



Copyright Info:

Bilder in dieser Präsentation wurden automatisch durch PowerPoint aus Onlinequellen unter der Creative Commons Lizenz eingefügt.

Einige Komponenten wie das AWSK.IT Logo und Fotos unterliegen dem Copyright.

Diese Unterlagen sind nur als Handout für die Teilnehmer:innen des Hydro+Vortrags gedacht und nicht zur Weiterverteilung und Verwendung freigegeben.

Bei Bedarf oder Anfragen wenden Sie sich gerne an AWSK.IT.

Informazioni sul copyright:

Le immagini presenti in questa presentazione sono state inserite automaticamente da PowerPoint da fonti online sotto licenza Creative Commons.

Alcuni componenti, come il logo AWSK.IT e le foto, sono soggetti a copyright.

Questi documenti sono intesi solo come dispensa per i partecipanti alla presentazione Hydro+ e non sono rilasciati per ulteriori distribuzioni e utilizzi.

Per qualsiasi domanda o esigenza, contattare AWSK.IT.



DER REFERENT

Alan Hofer

IT-Infrastruktur und IT-Sicherheit seit über **16 Jahren**

AWSK.IT
Beratung von Unternehmen und IT-Abteilungen im Bereich Cybersecurity

Sensibilisierungs-Kurse für Mitarbeiter:innen
um Hackerangriffe vorzubeugen

Ziel des Vortrags
Aufzeigen der Herausforderungen und Lösungsansätze im
Bereich Cybersecurity im Kontext von KI



