容大互联安全加固项目
IT 设备安全加固操作指引参考

目录

1 IT 设备安全加固方法

- 工具扫描：使用业界优秀的安全弱点扫描工具进行漏洞扫描，高效率地从技术角度发现信息资产存在的安全弱点，并进行风险分析。

  建议可采用专业的漏洞扫描工具 nessus

- 专家评估：参照各类标准和行业经验在工作准备过程中建立针对上述设备的各类安全评估检查列表（CheckList），依照这些检查表，专家登录到设备进行逐项配置比对，对设备的安全现状进行综合分析评估。

根据前期的安全评估的结果，制定安全加固实施方案，对各类安全漏洞进行加固，弥补由此产生的安全弱点。

应提前制定安全加固报告，其内容应包括如下方面：安全加固项，加固内容，实施步骤和具体操作，加固实施风险，风险规避措施。

安全加固类别包括：

- 主机操作系统加固
- 数据库系统加固
- 网络设备安全加固
- 网络安全设备安全加固
-

2 安全加固内容评估

2.1 操作系统

通过对主机操作系统进行安全检测，发现当前操作系统中存在漏洞，测试系统的抗攻击能力攻击。对于发现的问题，给出安全解决建议，防止黑客利用主机系统漏洞和攻击工具进行破坏。主机系统安全评估包括以下内容：

- 主机系统的版本及其补丁
- 相关的日志分析，检查可疑和行为
- 检测系统后门程序
- 文件系统安全设置
- 系统帐号安全设置

- 主机信任关系检查
- 系统配置文件检查
- 口令强度检查
- 系统安全漏洞检查
- 网络和服务安全配置

2.2 数据库

数据库安全评估内容如下：

- 安全补丁状况
- 帐号检查
- 策略配置
- 重要文件访问控制
- 数据库参数设置
- 权限设置
- 备份与恢复

2.3 网络设备

网络设备安全评估内容为：

- 弱密码检查
- 设备稳定性
- 策略严格性
- 防火墙运行情况检查
- 检查 SNMP
- 检查远程管理方式
- 检查防火墙日志
- 检查防火墙自身抗攻击能力

2.4 网络安全设备

网络安全设备如 IDS/IPS、防火墙、防病毒等，将根据不同设备类型的 checklist 进行配置检查。检查内容包括：安全配置、帐号设置、告警设置、日志保存设置等内容。

2.5 其他 IT 组件

可根据需要，增加如中间件设备、应用系统安全、渗透测试等方面内容，以实现完整的技术类安全评估。

3 IT 设备安全加固方法

根据前期的安全评估的结果，制定安全加固实施方案，对各类安全漏洞进行加固，弥补由此产生的安全弱点。

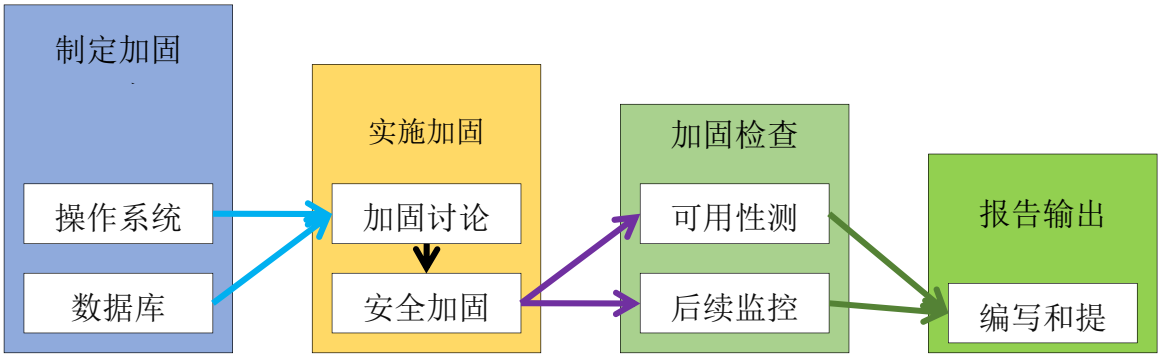
应提前制定安全加固报告，其内容应包括如下方面：安全加固项，加固内容，实施步骤和具体操作，加固实施风险，风险规避措施。

