HAN-CIX powered by DE CIX

GRASS-MERKUR

Sichere IT-Betriebskonzepte und Vernetzung im Zeitalter von Cybersecurity

12.09.2024
9. Fachkonferenz Cybersecurity

GRASS-MERKUR GmbH & Co. KG
Rothwiese 5
30559 Hannover
0511 47 54 14 0
info@grass-merkur.de
www.grass-merkur.de

KÄMMER CONSULTING

GRASS MERKUR

NIS2-Richtlinie – Sind Sie betroffen?

Branche

- [ ] Energie- und Wasserversorgung
- [ ] Transport und Verkehr
- [ ] Finanzwesen (Kreditinstitute)
- [ ] Gesundheitswesen (Gesundheitsdienstleister, Hersteller pharmazeutischer Erzeugnisse)
- [ ] Finanzmarktinfrastrukturen (Betreiber von Handelsplätzen, zentrale Gegenparteien)
- [ ] Digitale Dienstleistungen (Online-Marktplätze, Suchmaschinen, soziale Netzwerke)
- [ ] Raumfahrt
- [ ] IKT (Informations- und Kommunikationstechnologie)
- [ ] Post- und Kurierdienst
- [ ] Abfall
- [ ] Herstellung und Vertrieb von chemischen Stoffen
- [ ] Herstellung und Vertrieb von Lebensmitteln
- [ ] Forschung (Forschungsinstitute)
- [ ] Industrie (u. a. Maschinen- und, Fahrzeugbau ...)
- [ ] Verarbeitendes Gewerbe (inklusive Medizinprodukte)
- [ ] Öffentliche Verwaltung

Unternehmensgröße

- [ ] Mehr als 50 Mitarbeiter
- [ ] 10 Millionen Euro Umsatz

Sie gehören einer der genannten Branchen an und haben die relevante Größe - dann sind Sie von der NIS-2 Richtlinie betroffen!

Was müssen Sie jetzt tun?

NIS2-Richtlinie – Sicherheitsanforderungen

- **Risikomanagement:**
  - Identifikation von Cyber-Risiken
  - Bewertung der Auswirkungen von Sicherheitsvorfällen
  - Entwicklung von Risikobewertungen und -managementplänen
- **Sicherheitsrichtlinien und -verfahren:**
  - Erstellung und Implementierung von Sicherheitsrichtlinien
  - Definition von Sicherheitsverfahren und -standards
  - Schulung der Mitarbeiter zu Sicherheitsbest practices
- **Zugangskontrolle:**
  - Verwaltung von Zugriffsrechten und -berechtigungen
  - Implementierung von Identitäts- und Zugriffsmanagement
  - Überwachung und Protokollierung von Zugriffen
- **Incident Response und Management:**
  - Einrichtung eines Incident-Response-Teams
  - Entwicklung von Incident-Response-Plänen
  - Schnelle Reaktion auf Sicherheitsvorfälle und Berichterstattung an Behörden
- **Informationssicherheit:**
  - Verschlüsselung von sensiblen Daten
  - Sicherung von Netzwerken und Systemen
  - Schutz vor Malware und Viren
- **Überwachung und Audit:**
  - Echtzeitüberwachung von Netzwerkaktivitäten
  - Regelmäßige Sicherheitsaudits und -prüfungen
  - Archivierung von Sicherheitsereignisdaten
- **Meldung von Sicherheitsvorfällen:**
  - Pflicht zur Meldung von Sicherheitsvorfällen an nationale Be
  - Zusammenarbeit mit CERTs (Computer Emergency Response Teams)
- **Zusammenarbeit und Koordination:**
  - Zusammenarbeit mit anderen kritischen Infrastrukturen und Behörden
  - Teilnahme an Informationssicherheitsforen und -gemeinschaften
- **Technische Sicherheitsmaßnahmen:**
  - Netzwerksicherheit (Firewalls, Intrusion Detection/Prevention Systems)
  - Patch-Management und regelmäßige Systemupdates
  - Sicherheitssoftware und -tools
- **Business Continuity und Wiederherstellung:**
  - Entwicklung von Notfall- und Wiederherstellungsplänen
  - Sicherung wichtiger Geschäftsdaten und -prozesse
  - Regelmäßige Durchführung von Notfallübungen

