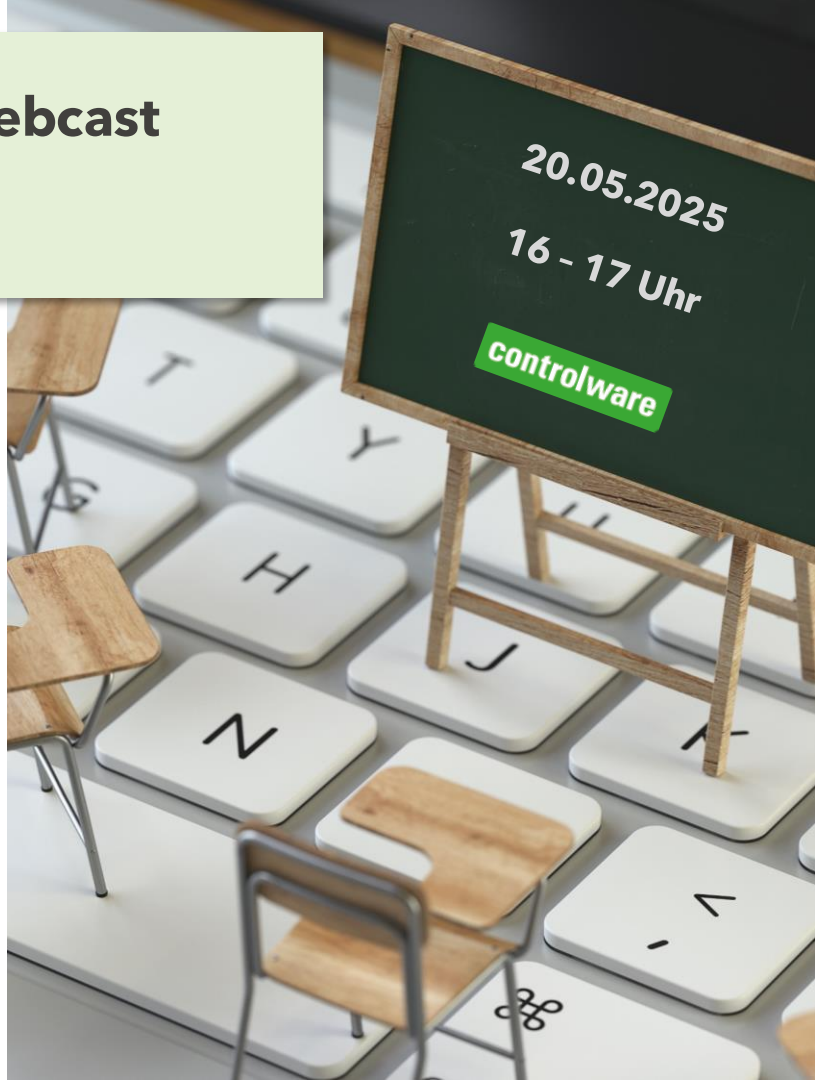
Willkommen zum Competence Webcast

Housekeeping

- Alle Teilnehmer sind stummgeschaltet
- Diese Session wird aufgezeichnet und Ihnen im Nachgang zusammen mit der Präsentation zur Verfügung gestellt
- Unter Fragen und Antworten gestellte Fragen werden am Ende des Webcast mündlich beantwortet
- Bitte nehmen Sie sich nach dem Webcast kurz für eine Bewertung unseres Webcasts Zeit



Von Pflicht zur Chance: Compliance mit DevSecOps automatisieren

Effizienzsteigerung & Compliance durch smarte Lösungen

Guillermo Canedo Otero, Controlware GmbH, Technical Consultant
Giuliano Di Biase, Controlware GmbH, Technical Consultant

Cyberbedrohungen auf dem Vormarsch

controlware

Risikobarometer: Deutsche Unternehmen plagt die Cyberangst

Ransomware, Hackerangriffe, Datenlecks und Ähnliches sehen deutsche Unternehmen als größte Bedrohung für ihr Geschäft.

(Bild: aslysun/Shutterstock.com)

15.01.2025, 16:50 Uhr Lesezeit: 3 Min. | iX Magazin

Von Axel Kannenberg

Quelle: Heise.de, 2025

Nato befürchtet neue schwere Sabotageakte und Cyberangriffe

Das Ausmaß der Schäden durch russische oder chinesische Angriffe auf Infrastruktur in Nato-Ländern nimmt langsam aber stetig zu. Das Bündnis will nun reagieren.

(Bild: Harinnita Detta/Shutterstock)

04.12.2024, 12:54 Uhr Lesezeit: 4 Min.

Von dpa

Quelle: Heise.de, 2024

Ransomware-Statistik: Angriffe legen über die Hälfte der betroffenen Firmen lahm

Ransomware-Angriffe bedeuten für deutsche Unternehmen viel Arbeit und Betriebsausfälle. Nur ein Bruchteil der Betroffenen bekommt alle Daten zurück.

