网络安全

作者：19网128郑俊奕

● 我国网络安全现状

随着人工智能、大数据、5G等新兴技术的发展，企业面临的威胁日益增加。相关数据显示，在2015年至2025这十年间，网络攻击引发的全球潜在经济损失可能高达2940亿美元。网络风险的升级，让政府、企业和个人都对该风险愈加关注。各国纷纷颁布数据保护方面的法律法规，我国自2017年6月 开始实行《网络安全法》。2019年5月，我国发布了等级保护2.0 国家标准，增加了个人信息保护、云计算扩展等要求。

国家互联网应急中心发布的《2019年上半年我国互联网网络安全态势》显示，2019年上半年，我国互联网网络安全状况具有四大特点：个人信息和重要数据泄露风险严峻；多个高危漏洞曝出给我国网络安全造成严重安全隐患；针对我国重要网站的DDoS攻击事件高发；利用钓鱼邮件发起有针对性的攻击频发。

国家互联网应急中心从恶意程序、漏洞隐患、移动互联网安全、网站安全以及云平台安全、工业系统安全、互联网金融安全等方面，对我国互联网网络安全环境开展宏观监测。数据显示，与 2018 年上半年数据比较，2019 年上半年我国境内通用型“零日”漏洞收录数量，涉及关键信息基础设施的事件型漏洞通报数量，遭篡改、植入后门、仿冒网站数量等有所上升，其他各类监测数据有所降低或基本持平。

● 我国网络安全目前存在的问题

- 我国网络威胁监测技术仍待加强

  一是信息技术安全监测能力不强。

  二是网络攻击追溯能力不足

- 我国信息技术产品自主可控生态亟待建立

目前，我国对国外信息技术产品的依赖度较高，CPU、内存、硬盘和操作系统等核心基础软硬件产品严重依赖进口。如CPU主要依赖英特尔和AMD等厂商;内存主要依赖三星、镁光等厂商;硬盘主要依赖东芝、日立和希捷等厂商;操作系统则被微软垄断。2017年，欧美跨国企业提升了核心技术的开放程度，国内信息技术产业曾出现新一轮引进式的创新热潮。然而，2018年，随着中兴事件和中美贸易战的持续发酵，各界人士逐渐在构建信息技术产品自主可控生态方面达成共识。一方面是亟需研发出可用乃是好用的核心信息技术产品;另一方面是急需对自主可控的网络产品和服务进行评估、扶持和推广，进而构建良好自主可控生态。

- 我国网络可信身份生态建设尚需强化

《网络安全法》明确提出，“国家实施网络可信身份战略，支持研究安全和方便的电子身份认证技术，推动不同电子身份认证之间的互认”。然而目前，我国网络可信身份生态建设仍需强化

● 网络安全防护措施

访问控制：对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限，等等。数据加密防护：加密是防护数据安全的重要手段。加密的作用是保障信息被人截获后不能读懂其含义。

网络隔离防护：网络隔离有两种方式，一种是采用隔离卡来实现的，一种是采用网络安全隔离网闸实现的。

根据网络安全现状，以及各领域企业的网络安全需求，能够简单、快捷地实现整个网络的安全防御架构。企业信息系统的安全防御体系可以分为三个层次：安全评估，安全加固，网络安全部署。

通过对企业网络的系统安全检测，web脚本安全检测，以检测报告的形式，及时地告知用户网站存在的安全问题。并针对具体项目，组建临时项目脚本代码安全审计小组，由资深网站程序员及网络安全工程师共通审核网站程序的安全性。找出存在安全隐患程序并准备相关补救程序。

以网络安全评估的检测结果为依据，对网站应用程序存在的漏洞、页面中存在的恶意代码进行彻底清除，同时通过对网站相关的安全源代码审计，找出源代码问题所在，进行安全修复。安全加固作为一种积极主动地安全防护手段，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵，加强系统自身的安全性。