当员工转换岗位时

数字资产的最佳实践

cscdbs.com/cn

前言

在管理公司的域名、域名系统 (DNS) 和数字证书等数字资产时，所有管理员均需关注这部分内容：有权访问资产组合的人员，及其详细信息列于何处。随着安全事件的增加以及数据和隐私保护法律的日益严格，追踪使用中的用户证书和个人信息比以往任何时候都更显重要，从而确保定期更新数据以避免安全和合规风险。

当相关员工离职或转换岗位时，CSC 建议审计所有供应商门户、域名和其他资产，以确保立即更新所有产品和服务的用户信息。

1

审查

我们建议定期审查所有供应商门户的用户和访问级别。由于容易发生人为错误，因此人是任何组织中最薄弱的环节，而良好的用户管理政策对于保持高水平的安全性至关重要。

定期审计您的用户（至少每 90 天审计一次）。
CSC Security Center℠ 可帮助您轻松查看任何授权用户并请求更新，还可以设置添加新用户通知。

每年至少审查一次您的 WHOIS 组合信息。
遵循 WHOIS 数据提醒政策 (WDRP)，确保您的 WHOIS 信息为准确的最新信息。

审查您的社交媒体帐户。

请记住要忘记用户。
被遗忘权——也称为“删除权”——是指欧盟公民有要求删除其个人数据的权力。出于安全风险考虑以及根据隐私和数据保护法规的规定，建议在用户离职时，将其个人身份信息从公开的 WHOIS 中删除。CSC 可以帮助您审计员工拥有访问权的所有工具和服务，并确保完全删除旧联系人，从而帮助您降低风险。

2

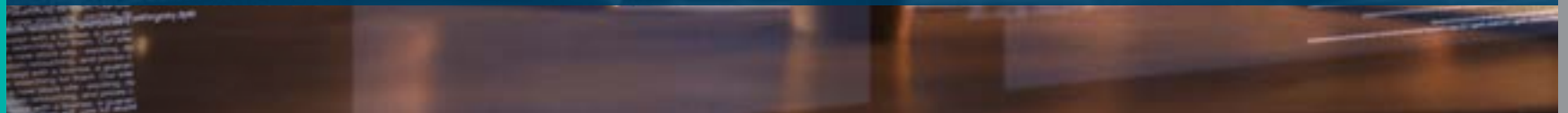
替代

在每个组织中，用户通常被分配多个超出常规用户门户访问权的职责。因此，必须评估该人执行的额外职能，并确保找到合适的替代人员。

员工是否：

- 被列为续约联系人？
- 被列为特殊通知联系人？
- 列入域名 WHOIS 联系人信息中？
- 负责接收和处理组织的发票？
- 与任何安全服务相关？

在确定了所有这些领域之后，您就可以轻松确定谁应替换该联系人并相应地更新访问权信息。



3

停用

首先，您务必要确保及时停用用户证书。单点登录或联合 ID 设置使您可以直接控制用户证书，从而使您拥有可以快速将其禁用的访问权。

- CSCDomainManager℠
- CSC Security Center
- 品牌保护门户
- DNS 和数字证书门户

请务必追踪员工拥有访问权的所有第三方工具，并确保对访问权限进行相应更新。

将所有组织变更情况告知您的供应商合作伙伴。CSC 很乐意审计现有的访问权限，并确保在所有可用平台上及时完成更新。
我们的使命是为您提供帮助。

4

最佳实践

- 仅给必要用户提供供应商帐户访问权。确保供应商门户允许实施额外安全措施，例如双重验证和 IP 验证。
- 考虑单点登录以控制用户证书。
- 尽可能整合供应商。减少门户和供应商帐户就意味着减少了需要管理的证书。
- 定期审计您的用户（至少每 90 天审计一次）。CSC Security Center℠ 可帮助您轻松查看任何授权用户并请求更新，还可以设置添加新用户通知。
- 在供应商门户中停用所有联系人之前，请确保您已找到合适的替代人员。

cscdbs.com/cn @cscdbs CSC Digital Brand Services

DBS03302021