第9章　数据泄露网络安全应急响应

9.1　数据泄露概述

9.1.1　数据泄露简介

数据泄露指对存储、传输或以其他形式处理的个人或机构数据造成意外或非法破坏、遗失、变更、未授权披露和访问的一类安全事件。

确认是否为数据泄露安全事件主要依据以下三条基本原则。

（1）违反机密性：未授权或意外披露机密数据。

（2）违反可用性：意外丢失数据访问权或对机密数据造成不可逆转的破坏。

（3）违反完整性：机密数据未授权或意外变更。

9.1.2　数据泄露途径

1.外部泄露

外部泄露是指数据通过非企业自身系统进行泄露，如攻击者通过入侵企业内部系统、广泛收集网络信息等方法获取敏感信息。

1）供应链泄露

（1）自身供应链泄露。自身供应链是指企业自身产品生产和流通过程中的采购部门、生产部门、仓储部门、销售部门等组成的供需网络。如电商体系中的物流系统、仓储管理系统、支付系统等，往往包含企业大量敏感信息，该类系统被恶意攻击者入侵，可造成数据泄露。

（2）第三方供应商泄露。企业由于业务需要，使用或者购买了第三方服务，如供应商代码仓库、供应商外包人员服务、供应商提供的SaaS服务等。恶意攻击者通过入侵相关系统，造成数据泄露，或是第三方供应商为了牟取利益泄露数据。

2）互联网敏感信息泄露

（1）搜索引擎。企业违规将敏感数据上传至公开的互联网网站，随后搜索引擎收录企业相关网站，导致数据通过搜索引擎泄露。

（2）公开的代码仓库。企业相关研发运维人员违规将代码主动上传至公开的代码仓库，如GitHub、Gitee等，导致数据泄露。

（3）网盘。企业相关人员违规将未加密的敏感数据主动上传至公开网盘，并进行分享，导致数据泄露。

（4）社交网络。企业相关人员通过社交网络违规或无意识地披露敏感数据，导致数据泄露。

3）互联网应用系统泄露

企业相关的互联网系统存在缺陷，如商城系统、VPN系统、邮件系统等，恶意攻击者利用未授权访问、数据遍历、管理弱密码、SQL注入等漏洞，造成数据被动泄露。

2.内部泄露

内部泄露是指数据通过企业自身系统进行泄露。

1）内部人员窃密（主动泄密）企业内部人员非法窃密，并将数据售卖给他人牟利。如客服人员、内部研发运维人员、数据运营人员等，通过自身权限获取企业数据以转售。

2）终端木马窃取企业内部人员的办公终端被植入木马，造成数据被窃取。如员工在办公终端上插入来历不明的U盘，使用非正规渠道下载的盗版软件，单击钓鱼邮件的诱导内容等，导致终端被控制，造成数据泄露。

3）基础支撑平台泄露部署在企业内部的基础支撑平台，如包含企业敏感数据的ES平台、Redis缓存数据库、数据仓库等基础平台，因被攻击，而导致数据泄露。

4）内部应用系统泄露攻击者利用未授权访问、数据遍历、管理弱密码、SQL注入等漏洞，攻击企业内部的业务应用系统，获取相关数据。

9.1.3　数据泄露防范

1.数据外部泄露防范

应对数据外部泄露，需要做好如下防范工作：

（1）做好自身供应链（如物流、仓储、支付系统）和第三方供应商（如海外购、第三方商店）的数据访问控制，尤其需要完善审计措施。

（2）做好互联网应用服务的安全配置并定期巡检，避免违规共享内容被搜索引擎收录。针对内部员工进行全面的网络安全意识培训，规范数据存储和共享，杜绝内部机密数据通过互联网存储和传输。建立邮件和社交网络使用规范，建立红线机制并设定奖惩措施，防微杜渐。

（3）互联网应用系统正式上线前应进行全面的渗透测试，尽可能避免存在未授权访问、管理弱密码、SQL注入等漏洞，导致数据泄露。

2.数据内部泄露防范

应对数据内部泄露，需要做好如下防范工作：

（1）业务系统运营人员和运维研发人员等的访问权限应做好访问控制，建立相应角色并根据需求最小化原则分配访问权限，指派专员对业务系统的访问进行审计。

（2）建立终端准入机制，统一部署杀毒和终端管控软件。

（3）通过安全意识培训，培养员工良好的终端使用习惯，避免数据通过终端被窃取。

（4）内部应用系统正式交付前应做好全面的软件测试，避免存在隐藏的数据调用接口。并在正式上线前做好渗透测试，避免攻击者通过数据遍历、未授权访问和SQL注入等漏洞批量获取数据。

9.2　常规处置方法

1）发现数据泄露

2）梳理基本情况

3）判断泄漏路径

4）数据泄漏处置

9.3 常用工具

9.3.1 Hawkeye

Hawkeye是一个开源GitHub数据泄露监控系统。通过该系统监控GitHub代码库，可及时发现员工托管公司敏感信息到GitHub的行为并预警，降低数据泄露风险。

1.Hawkeye功能概述

（1）企业GitHub信息监测；

（2）告警推送；

（3）周期性监控；

（4）Web端管理。

9.3.2 Sysmon

系统监视器（Sysmon）是Windows系统服务和设备驱动程序，可监视系统活动并将其记录到Windows事件日志中。