全场景应对终端安全威胁，构建多位一体终端防护体系

王　浩，智　佩，云成龙，郑　晨
（中国联合网络通信有限公司内蒙古分公司，内蒙古自治区 呼和浩特 010050）

摘要：办公终端、监控终端、营业终端等计算机终端（以下简称终端）使用场景、网络接入方式众多，且短时间内无法进行统一管理，染毒终端或未授权终端入网后将对整体内部网络带来极大威胁。为此，内蒙古联通在 2020 年引入集团集约化终端安全管控能力后，积极与集团终端团队沟通、学习，深入研究产品功能、策略，结合省内自研能力，通过对终端管控平台数据治理后，实现了终端多位一体的安全防护架构，极大的降低了终端安全威胁事件产生几率。

关键词：终端安全；多位一体
中图分类号：TP391　　**文献标识码：**A　　**文章编号：**2096-9759（2023）06-0162-03

0 引言

中国联通全面贯彻落实国家总体安全观，筑牢网络空间安全可信的第一道防线，守护新型数字信息基础设施，构建数字经济“国家首席、政府首选、人民首信”的“安全第一盾”。

内蒙古联通坚决贯彻落实集团公司《中国联通坚强网络和安全产品服务行动计划》相关要求，在业务发展方向由传统线下逐渐向线上迁移的数字化转型过程中积极推进集团集约化安全能力落地，在尽用集团能力的同时自查省内短板，及时补充省内缺失安全能力。

1 现状分析

为了应对网络与信息安全威胁风险，省内关键基础设施已完成统一出入口收敛，并处在集中部署的安全能力严密的监控之下；而来自网络内部计算机终端的安全威胁由于操作系统自身问题以及使用人员安全防范意识差异化更为突出，已经成为了网络与信息安全管理者亟待解决的重要问题之一。

经调研，办公终端、监控终端、营业终端等计算机终端（以下简称终端）使用场景、网络接入方式众多，且短时间内无法进行统一管理，染毒终端或未授权终端入网后将对整体内部网络带来极大威胁。

为此，内蒙古联通在 2020 年引入集团集约化终端管控能力后，积极与集团终端团队沟通、学习，深入研究产品功能、策略，结合省内自研能力，通过对终端管控平台数据治理后，实现了终端多位一体的安全防护架构，极大地降低了终端安全威胁事件产生的几率。

2 场景化终端安全威胁应对

2.1 接入方式

运营商主要以提供基础及增值服务为主营业务，早期受线下受理条件制约，导致终端接入方式多种多样。

（1）互联网场景：为满足代理商和经常变更受理地点的终端，以及员工外出期间可正常办公而应运而生的场景；

（2）办公网场景：除正常办公终端外，部分营业厅设置在运营商办公楼下，网络环境以办公网络连接成本较低；

（3）生产网场景：传统网络架构，便于营业终端与维护终端快速访问业务系统，有效降低网络延迟而长期存在。

为确保以上场景终端使用期间安全稳定，在有效安装统一防病毒软件的同时，安全防护管控区针对互联网只开放了通过零信任 SDP 客户端接入系统网络的场景，并且在终端连接期间实时监测终端统一防病毒软件进程，一旦发现进程异常或终端连接行为异常，将及时触发对该终端的阻断策略；针对内网区终端访问，将核心交换机流量引流至防病毒配套 NAC 管控设备，未安装统一防病毒软件终端将会被设备进行识别，并强制将终端访问页面指向统一防病毒软件下载界面。