2

Il relatore

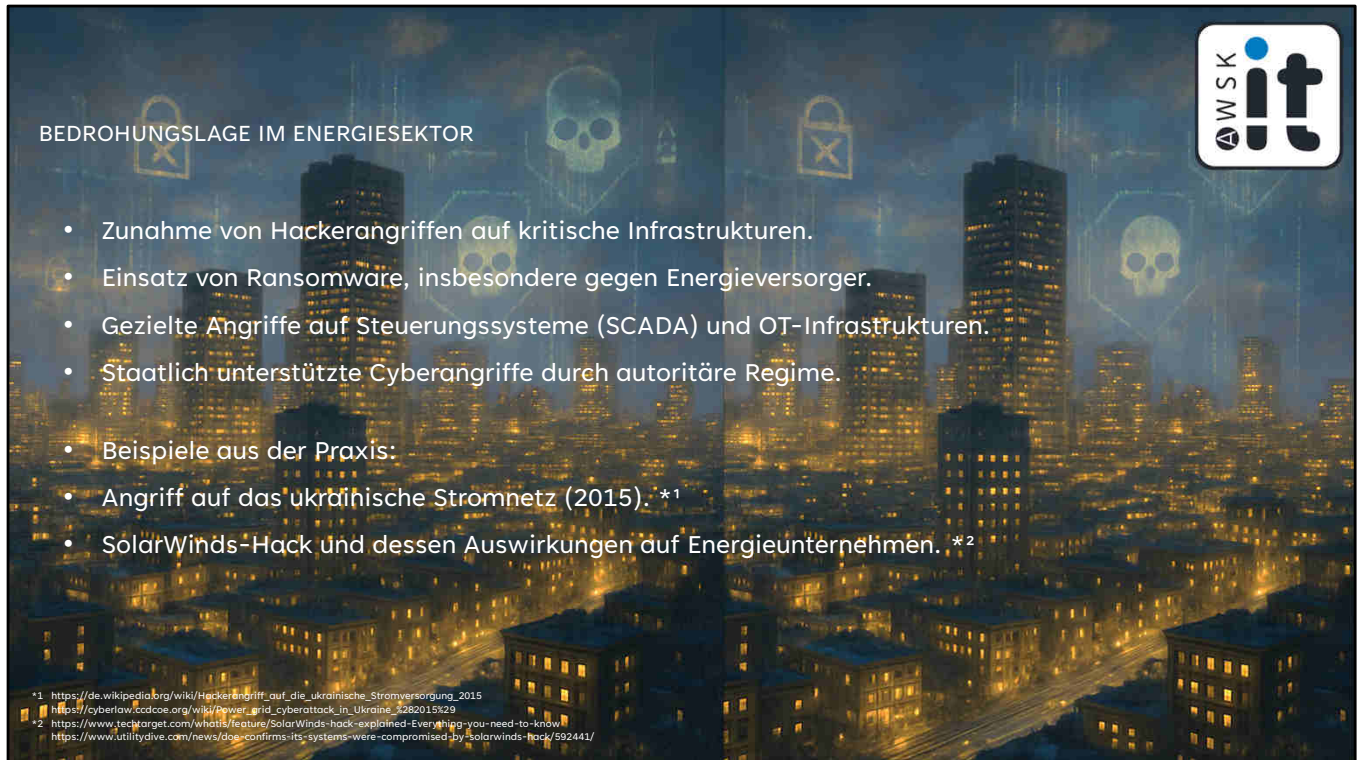
Alan Hofer

Infrastruttura IT e sicurezza IT da oltre 16 anni

AWSK.IT Consulenza per aziende e dipartimenti IT nell'ambito della cybersecurity

Corsi di formazione di sensibilizzazione per i dipendenti per prevenire gli attacchi hacker

Obiettivo della presentazione: Mostrare le sfide e le soluzioni nell'ambito della cybersecurity nel contesto dell'IA



BEDROHUNGSLAGE IM ENERGIESEKTOR

- Zunahme von Hackerangriffen auf kritische Infrastrukturen.
- Einsatz von Ransomware, insbesondere gegen Energieversorger.
- Gezielte Angriffe auf Steuerungssysteme (SCADA) und OT-Infrastrukturen.
- Staatlich unterstützte Cyberangriffe durch autoritäre Regime.
- Beispiele aus der Praxis:
 - Angriff auf das ukrainische Stromnetz (2015). *1
 - SolarWinds-Hack und dessen Auswirkungen auf Energieunternehmen. *2

*1 https://de.wikipedia.org/wiki/Hackerangriff_auf_die_ukrainische_Stromversorgung_2015
*2 https://cyberlaw.ccdcoe.org/wiki/power_grid_cyberattack_in_Ukraine_282015x29
*2 <https://www.techtarget.com/whats/feature/SolarWinds-hack-explained-Everything-you-need-to-know>
<https://www.utilitydive.com/news/doe-confirms-its-systems-were-compromised-by-solarwinds-hack/592441/>

it
AWSK

Situazione delle minacce nel settore energetico

Aumento degli attacchi hacker alle infrastrutture critiche.

Uso di ransomware, soprattutto contro i fornitori di energia.

Attacchi mirati ai sistemi di controllo (SCADA) e alle infrastrutture OT.

Attacchi informatici sostenuti dallo Stato da parte di regimi autoritari.

Esempi pratici:

Attacco alla rete elettrica ucraina (2015). *1

L'hack di SolarWinds e il suo impatto sulle aziende energetiche. *2



REGULATORISCHE RAHMENBEDINGUNGEN

NIS2-Richtlinie:

- Einführung eines einheitlichen Rechtsrahmens für Cybersicherheit in 18 kritischen Sektoren, einschließlich Energie.
- Verpflichtung der Mitgliedstaaten zur Entwicklung nationaler Cybersicherheitsstrategien und Zusammenarbeit auf EU-Ebene.
- Anforderungen an Unternehmen: Risikomanagementmaßnahmen, Meldepflichten bei Sicherheitsvorfällen, Schulungen für Führungskräfte und Mitarbeiter.
- Sanktionen bei Nichteinhaltung: Geldstrafen bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes.

Weitere relevante Regelungen:

EU Cybersecurity Act:
Einführung eines EU-weiten Zertifizierungsrahmens für digitale Produkte und Dienstleistungen.

DSGVO – GDPR:
Schutz personenbezogener Daten und Anforderungen an Datenverarbeitung.

4

Quadro normativo

Direttiva NIS2:

Introduzione di un quadro giuridico standardizzato per la sicurezza informatica in 18 settori critici, tra cui l'energia.

