部署有效的微分段来保护连接的设备

目前针对网络安全威胁的数量和严重性正在增加。助长这些攻击的主要动机包括泄露个人数据、商业秘密、有价值的研究数据以及其他可以在黑市上出售或交易的机密信息。索取系统赎金或破坏服务来玷污组织的声誉以获得竞争结果也可能是激励因素。除了高度组织化的网络犯罪框架之外，各国政府也加入了推进政治议程或实施网络恐怖主义的斗争。

除了悲观论调，事实仍然是物联网设备是网络攻击的主要目标。这些设备不同于常见的多功能用户设备(服务器、工作站和移动设备)，可以不断接收的操作系统更新和补丁，采用当前的端点安全技术进行增强，通常需要凭据才能连接到网络。

ORDR 解决方案文件

这些设备通常位于产品链的另一端，因为它们是使用精简操作系统为特定目的而构建的，并且无需用户干预或凭据即可连接到网络。物联网设备通常缺乏高级安全控制和保护，如反恶意软件或连续威胁监控。它们可能终身不打补丁，或者在较长的服务间隔后不经常打补丁。漏洞扫描这一简单行为可能会中断他们的操作。

意识到互联设备安全性缺陷的机构可以组织团队跟踪资产并监控其漏洞。这些团队可能会对新购买的设备设置安全标准，并试图强制实施定期服务间隔或维护窗口来修补暴露的设备，通常是在制造商或其他安全通知服务机构正式宣布易受攻击之后。尽职调查以减少暴露是至关重要的，但大多数机构承认这些措施不足以保护设备。

在这种情况下，分段可以为无法充分自我保护的设备提供所需的保护。分段是将相同类型或功能的设备放入同一物理或逻辑网段的概念。区段之间的通信是有限的，但通常对区段内的横向通信很少或没有限制。因此，即使采用了基本的分段，一个连接设备的危害也会影响或危害所有其他同类物联网设备。影响物联网设备的广泛攻击的例子包括 Mirai Botnet、WannaCry 和 NotPetya。

段内和段间的自由通信是物联网设备需要微分段的关键原因。微分段是将通信细分到细粒度级别的概念，理想情况下是适当操作和管理所需的最低限度的通信。分段通常有助于在更全局的级别上分离流量，例如，将来宾用户与内部网络分开，或者建立 PCI 区域。当一个网段内的用户和设备在组内有广泛的通信要求时，网络分段也是有益的。另一方面，物联网设备有非常规范的通信要求，并且适合微分段。

举个简单的例子，考虑一个连接到网络的传感器/控制器。这个设备需要 DHCP 和 DNS 来获取一个地址，以便在网络上找到它的“主”服务器并与之通信。它不需要和它的同伴交流。它可能需要从收集数据的监控站或远程站进行访问，以进行故障排除，但所有其他通信都应被视为外来的和未经授权的。这是微分段应用的理想用例。将有限的一组目标设备强制放入同一个网段是不切实际的，很可能是在数据中心或远程(例如，支持供应商)。将所有物联网传感器/控制器放在同一个网段中听起来也是一个好主意，但这样会使每个传感器/控制器都暴露给另一个(一个妥协，所有妥协)。通过微分段，通信可以仅限于物联网设备和业务的核心需求。

虽然细分甚至微细分可能是解决方案，但是在工具化方面，很少为行业提供工具，使组织能够高效和有效地实施细分。

为什么选择 ordr?

Ordr 系统控制引擎(SCE)提供了保护网络连接设备和系统设备所需的工具，无论是从“我有什么？它容易受到攻击吗？”以及“我如何实现微分段？”

首先，Ordr SCE 自动发现所有连接的设备和系统，并对其进行准确的分类和分组。Ordr SCE 通过一系列广泛的安全检查来验证每个设备的漏洞、威胁和风险级别。嵌入式安全分析将分类的端点与一套行业威胁情报源、网络漏洞数据库、ICSA-ICS-CERT 咨询、FDA 对医疗设备召回和警报的查找进行比较，并与制造商发布的漏洞数据的 MDS2 表格进行比较。主动安全监控检测弱密码和不可信证书的使用。结果被输入到您的安全监控系统，资产管理系统被更新，并且通过隔离或服务标签触发补救。