Ransomware-Nachricht auf einem Laptop. (Bild: Bild erstellt mit KI in Bing Designer durch heise online / dmk)

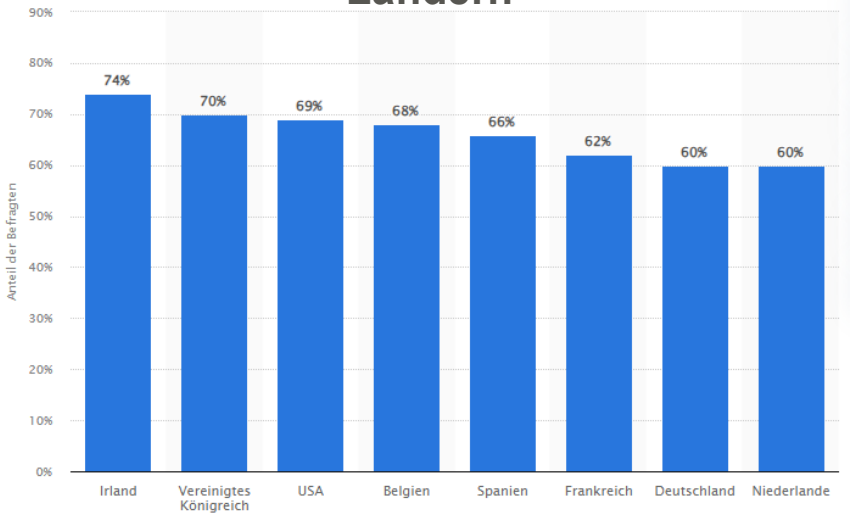
28.01.2025, 10:55 Uhr Lesezeit: 4 Min. | iX Magazin

Von Sven Festag

Quelle: Heise.de, 2025

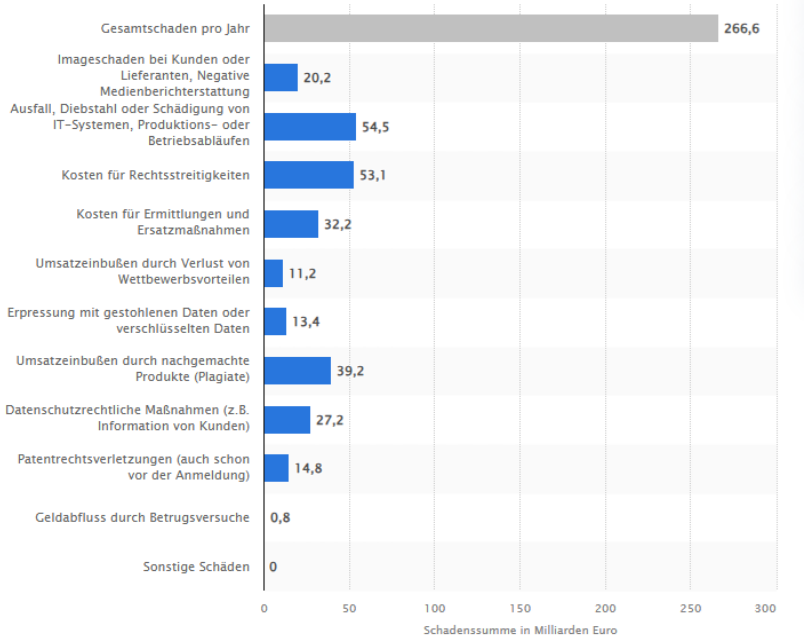
Zunahme der Cyberangriffe

Zunahme von Cyberangriffen nach Ländern



Quelle: Statista, 2024

Cyberangriffsschäden in Deutschland



Quelle: Statista, 2024

Compliance als Hilfsmittel

controlware

Compliance ist **nicht optional**!

„Einhaltung gesetzlicher, regulatorische & unternehmensinterner Vorgaben“ IDW (Institut der Wirtschaftsprüfer in Deutschland) PS 980

Beispiele:

- DSGVO
- IT-Grundschutz
- **DORA**
- **NIS2**

Umsetzungen bis Herbst 2025 – Wie ist Ihr Status?

controlware

Kommentar: Deutsche Unternehmen haben noch nicht genug Angst vor Cyberangriffen

Viele Firmen machen sich Sorgen über potenzielle Cyberangriffe. Aber trotzdem bleiben die Investitionen in IT-Sicherheit dürftig, findet Tobias Glemser.

30

(Bild: Song_about_summer/Shutterstock.com/Bearbeitung heise online)

31.01.2025, 08:05 Uhr Lesezeit: 5 Min. | iX Magazin

Von Tobias Glemser

Quelle: Heise, 2025

Der Goldstandard für die Cyber-Sicherheit europäischer Unternehmen? Mit Plattformen wie HYPERSECURE können NIS2-Anforderungen schon jetzt umgesetzt werden. (Foto: BS/Maxim, stock.adobe.com)

Die Zeit drängt: Organisationen in der EU müssen sich auf die NIS2-Richtlinie vorbereiten, die bis zum 17. Oktober 2024 in nationales Recht umgesetzt sein soll. Die deutsche Gesetzgebung ist noch nicht abgeschlossen. Doch auch wenn es noch kein verabschiedetes Gesetz gibt, können betroffene Organisationen bereits jetzt nützliche Schritte für ein aktives Risikomanagement und eine Stärkung ihrer Cyber-Sicherheit umsetzen.

NIS2 betrifft insbesondere Organisationen mit über 50 Mitarbeitern, mehr als 10 Mio. Euro Umsatz oder Organisationen, die als kritisch eingestuft sind – insgesamt sind es fast 40.000 in Deutschland.

