网络安全策略：最佳实践白皮书

Contents

Introduction

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。

本文被划分成三个区域：准备、预防和回应。请详细查看这些步骤中的每一个。

准备

在实现安全策略之前，您必须执行以下：

- 创建使用策略声明。
- 进行风险分析。
- 设立一个安全小组结构。

创建使用策略声明

我们推荐创建使用策略声明概述用户角色和责任关于安全。您能从包括所有网络系统和数据在您的公司内的一般政策开始。本文应该提供一般用户属性对安全策略、其目的、他们的安全责任的指南为改进他们的安全实践和定义的了解。如果您的公司识别可能导致惩罚或处分员工的特定动作，在本文应该清楚地明确表达这些动作和如何避免他们。

下一步是创建合作伙伴可接受的使用语句提供合作伙伴供给他们对信息的了解，该信息的期望的处理，以及您的公司的员工的进行。您应该清楚地解释被识别作为安全攻击和惩罚措施将采取的所有

特定操作如果发现安全攻击。

最后，请创建管理员可接受的使用语句解释用户帐户管理、策略执行和权限复核程序。如果您的公司有特定策略关于用户密码或数据随后的处理，请清楚地提交那些策略。根据合作伙伴可接受的使用和用户可接受的使用规定语句检查策略保证一致性。切记在可接受的使用规定列出的管理员要求在培训的计划和性能评估被反映。

进行风险分析

风险分析应该识别风险到您的网络、网络资源和数据。这不意味着您应该识别每可能的进入点到网络，亦不每攻击可能的平均值。风险分析的目的是识别您的网络的部分，分配对估计一个的威胁对每个部分和运用适当级别安全。这帮助维护在安全和必需的网络访问之间的一个可使用的平衡。

分配以下三个风险级别的每种网络资源一：

- **低风险**系统或数据，如果折衷(未授权人员查看的数据，数据损坏的或者数据失去)不会打乱事务也不会导致合法或财政分歧。可以容易地恢复目标系统或数据和不允许其他系统进一步访问。
- **中等风险**系统或数据，如果折衷(未授权人员查看的数据，数据毁损了或者数据失去)的事务，较小合法或财政分歧将导致一次中等中断或者提供对其他系统的进一步访问。目标系统或数据要求适度工作量恢复或恢复过程是制造混乱对系统。
- **高危险的**系统或数据，如果折衷(未授权人员查看的数据，数据损坏的或者数据失去)的事务将导致一个极端中断，导致主要合法或财政分歧或者威胁人的健康与安全。目标系统或数据要求大量工作恢复或恢复过程是制造混乱对事务或其他系统。

指定风险级别到以下每一个：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监控程序和RMON探测)，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、应用服务器(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)。

因此网络设备例如交换机、路由器、DNS服务器和DHCP服务器能允许进一步访问到网络，并且是中等或高危险的设备。也很可能，此设备的损坏可能造成网络崩溃。这样故障可以是十分破坏性的对事务。

一旦指定了风险级别，识别该系统的用户的种类是必要的。用户的五种常用类型是：

- **管理员**内部用户负责对网络资源。
- 有需要的**特许**内部用户对更加极大的访问。
- 有一般访问的**用户**内部用户。
- **合作伙伴**外部用户以需要访问一些资源。
- **其他**外部用户或用户。

风险级别和访问的种类的证明需要每个网络系统形成以下安全矩阵的基底。安全矩阵为每个系统提供一个快速参考和一个起始点为进一步安全措施，例如创建适当的策略进入对网络资源的限制的入口。

系统	说明	风险级别	用户的类型
ATM交换机	核心网络设备	高	设备配置的(仅支持人员管理员);其他为使用作为传输

网络路由器	分布式网络设备	高	设备配置的(仅支持人员管理员);其他为使用作为传输
布线室交换机	接入网络设备	媒体	设备配置的(仅支持人员管理员);其他为使用作为传输
ISDN或拨号服务器	接入网络设备	媒体	设备配置的(仅支持人员管理员);合作伙伴和特权用户特殊访问的
防火墙	接入网络设备	高	设备配置的(仅支持人员管理员);其他为使用作为传输
DNS和DHCP服务器	网络应用程序	媒体	配置的管理员;一般和特权用户为使用
外部电子邮件服务器	网络应用程序	低	配置的管理员;其他在互联网和内部邮件服务器之间的邮件传输
内部电子邮件服务器	网络应用程序	媒体	配置的管理员;其他内部用户为使用
Oracle数据库	网络应用程序	中或高度	系统管理的管理员;数据更新的特权用户;数据存取的一般用户;其他部分数据访问

设立安全小组结构

用参与者创建安全经理导致的一交叉功能安全团队从您的公司的操作区域中的每一个。在小组的代表应该知道安全策略和安全设计和实施的技术方面。通常，这为小组成员要求其它培训。安全团队有三个责任范围：策略制定、实践和回应。

策略制定集中于设立和查看公司的安全策略。最少，请每年查看风险分析和安全策略。

实践是期间安全团队执行风险分析、安全性变化请求审批，复核从两个供应商的安全性预警和CERT邮件列表的阶段 在，并且把普通语言安全策略需求变成特定技术实施。

最后责任范围是回应。当网络监控经常识别一个破坏安全时，它是执行实际故障排除和修正这样侵害的安全团队成员。每安全团队成员在他们的操作区域应该详细认识设备提供的安全功能。

当我们定义了整体上时小组的责任，您应该定义安全团队成员的各自的作用和责任在您的安全策略。

预防

预防可以分成两部分：您的网络满意的安全性变化和监控安全。

满意的安全性变化

安全性变化被定义成有在网络的整体安全的一潜在影响对网络设备的更改。您的安全策略应该识别特定安全配置需求用非技术性的术语。换句话说，而不是定义需求成“没有外部来源FTP连接通过防火墙将允许”，定义了需求成“外部连接不应该能从内部网络检索文件”。您将需要定义您的组织的特有的需求。

