komd@t

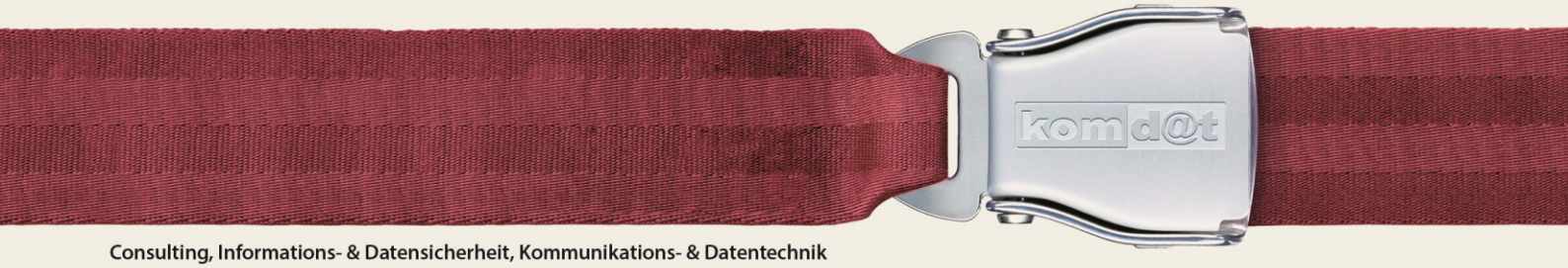
WERTE FÜR
DIE ZUKUNFT
SICHERN.

White-Paper

Datenschutz-Strategie und Netzwerk-Sicherheit im Kontext des gesetzlichen Datenschutzes nach DSG 2000 und EU-Datenschutz-Grundverordnung

Autor: Ronald Kopecky

Datum: 27.07.2016



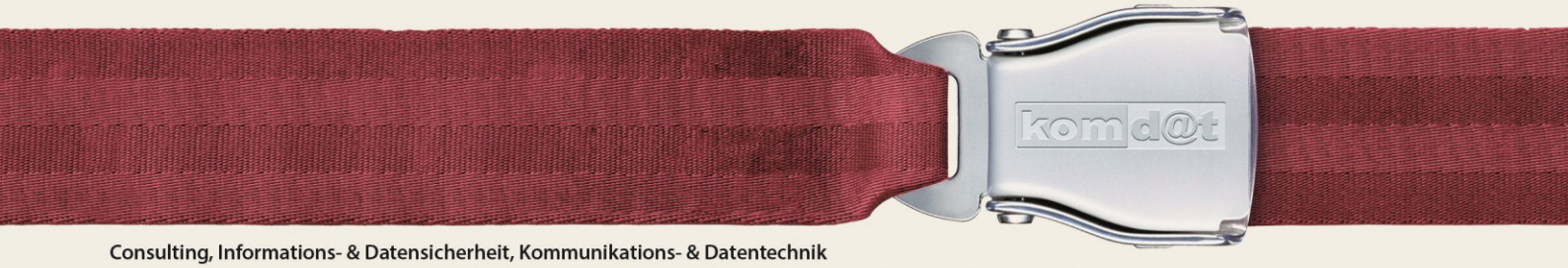
Consulting, Informations- & Datensicherheit, Kommunikations- & Datentechnik
Linzer Strasse 74, 4614 Marchtrenk / Telefon +43 (0) 7243 / 54300-0 / Fax -9 / E-mail: office@komdat.at / www.komdat.at

komd@t

WERTE FÜR DIE ZUKUNFT SICHERN.

Inhaltsverzeichnis

1. Zusammenfassung 3
   Strategische Netzwerksicherheit 3
   Ganzheitliche Netzwerksicherheit 3
   Ressourcen 4
2. Netzwerksicherheit muss flexibel sein 4
   Unternehmen und Mitarbeiter wollen maximale Flexibilität 4
   Bedrohungen ändern sich permanent 4
3. Mitarbeiter-Schulungsprogramme als fester Bestandteil 6
4. Risikoanalyse 6
5. Schatten-IT 8
6. Anomalitäten finden 8
7. Netzwerksicherheit benötigt eine Organisation 9
8. Der Datenschutzbeauftragte 9
9. KOMDAT – als kompetenter Partner 10



komd@t

WERTE FÜR DIE ZUKUNFT SICHERN.

