Die DSGVO in der Praxis

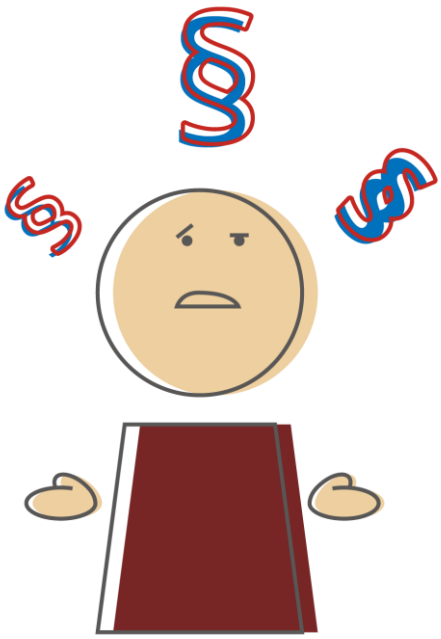
PRAKTISCHE AUSWIRKUNGEN AUF DEN IT-BETRIEB

Wien, im Jänner 2018

Kaum ein Thema bringt für Unternehmen so viel Unklarheit mit sich, wirft so viele Fragen auf und schafft so viel Verunsicherung wie die Datenschutzgrundverordnung, kurz DSGVO genannt. Einer der größten Irrtümer rund um die DSGVO ist dabei wohl, dass sie ein reines IT-Thema wäre. Natürlich stimmt es, dass sich die DSGVO um Datensicherheit dreht und dass die IT eines Unternehmens davon betroffen ist. Die Forderungen der DSGVO reichen aber so weit, dass es für eine Organisation unmöglich ist, sich dem Thema ausschließlich aus dem Blickwinkel der IT zu nähern. Vielmehr braucht es einen Ansatz, der sich mit den Prozessen beschäftigt, die rund um die personenbezogenen Daten bestehen. In vielen Organisationen werden diese Prozesse überhaupt erst einmal aufzuspüren sein. Erst wenn über diese Prozesse Klarheit besteht und sobald sie ausreichend definiert sind, macht es Sinn, praktische Konsequenzen abzuleiten und über die Umsetzung auf der IT-Ebene nachzudenken. Wenn eine Organisation also anstrebt, Compliance mit der DSGVO herzustellen, dann wäre es vollkommen falsch, diese Aufgabe alleine an die IT-Abteilung zu delegieren. Ein sinnvollerer Ansatz ist eine Zusammenarbeit von der Geschäftsleitung, dem Datenschutzbeauftragten, den Abteilungen und der IT der Organisation mit einer kompetenten Rechtsberatung und einem zuverlässigen IT-Partner. Nur dann ist es möglich, ein höchstmögliches Maß an DSGVO Compliance zu erreichen.

DIE GROSSE VERWIRRUNG

Wir von d-con.net versuchen seit einiger Zeit, für unsere Kunden mehr Klarheit rund um die DSGVO zu schaffen. Im November 2017 haben wir Rechenzentrumsbetreiber, Wirtschaftsprüfer, IT Security Hersteller, Rechtsanwälte und CIOs von internationalen Großbetrieben im Rahmen einer Podiumsdiskussion zusammengebracht. Das große Interesse hat uns gezeigt, dass vor allem bezüglich der praktischen Auswirkungen der DSGVO noch viele Fragen offen sind. Wir wollen daher mit diesem Beitrag mit Hilfe von konkreten Beispielen herausarbeiten, was die DSGVO in der Praxis bedeutet und wie wir unsere Auftraggeber dabei unterstützen, gängige Fallen zu entschärfen. Vorab gehen wir aber noch kurz auf das neue Regelwerk der DSGVO ein.



KONKRET: WAS IST DIE DSGVO?

Die Datenschutzgrundverordnung (DSGVO) ist eine EU-Verordnung. Sie tritt am 25. Mai 2018 in Kraft und wird von der Republik Österreich unmittelbar angewendet. Ganz allgemein gesprochen regelt die DSGVO die Verarbeitung von personenbezogenen Daten. Die Datenverarbeitung für persönliche Zwecke ist ausgenommen; eine weitere Einschränkung besteht durch Aufbewahrungspflichten, die durch andere Rechtsvorschriften gegeben sind und weiterhin Vorrang haben. Abgesehen von diesen Ausnahmen ist aber so gut wie jede Organisation, die personenbezogene Daten speichert und verarbeitet, von der DSGVO betroffen. Die politische Idee hinter der DSGVO ist wohl schlichtweg der Schutz der natürlichen Person vor dem Missbrauch ihrer persönlichen Daten. Die natürliche Person erhält durch die DSGVO das Recht auf Auskunft zu ihren Daten, das Recht auf Löschung ihrer Daten und das Recht darauf, dass ihre Daten mit angemessenen Sicherheitsmaßnahmen geschützt werden. Im Detail beinhaltet das Regelwerk der DSGVO zehn Kapitel mit insgesamt 99 Artikeln. Im Original ist die DSGVO ohne Rechtsberatung wohl kaum zu verstehen. Es gibt aber unterstützende Interpretationen, zum Beispiel einen Leitfaden zur DSGVO, herausgegeben von der dsb, der Datenschutzbehörde der Republik Österreich. Der Leitfaden arbeitet auch die Neuerungen heraus, die sich durch die DSGVO für informationsverarbeitende Organisationen ergeben. Um nur ein paar Beispiele zu nennen: Mit Artikel 25 wird „Privacy by Design" gefordert, das bedeutet, dass generell nur unbedingt erforderliche personenbezogene Daten verarbeitet werden dürfen. Artikel 33 zum Beispiel regelt die nun komplett neue Meldung von Datenschutzverstößen, also welche Handlungen bei einem Diebstahl von personenbezogenen Daten zu setzen sind.

