网络安全 FCIS 2023 创新大会

AI在企业内部的机遇与挑战

巴斯夫中国数字化中心

Holger Petersen

FREEBUF

- **计算机科学博士**，密码学专业
- **30 年**信息/网络安全经验
- 在巴斯夫工作**20 年**，负责安全架构和战略
- 网络安全与安全风险管理**高级专家**
- 自 2022 年起担任**中国网络安全团队负责人**

扫描二维码，关注
巴斯夫中国数字化中心

BASF - We create Chemistry | 巴斯夫集团简介

- 我们将经济成功、社会责任和环境保护融为一体
- 我们的产品几乎应用于所有行业，分为**6 个**产品组合
- 2022 年销售额：**873 亿欧元**，2022 年未计特殊项目的息税前利润：**69 亿欧元**
- **111，481 名员工***为客户的成功做出贡献
- 公司遍布**90 多个**国家
- **6 个**一体化生产基地和**239 个**其他生产基地
- **~82,000 个**客户来自世界上大多数国家的不同行业

* 截至 2022 年 12 月 31 日的雇员人数

巴斯夫在中国

深耕中国**138 年** - 自 1885 年起

26 家全资子公司

10 家合资企业

30 个生产基地

11，411 名员工*

2022 年销售额**约 116 亿欧元****

2005：南京 扬子石化-巴斯夫有限责任公司

2020：南京 中国数字化中心

2012：上海 创新园（研发）

2015：巴斯夫聚氨酯（重庆）有限公司

2021：长沙 巴斯夫杉杉电池材料有限公司

2022：巴斯夫湛江一体化基地（首套装置）

* 截至 2022 年 12 月 31 日的雇员人数
** 截至 2022 年 12 月 31 日按客户所在地分列的情况

BASF
We create chemistry

巴斯夫中国数字化中心（南京）介绍

数字化是巴斯夫的优先事项，并支持巴斯夫企业战略的目标

为巴斯夫的愿景：成为**最领先的数字**化工企业贡献力量

运用独特的**中国技术生态系统**

依托中国**数字人才创建全球**的足迹

实现业务需求的数字化，以便**在中国市场竞争和发展**

构建**合规的**数字解决方案，保护企业以**安全的方式**运行数字解决方案

我们是谁：超过百人的数字化团队

我们的位置：南京市中心

我们的工作方式：敏捷、精益、学习心态

我们为什么在这里：靠近客户-"在中国为中国"

BASF
We create chemistry

人工智能

"可能是自互联网发明以来最具颠覆性的技术"

引自:Roger Halbheer - 微软首席安全顾问

人工智能 - 机遇与挑战

人工智能为企业带来了新机遇，也带来了新风险

人工智能带来的新机遇

1. **提高效率**
   例如-田间试验的自动图像分析（农产品事业部）
2. **改善客户服务**
   例如-面向客户的产品和文件搜索解决方案（个护事业部）和虚拟医药助理（营养品及保健）
3. **更好的决策**
   例如-信贷管理流程自动化（预测和智能信贷优化器）
4. **节约成本**
   例如-更复杂的流程自动化（RPA 与人工智能的结合）
5. **竞争优势**
   例如-预测分子气味和模拟客户苯乙烯工厂的行为

网络安全

人工智能带来的新风险

人工智能 - 风险概述

随着人工智能的兴起，新的风险不断涌现，威胁格局也随之改变

人工智能网络安全 风险

攻击的数量和复杂程度以及新的攻击载体不断增加

新的威胁行为者，
因为攻击操作简单

类人社交攻击
（如网络钓鱼）

人工智能作为攻击面
（如模型盗窃）

虚假信息，
如可信度、幻觉

绕过现有**安全措施**

数据盗窃

其他人工智能 风险

必须确保符合法律要求

数据保护：

- 不恰当的个人数据管理
- 第三方个人数据的违规处理

知识产权：

- 知识产权保护不足

法律

- 违反合同，如侵犯版权
- 违反法律法规

其他

- 无法提供人工智能服务
- 过度依赖人工智能会导致错误或无意义的反应或不合理的反应
- 违反道德标准

资料来源Gartner (2023) | ENISA (2023) | Team8 (2023)

人工智能 - 网络安全风险 (1/3)

