国家网络安全宣传周
China Cybersecurity Week

筑盾
北京市网络安全公益宣传

首都网警

2025

北京市国家网络安全宣传周
主题巡展

网络安全为人民　网络安全靠人民

首都网警在您身边

百家号　抖音　快手　头条号　微博　微信

北京市互联网信息办公室　北京市公安局

国家网络安全宣传周

当前网络安全形势

随着互联网技术不断发展， 网络安全的威胁来源和攻击手段不断变化， 不管是个人层面， 还是国家领域， 网络安全牵一发而动全身的效应愈加明显。

认清当下严峻形势，
是守住经营底线的第一步。

主要威胁表现 >>>>>>>

1. 攻击频率激增

近年来， 因勒索病毒感染、 数据泄露攻击等引发的网络安全事件层出不穷， 每每引发全球震惊。 包括中国在内的多个国家和地区频频遭受网络攻击，一些国家甚至因遭受网络攻击， 导致交通、 金融、 医疗、 政务等领域无法运转。

2. 漏洞数量攀升

根据国家信息安全漏洞库 （CNNVD） 统计， 2024 年收录的漏洞总数为 40034 条，比 2023 年（28691 条）增长 39.54%，其中，超危漏洞 2883 条，高危漏洞 9994 条， 漏洞泛滥使网空形势更趋复杂。

3. 攻击手段升级

当前， 数字化转型加速， 网络技术快速发展， 恶意软件攻击也在不断升级。 从简单的病毒木马事件到高级持续性威胁 （APT）， 从黑灰产到勒索软件， 网络攻击手段日益复杂化、 专业化， 互联网黑灰产业链日渐完善， 经济利益更加明确， 给网络安全构成较大威胁。

政策法规解读 明确责任边界

网络安全不是某个人的事， 而是企业与每一位员工共同的“ 责任场 ”。 了解网络安全政策法规， 既是企业必须履行的法定义务， 更与员工日常工作中的操作规范、 职业风险紧密相连， 直接关系到每个人的切身利益。

了解政策法规 明确责任红线

基础

《网络安全法》：

网络运营者开展经营和服务活动， 必须遵守法律、 行政法规， 尊重社会公德， 遵守商业道德， 诚实信用， 履行网络安全保护义务， 接受政府和社会的监督， 承担社会责任。

核心

《数据安全法》：

规定根据数据重要程度实行分类分级保护， 对重要数据采用目录管理， 建立数据安全风险评估、 报告、 信息共享、 监测预警和应急处置机制等。

隐私

《个人信息保护法》：

任何组织、 个人不得非法收集、 使用、 加工、 传输他人个人信息， 不得非法买卖、 提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

关键

《关键信息基础设施安全保护条例》：

运营者应当建立健全网络安全保护制度和责任制， 保障人力、 财力、 物力投入。 运营者的主要负责人对关键信息基础设施安全保护负总责， 领导关键信息基础设施安全保护和重大网络安全事件处置工作， 组织研究解决重大网络安全问题。

标准

《信息安全技术 重要信息基础设施安全保护与评估要求》：

是本市重要信息基础设施安全保护领域首个地方标准。 标准从安全通信网络、 安全区域边界、 安全计算环境、 安全管理中心、 安全管理制度、 安全管理机构、 安全管理人员等方面， 提出重要信息基础设施增强型安全保护与评估要求。 明确对业务连续性要求较高的， 应采用至少两条不同运营商的通信线路， 并实现通信线路的故障实时检测和链路自动切换。 数据安全管理方面， 应采用加密、 脱敏、 去标识化等技术手段保护个人敏感信息安全。

企业易遭攻击

企业在网络环境中面临多种攻击威胁， 这些攻击可能导致严重的后果， 影响企业的正常运营和发展。

<<< 常见攻击类型 >>>

木马攻击：

伪装成合法程序， 植入企业系统后， 窃取敏感信息、 远程控制设备等。

漏洞攻击：

利用企业系统存在的安全漏洞， 非法进入系统， 窃取数据、 篡改信息或进行破坏活动。

社工攻击：

利用人的心理弱点， 诱导内部人员泄露敏感信息或执行特定操作， 从而达到非法入侵系统、 窃取数据等目的。

勒索攻击：

黑客入侵企业系统后， 加密重要数据， 向企业索要赎金， 否则将删除或公开数据。

<<< 可能遭受的后果 >>>

数据损坏或丢失：

重要的业务数据、 客户信息等被病毒破坏或被木马窃取， 给企业造成不可挽回的损失。

系统瘫痪：

病毒和木马可能导致企业计算机系统、 服务器等无法正常运行， 业务中断， 影响企业的生产经营。

经济损失：

企业为了恢复数据或系统， 可能需要支付高额的赎金， 同时业务中断也会带来直接的经济损失。

声誉受损：

数据泄露、 系统被攻击等事件会影响企业的信誉， 导致客户流失、 合作伙伴不信任等。

法律追责：

若因攻击导致客户信息、个人数据泄露，企业将违反《网络安全法》《个人信息保护法》 等法规， 面临监管部门的行政处罚； 若造成重大损失或恶劣影响， 企业负责人及直接责任人可能承担民事赔偿责任， 甚至涉及刑事责任。

