信息化摘编 NO.16

2023-09-05 东师信息化办

本期导读

汇 高校信息化新业态

聚 兄弟院校之优长

高校信息化新业态

一．2023：网络安全的关键一年

随着经济和地缘政治的不稳定，2023 年将是网络安全的关键一年，威胁环境日益扩大，攻击类型更为复杂。

1. 正在酝酿的攻击风暴

钓鱼邮件、勒索软件和分布式拒绝服务攻击的数量依旧呈上升趋势。网络攻击的潜在目标正在增加。当下，目标不仅包括政府机构或大公司，而是基本包括任何拥有消费者数据的组织——无论其规模有多小。

2. 网络安全现状：落后还是领先？

近期，网络安全公司 CYE 发布了《2023 年网络安全成熟度报告》，报告显示，挪威的整体网络安全水平得分最高，其次是克罗地亚和日本。这些国家较早关注网络安全防御，政府和组织有统一规划，它们没有大量的网络安全预算，有的是先进的监管体系。

在各行业中，能源和金融业在整体网络安全成熟度较高，而医疗保健、零售和政府机构的网络安全水平最低。科技行业的得分位于平均水平，可能是因为科技公司：面临着更大的攻击面；采用了易受攻击的新技术；增长速度更快导致。

报告最终表示，大多数组织没有为网络攻击威胁做好充分准备。如果规划和决策正确，在没有大量预算的情况下可以提高网络安全成熟度。企业更应投资于能力，并对自身进行全面评估，制定综合的网络安全方法，以防止黑客利用漏洞。

3. 关键基础部门受格外重视

去年 11 月，欧盟议会和欧盟理事会通过了一项有助于维护欧盟网络安全的新立法——《关于在欧盟全境实现高度统一网络安全措施的指令》（简称 NIS2.0 指令），以进一步提高公共和私营机构的网络安全性、韧性及事件响应能力。

NIS2.0 指令将注重保护关键基础设施部门，并加强欧盟内部各国的连接与国际范围内的立法合作。规定要求企业在事件发生 24 小时内向有关部门报告网络安全事件、修补软件漏洞并准备风险管理措施以保护网络。

4. 建设可靠的数字生态系统

除欧盟外，美国也开始了行动。今年 3 月初，美国发布了新的《国家网络安全战略》，

阐述了政府为确保网络空间安全和建立有弹性的数字生态系统所将采取的行动。该战略所涉及的五项主题分别为：捍卫关键基础设施； 打击和瓦解威胁者；塑造市场力量以提升安全性和复原力；投资于有弹性的未来；加强国际合作以实现共同的目标。

（信息来源：https://mp.weixin.qq.com/s/fzKvXQ8zv-txa_ypq5JHZg）

二．案例分享丨高校网络安全风险评估策略

在网络安全风险不断向政治、经济、文化等领域传导渗透以及国家积极发展内外合作关系的大背景下，高校网络安全防护进入攻坚期。如何有针对性地选择网络防御策略，使防御效果最大化，是各高校需要不断探索的新课题。

1.网络安全策略内视

网络安全策略主要包括互联网暴露面收敛性、账号泄露排查、供应链排查等。网络安全策略的实施需要网络安全投入（设备、人员），最直接的体现是提高网络安全成熟度，网络安全成熟度越高，需要的投入也越大。网络安全是为业务服务的，安全团队要避免过分追求安全技术，在时间和资源有限的情况下，安全团队需评估自身所要达成的成熟度目标，基于风险评估的方法，选择合适的流程、技术和策略，以期达到理想效果。

