TA Triumph-Adler
The Document Business
A KYOCERA GROUP COMPANY

Ganzheitliche IT-Sicherheitslösungen für Ihr Unternehmen

Bundesdruckerei und TA Triumph-Adler

Zwei starke Partner für Ihre IT-Sicherheit

Konsequenzen des digitalen Wandels.

Unternehmen agieren in einem Spannungsfeld, das durch vielfältige Kundenbedürfnisse, neue gesetzliche Regelungen sowie zunehmende Cyberangriffe geprägt ist. Dies erfordert eine kontinuierliche Überprüfung und Anpassung von Strukturen, Prozessen, Technologien und Services, um Ihre IT-Sicherheit immer wieder auf den neuesten Stand zu bringen.

Die Kooperation zwischen TA Triumph-Adler und der Bundesdruckerei bietet Ihnen maßgeschneiderte Beratungsleistungen zu allen Themen der Digitalisierung und IT-Sicherheit. Dies umfasst auch die Unterstützung bei der Umsetzung der gesetzlichen Vorgaben für Unternehmen mit höchsten Sicherheitsansprüchen.

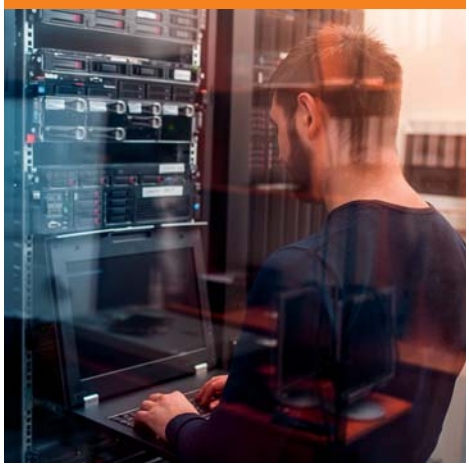
Mit dem digitalen Wandel wachsen die Anforderungen an die IT-Sicherheit – sind Sie bereit?

54 %

aller Unternehmen hatten in den vergangenen 24 Monaten einen konkreten IT-Sicherheitsvorfall. *

37 %

nutzen bereits eine externe Beratung zur Definition und Umsetzung ihrer IT-Sicherheitsstrategie.*



18 %

verfügen trotzdem bislang nicht über eine eigene IT-Sicherheitsstrategie.*

*Quelle: Studie IT-Sicherheit, Bundesdruckerei

Gut für Sie aufgestellt:
TA Triumph-Adler und die Bundesdruckerei

Innerhalb der vergangenen Jahre hat sich die Bundesdruckerei von einem Hersteller von Pässen, Ausweisen, Banknoten & Co. zu einem führenden Anbieter von Hochsicherheitstechnologien gewandelt. Im Fokus stehen heute die sichere digitale Kommunikation sowie das Management und die Anwendung sicherer Identitäten von Personen und Daten, Prozessen und Systemen.

Sowohl die Berater der Bundesdruckerei als auch die Experten von TA Triumph-Adler verfügen über fundierte Projekterfahrung, langjährige Expertise und tiefgehende Technologiekenntnisse. Nutzen Sie diese doppelte Kompetenz für die Umsetzung individueller Lösungen, die Ihren spezifischen Anforderungen gerecht werden.

Gesetzliche Rahmenbedingungen – und die Konsequenzen für Ihr Unternehmen.

Seit den Schlagzeilen über gehackte Großkonzerne oder Angriffe auf öffentliche Institutionen bis hin zum Bundestag ist jedem klar: Die digitale Transformation hat das Thema IT-Sicherheit neu definiert. Das neue **IT-Sicherheitsgesetz** soll den Herausforderungen der fortschreitenden Digitalisierung und der zunehmenden Vernetzung unterschiedlichster Organisationen begegnen.

