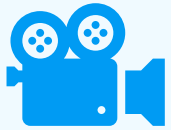
Detektion und Reaktion mit SOC, EDR & Co.

So gewährleisten innovative Security-Lösungen die Einhaltung der NIS2-Richtlinie

Housekeeping Rules



Das Webinar wird aufgezeichnet

Teilnehmer sind während des Webinars stummgeschaltet

Fragen bitte während des Webinars in das Q&A-Fenster stellen

Herzlich willkommen

Ihre Experten

Andreas Buhlmann

Senior Presales Engineer

Peter Weber

Technical Account Manager Security

Daniel Graßer

Senior Director of Security Services

plusserver

Agenda

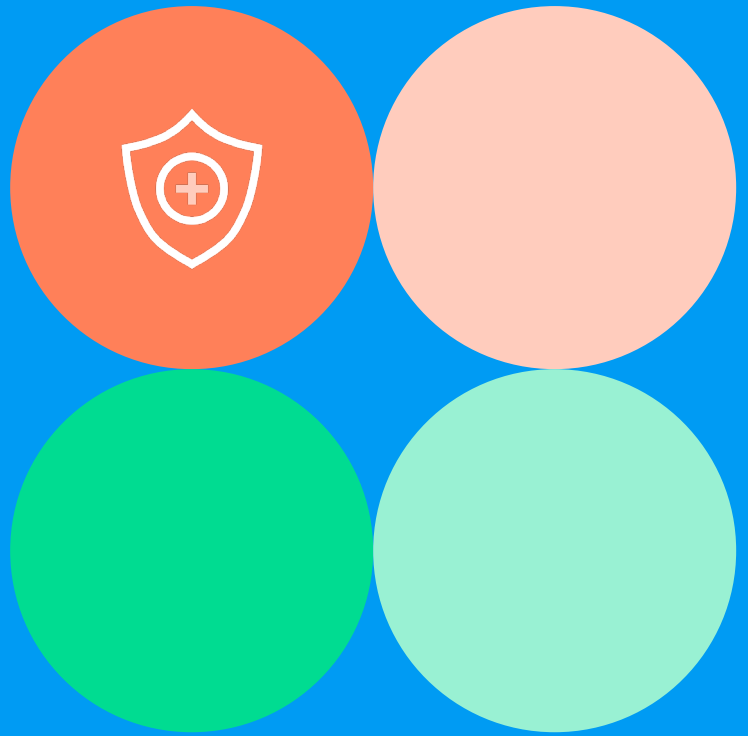
Detektion und Reaktion

- Übersicht: Umsetzungsszenarien und Projektmöglichkeiten
- Schwachstellen, aber doch nicht bei uns?
- Angriffe auf meine Infrastruktur – was ich nicht sehe, ist nicht passiert!
- Warum jetzt auch noch ein SOC – was noch alles?
- Jetzt ist es doch passiert - was jetzt?
- Q & A

plusserver

Umsetzungsszenarien und Projektmöglichkeiten

Security Services



plusserver

Wie kann plusserver unterstützen?

NIS2-Assessment (plusserver oder Partner)

Security-Beratung/ Consulting

+ Feinkonzeption und Design von Security-Maßnahmen und -Architekturen
+ Pentests und Audits

Security-Lösungen

+ SOC as a Service
+ EDR as a Service
+ Schwachstellenmanagement
+ Next Gen Firewall
+ DDoS-Schutz
+ Backup/Disaster Recovery

Zertifizierte Infrastruktur

+ Standorte in DE
+ ISO 27001
+ BSI C5 (Typ-II)

Sales Cases mit NIS2

Einfache Beispiele

Security auf dem Stand der Technik	NIS2-Assessment und Security Services als Projekttreiber zur Reduzierung von Komplexität
Incident Management	Security Scanner, SOC-Module, Security Operations Center aaS, Endpoint Detection & Response
Business Continuity	plusserver Cloud Services (made in Germany / certified) mit Backup as a Service in Kombination mit Cloud Security

plusserver

360-Grad-Ansatz

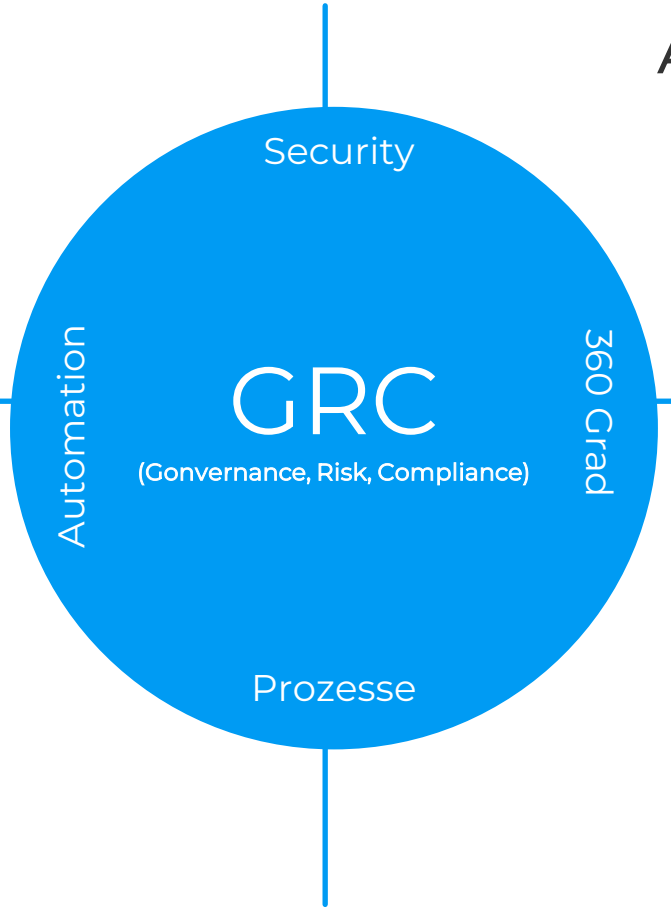
Security als Prozess etablieren

Wiederherstellung (Recovery)

- Backup as a Service

Analyse und Risikomanagement

- IT-Security Consulting
- Audits und Penetrationstests (@-Yet)



Detektion & Reaktion

- SOC as a Service
- Security Scanner
- Endpoint Detection with SOC

Prävention nach Schutzbedarf

- Next Generation Firewall (Cloud)
- Endpoint Detection and Response
- Workload Protection
- DDoS und WAF (Akamai und Link11)