安全团队应该查看符合要求的普通语言需求列表识别特定网络配置或设计问题。一旦小组造成必需的网络配置更改实现安全策略，您能适用这些于所有将来配置更改。当检查所有更改时安全团队是可能的，此进程给他们只检查形成足够的风险担保特殊处理的更改。

我们建议安全团队复核更改的以下类型：

- 其中任一变成防火墙配置。
- 其中任一变成访问控制列表(ACL)。
- 其中任一更改到简单网络管理协议(SNMP)配置。
- 任何变化或更新在与批准的软件修订级别列表有所不同的软件上。

我们也推荐遵守以下指南：

- 定期地更改密码到网络设备。
- 对人员一张批准的列表限制对网络设备的访问。
- 保证网络设备和服务器环境的当前软件修订级别是与安全配置需求一致。

除这些审批指南之外，请安排从安全团队的一个代表坐变更管理审批板，为了监控该所有的更改板复核。安全团队代表能拒绝考虑安全性变化的所有更改，直到由安全团队审批了。

监控您的网络安全

安全监控类似于网络监控，除了它着重发现指示一个破坏安全在网络上的变化。安全监控的起始点确定什么是侵害。在进行风险分析，我们识别根据对系统的威胁要求的监控的级别。在满意的安全性变化，我们识别对网络的特定威胁。通过查看这两个参数，我们将开发一张清楚的图片的什么您多频繁需要监控和。

在风险分析矩阵，防火墙认为一个高危险的网络设备，表明您在实时应该监控它。从Approving Security Changes部分，您看到您应该为对防火墙的所有更改监控。这意味着SNMP轮询代理程序应该监控作为登录失败、异常的数据流、通过防火墙被准许的对防火墙和连接建立更改对防火墙，访问的这样事。

在此示例后，请创建在您的风险分析识别的各个区域的监控策略。我们推荐每小时监控低风险设备每周，中风险设备日报和高危险的设备。如果需要更加迅速的检测，请监控在一个更短的时间段。

最后，您的安全策略应该寻址如何通知破坏安全安全团队。通常，您的网络监控软件将是发现侵害的第一个。它应该如果需要，触发通知到操作中心，应该反过来通知安全团队，使用传呼器。

回应

回应可以分成三部分：破坏安全、恢复和复核。

破坏安全

当发现时侵害，能力保护网络设备，确定闯入的范围和恢复正常运行取决于快速决策。安排这些决策做提早使回应闯入更加易管理。

第一个动作在闯入的检测后是安全团队的通知。如果不到位程序，将有使正确的人民的严重的延迟适用正确答复。定义在一天24小时是可用的您的安全策略的一个程序，每星期七天。

其次您应该定义权力标准产生安全团队做变动，并且在什么顺序应该做更改。可能的纠正措施是：

- 实现更改防止对侵害的进一步访问。
- 查出非法系统。
- 与载波或ISP联系为跟踪攻击。
- 使用收集记录的设备证据。
- 断开非法系统或侵害的来源。
- 与联系的police，或者其他政府机构。
- 关闭非法系统。
- 恢复根据一张优先安排的列表的系统。
- 通知内部管理和合法的人员。

请务必详述可以执行，不用在安全策略的管理审批的所有更改。

最后，在安全攻击期间，有两个原因对于收集的和维护的信息：确定系统由安全攻击减弱了的范围和检控外部侵害。您收集它信息和方式的种类根据您的目标有所不同。

要确定侵害的范围，请执行以下：

- 通过获得网络的日志文件的嗅探器跟踪，复制，活动用户帐户和网络连接记录事件。
- 通过禁用帐户，断开网络设备从网络和断开限制进一步妥协从互联网。
- 备份减弱的系统帮助在对损伤的一个详细分析和攻击方法。
- 寻找妥协的其他符号。通常，当系统减弱时，有介入的其他系统或帐户。
- 维护和复核安全设备日志文件和网络监控日志文件，他们经常提供提示向攻击方法。

如果是对采取诉讼感兴趣，请安排您的法律部门查看采集权限的证据和介入方法。这样复核增加证据的效果在法律诉讼的。如果侵害是内部本质上，与您的人力资源部门联系。

恢复

正常的网络操作的恢复是所有破坏安全回应的最终目标。定义在安全策略您进行，如何巩固，并且做可用的正常备份。因为每个系统有其自己的平均值和方法备份，安全策略应该作为元政策，选派为每个系统要求恢复从备份的安全条件。如果需要审批，在恢复可以完成前，请包括获得的审批进程。

复核

审核流程是在创建和维护安全策略的最终努力。有您将需要查看的三件事：策略、状态和实践。

安全策略应该是适应一个不断变化的环境的一个活文件。查看已知最佳实践的现有策略保持网络最新状态。并且，请检查CERT网站 可以合并到您的安全策略里的有用的提示、运作、安全改进和戒备。

与期望安全形式比较，您应该也查看网络的状态。专门化安全的公司外能尝试击穿网络和测试网络的不仅状态，但是您的组织安全回应。对于高可用性网络，我们推荐每年进行这样测试。

最后，实践被定义作为支持人员的查询或测试确保他们有对什么的清除了解执行在破坏安全时。通常，此查询由管理是未宣布的并且与网络状态测试一道执行。此复核识别在程序和人员培训的空白，以便纠正措施可以采取。

Related Information

- 更多最佳实践白皮书
- Technical Support - Cisco Systems