网络安全策略：最佳实践白皮书

目录

简介

如果没有安全策略，可能会影响网络可用性。策略开始于估计网络风险，并组建队伍以回应。政策的继续需要为安全违规实施安全更改管理实务和监控网络。最后，审核流程将会修改现有策略，并根据所取得的经验教训进行相应的调整。

本文档分为以下三个部分：准备、预防和响应。请详细查看这些步骤中的每一步。

准备

在实施安全策略之前，您必须完成以下步骤：

- 创建使用策略声明。
- 进行风险分析。
- 建立安全小组结构。

创建使用策略声明

我们建议您创建用于概述用户角色以及安全方面责任的使用策略声明。您可以从一般策略开始，一般策略覆盖贵公司内部的所有网络系统和数据。本文应该为一般用户群提供安全策略及其目的、安全实践改进指南、安全责任定义。如果您的公司已经确定可能导致惩罚或处分员工的特定措施，本文应该清楚说明这些措施及其避免方法。

下一步是创建合作伙伴可接受的使用声明，为合作伙伴提供可用信息的理解、该信息的期望处理，以及贵公司的员工行为。您应该清楚说明已被确定为安全攻击的任何特定行为，对于检测到的安

全攻击应当采取惩罚措施。

最后，创建一个管理员可接收的使用语句解释用户帐户管理、策略执行和权限复核规程。如果您的公司有关于用户密码或随后处理数据的特定策略，请清楚地介绍那些策略。检查合作伙伴接收的用法和客户接收的用法策略语句，确保它们的统一性。切记在可接受的使用政策中列出的管理员要求反应在培训计划和性能评估中。

进行风险分析

风险分析应该确定对于网络、网络资源和数据的风险。这不意味着您应该识别流入网络的每个可能的进入点或每种可能的攻击方式。风险分析的目的是确认您的网络的组成部分，把威胁比率分配到每个部分，并使用适当的安全级别。这有助于在安全和所需网络访问之间维持可行的平衡。

为每个网络资源分配以下三个风险级别之一：

- **低风险系统或数据如果受到威胁（未授权人员查看数据、数据毁损或数据丢失），不会中断业务或者引起法律或财务分歧。**目标系统和数据可以容易地恢复，不允许其它系统的进一步访问。
- **中等风险系统或数据如果受到威胁（未授权人员查看数据、数据毁损或数据丢失）将导致业务适度中断、较小法律或财务分歧，或者提供对其他系统的深入访问。**目标系统或数据要求适度地进行恢复，否则恢复过程可能会破坏系统。
- **高风险系统或数据如果受到威胁（未授权人员查看数据、数据毁损或数据丢失），可能导致业务的严重中断，导致主要的合法或财政分歧，或者威胁人的健康与安全。**目标系统或数据需要做大量工作进行恢复，否则恢复过程可能会破坏业务或其他系统。

为以下每个设备分配风险级别：核心网络设备、分布式网络设备、接入网络设备、网络监控设备(SNMP监控器和RMON探测器)、网络安全设备(RADIUS和TACACS)、电子邮件系统、网络文件服务器、网络打印服务器、网络应用程序服务器(DNS和DHCP)、数据应用服务器(Oracle或其他独立应用程序)、台式机和其它设备(独立打印服务器和网络传真机)。

网络设备（如交换机、路由器、DNS服务器和DHCP服务器）允许深入访问网络，因此它是中等风险设备或高风险设备。设备的损坏可能造成网络崩溃。此类故障可能会对业务造成极大的干扰。

一旦您指定风险级别，就必须识别该系统的用户类型。以下为五种最常见的用户类型：

- **管理员 负责网络资源的内部用户。**
- **特权用户 需要更高访问权限的内部用户。**
- **用户 拥有一般访问权限的内部用户。**
- **合作伙伴 需要访问某些资源的外部用户。**
- **其他 外部用户或客户。**