1. Zusammenfassung

Gemäß §14 DSG 2000 haben alle Unternehmen den Schutz personenbezogener und sensibler Daten vor zufälliger oder unrechtmäßiger Zerstörung, vor Verlust, vor einer nicht ordnungsgemäßen Verwendung sowie vor der Verwendung und Einsicht durch Unbefugte zu gewährleisten.

Unternehmen stehen dabei vor einer schwierigen Herausforderung.

Ersten ist man permanenten mit sich stets weiterentwickelnden Angriffen (Viren, Malware, RansomWare, Hacker, etc.) konfrontiert und zweitens nehmen immer mehr unterschiedliche Geräte (Smartphones, Tablets, Home-Office, etc.) Einzug in den IT-Verbund.

Wie können sich Unternehmen vor diesen hoch dynamischen Risiken wirkungsvoll schützen und dadurch die gesetzlichen Pflichten erfüllen? Wir zeigen Ihnen dazu einige Ansätze.

Strategische Netzwerksicherheit

Die Vielzahl der Geräte (Smartphones, Tablets, BYOD, Home-Office, etc.) und die Komplexität der Vernetzungen (Cloud, etc.) nimmt rasant zu. Sicherheitskonzepte müssen darauf ausgerichtet sein.

Das bedeutet, dass die Netzwerksicherheit einem Plan bzw einer Strategie folgen muss und keine Angelegenheit von schnellen und punktuellen Entscheidungen sein darf.

Daten-Sicherheit im Sinne des gesetzlichen Datenschutzes nach DSG 2000 und EU-Datenschutz-Grundverordnung muss im Vordergrund stehen. Manchmal auch zu Lasten des Komforts.

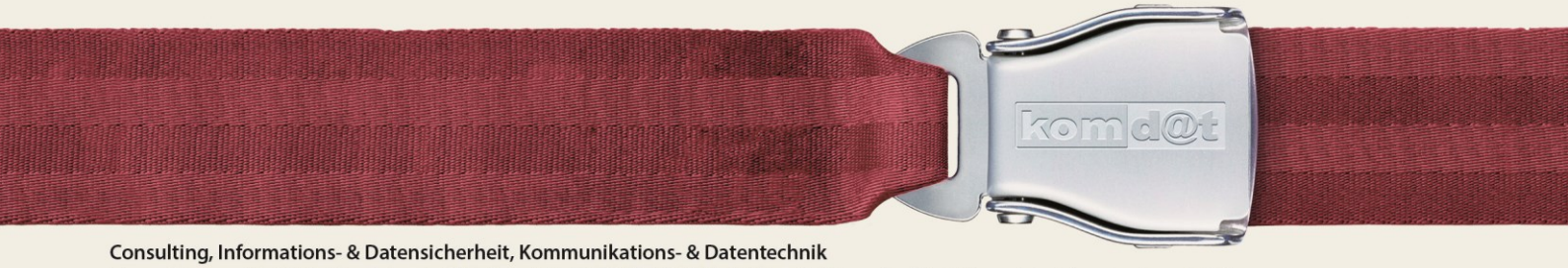
Ganzheitliche Netzwerksicherheit

Ein Bestandteil der strategischen Netzwerksicherheit ist der ganzheitliche Ansatz.

Im Zwiebelschalen-Prinzip müssen Sicherheitsringe um die IT und den darin verarbeiteten Daten gebildet werden. Einzelmaßnahmen müssen ineinandergreifen.

