

基于社会工程的网络攻击方式及其 预防措施

王贵骊 张利 江常青 邹琪

中国信息安全产品测评认证中心

摘要

社会工程作为信息安全的威胁之一，并没有引起人们的广泛注意。本文针对社会工程攻击的一些细节进行了详细论述，剖析了社会工程攻击的成因，阐述了社会工程攻击的方式和预防措施。研究表明，制定合理的安全策略，规范的操作流程，并持续地对员工进行安全意识培训等是预防社会工程攻击的必要手段。

关键词：威胁，信息安全，社会工程攻击

The Attack Categories and Protection of Social Engineering

Wang Guisi Zhang Li Jiang Changqing Zou Qi

China Information Technology Security Certification Center

Abstract

Social engineering is often a forgotten risk of information security. This paper attempts to shed some light on social engineering by examining how this attack works, what are the common methods used, and how we can mitigate the risk of social engineering by proper education, awareness training, and other controls.

Key words: threat, information security, social engineering attack

社会工程并不是一个新的术语，它来源于社会学领域。它指的是为了使人们遵从某个新的系统，所采用的以一种可预测的方式来试图改变人们的行为的过程。在我们信息安全领域，社会工程指的是：导致人们泄漏信息或诱导人们的行为方式并造成信息系统、网络或数据的非授权访问、非授权使用、或非授权暴露的一切成功或不成功的尝试。

社会工程是一种常常被人们所忽略的安全风险。在信息安全领域，人们的注意力通常集中在与计算机及其技术相关的工具的使用，配置，安装，实施以及预防工具滥用等方面，忽

视了使用工具的人这个要素^[1]。信息安全不仅仅就是应用一些复杂的技术控制措施，它还包
括对于人们违规行为的处罚。在技术层面，可以通过花费更多的钱和人力来产生更好的防护
体系和安全的代码，但是一旦管理员泄漏了密码，所有的一切均徒劳无益。社会工程攻击不
需要特殊的技术手段，不依靠调查和扫描来寻找系统的脆弱点，仅通过向某个人询问口令就
能够获得相关系统或数据库的访问权。而且大多数计算机罪犯均是机会主义者，他们总是寻
求进入系统最简单的方式。网络攻击的最新调查表明社会工程是罪犯获得系统非授权访问权
限的常用手段。

本文的重点不在于阐述社会工程是如何发生的，更多的是对社会工程这种攻击方式的一
些细节和如何防止成为社会工程攻击的受害者进行讨论。本文将从以下几个方面对社会工程
进行论述：该攻击方式是如何发生的；所使用的常用方法；如何通过适当的教育、意识培训
和其他控制措施来降低社会工程的风险。

1 社会工程为何能成为一种攻击手段

社会工程之所以能够成为一种有效的攻击方式，主要是由于两个要素：人的本性和商务
环境。

1.1 人的本性

大多数情况下，某个人成为社会工程攻击的受害者，与这个人的智力无关，有关的仅仅
是这个人的本性和没有正确的意识和教育来处理这种攻击方式。在大多数情况下，人都是信
任性的且具有合作性。社会心理学领域研究了人类群体之间和个体之间的交互作用。这些研
究表明任何一个处于合适位置并具有很高技能的人均能被某种特定的方式影响其行为，并泄
漏一些在其他一些情形下不会泄漏的信息。

对于大多数情况，社会工程攻击的主要目标是咨询接待人员及行政或技术支持人员。
对这些对象发起社会工程攻击不须是面对面的，经常只需通过电话、电子邮件或聊天室等
方式。攻击者常常倾向于寻找那些易于受这种心理攻击影响的个人。

1.2 商务环境

同时，当前商业的并购趋势，技术和广域网的快速发展使得商务环境变得易于遭受社会
工程攻击。在当前的商务世界，人们不在统一的规范基础上处理问题是极为正常的，包括那
些来自同一个公司的员工，更不用说供货商，卖方和客户了。随着通讯技术的普及，雇员之
间面对面的交互方式越来越少。在当前的市场领域中，某人能够为公司工作而很少到办公室
办公。