Neue Vorschriften zum Schutz der IT-Infrastruktur

Durch die zunehmende IT-Durchdringung und Vernetzung praktisch aller Lebensbereiche entstehen neben Chancen und Potenzialen auch verstärkt neue Gefährdungslagen, auf die schnell und konsequent reagiert werden muss. Die Gefahr durch gezielte Cyberangriffe betrifft staatliche Stellen ebenso wie Unternehmen, die mit besonders wertvollen Informationen umgehen. Im Fokus der gesetzlichen Neuregelungen stehen allerdings nach dem IT-Sicherheitsgesetz klar definierte

Branchen und Bereiche, die eine zentrale Bedeutung für die Gesellschaft haben: die sogenannten „Kritischen Infrastrukturen“ (kurz **KRITIS**). Betreiber dieser Anlagen müssen künftig ein Mindestniveau an IT-Sicherheit einhalten und „erhebliche“ IT-Störungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Zu den Kritischen Infrastrukturen werden folgende Bereiche gezählt:

- Energie (Elektrizität, Gas, Öl, alternative Energien)
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit (Krankenhäuser, Pharmahersteller, Labore)
- Medien und Kultur
- Wasser (Wasserversorgung und Abwasserentsorgung)
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung

Ausgenommen sind nur Kleinstunternehmen, d. h. Firmen mit weniger als 10 Mitarbeitern und weniger als 2 Millionen Euro Jahresumsatz. **Für alle anderen Unternehmen gilt: Werden sie als Kritische Infrastrukturen eingeordnet, müssen sie die neuen Anforderungen umsetzen. Bei Verstößen dagegen droht ein Bußgeld von bis zu 100.000 Euro.**

Um den Schutz Kritischer Infrastrukturen sicherzustellen, hat das Bundesinnenministerium drei strategische Ziele definiert:

1 **Prävention:** Identifikation und Vermeidung von Risiken sowie kritischen Elementen und Prozessen, die gravierende Störungen und Ausfälle von wichtigen Infrastrukturleistungen zur Folge haben könnten.

2 **Reaktion:** Folgen von gravierenden Störungen und Ausfällen durch ein effektives Notfall- und Krisenmanagement so gering wie möglich halten.

3 **Nachhaltigkeit:** Aus kontinuierlichen Gefährdungs- und Störungsanalysen resultieren Erfahrungen für die Umsetzung abgestimmter Schutzstandards.

Aufgrund der aktuellen Entwicklung ergeben sich wichtige Fragen für Sie, die wir rechtzeitig gemeinsam klären sollten:

- Sind Sie nach der Rechtslage ein Betreiber Kritischer Infrastrukturen oder haben Sie aus anderen Gründen Verpflichtungen durch das IT-Sicherheitsgesetz?
- Haben Sie einen verantwortlichen Ansprechpartner für die IT-Sicherheit im Unternehmen benannt?
- Wurde ein Informations-Sicherheits-Management-System (ISMS) installiert?
- Welche Ihrer IT-Systeme werden als „kritisch“ für die Erbringung Ihrer Dienstleistungen eingestuft?
- Welche Möglichkeiten gibt es, diese kritischen Systeme nach Stand der Technik besonders gut abzusichern?

Strategien, Tools und Maßnahmen – Ihr optimaler Weg zu mehr IT-Sicherheit.

Wie lassen sich die Herausforderungen des digitalen Wandels meistern? Als Erstes müssen von KRITIS betroffene Unternehmen für sich identifizieren, welche ihrer IT-Systeme von zentraler Bedeutung für die Erbringung ihrer Kernleistungen sind – und ob sie im Sinne des Gesetzes dann als kritisch einzustufen sind. IT-Verantwortliche sollten hierbei auch die Wechselwirkungen zwischen unterschiedlichen Systemen mit berücksichtigen.

Alles im Blick: mit dem Informations-Sicherheits-Management-System (ISMS)
Die Etablierung eines funktionsfähigen ISMS nach ISO 27001 ist der richtige Schritt, um sich einen Überblick zu verschaffen. ISMS steht für eine Aufstellung von Verfahren und Regeln in einem Unternehmen, die dazu dienen, die IT-Sicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren und aufrechtzuerhalten sowie fortlaufend zu verbessern.

Die internationale Norm **ISO 27001** ist dabei die optimale Grundlage für gesetzeskonformes Handeln und bildet die strukturelle Basis zum Schutz von vertraulichen Daten, für die Sicherstellung ihrer Integrität sowie zur Verbesserung der Verfügbarkeit von Informationen.