Inhalte für Ihre Kommunikation

Kostenfreie Verwendung, hochwertige Inhalte

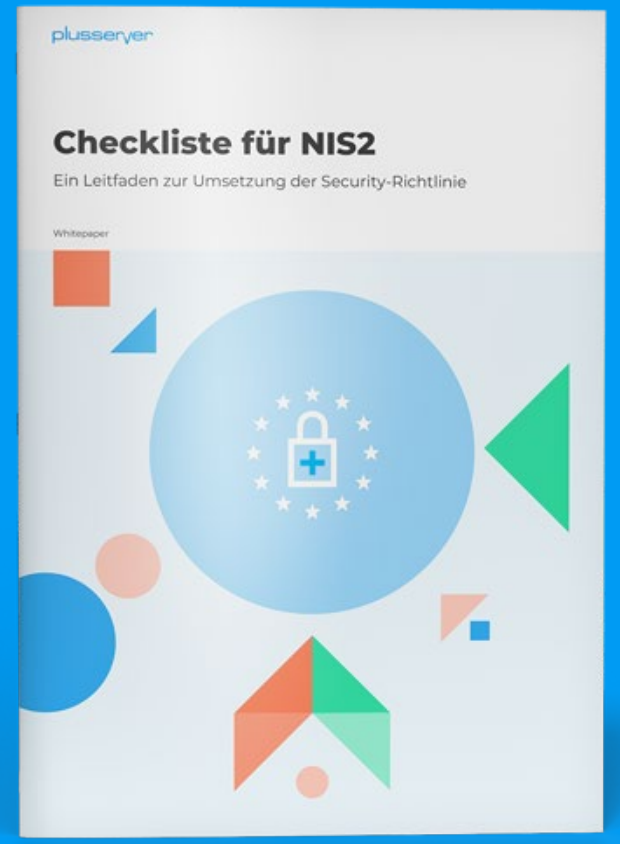
Nutzen Sie unsere Assets für die Ansprache Ihrer Kunden oder für die eigene LeadGen. Zum Thema NIS2 und unseren Security-Produkten bieten wir verschiedene Inhalte, die Sie passend zu den Bedürfnissen Ihrer Kunden einsetzen können.

+ **(Produkt-)Datasheets für den ersten Kontakt mit den Kunden**

+ **Präsentationen und Playbooks für Ihre Gespräche mit den Kunden**

+ **Checklisten und Blog-Beiträge für den Wissensaustausch**

Alle Inhalte finden Sie in unserem neuen MarketingHub und auf der Landingpage zur NIS2-Initiative.

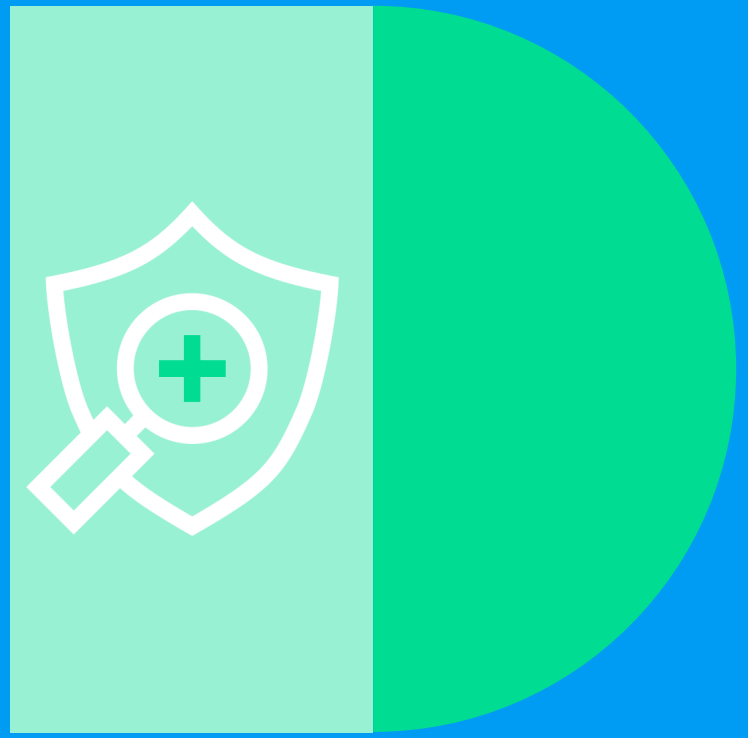


plusserver

Schwachstellen, aber doch nicht bei uns?

Wie zahlt Vulnerability Management auf NIS2 ein?

Incident Management



plusserver

Warum Schwachstellenmanagement?

1

+ Lassen Sie die Tür nicht offen – Schwachstellen-Management: ein MUSS!

+ Hohes Risiko

2

+ Schwachstellen-Management ist ein Kern-Element einer State-of-the Art Security-Strategie!

+ Ohne Detektion keine Reaktion

3

+ Schnell und effektiv ein unattraktives Ziel werden!

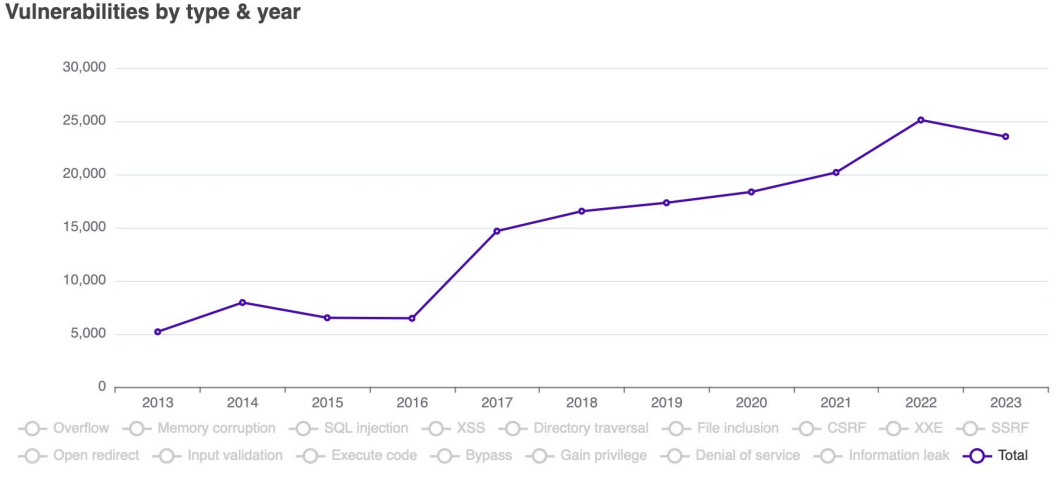
+ Zahlt direkt in die Ziele, Maßnahmen und Anforderungen von NIS2 ein

plusserver

Bedrohung durch Schwachstellen

Die Anzahl an Schwachstellen steigt und die Zeit bis zur Ausnutzung liegt nur noch bei 12 Tagen!

Pro Jahr werden immer mehr Schwachstellen (CVE) registriert



Schwachstellen werden bereits kurz nach Veröffentlichung ausgenutzt!

