企业 IT 系统大排查

安全趋势：生物认证技术引领 IT 安全新趋势

IT 安全大排查：

采购篇/系统篇/设备篇/云计算篇

大话安全：金钱买不来 IT 安全

生物认证技术引领 IT 安全新趋势

在 Google2013 年最常见密码榜单上，你会发现 123456 已经成功登顶了。是的，那些非常容易记住超级容易破解的最受欢迎密码们仍然还在被使用，这个结果可能会让首席信息官们很无奈，但还好在可期待的未来会有点好消息。

专门从事生物认证的创业公司现在是到处开花。使用生物特征认证技术能够识别身体这样一台有独特代码的，由各种稀有零部件构成的精密仪器。指纹仅仅是个开始。虹膜，视网膜，面部特点和语音特点，甚至一个人的步态或心脏节律，都可以用作个性化密码的基础。这些独特的身体特征可以被用来验证一个人的身份 –以及限制访问和保护敏感信息。

一个人体如何作用于 IT 安全的例子是 EyeVerify 公司的专利技术。这家位于 Kansas 的创业公司基于眼球中眼白球血管分布图形（他们称之为“眼纹”）开发了一款移动银行应用程序。

眼睛就是验证密码

这一切是不是听起来有点少数派报告(科幻小说) 如果在 2002 年的话 那大概的确如此。EyeVerify，这家成立于 2012 年的创业公司以及 2014 年消费电子展两次获奖者，却并不奢求太过未来的技术，公司首席执行官和联合创始人 Toby Rush 说道。你智能手机上的摄像头就足够啦。旧有技术与 Kansas 密苏里大学副教授兼公司首席科学家 Reza Derakhshani 建立的非常巧妙并经过工程师们微调的算法相结合，效果刚刚好。

有点怀疑？是的，一个人的眼睛可能因为发痒或干燥或摄入酒精（就是在说你，科罗拉多州）或大麻而变红 - 但血管形态呢？ “他们不会改变的。” Rush 说，“他们可能会看起来更明显，但形态本身并不发生改变。”

初始图像捕捉被称为注册程序，Rush 说。用户需要从一侧向另一侧转动眼球，以便摄像头捕获每一侧虹膜的血管图形 – 每个用户 4 个眼纹 – 从而建立验证密码。当用户需要解锁安装在员工智能手机

或平板电脑上的移动应用程序时，被通过网络传输以验证身份的只是验证密码而不是生物特征本身。

那么，这种东西的精确水平如何呢？据 Rush 所说准确度高达令人震惊的 99.99 % 。外界评论并不十分信服这一点。一篇发表于 2013 年 12 月麻省理工学院技术评论上的文章称，该公司需要做进一步的测试，以更彻底地确认该数字。

保持领先一步

那么，我们不可避免的要谈谈众所周知的硬币的另一边了。无密码的前景确实是令人兴奋的，但大部分开发生物认证技术的创业公司都还只是-创业公司。该技术仍是新兴技术，这意味着还有许多故障和错误需要解决。并且，至少在目前，这些错误都足以否定掉任何形式的威胁到 IT 安全或工作安全或者说用户良好意愿来的企业解决方案。

“这是所有生物识别技术共同的问题，”佛罗里达州迈阿密安全服务提供商 Immunity Inc.公司首席技术官 Dave Aitel 说。“总有问题问我到底有多么严格，而一般来说回答都是并不多么严格，因为没有什么比冲着一台机器瞪着自己的眼睛却被拒绝访问更令人沮丧的了 。

Aitel 认为首席信息官们需要花更多的时间搞清楚哪些数据是绝密的并把它们恰当的划分出来。他明白这可能很难- 尤其是考虑到不断增长的打破数据孤岛的需求和整个企业的集成数据 - “但是除非你已经真正划分了数据 ，否则移动安全和云安全都没有任何实际意义。”他说。

但这并不意味着首席信息官们要忽视生物认证技术。相反 ,Aitel 建议他们去了解这些技术的局限性：例如指纹技术，它不够隐私。我们会把指纹留得到处都是。而一旦指纹验证被黑（你有没有听说过小熊软糖的事例？），指纹却并不像密码那样可以被重新编程。不过，他说，“这聊胜于无，毕竟很多人一无所有。”

由指纹推及虹膜以及视网膜，包括用户眼白上的血管图形，很明显的，这些系统可能（毋庸置疑都会）被欺骗。CIO 们需要接受这一事实，与其试图建立一个不能被黑客攻击的安全系统，倒不如弄清楚

如何给网络罪犯设置足够多的障碍，以阻止其中断服务或接触到最敏感的信息。生物识别技术可以加多一层保护。

“生物识别技术将会是重要的，而且是有需求的，Target 公司最近的信用卡灾难正说明了这一点。”马萨诸塞州剑桥 Forrester Research 分析师 JP Gownder 说。 “我们甚至不能保证作为经济基础的传统系统。所以说，那些只想要保护他们的数据的公司，显然缺了点什么。 ”

而且 Gownder 认为，一些生物识别技术对企业首席信息官们来说已经足够强大了，应该被像 Target 那样经历过违约的公司予以考虑。但是，在选择供应商时也要保持谨慎，他补充道。 “你要跟已经达到一定规模的，或者至少与有一定规模公司有某种程度合作伙伴关系的供应商进行合作，这样你才能确定这个解决方案不会昙花一现。”