Quelle: behoerden-spiegel, 2024

NIS2 für mehr IT-Sicherheit: Viele Unternehmen sind noch nicht gut vorbereitet

Lediglich ein Drittel der betroffenen rund 30.000 Unternehmen in Deutschland ist bereits gut auf das Inkrafttreten der NIS2-Richtlinie vorbereitet.

1

(Bild: iX)

26.09.2024, 11:49 Uhr Lesezeit: 2 Min. | iX Magazin

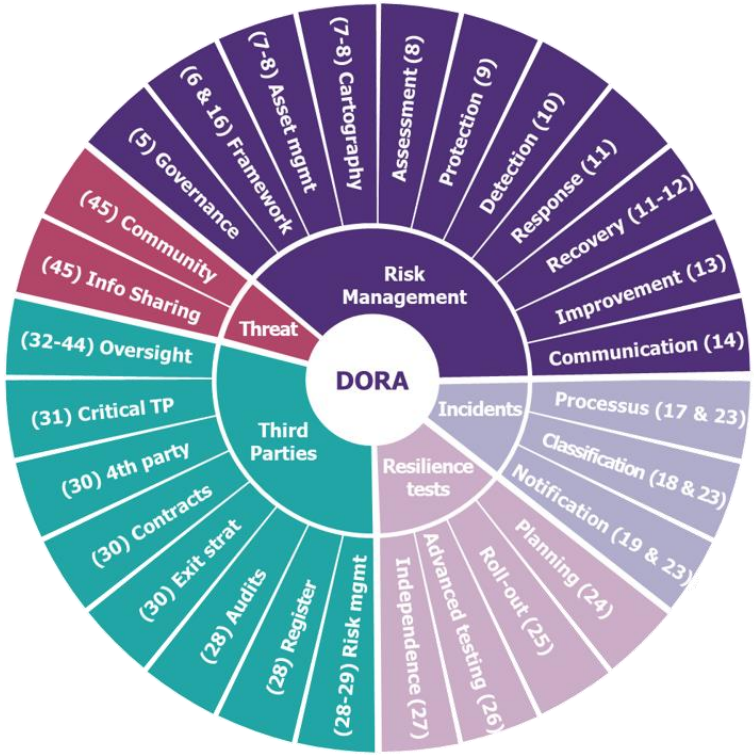
Von Dr. Oliver Diedrich

Quelle: Heise, 2025

Überblick DORA

DORA (Digital Operational Resilience Act)

- **Risikomanagement** und Überwachung
- Sicherstellung von **Geschäftskontinuität**
- Berichterstattung und **Compliance**
- Incident Response und **Incident Management**
- **Sicherheitsprüfungen** und Penetrationstests

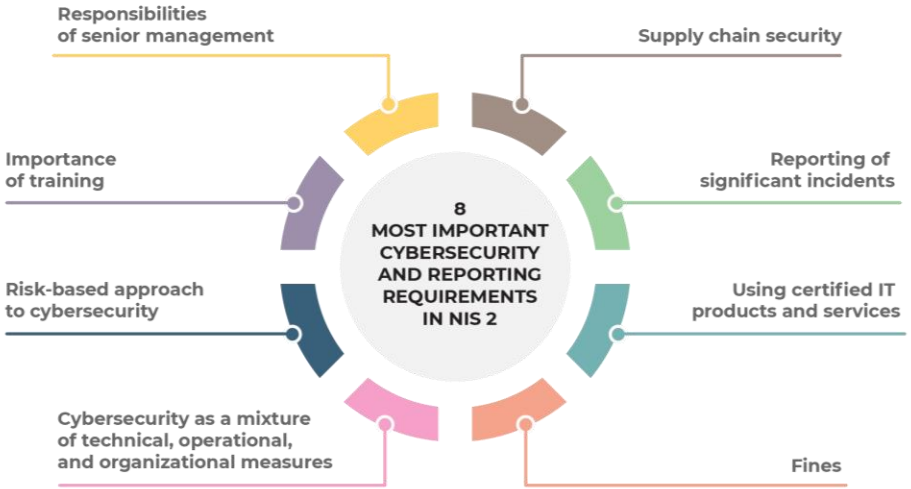


Quelle: RiskInsight, 2023

Überblick NIS2

NIS2 (Network and Information Security Directive 2)

- Erweiterte Anforderungen an Cybersicherheitsmaßnahmen
  - **Erkennung** und **Reaktion** auf Sicherheitsvorfälle
  - Patch- und Update-Management
  - Identitäts- und Zugriffsmanagement (**IAM**)
- Verpflichtung für kritische und **wichtige Sektoren**
  - mittelgroße und große Unternehmen (öffentlich und privat)
- Strengere Berichtspflichten und Compliance-Anforderungen
  - **Risikomanagement** & Compliance
  - Sicherheitsüberwachung und **Log-Management**
  - Backup- und Wiederherstellungsprozesse