CVE-2021-44228 Detail

MODIFIED

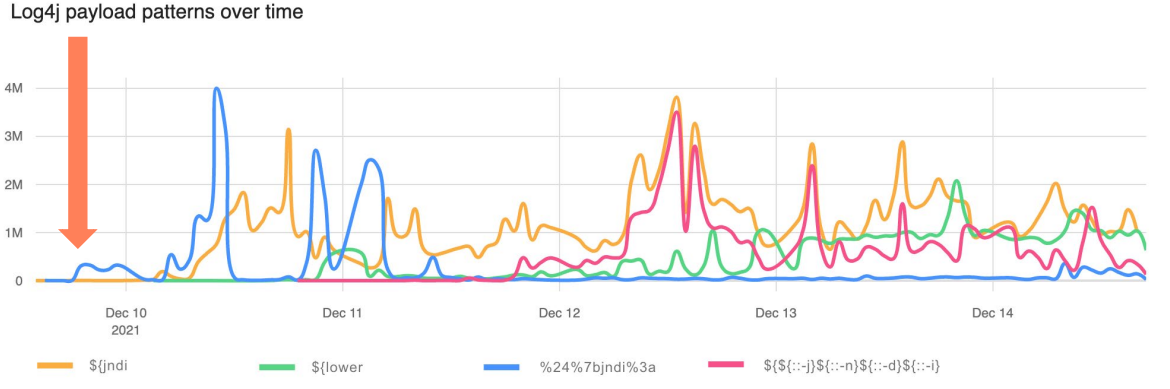
This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

QUICK INFO

CVE Dictionary Entry:
CVE-2021-44228
NVD Published Date:
12/10/2021
NVD Last Modified:
04/03/2023
Source:
Apache Software Foundation



plusserver

Security Scanner as a Service

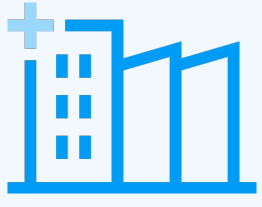
Zuverlässiges Schwachstellenmanagement

+ **Erkennung von Schwachstellen** durch netzwerkbasierte Scans (IPv4 & IPv6)
+ **Veränderungen** in der Cloud-Umgebung werden sofort sichtbar
+ **Steigerung der Transparenz des Security-Levels**
+ **Alarmierung** und **Berichte** über erkannte Schwachstellen
+ Self-Service-Produkt
+ 24/7 Support

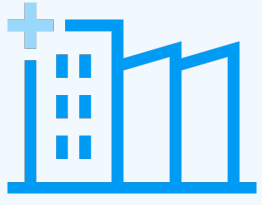
Kompatibel mit:

pluscloud open

pluscloud VMware



pluscloud local

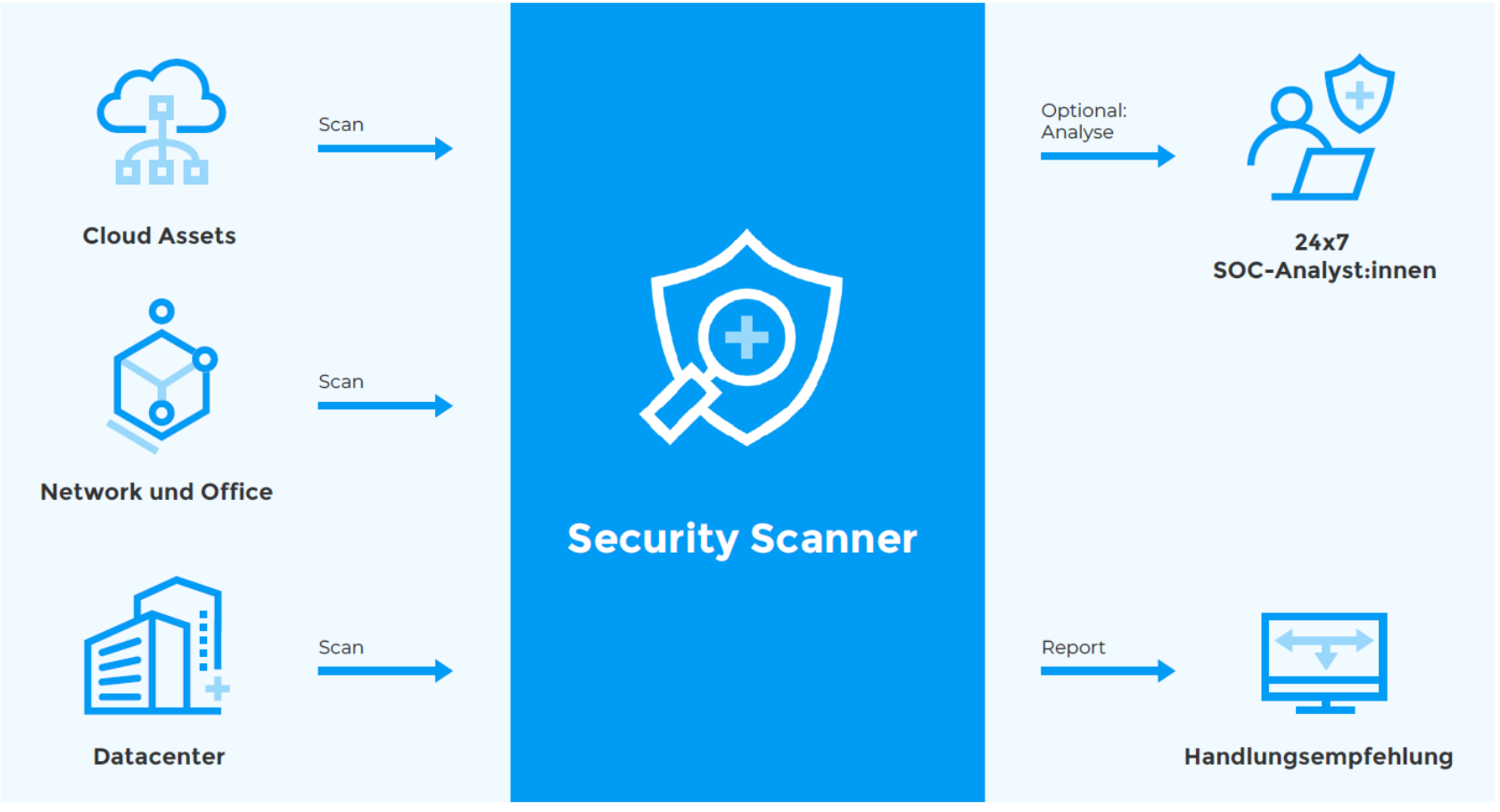


On-Premises

plusserver

Security Scanner as a Service

Einsatzmöglichkeiten & Produktdetails



plusserver

Angriffe auf meine Infrastruktur – was ich nicht sehe, ist nicht passiert!

EDR, Managed Detection und Response – wie hilft mir das bei NIS2?

State of the Art Security & Incident Management

plusserver

Warum EDR?