Jede Schutz-Maßnahme benötigt ein Konzept für:

- die Überwachung der Qualität der Funktionalität,
- ein Meldewesen, sowie



- eine Protokollierung um Vorgänge nachvollziehbar zu machen und
- eine detailreiche Dokumentation.

Ressourcen

Die notwendigen Ressourcen müssen ordentlich geplant sein und eine Reaktion auf spontane Ereignisse zulassen.

2. Netzwerksicherheit muss flexibel sein

Der Aufbau einer funktionierenden Netzwerksicherheit zum Schutz personenbezogener und sensibler Daten ist ein steter Prozess, der laufende Anpassungen und Qualitätskontrollen benötigt. Dabei wird es angesichts der steigenden Kosten immer schwieriger, die richtigen Entscheidungen zu treffen.

Unternehmen und Mitarbeiter wollen maximale Flexibilität

In der Vielzahl und Komplexität von Geräten und Applikationen nicht den Überblick zu verlieren ist eine Herausforderung. Die Wünsche nach Flexibilität und Mobilität verschärfen die Situation.

Diese Anforderungen lassen sich mit technischen Mitteln alleine nicht mehr bewältigen.

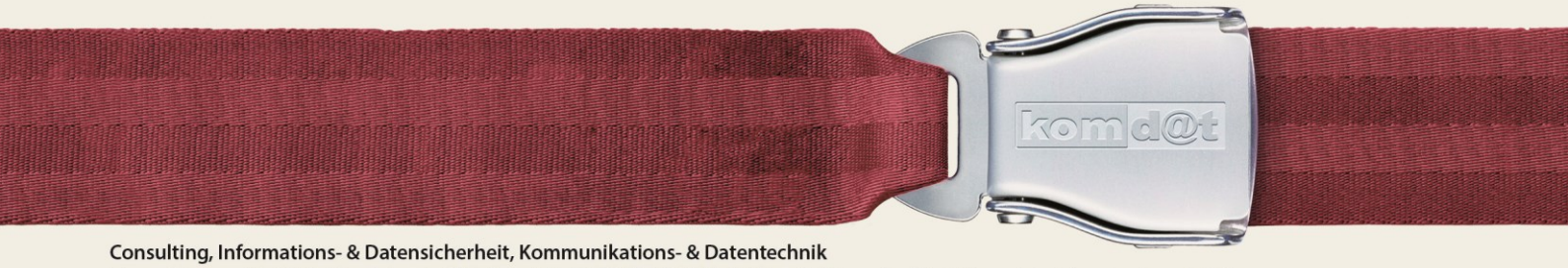
Es benötigte dazu Unternehmens- und Informations-Sicherheits-Handbücher, Vereinbarungen und Reglements. Diese müssen den betroffenen Personen nachweislich in einer Art und Weise zur Kenntnis gebracht werden, dass die Vorgaben auch anwendbar werden.

Bedrohungen ändern sich permanent

Es gibt unzählige Studien die belegen, dass der Anstieg von Angriffen auf personenbezogene und sensible Daten rasant vorangeht.

Das Problem dabei ist, dass die Angriffe immer intelligenter werden und Mechanismen besitzen, welche ganz gezielt Schwachstellen suchen und ausnutzen. Je nach gefundener Schwachstelle entscheidet der Angriff wie weiter vorgegangen wird, um die Effizienz des Angriffs zu maximieren.

Die Angriffs-Motivationen können dabei wirtschaftlich geprägt sein, kriminell oder emotional.



