大数据时代的个人隐私：深入了解社会工程学攻击

前言：目前该领域还是安全领域的短板，就是社会工程学攻击，在攻防技术不断的提高的时候，这个领域还是很欠缺这类意识。你企业的防火墙做的再好，可一些人不使用线上攻击，而采用“物理”攻击你的某个粗心的员工或抑是总管？

这个就好比我和朋友开玩笑“朋友：怎么搞掉这个WTF啊？我：冲到总部给他砸了！！”是的这虽然是个玩笑，但是运用物理攻击，一旦攻击成功，往往企业遭受巨大损失。我打一个比方，每个人的关系链，就像一张蜘蛛网，这张蛛网铺满了你的社交互联，一个地方破了，可能会造成巨大的连锁反应，

大数据时代信息对撞，谁掌握了更多的信息，谁就有更多的权利，网络攻防的本质是信息不对称。不要等到用户信息泄露，企业遭受致命打击，才开始明白信息安全的重要。人人都应该学会像黑客一样思考。

什么是社会工程学

针对社会工程学的定义是，百度百科是这样讲的，社会工程学是一种通过对受害者心理弱点，本能反应、好奇心。信任、贪婪等心理进行陷阱攻击，对受害者进行诸如欺骗、恐吓等手段，取得自身利益的手法，总体来讲呢，社会工程学就是使受害者顺从你的意愿去做你希望做的事情。

听起来像某神秘的心理控制？有那么一点意思。但是过程是漫长的，因为常常需要收集大量的信息，并针对对方的实际情况，作出不同的攻击策略，拉心理战，获取信任。

社会工程学攻击应用场景

常见的，渗透测试中所用的一种技巧，如前言所讲，玩得好，可以无差别的“撸穿”你的企业上上下下。在你眼里高大上，牢不可破的企业，但有些人就真的黑了，把你眼中高大上的企业黑了。

如果你是一个企业管理者，刚创业起步，拼搏几年过的很辛苦，好不容易拿到了天使轮投资。用尽上上下下几十号员工的精力去做新产品，保护商业机密，买各种WAF，挡住了一切攻击手段，保证了数据库的绝对安全。

但事实很巧，有一天发现自己的商业机密被同行知晓，几千万的投资打水漂，公司Game over，破灭的还有你的老板梦，带上你的员工们。睡觉翻来覆去都想不清楚问题出在哪里，网站没问题啊，安全杠杠的！找运维找安全查日志，于是就可能有下面这一幕。

> “小周，你说到底是哪里的问题？可急死我了”
>
> “老板，网站没有问题啊，各种安全评估都做了，专家都请了，不存在代码和设计逻辑问题啊。”
>
> “等等…我看看系统日志…哎，我尼玛！我的账号没在这个时间段登陆啊过啊？”

系统日志赫然显示，事发当天下午小周的账号在服务器数据库上进行了多种操作，其中就有拷贝数据库文件。

是的，网站也正常，不存在被黑的地方，他是这么取得文件的。

原因是小周暴漏了个人的使用密码习惯，黑客盯上他，把他的数据进行对撞，就成功使用了他的账号进行操作。

可能听起来是有点天方夜谭，但这些不重要，我是个黑客，你万元的WAF上的再好，安全渗透测试服务做的再多，我不需要对着你的网站下手，我需要的，仅仅是找你手下的员工进行信息攻击，取得一个口令，或者是钥匙，登堂入室就可以了，没必要砸你家的门。

其实，把一带有木马的U盘丢到某个办公区，肯定有人会手贱插上电脑，看看你的文件，那么正巧了，国内的一些安全软件都是不拦截Badusb这种模拟键盘进行攻击的命令的，手贱造成一个公司的巨大损失也不在少数。

这类新闻在网上也不少，冒充老板，利用能接触到财务的新进门的员工，进行社会工程学攻击。比如：老板下午要开会，你叫人给你送个U盘来，你拿去借财务电脑用一下，把里面的“研究资料”文档发我，邮箱xxxxxx@xxx.com 这种信息。

该案例攻击者，利用的是新员工对老板的不熟悉，抱着刚进门，就被老板找到头上做事诚惶诚恐的心理，成功的坑了一波，当然 U盘可能是Badusb 种下木马，还是在财务电脑上。也许你在想，我花这么多钱买设备，雇佣牛B的开发人员，运维都是杠杠的，这么可能被你如此简单的社工手段所突破。

还有个故事，有个互联网公司的想去挖竞争对手公司的员工，A公司就让甲乙丁三人搞定，甲乙丁三人想了个办法，就假称自己是一个蛋糕店的老板，最近在搞一个活动，免费送蛋糕，给B公司前台一张表，只要登记姓名，电话，就送你一块蛋糕吃，员工当然高兴啊，有免费的蛋糕不吃么？于是纷纷写了联系方式，于是A公司顺顺利利的拿到了B公司所有人的联系方式，岂不美哉？

这就是攻防双方的不对等。

对于攻击者来讲，我只需要找到你的一个点，然后把浑身手段打击在你的这个点上，一个点破了，完整的系统也有个缺口，继续裂开也只是时间问题，防御方看似牢不可破的系统便会彻底崩溃。

然而对于防御者来说，就算你防火墙花了再多的钱，人才花了再多的钱，代码审计了一遍又一遍。依然可以被社工所突破，攻击者不必去撬门，只需要拿到钥匙进门即可，拿

到钥匙，就是合法的内部人员，再牛的警报也不会对一个身份已经认证的人员报警。

当然社会工程学还被广泛利用到电信诈骗等场景，这里笔者不多谈。总的来说，突破口往往是人。系统可能是无懈可击的，底层代码可能是无懈可击的。但老话说的好，“规矩是死的，人是活的。”人懂的变通，人有感情。所以，这个突破点就是人。人性弱点在安全体系中有很多，比如弱口令，信息对撞进行渗透，这里我们以后再讲。比如弱口令，信息对撞进行渗透，这里我们以后再讲。