1

+ Ohne Detailanalyse an den Endpoints und Servern ist man im BLINDFLUG
+ Hohes Risiko

2

+ EDR ist die Basis für Incident Management und somit State-of-the-Art Security
+ Ohne Detektion keine Reaktion

3

+ Schneller und einfacher Schutz des Geschäftsbetriebs
+ Zahlt direkt auf die Ziele, Maßnahmen und Anforderungen von NIS2 ein

plusserver

Endpoint Detection & Response (EDR)

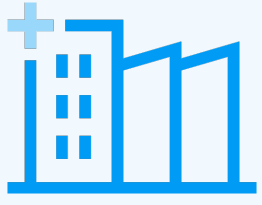
Moderne Endpoint und Server Protection

+ Schutz von **Daten, Prozessen, Netzwerkverkehr auf Servern und Endpoints**
+ **Abwehr** von Malware, Netzwerkangriffen, Phishing sowie Schutz des E-Mail-Clients und Browsers
+ **Steigerung** des **Security Levels durch Malware und Ransomware Protection**
+ Erkennung von **zielgerichteten Attacken in der Infrastruktur**
+ EDRaaS als Full-Management-Produkt mit 24/7 Support
+ SOC-Integration für Advanced Monitoring

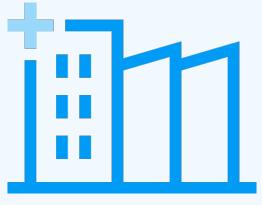
Kompatibel mit:

pluscloud open

pluscloud VMware



pluscloud local



On-Premises

plusserver

Endpoint Detection & Response (EDR)

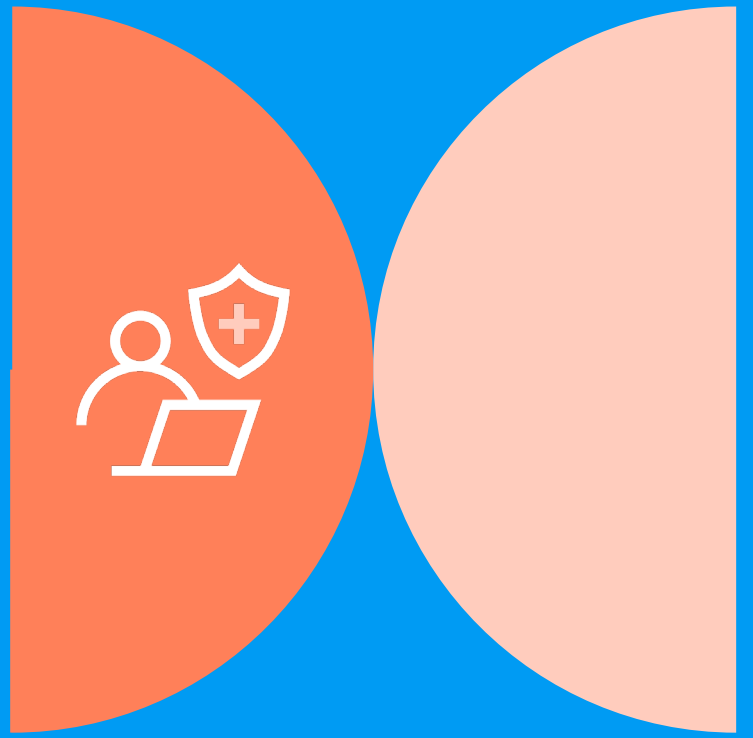
Einsatzmöglichkeiten & Produktdetails

plusserver

Warum jetzt auch noch ein SOC – was noch alles?

SOC ist Key, ist es kompliziert? Nicht bei uns!

State of the Art Security & Incident Management



Warum SOC?

1

+ Ohne Transparenz keine Zusammenhänge und schnell die falschen Entscheidungen getroffen!

+ Legen Sie Cyber-Kriminellen das Handwerk

2

+ SOC ist das Core-Element jeder Security-Strategie

+ Ohne Detektion keine Reaktion und keine Prävention

3

+ Direkter Einfluss auf den Schutz des Geschäftsbetriebs der Unternehmen

+ Zahlt direkt auf die Ziele, Maßnahmen und Anforderungen von NIS2 ein

plusserver

+ Was ist passiert?
+ Sind die Daten weg?
+ Können wir auch 24x7?
+ Was ist wirklich los und was wäre eine angemessene Reaktion?
+ Oder ist es falscher Alarm?

… welche Fragen stellen sich jetzt?

IT-Department

Bereiche
Keller, Erdgeschoss, Dachgeschoss, Garten, Garage etc.

Bereiche
Datacenter, Cloud und Clients & Mobile Worker

Kameras & Überwachung

IT-Security Technologie

Brandmelder

Alarmierung

Alarmierung

plusserver

+ Passen unsere Prozesse?
+ Haben wir die richtigen Fachkräfte?
+ Haben wir die richtige Technologie?
+ Wie komplex sind unsere Lösungen?
+ Kann uns ein externer Partner helfen?

… welche Fragen stellen sich jetzt?

IT-Department

Bereiche
Keller, Erdgeschoss, Dachgeschoss, Garten, Garage etc.