2.网络安全现状与理想状态

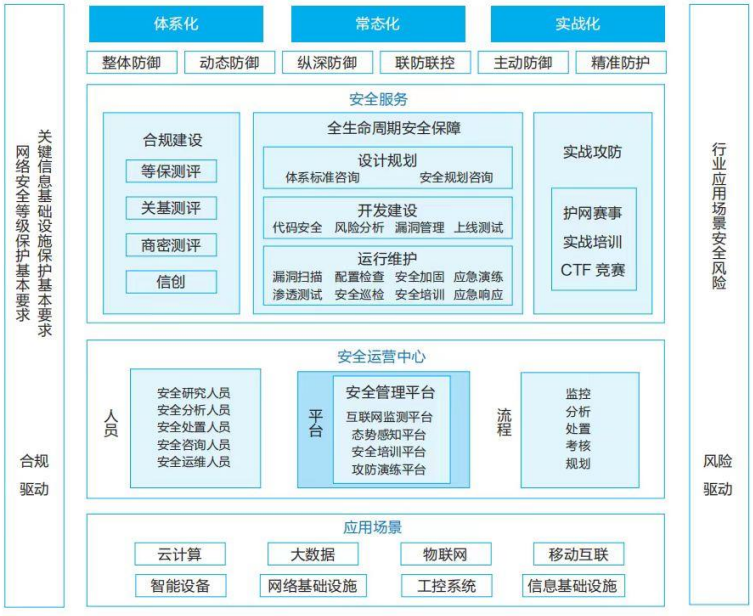
①华中师范大学网络安全现状分析

第一，信息资产复杂。第二，漏洞难以修补。第三，安全意识不足。第四，网络环境复杂，用户需求复杂。第五，难以应对有组织的攻击。第六，安全设备的防护效果缺乏验证。

②理想的网络安全状态

华中师范大学打造了“三化六防”的理想防控体系(如图)。

主要从三个方向出发，即打通学校的各种安全要素，整合安全数据，通过实时风险数据进行决策；具备快速发现、定位威胁与风险的能力，缩短事件响应时间，提高处置效率；完善面向实战的纵深防御体系，形成面向过程的动态防御能力，建立基于情报数据的精准防御能力，打造高效一体的联防、联控机制。



③采用 PDCA 循环实现理想状态

PDCA 循环由美国质量管理专家沃特·阿曼德·休哈特提出，经戴明采纳、宣传、普及，又称“戴明环”。PDCA 循环将质量管理分为四个阶段，即 PLAN（计划）、DO（执行）、CHECK（分析）和 ACT（改善）。

从当前状态开始，不断进行 PDCA 循环，经过多轮的风险评估和处置，螺旋提升网络安全成熟度直至达到理想的网络安全状态。

3. 风险评估过程

①风险评估准备与识别资产：风险评估准备工作一般包括确定本次风险评估的范围，组建风险评估核心小组，准备业务连续性计划，确定风险接受准则，制定详细可行的工作计划表。

②识别威胁和脆弱性：评价资产可以用定量的方法或者定性的方法。定性方法的结果是资产的重要度列表。

③识别可能性和影响：可能性级别是要说明一个脆弱性在相关环境下被威胁所利用的可能性大小等级。此外，风险矩阵是一种能够把风险发生的可能性和伤害程度综合评估的分析方法，它是一种风险可视化的工具，如下图表。可能性和影响都分为 3 级，采用乘法得到风险矩阵，矩阵中不同的数值区域代表不同的风险级别，分为高、中、低 3 个级别。

影响

可能性	1	2	3
1	1	2	3
2	2	4	6
3	3	6	9

风险级别	范围	风险描述
高	7~9	要立即采取措施进行处理
中	4~6	要在合理的时间段内进行处理
低	1~3	可以决定是否需要采取措施进行处理

④识别现有控制措施

可按照四个层次进行：网络层，关注网络层面的安全技术控制措施；系统层，关注系统层面的安全技术控制措施，一般用于保护特定的系统；应用层，关注专门针对应用或自身所固有的安全技术控制措施；数据层，关注专门用于数据防护的安全技术控制措施。