Die Fakten zur DSGVO:

- *Die DSGVO regelt die Verarbeitung personenbezogener Daten*
- *Die DSGVO ist die EU-Verordnung 2016/679*
- *Die DSGVO tritt mit 25. Mai 2018 in Kraft*
- *Die DSGVO löst die bisherige EU Datenschutzrichtlinie (DSRL) ab*
- *Die DSGVO stellt hohe Anforderungen an Organisationen*
- *Die DSGVO sieht empfindliche Strafen vor*

Rund um die DSGVO ist besonders hervorzuheben, dass viele Bestimmungen großen Interpretationsspielraum geben. Viele der Forderungen gewähren Handlungsspielraum bezüglich des aktuellen Stands der Technik, den Implementierungskosten, der Eintrittswahrscheinlichkeit und der Schwere der Risiken. Dieser interpretative Spielraum bedeutet aber keineswegs, dass die DSGVO auf die leichte Schulter genommen werden kann. Was genau im einzelnen Fall wie auszulegen ist, darüber wird erst die Judikatur der kommenden Jahre Klarheit schaffen. Wir empfehlen aber schon heute, den Grundgedanken der DSGVO zu übernehmen und angemessene Schritte zu setzen. Wie bereits eingangs erwähnt, lässt sich das nur mit einem ganzheitlichen, unternehmensweiten Ansatz bewältigen. Im Folgenden arbeiten wir anhand einiger konkreter Beispiele heraus, welche praktischen Auswirkungen die DSGVO auf die IT haben kann und wie wir unsere Auftraggeber dabei unterstützen.

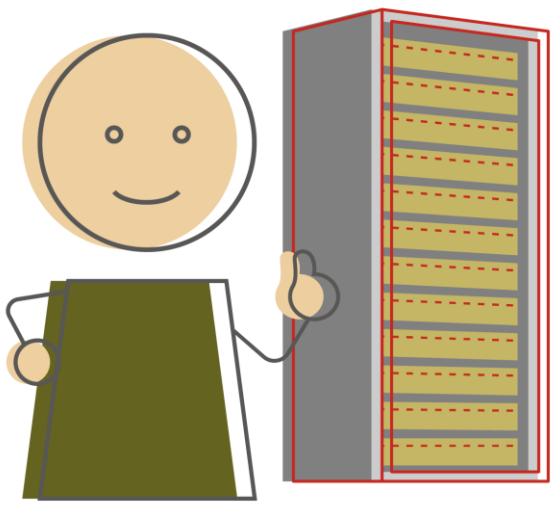
1. BEISPIEL: DATEN AM FILESERVER

Unstrukturierte Daten auf Fileservern enthalten oft personenbezogene Daten, die abgesichert werden müssen.

Auf vielen Fileservern existiert eine große Menge von Daten, die von den Benutzern des Unternehmens erzeugt wurde. Die Daten am Fileserver sind oft weitgehend unstrukturiert und wurden mit den unterschiedlichsten Werkzeugen erstellt, wie zum Beispiel Microsoft Office Programmen. Vor allem dann, wenn ein Fileserver schon länger in Verwendung steht, wird sich auf diese Weise über die Jahre höchstwahrscheinlich ein unüberschaubares Dickicht aus User Daten gebildet haben. Aus der Sicht der DSGVO sind in diesem Dickicht natürlich besonders die personenbezogenen Daten relevant. Auch wenn die Haltung all dieser Daten im Sinn der DSGVO in Ordnung sein kann, so bleibt aber immer noch die Frage, wer aller darauf Zugriff hat. Denn die DSGVO verlangt, dass personenbezogene Daten nur jenen Personen zugänglich sind, die sie tatsächlich für ihre Arbeit brauchen.