Obbligo per gli Stati membri di sviluppare strategie nazionali di sicurezza informatica e di cooperare a livello europeo.

Requisiti per le aziende: Misure di gestione del rischio, obblighi di segnalazione in caso di incidenti di sicurezza, formazione per dirigenti e dipendenti.

Sanzioni in caso di non conformità: multe fino a 10 milioni di euro o al 2% del fatturato globale annuo.

Altre normative rilevanti:

Cybersecurity Act dell'UE: introduzione di un quadro di certificazione a livello europeo per i prodotti e i servizi digitali.

DSGVO - GDPR: protezione dei dati personali e requisiti per il trattamento dei dati

MYSTERIUM KI GELÜFTET



**“ I Don’t know what AI is,
I didn’t see anything as artificial intelligence
– it is a convenience term – not a tech term “**



Zitat:

George Sadowsky

Internet Pioneer & Internet Hall of Fame Member
during Cloudfest 2025

" Ich weiß nicht, was KI ist, ich habe noch nie etwas gesehen, das als künstliche Intelligenz bezeichnet wurde - es ist ein praktischer Begriff, kein technischer Begriff.

smantelliamo il mistero del AI

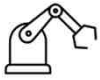
“ Non so cosa sia l'AI, non ho visto nulla come intelligenza artificiale - è un termine di convenienza - non un termine tecnico ”

Citazione:

George Sadowsky

Pioniere di Internet e membro della Internet Hall of Fame
durante il Cloudfest 2025

KÜNSTLICHE INTELLIGENZ: KOMPONENTEN UND RISIKEN



- Automatisierung: einfache Regelwerke, ohne "Lernen"



- Machine Learning: Systeme, die auf Basis großer Datenmengen Muster erkennen



- Deep Learning: künstliche neuronale Netze, die komplexe Aufgaben wie Bild- oder Spracherkennung meistern



- Language Models (LLMs): z.B. ChatGPT – Mustererkennung im Sprachgebrauch



- Kognitive Intelligenz?: noch weit entfernt, nicht autonom, nicht selbstbewusst

Intelligenza artificiale: componenti e rischi

Automazione: semplici regole, senza "apprendimento"

Machine learning: sistemi che riconoscono modelli basati su grandi quantità di dati

Deep learning: reti neurali artificiali che padroneggiano compiti complessi come il riconoscimento di immagini o del parlato

Modelli linguistici (LLM): ad esempio ChatGPT - riconoscimento di modelli nell'uso del linguaggio

Intelligenza cognitiva?: ancora lontana, non autonoma, non autocosciente



SERVICEMODELLE UND DEREN SICHERHEITSIMPLIKATIONEN

- KI läuft auf altbekannten Plattformen
aber teilweise mit enormer und spezifischer Rechenleistung (IaaS PaaS SaaS oder Hardware)

Private Server (inhouse)	Private Cloud	Public Cloud
Volle Kontrolle über Daten und Infrastruktur.	Kombination aus Kontrolle und Skalierbarkeit.	Höchste Skalierbarkeit und Flexibilität.
Höhere Investitions- und Betriebskosten.	Höhere Mietkosten	Höhere Fachkräftekosten (spezifisches Know-How benötigt)
Geringeres Risiko von Datenzugriff durch Dritte	Abhängigkeit von Dienstleistern, jedoch mit vertraglich geregelten Sicherheitsstandards.	Risiken durch geteilte Infrastruktur und potenziellen Zugriff durch EU-ausländische Behörden

- Risikoabwägung:
Bewertung basierend auf Sensibilität der Daten, regulatorischen Anforderungen und Unternehmensstrategie.

7

Modelli di servizio e implicazioni per la sicurezza

L'IA viene eseguita su piattaforme familiari, ma a volte con una potenza di calcolo enorme e specifica (IaaS PaaS SaaS o hardware).

- Server privato (in-house)

Pieno controllo sui dati e sull'infrastruttura.

Costi di investimento e operativi più elevati.

Minor rischio di accesso ai dati da parte di terzi

- Cloud privato

Combinazione di controllo e scalabilità.

