信息安全保障人员培训教程

网络安全意识提升

WANGLUO ANQUAN YISHI TISHENG

中国信息安全认证中心

◎主 编 张 剑 副主编 张会平

★★★ CISAW ★★★

电子科技大学出版社

信息安全保障人员培训教程

网络安全意识提升

WANGLUO ANQUAN YISHI TISHENG

中国信息安全认证中心

◎主 编 张 剑 副主编 张会平

★★★ CISAW ★★★

电子科技大学出版社

图书在版编目(CIP)数据

网络安全意识提升 / 张剑主编. ——成都:电子科技大学出版社,2017.5

ISBN 978-7-5647-4501-1

Ⅰ. ①网… Ⅱ. ①张… Ⅲ. ①网络安全—基本知识 Ⅳ. ①TN915.08

中国版本图书馆 CIP 数据核字(2017)第 109315 号

网络安全意识提升

张剑 主编　　张会平 副主编

出　　版:	电子科技大学出版社(成都市一环路东一段 159 号电子信息产业大厦　邮编:610051)
策划编辑:	万晓桐　徐守铭
责任编辑:	万晓桐　徐守铭
主　　页:	www.uestcp.com.cn
电子邮箱:	uestcp@uestcp.com.cn
发　　行:	新华书店经销
印　　刷:	成都市火炬印务有限公司
成品尺寸:	185 mm×260mm　　印张:16.75　　字数:429 千字
版　　次:	2017 年 5 月第一版
印　　次:	2017 年 5 月第一次印刷
书　　号:	ISBN 978-7-5647-4501-1
定　　价:	60.00 元

前　言

2016年4月19日，习近平总书记在主持召开网络安全和信息化工作座谈会时指出："没有意识到风险是最大的风险。"统计结果显示：在所有信息安全事件中，只有20%-30%是由于黑客入侵或其他外部原因造成的，其他70%-80%是由于内部员工的疏忽或有意泄密造成的。在保障信息安全的这场"持久战"中，"人"的因素是第一位的。当前，我国与信息安全相关的人员意识不容乐观，表现为：不清楚风险在哪里、不了解基本的安全常识、不知道如何应对常见风险；其结果是："一念之差就把敌人引进了家门""一项误操作就进入了别人设下的圈套""出了大事还在火上浇油"。提升相关人员的信息安全意识迫在眉睫。

本书共分为9章。第1章从信息安全的内涵出发，介绍了信息安全意识普及状况，解读了一些典型信息安全事件；第2章从社会工程学出发探讨了信息安全中人的因素，给出了一个信息安全意识模型，并介绍了信息安全意识测评方法；第3章介绍了数据面临的主要威胁、保护技术以及防范措施；第4章分析了载体面临的主要威胁、如何防范载体的安全威胁，以及典型载体的安全防护措施；第5章介绍了如何认识物理环境和逻辑环境，以及典型物理环境和逻辑环境的安全防护措施；第6章介绍了如何认识物理边界和逻辑边界，以及典型物理边界和逻辑边界的安全防护技术、手段和措施；第7章探讨了信息安全资源如何保障，包括人力、财务、信息、技术四类资源；第8章分析了信息安全中的重要管理问题，包括责任制度、保密制度、应急管理三个方面；第9章对《网络安全法》进行了全面介绍并对条款内涵进行了深度解读。

本书按照信息安全保障统一模型以及信息安全意识模型进行编写，适合于从事与信息安全保障工作相关的各类人员，既包括相关的技术人员，也包括相应的管理人员，还包括使用重要信息系统的所有用户和工作人员。本书可以作为参加信息安全意识提

升培训学员的教材，也可以作为政府、金融、通信、医疗、能源等重要行业、重点领域相关人员的普适性信息安全读物。本书由张剑、罗小兵、张会平、万里冰、张徐亮、钱伟中、吴凤翼、赵平、刘博等共同编写完成。本书在成书过程中得到了《信息安全保障人员认证考试用书》编委会的指导和中国信息安全认证中心、四川省中认信安技术服务有限公司、四川亚和企业咨询服务有限公司的大力支持，在此表示衷心感谢。

本书力图以明确的思路、清晰的结构和流畅的语言来展现本书的知识体系，但难免会出现纰漏、差错和不足，在此，恳请广大读者和同行批评指正，以便我们再版修订时加以改正和完善。

编　者　张　剑

2016 年 10 月 20 日

目　录

第 1 章

概 述

本章分为三个部分：第一部分介绍网络安全的基本概念；第二部分详细介绍我国的国家网络与网络安全建设和发展情况；第三部分解读当前国内外典型的网络安全事件。

1.1 引言

2016 年 3 月，谷歌人工智能机器人 AlphaGo 以 4∶1 的比分战胜韩国棋手李世石，以 3612 分世界第一排名震惊全球，成就了信息技术的划时代意义，也代表着全球信息技术的进步已经进入了一个新的发展阶段。与之相伴的是，计算机系统和互联网络也在面临着越来越智能化和多元化、后果越来越严重的威胁、攻击和破坏。

图 1-1 科技发展是否百利无一害

• 2013 年 3 月，美国国家安全局前雇员斯诺登·爱德华揭露了骇人听闻的“棱镜”电子监听计划，一时间人人自危，引发全球各国高层的密切关注。

• 2014 年 4 月，Windows XP 系统停止服务，影响中国近 70%的计算机系统，用户量超过 2 亿人。

• 2015 年 4 月，从补天漏洞响应平台获得的数据显示，重庆、上海、山西、沈阳、贵州、河南等超 30 个省市卫生和社保系统出现大量高危漏洞，数千万用户的社保信息可能因此被泄露，后果不可估计。