国家网络安全宣传周

北京市网络安全公益宣传

防范木马攻击

木马病毒是什么？

木马病毒就像藏在电脑里的“电子间谍”，伪装成文件、软件、链接，一旦点开，就悄悄潜伏，偷密码、传数据，甚至遥控你的鼠标干坏事！

木马的“骗人把戏”

1. 文件伪装术：把木马藏进“工作报告.doc”“客户资料.xls”，看着正常，点开就入侵！
2. 盗版陷阱：破解软件、免费工具里藏木马，“免费馅饼”其实是“中毒陷阱”！
3. 钓鱼附件：邮件里的“账单.pdf”“福利通知.zip”，点开就给黑客开门！

中木马的信号

- 电脑突然变卡，程序自动乱弹
- 密码莫名失效，账号异地登录
- 文件偷偷消失/被改，硬盘空间骤减

中木马病毒该如何急救？

- 断网！立即断开电脑网络，别让木马传数据！
- 杀毒！启动杀毒软件全盘扫描，顽固木马找IT支援！
- 补救！改密码、查数据，赶紧向有关部门报告！

个人防范技能包

- 装带行为监控的杀毒软件，每天更新病毒库！
- 软件只装正版！盗版=主动放木马进门！
- 邮件附件先扫毒，陌生链接别乱点！
- 定期给系统打补丁，漏洞不补=给木马留门！

企业防范技能包

- 部署终端安全管理系统，对所有办公设备的软件安装、文件传输进行统一监控，及时发现异常操作。
- 建立软件白名单制度，仅允许经安全审核的正版软件在企业内网运行，禁止员工私自安装来源不明的程序。
- 搭建邮件安全网关，对进出企业的邮件附件自动进行病毒扫描和风险评估，拦截可疑邮件。
- 定期开展全网木马查杀行动，结合漏洞扫描结果，对高风险设备进行重点排查和加固。
- 制定木马攻击应急响应预案，明确各部门职责和处置流程，定期组织演练，确保事件发生时能快速响应。

国家网络安全宣传周

防范漏洞攻击

漏洞 = 黑客的「穿墙密道」

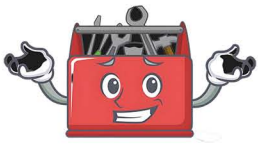
系统 / 软件里的设计缺陷， 就像没锁的门， 黑客顺着 “ 漏洞 ” 直接闯进系统， 偷数据、 搞破坏！

遭遇漏洞攻击该怎么急救？

断业务！立刻停受影响系统，拖延 = 让损失 “ 滚雪球 ”，违反《网络安全法》要挨罚！

查原因！全面检查漏洞咋被利用的， 员工必须配合查记录， 抗拒不配合 = 担责任！

救数据！用备份恢复系统， 涉及用户信息泄露， 赶紧报监管 + 通知用户！瞒报 = 法律追着罚！



个人防范技能包

- 定期检查个人办公设备的系统更新， 发现补丁提示立即安装， 不给漏洞留机会！
- 设置复杂密码 （字母 + 数字 + 符号），不同账号用不同密码，避免 “ 一串密码走天下 ” ！
- 不随意在工作设备上安装非工作软件，减少第三方程序带来的漏洞风险。
- 发现系统异常 （如频繁崩溃、 弹窗）， 第一时间向企业 IT 部门报告，不擅自处理。

企业防范技能包

- 部署自动化漏洞扫描工具， 每周对全网系统、 设备进行扫描， 生成漏洞清单并分级修复。
- 建立补丁管理机制， 对重要系统补丁进行兼容性测试后 48 小时内完成部署， 高危漏洞 “ 零延迟 ” 修复。
- 实施最小权限原则， 根据岗位需求分配操作权限， 普通员工禁止接触核心系统和敏感数据。
- 定期开展内部渗透测试， 模拟黑客攻击场景， 提前发现隐蔽漏洞并加固。

国家网络安全宣传周

防范“社会工程学”攻击

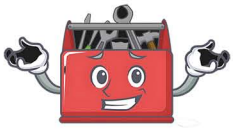
都是坑啊

社会工程学攻击 = 黑客“套出”的「心理陷阱」

社会工程学攻击，就是黑客不依赖复杂技术，专挑人性弱点下手：装领导、扮客服，用“紧急”“好奇”“恐惧”等心理诱导，骗你交出密码、转账或执行其他操作。

常见套路：骗你没商量

- 领导急令：“快转款到新账户！这是紧急任务”（实则诈骗）
- 技术支援：“系统有漏洞，点链接装修复工具”（木马藏里面）



个人防范技能包

- 收到“领导指令”“紧急通知”，先通过企业内部群、座机电话二次核实，不轻易执行操作。
- 不在非工作软件（如私人微信、QQ）中谈论工作敏感信息，避免被黑客截获。
- 遇到“技术支持”索要账号密码、远程协助时，直接联系企业IT部门确认，拒绝陌生操作。
- 参加企业钓鱼演练时认真对待，把演练当实战，提升识别诈骗的敏感度。