Costi di noleggio più elevati

Dipendenza dai fornitori di servizi, ma con standard di sicurezza regolati contrattualmente.

- Cloud pubblico

Massima scalabilità e flessibilità.

Costi di manodopera qualificata più elevati (sono necessarie competenze specifiche)

Rischi dovuti all'infrastruttura condivisa e al potenziale accesso da parte di autorità straniere dell'UE.

Valutazione del rischio:

Valutazione basata sulla sensibilità dei dati, sui requisiti normativi e sulla strategia aziendale.

MENSCHLICHE INTELLIGENZ VS. KÜNSTLICHE INTELLIGENZ: GOVERNANCE UND KONTROLLE



Rolle des Menschen:

- Überwachung und Validierung von KI-Entscheidungen.
- Verantwortung für ethische und rechtliche Implikationen.
- Governance-Modelle:
- Implementierung von Kontrollmechanismen und Notfallsystemen.
- Etablierung von Transparenz und Nachvollziehbarkeit in KI-Systemen.
- Notfallmanagement:
- Entwicklung von Reaktionsplänen bei Systemausfällen oder Fehlfunktionen.
- Schulung von Mitarbeitern im Umgang mit KI-bedingten Vorfällen.

Intelligenza umana vs. intelligenza artificiale: governance e controllo

Il ruolo dell'uomo:

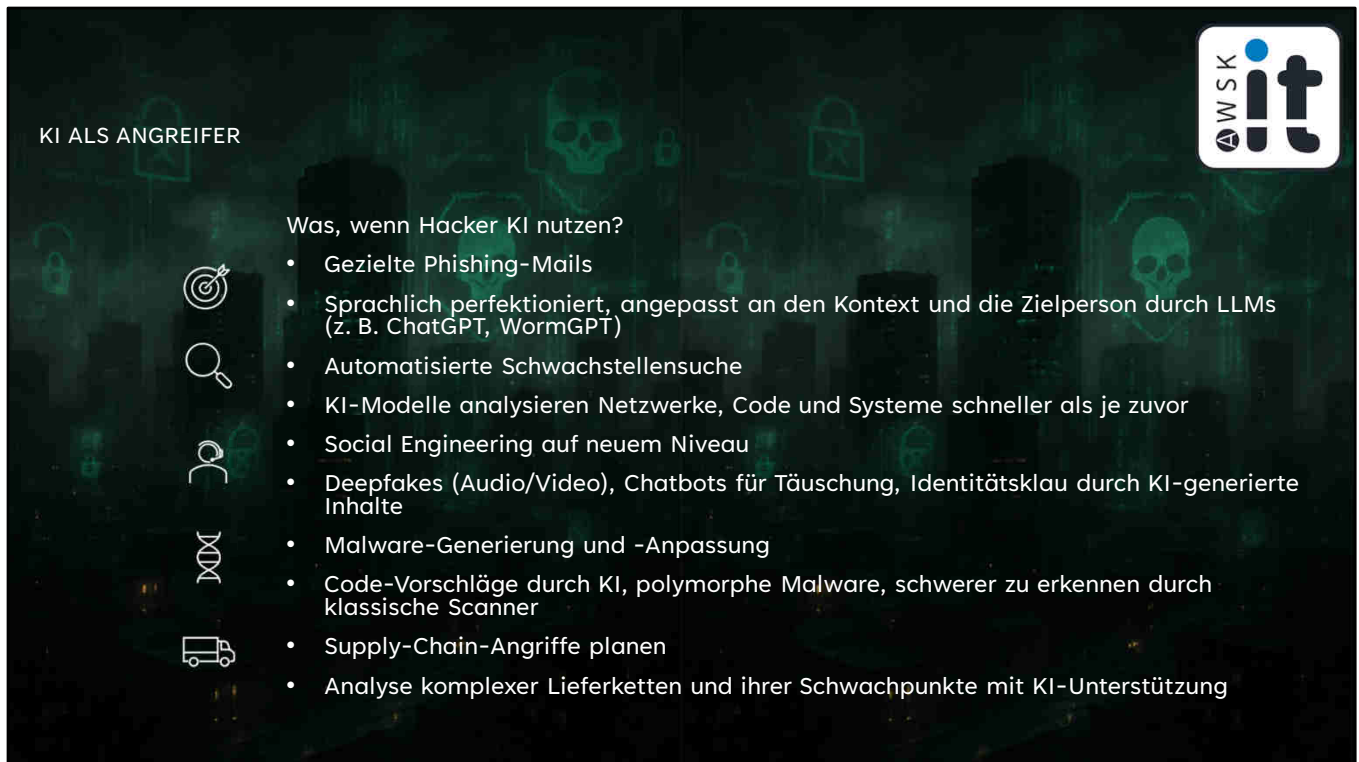
- Monitoraggio e convalida delle decisioni dell'IA.
- Responsabilità per le implicazioni etiche e legali.