Umsetzung in nationales Recht bis Oktober 2024

Anforderungen an Rechenzentren

Wachsende Anforderungen an Rechenzentren werden von GRASS-MERKUR erfüllt	
Physische Sicherheit (Zugangskontrolle, Videoüberwachung, Alarmsysteme, …) ✓	**Hybride Betriebsmodelle** kombinierbar (Cloud & On-Premise) ✓
Betriebs- und Ausfallsicherheit der betriebsrelevanten Systeme (Energie, Klima) ✓	RZ für **leistungsstarke GPU-Systeme** (High Performance Computing) ✓
Redundanz, Disaster Recovery und **Hochverfügbarkeit** der IT-Systeme ✓	**Regulatorische Anforderungen** (NIS2, DORA, …) ✓
Skalierbarkeit und **Effizienz** bei IT- und RZ-Betrieb ✓	**Datensicherheit und Datenschutz** ISO-zertifiziert ✓
Datennetz-Anbindung zu Hyper-Scalern HAN-CIX powered by DE-CIX (kurze Latenz) ✓	**Erkennung und Abwehr von Cyberrisiken** (Managed Detection and Response) ✓
Nachhaltigkeit beim RZ-Betrieb (Grünstrom, PV-Anlage, Windkraft, Abwärmenutzung, …) ✓	**Managed-Services** mit klaren Verantwortlichkeiten (RACI) ✓

Ganzheitliches Service-Angebot zur Umsetzung hybrider Betriebsmodelle

Modul 5

SIEM / SOC

(XDR-Lösung – Extended Detection and Response)

Modul 1

Datacenter Services

Colocation

Modul 2

Managed Services

Professional Services

Modul 3

Cloud Services

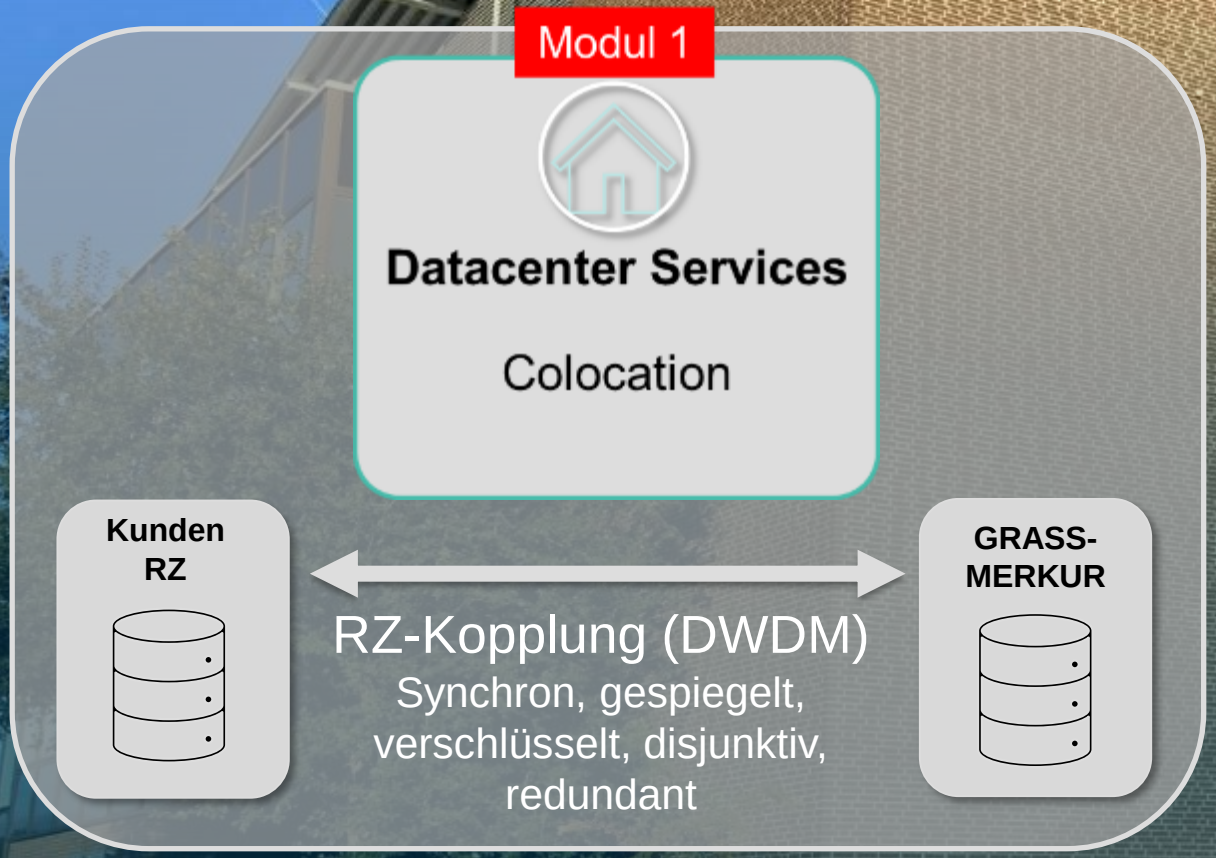
Storage & Compute

Modul 4

Netzwerk Services

DWDM & DE-CIX

Hybrides Betriebskonzept
Modul 1: Colocation



Colocation-Modelle nach Kundenbedarf, z.B.