（本文链接：http://www.searchcio.com.cn/showcontent_80309.htm ）

安全大排查之采购篇

IT 人员应向供应商确认产品安全性

德国明镜周刊获得的文件显示，美国国家安全局（NSA）一直在有组织地在世界顶级供应商的防火墙、路由器、个人电脑和服务器中植入后门，其中包括思科、瞻博、惠普、戴尔和华为。明镜周刊还在 NSA 后门泄密事件报告指出，安全局的做法还不仅限于此，他们还截获这些公司向客户销售的硬件，然后在上面偷偷安装隐藏的监控设备。

一位就职于全球制造商的网络工程师 Jonathan Davis 说：“我更关心的是 NSA 后门可能在企业网络中产生的漏洞，特别是明镜周刊这份报告的信息发布之后。IOS 更新或软件更新都无法解决这些漏洞。”

Davis 指出，几年前，一旦发生来自海外的攻击，公司会因此损失几百万美元。黑客会盗取数据，然后用这些数据开发克隆产品，从而继续破坏公司收益。Davis 担心 NSA 的监控可能会引发更多的工业间谍和数据盗取活动，从而导致“金钱直接从公司本身流出”的后果。

旧金山 Electronic Frontier Foundation 的数字公民自由团队的法务专员 Nate Cardozo 说："如果 NSA 在路由器及其它网络硬件上发起零日攻击，那么其他国家肯定也已经知道并在设法发起相同的攻击。可能在这种事情上，NSA 是做得最好的，但是他们就不是唯一会做这种事情的组织了。如果 NSA 真的在做零日攻击的勾当，那么这是极不负责任的。"

明镜周刊的 NSA 后门报告意味着：您的网络也成了攻击目标

几乎每一位网络工程师都应该认识到他或她的企业网络也是一个潜在攻击目标，这些攻击不仅可能来自于 NSA 监视和硬件黑入，也可能来自于其他企图攻击这些设备的人。

Cardozo 说："毫无疑问，NSA 将会继续危害那些为美国民众提供通信或事务服务的美国公司。"他指出，这些攻击目标涉及各个领域，既包括电信提供商和互联网公司，如谷歌和雅虎，也包括金融服务、医疗和交通行业。

明镜周刊的 NSA 报告引用的档案日期为 2008 年。这些档案中许多被修改过的产品已经停产，如 Juniper NetScreen 和 Cisco PIX 防火墙。工程师不能假定新产品就一定是安全的。网络工程师 Nick Buraglio 指出，NSA 一定会跟上市场发展，针对每一个供应商和每一个版本的产品开发攻击程序。此外，他还断定 NSA 的攻击目录要远远大于明镜周刊所曝光的范围。受攻击的范围肯定不仅仅只有思科、瞻博、惠普、戴尔和华为。

Buraglio 问道："最恐怖的事情是这些档案已经非常旧。从技术角度看，2008 年已经恍如隔世。他们的最新动作可能会更让人发指!"

Buraglio 说："要开始分析流量，检查数据流日志。从中发现是否有一些不合理的迹象。如果您自己没有发现异常情况，那么还要询问上游提供商，看看他们是否遇到了异常数据。一定有一些设备是不会破坏数据的。流量不会说谎。我一直坚持一点：对网络执行基线分析。但是有很多人不这样做。记住，数据越多越好。"

由于 NSA 监视程序涉及的范围非常大，因此所有 IT 人员都应该考虑数据的安全性和基础架构中设

备的完整性。Cardozo 说："微软已经指出，他们现在已经将美国政府视为一个永久性高级别威胁，而我认为这绝对是正确的。一家公司有责任保护其客户数据不会受到一些已知攻击手段的危害，而且有一点也变得更清晰了——NSA 的魔爪不会放过美国自己的公司。"

思科及其他几个供应商已经公开否认参与或了解 NSA 的后门黑客和漏洞植入行为。思科已经表示公司正在调查这个问题，确保自己的产品是安全的。

Buraglio、Davis 和 Cardozo 都认为这些供应商说的是实话。但是，IT 人员应该更主动地与供应商严正交涉这些问题。

Cardozo 说："其中一个最大的问题是：'我如何确定我数据中心的硬件就是从你那些购买的原版硬件？'如果他们能够给客户提供一些电路图，甚至派技术人员打开并检查设备，保证设备里没有额外的部件，那么或许这样才能消除客户的疑虑。"

供应商也需要把产品做得更安全，让 NSA 无从下手。Cardozo 说："如果这意味着需要移除 JTAG（Joint Test Action Group，联合测试行为组织）端口，或者要移除 I2C，那么硬件供应商就应该开始这样做。如果他们在主板上留下调试端口，那么就可能给 NSA 留下可乘之机。或许现在是时候开始在产品出厂之前关闭这些漏洞了。"

Buraglio 准备与供应商沟通这些问题，不仅仅包括那些已经购买过他们产品的供应商。他希望从将来可能购买或推荐的供应商那里得到保证，其中不公限于明镜周刊所报道的供应商。他准备询问的一个主要问题就是，他们兼容联邦信息处理标准（FIPS）的设备是否提供了一些防御这些黑客和漏洞植入行为的保护措施。兼容 FIPS 的网络设备可以向工程师报告它们的完整性。

Buraglio 说："FIPS 一定会验证系统二进制文件的完整性。它会以加密方式验证操作系统。如果有一些东西被修改过，那么密码就无法匹配。大多数人的网络设备都兼容 FIPS，但是他们可能还没有用过，因为这有点复杂。我想知道它是否能够保护设备不受 NSA 攻击的影响。您也应该向供应商询问这个问题。"