Eine ISO-27001-Zertifizierung gibt Ihnen einen systematischen Leitfaden an die Hand, mit dem Sie die eigenen Informationssysteme zur Unterstützung der Geschäftsprozesse unter Berücksichtigung von Compliance- und Sicherheitsaspekten planen, umsetzen, überwachen und stetig verbessern können. Zudem profitieren Sie von vielen weiteren Vorteilen:

- → Geringere Prozess- und Finanzierungskosten
- → Reduzierte Versicherungsbeiträge
- → Weniger Geschäfts- und Haftungsrisiken
- → Gesteigerte Wettbewerbsfähigkeit
- → Besseres Image in der Öffentlichkeit und bei Geschäftspartnern

Kostenlose Reifegrad-Analyse: Sind Sie bereit für die digitale Zukunft?
Die Einführung eines ISMS bringt viele Fragen mit sich. Machen Sie jetzt unter **www.triumph-adler.de/digicheck** den kostenlosen Check zur „digitalen Reife“ Ihres Unternehmens. So erfahren Sie den aktuellen Status Ihrer Unternehmensdigitalisierung und erhalten anschließend konkrete Empfehlungen für die nächsten Schritte – hin zur digitalen Transformation.

Bundesdruckerei und TA Triumph-Adler: 3 Beispiele für unsere Leistungsfähigkeit.

1 Beratungs-Workshop zur Vorbereitung der Einführung eines ISMS

Je nach Reifegrad, Ausgangssituation bzw. Herausforderung werden wir z. B. folgende Fragen gemeinsam mit Ihnen erörtern:

- Was bedeutet Digitalisierung für Ihr Unternehmen, was sind die Herausforderungen?
- Wie können Sie dabei sicher, effizient und regelkonform agieren?
- Wie können Sie aus den Herausforderungen konkrete Handlungsempfehlungen ableiten?
- Welche Lösungen benötigen Sie für die Digitalisierung Ihres Unternehmens?

Inhalte und Ziele des Beratungs-Workshops:

Reifegrad-Definition
- Check des aktuellen Sicherheitslevels
- Maßnahmenempfehlung mit Aufwandsschätzung

Awareness-Schulung Informationssicherheit
- Sensibilisierung für Gefährdungen
- „Quick Wins“ Informationssicherheit

Ziele
- Bewusstsein für IT-Sicherheit stärken
- Maßgeschneiderte Implementierung
- Individuelle Beratungsleistung

2 GoID – der Schlüssel zur sicheren Identifizierung

Sichere digitale Identitäten werden immer wichtiger, damit wirklich nur berechtigte Personen Zugang zu vertraulichen Daten und den ihnen zugewiesenen Rechten und Rollen haben. Denn der Diebstahl von Identitäten nimmt im Rahmen der Cyberattacken zu. Gleichzeitig setzen Rahmenbedingungen wie KRITIS und EU-DSGVO (siehe Infokasten rechts) auf höhere Sicherheitsstandards. Eine Zwei-Faktor-Authentifizierung mit der GoID – der Kombination aus dem Besitz der Karte und Fingerabdruck oder auch PIN – erhöht die Sicherheit Ihrer Unternehmensdaten deutlich (siehe Abb. oben).

Ihre Vorteile mit GoID:

- **„All-in-one“** – GoID sichert alle Unternehmensanwendungen rund um die Themen sichere Authentifizierung, Verschlüsselung, digitale Signatur und Bezahlen ab.
- **Hochsicher** – GoID nutzt bewährte Technologien des Personalausweises sowie Zwei-Faktor-Authentifizierung mit Biometrie.
- **Vertraulich** – Die Fingerabdruckdaten werden ausschließlich auf der Karte gespeichert und verarbeitet. Es gelangen keine biometrischen Daten in außerhalb der Karte befindliche Systeme.
- **Langlebig** – Der passive Kontaktlos-Chip schützt GoID vor physischer Abnutzung und garantiert eine lange Lebensdauer.
- **Kostensenkend** – Die Rücksetzung von Passwörtern und die Entsperrung von Nutzerprofilen beschäftigen vor allem Help-Desk-Mitarbeiter und kosten Zeit. Dieser Zeitaufwand wird durch den Einsatz der GoID deutlich reduziert.

Was bedeutet die EU-Datenschutz-Grundverordnung (EU-DSGVO) für Ihr Unternehmen?

Gilt ab Mai 2018 – jetzt Übergangsfrist nutzen!

Die DSGVO ist eine Verordnung der Europäischen Union, mit der die Regeln für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Sie ist ab Mai 2018 gültig, nach der darin geregelten Übergangsfrist kommt sie allerdings erst zwei Jahre nach Inkrafttreten zur Anwendung.