⑤计算残余风险

残余风险指在实现了新增的安全控制后还剩下的风险。如果残余风险没有降低到可接受的级别，则必须重复风险管理过程，以找出一个将残余风险降低到可接受级别的方法。

⑥风险处置

风险处置的方法主要有降低风险、转移风险、规避风险、接受风险等。学校可以根据可接受的风险程度，选择不同的风险处置方法。

（信息来源：https://mp.weixin.qq.com/s/z_jAb8eYGnEX7_FfPnzupw）

兄弟院校之优长

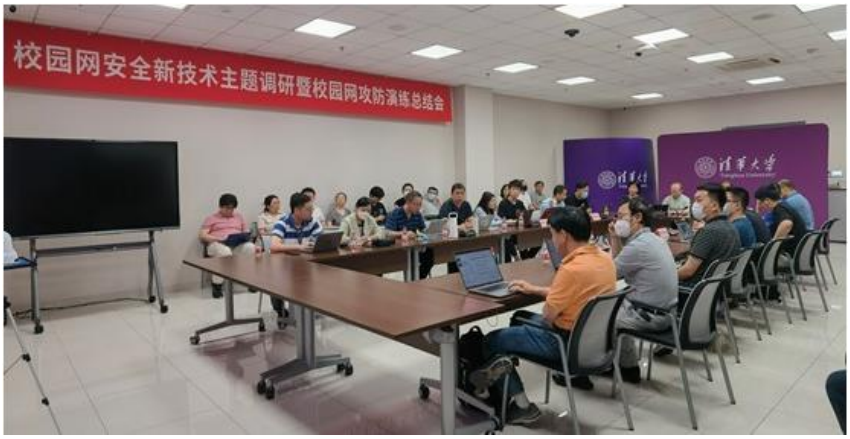
一． 研讨网络安全新技术，提升校园网安全防护能力（清华大学）

——网络研究院和信息化技术中心组织校园网安全新技术主题调研

2023 年 6 月 9 日上午，清华大学网络研究院和信息化技术中心在李兆基科技大楼组织召开“校园网安全新技术主题调研暨校园网攻防演练总结会”。网络研究院、信息办、信息化技术中心相关教职工以及企业代表 40 余人参加了此次会议。

会议主要围绕前期面向科研人员和安全企业的问卷调研结果，结合在网络安全攻防演练活动中发现的问题，集合科研、运维和企业领域的专家，共同探讨网络安全新技术以及新形势下如何提升校园网的安全防护能力。

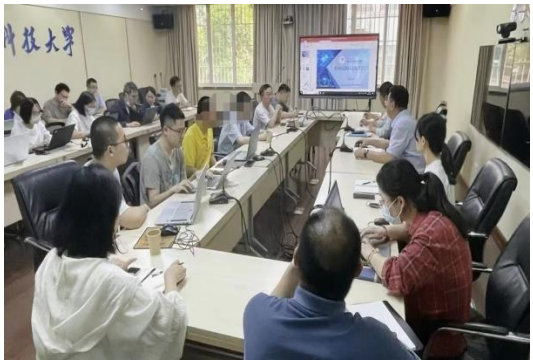
信息化技术中心刘乃嘉老师和网络研究院诸葛建伟老师分别从网络安全防护和攻击两个角度介绍了网络安全攻防演练活动的基本情况。同时邀请绿盟科技、奇安信、奇虎科技、微步在线以及迪普科技等国内知名安全企业分享了业界开展的网络安全新技术研发以及对提升校园网安全防护能力的建议。在讨论环节，学校科研人员与企业技术专家共同就软件供应链安全、数据安全防护、安全保障队伍建设、大模型在安全领域应用等共同关心的话题进行了深入的交流。



（信息来源：https://www.itc.tsinghua.edu.cn/info/1004/1687.htm）

二． 网络安全攻防演练经验交流会举行（华中科技大学）

4 月 17 日下午，在华中科技大学网络与计算中心 207 会议室，网络与信息化办公室、网络空间安全学院、网络与计算中心开展了关于网络安全攻防演练的经验交流会。相关部门领导和老师参加了交流会。



网安学院韩兰胜教授做了关于“网络安全攻防演练实测行动相关知识”的报告，从攻防演练的一般组织方式、攻击方渗透技术、防守方注意事项、渗透测试智能化等方面对网络安全攻防演练做了全面深入的介绍。与会人员结合工作中的实际情况，开展了关于网络安全攻防演练的经验分享和交流讨论。

网信办联合网安学院、网络中心开展此次经验交流活动，充分利用了学校学科专业优势和师资力量，为开展网络安全工作提供指导和建议，有助于进一步提升学校网络安全整体防护水平。

（信息来源：http://imo.hust.edu.cn/info/1060/3851.htm）

策划：李向龙　　摘编：刘玉燕　　微信发布：张丽丽　　网站发布：郭思佳