Davis 指出，他已经与供应商商定的约谈会议，讨论关于 NSA 泄密事件的短期和长期响应方式，但是他认为他还不能拆开各个设备逐一检查是否有监视程序植入。他说："即使我开始逐一检查所有设备，但是我的网络中一共有近 25，000 台设备，而且这还只是网络和防火墙设备。我们需要在系统级上定位这些设备。在不久的将来，防火墙供应商可能会提供一些工具，帮助我们检查这些设备是否有问题。"（本文链接：http://www.searchnetworking.com.cn/showcontent_79784.htm ）

安全大排查之系统篇

企业系统安全管理和强化的十个建议

企业系统的安全管理运维涉及到公司信息化系统和数据的防入侵、防泄露工作，这是为所有 CSO、COO 非常关注的基础性工作。虽然基础，但是一旦处理不到位，将会给企业带来重大数据、经济损失或者声誉损失。本文针对企业系统的安全管理，给出了 10 个非常实用、有效的系统强化措施，能够较好地帮助企业系统管理员发现和提前处理系统可能存在的风险和漏洞，从而在事前保证企业系统的安全运营。

1、从运行路径中去掉"."

在超级用户（root）模式下，用户必须明确正在运行的命令是用户想要的。考虑下面的场景，用户在哪里登录了超级用户，那么用户的路径变量就是

.：/usr/bin：/usr/sbin：/bin：/sbin.

用户在 ls 目录下创建了一个包含如下命令的脚本：

```
#!/usr/bin/ksh
cp /usr/bin/ksh /tmp
chown root：bin /tmp/ksh
```

chmod 6755 /tmp/ksh

rm -f ls

/bin/ls $*

现在 A 用户呼叫并上报一个问题，在他的主目录里有些不明文件。用户作为超级管理员，使用 cd 命令进入他的目录并运行 ls -l 命令去查看。突然，在用户不知情的情况下，A 用户可以运行一个 shell 脚本来获取用户的超级用户权限!

这样的情况经常发生，但是很容易避免。如果在用户的路径中没有“.”，用户会看到一个名为 ls 的脚本在他的主目录中，而不会去执行它。

2、规避风险脚本

当用户写一个脚本，总是指定正在使用的应用程序的完整路径。参考下面的脚本：

#!/usr/bin/ksh

date > log

find . -mtime +7 -ls -exec rm -rf {} \; >> log 2>&1

虽然只有三行，并且只有两行执行命令，然而却存在很多安全漏洞：

- 它没有指定一个路径。
- 它没有给出日期的完整路径。
- 它没有给出查找的完整路径。
- 它没有给出 rm 的完整路径。
- 它执行错误检查。
- 它没有验证目录的正确性。

让我们再看一下另外一个脚本是如何解决其中的一些问题的。

```
#!/usr/bin/ksh
cd /directory || exit -1
PATH=/usr/bin; export PATH
/usr/bin/date > log
/usr/bin/find /directory -mtime +7 -ls -exec /usr/bin/rm -rf {} \; \
>> log 2>&1
```

第二行，cd /directory || exit -1，告诉 ksh 的尝试使用 CD 命令进入/directory。如果命令失败，它需要退出脚本并且返回一个–1 的代码。在 Ksh 命令中||意味着“如果上个命令失败”，&&则意味着“如果上个命令成功”。举一个额外的例子，使用命令 touch /testfile || echo Could not touch 创建一个名为/testfile 的文件，或者如果文件不能被创建（也许用户没有足够的权限来创建它），那么在屏幕上会显示“Could not touch”。使用命令 touch

/testfile && echo Created file 来创建/testfile 文件，如果 touch 命令成功，在屏幕上只会显示“Created file”。用户检查的条件将决定用户是使用||还是&&。

如果脚本继续运行，用户将进入/directory。现在用户可以明确指定用户的路径，如果用户忘记了完整路径可以使用系统搜索命令来锁定。这个方法的例子并没有在这个小脚本中，但它是一个很好的习惯，尤其是在当用户写长的并且更复杂的脚本时;如果用户忘了指定完整的路径，用户的脚本调用木马程序几率将会非常小。

接下来用户调用 date 的全名是 ;/usr/bin/date。用户也可以完全指定/usr/bin/find 和/usr/bin/rm。通过执行此操作，用户可以让希望在用户系统中插入木马程序并且在用户不知觉的情况下运行的人更加困难。毕竟，如果他们有足够的权限来修改文件/usr/bin，他们可能就有足够的权限来做任何他们想做的事情。

当编写一个脚本，经常需要遵循这些简单的规则：

- 总是指定一个路径。
- 总是为每个应用程序使用的完整路径。
- 始终运行错误检查，特别是在运行具有潜在破坏性的命令时，如 rm 命令。

3、盯紧容易忽视的计划任务

用户知道什么工作在用户的系统无人值守下正在运行吗？当系统安装完成后，许多操作系统都提供了各种各样的自动化任务自动为用户安装和配置。其他工作随着时间推移而增加的应用程序，会定期的运行。

要掌握用户的系统，用户需要清楚的了解它正在运行的程序。定期审核用户的计划任务列表文件中哪些程序正在运行。许多系统的计划任务文件存储在/var/spool/cron 中。一些计划任务守护进程另外支持每小时计划任务，每周计划任务，每月计划任务和每年计划任务的文件，以及一个 cron.d 目录。使用 man cron 命令来将确定用户的计划任务守护进程的确切功能。