安全加固类别包括：

- 主机操作系统加固
- 数据库系统加固
- 网络设备安全加固
- 网络安全设备安全加固

3.1 加固流程

安全加固实施流程如下：



图表 3-1 安全加固实施流程

安全加固实施过程中，建议客户由安全工程师逐一登录到设备中进行操作。本文第 4 章简要描述安全加固阶段的准备工作内容。

3.2 加固内容

3.2.1 操作系统

针对不同主机平台（UNIX，WINDOWS），通过相应的安全设置使主机更加安全可靠。

操作系统安全加固适合以下系统：

UNIX 系统平台（Solaris、HP-UX、IBM AIX, Linux,BSD）

Windows 系统平台（NT，2000，XP，2003）

操作系统安全加固的具体实施内容如下：

实施的环境准备：对现有系统的运行状况进行评估，对关键业务主机进行备份，需要磁带机，磁带等备份工具。如有可能建议最好在模拟机器上作测试，成功后再推广实施。

- 微软操作系统

  补丁、文件系统、帐号管理、网络及服务、注册表、共享、应用软件、审计/日志，其它（包括紧急恢复、数字签名等）。

- UNIX 操作系统

  补丁、文件系统、配置文件、帐号管理、网络及服务、NFS 系统、应用软件、审计/日志，其它（包括专用安全软件、加密通信及数字签名等）。

3.2.2 数据库

对于数据库的加固，需要结合应用帐号的使用状况来确定，通常需要进行必要的测试，以避免数据库安全加固实施后对应用系统运行造成影响，最大程度的降低风险。

安全加固内容如下：

主流数据库系统（包括 Oracle、SQL Server、Sybase、MySQL、Informix）的补丁更新列表、锁定或删除数据库无关帐号；数据库安全配置；建立数据库账号安全策略；角色权限设置；对部分的存储过程进行修改或删除；备份恢复设置；开启数据库的相关审计功能或者通过其他审计手段，审计数据库的数据操作，以增强数据库的安全性。

3.2.3 网络设备

网络设备的加固内容主要为：

- 根据现有路由器和交换机的软件版本，提供升级或补丁列表以解决当前版本的安全隐患
- 控制管理权限设置
- 帐号设置
- 配置 AAA
- 关闭不必要的服务
- 安全日志配置

3.2.4 网络安全设备

将根据安全评估结果，加固主要内容为：

- 访问控制设置
- 安全策略配置
- 安全日志配置
- 告警设置

3.2.5 网络设备具体操作指引：

在网络设备上具体分 JUNIPER 路由器、华为路由器、思科路由器等几种型号。在实际评估检查中，针对不同的设备将进行不同的检查内容。

- **JUNIPER 路由器**
  - 账号
    - 应按照不同的用户分配不同的账号，避免不同用户间共享账号，避免用户账号和设备间通信使用的账号共享。
    - 应删除与设备运行、维护等工作无关的账号。
    - 为了控制不同用户的访问级别，建立多用户级别，根据用户的业务需求，将用户账号分配到相应的用户级别。
  - 口令
    - 对于采用静态口令认证技术的设备，口令长度至少 6 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类。
    - 对于采用静态口令认证技术的设备，账户口令的生存期不长于 90 天。
    - 修改 root 密码。root 的默认密码是空，修改 root 密码，避免非管理员使用 root 账号登录。
  - 授权
    - 在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
  - 认证
    - 设备通过相关参数配置，与认证系统联动，满足帐号、口令和授权的强制要求。
  - 日志管理
    - 设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址。
    - 设备应配置日志功能，记录用户对设备的操作，比如以下内容：账号创建、删除和权限修改，口令修改，读取和修改设备配置，涉及通信隐私数据。记录需要包含用户账号，操作时间，操作内容以及操作结果。