komd@t

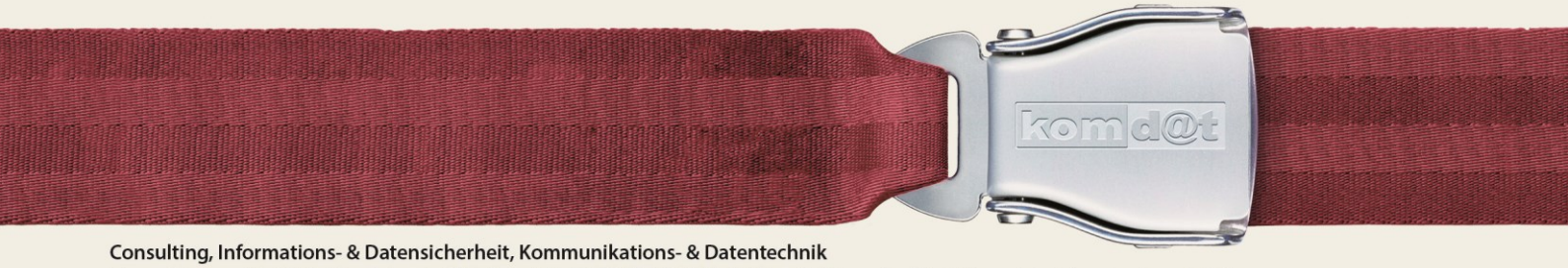
WERTE FÜR DIE ZUKUNFT SICHERN.

Die Angriffsziele sind unterschiedlich:

- Auslesen von Nutzerverhalten
- Datendiebstahl
- Erpressung
- Datenzerstörung
- usw

Immer gezielter werden mobile Geräte (Smartphones, etc) mit unterschiedlichen Betriebssystemen ins Fadenkreuz genommen, da es auf diesen Geräten erfahrungsgemäß noch die wenigsten Schutz-Mechanismen gibt. Geeignete Lösungen wie Mobile-Device-Management und ähnliches sind aber bereits erprobt und in allen Größen- und Funktionsumfängen verfügbar.

KOMDAT verfügt über die juristischen und technischen Experten um Unternehmen bei der Erstellung und Umsetzung von Netzwerk-Sicherheits- und Verteidigungsmaßnahmen zu unterstützen.



komd@t

WERTE FÜR DIE ZUKUNFT SICHERN.

3. Mitarbeiter-Schulungsprogramme als fester Bestandteil

Aufgrund der immer komplexer werdenden Angriffsmuster ist es sehr wahrscheinlich, dass Fehler durch menschliches Versagen, Unwissenheit oder Fehlverhalten verursacht werden. Ganz gezielt wird der Faktor Mensch als Schwachstelle angesteuert.

Dagegen hilft nur ein laufendes Mitarbeiter-Schulungs- und Sensibilisierungsprogramm, welches im §14 Abs. 2 Z. 3 DSG 2000 auch gesetzlich vorgeschrieben wird. Dieses sollte fester Bestandteil der Netzwerk-Sicherheits-Strategie sein. Es ist empfehlenswert, die Mitarbeiter in einem kontinuierlichen Prozess an die Themen heranzuführen, die allgemeinen Datenschutzstandards nach dem Datenschutzgesetz DSG 2000 sowie die unternehmenseigenen Schutzmaßnahmen und Abwehrmechanismen den Mitarbeitern zu erklären.

KOMDAT ist auf Mitarbeiter-Schulungen und Workshops spezialisiert.

4. Risikoanalyse

Auf die Frage nach der richtigen Strategie lässt sich keine pauschale Antwort finden.

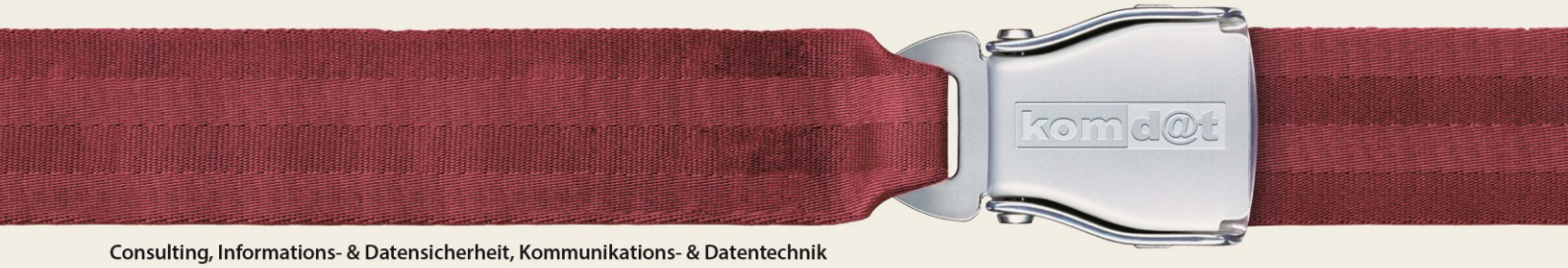
Eine Konstante lässt sich im Maßnahmen-Variablen-Dschungel jedoch erkennen.
Die Risikoanalyse.