- 2 RZ synchron gespiegelt
- Ein oder mehrere getrennte Brandabschnitte

Sicherer Basisbetrieb im Colocation-RZ betriebswirtschaftlich optimiert

Hybrides Betriebskonzept
Modul 2: Managed-Services

Modul 2

Managed Services

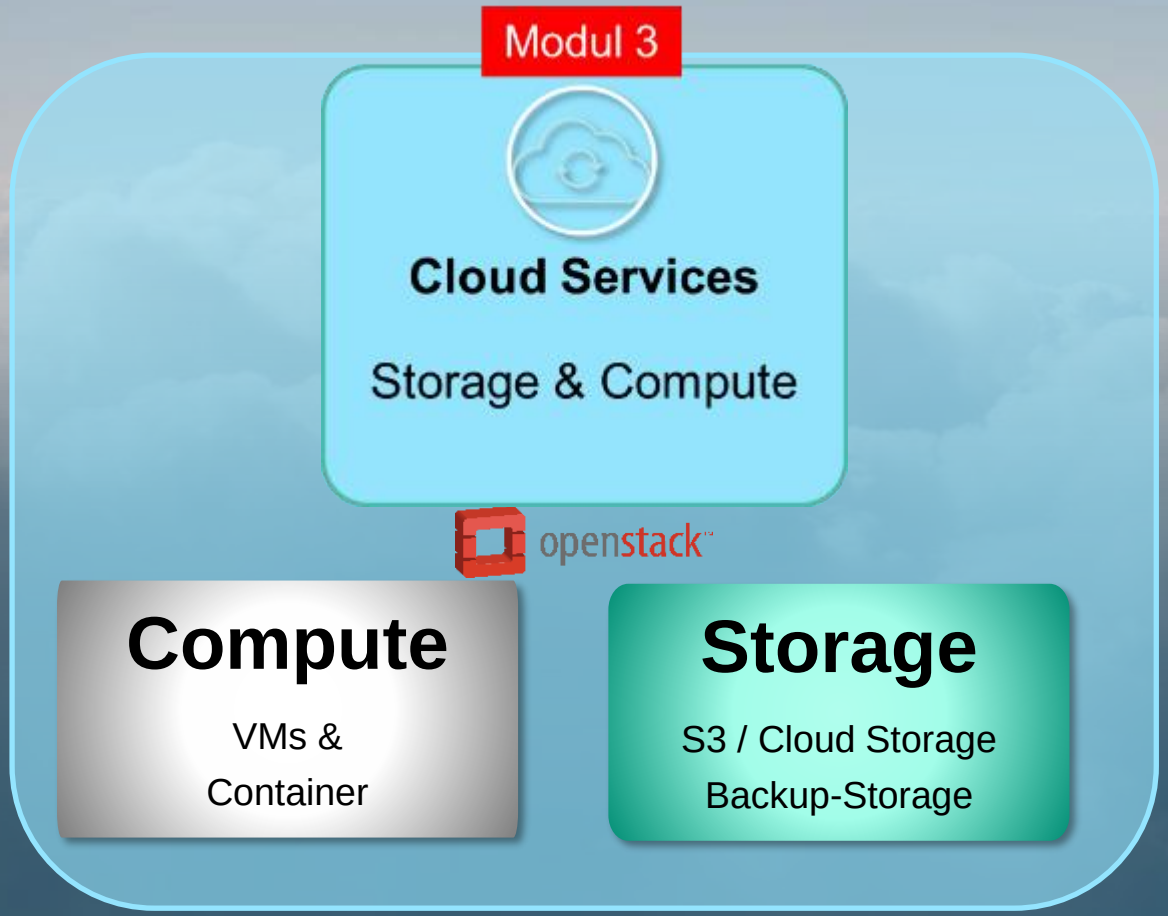
Professional Services

Managed Backup
Managed DWDM
Managed Citrix
Managed Windows Server
Managed Linux -Server
Managed Job Scheduling