- 设备应配置日志功能，记录对与设备相关的安全事件，比如：记录路由协议事件和错误。
- 设备配置远程日志功能，将需要重点关注的日志内容传输到日志服务器。
- 设置系统的配置更改信息保存到单独的 change.log 文件内。
- 开启 NTP 服务，保证日志功能记录的时间的准确性。路由器与 NTP SERVER 之间开启认证功能。

◆ 基本协议安全

- 对于具备 TCP/UDP 协议功能的设备，设备应根据业务需要，配置基于源 IP 地址、通信协议 TCP 或 UDP、目的 IP 地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。

◆ 路由协议安全

- 对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议。
- 配置动态路由协议（BGP/ MP-BGP /OSPF 等）时必须启用带加密方式的身份验证功能，相邻路由器只有在身份验证通过后，才能互相通告路由信息。
- 配置 MP-BGP 路由协议，应配置 MD5 加密认证，通过 MD5 加密认证建立 peer。
- 配置 MP-BGP 路由协议，应配置 MD5 加密认证，通过 MD5 加密认证建立 peer。
- 对于非点到点的 OSPF 协议配置，应配置 MD5 加密认证，通过 MD5 加密认证建立 neighbor。
- 制定路由策略，禁止发布或接收不安全的路由信息。

◆ SNMP 协议安全

- 设置 SNMP 访问安全限制，只允许特定主机通过 SNMP 访问网络设备。
- 系统应关闭未使用的 SNMP 协议及未使用的 RW 权限。
- 系统应配置为 SNMP V2 或以上版本。
- 系统应配置可接收 SNMP 消息的主机地址。

◆ MPLS 安全

- 启用 RSVP 标签分发协议时，打开 RSVP 协议认证功能，如 MD5 加密，确保与可信

方进行 RSVP 协议交互。

- 其他安全
  - 对于 Juniper 路由器，应配置定时账户自动登出。
  - 对于具备 consol 口的设备，应配置 consol 口密码保护功能。
  - 开启配置文件定期备份功能，定期备份配置文件。
  - 关闭网络设备不必要的服务，比如 FTP、TFTP 服务等。
  - 开启安全防护功能，如状态防火墙等（如果具备类似功能）。
  - 如接受统一网管系统管理，建议配置 SNMP VERSION3 协议。
  - 系统远程管理服务 TELNET、SSH 默认可以接受任何地址的连接，出于安全考虑，应该只允许特定地址访问。
  - TELNET 默认可以接受 250 个同时连接。配置 TELNET 等远程维护方式时，应配置连接最大数量限制为 10 个，并且每分钟最多有 5 个可以连接，可以防止在 TELNET 端口上的 SYN flood DoS 攻击。
  - 在网络边界，设置安全访问控制，过滤掉安全攻击数据包，例如 udp 1434 端口（防止 SQL slammer 蠕虫）、tcp445,5800,5900（防止 Della 蠕虫）。

■ **华为路由器**

- 帐号
  - 应按照用户分配账号。避免不同用户间共享账号。避免用户账号和设备间通信使用的账号共享。
  - 应删除与设备运行、维护等工作无关的账号。
- 权限
  1) 限制具备管理员权限的用户远程登录。远程执行管理员权限操作，应先以普通权限用户远程登录后，再切换到管理员权限账号后执行相应操作。
  2) 在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
  3) 设备通过相关参数配置，与认证系统联动，满足帐号、口令和授权的强制要求。
- 口令

1) 对于采用静态口令认证技术的设备，口令长度至少 6 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类。