在每个目录检查所有的文件。注意每个工作的所有者，如果用户的计划任务守护进程(crond 服务) 支持，请锁定计划任务并且只对需要使用的用户 ID 开放。请注意每个正在运行的文件和它所运行的时间。如果预定的计划用户不清楚，研究来确定到底是什么文件以及用户是否需要它。如果用户正在运行一些用户觉得他们不需要的东西，与他们联系，问其原因，然后进行相应处理。

持续跟踪用户的计划任务作业并且定期检查他们是否有任何的变化。如果用户发现有些事情已经改变了，进行调查并确定原因。持续跟踪用户的系统正在做什么是保持用户系统安全的一个关键步骤。

4、记录所有守护进程的日志

众所周知，如果守护进程不在第一个时间记录任何信息，那么保存和记录日志也是没用的。在默认情况下有一些守护进程会创建日志，有一些则没有。当用户审核用户的系统时，验证用户的守护进程是

否记录日志信息。

任何公开的守护进程都需要配置日志，日志需要被保存。试着访问用户的一些服务，查看用户的日志服务器收集的日志。如果没有，阅读该服务的线上说明手册并查找所需的操作来激活记录。启动它，并尝试再次使用该服务。持续检查用户所有的服务直到确保记录和保存了所有的日志。

5、运行 CIS 扫描

互联网安全中心（CIS）创建了一个系统安全基准测试工具。用户可以从 www.cisecurity.org 下载这个工具，对用户的本地系统进行审计并报告其分析结果。该工具会扫描到好的和坏的结果，并在扫描结束后给出一个整体排名。扫描工具可用于 Solaris， HP-UX，Linux，Windows，以及思科路由器。

CIS 基准测试最好的地方是他们给出的说明，报告中并不会只是简单的提到“用户有什么，哪个不好”;它会告诉用户为什么说它不好的更深层的原因，它可以让用户自己决定是否要禁用“坏东西”或维持原样。基准工具可能会检查很多用户没有想到的地方，并且给用户一份系统的详细报告。

下载并解压缩 CIS 工具，阅读 README 文档和 PDF 文档。 （PDF 文档针对系统安全提供了很好的参考材料。)按照 README 文档说明进行安装包安装 ,工具安装完成后 ,用户应该有一个目录/opt/CIS。运行命令 cis-scan 来了解用户的系统。这取决于用户服务器的速度和所连接的硬盘数量，扫描可能需要花很长时间才能完成。扫描完成后 ,用户将会有一个名为 cis-ruler-log.YYYYMMDD-HH :MM :SS.PID 的文档。该文档是系统的总结报告，包含了所有的测试结果。其中该文档不包详细信息--这意味着只能作为索引来参考扫描工具自带的 PDF 文档。逐行审阅 ruler-log 文件，如果有一个负面的结果，建议在 PDF 文档中确定是否可以执行变更。大部分变更可以在不影响服务器的操作下实现，但并不是所有。谨防漏报;用户可能需要使用 PortSentry 工具查看端口 515 是否存在 lp 漏洞，这会导致了 CIS 工具报告用户有 lp 漏洞的错误。在报告末尾，数字越高用户的系统越“坚固”。

这是一个很好的信息安全工具，定期在用户的服务器上运行可以保持服务器的健康。访问互联网安

全中心的网站，随着关注该工具的不断发展和变化。

6、运行过程避免使用超级用户特权

许多运行在的服务器上的服务并不需要超级用户权限来执行他们的功能。通常，他们不需要任何特殊权限以外的读取和写入数据目录的能力。但由于 Unix 安全措施规定由超级用户权限的运行的开放的 TCP / IP 端口必须低于 1024，加上这一事实，大多数著名的端口都低于 1024，意味着用户的守护进程必须在超级用户权限下开放其端口。

这种困境有几个解决方法。第一，最安全的并不是运行所有的服务。如果守护进程没有运行，那么它不需要作为超级用户运行。然而，这并不是每次都管用的。有时候用户也需要为守护进程提供运行服务。在这种情况下，创建一个专门的用户 ID 来运行守护进程，并且尽可能的严格控制它。只使用这个 ID 写入可写的目录，并且不要给这个 ID 特别高的权限。然后更改启动脚本，守护进程只属于这个新的用户 ID。现在如果攻击者利用漏洞攻击用户的服务器并且损害用户的守护进程，攻击者将获得非特权账户并且必须做进一步的工作来获得超级用户权限，在更多的损失发生之前将给予用户更多的时间来跟踪和阻止他或她。

7、扫描并处理高权限文件

所有系统都有设置用户 ID（SUID）和设置组 ID（SGID）文件。这些文件可以使用特定的用户或组来运行应用程序、脚本和守护进程，而不是个人用户 ID 或组 ID 来运行。top 命令是一个很好的例子，它的运行权限较高，所以它可以扫描内核空间中的进程信息。因为大多数用户的默认权限不能读取这些信息，top 需要运行更高的权限是有必要的。

许多操作系统允许用户的指定某些磁盘不支持 SUID 和 SGID，通常是通过在用户的系统挂载文件中使用一个命令来完成。在 Solaris 中，用户会在/etc/vfstab 中指定 nosuid 命令。例如，使用 nosuid