网络安全需要与时俱进，以适应不断变化的网络风险形势

Mandiant: 攻击者对生成式人工智能感兴趣，但使用仍然有限

新的威胁行为者

由于以前需要花费大量时间的任务变得简单易行，新的威胁参与者将不断涌现，攻击的复杂程度将不断提高，总体门槛将有所下降。→ 成熟攻击的频率预计会提高

Theverve.com：Meta 强大的人工智能语言模型 LLaMA 已在网上泄露

LLaMA

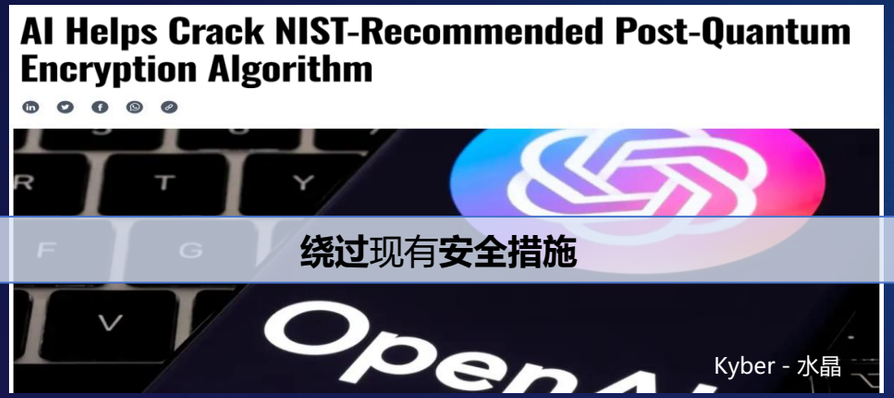
Meta

作为攻击面的人工智能

通过对抗性攻击，攻击者可以操纵人工智能模型，获得未经授权的访问权，复制或外流 LLM 模型，导致人工智能决策受损，造成经济损失，或可能获取敏感数据。

人工智能 - 网络安全风险 (2/3)

网络安全需要与时俱进，以适应不断变化的网络风险形势



绕过现有安全措施

在计算机上安装微软Co-Pilot等人工智能解决方案，可以让人工智能系统绕过邮件加密等程序，完全访问邮件，从而增加数据泄漏的风险。

数据盗窃

人工智能驱动的恶意软件可能会从网络行为中学习，并以不显眼的小爆发形式外泄机密数据，以躲避检测

人工智能 - 网络安全风险 (3/3)