Es geht darum, sämtliche Risikoflächen welche auf personenbezogene und sensible Daten einwirken ausfindig zu machen und geeignete Maßnahmen und Verteidigungsmechanismen zu erstellen. Die einzelnen Maßnahmen müssen dann noch so gewählt werden, dass sie ineinandergreifen.

Durchschnittlich werden Angriffe erst nach über 260 Tagen entdeckt. Auch diesem Risiko ist vorzubeugen. Denn, was man nicht erkennt, kann man auch nicht behandeln.

Geeignete Lösungen dagegen sind:

- die Protokollierung,
- das Monitoring bzw
- das Log-Management



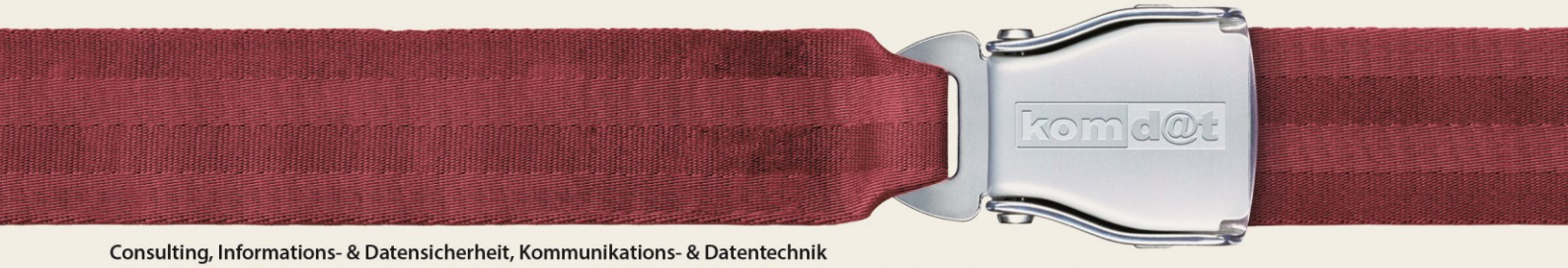
Diese Überwachungseinrichtungen müssen so ausgelegt sein, dass Angriffe bzw Alarmierungen sofort sichtbar werden bzw die zuständigen Personen erreichen. Über die dann zu treffenden Gegenmaßnahmen sollte man sich allerdings bereits im Vorfeld Gedanken gemacht haben.

Das bedeutet wiederrum, dass bei der Auswahl von Hardware-Komponenten die Filigranität der Log-Mechanismen und die Möglichkeiten zur Auswertung (SNMP, Syslog, etc) ein Entscheidungskriterium sind.

Ein wichtiger Punkt ist ein allumfassendes **Patch-Management**. Die regelmäßige Aktualisierung von Software ist Bestandteil des Risiko-Managements. Es muss jedoch eine Ausgewogenheit zwischen wirtschaftlicher Tragbarkeit und tatsächlicher Netzwerksicherheit gefunden werden.

Nicht zu vergessen sind Dienstleister, welche mit unternehmenseigenen personenbezogenen und sensiblen Daten in Berührung kommen. Entsprechende Vereinbarung in Hinblick auf §10 und §11 DSG 2000 sind hier verpflichtende Maßnahmen.

