Acronis 安全服务

抵御现代网络威胁

数据是世界上最宝贵的资源。数据可以让组织实现自己的目标，也正是因为数据对组织如此重要，所以它成为了日益复杂且不断增加的网络攻击的目标。

为了应对这种局面，组织开始使用越来越多的安全解决方案。然而，如今的防病毒软件会错过 57% 的攻击。目前的技术并不足以防御网络攻击。因此，我们需要使用一种覆盖范围更广的网络安全保护方法。事实上，每次对 IT 基础架构进行更改（例如，部署新的业务应用程序或自带 (BYOD) 设备，或者使用云服务）时，都需要对安全计划进行审核，因为这可能会引入新的攻击途径。

由于企业需要遵守的法规越来越多，因此企业需要建立以隐私为中心的流程或进行强制性安全评估。但是，向所有员工灌输关键技能和习惯仍然是当务之急：据企业高管称，47% 的数据泄露是由人为错误造成的。

网络攻击越来越复杂，每天都会出现以前从未见过的恶意软件威胁。虽然无法阻止所有攻击，但组织可以及时检测出这些攻击，将危害和潜在损失降到最低，并采取适当的措施来确保未来不会出现同样的攻击。

ACRONIS SECURITY SERVICES

多年来，Acronis 一直提供业内一流的网络安全保护技术。凭借 Acronis Security Services，Acronis 提供了一种覆盖范围更广的网络安全保护方法。现在，我们的单一安全点产品涵盖了技术、人员和流程，可以解决各种规模组织当前面临的安全性、可访问性、隐私性、真实性和可靠性挑战。

ACRONIS SECURITY SERVICES 的优势

安全评估

- 改善组织的安全状况
- 最大限度地减少补救成本
- 满足行业法规要求
- 使网络安全策略和路线图与业务目标保持一致
- 明确 IT 投资决策
- 利用补救计划来降低风险

安全意识

- 提高员工应对网络攻击的准备程度
- 降低人为错误的风险
- 确保遵守法规和既定流程
- 减少与安全相关的支持呼叫量

事件响应

- 确保业务连续性
- 限制安全漏洞所造成的损害
- 降低因网络攻击而导致的财务和声誉损失
- 最大程度地减少系统停机时间

ACRONIS SECURITY ASSESSMENT SERVICE

迅速应对不断增长的监管合规性挑战和日益增多的数字威胁。通过审核安全计划、IT 基础架构以及防护和检测控制方法，识别安全缺口和漏洞。寻求网络安全专家的建议，彻底消除数据中的所有攻击途径。

您将获得以下功能：

- 风险评估 – 基于行业标准（例如 NIST 和 ISO/IEC 27001）对企业当前的安全状况进行评估。评估您的网络安全成熟度和与第三方相关的风险。重点评估可能会导致漏洞的安全缺口。
- 漏洞扫描 – 主动识别网络、应用程序和终端中的已知漏洞，限制 IT 环境的攻击面，从而实现安全的软件开发生命周期。
- 渗透测试 – 识别网络、移动设备、Web 和应用程序的攻击途径，我们的网络安全专家演示了攻击是如何发起的以及它们是怎样试图利用漏洞和绕过安全控制机制来获取敏感数据。
- 社会工程 – 评估员工是否准备好应对通过如下方法发起的网络攻击：通过电子邮件、电话、媒体滴灌式营销或物理访问来利用人工操作的网络钓鱼。
- 补救 – 获取执行摘要、详细报告（包括合规性报告）以及可根据评估方法来解决问题和降低风险的补救计划。

ACRONIS 安全意识培训

提高员工的工作效率，缓解包括社会工程入侵在内的各种风险，同时通过由顶级网络安全专家讲授且专为您的业务需求量身定制的安全意识培训，缩短因“读书”而耽搁的时间。

您将获得以下功能：

- 基于角色的培训 – 为普通员工、IT 人员、开发人员和高管提供基础级到专家级的培训，包括合规性培训以及旨在帮他们为认证（如 CISSP、CEH、CCSK 等）做好准备的培训模块。
- 多种交付选项 – 利用 700 多个专为企业和用户量身定制的在线模块或现场培训课程。

ACRONIS INCIDENT RESPONSE SERVICES

Acronis 的网络安全分析师和漏洞调查员会在安全事件发生时立即做出响应。您可以通过全面评估环境和数据泄露的根本原因来进行深入分析。提供了详细的补救计划，确保采取适当的措施来进行恢复并帮助贵公司管理法规要求和任何声誉损失。

您将获得以下功能：

- 识别受损资产 – 查明受损资源后，查找并分析可能受损的系统，以了解数据泄露的整个范围。
- 业务连续性 – 隔离威胁以防扩散。
- 取证 – 分析根本原因并收集和保存证据（例如使用 HDD 镜像、网络跟踪和内存转储），以便进行后续调查和出席庭审。
- 补救报告 – 获取有关攻击的详细报告，包括来源、主机、应用程序、恶意软件分析和风险概况。我们的专家将规划并执行详细的路线图，以确保事件得到全面补救。该报告中还提供了防止今后出现类似攻击的建议步骤。
- 经济高效 – 每年将未使用的事件响应服务时间转换为其他服务。