2) 静态口令必须使用不可逆加密算法加密后保存于配置文件中。

◆ 日志

1) 设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址。

2) 设备应配置日志功能，记录用户对设备的操作。例如：账号创建、删除和权限修改，口令修改，读取和修改设备配置，读取和修改业务用户的计费数据、身份数据、涉及通信隐私数据。记录需要包含用户账号，操作时间，操作内容以及操作结果。

3) 设备应配置日志功能，记录对与设备相关的安全事件。

4) 设备应支持远程日志功能。所有设备日志均能通过远程日志功能传输到日志服务器。设备应支持至少一种通用的远程标准日志接口，如 SYSLOG、FTP 等。

5) 开启 NTP 服务，保证日志功能记录的时间的准确性。路由器与 NTP SERVER 之间要开启认证功能。

6) 对于具备 TCP/UDP 协议功能的设备，设备应根据业务需要，配置基于源 IP 地址、通信协议 TCP 或 UDP、目的 IP 地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。

◆ 其他

1) 对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议。

2) 通过 ACL 配置对常见的漏洞攻击及病毒报文进行过滤。

3) 条件允许情况下，端口配置 URPF（Unicast Reverse Path Forwarding），即单播反向路径查找，其主要功能是防止基于源地址欺骗的网络攻击行为。

4) 动态路由协议口令要求配置 MD5 加密。

5) 制定路由策略，禁止发布或接收不安全的路由信息。

6) 系统应关闭未使用的 SNMP 协议及未使用 RW 权限。

7) 系统应修改 SNMP 的 Community 默认通行字，通行字应符合口令强度要求。

8) 系统应配置为 SNMPV2 或以上版本。

9) 设置 SNMP 访问安全限制，只允许特定主机通过 SNMP 访问网络设备。

10) 启用 LDP 标签分发协议时，打开 LDP 协议认证功能，如 MD5 加密，确保与可信方进行 LDP 协议交互。

11) 关闭未使用的端口。

12) 配置定时账户自动登出，登出后用户需再次登录才能进入系统。

13) 配置 consol 口密码保护功能。

14) 关闭网络设备不必要的服务，比如 FTP、TFTP 服务等。

15) 系统远程管理服务 TELNET、SSH 默认可以接受任何地址的连接，出于安全考虑，应该只允许特定地址访问。

- **思科路由器**
  - 权限
    1) 限制具备管理员权限的用户远程登录。远程执行管理员权限操作，应先以普通权限用户远程登录后，再切换到管理员权限账号后执行相应操作。
    2) 在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。
  - 口令
    1) 对于采用静态口令认证技术的设备，口令长度至少 6 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类。
    2) 静态口令必须使用不可逆加密算法加密，以密文形式存放。如使用 enable secret 配置 Enable 密码，不使用 enable password 配置 Enable 密码。
  - 日志
    1) 设备应支持远程日志功能。所有设备日志均能通过远程日志功能传输到日志服务器。设备应支持至少一种通用的远程标准日志接口，如 SYSLOG、FTP 等。
    2) 对于具备 TCP/UDP 协议功能的设备，设备应根据业务需要，配置基于源 IP 地址、通信协议 TCP 或 UDP、目的 IP 地址、源端口、目的端口的流量过滤，过滤所有和业务不相关的流量。

3) 对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议。

4) 与记账服务器(如 RADIUS 服务器或 TACACS 服务器)配合，设备应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号，登录是否成功，登录时间，以及远程登录时，用户使用的 IP 地址。

5) 与记账服务器(如 TACACS 服务器)配合，设备应配置日志功能，记录用户对设备的操作，如账号创建、删除和权限修改，口令修改，读取和修改设备配置，读取和修改业务用户的话费数据、身份数据、涉及通信隐私数据。记录需要包含用户账号，操作时间，操作内容以及操作结果。