- modular
- flexibel
- definierte Verantwortlichkeiten
- SLA-basierte Verträge

Individuell nach Kundenbedarf zugeschnittene Services

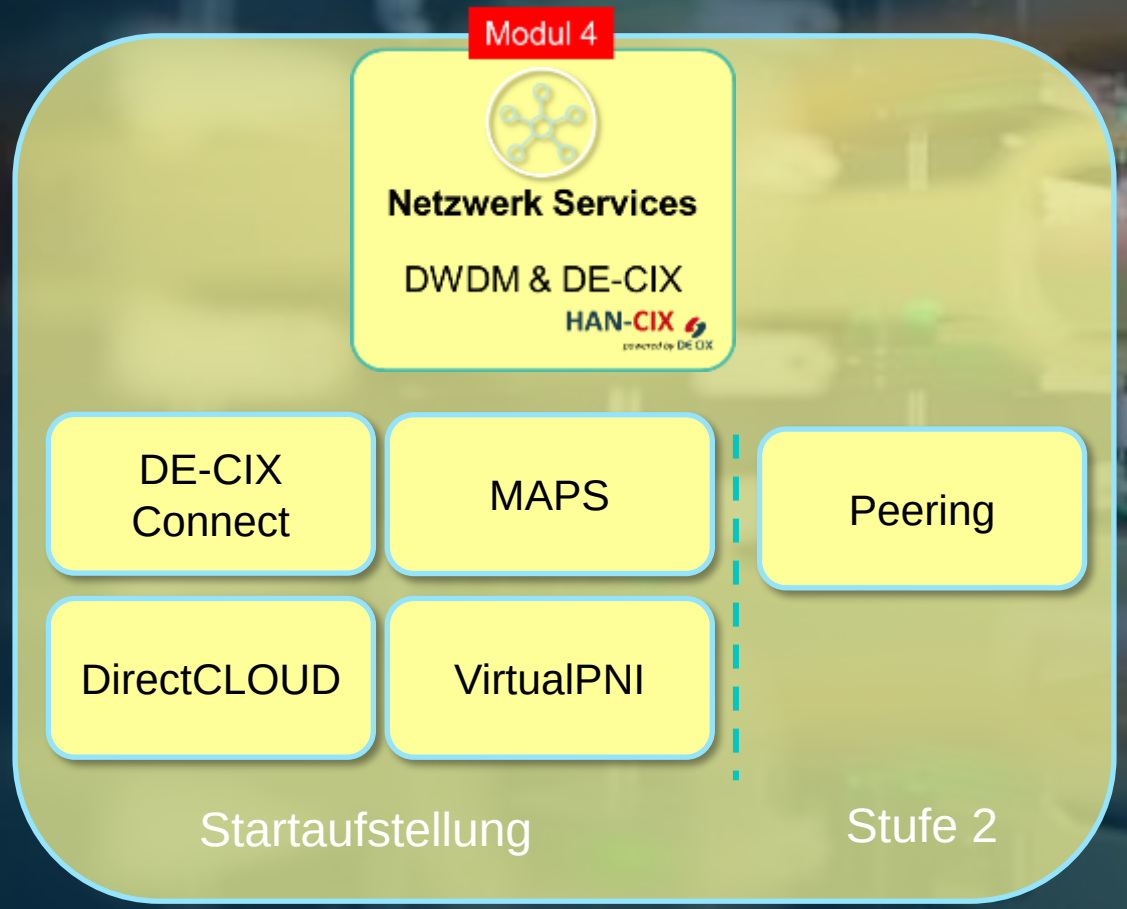
Hybrides Betriebskonzept
Modul 3: HAN-CLOUD – die GRASS-MERKUR Cloud.



- granular & flexibel
- kostentransparent
- „all-in“-Preise
- Anbindung an HAN-CIX
- internationale Standards
- umfassendes Reporting

flexibel / schnell / einfach / kostenoptimiert

Hybrides Betriebskonzept
Modul 4: Netzwerk-Services & HAN-CIX



- Sicher & performant
- kurze Latenzen
- Stabile, DDoS-freie Lösung
- Flexibel kombinierbar
- On-premise & Cloud
- Muli-Cloud-Konzepte

Sicher, flexibel, schnell & kostenoptimiert

Hybrides Betriebskonzept
Modul 4: Netzwerk-Services & HAN-CIX

DE-CIX Connect	Anbindung zum DE-CIX im GRASS-MERKUR Rechenzentrum.
DirectCLOUD	Direkte Verbindung (Cloud-Exchange) zu über 50 Cloud-Anbietern für hybride Multi-Cloud-Lösungen.
MAPS	**M**icrosoft **A**zure **P**eering **S**ervice, garantierte, hochperformante Verbindung mit geringstmöglicher Latenz, unterstützt von Microsoft.
VirtualPNI	Virtuelle Punkt-zu-Punkt-Verbindungen zwischen Metroregionen, flexible Bandbreiten, ideal für die standortübergreifende Vernetzung.
Peering	Datenaustausch am Internetknoten, Verbindung der beteiligten Netzwerke (über 1.000 am DE-CIX Frankfurt).