今天的商务机构变得比以前更多的是依靠服务来作为雇员的评价标准。常常根据雇员对
于“团队”的贡献和对客户和其他部门的服务等级来划分级别。而不是根据测量某个人应用
常识的程度或依据雇员在执行他们职责时是否意识到安全来进行评估，而这些恰恰是有效对
付社会工程威胁的一个重要手段。

2 社会工程攻击

社会工程攻击采用阶段性的方法，在多数情况下，这种攻击方式与情报机关渗透他们的

目标的方法非常相似。

为了简单起见，这种攻击能够分类为三个阶段：

- 情报收集；
- 目标选择；
- 攻击。

2.1 情报收集

一次成功的社会工程攻击的关键之一是信息。为了成功伪装成公司的雇员、卖方代表，或某些情况下伪装成执法部门的成员，收集有关组织及其员工的充分的信息是非常重要的同时也是极端容易的。组织通常将在其网站上发布详尽的信息作为其市场战略的一部分。这些信息包括提供给顾客的详细线索，如联系电话，email 地址，并指明是否有分支机构以及分支机构地址等等。一些机构甚至将他们的整个组织结构图发布到网站上。所有这些信息对于其潜在的投资者均是非常有用的，但是这也可以用于构成一次社会工程攻击的基础。

网页并不是公开情报的唯一来源。组织内所丢弃的垃圾也可能是重要信息的来源，组织的垃圾里可能会有发货单、信件和手册等能帮助攻击者获得重要信息等媒介。很多被起诉的计算机罪犯均坦白他们曾从倾倒的垃圾中收集信息^[1]。

在该阶段，攻击者的目标是收集足够多的信息，以便于伪装成一个合法的雇员、卖方、卖方、战略合作伙伴，甚至是执法官员。

2.2 目标选择

一旦收集到了足够的信息，攻击者就开始寻找组织员工的一些明显的弱点。最通常的目标是组织内部咨询接待部门的员工，这些员工的职责就是对修改口令，创建账号和重新激活账号等等提供帮助。特别是在一些组织中，咨询的功能被承包给与组织没有实际联系的第三方来完成，作为合同的第三方，他通常并不认识组织内的所有雇员，这更增加了社会工程攻击成功的机会。大多数攻击者的目的要么是收集敏感的信息，要么是获得进入系统的跳板。攻击者清楚一旦他们获得访问权，甚至仅仅是 guest 权限，进行特权升级、发起更具破坏性的攻击或隐藏踪迹也是相对简单的。

行政助理是另一个最可能成为社会工程攻击的目标，这主要是因为这个职位能够获悉大量高级管理层才拥有的敏感信息。行政助理人员可以作为一个攻击点或者是一个额外信息（例如组织内最具影响力者的姓名）的来源。如果想冒名，获悉组织内最高管理者的姓名将非常有价值。更让人惊喜的是，行政助理通常知道执行经理的口令，因为很多行政助理的任务就是帮助经理处理日常事务(如更新电子数据表，电子日历预定等)，这就需要他们具有经理权限。

2.3 攻击

社会工程攻击可以分为三种类型：（1）基于受害者虚荣心和自负心理的攻击；（2）利用同情心和情感的攻击；（3）利用胁迫进行的攻击。

2.3.1 基于虚荣心的攻击

虚荣心或自负心理攻击——攻击者利用很多人的基本本性。每个人都喜欢被人赞扬具有很高的才智，同时这些攻击目标确实对自己的工作很精通或对公司的优缺点很清楚。攻击者

常常扮演成攻击目标的虔诚的听众，并让他们觉得自己是多么的渊博，这样攻击者就有可能从与这些目标的交流过程中获得信息。攻击者通常挑选那些自认为怀才不遇的员工作为攻击的对象，只要经过一次简短的对话，攻击者就可以感觉到受害者的这种情绪。攻击者通常会利用这种方式来给不同的雇员打电话，直到找到合适的攻击对象。不幸的是，在大多数情况下，受害者均没有意识到他们行为的后果。