命令将/users 安装在磁盘 c2t0d0s3 上，用户可以输入如下命令：

/dev/dsk/c2t0d0s3 /dev/rdsk/c2t0d0s3 /users ufs 2 yes nosuid

这个/users 安装引导并禁用了 SUID 和 SGID 应用程序。应用程序仍然可以运行，但是 SUID 和 SGID 位将会被忽略。在所有的文件系统上禁用 SUID 和 SGID 是一个良好的安全实践。

不过，用户需要定期扫描用户的系统并获得一个所有存在 SUID 和 SGID 进程中的列表。查找 SUID 的命令是：-perms +4000，而查找 SGID 的命令则是：-perms +2000。在整个服务器扫描所有 SUID 文件，运行这个命令：

find / -type f -perms +4000 -ls

-type f 命令只是查看“常规”的文件，无法查看目录或通过其他命名管道的特殊文件等。这个命令可以列出每个文件上的 SUID 位设置。仔细检查和验证所有输出和真正需要 SUID 和 SGID 的文件，对于不需要的，毫不犹豫地进行清除处理。

8、掌控开放的端口

在用户向外界发布用户的系统之前，用户需要知道哪些端口是打开的并且允许连接。有些端口是在用户不知情的情况下开放的，用户应该在人们通过这些端口访问用户的服务器之前关闭它们。有一些工具可以让用户知道用户的系统是暴露的。

可以使用 Netstat 工具来进行排查。几乎每一个操作系统都附带 Netstat 命令。Netstat 是一个简单的工具，可以显示用户的网络信息，如网络端口、路由表和网络连接信息。Netstat 工具显示了/etc/services 下所有已经被使用类似人名定义的端口，使其更容易解析和导出。这是一个确保用户系统上/etc/services 持续更新的好理由。在用户的系统上使用 man 命令来发现 netstat 的能力。

下面我们将通过一个简单的例子来说明：

netstat

Local Address Remote Address Swind Send-Q Rwind Recv-Q State

server.smtp 192.168.3.4 6144 0 65700 0 CONNECTED

在这个例子中，有人从 IP 地址 192.168.3.4 连接到用户服务器的 SMTP 服务。用户应该运行 SMTP 吗？应该允许这个人连接到服务器吗？注意，重大漏洞。用户打开了远程连接，用户最起码应该使用 TCP Wrappers 安全机制来保护它。用户应该禁用它吗？

netstat -a | more

UDP： IPv4

Local Address Remote Address State

localhost.ntp Idle

TCP： IPv4

Local Address Remote Address Swind Send-Q Rwind Recv-Q State

*.telnet *.* 0 0 24576 0 LISTEN

建议用户花些时间去学习 netstat 吧。如果用户学会了如何使用，它将为用户提供丰富的网络信息，并且让用户清楚地看见是谁在什么时间连接到了用户的系统。

另一个有用的实用程序是 lsof （打开的文件列表） 工具。刚开始它只是一个用来显示有哪些进程打开了文件的简单工具，但是现在已经进化到可以显示端口、通道和其他通信。一旦用户安装了 lsof 工具，尝试一下。只运行 lsof 来查看系统上打开的所有文件和端口。用户可以感受一下 lsof 工具能做什么，同时它也是一个快速审核系统的绝佳方式。lsof | grep TCP 命令将显示系统上所有打开的 TCP 协议的连接。这个工具功能非常强大，当用户需要卸载文件系统，而文件系统报告忙碌时也是很有帮助的，lsof 可以快速的显示那个进程正在使用该文件系统。

9、使用一个集中的日志服务器

如果用户负责维护多个服务器，那么检查每台服务器的日志将非常繁琐。为此，建立一台专用服务器来搜集其他所有服务器的日志消息。通过整合用户的日志，用户只需要扫描一台服务器，将大大节省用户的时间。在用户的服务器被攻破后，这也是一个好的归档文件;用户仍然可以在别的地方查阅这些日志文件。

创建一个核心日志服务器，使用高速 CPU 和大量的磁盘可用空间。关闭除 syslogd 之外的其他所有端口和服务，这个系统受到损害的几率降到最低，可能除了使用 TCP-wrapped SSH 守护进程来限制用户的工作站进行远程访问。然后验证 syslogd 可以从远程系统接收消息。这不同于从消息提供服务器到消息提供服务器。有些服务器默认接收消息，用户可能需要关掉它;有些默认不接收消息，用户需要打开它。

创建一个系统来归档旧日志并形成文件。如果用户的日志曾经被用作为证据，用户需要能够证明它们没有被更改过，用户需要出示他们是如何创建的。建议用户压缩一个星期以上的所有带时间戳的日志并且通过只读的媒体，例如 CD 光盘来复制他们。

一旦用户有了一个接收日志的服务器，用户需要启动其他服务器指向它。编辑/etc/syslog.conf 并且确定用户想复制的信息。最起码，用户应该复制最高的紧急程度状态，紧急状态，重要信息，临界状态和警告信息和更多用户认为有用的信息。当用户知道什么是用户想要复制的信息，添加一个或多个像下面这样的/etc/syslog.conf 命令行：

.emerg;.alert;*.crit;*.err;*.warning;*.notice @ip.of.log.srvr

在这个例子中，我们将所有最高的紧急程度状态，紧急状态，重要信息，临界状态，警告和出现不寻常的事情日志信息发送到远程服务器。值得注意的是：用户可以让它们在同一时间将日志归档到远程服务器。用户也可以复制到多个日志服务器。Syslog.conf 扫描的是所有匹配的条目—syslogd 守护进程不会在找到第一个后停止。