6) 开启 NTP 服务，保证日志功能记录的时间的准确性。

◆ 帐户

1) 应按照用户分配账号。避免不同用户间共享账号。避免用户账号和设备间通信使用的账号共享。

2) 应删除与设备运行、维护等工作无关的账号。

3) 设备通过相关参数配置，与认证系统联动，满足帐号、口令和授权的强制要求。

◆ IP 协议安全

1) 配置路由器，防止地址欺骗。

2) 路由器以 UDP/TCP 协议对外提供服务，供外部主机进行访问，如作为 NTP 服务器、TELNET 服务器、TFTP 服务器、FTP 服务器、SSH 服务器等，应配置路由器，只允许特定主机访问。

3) 过滤已知攻击：在网络边界，设置安全访问控制，过滤掉已知安全攻击数据包，例如 udp 1434 端口（防止 SQL slammer 蠕虫）、tcp445,5800,5900（防止 Della 蠕虫）。

4) 功能禁用：

5) 禁用 IP 源路由功能，除非特别需要。

6) 禁用 PROXY ARP 功能，除非路由器端口工作在桥接模式。

7) 禁用直播（IP DIRECTED BROADCAST）功能

8) 在非可信网段内禁用 IP 重定向功能。

9) 在非可信网段内禁用 IP 掩码响应功能

10) 5)启用协议的认证，加密功能

11) 设备与 RADIUS 服务器、TACACS 服务器、NTP 服务器、SNMP V3 主机等支持认证加密功能的主机进行通信时，尽可能启用协议的认证加密功能，保证通信安全。

◆ 路由协议安全

1) 启用动态 IGP（RIPV2、OSPF、ISIS 等）或 EGP（BGP）协议时，启用路由协议认证功能，如 MD5 加密，确保与可信方进行路由协议交互。

2) 采用 BGP 协议作为 EGP 协议时，使用 Route flap damping 功能防止路由风暴。

3) 在网络边界运行 IGP 或 EGP 动态路由协议时，配置路由更新策略，只接受合法的路由更新，防止非法路由注入。只发布所需的路由更新，防止路由信息泄漏。

➢ SNMP 协议安全

4) 修改 SNMP 的 Community 默认通行字，通行字符串应符合口令强度要求。

5) 只与特定主机进行 SNMP 协议交互

6) 未使用 SNMP 的 WRITE 功能时，禁用 SNMP 的写（WRITE）功能。

◆ MPLS 安全

启用 LDP 标签分发协议时，打开 LDP 协议认证功能，如 MD5 加密，确保与可信方进行 LDP 协议交互。

◆ 其他安全

1) 关闭未使用的接口，如路由器的 AUX 口。

2) 要修改路由缺省器缺省 BANNER 语，BANNER 最好不要有系统平台或地址等有碍安全的信息。

3) 配置定时账户自动登出。如 TELNET、SSH、HTTP 等管理连接和 CONSOLE 口登录连接等。

4) 配置 consol 口密码保护功能。

5) 关闭不必要的网络服务或功能

6) 禁用 TCP SMALL SERVERS

7) 禁用 UDP SMALL SERVERS

8) 禁用 Finger

9) 禁用 HTTP SERVER

10) 禁用 BOOTP SERVER

11) 关闭 DNS 查询功能，如要使用该功能，则显式配置 DNS SERVER

3.2.6 安全加固实施步骤

1. 详细了解安全操作工作指引的内容，与公司安全工程师一起讨论确定安全加固时间、安全加固内容、安全加固操作流程以及风险控制流程。
2. 由于安全加固实施前和后需要重启设备以便进行配置验证，因此客户需提前申请业务停机时间。
3. 如有条件，需提前在测试环境中进行安全加固测试，确认无误后再进行真实环境加固。
4. 提前进行设备备份，备份数据、操作系统、重要配置文件，关键网络设备的配置等。
5. 安全加固实施期间，客户需配合工程师进行系统检查，设备重启、监控和测试等工作。
6. 安全加固实施期间针对每一个步骤建立回退措施，以便意外情况下可恢复到初始状况。