每个网络系统需要的风险级别和接入类型识别形成了以下安全矩阵。安全矩阵可以为每个系统提供一个快速参考，并为进一步安全措施提供一个起始点，例如创建适当策略以限制网络资源访问。

system	描述	风险级别	用户类型
ATM 交换机	核心网络设备	高	管理员可进行设备配置（仅限支持人员）；所有其他用户可用于进行传输
网络	分布	高	管理员可进行设备配置（仅限支持人员

路由器	式网络设备		）；所有其他用户可用于进行传输
布线室交换机	访问网络设备	中	管理员可进行设备配置（仅限支持人员）；所有其他用户可用于进行传输
ISDN 或拨号服务器	访问网络设备	中	管理员可进行设备配置（仅限支持人员）；合作伙伴和特权用户可进行特殊访问
防火墙	访问网络设备	高	管理员可进行设备配置（仅限支持人员）；所有其他用户可用于进行传输
DNS 和 DHCP 服务器	网络应用程序	中	管理员可进行配置；一般用户和特权用户可进行使用
外部电子邮件服务器	网络应用程序	低	管理员可进行配置；所有其他用户可在 Internet 和内部邮件服务器之间进行邮件传输
内部电子邮件服务器	网络应用程序	中	管理员可进行配置；所有其他内部用户可进行使用
Oracle 数据库	网络应用程序	中或高	管理员可进行系统管理；特权用户可进行数据更新；一般用户可进行数据访问；所有其他用户可进行部分数据访问

建立安全小组结构

在安全经理带领下，与公司的操作区域中的每一个参与者创建交叉功能安全小组。团队代表应该了解安全策略、安全设计和实施方案的技术方面。通常，这要求对团队成员进行其他培训。安全团队的责任包括以下三个方面：策略制定、实践和响应。

策略制定的重点是制定和审核公司的安全策略。至少应每年对风险分析和安全策略进行一次审核。

实践是安全团队进行风险分析、批准安全更改请求、审核供应商和CERT 邮件列表的安全警报并将纯语言安全策略要求转变为特定技术实施的阶段。

最后一个责任范围是响应。当网络监控经常识别到安全侵害时，安全团队成员将执行实际故障排除并修正这种侵害。每个安全小组成员应该详细了解在他或她的操作区域内设备提供的安全功能。

尽管整体上我们定义了团队的责任，但是您应该在您的安全策略中定义安全团队成员各自的角色和责任。

预防

预防可以分为两部分：批准安全变化和监控网络安全。

批准安全性更改

安全性变化定义为网络设备变化，对网络的整体安全可能有影响。安全策略应使用非技术术语确定特定的安全配置要求。换句话说，不是把要求定义为“外部来源FTP连接都不允许通过防火墙”，而是把要求定义为“外部连接不能从内部网络检索文件”。 您需要为您的组织定义一系列特定的要求。

安全小组应该查看符合要求的普通语言需求列表来识别特定网络配置或设计问题。一旦小组创建所需的网络配置更改，以实施安全策略，您就能使用这些适用于所有将来的配置更改。当安全团队可以检查所有更改时，此程序允许他们只检查对担保特殊处理形成足够风险的更改。

我们建议安全团队审核以下几种类型的更改：

- 对防火墙配置的任何更改。
- 对访问控制列表 (ACL) 的任何更改。
- 对 Simple Network Management Protocol (SNMP) 配置的任何更改。
- 不同于已批准软件修订列表的软件的任何变化或更新。

我们还建议遵循以下指导原则：

- 定期更改网络设备口令。
- 将网络设备限制为仅允许批准的人员列表中的人员访问。
- 确保网络设备的当前软件修订级别和服务器环境符合安全配置要求。

除这些审批指南外，从安全小组安排一个代表参与变更管理审批委员会，以便对所有委员会复核的所有更改进行监控。在安全小组进行审批前，安全小组代表可以拒绝当作安全性更改的所有更改。

监视您的网络安全

安全监控类似于网络监控，但安全监控注重检测网络中的变化，显示完全违规情况。安全监控的起点是确定什么是违规。在进行风险分析时，我们识别根据系统威胁所要求的监控级别。在批准安全性更改中，我们已确定网络面临的特定威胁。通过查看这两个参数，我们便非常清楚您需要监控的对象和监控的频率。