KOMDAT hat die juristischen Kompetenzen um vorhandene Vereinbarungen zu prüfen und/oder neue Vereinbarungen zu erstellen.



komd@t

WERTE FÜR DIE ZUKUNFT SICHERN.

5. Schatten-IT

Eine nicht zu unterschätzende Risikofläche ist die **Schatten-IT**.

Ob ungerechtfertigte oder zu hohe Rechte am Arbeitsplatz oder das Vergessen von Richtlinien zur Ausführung von Software in temporären Verzeichnissen. Es gibt viele Ursachen.

Nicht zu unterschätzen ist auch die Tatsache, dass Mitarbeiter, sollten sie vom Unternehmen keine für sie angemessenen Lösungen bereitgestellt bekommen, sich auf kreative Weise eigene Lösungen schaffen. So wird schnell aus einer gemanagten IT eine ungemanagte IT und die Risikofläche vergrößert sich unbemerkt.

Es lässt sich die Schatten-IT nicht alleine mit technischen Mitteln bekämpfen. Es wird dazu auch ein gut durchdachtes und verschriftlichtes Reglement notwendig. Das ist – auch mit seinen Konsequenzen – den Mitarbeitern in geeigneter Form zur Kenntnis zu bringen und der Nachweis darüber ist herzustellen.

KOMDAT hat sich auf Methoden zu Bekämpfung von Schatten-IT spezialisiert.

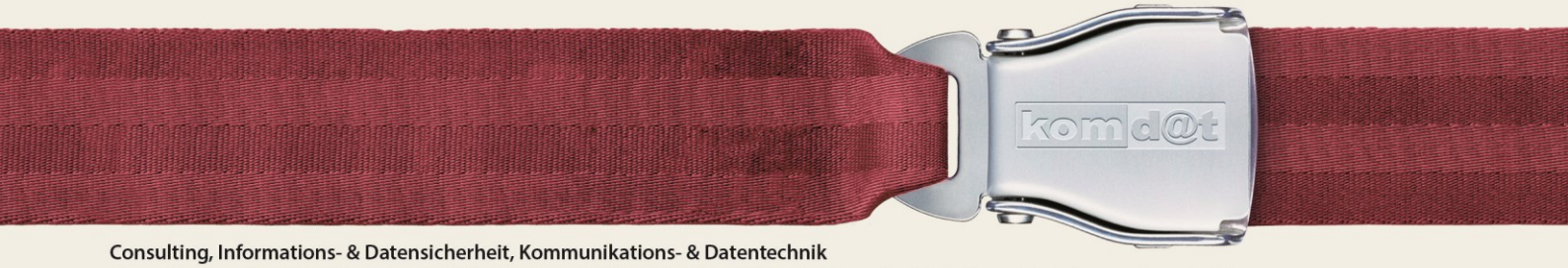
---

6. Anomalitäten finden

Das Erkennen von Anomalitäten im Netzwerk ist eine weitere Herausforderung. Melden sich Personen an ihnen nicht zugewiesenen Geräten an, erfolgt ein Zugriff auf nicht freigegebene Ordner, versuchen sich unbefugte Geräte einzuloggen, etc.

Die Windows-Boardmittel liefern hier bereits einen Lösungsansatz. Um die aufgezeichneten Events auswertbar zu machen, benötigt es jedoch eine Log-Management und eine Alarmierungs-Lösung.

Bei größeren Firmen ist auch auf die Möglichkeiten von Geo-Logging- oder Geo-Blogging-Maßnahmen nachzudenken.



komd@t

WERTE FÜR DIE ZUKUNFT SICHERN.

7. Netzwerksicherheit benötigt eine Organisation

Viele Maßnahmen lassen sich technisch umsetzen. Der Faktor Mensch ist jedoch in seiner Kreativität oder Naivität unberechenbar und kann viele technische Maßnahmen aushebeln.