Bereiche
Datacenter, Cloud und Clients & Mobile Worker

Kameras & Überwachung

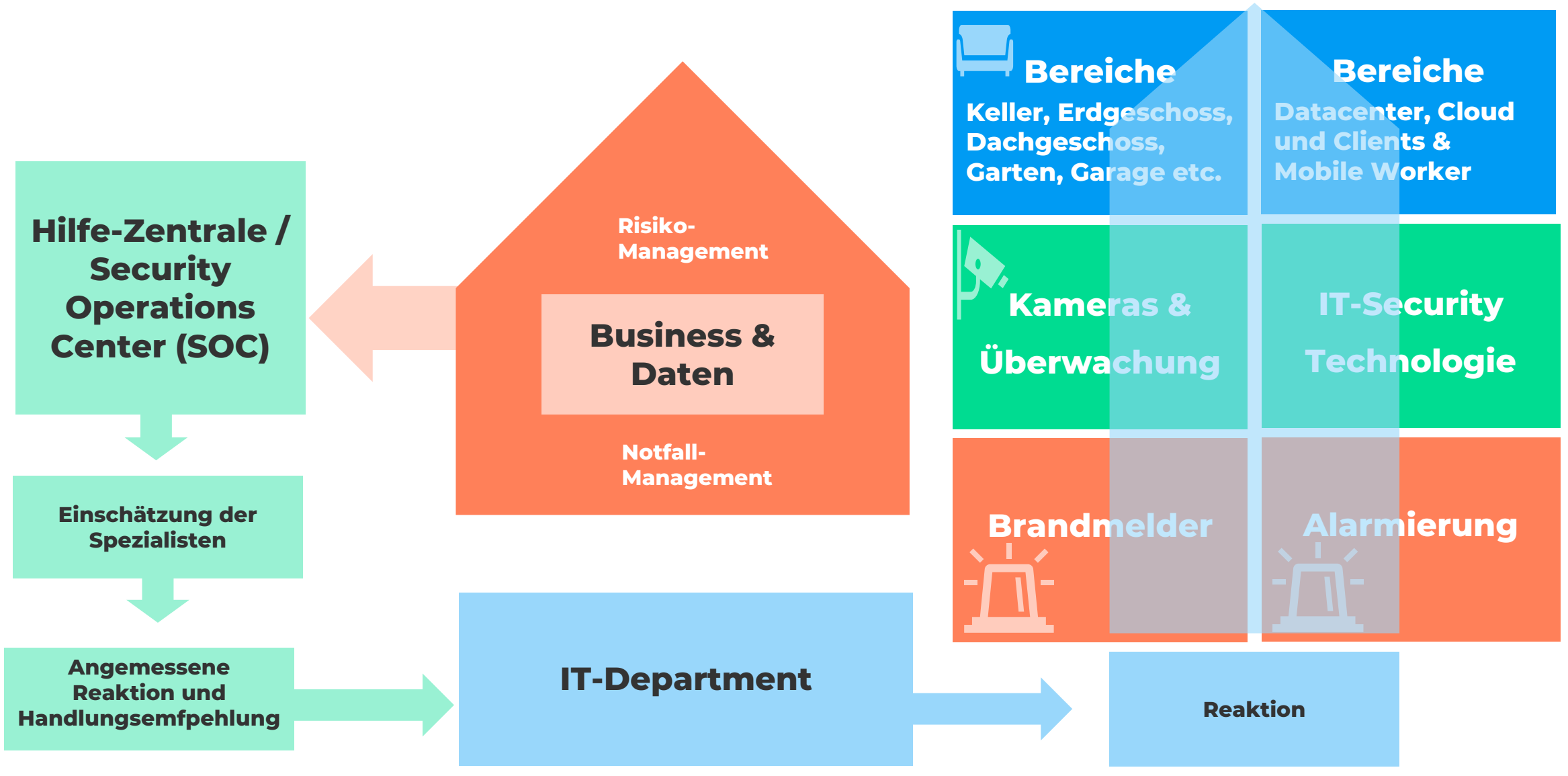
IT-Security Technologie

Brandmelder

Alarmierung

Alarmierung

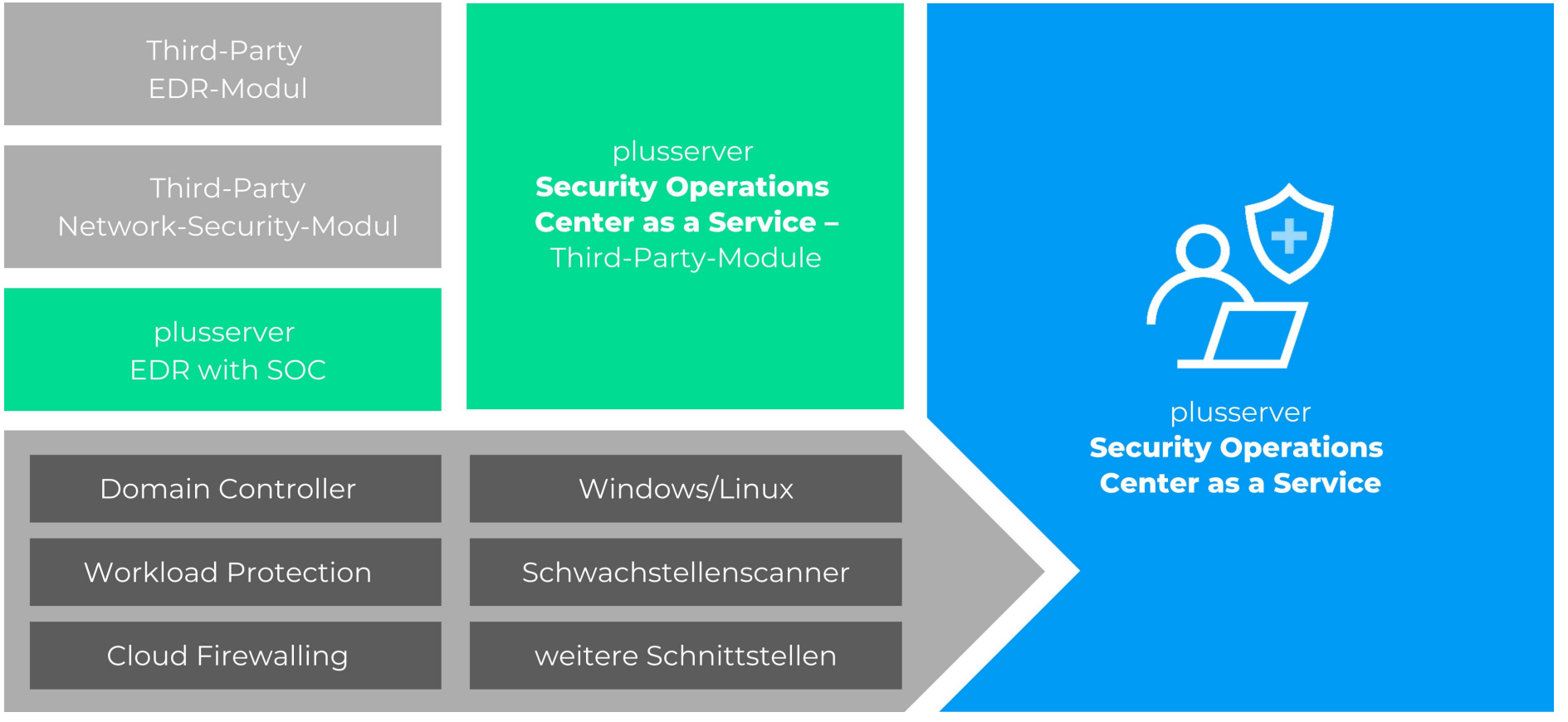
plusserver



Mit unserem modularen Aufbau zum nachhaltigen Kundenerfolg

Mehr Flexibilität und Geschwindigkeit

Einfacher und schneller Einstieg – jederzeit erweiterbar



plusserver

SOC vs. SOC as a Service

Selber machen oder als Service beziehen?

Ihre Kosten für eigene Technik und Personal

150.000 €

SIEM-Plattform

10.000 € p. a.

Wartung

>250.000 € p. a.

Analysten-Team

Kosten für das Jahr 1

>400.000 €

Kosten ab Jahr 2

>250.000 € p. a.

Unser Angebot

plusserver SOC aaS für den Mittelstand

ab 47.000,00 € p. a.

Berechnungsbeispiel:

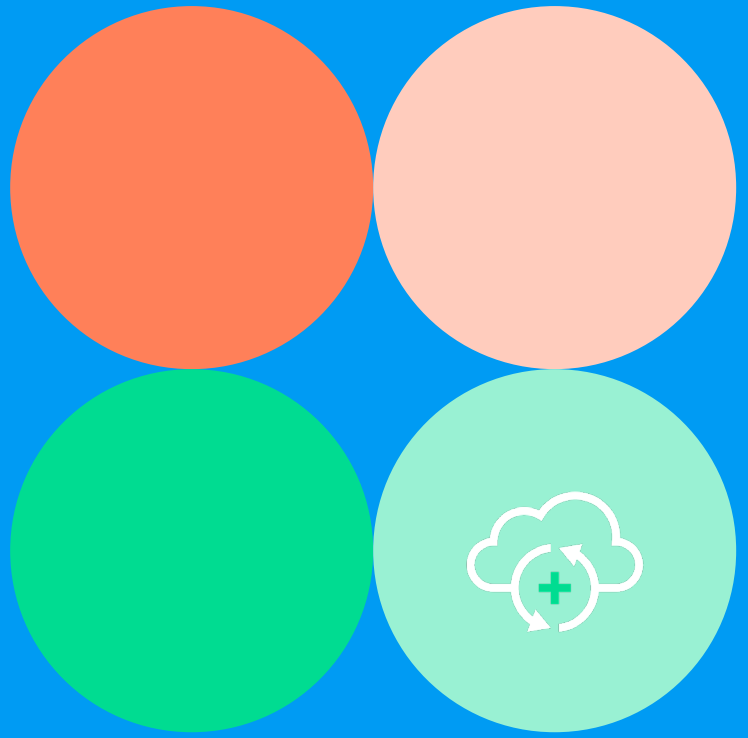
- Unternehmen mit 600 Mitarbeitenden
- Anbindung Log-Quellen des Kunden: Windows Server, Linux Server, Firewall und EDR-Plattform
- 500 Events per Second (Standard)
- Monatliche Kosten: **3.930,00 €**

plusserver

Jetzt ist es doch passiert - was jetzt?

