SOPHOS
Cybersecurity delivered.

事件响应指南

制定有效网络事件响应计划的 10 个步骤

“开始任何工作前，准备都是成功的关键。”

Alexander Graham Bell

避免网络攻击演变成全面破坏的最佳方法是什么?提前准备。

遇到外泄后,企业往往意识到如果制定过有效的事件响应计划,本可以避免大量成本、痛苦和中断。

本指南旨在帮助您定义网络安全事件响应计划框架,尽可能提高您战胜对手的机会。这些建议基于 Sophos Managed Detection and Response 和 Sophos Rapid Response 团队的真实经历,这两个团队在处理网络攻击方面有着数万小时的经验。

网络安全事件响应计划

有效事件响应计划有 10 个主要步骤。

事件响应计划框架

1. 确定主要干系人
2. 确定关键资产
3. 开展桌上模拟演练
4. 部署防护工具
5. 确保最大可见性
6. 实施访问控制
7. 投资调查工具
8. 制定响应措施
9. 开展意识培训
10. 雇佣托管安全服务

1. 确定主要干系人

正确计划潜在事件不仅仅是安全团队的职责。事实上，事件很可能影响企业的几乎每个部门，尤其是事件转变为完全规模的破坏后。要正确协调响应，您必须先确定应涉及的人。这通常包括高管、安全、IT、法务和公关代表。

应提前确定了解哪些人应该参会和参与企业规划做法。此外，需要确定沟通方法以确保快速响应。应考虑您的通常沟通渠道（如企业电子邮件）可能受到事件影响。

2.确定关键资产

要确定攻击范围和影响，您的企业首先需要确定最高优先级资产。确定最高优先级资产不仅帮助您确定保护战略，而且更容易确定攻击范围和影响。此外，提前确定这些内容后，您的事件响应团队将能够在攻击过程中专注最关键的资产，减少业务中断。

3.开展桌上模拟演练

事件响应和许多其他学科一样 – 练习才能做到完美。虽然难以完全复制您的团队将在潜在入侵时遇到的巨大压力，但练习将确保发生实际情况时更加紧密协调有效地响应。不仅开展桌上模拟演练很重要（通常是红色团队演练的一部分），包含以前确定的各个业务干系人的更广泛练习也很重要。

桌上模拟演练应测试您的企业对各种潜在事件响应场景的应对。每种场景还可能包含直接技术团队以外的干系人。您的企业应提前确定发现攻击时应通知的人，即使成功防御。

常见事件响应场景包括：

- **在网络中发现的活跃对手**：在此类场景中，响应团队确定攻击者如何渗透您的环境，采用的工具和技术，针对的目标，以及是否长期驻留很关键。这些信息将帮助确定消除攻击的正确行动过程。

  尽管明显地您应立刻将对手驱逐出环境，但一些安全团队选择等待和观察攻击者以获取重要情报，从而确定他们要实现的目标，和用于实现目标的方法。

- **确定数据外泄**：如果侦测到确实的数据外泄，您的团队应能够确定外泄内容和方式。然后这将提示正确响应，包括考虑合规性和监管政策影响的潜在需求，是否需要联系客户，以及潜在法律或执法参与。
- **确定勒索软件攻击**：如果加密关键数据和系统，您的团队应遵循计划尽快恢复此类损失。这应包括从备份还原系统的过程。要确保恢复上线后不会重复攻击，团队应调查对手的进入渠道是否已切断。此外，更广泛的组织应确定是否愿意在极端情况下支付赎金，如果愿意，愿意支付的金额。
- **高优先级系统受到威胁**：如果高优先级系统受到威胁，您的企业可能无法正常运营。除了事件响应计划中需要的所有措施，您的企业还需要考虑制定业务恢复计划，以确保此类场景下中断最短。

4.部署防护工具

处理事件的最佳方法是在第一时间保护。确保您的企业具有合适的端点、网络、服务器、云、移动和电子邮件保护。

5.确保您取得最大可见性

如果没法妥当了解攻击时发生情况，您的企业将难以正确应对。攻击发生前，IT 和安全团队应确保其能够了解攻击范围和影响，包括确定对手进入点和驻留点。正确可见性包括收集日志数据，重点关注端点和网络数据。由于许多攻击用数天或数周才能发现，您务必具备回溯数天或数周（甚至数月）的历史数据以便调查。此外，确保备份此类数据，这样可以在活跃攻击发生期间访问。

6.实施访问控制

攻击者可以利用脆弱的访问控制渗透您的企业防御，提升权限。定期确保您有合适控制以建立访问控制。这包括但不局限于部署多因素身份验证，将管理员权限限制在尽可能少的帐户（遵循最低权限原则），更改默认密码，减少需要监测的进入点。