Quelle: Advisera, 2024

Herausforderungen bei der Umsetzung

controlware

Technische Maßnahmen NIS2

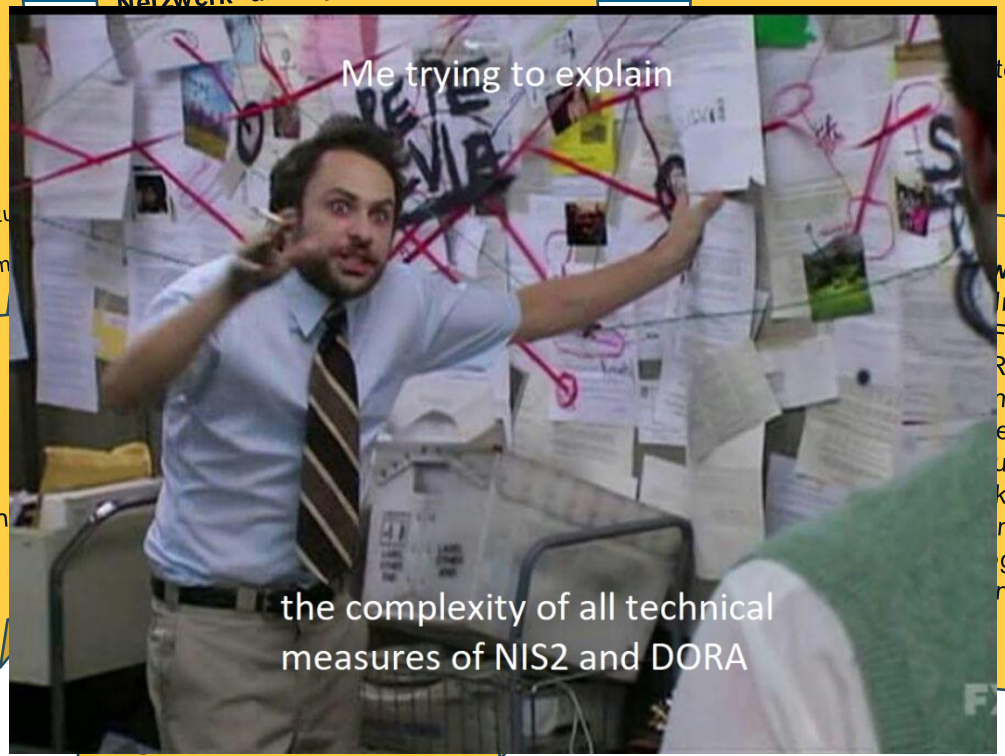
Implementierung eines Risikomanagements:
- Durchführung Risikoanalysen zur Identifizierung von Schwachstellen
- Erstellung eines Risikobehandlungsplans zu Priorisierung und Umsetzung von Maßnahm

Netzwerk- und Systemsicherheit:

Multifaktor-Authentifizierung:

teme,

Physische Sicherheit:
- Einrichtung von Zugangskontrollen für Anlagen und kritische Infrastrukturen
- Implementierung von Überwachungssystemen für Temperatur und Luftfeuchtigkeit in kritischen Bereichen

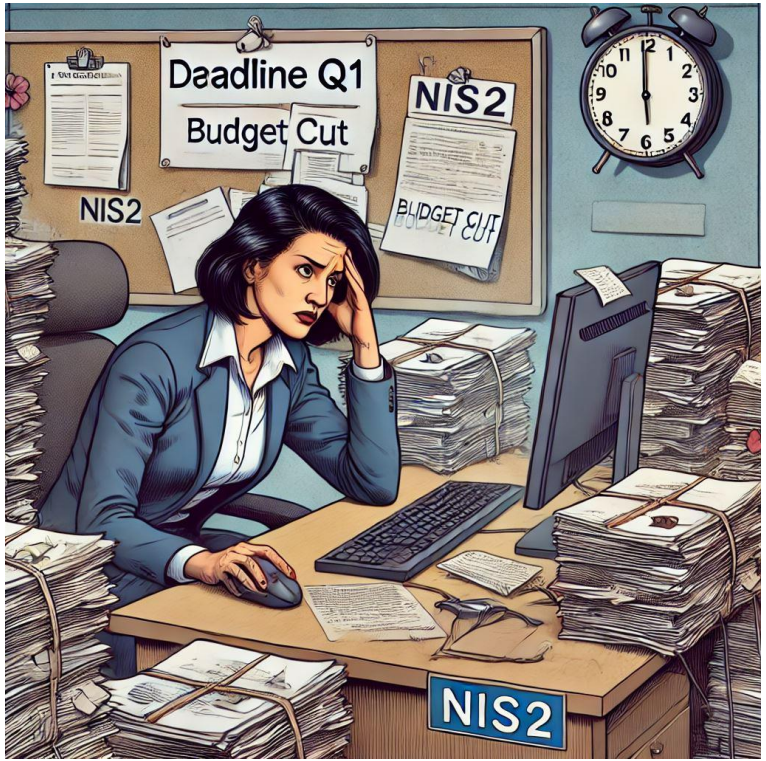


wachung und Erkennung:
Installation von KI-gestützten Frühwarnsystemen für Ransomware-Angriffe
mplementierung von KI-estützter Verhaltensanalyse ur Erkennung verdächtiger ktivitäten
nführung von Monitoring- und gging-Systemen zur ntinuierlichen Überwachung