其次，Ordr SCE 监视每个设备的实际流量，并学习设备正常运行所需的最小流量的基线。与组织内其他 IP/VLAN 部门的通信以及与外部网络的通信很容易可视化。Ordr SCE 自动将这些外部和内部通信分为国外和国内通信，并通过 URL/IP 信誉分析将其与已知的恶意网站进行比较。流量不断受到监控，以发现主动威胁，如试图访问命令和控制以及其他不良行为。

这种自动化流程和威胁分析的结果是为每个设备和设备类别中的设备(例如，AllenBradley-PLC、Hospira-Symbiq 输注系统或 Axis-网络摄像机)建立规定的通信基线。一旦建立，Ordr SCE 将这些基线转换为微分段策略，这些策略可以手动或自动直接应用于您的网络和安全设备，或者通过您的 NAC 解决方案。

由于 Ordr SCE 不断验证所有通信，如果设备的行为超出预期和批准的基线，它能够提供警报。这使得能够有效、实时地检测危害，并对强制实施的策略进行审核，以回答以下问题:

- 我的连接设备是否按预期运行？
- 我的执法策略是否如预期的那样有效？

Ordr 系统控制引擎是同类解决方案中唯一一个跨所有领先供应商的有线交换机、无线控制器和接入点、防火墙和网络访问控制(NAC)解决方案提供微分段策略自动配置的解决方案。它具有高度的网络感知能力，因此它不仅了解要应用哪些策略，还了解在哪里以及如何应用它们。总之，Ordr SCE 可以快速确定网络上有哪些设备以及应该允许它们做什么，然后自动将这些知识转换成您的网络能够理解的语言，以提供有效的微分段。

基于 ACL 的微分段

在下面的简单示例中，Baxter 35700BAX 西格玛光谱输液泵已被 Ordr SCE 准确分类，并通过主动监控了解到允许的流量策略。由此生成的访问控制列表在网络入口点建立零信任边界，通信仅限于位于网络其他位置的特定监控和数据收集服务器。Ordr SCE 以目标系统(交换机、无线控制器/接入点、防火墙、NAC 策略服务器等)理解的“语言”自动生成 ACLs。)。

```
ip access-list extended CPN-Baxter-
35700BAX- SpectrumInfusionPump-in
  permit tcp any host 10.0.60.28
  permit tcp any host 10.0.60.29
  permit tcp any host 10.254.13.52
  permit udp any host 10.254.13.52
  permit tcp any host 192.168.101.181 eq 80
  permit icmp any any
  permit udp any eq bootpc any
  permit udp any eq bootps any
  deny ip any any

ip access-list extended CPN-Baxter-
35700BAX- SpectrumInfusionPump-out
  permit tcp host 10.0.60.28 any
  permit tcp host 10.0.60.29 any
  permit tcp host 10.254.13.52 any
  permit udp host 10.254.13.52 any
  permit tcp host 192.168.101.181 eq 80 any
  permit icmp any any
  permit udp any eq bootpc any
  permit udp any eq bootps any
  deny ip any any
```

基于标签的微分段

这是同一策略的一个示例，但用于基于组的实施策略设备或微分段服务。采用基于组的策略的典型解决方案包括防火墙和 NAC 策略服务器。同样，Ordr SCE 以目标系统能够理解的语言自动生成策略。根据组织的要求，可以使用相同或不同的实施方法将实施策略应用于单个目标或多个目标。

Source Group
Group Name:
Baxter-35700BAX-Spectrum Infusion Pump
Group Value: 257
IP Address List:
192.168.106.18, 192.168.106.19,
192.168.106.20, 192.168.106.21

Target Group 1
Group Value: 258
IP Address List: 10.0.60.28, 10.0.60.29
Target Group 2
Group Value: 260
IP Address List: 192.168.101.181
Group-based ACLs

- CPN-257-To-258:
  - permit tcp
- CPN-257-To-259:
  - permit tcp dst
  - permit udp
- CPN-257-To-260:
  - permit tcp dst eq 80
- CPN-260-To-257:
  - permit tcp src eq 80

ordr

take control.

info@ordr.net
www.ordr.net

加利福尼亚州圣克拉拉市奥
古斯丁大道 601 号 2445 室
邮编 95054