7.投资调查工具

除了确保您有所需的可见性，您的企业还应投资在调查时提供所需环境脉络的工具。

一些用于事件响应的最常见工具包括端点侦测与响应 (EDR) 或扩展式侦测与响应 (XDR)，支持您在环境内追踪，发现入侵指标 (IOC) 和攻击指标 (IOA)。EDR 工具帮助分析师确定已经攻破的资源，反过来帮助确定攻击影响和范围。收集的数据越多 – 从端点和其他 – 调查时的可用环境越多。具备更广泛的可见性将允许您的团队不仅确定攻击者针对的目标，还可以确定如何进入环境，是否仍有能力再次进入。

除了 EDR 工具，先进安全团队还可能部署安全协作、自动化和响应 (SOAR) 解决方案，协助响应工作流。

8.制定响应措施

发现攻击只是整个过程的一部分。要正确响应攻击，IT 和安全团队需要确保其具备开展广泛补救措施的能力，中断和消除攻击者。响应措施包括但不局限于：

- 隔离受影响的主机
- 阻止恶意文件、进程和程序
- 阻止命令与控制 (C2) 和恶意网站活动
- 冻结受威胁的帐户，切断攻击者进入渠道
- 清理对手工件和工具
- 关闭攻击者利用的进入点和驻留区域（内部和第三方）
- 调整配置（威胁政策，在不受保护的设备上启用端点安全和 EDR，调整排除项等）
- 通过离线备份还原受影响的资产

9.开展意识培训

任何一个培训计划都无法 100% 有效防范确定的对手，但培训计划（如网络钓鱼意识）有助于降低您的风险等级，限制团队需要响应的提醒数量。利用工具模拟网络钓鱼攻击，可以让您的员工安全体验网络钓鱼（和潜在成为受害者），让受害者参与培训，辨识需要额外培训的高风险用户组。

10.雇佣托管式安全服务

许多企业不具备自行处理事件的能力。快速有效响应需要经验丰富的安全运营人员。要确保您正确响应，请考虑与外部资源合作，例如托管式侦测与响应 (MDR) 提供商。

MDR 提供商以托管服务形式提供 24/7 全天候威胁追踪、调查和事件响应。MDR 服务不仅帮助您的企业在事件变为破坏前响应事件，而且可以减少最初发生事件的可能性。MDR 服务正变得非常流行：据 Gartner* 表示，到 2025 年，50% 的企业将使用 MDR 服务（2019 年不到 5%）。

有时候事件后还采取数据鉴证事件响应 (DFIR) 服务，收集证据以支持法律或保险索赔。

总结

发生网络安全事件后，分秒必争。制定充分准备、理解到位的响应计划，让所有关键方能够立刻采取行动，将极大减少攻击对企业造成的影响。

Sophos 如何帮助

Sophos Managed Detection and Response (MDR) 服务

Sophos Managed Detection and Response (MDR) 托管式侦测与响应提供由专家团队以全托管服务形式带来的 24/7 全天候威胁追踪、侦测和响应能力。Sophos MDR 团队不仅仅能将攻击或可疑行为告知您，更代表您采取针对性操作，清除最复杂成熟的威胁。

Sophos MDR 威胁猎手和响应专家团队将：

- 主动追踪和验证潜在威胁与事件
- 利用所有可用信息确定威胁范围和严重程度
- 对有效威胁布置合适的业务环境
- 采取操作远程中断、隔离和清除威胁
- 提供解决反复出现事件根本原因的可行建议

了解更多 www.sophos.com/mdr

Sophos Rapid Response 服务

由事件应对专家团队提供的 Sophos Rapid Response，为企业提供识别并消除活跃威胁的快速协助。数小时内就位，大多数客户在 48 小时内得到分配。服务为现有 Sophos 客户和非 Sophos 客户提供。

Sophos Rapid Response 远程事件响应、威胁分析和威胁追踪团队：

- 快速采取措施识别、隔离和消除作用中的威胁
- 将对手挡在企业之外，避免进一步破坏您的资产
- 执行持续 24/7 全天候监测和应对，增强您的防护
- 建议实时预防措施，解决攻击根本原因
- 提供事件结束后的详细威胁总结，说明我们的调查情况

了解更多 www.sophos.com/rapidresponse

Sophos XDR

Sophos XDR 扩展式侦测与响应是业内唯一同步本机端点、服务器、防火墙、电子邮件、云和 M365 安全的 XDR 解决方案。凭借最丰富的数据集获取您企业环境的全盘视图和，方便专业 SOC 团队和 IT 管理员开展深度分析进行威胁侦测、调查和响应。

了解更多和免费试用 www.sophos.com/xdr

* Gartner，托管侦测和应对服务市场指南，2020 年 8 月 26 日，分析师：Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneiderd

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

20-10-30 WPZHCN (PS)