Herausforderungen bei der Umsetzung

De Facto

- **Hohe Komplexität** der Compliance-Anforderungen
- **Zeitaufwändige** und **fehleranfällige** manuelle Prozesse
- Schwierigkeiten bei der kontinuierlichen **Überwachung** und **Berichterstattung**
- Integration neuer **Sicherheitsvorgaben** in bestehende IT-Landschaften



Herausforderungen bei der Umsetzung

controlware

Das liebe Geld

Hohe Kosten bei der Umsetzung

NIS2 verschlingt Budgets für Security und Recruiting

02.01.2025 · Quelle: Pressemitteilung · 3 min Lesedauer ·

Die Umsetzung von NIS2 scheint sich in vielen Unternehmen als schwierig zu gestalten. Grund dafür sind einer Umfrage von Veeam hohe Kosten. Zudem wirkt sich NIS2 negativ auf andere Budgets aus.

Unter den hohen Kosten bei der Umsetzung von NIS2, leiden die Budgets für IT-Security und Personalbeschaffung.
(Bild: KI-generiert)

Quelle: security-insider, 2025

„Besonders besorgniserregend ist die Tatsache, dass Mittel aus der Personalbeschaffung und Notreserven abgezweigt werden. NIS2 sollte nicht als Krise behandelt werden, doch ein Viertel der Unternehmen scheint dies so wahrzunehmen.“ (Edwin Weijdema, Field CTO EMEA bei Veeam)

Herausforderungen bei der Umsetzung

controlware

Lösung: AUTOMATISIERUNG!

The Role of IT Automation in Reducing Operational Costs for Enterprises

Geeta Malhotra
Chief Operating Officer at WalkingTree Resources Pvt. Ltd.

12. Dezember 2024

In today's fast-paced business world, enterprises are constantly looking for ways to improve efficiency and reduce costs. One powerful solution that has gained tremendous traction is **IT automation**. By streamlining repetitive tasks, optimizing workflows, and improving overall system management, IT automation is playing a pivotal role in reducing operational costs for businesses across industries. In this article, we'll explore how IT automation can drive cost savings and enhance operational efficiency.

Quelle: Greta Malhotra, 2024

Prozessautomatisierung: Die smarte Lösung um Zeit und Kosten zu sparen

von Julian Funke | 17.07.2023 | Prozessautomatisierung

Quelle: IT-P, 2023

How Infrastructure as Code (IaC) Can Help Your Organization Reduce Costs

Reduce IT costs, boost efficiency, and accelerate deployment with Infrastructure as Code (IaC). Discover how IaC can transform your business.

StratusGrid
Jul 23, 2024

Quelle: Statusgrid, 2024

https://extraetf.com/de/news/etf-news/boersenprofi-chancen-fuer-anleger-in-corona

Automatisierung als Lösungsansatz

controlware

Vorteile der Automatisierung

- Automatisierung **reduziert** manuelle Aufgaben und **Fehlerquellen**
- Erhöht die **Produktivität** und **Schnelligkeit** der Arbeitsabläufe
- Ermöglicht den Fokus auf **wertschöpfende** Tätigkeiten

Automatisierung als Lösungsansatz

controlware

Vorteile der Automatisierung

- Echtzeit-Überwachung ermöglicht **sofortige Erkennung** von Bedrohungen
- Automatisierte Reaktionen **minimieren Verzögerungen**
- **Verstärkter Schutz** vor Cyberangriffen und Systemausfällen

Automatisierung als Lösungsansatz

controlware

Vorteile der Automatisierung

- **Automatisierte Protokolle** bieten vollständige Dokumentation
- Erleichtert **Audits** und Compliance-Kontrollen
- **Transparenz** in allen Arbeitsprozessen

Automatisierung als Lösungsansatz

controlware

Vorteile der Automatisierung

- **Reduzierung von Arbeitskosten** durch weniger manuelle Compliance-Checks
- Effizientere **Ressourcennutzung**
- Langfristige **Einsparungen** durch weniger Fehler und Ausfälle

Automatisierung als Lösungsansatz

controlware

Vorteile der Automatisierung

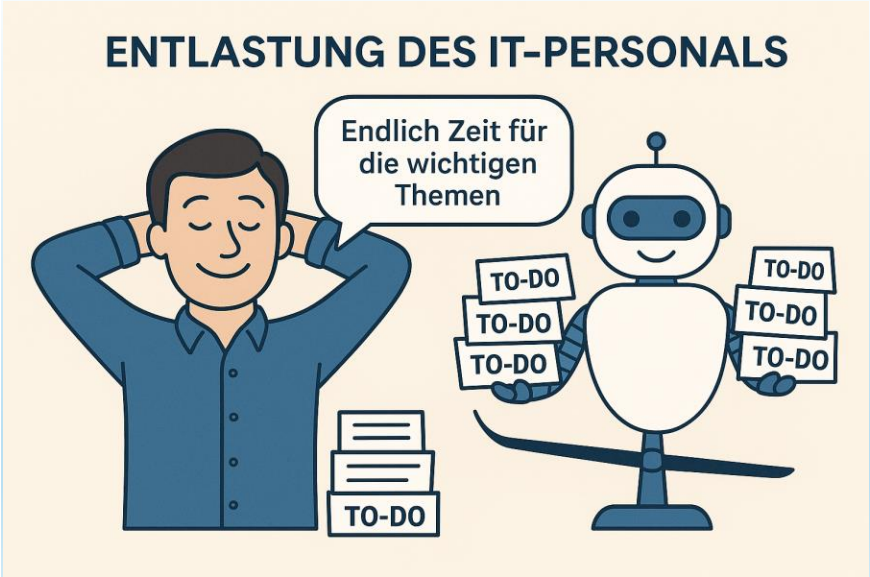
- Automatisierte Systeme können problemlos **mitwachsen**
- **Flexibilität** bei der Anpassung an neue Anforderungen und Märkte
- Leichte **Integration** von zusätzlichen Prozessen