Hybrides Betriebskonzept
Modul 5: XDR Lösung (SIEM / SOC)

Modul 5

SIEM / SOC
(XDR-Lösung – Extended Detection and Response)

- Managed Detection and Response
- Managed Security Awareness
- Managed Risk

- Mix aus Technik und Security Experten
- Trifft Voranalyse
- Die „verlängerte Cyber-Security-Werkbank“
- Schnelle Reaktion und frühzeitige Alarmierung

Sicher, flexibel, schnell & kostenoptimiert

Hybrides Betriebskonzept
Modul 5: XDR Lösung (SIEM / SOC)

Modul 5

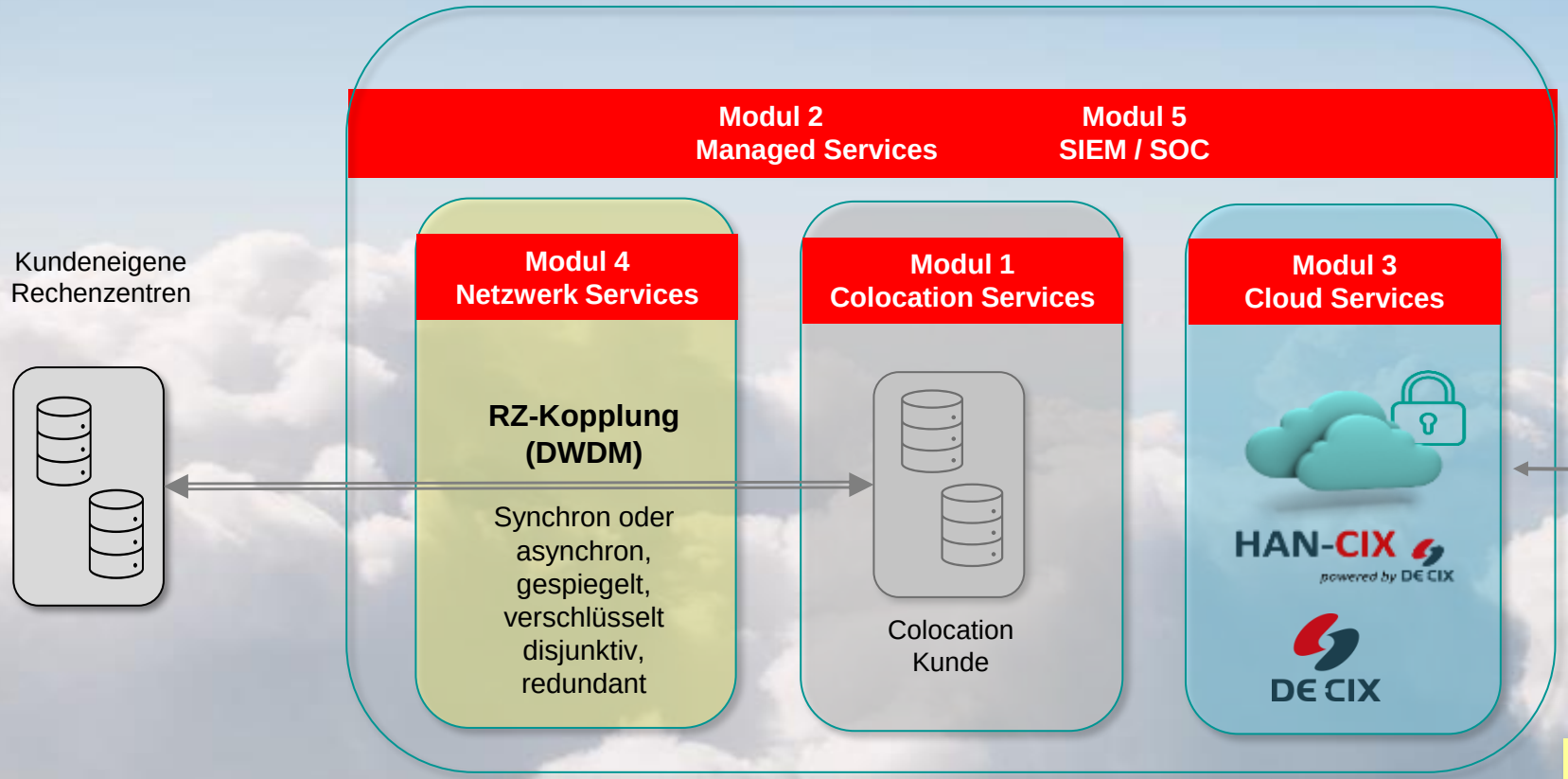
SIEM / SOC

(XDR-Lösung – Extended Detection and Response)

Managed Detection and Response	**Rund-um-die-Uhr Überwachung** von Netzwerken, Endgeräten, und Cloud-Umgebungen, um aktuelle Cyber-Angriffe frühzeitig zu erkennen und Gegenmaßnahmen zu ergreifen.
Managed Risk	Ermöglicht Unternehmen, die eigene IT-Umgebung zu schützen, Risiken in Netzwerken und bei Endgeräten zu erkennen, zu bewerten und Maßnahmen zu ergreifen (**Schwachstellen-Management**)
Managed Security Awareness	Mitarbeitenden wird auf ansprechende Weise das notwendige **Wissen vermittelt**, um Social-Engeneering- Angriffe zu erkennen und so Cyberrisiken zu minimieren.