2.3.2 基于同情心的攻击

在第二类攻击中，攻击者常常假装成一个恰巧陷入困境并需要帮助来解决问题的同事（如新员工）或者是买方、卖方、战略伙伴的新员工。此时，情报收集阶段的重要性就表现得非常明显，因为攻击者必须与受害者建立一定的信任关系，让受害者相信他确是其人。这可以通过冒名，使用恰当的行话或知晓组织的一些知识来完成。攻击者会假装他们需要立即完成某些任务，但是需要访问权限，而他们忘记了账号和口令，或者是不经意间账号被锁死了。在这种情形下，任务的紧迫性是一个很重要的要素，因为这提供了绕过某些必须手续的借口。人的本性中就具有同情心，这样，在大多数情况下，就被攻击者得逞了。如果攻击者不能够获得访问权或从中获得一些信息，他会一直努力，直到发现一个具有同情心的对象，或直到意识到其行为已经引起了组织的疑心为止。

2.3.3 胁迫攻击

在第三种攻击中，攻击者假装成权威人士，要么是组织内的高层人员，要么是执法人员。攻击者会选择其职位之下的几个不同层次的人作为目标。攻击者会制造一个借口来要求重设口令，改变账号，访问系统或敏感信息。如果遇到抵制，攻击者会利用职权胁迫这些员工就范。

3 降低风险的措施

不管采用何种社会工程攻击的方式，成功率都是非常高的。很多计算机罪犯开玩笑说，愚弄受害者是如此容易，以至于他们可以很轻易地进入系统。社会工程攻击的风险和影响是很高的。这些攻击通常难于跟踪和识别。因为攻击者利用合法账号进入系统，控制措施和警报就不会被激活^[2]。

社会工程攻击是如此简单，那么组织如何防卫这种攻击的风险呢？答案相对简单，这需要改变了整个组织的思维方式。为了降低社会工程攻击的风险，组织必须有效地对员工进行关于信息安全威胁和如何识别潜在的攻击的培训和教育。这类攻击的控制可以通过教育，意识，培训和其他控制措施进行。

社会工程针对的是信息安全链中最薄弱的环节——人。可以诱导员工提供敏感信息的事实意味着大多数安全的系统变得脆弱起来。任何信息安全解决方案中，人的因素均是最重要的。事实上，几乎所有的信息安全解决方案在很大程度上都要依赖人的要素。人——这一弱点是普遍的，独立于硬件、软件、平台和网络的。很多公司花费大量的财力来确保有效的信息安全，用于保护公司最重要的资产（包括信息）。不幸的是，使用社会工程技术，就算是最好的安全机制也可以被绕过。社会工程应用非常低的成本以及很低的技术手段来克服信息安全措施设置的障碍。

4 社会工程攻击防护手段

4.1 策略、意识和教育

对抗社会工程攻击是非常困难的。对抗社会工程攻击的困难在于大多数逻辑（技术）安全控制措施是无效的。因为社会工程攻击的目标是人，所以其防范措施需要集中在信息安全管理部分^[3]。一个有效的防御措施就是建立非常好的、集中全组织智慧的信息安全策略。策略指导制订所有员工的“行为规则”。第二个有效的抵抗措施就是用户意识培训。综合这两个信息安全管理方面的控制措施，就可以形成一个完整的安全操作程序，并且使所有员工均能够理解和相信这是他们日常职责的一部分。在整个公司的层面上，将这个信息传递给所有员工是非常关键的。这样，整个公司在所有层次上都非常警觉，而且每个人都相信他们对公司都做出了贡献。这种感觉非常重要，也极大地提高了员工的成就感。这样也降低了不满员工所带来的风险^[4]。为了使一个组织对于社会工程攻击具有更高的免疫力，建立一个讨论其它公司经验的论坛将非常有作用，因为持续的意识培训也非常重要。建立这种论坛的一个好的方式就是使用 Intranet 网址，该网页不仅仅包含公司的安全策略，安全小技巧，而且包括一些有关社会工程攻击的小故事。

