接到莫名其妙的推销电话,邮箱、QQ甚至网银密码被盗……在互联网时代,我们的个人信息正在“裸奔”。到底是谁出卖了我们的信息?近日,齐鲁晚报记者联合专注于信息安全的技术公司——山东安云信息技术有限公司进行了一系列实验。

输入十几行代码,网购资料随便看

本报权威实验揭秘信息泄露

仅需输入十几行代码,工程师成功“变身”管理员,登录某模拟购物网站后台。 本报记者 韩笑 摄

本报记者 韩笑

输入一串乱码 用户信息轻易拿到

我们每天登录的网站、爱不释手的APP,是否潜藏着信息泄露的风险?

近日,安云科技的技术员对市民常用的网站进行监测,发现某酒店官网存在安全漏洞。“我们不会直接入侵该酒店网站,但可以模拟该网站的漏洞环境,搭建一个类似网站,并导入海量模拟用户信息,在这个实验环境中看看,类似网站有没有用户信息泄露的风险。”

工程师在模拟网站中注册了一个会员,登录后开始寻找网站逻辑漏洞。找到一个可利用的漏洞后,工程师通过特殊技术构建了一个查询对话框,在对话框中输入了“王”字,26万余条王姓会员信息跳了出来。

工程师又用弱密码123456进行破解,当场提取了1000个王姓会员的信息,包括姓名、手机号、身份证号、积分、会员卡号。“我用的是较为常见的123456密码,就能得到这么多人的信息。工程师在使用更高级的攻击及破解技术后,则获得了该网站所有会员的数据,多达数十万。”

一些购物网站也没能幸免,工程师发现一个有安全隐患的购物网站。按照同样的方法,工程师搭建了个一模一样的虚拟网站,输入了十几行代码,半小时后成功获得了该虚拟网站的管理员权限。“我化身成了该网站的管理员,登录后,网上会员资料、商品订单、数据库备份等资料随便看。”

在一款有漏洞的手机APP上,经过一番探查,工程师发现,这个漏洞主要存在于信息查询功能上。在记者的见证下,工程师在模拟的APP中输入“张敏”,查询出了该用户的住址、电话、身份证号。随后,工程师又输入了一串乱码,APP中所有用户的住址、电话、身份证号都出现在了屏幕上。

“这个乱码就是我们分析出的程序漏洞,相当于配了一把打开别人家门的钥匙,进去之后所有的信息就都看见了。这种漏洞存在于具有信息查询功能的对话框中,比如大家熟悉的快递网站首页,输入运单号查询物流信息。如果物流网站具有这种逻辑漏洞,被黑客攻击后,所有人的物流信息就被泄露。”该工程师说。

测试400个网站 60个存重大漏洞

安云科技介绍,近日,Struts2被曝存在高危漏洞,黑客利用漏洞可以实现远程命令执行。该漏洞引起了业界的广泛关注。

什么是Struts2?“它相当于网站搭建的框架,目前广泛应用于大型互联网企业、政府、金融机构等网站建设,只要是用这种框架搭建的网站都有这个漏洞。在我们监测的400个网站中,就有60个网站不幸中招了。”工程师介绍。

安云科技发现,某地政府的信息网上就存在这个漏洞,技术员利用该漏洞成功获取了网站的最高ROOT权限。“这个权限等于是开发者权限,黑客要是有了这个权限,就能为所欲为,可以更改网站的网页数据,也可以把数据库全都下载下来。”

安云科技还针对高校网站进行了一次安全测试,对243所高校官网进行数据采集,从业务安全、隐私安全、应用安全、主机安全、网络安全等五个维度进行综合打分。其中,80所高校评价为“良好”,103所评价为“一般”,60所评价为“较差”。

“可以直观地理解为,一般和较差的网站都是存在漏洞的,给了黑客可乘之机。”工程师说道。

安云科技还对医疗网站进行过分析,68个网站中,56个评价为“良好”,8个评价为“一般”,4个评价为“较差”。

“在实际的攻击中,黑客在一个网站获取个人密码后,还可以拿密码等个人信息到其他网站中‘撞库’分析,通过多家网站中的信息获取,经过关联、对比后,能将个人信息进行更为详细的还原。”安云科技介绍。