10、保持软件更新

每款软件都有漏洞。大多数厂商对代码进行审计并且删除发现的所有漏洞，但也有些不可避免地发布到外界。某些人花大量的时间去试图找出这些漏洞;有的人会报告给厂商 ,但有的人则是自己个人利用。

实际上，偶尔发现的漏洞会补丁修补程序来修正它们。除非脆弱性严重，或在外界存在一个已知的漏洞攻击，那通常不会大张旗鼓地宣布发布这些补丁。用户的责任是偶尔查看下哪些补丁适合用户并且可以从软件厂商处下载。

许多厂商会提供一个工具来帮助您保持您的系统上的补丁。HP-UX 有软件更新管理软件、Solaris 有 patchdiag 和 patchpro，AIX 使用 SMIT，等等。至少每月运行用户的诊断工具一次，看看用户的系统可以更新的补丁 ,并决定是否需要安装它们。每个周日下午留出至少一个小时（或者更多的时间）专门作为系统维护时间，利用这段时间来安装补丁和执行其他必要的维护。

用户应该养成为一个习惯经常去网站上查看用户安装的每个应用程序是否有 bug 修复或安全补丁发布。使用前面创建的应用程序列表来确定是否有适用于用户的补丁。当用户更新完补丁后记得更新用户的列表信息。

（本文链接：http://www.searchsecurity.com.cn/showcontent_79623.htm ）

安全大排查之设备篇

数据、应用和设备：三维度做好企业移动安全管理

BYOD 的盛行使得企业移动应用管理已经成为企业 CIO、CSO 需要高度关注的一个问题。解决不好这个问题，将会使得员工工作效率低下，企业应用存在安全隐患或者风险。因此，企业急需要制定一套企业移动应用管理体系，在该体系中，数据、应用和设备管理是非常关键的三个要素。本文将详细介绍这方面的安全管理最佳实践。

实践一：数据隔离是核心

企业移动应用管理最核心的关键是进行数据管理。用户在移动设备中使用的不仅仅是个人数据，还会大面积地使用企业数据，那么如何进行有效的进行企业和用户的数据隔离是非常重要的问题。“数据隔离”是指用户在指定的企业应用内阅览和编辑的所有内容都不能拷贝到该应用外部，也不能把外部的数据拷贝到该应用里面来。从企业的角度看，返种手段既保证企业数据不被外泄，也防范个人数据中可能存在的信息（如新闻、娱乐信息）以及病毒、木马等非法程序在企业内部的传播和感染。从用户的角度看，用户个人数据都被隔离在“安全沙箱”之外，因此，不必担心 BYOD 设备中的个人数据会在移动办公的过程中流入企业内网而引起个人隐私的泄露。

当然，安全的要求不能够以牺牲用户体验和办公效率为前提。所以为了保证数据隔离后的文档可使用性，企业移动应用在文档办公方面有一定的要求，企业应用一方面可以通过文档转换将主流的 Windows Office 文档转换成移动终端系统可识别的格式，并呈现给用户，譬如，将 PowerPoint 格式转换为图片格式;也支持对 ZIP、RAR 压缩包的解压、PDF 文档的呈现、GIF 等图片格式的呈现。 文档转换模块为安全浏览器和安全邮件客户端提供方便快捷的文件在线浏览能力，通过这个转换，用户可以用安全浏览器直接浏览公司文档，也可用安全邮件客户端打开邮件附件中的各类文档，而不必担心手机或平板不识别 Office 文档的问题，也不必安装第三方的文字处理软件。

实践二：应用管理需强化

企业应对应用实现细粒度的管理，主要是对企业移动应用的管理。由于实现了实践一中介绍的数据隔离，则不需要对个人移动应用实现太大强度的管理，否则容易造成用户可用性的丧失，当然，对于安全意识较好的用户来说，也可以对其采取相关的机制来进行保障，而在一般情况下，仅对企业应用进行控制也是可行的，毕竟已经进行了数据的隔离，应该将安全的力度放在企业数据区的安全防护上比较合理。

企业应用管理较常采取黑白名单的方法。其中，黑名单是通过禁止用户将黑名单中出现的应用安装在企业数据区来实现安全;而白名单是明确地给出用户可以将哪些应用安装在企业数据区。具体黑白名单的定义由企业根据实际情况决定，这个没有统一的规定。

实践三：设备管理打基础

设备管理是移动安全方案的一个核心组件，通过 MDM（移动设备管理，Mobile Device Management）可以避免用户在移动终端上操作可能带来的安全隐患，防止移动终端不慎丢失后造成数据泄露。企业需要明确使用 MDM 来达到如下安全管控效果：

资产管理和策略管理：在对 BYOD 设备执行 MDM 安全管控前，首先要将用户的 BYOD 设备注册到企业的 MDM 管理平台，可与员工签署相关使用协议，然后将 MDM 客户端安装到 BYOD 设备。然后，企业便可根据双方的协议，通过管理平台对移动终端进行状态查询、安全管控策略下发、应用分发等操作。管理员可据企业的实际情况和协议要求，通过 MDM 策略管理后台对终端进行“设备硬件硬件控制”、“越狱检测”、“远程锁定”、“GPS 定位”、“远程擦除”、“应用一键配置”等操作。若员工需更换办公终端或离职，也可将终端仍管理平台注销，脱离企业的 MDM 安全管控。

