## 重要时期安全运营服务

## 1、安全工作内容

我院在信息系统全运营工作中，将引入专业安全服务厂商提供专业安全技术能力，配合我院信息部安全运营工作开展。具体工作内容如下：

### 2、重要时期保护工作

针对“两会”、“国庆”、“春节”、“护网行动”等重大活动期间安全。分别在重保前进行全面风险评估，排查安全隐患、重保中进行安全监测与事件处置响应，积极防御网络安全攻击，重保后完成安全事件分析分析、安全策略调优等工作。全面深入排查我院安全隐患，发现可能存在的安全风险以及安全防御体系可能存在的薄弱环节，并修复，确保重保从筹备到执行期间的关键信息系统和数据资产安全。

### 3、入网安全评估工作

在我院新业务系统入网前将安全评估应与安全管理工作紧密结合，在确保业务系统安全的基础上，保障业务系统上线后对整体网络的安全。通过开展入网安全评估工作，有效的发现sql注入、XSS、信息泄露、业务逻辑等安全隐患，并完成整改。以此将风险关口前移，确保新业务的安全上线，防止“带病”入网。评估内容包括但不限于：检查网络结构和安全域划及访问控制是否合理；梳理进程、端口服务开放情况；检查网络设备、主机、数据库、应用层配置是否符合安全规范，是否存在安全漏洞等。

### 4、驻场技术支持工作

我院当前已采购并上线完备的安全设备，但受限于我院安全专业人员数量与安全专业能力薄弱的原因，在安全设备的日常使用中，缺乏专业技术人员对安全设备运行情况，安全设备告警、安全设备日志等进行周期性监测，安全设备使用效率较低。对此，在安全工作中，引入专业安全服务厂商提供安全技术人员开展驻场技术支持工作，周期性对安全设备进行监测并及时响应技术需求。从而补足我院当前安全设备使用效率较低，安全专业能力薄弱的现状。

### 5、基线核查工作

基线核查工作是一项全面审查系统、网络或应用的过程，以确认其安全配置是否符合特定标准或最佳实践。主要包括对操作系统、数据库、中间件、网络设备等进行设置的检查，以确保其符合预先设定的安全基线，从而降低系统遭受攻击的风险。基线核查内容普遍集中于设备的账号管理和口令策略、认证授权、日志配置、通信协议等方面，覆盖了与安全问题相关的各个层面。

从安全事件与系统稳定的角度出发，通过定期的基线核查工作能够降低我院系统被篡改或瘫痪的风险，同时及时发现和修复潜在的漏洞。从守法合规的角度出发，基线核查工作则能够确保系统符合相关法规和标准，降低了违规可能带来的法律责任和业务风险。

### 6、风险评估工作

网络安全脆弱性并不是单纯的是一个硬件或系统漏洞，或是某块安全制度缺失。通常情况下安全事件的发生都是由一系列逻辑联系不强的微小事件逐步扩大。从网络安全事件发生的原因分析，主要集中于以下两点：1、单位未对单位整体安全生态系统的健康状况进行全面评估，无法对单位整体网络风险形成具象、可视化认知。2、在信息化建设中不完整或非集成的解决方案会让单位出现多种特性或功能叠加的产品出现，造成一个脱节或重复的安全防御网络，这种具有不兼容的安全解决方案为基础设施留下漏洞，从而被攻击者利用。

我院作为医疗卫生机构，在信息化建设过程中所面临的网络安全风险逐步扩大，因此开展网络安全风险评估变得尤为重要。按照国家相关风险评估标准，结合我院当前网络安全现状，对信息系统涉及的信息化资产开展全面风险评估。有效发现各信息系统潜在的安全风险，降低因系统漏洞、配置错误、黑客攻击、病毒传播、系统故障等问题对业务产生的影响，保障业务系统的安全、稳定运行。

### 7、网络安全应急响应工作

我院作为关键基础设施单位，不论从合规或是业务安全角度出发，都需开展网络安全应急响应工作，应急响应工作包括应急演练与安事件应急响应两部分。

（1）应急演练

通过模拟真实的网络安全事件开展应急演练工作。真实的呈现我院网络安全事件处置能力，检验应急响应中各部门范围的协同反应水平与实战能力。同时评估我院应急响应预案的实用性、可行性、有效性。