Automatisierung als Lösungsansatz

controlware

Vorteile der Automatisierung

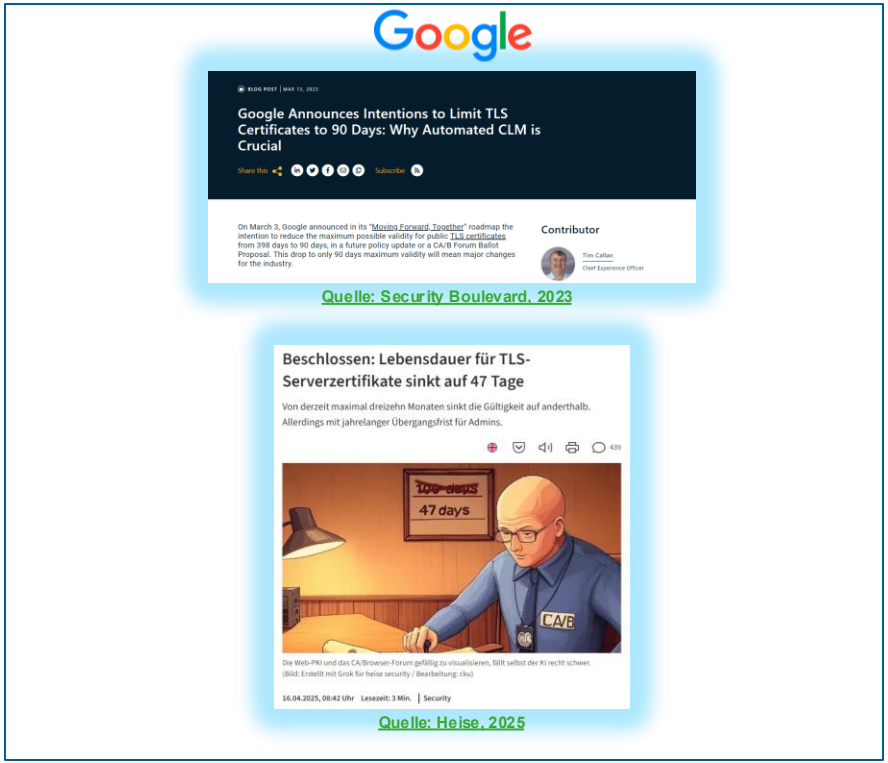
- Automatisierung von Routineaufgaben **reduziert den Druck** auf IT-Teams
- IT-Mitarbeiter können sich auf **strategische Aufgaben** konzentrieren
- **Weniger manuelle Eingriffe** bei der Fehlerbehebung



Automatisierung als Lösungsansatz

controlware

Vorteile der Automatisierung: Aktuelles Beispiel



Join at slido.com
#CW0525

Welche dieser Chancen haben Sie in Ihrem Unternehmen bereits identifiziert – aber noch nicht gelöst?

Kernprinzipien

- **Automatisierung** statt manuell (wenn möglich)
- **Sicherheit** & **Compliance** by Design
- Frühzeitige Einbindung von Security-Cheks (**Shift Left**)
- Transparenz & **Monitoring**
- **Kollaboration** über Teams hinweg

Ergebnisse: Schneller, sicherer, zuverlässiger Software-Delivery-Prozess

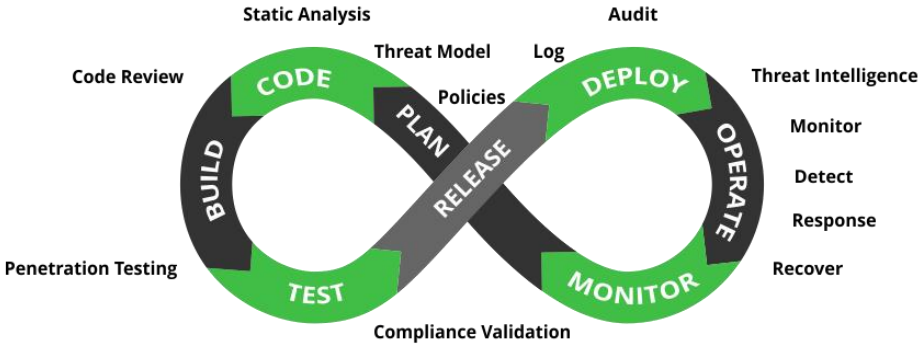
DevSecOps & Compliance

controlware

Wie passt das zusammen?