设备硬件控制：MDM 提供对移动终端设备摄像头/蓝牙/Wi-Fi/USB 网络共享/GPS/VPN/蓝牙扫描/热点功能/USB 存储模式/麦克风/云服务和备份服务/截屏的控制能力，管理员可根据企业的实际情况下发策略，在员工使用移动终端接入企业内网期间，禁用其中的部分或全部功能。 用户通过移动客户端登录企业移动网关时，网关根据用户和设备信息下发相应的控制策略，客户端根据这些策略进行控制。移动终端会把这些对系统硬件接口的修改记录下来，在用户在退出移动应用时，根据记录自动将这些配置恢复到登录前的状态，不影响用户在非办公期间对 BYOD 设备的使用体验。

“越狱”检测：越狱会对企业移动应用带来较大的安全威胁。越狱检测策略是网关在用户登录时下发给移动客户端的，如果检测到越狱，移动客户端可根据策略的指示作出不同级别的响应：审计、提示、

告警或断网。

设备远程锁定/GPS 定位/远程擦除：若终端丢失，员工可以登录企业的自助管理 Portal 或者通过移动设备管理员下发控制命令，对自己的 BYOD 设备进行远程锁定和 GPS 定位，若确认无法找回，也可远程擦除终端上的数据。在员工离职、更换办公终端等场景下，管理员也可通过管理后台给 BYOD 终端下发选择性数据擦除的指令，即仅仅擦除企业数据和卸载企业移动应用，而保留 BYOD 终端上所有的个人数据和个人应用，这样既保证企业数据不外泄，又不破坏用户个人的数据和应用，用户完全可以继续正常的使用自己的个人终端。

应用一键配置：管理员可以通过 MDM 管理后台为所有员工的移动办公终端下发统一的应用配置，譬如，企业邮箱、微信、VPN 软件等的配置，这样既保证所有员工的办公软件的配置是安全的、一致的，也免去了每个员工分别去手工配置应用的麻烦。

企业应用商店管理：对于能够提供大量企业移动应用的企业，应该需要配套提供企业应用的下载、升级、查询、搜索等功能，以方便员工使用，并确保该商店的安全性，防止和减少员工从其他渠道下载相关应用进行企业办公的安全风险。

自助管理 Portal：若用户不希望管理员干涉，则可以登录自助管理 Portal，在终端丢失时，通过 GPS 定位功能，在地图上直观地查看终端的物理位置，并进行远程锁定、远程擦除等操作。

（本文链接：http://www.searchnetworking.com.cn/showcontent_79537.htm ）

安全大排查之云计算篇

云数据安全性：可接受的风险等级

即便是对安全性问题方面的一个小小建议也都足以让一个云计算项目泡汤，并让整个云计算规划过程及其规划者饱受质疑。为了避免出现这种情况，企业必须以辩证的方法来看待安全性问题，集中精力加强对新风险的管理，并从理念上理解可接受的风险等级。

大多数问题的发生都是由于企业是在理想情况下对云计算安全性进行评估的。很少有企业会考虑在云计算中运行一个全新的应用程序;他们往往会希望把一个现成的成熟应用程序迁往云计算。这就意味着，他们并不会对应用程序的安全性进行完整的评估，而是把云计算安全性与他们目前的数据中心托管安全性进行类比。

从这个角度来看，云计算数据安全性评估就是指确定可接受的风险。如同其他所有类比的风险管理一样，安全性风险管理是一个在风险与成本之间进行权衡的过程。对你在现有的数据中心中运行的现有应用程序进行风险评估并担忧应用程序在云计算中运行的风险是非常重要的，这是因为应用程序在云计算中运行所带来的风险往往会高于你所能接受的程度。此举可确保与云计算安全性相关的成本支出不会导致云计算项目因财务原因而流产，其实在现实生活中，这种情况发生的概率是比较高。

从传统意义上进行分类，应用程序的安全性可分为三个层次：网络拦截、应用程序访问和物理数据安全。下面，我们将逐一进行介绍，并重点关注其中云计算与目前程序的差异。

网络拦截。网络拦截是未授权方通过监控网络流量查看机密数据而存在的风险。当通过 Wi-Fi、3G 或 4G 等无线方式访问应用程序时，网络拦截的风险是最高的，但是在大多数情况下，把应用程序迁往云计算并不会改变使用无线技术的用例。例如，如果一家企业希望用户能够更多地通过公共 Wi-Fi 热点访问基于云计算应用程序，那么就可以使用 SSL 加密技术以保护数据信息流。对于通过浏览器进行访问的应用程序，就可提供一个安全的 https URL，但是请注意，对于使用客户端软件的应用程序，可能必须对应用程序进行二次开发以确保实现基于 SSL 加密技术的会话。

密钥管理是确保云计算中应用程序安全性的最大问题。最常见的做法就是把应用程序的安全密钥存储在应用程序镜像中。如果是在云计算应用程序中完成这一工作的，那么密钥就成为了云计算供应商所保留的机器镜像的一部分，从而也就存在被具有机器镜像存储设备访问权的恶意人士窃取的可能性。使用公共密钥存储服务或技术可确保云计算中的密钥、应用程序代码以及数据永远不会被窃。

应用程序访问。云计算中的访问安全性通常也是一个广受关注的重要问题，但事实上它完全不是一

个日益严重的风险。如果你是使用互联网访问你的应用程序，那么通过互联网访问云计算中同样的应用程序就不会存在更多的风险，当然其前提条件是你能够如上所述正确地管理 SSL 和加密密钥。如果你打算使用虚拟专用网络访问来代替互联网访问，尤其是创建一个互联网 VPN，那么就会出现新的挑战。