（2）应急响应

针对我院当前无法无法迅速解决的网络入侵、拒绝服务攻击、大规模病毒爆发、主机或网络异常事件等紧急安全问题引入专业安全服务厂商提供应急响应能力，提供安全技术支持。在网络安全事件发生时及时控制事态发展，保护或恢复主机、网络服务的正常工作；在安全事件后进行分析，找出系统的安全漏洞，并根据现场保留情况尽可能对入侵者进行追查。

### 8、漏洞扫描工作

我院在以往建设中引入有专业漏洞扫描工具，但受限于人员配置与安全专业能力原因。在过往安全运营工作中并未定期开展漏洞扫描工作。因此在安全运营工作中，引入专业安全服务厂商，通过人工+工具的形式定期对我院的服务器、网络设备、中间件等进行全面的漏洞扫描，从内网和外网不同的角度找出当前网络结构、网络设备、服务器主机等目标存在的安全漏洞。同时针对发现漏洞形成跟踪台账与整改解决方案，对漏洞进行全生命周期管理。

### 9、重要系统内渗透测试工作

渗透测试不同于漏洞扫描，而且在实施方式和方向上与其有着很大的区别。漏洞扫描是在已知系统上，对已知的弱点进行排查。而渗透测试往往是“黑盒测试”，渗透测试工程师模拟黑客行为，不但要在未知系统中发现弱点，而且还要验证弱点，甚至还会挖掘出一些未知的弱点。

因此我院在漏洞扫描基础上，还需引入安全服务厂商对重要系统开展渗透测试工作。由专业的渗透测试工程师模拟黑客的行为模式，采用黑客的漏洞发现和利用技术，技术尽可能多的攻击方式发现入侵信息系统的潜在可能途径，分析系统可能存在的安全隐患。同时提供对发现漏洞的详细描述与验证过程记录，并根据我院需求完成重大漏洞的整改与复测。

### 10安全培训工作

对医疗行业过往发生网络安全事件的原因进行深入分析，大多数网络安全事件都是由于人员安全意识薄弱、无心疏忽或者恶意造成的。我院作为传染病专科医院，院内绝大部分人员都是医疗专业人员，在网络安全上缺乏清晰的认知或是在日常工作中毫无网络安全意识。对此我院在安全运营工作中需定期的进行安全意识培训，不断强化员工网络安全意识。特别是在国庆、两会、HW等重要时期前开展网络安全意识培训通过以案说法、警示教育等形式，普及工作中的基本网络安全知识，能够极大的提升网络安全防范意识，提高员工识别和应对网络安全威胁的能力。防止黑客通过安全意识薄弱的员工采取钓鱼、社工等方式带来攻击事件。

### 11、网络安全保险兜底工作

无论是技术手段建设还是定期安全运营工作的目标都是对网络安全事件进行预防。但当安全事件突破技术手段后将会对医院造成巨大经济损失、名誉损失等。对此通过网络安全保险，作为网络安全最后的“兜底”，能够在我院当前有限安全预算情况下以其保险产品的属性为我院提供风险兜底及财务补偿，从而提升我院运营的稳定性。结合我院当前的信息化建设现状、配套安全建设现状与医疗行业网络安全风险现状，我院在25年网络安全运营工作中将采购网络勒索损失保障、应急响应费用保障、数据恢复费用保障以及保密责任保障等相关保险保障。以此对安全事件发生后的安全风险进行转移，在提升网络安全事件应对能力的同时提升网络安全投入与产出比，优化我院对于网络安全风险管理的成本投入。

### 12、安全工作清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作项 | 频率 | 备注 |
| 1 | 重要时期保护工作 | / | 五一、国庆、两会、HW等重要时期前一两周开始直至重要时期结束。 |
| 2 | 入网安全评估工作 | / | 新系统正式入网使用前进行。 |
| 3 | 驻场技术支持工作 | 常态化 |  |
| 4 | 基线核查工作 | 2次/年 |  |
| 5 | 风险评估工作 | 1次/年 |  |
| 6 | 应急响应工作 | / | 包括应急演练工作和安全事故应急响应。 |
| 7 | 漏洞扫描工作 | 4次/年 |  |
| 8 | 重要系统内渗透测试工作 | 2次/年 |  |
| 9 | 安全培训工作 | 2次/年 | 针对业务人员的安全意识培训2次。 |
| 10 | 网络安全保险兜底工作 | / | 采购网络勒索损失保障、应急响应费用保障、数据恢复费用保障以及保密责任保障等相关保险保障。 |