Last line of defense mit Backup aaS

Business Continuity (BCM)



plusserver

Backup, Disaster Recovery, WORM-Technologie?

1

+ Backup hebt die Daten in verschiedenen Zeitständen auf

+ Wiederherstellung von Daten zum Zeitpunkt X

2

+ Disaster Recovery spiegelt alle aktuellen Daten in einen zweiten Standort

+ Schnelle Verfügbarkeit des letzten Datenbestandes

3

+ WORM schütz Daten vor Löschung oder Veränderung

+ Gewährleistung für Datenunveränderlichkeit

*WORM = Write Once Read Many

plusserver

Backup vs Disaster Recovery

BACKUP

Montag 11:13

Datenkopie zu festen Zeiten

Scheduler jeden Tag 23:59 (7 Tage aufheben)

Aufheben von älteren Versionen

Archiv (S3, Disk, Tape, ...)

Medienbruch

DISASTER

Montag 11:13

Replikation zu festen Zeiten

Scheduler: Alle 6 Stunden

Spiegel der aktiven Daten

Zweite Geolokation

Montag 11:13

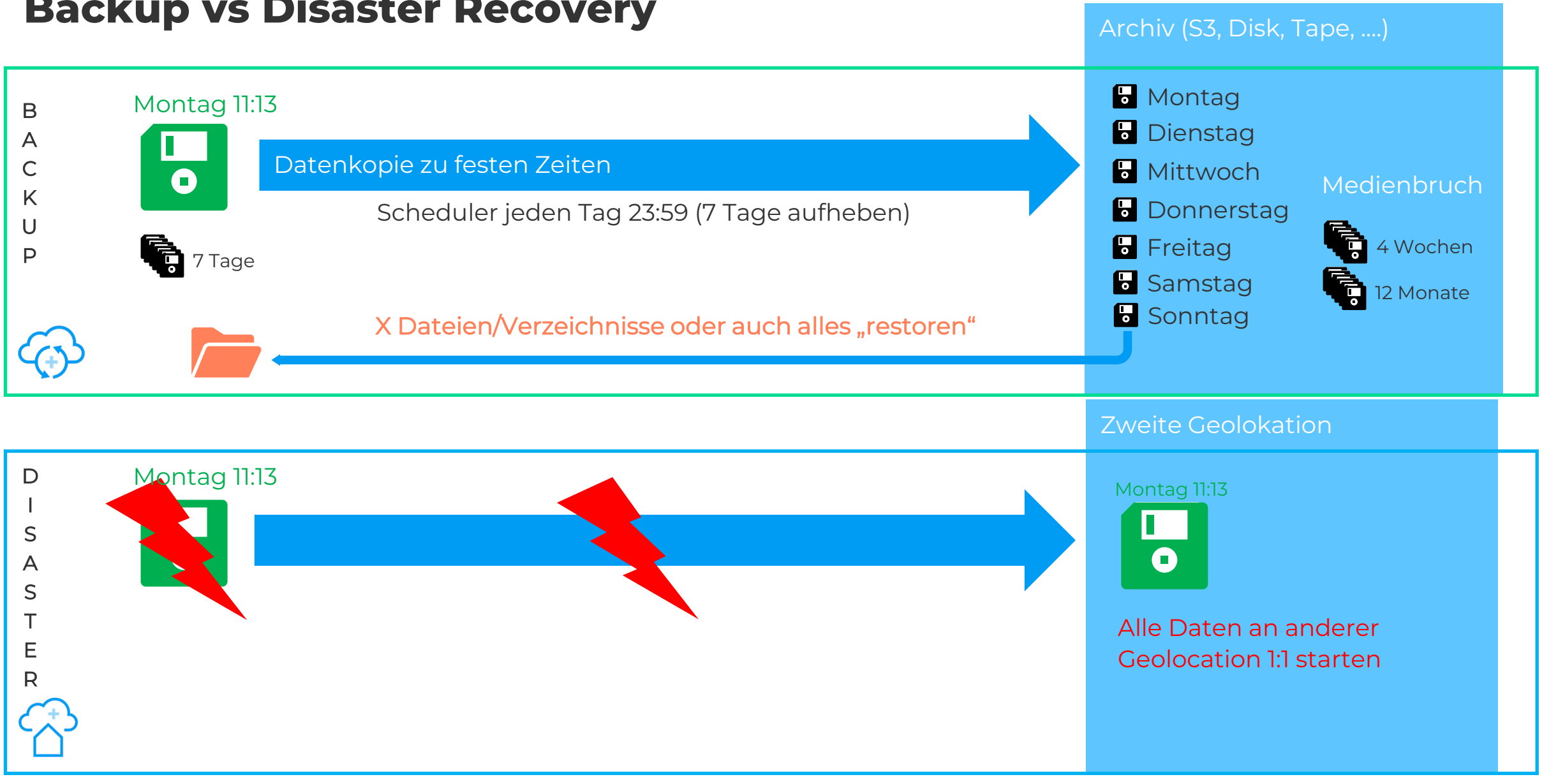