Eine funktionierende Netzwerk-Sicherheits-Strategie benötigt daher:

- das Commitment der Geschäftsleitung
- ein Unternehmens- bzw Informations-Sicherheits-Handbuch
- einen Satz aus verbindlichen Vereinbarungen und Reglements
- eine umfangreiche Dokumentation der getroffenen Maßnahmen zum Schutz personenbezogener und sensibler Daten
- eine umfangreiche Protokollierung von Verarbeitungsvorgängen zur Herstellung einer Nachvollziehbarkeit
- die Verfügbarkeit notwendiger Ressourcen

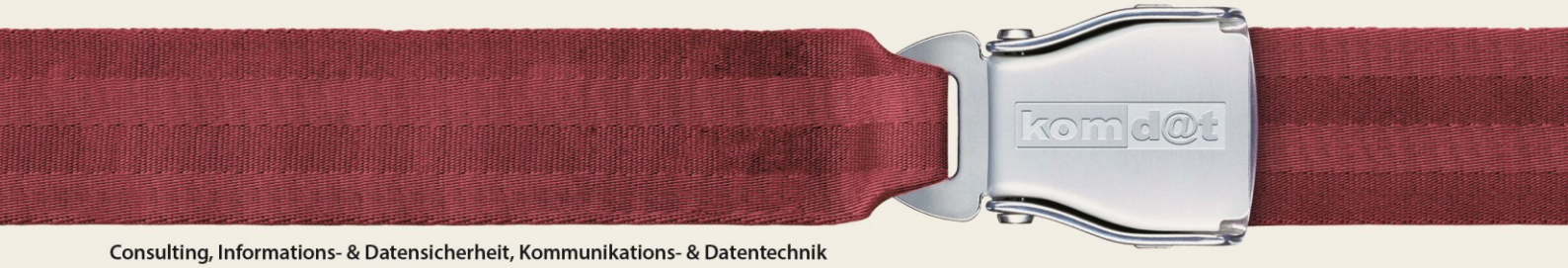
Sicherheit benötigt Training. Training benötigt Planung und Kontinuität, damit schnell und effizient reagiert werden kann.

8. Der Datenschutzbeauftragte

Die EU-Datenschutz-Grundverordnung verpflichtet Unternehmen unter definierten Voraussetzungen zur Benennung einer Datenschutzbeauftragten. Dieser muss spezielle Kompetenzen mitbringen und ist für alle Fragen und Belange rund um den gesetzlichen Datenschutz im Unternehmen zuständig.

Er kann sowohl aus eigenen Personalressourcen gestellt werden oder extern zugekauft werden, was aus Sicht der Haftung und Unabhängigkeit klare Vorteile hat.

Ab September 2016 bietet KOMDAT entsprechende Ausbildungen für zukünftige Datenschutzbeauftragte an – mehr dazu auf http://www.komdat.at.



komd@t

WERTE FÜR DIE ZUKUNFT SICHERN.

9. KOMDAT – als kompetenter Partner

Unternehmen benötigen im Bereich des gesetzlichen Datenschutzes Unterstützung. Das Unternehmen KOMDAT verfügt über die juristische und technische Kompetenz, um Unternehmen im Bereich gesetzlicher Datenschutz und Datensicherheit zu begleiten.

Wir verstehen uns als ein Unternehmen, welches Kunden beratend zur Seite steht und herstellerunabhängig agiert.

Die Kernkompetenzen von KOMDAT liegen in den Bereichen:

- Datenschutz-Expertisen und Analysen
- Datenschutz-Beratung
- Risikoanalysen
- Datenschutz-Folgeabschätzungen
- Mitarbeiter-Schulungen und Workshops
- Datenschutz-Seminare und Vorträge
- Erstellung von Unternehmens- und Informations-Sicherheits-Handbücher
- externe Datenschutzbeauftragte gem. EU-Datenschutz-Grundverordnung
- Penetration und Forensik
- ISO/IEC 27001:2015

Mehr Informationen unter http://www.komdat.at