- Kontinuierliche **Pipelines** und automatisierbare **Workflows**
- Compliance als **automatisierbares Regelwerk**
- Durch Integration von **Policies**, **Scans** und **Monitoring** wird Compliance „mitgeliefert“

Ziel: „**Compliance by Default**“ – ohne Geschwindigkeit zu opfern



Quelle: Jfrog DevSecOps Pipeline

controlware

Welche Prozesse können automatisiert werden?

Sicherheit

- **Bedrohungserkennung** und **Incident Response** (SIEM, SOAR)
- Kontinuierliche Sicherheitsprüfungen**, Audit Logs & Alerting**
- **Vulnerability** und **Patch-Management**
- Protokollierung und **Berichterstattung**
- **Identitäts**- und **Zugriffsmanagement** (IAM, Zero Trust)

controlware

Welche Prozesse können automatisiert werden?

Infrastruktur

- **Serverbereitstellung**: Automatisches Einrichten und Konfigurieren
- **Konfigurationsmanagement**: Automatische Verwaltung
- **Cloud-Bereitstellung**: Automatisierte Einrichtung von Cloud-Ressourcen
- **Netzwerkbereitstellung**: Automatisches Setup von Routern und Switches
- **Anwendungs-Deployment**: Schnelles und konsistentes Ausrollen

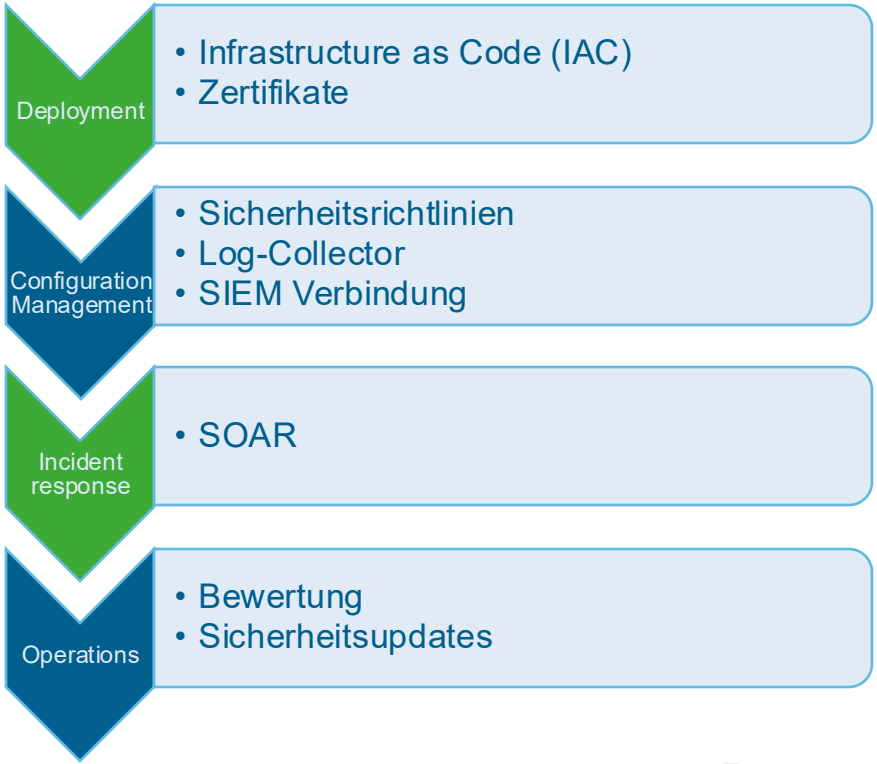
Praxisbeispiele & Best Practices

controlware

Beispiel 1: Automatisierte Bereitstellung einer VM & SIEM-Integration

Automatisierungsschritte:

1. Automatisiertes Deployment der VM über **Infrastructure-as-Code**
    1. Zertifikatsverwaltung
2. Configuration Management
    1. Vorkonfigurierte Sicherheitsrichtlinien
    2. Installation und Konfiguration eines **Log-Collectors**
    3. Verbindung zum zentralen **SIEM** für Überwachung und Analyse
3. Integration mit SOAR für **Incident Response**
4. Regelmäßige **Sicherheitsupdates** für die VM



Praxisbeispiele & Best Practices

controlware

Beispiel 2: Security durch **HashiCorp Vault** in DevSecOps

1. **Plan:** Anforderungen & Zugriffsrichtlinien definieren
2. **Code:** Keine Secrets im Code
3. **Build:** Build-Systeme beziehen Secrets direkt & temporär Missbrauchsrisiko minimiert.
4. **Test:** Temporäre Secrets für mehrere Umgebungen
5. **Release:** Vault schützt Release-Pipelines & bietet vollständige Audit-Logs zur Nachverfolgung.
6. **Deploy:** Sichere Bereitstellung von Secrets bei Deployments; Kubernetes-Integration möglich.
7. **Operate:** RBAC & dynamische Secrets sichern Betriebsprozesse; reduzierte Angriffsfläche
8. **Monitor:** Überwachung von Secret-Zugriffen; Anbindung an Monitoring- & SIEM-Systeme.

Welche der folgenden Themen bereiten Ihnen die meisten Kopfschmerzen?