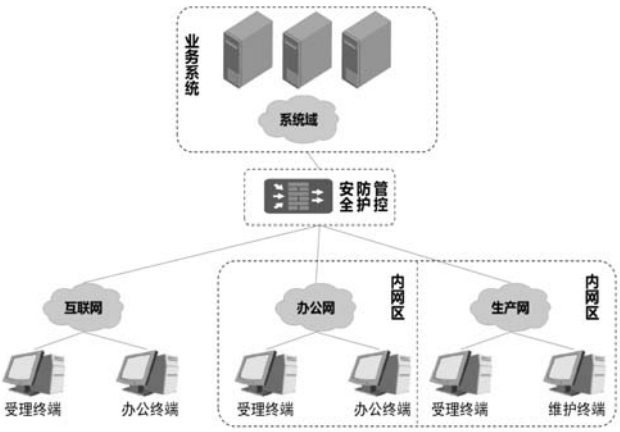

图 1 系统架构图

2.2 操作系统

由于终端类型多、品牌型号多、操作系统内核差异，针对不同的终端类型制定具有针对性的安装包和安装方式，包括 MAC 终端安装包、WINDOWS 安装包、服务器安装包、通用离线安装包等，同时结合现场安装、远程推送等安装方式满足不同终端的安装需求。

图 2 安全软件适配系统图

收稿日期：2023-03-20
作者简介：王浩（1982-），男，内蒙古呼和浩特人，硕士，工程师，主要研究方向：终端安全、信息安全、网络安全、数据安全等；智佩（1985-），女，内蒙古巴彦淖尔人，硕士，主要研究方向网络安全、信息安全等；云成龙（1993-），男，内蒙古巴彦淖尔人，本科，主要研究方向：网络安全、python、云计算、云安全等；郑晨（1994-），女，内蒙古赤峰人，本科，主要研究信息安全、数据安全、网络安全等。

2.3 风险软件

依托态势平台及云安全管控平台情报库判断终端访问系统触发的风险警报，结合统一终端防病毒软件管控平台获取到的终端安装列表研判风险目标软件，通过终端管控平台功能触发风险软件卸载或进程禁用策略，实现针对风险软件的及时处置。

2.4 实名认证

为确保每台接入终端在发现异常时及时进行处置，提供2种方式方便用户进行用户身份认证。同时为实现用户快速认证且用户信息准确，将终端防病毒平台数据与集团公司全国用户中心数据拉通，通过统一认证所使用的唯一用户名+密码的方式进行快速认证及关键信息自动补全，并将被认证终端实时拉取到该人员所在组织架构下，便于进一步安全管理。

图3 软件安全策略配置图

图4 软件安全策略配置图

图5 安全软件实名认证图

2.5 漏洞修复

由于操作系统使用的普遍性及广泛性，漏洞往往是最多的，也是最容易被利用的。同时使用人员的安全风险意识差异化，也导致终端风险容易被攻击人员利用，成为攻防战中一个重要的交火区。终端漏洞是否能够及时修复已成为防守方在攻防战中的一个重要指标。

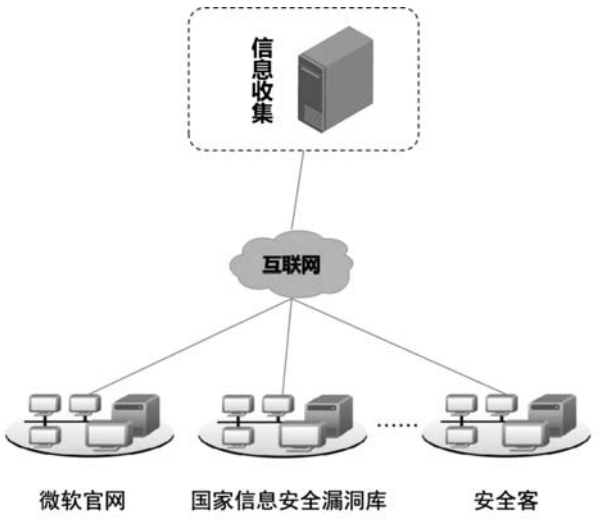

图6 漏洞修复架构图

图 7 漏洞自动修复图

为了有效提升修复效率，我们根据集团公司下发的漏洞预警内容进行风险排查，同时省内利用技术手段及时获取汇总各官方渠道有效的漏洞预警信息及修复指导方式。及时根据已获取的漏洞情报，利用防病毒管控平台对终端进行排查，并实现批量漏洞修复策略下发。