在风险分析矩阵中，防火墙认被当作一个高风险的网络设备，这表明您应对它进行实时监控。从Approving Security Changes部分，可以看到您应该对防火墙的所有更改进行监控。这意味着SNMP轮询代理程序应该监控登录失败、异常数据流、防火墙变化、防火墙的授权接入、通过防火墙的连接建立。

根据本示例，为风险分析中确定的每个方面创建监控策略。我们建议每周监控低风险设备，每天监控中等风险设备，每小时监控高风险设备。如果您需要更快地进行检测，请在较短的时间范围内进行监控。

最后，安全策略应确定如何通知安全团队有关安全违规的情况。通常，网络监控软件将首先检测违规情况。它应该向操作中心触发通知，并且应该通知安全小组（如果有必要的话，请使用传呼器）。

回复

响应可以分为三部分：安全违规、恢复和审核。

安全违规

检测到违规时，能够保护网络设备，确定入侵范围，快速做出决策，恢复正常运行。提前进行决策便于管理对入侵的响应。

入侵检测后的第一个操作是通知安全小组。当程序没有到位时，获得适当人选的正确答复会延迟相当长时间。在安全策略中定义一个全天候可用的程序。

其次，您应该定义授予安全团队进行改动的授权级别，并且依照适当的顺序进行改动。以下为可能的纠正措施：

- 实施更改，防止进一步访问违规。
- 隔离违规的系统。
- 联系运营商或 ISP 以尝试跟踪攻击。
- 使用录制设备收集证据。
- 断开违规的系统或违规源。
- 联系警方或其他政府机构。
- 关闭违规的系统。
- 根据优先次序列表恢复系统。
- 通知内部管理和法律人员。

确保详细说明在安全策略中不需要管理层审批而可执行的任何变化。

最后，在安全攻击期间，收集和维护信息有二个原因：确定系统受到安全攻击的危险程度，并检控外部侵害。根据您的目标，您收集信息类型和收集方式有所不同。

要确定违规范围，请执行以下操作：

- 记录事件的方法是获得网络的嗅探器跟踪、日志文件复制、活动用户帐户和网络连接。
- 通过禁用帐户进一步限制妥协，从网络和互联网上断开网络设备。
- 备份受影响的系统，有助于详细分析损伤和攻击方法。
- 查找其他受影响的迹象。通常，当系统受影响时，将会涉及其他系统或帐户。
- 应当维护和复查安全设备日志文件和网络监视日志文件，因为它们经常为攻击方法提供线索。

如果您有兴趣采取诉讼行动，请安排您的法律部门审查证据采集程序和有关人员。此类审核将会提高证据在法律诉讼中的有效性。如果违规实质上来源于内部，请联系人力资源部门。

恢复

使网络恢复正常运行是所有安全违规响应的最终目标。在安全策略中定义如何执行、保护和制作可用的正常备份。因为每个系统具有自己的备份方法和程序，因此安全策略应该作为元政策，详细设计每一个系统，及其需要从备份中恢复的安全条件。如果在恢复完成之前需要审批，也包括获得审批的进程。

审核

审核流程是创建和维护安全策略的最后工作。您需要审核三个方面：策略、状态和实践。

安全策略应该是一个动态文档，可适应不断变化的环境。根据已知最佳实践审核现有策略可使网络保持最新。此外，检查CERT网站 ，了解可纳入安全策略的有用提示、实践、安全改进和警报。

您还应将网络状态与所需的安全状态进行对比，以对其进行审核。专门从事安全行业的其他公司可

以尝试深入网络，不仅测试网络的状态，而且测试您的组织的安全回应。对于可用性较高的网络，我们建议每年进行一次此项测试。

最后，运行被定义为支持人员的培训或测试，它将确保支持人员清楚了解在安全违规期间应该采取什么措施。通常此查询不由管理来宣布，是与网络状态测试一起执行的。通过审核可确定程序和人员培训之间的差距，以便采取纠正措施。

相关信息

- 更多最佳实践白皮书
- 技术支持 - Cisco Systems