企业防范技能包

- 搭建内部沟通认证体系，重要指令需通过带有企业标识的官方渠道发布，附专属验证暗号。
- 开发敏感信息监测工具，对邮件、聊天记录中的账号、密码、银行卡号等进行自动拦截提醒。
- 每月组织针对性社会工程学攻击培训，用真实案例讲解最新诈骗手段，强化员工警惕性。
- 建立跨部门应急小组，一旦遭遇社会工程学攻击，能快速联动IT、财务、法务等部门协同处置。

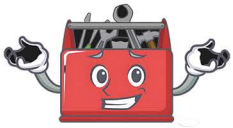
国家网络安全宣传周

防范勒索攻击

勒索攻击 = 数据被「绑架」！黑客逼你交赎金

黑客闯系统， 把重要数据加密锁死， 威胁：“交钱才解锁， 否则删数据！”

个人防范技能包



- 每天下班前备份个人负责的重要工作文件， 存到企业指定的离线存储设备， 不依赖电脑本地硬盘。
- 收到陌生邮件、 链接时， 先看发件人是否可信， 鼠标悬停链接查看真实地址， 不盲目点击。
- 及时更新个人办公电脑的杀毒软件和系统补丁， 开启实时防护功能，不给勒索软件可乘之机。
- 发现电脑文件突然打不开、 出现勒索提示时， 立即断开网络， 不重启电脑或尝试自行解密。

企业防范技能包

- 构建“321 备份策略”： 3 份数据副本、 2 种不同存储介质、 1 份离线备份， 确保数据万无一失。
- 部署反勒索软件和行为分析系统， 对异常加密行为实时预警， 自动阻断可疑进程。
- 关闭企业内网中不必要的端口和服务， 限制外部设备接入权限， 减少勒索软件入侵途径。
- 与专业网络安全公司合作， 定期进行勒索攻击应急演练， 确保员工掌握正确处置流程。

遭遇勒索攻击怎么急救？！

断网隔离！ 立刻断开感染设备， 防止勒索软件“扩散搞破坏”！
别付赎金！ 保存聊天记录、加密文件，马上报案！私付赎金 = 助长犯罪！
恢复数据！ 优先用备份恢复， 没备份找专业机构解密！

国家网络安全宣传周

北京市网络安全公益宣传

警惕
非自主可控产品风险
——暗藏危机的“隐形雷区”

非自主可控产品：
行业系统里的“ 不定时炸弹 ”

非自主可控产品是行业引入的外部软硬件产品， 其中部分产品如同嵌入系统的 “ 黑箱 ”， 其暗藏的安全漏洞、 恶意后门可能在关键时刻引爆， 威胁整个信息体系。

风险根源：
失去主导权的安全困局

非自主可控产品从底层架构到核心代码均由外部掌控， 企业难以全面掌握其设计逻辑与潜在风险。 外部厂商的技术壁垒可能导致漏洞修复滞后， 隐藏的 “ 预留接口 ” 可能成为数据窃取通道， 而关键功能的不可定制化更让防护措施处处受限， 系统安全处于被动地位。

真实案例：
2024 年微软蓝屏事件的连锁灾难

▲事件概览： 2024 年 7 月 19 日， 美国网络安全企业 CrowdStrike 因网络安全平台内容配置更新出现漏洞， 导致全球近千万台微软 Windows 设备突发蓝屏故障。

▲波及范围： 全球超 2000 家企业和机构受困， 覆盖金融、 医疗、 制造业等关键领域。 其中， 美国 1500 架次航班取消、 7400 架次延误， 特斯拉超级工厂生产线停工超 48 小时； 国内多家汽车集团、 电子代工厂因系统瘫痪暂停产能， 单日减产规模超 10 万台。

▲惨痛后果： 业务中断最长达 72 小时， 直接经济损失预估超 80 亿美元。 市场信心崩塌导致 CrowdStrike 美股一度暴跌 15%， 微软市值蒸发 520 亿美元， 企业声誉修复成本难以估量。

警示

你依赖的非自主可控产品， 可能藏着 “隐形漏洞”

核心技术自主可控， 才是安全防护的根本保障！

国家网络安全宣传周
China Cybersecurity Week

筑盾
北京市网络安全公益宣传

首都网警

网络安全为人民
网络安全靠人民

欢迎大家关注“网信北京”微信公众号

首都网警在您身边

百家号　抖音　快手

头条号　微博　微信

北京市互联网信息办公室　北京市公安局