Diese Übergangsfrist sollte von Unternehmen daher dringend zur Anpassung ihrer Workflows und Prozesse genutzt werden. Denn die EU-Datenschutzbehörden können bereits unmittelbar ab Mai 2018 Sanktionen verhängen, wenn die Vorgaben nicht oder nicht ausreichend erfüllt wurden.

3 genua – seit 25 Jahren auf IT-Sicherheit spezialisiert

genua hat sich seit der Gründung im Jahr 1992 als deutscher Spezialist für IT-Sicherheit etabliert und ist ein Unternehmen der Bundesdruckerei-Gruppe. Zum Leistungsspektrum der IT-Sicherheitsexperten gehören u. a. die Absicherung sensibler Schnittstellen, die Vernetzung hochkritischer Infrastrukturen, Lösungen für die zuverlässig verschlüsselte Datenkommunikation sowie Remote-Access-Anwendungen für mobile Einsätze.

Die Sicherheitslösungen von genua:

- Netzwerksicherheit
- Absicherung KRITIS und hochsensibler Schnittstellen
- Sichere Standortanbindung
- Sichere Anbindung an die Cloud
- Sichere Anbindung mobiler Anwender und von Homeoffices
- Verschlüsselte Kommunikation via VPN (Virtual Private Network)
- Absicherung Fernwartung von Maschinen und IT-Systemen
- Absicherung Automatisierung
- Absicherung Industrial Monitoring

Ihr Unternehmen ist in der Energiebranche aktiv?

Frist bis Januar 2018!

Dann ist es höchste Zeit für Sie, aktiv zu werden. Folgende Fragen können wir dabei gemeinsam klären:

→ Gibt es noch Lücken zwischen dem, was Ihr Unternehmen bereits umgesetzt hat, und dem, was nach den Vorgaben gebraucht wird?

→ Welche weiteren Maßnahmen sind aufgrund der Risikoeinschätzung für Ihr Unternehmen geeignet und angemessen?

→ Was kann Ihr Unternehmen allein stemmen und wobei sollten Sie besser auf externe Dienstleister setzen?

IT-Sicherheit steht auch bei Ihnen ganz oben auf der Agenda?

Mit der Digitalisierung wächst die Bedeutung der IT-Sicherheit – und sie stellt somit für viele Unternehmen eine erhebliche Herausforderung dar. Wir helfen Ihnen, beides koordiniert, effizient und zielführend miteinander zu verknüpfen. Sie wünschen mehr Informationen oder suchen den Dialog? Dann nehmen Sie doch einfach Kontakt mit uns auf. Wir beraten Sie gern.

TA Triumph-Adler
The Document Business
A KYOCERA GROUP COMPANY

Über TA Triumph-Adler

Wir entwickeln für Unternehmen individuelle Prozesslösungen rund um Dokumente, Informationen und IT. Basierend auf unserem Kerngeschäft, dem Document Business, erweitern wir kontinuierlich unser Portfolio und sind mit mobilen Lösungen und Cloud-Services gleichzeitig Wegbereiter für flexible, mobile Arbeitsplätze. Effiziente und sichere Abläufe sind ein entscheidender Erfolgsfaktor für Unternehmen. Wir beraten Sie, wie Sie bei Ihren Workflows Zeit und Geld sparen können und die Sicherheit erhöhen, und unterstützen Sie bei der Umsetzung mit professionellen Hardware- und Software-Lösungen.

www.triumph-adler.de

BUNDESDRUCKEREI

Über unseren Partner: die Bundesdruckerei

Die Bundesdruckerei GmbH bietet innovative und komplette IT-Sicherheitslösungen für Unternehmen, Staaten und Behörden. Mit Technologien und Dienstleistungen „made in Germany“ schützt sie sensible Daten, Kommunikation und Infrastrukturen. Die Lösungen basieren auf der sicheren Identifikation von Bürgern, Kunden, Mitarbeitern und Systemen in der analogen und digitalen Welt. Mit einem ganzheitlichen Ansatz unterstützt die Bundesdruckerei von der Beratung über die Konzeption und Umsetzung bis hin zum Betrieb und Service.

www.bundesdruckerei.de

TA Triumph-Adler GmbH
Ohechaussee 235
D–22848 Norderstedt

Telefon: +49 40 52849-0
Telefax: +49 40 52849-120
info@triumph-adler.net
www.triumph-adler.de

Triumph-Adler
The Document Business
A KYOCERA GROUP COMPANY