Modelli di governance:

- Implementazione di meccanismi di controllo e sistemi di emergenza.
- Stabilire trasparenza e tracciabilità nei sistemi di IA.

Gestione delle emergenze:

- Sviluppo di piani di risposta in caso di guasti o malfunzionamenti del sistema.
- Formazione dei dipendenti per la gestione degli incidenti legati all'IA.



KI ALS ANGREIFER

Was, wenn Hacker KI nutzen?

- Gezielte Phishing-Mails
- Sprachlich perfektioniert, angepasst an den Kontext und die Zielperson durch LLMs (z. B. ChatGPT, WormGPT)
- Automatisierte Schwachstellensuche
- KI-Modelle analysieren Netzwerke, Code und Systeme schneller als je zuvor
- Social Engineering auf neuem Niveau
- Deepfakes (Audio/Video), Chatbots für Täuschung, Identitätsklau durch KI-generierte Inhalte
- Malware-Generierung und -Anpassung
- Code-Vorschläge durch KI, polymorphe Malware, schwerer zu erkennen durch klassische Scanner
- Supply-Chain-Angriffe planen
- Analyse komplexer Lieferketten und ihrer Schwachpunkte mit KI-Unterstützung

L'IA come attaccante

E se gli hacker usassero l'IA?

Email di phishing mirate

Linguisticamente perfezionate, adattate al contesto e alla persona bersaglio grazie agli LLM (ad es. ChatGPT, WormGPT)

Scansione automatizzata delle vulnerabilità

I modelli di IA analizzano reti, codici e sistemi più velocemente che mai

Un nuovo livello di ingegneria sociale

Deepfakes (audio/video), chatbot per l'inganno, furto di identità attraverso contenuti generati dall'IA

Generazione e adattamento del malware

Suggerimenti di codice da parte dell'IA, malware polimorfo, più difficile da rilevare dagli scanner tradizionali

Pianificazione di attacchi alla catena di approvvigionamento

Analisi di catene di approvvigionamento complesse e delle loro vulnerabilità con il supporto dell'IA

FAZIT UND AUSBLICK



- Notwendigkeit einer ganzheitlichen Betrachtung von Cybersicherheit im Kontext von KI.
- Technisch von Infrastruktur über Datenmodelle, Code und Software
- Anwender Sensibilisierung
- Bedeutung von regulatorischer Compliance

Ausblick:

- Weiterentwicklung von Sicherheitsstandards und -technologien.
- Förderung von Zusammenarbeit zwischen Unternehmen, Regulierungsbehörden und Forschungseinrichtungen.

10

Conclusioni e prospettive

Necessità di una visione olistica della cybersecurity nel contesto dell'IA.

Tecnicamente, dall'infrastruttura ai modelli di dati, al codice e al software

Sensibilizzazione degli utenti

Importanza della conformità normativa

Prospettive:

Ulteriore sviluppo di standard e tecnologie di sicurezza.

Promozione della cooperazione tra aziende, autorità di regolamentazione e istituti di ricerca.



Wenn in Ihrem Unternehmen bedarf ist Mitarbeiter;innen zu sensibilisieren oder die Cybersicherheit zu überprüfen stehe ich gerne zur Verfügung

Se la vostra azienda ha bisogno di sensibilizzare i dipendenti o di rivedere la sicurezza informatica, sarò lieto di aiutarvi.