七成信息泄露 来自黑客攻击

近日,360互联网安全中心发布《2016年中国网站安全漏洞形势分析报告》。报告显示,在2016年,360网站安全检测平台共扫描各类网站197.9万个,发现存在漏洞的网站91.7万个,占比为46.3%,比2015年略有下降。虽然漏洞网站数量下降,但高危漏洞数量大幅增长,这说明,极少数网站集中出现大量高危漏洞。网站高危漏洞激增,导致大量信息被泄露。

上游黑客获取信息,下游信息贩子转手买卖,个人信息贩卖已经形成了产业链,类似交易每天都在发生。腾讯公司首席执行官马化腾援引公安部门数据称,当前我国网络非法从业人员已超过150万,黑产市场规模已达到千亿元级别。

山东省信息网络安全协会专家张朝伦介绍,网络信息泄露无外乎两个原因,一是外部攻击,二是内部窃取。“从信息泄露事件的概率来看,外部攻击要占到七成。对外部攻击者来说,其最主要的手段就是寻找并利用信息系统的漏洞。”

“知名的互联网公司技术团队庞大、技术水平较高,在个人信息保护上做得较好。有一些企业网站,因为自身数据管理意识薄弱、数据库安全防范技术水平较差,很容易泄露信息。”张朝伦说。

张朝伦认为,相关监管部门需要尽快规范企业网站的开发安全标准,并加大安全技术人员的培训力度。“国家需要制定一个统一的标准,不达标的网站不能运行,并对照标准进行监测、整改。现在专业的安全开发人员很紧缺,需要加快相关专业的设置和人才培养。”

律师说法

“企业泄露信息应加强处罚”

山东新亮律师事务所王新亮律师介绍,按照现行法律,如果用户信息泄露,企业是需要承担一定责任的。

有统计显示,目前我国涉及公民个人信息的法律有近40部,法规有30部,还有一些部门规章和地方法规,从总体上看数量并不少。

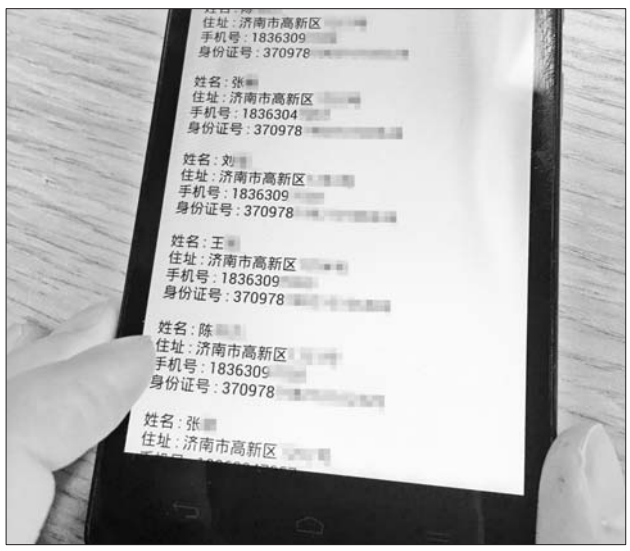
消费者权益保护法规定,经营者及其工作人员对收集的消费者个人信息必须严格保密,不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施,确保信息安全,防止消费者个人信息泄露、丢失。国务院网络交易管理办法第十八条规定:在发生或者可能发生信息泄露、丢失的情况时,应当立即采取补救措施。

2016年11月,网络安全法正式出台,明确了对侵害公民个人信息行为的惩处措施。网络运营者、网络产品或服务提供者以及关键信息基础设施运营者如未能依法保护公民个人信息,最高可被处以50万元罚款,甚至面临停业整顿、关闭网站、撤销相关业务许可或吊销营业执照的处罚,直接负责的主管人员和其他直接责任人员会被处以最高十万元的罚款。

“企业的信息安全管理不到位,政府主管部门可以对其进行行政处罚,公民个人如果权益受到侵害,也可以要求其进行民事赔偿。实施过程中的难点在于,网络信息泄露具有隐蔽性、追查困难、查处难度大,由于缺乏系统性、可操作性,现有立法难以满足实践需求。”王新亮介绍。记者注意到,虽然信息泄露、数据安全事件频出,却从未见到企业负责人被追责。

王新亮认为,法律要加大对企业、信息窃取者的监管和处罚力度。同时,加强法律宣传,让更多企业认识到增强网站安全性的重要性。

本报记者 韩笑



工程师利用某款APP的逻辑漏洞,查询到了所有模拟用户信息。 本报记者 韩笑 摄