网络安全需要与时俱进，以适应不断变化的网络风险形势

来源：Wired, 30.10.2023有线电视，2023 年 10 月 30 日

虚假信息

人工智能系统生成不真实的信息（假新闻）--由于质量上乘，看起来像是真实的，这将对社会或经济产生影响

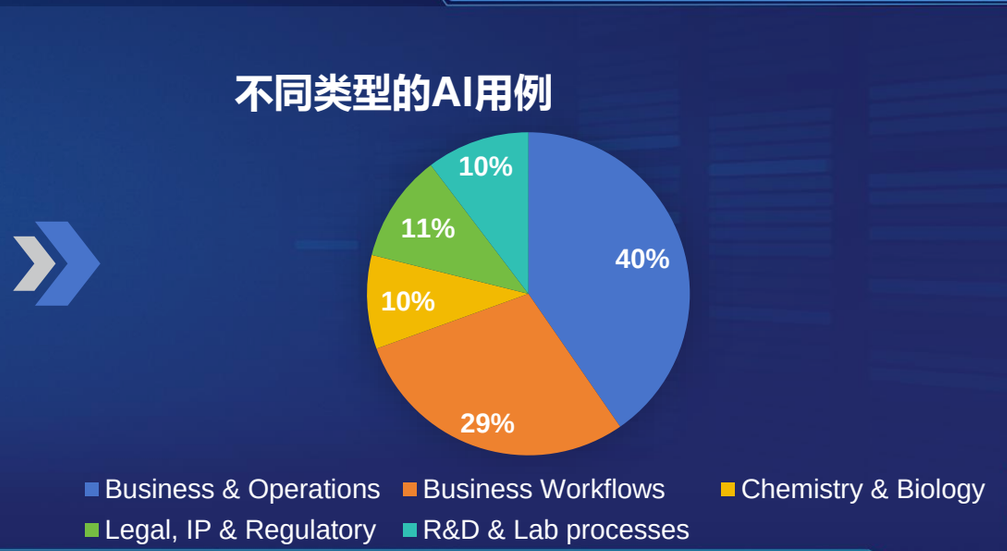
类人社交攻击

攻击者利用人工智能基于录音模仿人声（例如董事会成员的声音）进行冒充，目的是欺骗个人，让他们误以为自己是在与可信赖的人互动

巴斯夫内部生成式 AI 的用例收集

巴斯夫的数百个想法在实施前必须进行风险评估

技术原型
代理、工具和应用程序接口（API），例如将现有服务与LLM连接起来
聊天机器人，例如用于对话或支持用户导航的前端软件
与数据聊天，例如与结构化和非结构化数据互动
文本转换，例如文本摘要或将文本转换为本体
语音，例如在实验室或客户服务环境中使用自动语音理解或语音创建功能
分子化学，如分析小分子或大化学分子的性质
图像，例如理解图像并将其转换为文本；根据文本描述创建图像
代码，如创建、分析和转换程序代码



巴斯夫针对人工智能方案的风险评估方法

我们制定了一套方法，以实现风险透明并确保治理

- 建立了一致的**风险评估模板**
- 模板将用于**LLM 使用和基于人工智能的企业搜索**评估
- **每个人工智能用例都将**根据风险评估模板进行评估
- **确保**风险暴露的**透明度**为我们的业务提供基于人工智能的解决方案

制定评估人工智能风险的统一方法

风险评估

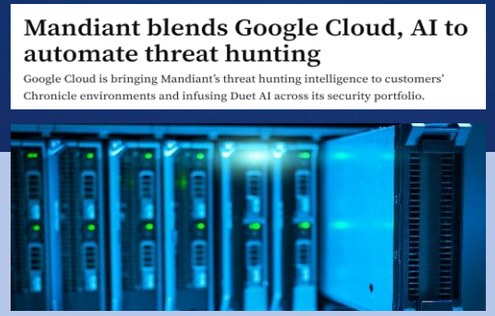
数据保护 ***知识产权*** ***网络安全*** ***法律***

成果

风险评级 + **缓解措施** + **风险接受度与残余风险**

执行所需的治理和控制职能

对于大型组织来说，拥抱人工智能作为技术进步至关重要



来源：《福布斯来源：《福布斯

下一代网络防御在 BASF 的使用场景

人工智能让网络防御更上一层楼

威胁检测
自动识别异常和样本

行为分析
用户活动（UEBA）

自动响应
响应措施自动化，例如阻止可疑的 IP 地址

预测分析
分析数据以预测未来的威胁，如新的恶意软件

风险评估
总体风险态势分析，例如通过识别和评估薄弱环节

我们为现代 SOC 提供的优势

- 增强防御能力
- 更有效
- 持续监测
- 增强上下文洞察力
- 高级自动化

- 瓦解攻击者
- 省力省钱
- 扩大覆盖范围，提高质量
- 端到端防御
- 加快响应

巴斯夫观点：AI 在网络安全中的风险和应对

保持竞争优势，获得人工智能的优势并抵御风险

风险

1. 使用不准确/错误的信息（如幻觉）
2. 使用不受信任的公开人工智能解决方案
3. 缺乏管理和实施缺乏适当的安全控制

对策

1. 人工智能宣传和用户培训
2. 一套标准的由可信供应商提供的人工智能解决方案
3. 加强数据分类和访问控制措施

巴斯夫中国网络安全团队

FREEBUF | FCIS 2023

[1]SME = 自我管理环境
[2]BCSO = 巴斯夫网络安全办公室
[3]IPO = 信息保护官

- 网络安全、治理与合规
- 网络安全风险管理
- 网络安全高级架构师
- AI 网络安全架构AI方向
- 网络安全架构
- 网络安全专家（审计&红队）
- 网络安全信息和漏洞修复管理
- 网络安全数据泄露管理
- 网络安全漏洞管理
- 网络安全专家（下属公司安全合规）
- 网络安全威胁情报
- 网络安全事件响应
- 网络安全分析师
- 网络安全数字取证
- 网络安全事件管理
- 巴斯夫网络安全服务台
- 信息保护官（员工安全意识提升）
- 网络安全经理

加入我们的团队！

欲了解更多信息、
关注我们的微信公众号
或访问我们的 **A20展台**。

BASF
We create chemistry

网络安全
FCIS 2023创新大会

谢　　谢

FREEBUF

BASF
We create chemistry


网络安全
FCIS 2023创新大会
FREEBUF
BASF
We create chemistry