另外，一些积极的识别方法往往更有效。例如，当在信息安全事故发生时，某员工做出了很有意义的工作，应当确认这些好的行动并且给与报酬，更应当通报给全公司。这样整个公司的预防意识都可以提高。

4.2 建立事故响应小组

所有的公司均应当有能力有效处理事故。从信息安全的观点，任何外部威胁的处理（包括社会工程）将被认为一次事故。事故响应小组的目的就是有效检测潜在的信息安全事件并且提供一个有效的手段来降低事件对公司的影响。第二个（但也是非常重要的）目的就是提供充分的信息来制定合适的行动过程。事故响应小组应当由来自公司不同关键部门的知识渊博的员工组成，他们经过良好培训并随时准备对社会工程攻击做出反应，这是有效的信息安全操作程序的一个关键方面。

4.3 测试预防程度

渗透性测试是一种从外部观点来评价安全控制措施的方法。为了更加有效，它涉及防范、跟踪、内部及外部入侵报警等所有的控制措施。公司如果想测试他们对于社会工程攻击的防备程度，也可以采用渗透性测试来发现一些证据。但是必须注意的是，尽管渗透性测试是评估组织的控制措施的最好方法之一，但这种方法的有效性强烈依赖于测试者的水平和努力程度。

另外，制定立即通告制度也很重要，一旦某员工发现一个社会工程攻击的企图，必须通知相关部门的人员。此时，处理该类问题的标准程序和步骤就非常重要。精心配备的事故响应小组也将起到非常重要的作用。假设已经建立了合适的程序，事故响应小组就能够快速的处理该问题，并在损失发生前有效地避免其发生。

4.4 应用可能的技术措施

并没有有效的技术措施能够预防社会工程攻击。但是，以下几种技术可以作为考虑的辅助措施：

- 电话跟踪，电话跟踪仅仅作为一种可以选择的手段。因为这需要一定的技术，而且需要事先的准备。而在社会工程攻击的过程中，根本没有时间给与准备。
- 确保物理安全；
- 根据数据的分类原则标记敏感文件。

5 总结

社会工程方法，一旦被攻击者采用，将给任何组织的信息安全带来威胁。迄今，在现实生活中，已经发生了太多的这类攻击的成功案例。然而，遵从信息系统安全的一些基本原则，可以有效地降低社会工程攻击的风险。例如：为了给组织内部敏感和关键信息的正确发布和处理提供指南，必须制定安全策略。信息安全意识同样发挥着重要作用。人们应当能够意识到威胁，更重要的是，他们需要确切地知道如何对这类事件进行响应。对员工进行信息安全教育，让他们意识到随时有人试图操控他们以获得系统的访问权是可行的防御计划的第一步。对可能攻击的预警能够使员工警觉并进行相应的响应。

针对技术性的安全设施（如防火墙等）进行攻击比针对人进行攻击要困难得多。而且，对员工进行培训使他们能够预防和识别社会工程攻击的企图比对员工进行防火墙系统培训的难度要小得多。因此，只要组织措施得当，人将不再成为信息安全链中最薄弱的一环。

参考文献

- 1 Debra S. Herrmann, A Practical Guide to Security Engineering and Information Assurance
- 2 Thomas R. Peltier, Information Security Risk Analysis
- 3 Thomas R. Peltier, Information Security Policies, Procedures, and Standards
- 4 Mark B. Desman, Building an Information Security Awareness Program