互联网 VPN 通常会使用 IPsec 加密系统，这是一种不同于 SSL 的安全技术，它会创建一个用户群，这个用户群中用户的数据流量都是通过他们与网络之间的软硬件进行加密和解密处理的。当企业在他们自己的内部 VPN 上使用 Ipsec 技术时，对于云计算是不存在任何额外安全性风险的;但是，云计算供应商们通常是不会支持在他们的云计算数据中心中增加安全设施的，因此就可能需要一个软件以支持至每一个云计算应用程序的 IPsec VPN 连接。一般而言，这可能是每个应用程序机器镜像的一部分，是一种中间件。请与你目前的 IPsec 供应商确认，以确保你有一个云计算兼容的 IPsec 功能可以使用。

物理数据安全。数据资产的物理安全是绝大多数用户所共同关心的最大问题，同时这也是规划者最难以解决的一个问题。如果机密信息被存储在云计算中，那么验证你的云计算供应商的安全性资质就是非常重要的了。虽然已经出现了大批的云计算安全合规性框架，如云计算安全联盟（CSA）的开放认证框架（OCF）;但问题是，这些框架都还未完全开发完成。如果你计划把机密信息存储在云计算中，那么你就需要确认你的云计算供应商提供何种框架以及这一框架是否能够满足你的实际需求。绝大多数的云计算项目规划者所面临的最大问题就是确定云计算供应商的框架是否支持你的合规性要求和政府法规，这项审查工作应由你的内部审计或法务办公室完成，如有必要可与政府监管部门合作进行。

在云计算项目中，也许可以通过杜绝存储机密数据而减少数据物理安全性问题的产生。如果应用程序使用结构化数据访问方法（DBMS/RDBMS 查询处理）而不是块级别的访问读写操作，那么就可以在把应用程序迁往云计算的同时把数据储存模块保留在企业内部。

独立审计是云计算项目规划者在研究云计算安全选项时另一个需要考虑的问题。严格遵循合规性需求的公司可能还需要拥有一个经第三方认证的云计算战略。如果你有一家合规审计公司为你的内部 IT 提供了到位的审计服务，那么这家公司很可能是你进行云计算合规性和安全性审计的最佳选择。如果你不

这么做，那么列出一份他们推荐的云计算供应商和安全合规性审计公司的名单。先按照这些公司的表现选出前三名，然后联系这三家公司进行项目竞标。

（本文链接：http://www.searchcloudcomputing.com.cn/showcontent_80233.htm）

大话安全

前中情局 CISO：金钱买不到安全

Robert Bigman 曾担任中情局首席信息安全官，如今他是安全公司 2BSecure 的总裁。在接受 TechTarget 记者独家专访时，Bigman 认为，首席信息安全官最大的挑战不是新技术，而是如何找到真正意义上能够保护计算机安全的工具。

问：什么技术趋势正在表现为企业的最大挑战？

Robert Bigman：这并非新事物，而是 25 年来一直的挑战，那就是 ：我们如何保护不受安全保护的计算机？现在需要问的问题是 ：市场上有什么新工具可以帮忙解决这个问题？25 年了，他们还一个没找到。这就是为什么每当你到一个展会，都有新供应商销售新东西。

如果你注意一下今天的科技展会，当你走过展厅并看过各个不同的展位，全都是关于云计算和大数据的。这些产品没有哪个是非常糟糕的，而且我敢肯定他们一定提供了一些很有意义的功能，但坦率地说他们没有解决问题。这个问题就是计算机本身是不安全的。除非你能从架构的角度上正确的做到这一点，否则实在没有多少你可以买的产品。

技术发展趋势是如何保护不受安全保护的计算机。将它们放在云上并不能让他们比在被放到云上之前更安全。散布在移动终端之间也不能让他们比全部限制在计算机数据中心之前更安全。

这些都不是解决问题的方法——它们只是在应对症状而已。这就是我们所说的 Nyquil 奈奎尔效应：您还没有治愈感冒，但你肯定觉得好了很多。你并没有解决计算机安全问题，但你觉得你已经做了很多事情。相信我：俄罗斯和中国的黑客们根本不在意你应用在你的网络上的产品。它真的不会成为他们的

路障。

问：首席信息安全官最忧心忡忡的事是或者看起来是什么？

Bigman：首先，每年，他们跑到高层或 CIO 那里告诉他们，“我们需要安装这个 RSA 刚刚出品的滴滴响亮闪闪的玩具。” 我并不是在批评 RSA， 这只是一个案例，因为他们今天也在场，相同的也可以是 McAfee 或其他任何一个供应商。这些都是昂贵的玩具。大公司的企业许可证花费不菲。你很难像买玩具那样，安装它，让他运行，然后一年后回来说，“好吧，我还需要一个做数据丢失保护的。”“再明年，我还需要另一个做数字版权管理的。” 然后，“我需要再一个做云安全的”。最终，首席执行官们会在这方面明智起来，并说，“等一下：为什么我们不去解决这个问题？”

很多首席信息安全官都会认识到，安全问题不像存储设施一样可以购买到，不像计算资源那样可以买到，也不像网络设施可以买到。

（本文链接：http://www.searchcio.com.cn/showcontent_79414.htm ）