Sicher, flexibel, schnell & kostenoptimiert

Hybrides Betriebsmodell / alles aus einer Hand



Zugriff über HAN-CIX (dedizierte, redundante, disjunktive Direktverbindung zum DE-CIX)

Vorteile der Lösung:

- ✓ Einfache Bedienbarkeit
- ✓ Transparente Kosten
- ✓ Flexibilität
- ✓ RZ Standort in Deutschland
- ✓ Einhaltung des BDSG, DSGVO

Nachhaltigkeit, ESG* und CSRD**

Operative Maßnahmen

Kaltgangeinhausungen
Hocheffiziente Klimasysteme
Intelligente Gebäudeleittechnik
Moderne der Kälteanlagen

Grünstrom Bezug

Energiegewinnung aus 100% regenerativen Energiequellen (Wasserkraft) inkl. Herkunfts-zertifikat (HKN Verfahren)

Bio-Fuel

Nutzung von HVO (Bio-Fuel) für den Betrieb der Netzersatz-anlagen (dadurch über 90% CO_2-Reduktion)

Elektromobilität

Umstellung des Fuhrparks auf Hybrid- bzw. Elektroantrieb für Firmen-KFZ, Ladesäulen auf dem Firmengelände

Eigenstrom Produktion

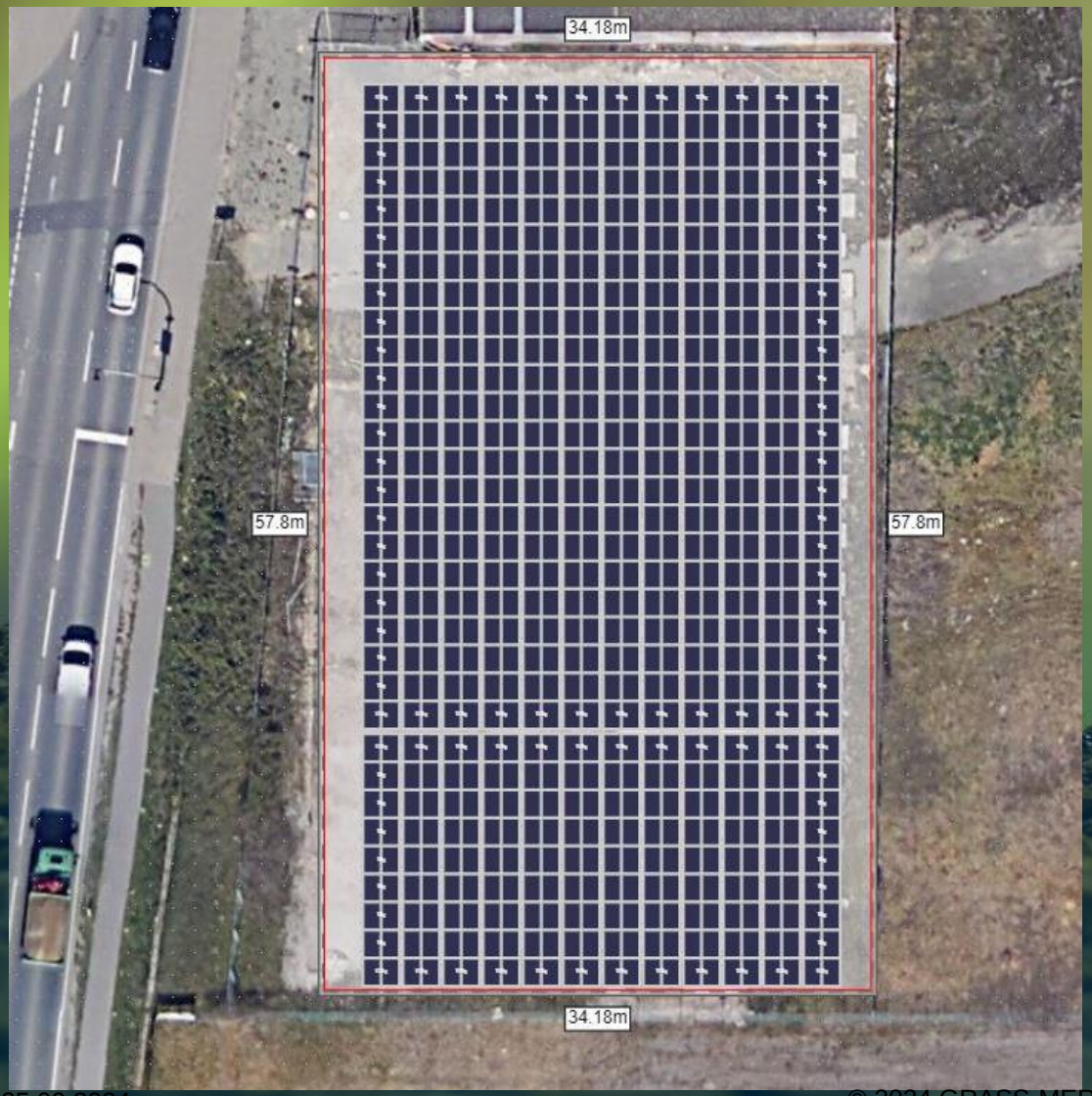
Energiegewinnung aus Windkraftanlage (Projektierung) und Photovoltaik-Anlage (in Umsetzung)