我的信息是如何泄露的

常见的信息泄露大概都是以下几种情况：

1. 黑客对论坛等注册网站进行脱库，获取数据库泄露。
2. 注册的各种信息被搜索引擎所检索收录。
3. 黑产交易。

被检索的情况都很多，这也是最简单的一种社工方式：QQ、人人、开心、新浪微博、QQ空间，这些地方我相信大部分人都会认真的填写真的信息，百度一波就全部刷刷刷的出来了。

笔者可以悄悄告诉大家，脱库后的账号和密码都是可以卖的，也就是所谓的黑产交易，整天有成千上亿的数据信息在进行交易，通过数据流，你的信息说不定就到了别人手里。这里也不多谈，注重个人信息安全尤为重要，相信你也不会希望有天无缘无故的收到法院传票。

常见的攻击点

1. 真实姓名。
2. 出生日期。
3. 身份证号。
4. QQ号。
5. 网络昵称。
6. 就读的高中。
7. 朋友圈子的人。
8. 共同朋友的资料。

这些信息拿到后，就可以针对下一步进行更高级别的渗透了。

我在前面所提到的一个案例，攻击者就是运用了信息收集和筛选，将管理者小周的信息进行对比，**去掉虚假数据和不属于被攻击者的信息。**

总结一下，网站管理者防护工作要做好，我们用数据告诉大家泄露信息有多少。

天涯：31,758,768条，CSDN：6,428,559条，微博：4,442,915条，人人网：4,445,047条，猫扑：2,644,726条，QQ数据库：大于6亿条。这还只是不完全统计。

互联网公司比想象中的要脆弱的多，稍微会使用搜索引擎，收集公开信息进行钓鱼等攻击轻而易举。看似牢不可破的系统其实已经满布裂痕。

攻击者不再看你的系统安全，选择去看你的关系链是否和重要人物有无挂钩，从关系链从而达到信任链。

连基本公开信息攻击都挡不住了，何况还有涉及个人隐私的社工库呢？那么，单单冲一个手机号能获得多少信息呢？

首先，百度你的手机号 就能 知道你的号码归属地，如果在58同城发布过什么信息 就可以看到联系人了 ，比如：

然后，用手机号码去试你的各个社交网络，微信、支付宝、微博、贴吧，等等，如果不注意信息防护，通过搜索肯定能得到你的部分社交网络，支付宝可以验证你的真实姓名，得到的数据可以分析出你的一部分兴趣习惯和社交网络。

进而还有QQ空间，QQ空间有人是不喜欢做权限的，对所有人都是开放状态，通过你的访客记录，点赞记录，留言记录，就能出卖你的个人隐私，还可以转向攻击你的亲友获得更多的信息，得到你的学习，居住地，年龄，姓名，兴趣爱好，百度地图开发者有一个高精准API，精度十分之高，知道你的IP一下就能看到坐在电脑前的你，身处何地何方。

信息该如何进行保护

针对保护个人信息这个问题，该上密保上密保，支付密码和普通密码不要混着用，密码口令设置安全一点，不要设置什么花式弱口令，爱人名字+生日号这种，太简单了，分析一个人的密码就能掌握这个人大多数的密码设置习惯，从已有数据分析用户关系链，这点，笔者很擅长（笑）。任何一个入口被逮着可能就会被黑。

企业信息该如何进行保护

针对企业的，我给的建议是：

1. 拒绝弱口令，尽量不要暴露自己的邮箱地址和手机号，如果不得不暴露，请注册一个公用的，和私用的分开。
2. 邮箱等联系东西，请使用二次验证。
3. 拒绝多个账号用一个密码，也不要使用同一个密码设定规则，最好不要有任何意义和规律。
4. 如果你嫌麻烦，确认任何人盗用后不会对你的公司、家人、员工造成任何损失，那么不必听从我的建议。
5. 公司不要将内网和私人WIFI搞混了，也许是你手下某个员工，装了万能钥匙，攻击者一到门口，万能钥匙连上公司网络，哎哟美滋滋，渗透到内网 心里仿佛吃了蜜一样甜蜜。
6. 进行员工安全意识培训，特别强调人际交往这点。
7. 不同员工，不同业务人员之间的账号权限管理应该严格设置。

以上只是尽可能的降低风险，并不是绝对有效的，因为，大数据时代，社工依靠的是你的关系链，以及一些动态信息，你真的毫无办法，你意识再高，你一个经理掉了链子，喔嚯~你又跟着被攻下。总之，做好了这些，基本上没有大问题，当然说起简单做起来是很难的。

如果泄露了怎么办

这是本场Chat的最后一个话题了，泄露了你也不必过多担心。

要相信国家，相信政府，6月1号实施的新网络安全法，这类信息保护是第一位，坏人自有天谴。

社会工程学攻击最大的缺点就是随机性，因为你无法保证你的攻击有效。因为信息是不可控的，被攻击者的心态，情绪，现状你都无法直接控制，如果被攻击者意识较高，具有一定的反社工能力，那么在短时间内进行攻击并且达到目的的很难的。人的观念不是跟系统打补丁似的，一下子装上去完事。
大数据世界里，或许我们每个人都是浑身赤裸，也无处可藏。