GlobalSign如何保护其环境

WHITE PAPER

在GlobalSign，我们的服务和客户数据的安全是我们的首要任务。本白皮书概述了我们为确保环境的完整性、机密性和可用性而实施的实践和控制。.

GlobalSign的信息安全方法

作为运营时间最长、规模最大的公共可信证书颁发机构之一，GlobalSign一直致力于提供高安全性的公钥基础设施(PKI)解决方案。信息安全是董事会议程上的一个重要议题，高级管理人员在制定和确保实施安全政策时，会大量参与，以确保我们提供的服务的机密性、完整性和可用性。

我们有一个专门的全球安全和合规团队，负责运营我们的信息安全管理系统。该系统以ISO27001标准及“网络信任”(WebTrust)原则及准则为基础，而“网络信任”原则及准则是全球认可的运作公开受信任核证机关的架构。我们的管理系统涵盖资讯安全的所有常见范畴，包括但不限于以下:

- 信息安全治理与战略
- 持续的威胁分析、风险评估和风险管理
- 人员意识和诚信
- 物理和环境安全
- 安全操作和监控
- 访问管理
- 系统开发及维护
- 事件管理和违规响应
- 业务连续性和灾难恢复

除了在公司范围内定义和分发必要的政策外，我们还部署了程序和技术安全控制，以保护我们的PKI服务:

- 在我们所有的应用程序和系统上进行多因素身份验证
- 具有强过滤控制的多层网络
- 高级恶意软件检测控件
- 关键密钥材料的气隙，如根CA密钥
- 军事级别的物理访问障碍限制访问我们的数据中心
- 我们办公室和数据中心网络中的入侵检测和防御系统
- 全磁盘加密我们的IT设备
- 重复脆弱性评估(季度)和渗透测试(每年)
- 审查关键应用程序的源代码
- 响应式补丁管理

除了追求我们自身环境的最高安全性，GlobalSign是最关键的、标准驱动的机构和组织的长期成员，包括认证机构(CA) /浏览器论坛、认证机构安全理事会(CASC)和工业互联网联盟(IIC)，并符合北美能源标准委员会(NAESB)，国家标准与技术研究所(NIST)和国家网络安全卓越中心(NCCoE)。

员工意识和信任度

随着信息安全威胁的迅速发展，我们为员工提供的信息、指导和培训也必须迅速发展。确保对数据隐私和信息安全威胁的意识是一个持续的过程。这不仅体现在对员工的专业培训中，也体现在推动整个组织内意识的众多其他活动中。为了确保时刻保持警惕，我们的员工经常会接受网络钓鱼测试和其他社会工程攻击的模拟。

GlobalSign还验证了在组织内履行关键职能的员工的可信性。员工验证包括技能，教育程度，以前的工作，专业推荐和犯罪背景调查(如果在当地管辖范围内允许)。

业务连续性和灾难恢复

系统的发展和维护我们的环境已经建立了弹性的方式，能够承受重大的环境灾害，有组织或蓄意的破坏，以及公用事业和服务的损失。我们的业务连续性管理和灾难恢复方法基于ISO22301标准，并包含以下内容:

- 业务影响分析以量化业务影响并确定适当的连续性策略
- 服务恢复时间和点目标与客户所需的关键性能指标(KPI)保持一致
- 紧急沟通和通知程序，以通知我们的客户和其他信赖方
- 连续的现场和场外的信息备份
- 每年重新评估业务连续性战略和业务连续性计划
- 定期测试业务连续性计划和恢复程序，以确保能够满足恢复时间和点目标
- 针对CA特有的灾难(如密钥泄露)，专门的恢复过程和计划

为了确保高可用性，我们在世界各地都有数据中心。如果其中一个遇到了自然灾害或人为事件，那么操作将在定义的恢复时间和恢复点目标内故障转移到另一个位置。此外，这些数据中心以及发布设施都受到标准预防措施的约束，如多检测系统、多连接线和24x7x365监测。这意味着我们将在任何此类事件发生或即将发生的最早机会得到警报，以使我们以最适当和最有效的方式作出反应。

数据保密

GlobalSign尊重客户的隐私权。我们的隐私政策符合欧盟通用数据保护条例(GDPR)，并适用于整个GlobalSign网络以及为发布GlobalSign产品和服务系列而收集的所有信息:

- 我们采用适当的物理、技术和组织安全措施来保护个人资料。
- 我们要求所有可能提交的个人资料当事人明确同意。
- 除非当事人提交，否则我们不会收集个人资料。
- 我们使用主题提交的数据仅用于我们的隐私政策中定义的目的。
- 我们会在使用后安全处理个人资料。
- 受试者有权查阅GlobalSign持有的个人资料，并检查其一致性。
- 如果发现我们的记录有错误，受试者有权远程更正数据。

合规性和审计

为了评估和证明合规性，GlobalSign的环境将接受多次内部和外部审计，包括:

- 独立的年度ISAE3000 SOC3 II类审计针对业界领先的认证机构框架，我们从2001年起就通过了该框架的认证——行业中第二长的认证:认证机构的WebTrust、扩展验证、SSL基线要求、代码签名和EV代码签名。
- 基于eIDAS法规和ETSI标准，对欧洲合格的信托服务提供商进行两年一次的eIDAS符合性评估
- 漏洞扫描研究主要集中在网络过滤、配置管理、补丁管理、应用安全和基础设施安全等方面
- 持续监测控制的有效性，以确保合规性和安全控制的有效设计和实施
- 根据ISO27001:2013(信息安全管理体系)和ISO22301:2012(业务连续性管理体系)进行年度独立评估。GlobalSign是第一家同时通过ISO27001和ISO22301认证的全球CA。

所有评估报告均可于以下网址公开查阅 https://www.globalsign.cn/repository/

关于 GlobalSign

GlobalSign是全球领先的可信身份和安全解决方案提供商，使全球的企业、大型企业、云服务提供商和物联网创新者能够确保在线通信的安全，管理数百万已验证的数字身份以及自动化认证和加密。其大规模公钥基础设施(PKI)和身份解决方案支持数以亿计的服务、设备、人和物组成的万物互联(IoE)。

CN: +86 021-60952260 www.globalsign.cn