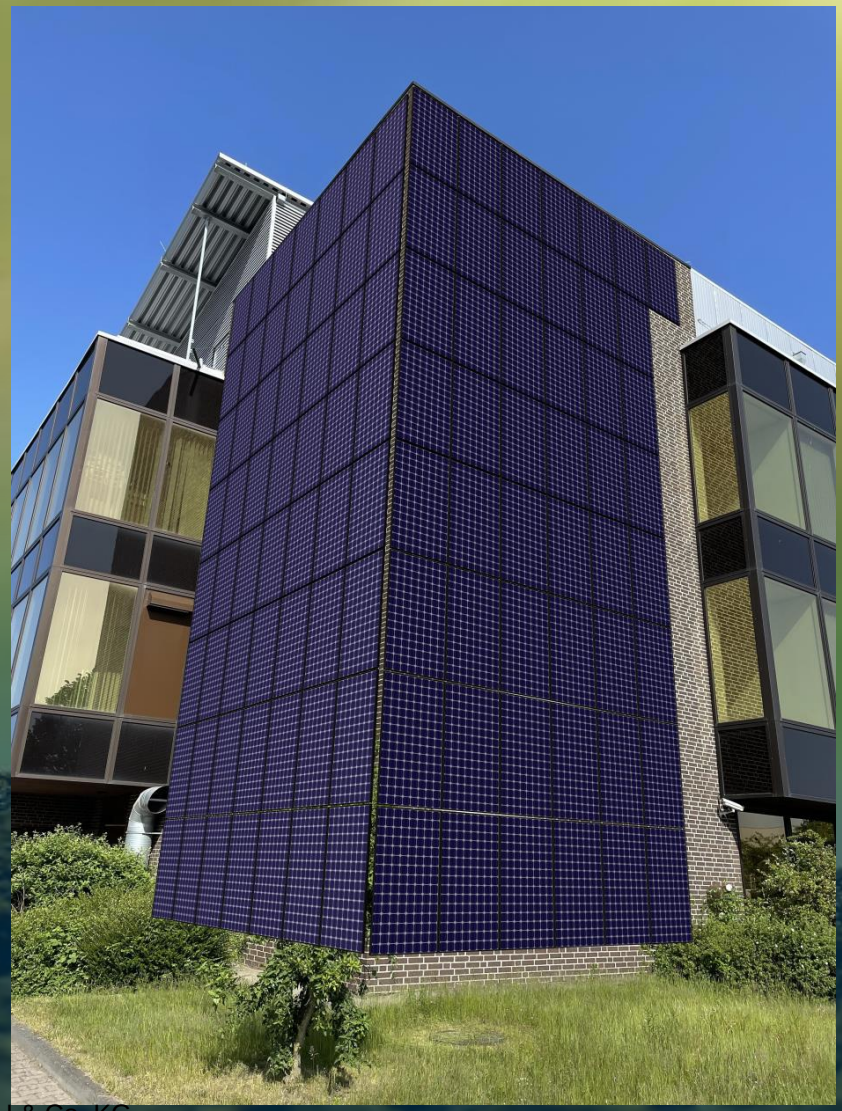
Abwärmenutzung

Konzepte zur Abwärmenutzung sind in Abstimmung mit dem Energieversorger und Industrie-unternehmen (in Prüfung)

*ESG: Environmental, Social und Governance **CSRD: Corporate Sustainability Reporting Directive

Projekt „PV-Anlage“





Schwachstellen-Management und netzwerkbasierte Bedrohungserkennung

XDR-LÖSUNG: WIE FUNKTIONIERT EIN SIEM / SOC IN DER PRAXIS?