• 2015 年 10 月，补天漏洞响应平台在此播出中国电信某系统的重大漏洞，通过该漏洞可以查询上亿用户信息，涉及姓名、证件号、余额，并可以进行任意金额充值、销户、换卡等操作，若没及时发现，经济损失难以估计。

• 2015 年 12 月，乌云漏洞报告平台爆出中国联通、中国移动和中国电信三大运营商流量计费系统漏洞，有些客户会对此漏洞加以利用从而使用远远超出其套餐的流量，倘若漏洞扩大，运营商损失将无法估计。

• 2016 年 4 月，土耳其爆发重大数据泄露事件，近 5000 万土耳其公民个人信息牵涉其中，包括姓名、身份证号、父母名字、住址等一连串敏感信息被黑客打包放在芬兰某 IP 地址下，人们可通过 P2P 任意下载他们感兴趣的数据。同时为了证明这些被盗取数据的真实性，黑客特地公布了土耳其总统埃尔多安的个人信息以作示范。

• 2016 年 8 月，网络上曝出包括顺丰、圆通等国内快递公司出现“内鬼”非法贩卖 20 万顾客信息的新闻，泄露内容包括姓名、地址、电话以及购买的物品种类等。更为骇人听闻的是，由于信息泄露造成的“精准营销”，围绕个人信息的采集、加工、开发和销售活动正悄然变为一条黑色“数据产业链”。

诸如此类的网络安全事件比比皆是，让人们触目惊心。

2015 年，国家互联网应急中心（CNCERT）共处置各类网络安全事件近 12.6 万起，其中网页仿冒事件数量位居第一，达 7.5 万余起。据国家信息安全漏洞库（CNNVD）统计，截至 2015 年 12 月 31 日，CNNVD 收录漏洞总量已达 80 300 个，其中 2015 年新增漏洞 7754 个，与 2014 年漏洞新增的 8623 个相比虽然有所下降，但仍旧将信息系统和网络暴露在严重的安全风险之中。

图 1-2 科技的利与弊

事实证明，科技是一把时代的“双刃剑”，技术的飞速发展固然为工作和生活带来了前所未有的便利，但科技的更新让“流氓”（黑客）变得越来越有文化，大环境下的网络安全形势不容乐观，组织信息系统和个人数据的安全问题亟待解决，刻不容缓。

1.1.1 到底什么是安全

在古代汉语中，并没有“安全”一词，但“安”字却在许多场合下表达着现代汉语中人们通常理解的“安全”这一概念，例如，“是故君子安而不忘危，存而不忘亡，治而不忘乱，是以身安而国家，可保也。”《易·系辞下》这里的“安”是与“危”相对的，并且如同“危”表达了现代汉语的“危险”一样，“安”所表达的就是“安全”的概念。“无危则安，无缺则全”，即安全意味着没有危险且尽善尽美。这是与人们的传统的安全观念相吻合的。“安全”作为现代汉语的一个基本语词，在各种现代汉语辞书有着基本相同的解释。

那么从字面上理解，网络安全就是采取各种手段和防护措施来保证和整个网络相关的信息资产没有危险也感觉不到会出危险。当然，网络安全不仅仅要关注信息或者网络设备本身，更要考虑可能造成信息出现安全风险的因素，比如用户缺乏网络安全意识、手机的丢失、计算机中病毒、数据库遭受攻击，甚至还有机房的门上没有安装牢固的锁具等。经过专家学者的归纳以后，网络安全的主要目的就是要保护信息或者数据的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability），它们的首字母组合起来就成为安全人员常说的“信息安全三要素——CIA”。

1.1.2 网络安全和谁有关

很多人会问，网络安全那是国家的事情，和个人能有什么关系呢？

这是一个很严重的误解。

从整体来看，我国信息化普及正随科技的迅猛发展而逐步加速。《第 38 次中国互联网络信息中心（CNNIC）调查》数据指出，截至 2016 年 6 月，我国网民规模达 7.10 亿，其中手机网民规模大 6.56 亿。网民最主要的上网设备是手机，使用率为 92.5%。网络办公、上网购物、网上支付、网上交友等行为已经成为人们生活和工作的重要组成部分。

图 1-3　公民身边的网络安全

然而，越来越多的电信诈骗、钓鱼邮件、撞库攻击等网络安全事件无时无刻不警醒着每一个使用网络电子设备的人，要及时提升网络安全意识，加强个人网络安全的防护。可以说，网络安全不仅仅是国家、某个组织或行业所关注的问题，手机、计算机等终端设备的普及和越来越多的个人网络安全事件使得每个人都与网络安全息息相关。

1.1.3　为什么要提升网络安全意识

“棱镜门”事件告诉人们，网络和信息安全关系到国防安全和国家机密。假设银行的信息系统停止工作、通信运营商无法传输手机信号、政府发布的政令随意被人篡改，难以想象，社会将会出现怎样的混乱。更糟糕的是，这样的场面很有可能就是某个组织的内部人员由于疏忽或误操作而造成的。因此，培养具有强烈网络安全意识的合格信息化从业人员是国家安全保障工作不可忽略的内容。