

安全与网络风险

Dr Alexander Ressos, TEP

Attorney-at-Law (Switzerland), Solicitor (Hong Kong),

Solicitor (England & Wales)

高价值企业和富裕人士集中在一个小州，带来了安全风险。近年来，针对瑞士企业和政府机构的网络攻击有所增加。2023 年，一家联邦行政部门 IT 供应商遭受攻击，导致联邦机构的敏感数据外泄。¹大宗商品贸易商、加密货币企业和财富管理人持有有价值的数据和资产，因而成为犯罪分子和国家行为者的诱人目标。加密行业已遭受多起黑客攻击，价值数百万的代币被盗。

州政府和企业已在网络安全方面进行投资，联邦也设立了联邦网络安全办公室（BACS）。²对富裕居民及其家人的保护是另一项关切，由私人安保公司和警方负责。这些风险不太可能改变大多数企业的选址决定，但会增加在该州经营的成本。一旦发生影响金融或大宗商品基础设施的重大网络事件，该州在安全与稳定方面的声誉可能受损。

1 注释

1. 联邦委员会，新闻稿 “Hackerangriff auf Firma Xplain: Bundesrat mandatiert politisch-strategischen Krisenstab ‘Datenabfluss’”，2023 年 6 月 28 日，[admin.ch](https://www.admin.ch/gov/de/press/pr/2023/2023-06-28-01)：针对 IT 服务提供商 Xplain 的勒索软件攻击影响了联邦行政部门的数据；联邦网络安全办公室（BACS），新闻稿 “Hackerangriff auf Firma Xplain: Bericht ... zur

Datenanalyse publiziert”（2024 年），ncsc.admin.ch：黑客组织“Play”于 2023 年 6 月 14 日在暗网上公布了数据，约 130 万个对象，其中约 6.5 万个与联邦行政部门相关。

2. 联邦委员会，新闻稿“Meldepflicht für Cyberangriffe auf kritische Infrastrukturen”，2025 年 3 月 7 日，admin.ch：自 2025 年 4 月 1 日起，关键基础设施运营者须在 24 小时内向联邦网络安全办公室（BACS）报告网络攻击。BACS 自 2024 年 1 月 1 日起作为国家网络安全中心（NCSC）的继任机构开始运作（联邦委员会 2022 年 12 月 2 日决定；de.wikipedia.org，“Bundesamt für Cybersicherheit”）。

仅供一般参考。本文不构成法律或税务意见，不能替代针对个案的专业意见，亦不建立律师与客户关系。本文反映截至 2026 年 9 月的法律状况。

在线版本：cn.helveticaregister.com/zug-security-and-cyber-risks