Funktionsprinzip SIEM & SOC

- **S**ecurity **I**nformation and **E**vent **M**anagement
  - Erkennung von Anomalien
  - Sensoren sammeln Log-Daten
  - Analyse der Daten
- **S**ecurity **O**peration **C**enter
  - Detailuntersuchung durch Spezialisten
  - Empfehlung von Maßnahmen
  - Behandlung und Behebung von Schwachstellen.

Funktionsprinzip SIEM & SOC (XDR Lösung)

KI kann den Menschen nicht ersetzten

Incident Detection and Response

FRÜHZEITIGE BEDROHUNGSERKENNUNG

Managed Detection and Response in der Praxis

eMail vom Threat Research Team mit potenzieller Bedrohung und Handlungsempfehlung:

Von: Threat Research Team
Gesendet: 11. April 2023
Betreff: Managed Detection Alert

„…Unser Threat-Research-Team hat eine Liste gefunden, auf der der Name Ihres Unternehmens als eines der Unternehmen aufgeführt ist, von denen Daten erworben werden konnten.

Laut Informationen konnten sie Zugang zu Archiven mit mehr als 172 GB erhalten, wie auf dem Screenshot zu sehen ist. Wir empfehlen eine sofortige Untersuchung im Rahmen des Incident Response (IR) bezüglich dieser Erkenntnis…“

Beispiel eines Sicherheitsberichts

ID	Abweichung	Status	Auswirkung auf Geschäftsbetrieb	Risiko	Nachweis / Quelle	Maßnahmen zur Fehlerbehebung
1	Operating System (OS) hat Laufzeitende erreicht (End of Life (EOL)	Risiko	Hoch	Das Betriebssystem (BS) auf dem entfernten Host hat das Ende seines Lebenszyklus (EOL) erreicht und sollte nicht mehr verwendet werden.	Host IP: …..	Aktualisieren Sie das Betriebssystem auf dem entfernten Host auf eine Version, die vom Hersteller noch unterstützt wird und Sicherheitsupdates erhält.
2	Offener Port	Risiko	Hoch	Offenes Eingangstor zum internen Netzwerk, auch wenn dieser sich in der DMZ befindet	Host IP …..	Den SSH-Port nicht der ganzen Welt freigeben. Dem Root-Benutzer nicht erlauben, ein SSH-Terminal zu verwenden. Zwingen Sie alle Benutzer, sich mit einem SSH-Schlüsselpaar anzumelden, und deaktivieren Sie dann die Passwortauthentifizierung.
3	Apache …… Mehrere Sicherheitslücken	Risiko	Mittel	Apache ….. Ist anfällig für Sicherheitslücken	Host IP ……	Es wurde keine Lösung vom Anbieter bereitgestellt. Allgemeine Lösungsoptionen sind ein Upgrade auf eine neuere Version, das Deaktivieren entsprechender Funktionen, das Entfernen des Produkts oder das Ersetzen des Produkts durch ein anderes. Es liegen folgende Sicherheitslücken vor: - CVE-2018-8032: Cross-Site Scripting (XSS) im Standard-Servlet/Services - CVE-2019-0227: Serverseitige Request-Fälschung (SSRF)

Beispiel

Handlungsempfehlungen

- „Wissen, was läuft“: Kennen Sie Ihre IT-Umgebung
- Prozesse etablieren
  - Risikomanagement, Notfall-Szenarien, ISMS, Wiederherstellungspläne, Backup (immutable)
- Mit zuverlässigen Dienstleistern zusammenarbeiten für
  - SIEM / SOC Lösungen
  - Colocation, Cloud-Services, Managed-Services
  - Sichere Netzanbindungen (Blackholing, DDoS-Protection, …)

Ihr Kontakt bei GRASS-MERKUR

Dipl.-Kfm.

MARKUS DIETZ

Leiter Business Development und Vertrieb

GRASS-MERKUR GmbH & Co. KG

Rothwiese 5 - 30559 Hannover

Tel. +49 511 47 54 14 – 13 Fax +49 511 47 54 14 – 33

Mobil + 49 178 7866 400

markus.dietz@grass-merkur.de

www.grass-merkur.de

Kontakt zur GRASS-MERKUR

GRASS-MERKUR GmbH & Co. KG

Rothwiese 5 - 30559 Hannover

Tel. +49 511 47 54 14 – 109

vertrieb@grass-merkur.de

https://www.grass-merkur.de/

Folgen Sie uns auf LinkedIn

Vielen Dank für Ihre Aufmerksamkeit…