Geographische Trennung

+ unabhängige HW/SW

Alle Daten an anderer Geolocation 1:1 starten

plusserver

Backup vs Disaster Recovery

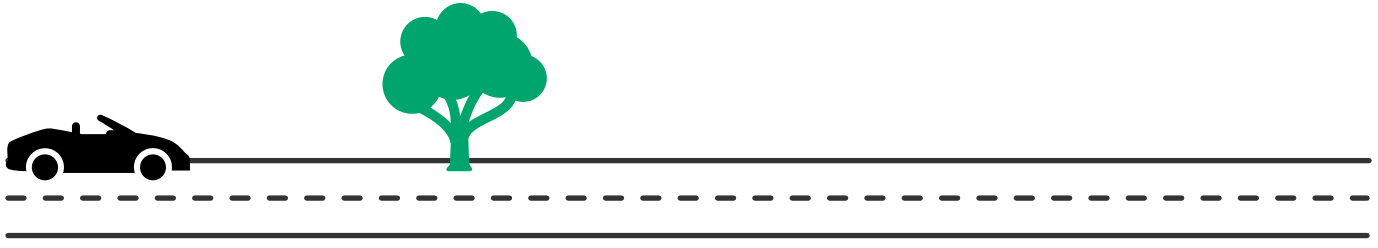


plusserver

Backup vs Disaster Recovery

BACKUP

Montag 11:13

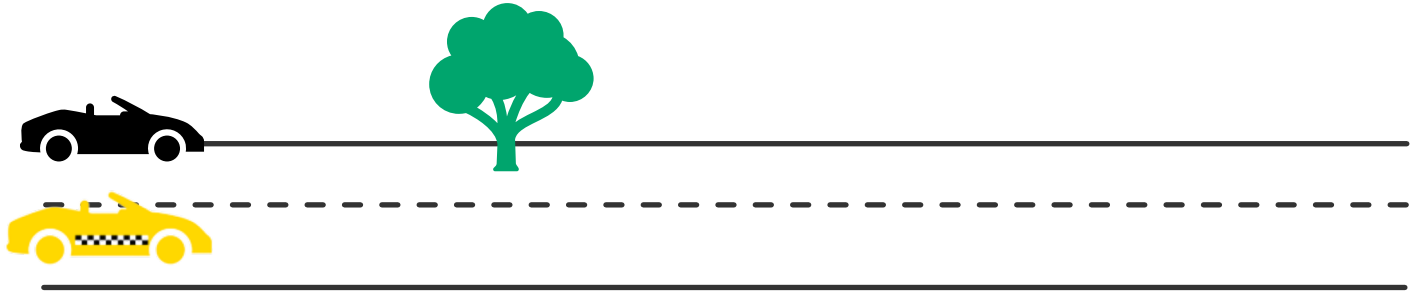


Private Garage

Montag, 23:59
Dienstag, 23:59
Mittwoch, 23:59
Donnerstag, 23:59
Freitag, 23:59
Samstag, 23:59
Sonntag, 23:59

DISASTER

Montag 11:13



Exklusiver Transportservice

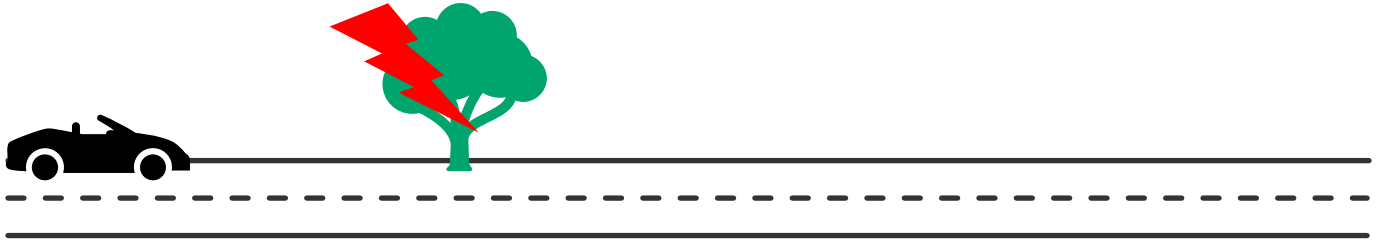
Intervall:
5 Uhr morgens
Alle 6 Stunden

plusserver

Backup vs Disaster Recovery

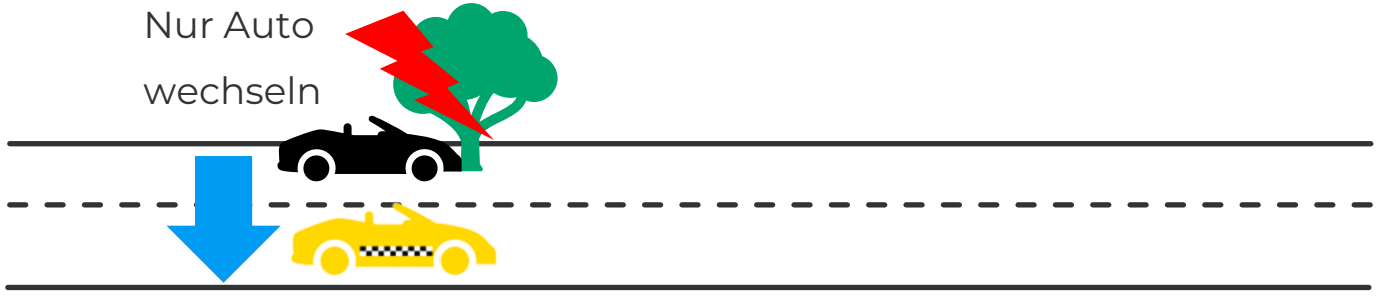
BACKUP

Montag 11:13 Montag 11:20



DISASTER

Montag 11:13 Montag 11:20



Private Garage

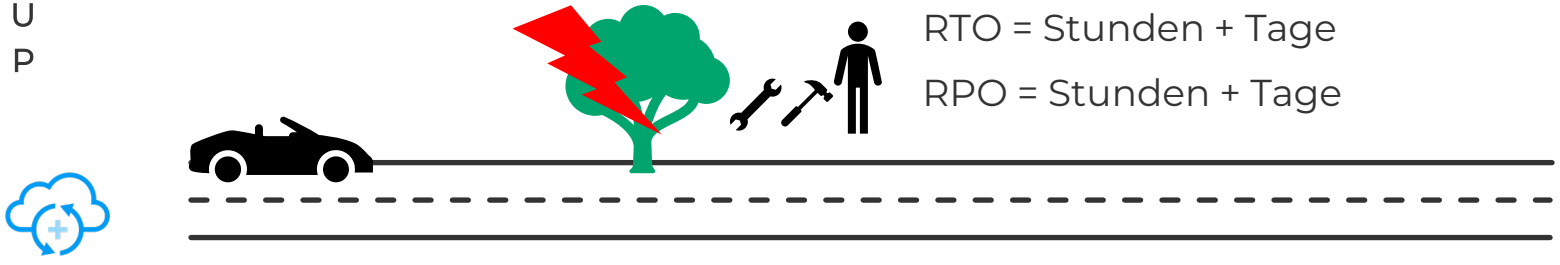
Montag, 23:59
Dienstag, 23:59
Mittwoch, 23:59
Donnerstag, 23:59
Freitag, 23:59
Samstag, 23:59
Sonntag, 23:59

