




# 关键信息基础设施安全保护的 对策措施

公安部网络安全保卫局 郭启全

# 全力阻击“蠕虫”勒索病毒攻击

- 2017年5月12日20时左右，新型“蠕虫”勒索病毒“永恒之蓝”爆发，可远程攻击Windows的445等端口（文件共享端口），直接远程执行任意代码，植入勒索病毒等恶意程序。已有150多个国家和地区电脑遭攻击。
- 该勒索病毒利用了基于445端口传播扩散的SMB漏洞MS17-010。2017年4月14日黑客组织Shadow Brokers（影子经纪人）公布的Equation Group（方程式组织）使用的“网络军火”中包含了该漏洞的利用程序。

- 
- 公安部和国家网络与信息安全信息通报中心及时组织专家、企业进行研判，利用各种渠道向200多重要行业、各地公安机关、全社会发布预警，组织各种力量进行快速处置。
  - 通告采取以下紧急措施：一是及时更新最新的Windows操作系统补丁，补丁地址为<https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx>；二是关闭Windows操作系统不必要开放的端口，如445、135、137、138、139等，关闭网络共享功能；三是定期备份重要文件数据。



# “蠕虫”勒索病毒攻击事件给我们的启示

启示一：物理隔离、逻辑隔离无法防范国家级、有组织的网络攻击，也无法防范高智能的网络攻击。

启示二：重要行业部门对内网防护重视不够，内网防护能力不强，非法外联问题突出，系统不定级、不测评、不整改，管理要求缺乏技术方法去落实。

启示三：应急处置能力不强，应急队伍、应急机制、应急装备缺乏。







# 一、如何确定国家关键信息 基础设施






## （一）什么是关键信息基础设施

- 关系国家重大利益、人民群众生命财产安全和社会生产生活秩序，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的网络设施、信息系统和数据资源。

（二）公安机关职责。保卫关键信息基础设施安全，监督、检查、指导关键信息基础设施安全保护工作，防范打击危害关键信息基础设施安全的违法犯罪活动。

### （三）《网络安全法》第三十一条规定

国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。（CII必须落实国家等级保护制度，突出保护重点）



## 二、关键信息基础设施首先要落实 国家网络安全等级保护制度








## （一）依据

一是《网络安全法》第二十一条明确要求：  
国家实行网络安全等级保护制度。

二是中央关于加强社会治安防控体系建设的  
意见、公安改革若干重大问题的框架意见要  
求“健全完善信息安全等级保护制度”。

三是习近平总书记等中央领导批示要求：健  
全完善以保护国家关键信息基础设施安全为  
重点的网络安全等级保护制度。



## （二）把等级保护制度打造成新时期国家网络安全的基本制度、基本国策

- 构建新的法律、政策体系
- 构建新的标准体系
- 构建新的技术支撑体系
- 构建新的人才队伍体系
- 构建新的教育培训体系
- 构建新的保障体系



### （三）等级保护制度的核心内容


- 将风险评估、安全监测、通报预警、案事件调查、数据防护、灾难备份、应急处置、自主可控、供应链安全、效果评价、综治考核等重点措施全部纳入等级保护制度并实施。
- 将网络基础设施、重要信息系统、网站、大数据中心、云计算平台、物联网、工控系统、公众服务平台等全部纳入等级保护监管。
- 将互联网企业纳入等级保护管理，保护互联网企业健康发展。



## （四）新时期等级保护制度的特点

等级保护制度进入2.0时代，网络安全也进入2.0时代：


- 一是全新的国家网络安全基本制度体系
- 二是以保护国家关键信息基础设施为重点
- 三是保护策略发生变化。变被动防御为主动防御，变层面防御为综合防御、纵深防御
- 四是保护对象、保护措施发生变化




# 三、正确处理网络安全等级保护 制度与关键信息基础设施保护 的关系






- 
- 网络安全等级保护制度是关键信息基础设施保护的基础，关键信息基础设施是等级保护制度的保护重点。
  - 网络安全等级保护制度是普适性的制度，关键信息基础设施是重点保护的核心点。
  - 等级保护制度和关键信息基础设施保护是网络安全的两个方面，不可分割。
  - 关键信息基础设施的范围必须在定级备案的第三级（含）以上的保护对象中确定。

- 
- 关键信息基础设施必须按照等级保护制度要求，开展定级备案、等级测评、安全建设整改、安全检查等强制性、规定性工作。
  - 关键信息基础设施保护，要落实公安机关、保密部门、密码部门的保卫、保护、监管责任，落实网络运营者和行业主管部门的主体责任。




# 四、关键信息基础设施安全保护的 对策措施





一是以国家级、有组织的网络攻击能力为标尺，举国家之力，强化保卫、保护、保障，打合成仗、整体仗，全面提高国家大数据安全防护能力。

二是以网络安全等级保护为抓手，以信息通报为平台，以情报侦察为突破，以侦查打击为支撑，构建“侦攻防管控”一体化的大数据安全综合防控体系。



三是关键信息基础设施安全综合防御能力、水平和技术要针对最强大对手去设计，去提升，去创新，防御要专业化、集团化、集约化。

四是全面提升网上行动能力：情报侦察能力、进攻能力、实时监测能力、技术检测能力、通报预警能力、应急处置能力、追踪溯源能力、综合防御能力、态势感知能力、固证打击能力、技术反制能力、数据获取能力。





谢谢!