信任宪章

迈向安全的数字世界

Charter
of Trust

信任宪章

迈向安全的数字世界

数字世界正在改变一切。人工智能和大数据分析正在彻底改变我们做决定的方式；数十亿台设备正在通过物联网进行连接，并在全新的深度和规模上进行交互。

尽管这些进步正在改善我们的生活和经济，**但遭受恶意网络攻击的风险也随之急剧增加。**对控制我们的家居、医院、工厂、电网和几乎所有基础设施的系统保护不当，可能会引发毁灭性的后果。**公众利益和经济价值需要得到保护，避免网络和混合威胁的影响。**

网络信息安全不仅仅是实行必须的安全措施，它更是数字经济成功的关键所在。必须让公众和各类组织能够相信自己的数字技术是安全可靠的，否则他们将不会接受数字化转型。**数字化和网络信息安全必须携手并进。**

为了适应市场的不断发展和应对犯罪分子的威胁，**企业和政府必须联合起来，采取果断行动。这意味着需要尽一切努力：**

- 保护个人和企业的数据和资产；
- 防止针对人员、企业和基础设施的损害；
- 为互联的数字化世界建立可靠的信任基础。

对数字化和网络信息安全的全面影响进行应对并构建一个整体的信任基础，只靠一家公司或实体是无法实现的；必须依靠各级力量的密切合作。**在本宪章中，签署合作伙伴勾勒了我们认为在社会、政界、商业伙伴和客户之间建立新的信任章程所必需的关键原则。**

AES　Atos　IBM　SIEMENS

AIRBUS　DAIMLER　Munich Security Conference MSC Münchner Sicherheitskonferenz　SGS

Allianz　enel　NXP　T

信任宪章的原则

1 网络和信息安全的所有权

政府指定具体的主管部门，企业设立首席信息安全官（CISO），将网络信息安全的责任定位于最高的政府和商业级别。在整个组织中制定明确的措施和目标，并树立正确的意识——“人人有责”。

2 整个数字供应链的责任

公司和（如有必要）政府必须制定基于风险的策略，确保所有物联网层面都能得到充分保护，并有明确规定的强制性要求。通过在以下方面设置安全基准确保机密性、真实性、完整性和可用性：

- **身份和访问管理：**连接的设备必须有安全标识和保护措施，只允许授权的用户和设备使用它们。
- **加密：**在必要的情况下，处于连接状态的设备必须确保数据存储和传输目的的机密性。
- **持续保护：**公司必须通过一个安全更新机制为其产品、系统和服务在合理的生命周期内提供更新、升级和补丁。

3 默认安全性

采用恰当级别的安全和数据保护，并确保将其预先配置到产品、功能、流程、技术、操作、架构和业务模型的设计中。

4 以用户为中心

作为一个可信的合作伙伴，在整个合理的生命周期中，根据客户的网络信息安全需求、影响和风险，提供产品、系统和服务以及指导。

5 创新和共同创造

结合领域专业知识，深化企业与网络信息安全需求和策略制定者之间的共识，不断创新并应用网络信息安全举措以应对新威胁；推动和鼓励公私合作伙伴关系。

6 教育

在学校课程中加入专门的网络信息安全课程——如大学学位课程、专业教育和培训——以引导未来所需的技能和职业需求的转变。

7 关键基础设施和解决方案的认证

企业和（如有必要）政府为关键基础设施和关键物联网解决方案建立强制性的独立第三方认证（基于面向未来的定义，特别是涉及人身安全的部分）。

8 透明度和响应

加入行业网络信息安全社区，分享新的见解、事件信息等；通报当前安全实践尚无法处置、涉及到关键基础设施的事件。

9 监管框架

促进监管和标准化的多边合作，为世界贸易组织(WTO)在全球范围创造一个公平的竞争环境；将网络信息安全策略纳入自由贸易协定(FTAs)。

10 联合行动

推动包括所有利益相关者在内的联合行动，以便在数字世界的各个部分及时地实施上述原则。


AES
AIRBUS
Allianz
AtoS
DAIMLER
enel
IBM
Munich Security Conference msc Münchner Sicherheitskonferenz
NXP
SGS
SIEMENS
T