很容易在不经意间让系统被恶意软件入侵。 5: 在必要的情况下没有使用SSL加密 我们都知道，当用户需要在网站上输入敏感信息时（比如用户名，密码，信用卡卡号等），网站都会使用SSL 技术对信息进行加密。但是很多企业在这个问题上犯了错。我曾经遇见过很多次，企业将敏感信息和非敏感

信息混合在一个网页中，当用户访问该页面时，会收到一条提示，询问用户是否同时查看安全内容和非安全的内容。大部分用户在面对这个提示时都是选择同时显示安全和非安全的内容，这就为网络安全带来了隐患。 一个不太明显但是更常见的错误是，企业很少加密自己网站上的一些关键页面。在我看来，任何涉及安全信息，安全设备以及联系人方式的信息都应该经过SSL 加密。这并不是因为这些内容都属于敏感信息，而是通过这些加密页面让用户确信自己所访问的是官方网站，而不是似是而非的网络钓鱼网站。 6: 使用自签名证书 由于一些企业完全忽视了SSL加密的重要性，因此微软开始在它的一些产品中加入了自签名的证书。这样用户在浏览网页时，就算企业的网站没有要求获得证书情况下，也可以使用SSL加密。 虽然自签名证书要比没有证书强，但它并不能作为一个来自受信的证书颁发机构所颁发的证书的替代品。自签名证书的主要作用其实只是用来激活软件的安全功能，直到管理员采取了相应的安全措施。虽然自签名证书可以实现SSL加密，但是用户会收到浏览器的警告信息，提示用户系统并不信任此类证书。另外，一些基于SSL的web服务（比如ActiveSync），由于信任关系，并不完全兼容自签名证书。 7: 过多的安全记录 虽然记录各种网络事件很重要，但是避免记录内容过于冗长也是很重要的。太长的日志会让管理员很难从中发现重要的安全事件。因此，与其将所有系统事件都记录下来，还不如将重点放在那些真正重要的事件上。 8: 随机分组虚拟服务器 虚拟服务器一般会根据其性能在主机上进行分组。比如在一台服务器上搭建了一个对性能要求较高的虚拟服务器应用后，与之搭配几个对系统性能要求较低的

虚拟服务器，可以实现资源的合理化应用。从资源利用的角度上说，这么做非常正确，但是从安全性的角度看，就不见得了。 从安全的角度，我建议在一台独立的服务器上放置针对互联网应用的虚拟服务器。换句话说，如果你需要搭建三个针对互联网用户的虚拟服务器，你可以考虑将这三个 虚拟服务器分为一组，放置在同一台主机上，但是不要将架构类服务器（如域控制器）放在同一台主机上。 之所以这样建议，是针对虚拟服务器上的溢出攻击。所谓溢出攻击，是指黑客从一个虚拟服务器中溢出，进而控制主机的攻击。虽然就我所知，目前现实生活中还没有真正出现过此类攻击，但是我肯定这是迟早的事。一旦那一天到来，同一台主机上如果还安装了其它重要的虚拟服务器，那么对整个企业网络来说，将是一个灾难，对于网络管理员来说，解除威胁也将变得更困难。 9: 将成员服务器置于DMZ 能避免的话，就尽量不要将任何成员服务器置于DMZ中。否则，一旦被入侵，这台成员服务器将可能泄露出很多有关活动目录的信息。 10: 升级补丁需要用户自己安装 本文所介绍的最后一个常见的网络安全错误是安全补丁的安装完全依赖用户人工操作。最近我见到很多公司网络中的电脑都依赖于Windows的自动更新服务进行自动打补丁。不幸的是，这类设计需要用户自己点击鼠标来进行补丁安装确认，而很多用户都知道，安装完补丁后系统会重新启动。为了避免这种麻烦，很多用户选择了停止自动更新。因此，与其将安装补丁的权利交给用户，不如通过某种补丁管理解决方案，自动将系统补丁分发到每台电脑上，绕过用户的任何操作。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com