3 多位一体的终端安全实现

虽然在各场景下都有对应的解决方案，但是各自为战，实战效果并不理想。

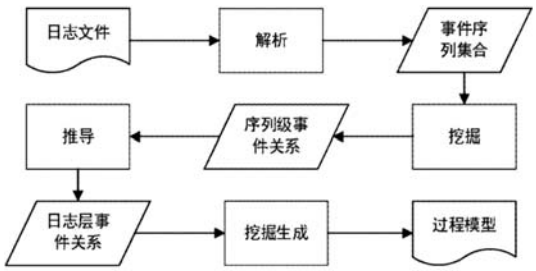

图 8 多位一体化终端安全

为解决该问题，我们以集团集约化终端管控能力为基础，利用终端管控平台可获取到的终端名、通信 IP 地址、真实 IP 地址、MAC 地址、使用人相关信息、终端漏洞信息、终端软件信息、在线状态、客户端版本、病毒库版本、病毒/木马查杀信息、操作系统版本、安全管控策略执行情况等相关数据，借助省内自研团队能力拉通态势感知、蜜罐防御、4A/堡垒机、零信任 SDP、内部网络认证、云安全管理等平台与终端地址、行为有关数据与终端管控平台数据进行海量数据智能分析，训练终端潜在风险模型，构建威胁链画像，并且对核心调度平台的功能进行拓展，制定个性化的防护策略，实现管控规则的优先级，动态调整与实时触发下达，以应对不同场景下的个性化策略聚合。

同时，通过收集汇总处置结果，持续扩充原始数据训练集，不断优化风险模型的精准度，进而与集团集约化安全指挥调度平台实现数据联动，使用调度工单下发、预警信息推送、设备实时封堵等多种方式，将整个发现、研判、处置过程形成闭环。

4 总结展望

4.1 存在不足

经过对整体终端安全防御体系的多位一体改造之后，虽然实战效果有所提升，但仍有部分场景策略需要专业人员参与分析、研判，个别事件仍需要通知下级管理员联合处置，特别是问题终端网络隔离处置后的取证溯源操作，仍无法实现自动调度。针对一些地域分布跨度大、现场处置人员能力不足的分支机构，实效性仍有提升空间。

4.2 后续计划

持续细化并补充场景化应对手段；提升研发能力；强化提升整体事件全流程风险处置闭环效率；进一步完善自动化处置能力，初步实现智能化运营。

参考文献：

[1] 奇安信行业安全研究中心著. 内生安全：新一代网络安全框架体系与实践[M].北京：人民邮电出版社,2021.4.
[2] 奇安信安服团队著.网络安全应急响应技术实战指南[M].北京：电子工业出版社,2020.11.
[3] 奇安信安服团队著. 红蓝攻防：构建实战化网络安全防御体系[M].北京：机械工业出版社,2022.6.

（上接第 161 页）

参考文献：

[1] 崔志诚,马胜.基于物联网技术的智慧工地[J].电子技术应用,2021,47(02):33-35+40.
[2] 吕基平,熊政华,邹容芳,等.智能视频分析技术在智慧工地安全监管中的应用研究[J].施工技术(中英文),2022,51(11):12-17.
[3] 陈刚,金树楼,张蔚,等.基于云技术的智慧化项目施工管理研究[J].施工技术,2021,50(06):68-70+79.
[4] 徐敬海,卜兰,杜东升,等.建筑物 BIM 与实景三维模型融合方法研究[J].建筑结构学报,2021,42(10):215-222.
[5] 阮小丽,钟建平,吴巨峰,等.基于 BIM 的寿春淮河大桥智慧场景信息管理系统[J].世界桥梁,2022,50(04):61-67.
[6] 邓院林,陈敏,王伟.基于数字孪生的大坝施工智慧管理平台[J].人民长江,2021,52(S2):302-304+311.
[7] 张颖.一种基于 BIM 建模的智慧家庭物品定位方法和系统[J].长江信息通信,2023(01):192-194.
[8] 王泽能,刘家庆,韦港荣,等.基于 BIM 与互联网技术相融合的施工管理模式运用研究[J].公路,2022,67(09):336-341.