plusserver

Backup vs Disaster Recovery

BACKUP

Montag 11:13 Montag 11:20 Sonntag 23:59



Wartezeit bis Auto repariert ist = RTO

Datenverlust = RPO

RTO = Stunden + Tage

RPO = Stunden + Tage

Backup

1 einzelne Datei wiederherstellen

1 einzelnen Ordner wiederherstellen

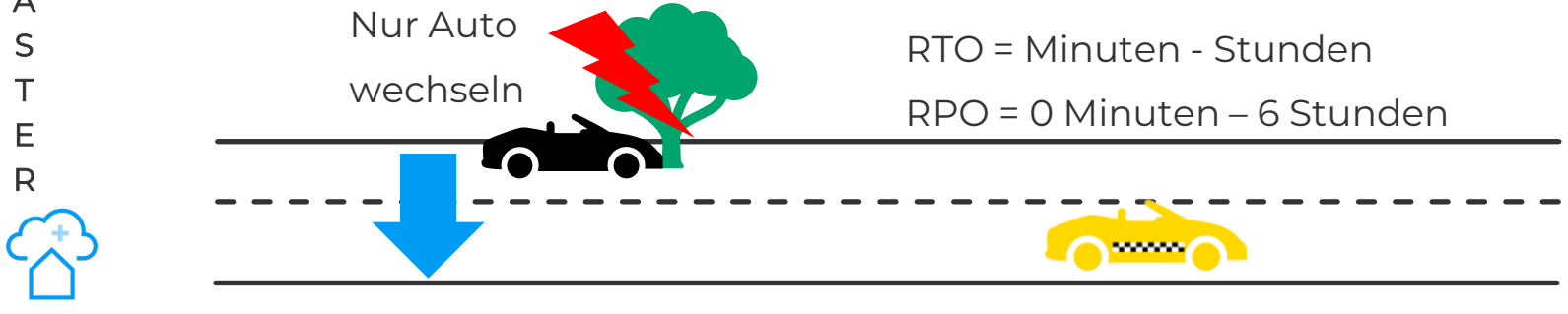
Alle Daten wiederherstellen

Vorteil: Historische Versionierung

Nachteil: Nicht sofort 1:1 wieder online

DISASTER

Montag 11:13 Montag 11:20 Sonntag 23:59



Wartezeit bis Auto repariert ist = RTO

Datenverlust = RPO

RTO = Minuten - Stunden

RPO = 0 Minuten – 6 Stunden

Disaster Recovery

Alle Daten sofort verfügbar

Komplette Daten wie vorher

Vorteil: Sofort wieder online

Nachteil: Keine historischen Daten

RTO = Recovery Time Objective
RPO = Recovery Point Objective

Was schützt mich wie?

Backupschutz vor Löschung/Verschlüsselung

Fragen:
Können die Backupdaten auch zerstört werden?

Kann ein Angreifer auf Geschäftsdaten und IT-Umgebungen auch Backupdaten verändern, verschlüsseln, löschen?

Antwort:

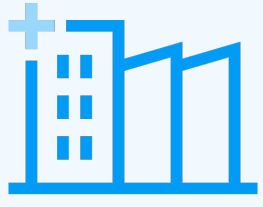
„**Ja, aber dagegen kann man sich schützen**“

+ Die Backupdaten werden täglich auf S3-Speicher kopiert
+ Die Backup-Kopie ist WORM-geschützt (S3 Object Lock) und in einem anderen Standort
+ **Abwehr** von Malware, Hackerangriffen sowie Ausfall von Rechenzentrums-Standorten

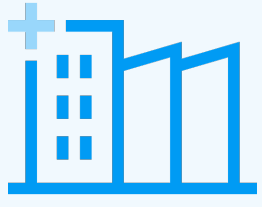
Kompatibel mit:

pluscloud open

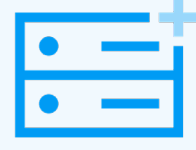
pluscloud VMware



pluscloud local



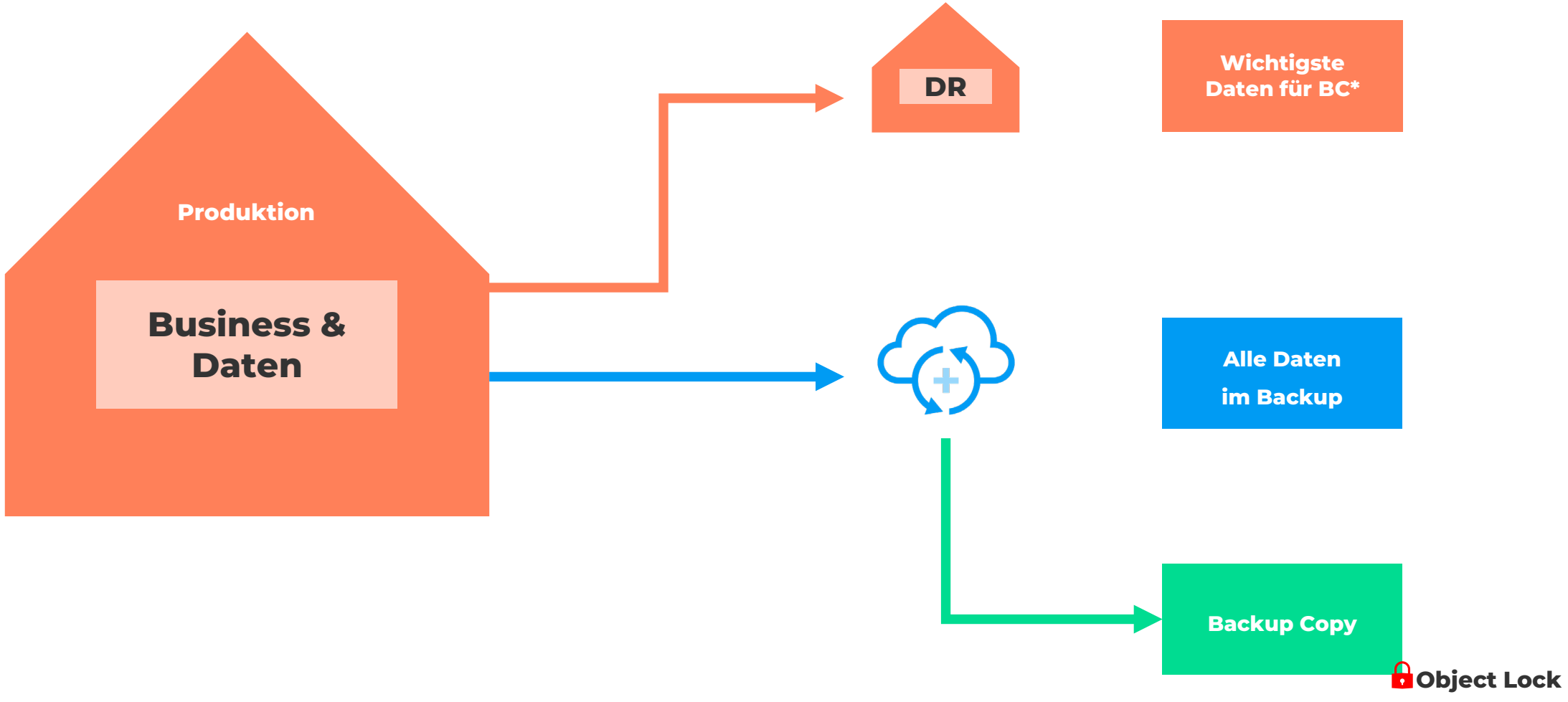
On-Premises



Dedicated Hardware

plusserver

Zusammenspiel: DR, Backup, Datenkopie, WORM



*BC = Business Continuty

Q&A

Wir helfen gerne!

Gemeinsam wachsen!

Jetzt mit der Umsetzung starten. Wir unterstützen Sie gerne.

Sie haben Fragen oder Anregungen zu unserer NIS2-Initiative? Wenden Sie sich gerne an folgende Kontakte:

Bei Fragen zur Initiative, Kommunikationsmitteln und unseren Webinaren:

partner.marketing@plusserver.com

Bei Fragen zu Produkten und technischen Details:

partner.technik@plusserver.com

Bei Fragen zu Projekten, Deal-Registrierungen und Sales-Unterstützung:

partner.sales@plusserver.com

plusserver

Vielen Dank für Ihre Aufmerksamkeit!

26. April **Agil, innovativ – und resilient**

14. Mai **A Beginner’s Guide to NIS2**

Unsere Security-Initiative wird unterstützt von

VEEAM ESET IBM