安全数字世界

预建未来
PLAN UP

作者版权所有
请勿转载

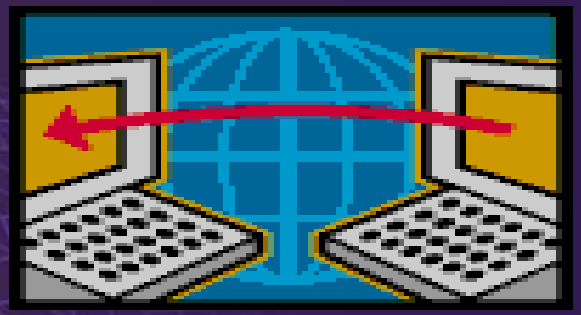
医院网络安全知与行

刘敏超
解放军总医院计算机应用与管理科 主任

作者版权所有
请勿转载

网络安全认知1：所处环境在变

- 底层环境改变：Intranet--Internet



- 底层互联网+生态环境，医院业务正在进行着迅速的解耦与重构
  - 信息系统功能“分解”与“重新组合”
  - 人：雇佣关系的解耦与重构，如多点执业；
  - 物：医院与设备解耦与重构，如区域影像中心、区域检验中心；
  - 院前、院中、院后业务一体化的流程聚合；
  - 康复、养老、护理等功能延伸拓展、业务聚合；
  - 集团、医联体、分级诊疗等机构聚合

作者版权所有
请勿转载

网络安全认知2：安全威胁在变

- 网络攻击低风险、高收益化
  - 人员信息贩卖、大数据交易市场等
- 攻击手段专业化、低门槛化
  - 暗网、黑客职业化、地下组织等
- 攻击对象随机化，不分贫富、国界、机构或个人
  - 如勒索病毒
- 内容攻击目标多样化
  - 数据资源
  - 业务处理过程
- 未知攻击手段和攻击目标越来越多
  - 攻击手段快速演化
  - 攻击目标涉无所不包

作者版权所有
请勿转载

网络安全认知3:权限诉求在变

1、更隐蔽

物联网设备、各种可穿戴设备等各种大数

作者版权所有
请勿转载

2、更牵强

各类手机app等，如一个时钟程序也要访问手机存储、通讯录、短信、位置等

3、更多样

传统授权机制满足不了新需求比如位置权限、三方授权、智能合约涉及的权限分配等

网络安全认知4:保护标的在变

网络安全

- 是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

更广泛

- 传统信息标的，如地址、电话、血型、姓名等
- 新型信息标的，如位置、行为轨迹、语音、图像特征等
- 需要保护的信息标的来自各种环境

更复杂

- 研究研发，安全策略的技术实现
- 各种信息安全技术方案的采纳与部署
- 业务处理过程

作者版权所有
请勿转载

网络安全行动之一:不断增强自身安全能力

组织管理	专门领导机构+专业的执行机构 细致的管理规章+长期持续的员工教育 严格的外来合作方管理
技术应用	研究研发，安全策略的技术实现 各种信息安全技术方案的采纳与部署
资金支持	软件与设备采购 团队建设、人员培训
持续学习	别人的教训变成自己的经验，如分析高阳医院LED屏事件

作者版权所有
请勿转载

网络安全行动之二:分级分类管理

- 对需要保护的标的进行分级、分类管理
  - 群体信息分类，如敏感人群、医保患者人群等
  - 从应用系统、数据层面进行分类分级内容放在这里

- 谨慎评估信息所处的环境安全因素
  - 不同等级的信息要与所处的环境匹配
  - 技术手段与技术能力是否和所处的信息安全环境匹配
  - 遵循谨慎性原则与必要性原则

作者版权所有
请勿转载

网络安全行动之三:管理信任者目录

- 信息安全管理本质是信任管理
  - 谨慎的选择合作厂商，选择有资质、有实力、信誉好的
  - 仔细的甄别每一款软件、每一个模块
  - 有没有第三方机构能对软件进行信任等级评定？内容放在这里

作者版权所有
请勿转载

网络安全行动之四:共建网络安全大环境

攻、防力量不可能平衡

- 明与暗不对等：针对信息安全的攻击可能来自任何时间、地点、针对任何标的
- 攻防成本不对等：防御需要巨大的人力、物力和财力，成本收益极不对称

安全的网络空间是信息安全管理的大前提

- 营造安全的网络空间需要政府、机构和个人的合力
- 网络安全法为营造安全的网络空间具有重大意义

➢CNCERT协调处置网络安全事件约10.6万；
➢年成功关闭772个控制规模较大的僵尸网络，成功切断了黑客对境内约390万台感染主机的控制；
➢据抽样监测，在政府网站安全方面，遭植入后门的我国政府网站数量平均减少了46.5%，遭篡改网站数量平均减少了16.4%
➢[illegible]发起DDoS攻击的活跃控制端数量同比下降46%、被控端数量同比下降37%
➢我国境内僵尸网络控制端数量在全球的排名从前三名降至第十名，DDoS活跃反射源下降了60%

作者版权所有
请勿转载

----------国家计算机网络应急技术处理协调中心《2018年我国互联网网络安全态势综述》

小结：网络安全“知难，行更难”

对现状的认知	行动的路径
封闭环境没了	让自己变得更强大
攻击手段强了	危险的地方不要去
权限复杂了	和靠谱的人做朋友
保护标的多了	共建安全的大环境

作者版权所有
请勿转载

Thank You

作者版权所有
请勿转载