美国审计署首席技术专家谈信息安全中人的因素

Keith A. Rhodes

随着个人电脑的普及，保护系统的安全日益困难，正如Gene Spafford博士所言“只有一种系统是真正安全的，即关闭电源、锁在保险柜内、埋于水泥掩体中、并由毒气和全副武装的卫士守护的系统。即便如此，我也不会完全依赖它”。

但如今我们却不得不依赖它，我们乘坐的航班是由电脑系统安排的；甚至我们的未来也依赖于它——我们的养老金也是由电脑管理和计算的。虽然电脑系统的安全难以做到百分之百，但可以控制在一定程度的风险下。这就是风险管理。

所有的系统都是由人设计和操作的，我们这里要讲的是人的因素对系统安全的影响，由于人的原因而产生的风险。密码容易被破解，是因为当事人没有好好设计他的密码；程序缺乏应有的控制，是因为设计员在设计时没有进行周密的思考。现在桌面电脑的功能越来越强大，对系统安全的控制也越来越困难。

我从事系统安全测试工作已有18年，现在使用的电脑与以前相比，已完全不一样。我们做的系统安全测试工作就是对系统的控制环境进行各种各样的攻击，以检测其是否具备保护性能、探测性能和反应性能。保护性能是指防止非授权者进入系统的功能，比如是否有密码和防火墙，是否一直有人在监控；探测性能是指在非授权者入侵后，系统管理员能否探测到其存在；反应性能是指在收集到数据后，系统管理员能否采取适当的措施解决问题。

安全检测的范围涉及内部因素和外部因素。内部因素是指机构内部员工，包括他们对机构的感情、对工作的态度、动机和道德，尤其是中层管理人员；外部因素是指来自网络的风险，只要与网络联系，IP地址是开放的，系统就时时处于受攻击的状态，即使是小孩，也可能成为网络黑客。安全检测还包括物体渗透检查，也包括逻辑渗透检查。物体渗透检查是指无身份证明能否进入系统所在的建筑；逻辑渗透检查是指采用某些软件，如通过电话线路进入系统。

上述这些方面就是检测系统风险所需考虑的。

什么是风险？

风险=内/外部威胁×系统弱点×后果/影响

内/外部威胁=敌手×蓄意×能力

系统弱点主要在以下方面：公共安全、社会工程、密码设置、弱性能扫描、标准命令、设置解调器、数据搜索和分析、端口扫描等。与人的因素相关的是公共安全和社会关系工程，比如机构发布在网页上的信息、机构内部的刊物等，可能由于编辑人员渴望向大家展示其工作成果或者显示其对机构的了解程度而披露一些敏感的内容；而社会关系工程是指个人选择的工作地点及与何种人共事，这些都会对系统产生不同程度的风险。

那么系统的安全到底意味什么呢？我们来看一组数据：去年美国在网络商务方面的经济业务高达8300亿美元，即使扣除双方重复记账，也有约4000亿美元；创造了309万个相关工作岗位，美国电子清算703万亿，至2001年7月，网址有1.26亿个。

这就是我们所处的环境。我们需要防范黑客的破坏，需要保护隐私权，而更重要的是我们要经营业务，要满足客户的要求。如果客户要求随时进入其资料库以进行交易，我们会上网，为他们提供在线交易服务，我们还可能把许多工作外包给别人，以降低成本。于是，我们的风险增大了，这些威胁和风险包括：黑客、隐私权、客户需求、关键设备结构、电子商务、版权、商标、股东、执行性分支机构、法律、智能财产等。

以下是一些人为的原因增加风险的例子：

某一高管人员要求单独使用打印机，并且要求与内部网和万维网相联，以便可随时用任何联网的电脑打印文件。于是，

这台打印机有内存、中央处理器，并与网络相联，但却在系统的防火墙之外，黑客便可通过这台打印机侵入内部系统。

另有一高管人员希望在家里工作，以便不需要请保姆照看孩子，于是他通过调制解调器拨号联入主机，也没有通过防火墙，这样，也给黑客提供了可乘之机。

系统的自动登陆记录文件可以检查是否有非授权者进入系统。但某一企业的系统登陆记录长期无人查看，结果发现一黑客竟在他们的系统中建了一个聊天室！

电脑部的帮助热线是为了及时解决员工操作电脑时遇到的问题或故障而设的，有时也会成为黑客了解系统的途径。比如，黑客装成第一天上班的新员工打热线求助电话，查询自己的用户名和密码。如系统管理员不仔细辨识，便可能提供信息给黑客。

各企业都希望相信自己的员工，认为他们是可信任的，而没有任何控制、检查措施。在某一天可能发现自己信任的员工是商业间谍。另外，在会议室、培训室、空置的办公室等处与机构系统联网但无人使用的电脑，也可成为非用户进入系统的入口。

无线上网的有效范围约450码，随着价格的下降，用户逐渐增加。大家都希望能随时了解信息，进行交易，但无线上网不便加密传送数据（否则速度非常慢），还有设备结构问题，使其易被黑客窃入。现在，有免费可得和便于使用的工具，加上免费软件、共享软件、教育软件等，无需丰富的经验，14岁的孩子也能成为黑客。

其他如个人数字辅助设备，包括数字相机等，采用无线调制解调器、无线网络进行无线联结，可从台式电脑存入敏感信息、从台式电脑传送敏感信息，都可成为黑客攻击的对象。起价仅139美元的（键盘）按键捕捉设备，只需几秒钟安装、不需要电池、软件无法探测和阻止、可存达200万的键数、138位密码、可在所有的操作系统使用，连接在键盘线和电脑之间，能捕捉每一次按键、密码，该设备很细小，易被系统安全人员忽视。

目前，没有统一的安全标准、统一供应商和能够满足机构安全需要的统一的产品，机构需要自己一部分一部分地配置，各部分之间需要接口/界面，如果系统管理员不作很好的设计，这些接口/界面也会增加风险。

系统安全的前线是人，而不是设备，不是技术。系统安全的威胁来自人，希望的弱点是由人和技术造成的；风险的后果/影响也是由人和技术决定的。我们需要关注人的因素对系统安全的影响，经常思考以下问题：我们靠什么生存，谁是竞争对手，什么是我们的关键数据，多久可不更新，需要多少步骤建立这些数据？

任何忽略人的因素的系统一定是失败的系统，而受过良好训练的员工才是不可战胜的。（中国内部审计协会 组织编译）

协会地址：北京市海淀区中关村南大街4号
联系电话：010-82199846/47 电子邮件:xinxibu@263.net