Competence Center DevOps & Automation

controlware

Themen, Lösungen und Leistungen

Technologie-Unabhängigkeit: Data Center & Cloud

Infrastructure-as-Code (IaC)	Infrastrukturbetrieb mit den Methoden der Software-Entwicklung
CI/CD-Pipeline & Toolchain	Aufbau und Optimierung der automatisierten Anwendungsbereitstellung
Secret Management	Sichere Speicherung von Zugangsdaten, Tokens, Zertifikaten (PKI-Management) und Schlüsseln
Container Technologien	Anwendungen in geschlossenen und wiederverwendbaren Einheiten – Microservices und „Immutable Infrastruktur“
Applikations Modernisierung	Migration vorhandener Anwendungslandschaften in skalierbare und serviceorientierte Umgebung – „Cloud-native“

Consulting (T&M)

Projekte (T&M)

Managed Service (CCS)

Managed Service (COS)

HashiCorp Terraform

HashiCorp Packer

ANSIBLE

cloud-init

GitLab

Jenkins

GitHub

JFrog ARTIFACTORY

HashiCorp Vault

HashiCorp Boundary

HashiCorp Nomad

docker

RANCHER BY SUSE

kubernetes

OPENSHIFT by Red Hat

HashiCorp Consul

Cons. Proj. CCS COS

Secret Management als Controlware Managed Service

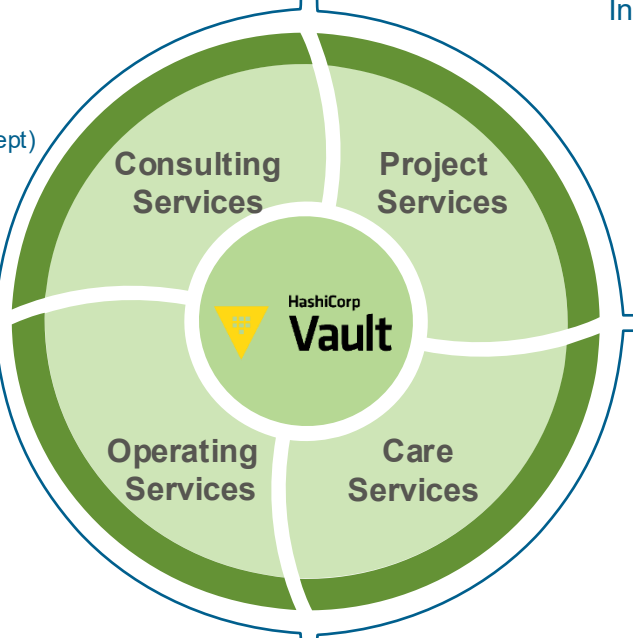
Controlware begleitet Kunden von der **Idee** bis zur erfolgreichen **Umsetzung** – und **darüber hinaus**.

Consulting

- Anforderungs- und Marktanalyse
- Strategieberatung und Konzeption
- Design- und Machbarkeitsstudien
- Machbarkeitsnachweis (Proof-of-Concept)
- Konzept- /Designreviews
- Entscheidungsvorlagen
- Innovationsworkshops

Projekte

- Installations- und Migrationskonzepte
- Projektmanagement / -controlling
- Remote- und On-Site-Installation
- Internationale Projekte
- Staging
- Produktivsetzung (Use-Cases)
- Schulungen



Managed Service (COS)

- 24/7 Managed Services
- Infrastructure Operating Services
- Cyber Defence Services
- Managed Cloud Services

Wartung (CCS)

- 24/7 Service-Organisation
- Service Desk
- Remote Diagnose
- Expertenhotline

Bild-Quelle: https://www.it-daily.net/it-management/digitalisierung/fuenf-prio[illegible]n-fuer-einen-stoerungsfreien-it-betrieb

CALL TO ACTION!

Wie geht es weiter?

- **Kontakt:**
  Über Ihren Account-Manager, oder per Mail
  cccloud.devops@controlware.de

- **Wie geht es weiter? – Analyse, Beratung, PoC…**


Q&A
Fragen ?


controlware
controlware
Vielen Dank für Ihre Aufmerksamkeit!

…wie geht es weiter?

Controlware Veranstaltungen: IT – Aktuell & Informativ

Webcast

24.06.25, 16:00 – 17:00 Uhr

Sicher verbunden: Wie OPSWAT IT und OT vereint –

und damit Sicherheitsanforderungen und regulatorische Vorgaben in der Praxis effektiv umsetzt.

Erfahren Sie, wie Sie mit den Lösungen unseres Partners OPSWAT und den Controlware Dienstleistungen unter anderem KRITIS-Anforderungen zuverlässig erfüllen.

Webcast

15.07.25 16:00 – 17:00 Uhr

Private 5G – Was steckt wirklich dahinter und warum ist es gerade jetzt relevant?

Im gemeinsamen Webcast mit Alcatel-Lucent Enterprise erfahren Sie, wie Unternehmen, unabhängig von Größe und Branche, durch den Aufbau eines eigenen 5G-Netzes Innovationspotenziale erschließen und sich entscheidende Wettbewerbsvorteile sichern können.

Präsenz

16.-17.09.25

Security Day 2025, Congress Park Hanau

+ Über 40 Fachvorträge
+ Hochkarätige Keynote Speaker
+ Partnerausstellung mit über 25 führenden Security-Herstellern
+ Fachkonferenz mit über 500 Teilnehmern

Anmeldung & weitere Informationen unter: www.controlware.de/termine