Klare Zugriffsregelungen bestehen zumeist nur für personenbezogenen Daten, die von Applikationen wie einem CRM, einer Warenwirtschaft oder einer Patientenverwaltung gehalten werden. Innerhalb dieser Applikationen kommen rollenbasierte Berechtigungskonzepte zur Anwendung, ganz im Sinn der DSGVO. Was die angesammelten Daten auf einem Fileserver betrifft, sieht die Lage oftmals ganz anders aus, denn hier sind die Zugriffsberechtigungen auf bestimmte Daten nicht so klar festgelegt. Sind Personen für den direkten Zugriff auf den Fileserver (oder Teilen davon) berechtigt, so haben sie höchstwahrscheinlich aus Sicht der DSGVO unerlaubten Zugriff auf personenbezogene Daten. Lösbar wäre dieses Problem nur dadurch, dass auch für die Daten auf dem Fileserver ein rollenbasiertes Berechtigungskonzept eingerichtet wird. Bei einem historisch gewachsenen Fileserver ist es aber in der Praxis unmöglich, das bestehende umfangreiche Datengeflecht zu entwirren und ein rollenbasiertes Berechtigungskonzept nachträglich zu implementieren.

Um dennoch den DSGVO Vorgaben zu genügen, bewährt sich folgender praxisorientierter Lösungsansatz: Parallel zu der bestehenden Fileserver-Struktur wird eine neue, zweite Fileserver-Struktur eingerichtet. Die Daten werden langsam und koordiniert übertragen, parallel dazu wird ein rollenbasiertes Berechtigungskonzept erarbeitet und implementiert. Nach der Migration ist klar, welche Daten wo abgelegt sind und wer aller darauf Zugriff hat. Das ist eine wesentliche Voraussetzung dafür, die DSGVO Compliance zu erreichen. Darüber hinaus werden die Daten durch den Wechsel auf eine neue Version auch von Altlasten bereinigt, was ebenfalls das Risiko für böse Überraschungen (z.B. durch vergessene personenbezogenen Daten) minimiert.



2. BEISPIEL: DATEN AUF NOTEBOOK

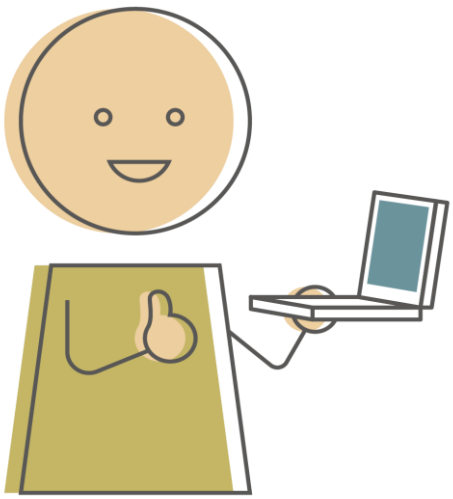
Notebooks mit personenbezogenen Daten sollten verschlüsselt sein, um aufwändige Pflichten abzuwenden.

Außendienstmitarbeiter in Service oder Vertrieb sind in vielen Fällen mit Notebooks ausgestattet. Auf den Datenträgern dieser Notebooks finden sich oft auch lokale Kopien von personenbezogenen Daten, die aus dem Datenbestand des Unternehmens stammen. Auch hier gilt wieder: Sofern der Außendienstmitarbeiter diese Daten im Rahmen klar definierter Prozesse für seine Arbeit einsetzt, ist aus der Sicht der DSGVO alles in Ordnung – allerdings nur, solange ausschließlich er und andere autorisierte Personen Zugriff auf die Daten des Notebooks haben.

Nun haben aber gerade mobile Geräte wie Notebooks die Tendenz, abhanden zu kommen. Sie müssen dazu gar nicht aktiv gestohlen werden, etwa aus einem Auto oder einem Büro. Oft genügt es, dass ein Notebook einfach vergessen liegen bleibt, zum Beispiel in einem Lokal, in einem öffentlichen Verkehrsmittel, in einer Garderobe oder irgendwo sonst unterwegs. Das passiert sehr leicht und häufig. In manchen Fällen findet dann irgendjemand Gefallen an dem Fundstück und behält es. Nun ist der Verlust eines Notebooks sowohl für den Außendienstmitarbeiter als auch für seinen Arbeitgeber eine ärgerliche Angelegenheit. Der wirklich kostenintensive Schaden tritt aber erst jetzt mit der DSGVO ein. Befinden sich auf dem Notebook nämlich personenbezogene Daten, die nun von nicht autorisierten Personen eingesehen und weiterverwendet werden können, so ist ein Datenverlust eingetreten.

Die DSGVO schreibt für solche Fälle sehr genau vor, wie zu handeln ist. Abgesehen von einer Meldung bei der Aufsichtsbehörde ist auch eine Data Breach Notification durchzuführen. Das bedeutet, dass alle Personen zu verständigen sind, deren Daten von dem Datenverlust betroffen sind. Für das bestohlene Unternehmen kann es sehr schwer bis unmöglich sein, diese Auflage zu erfüllen, da ja mit dem Notebook auch die Information über den tatsächlich betroffenen Personenkreis abhanden gekommen ist. Und selbst wenn es möglich ist, ist die Verständigung zeitaufwändig, teuer und rufschädigend.

Um der DSGVO auf einfacherem Wege Genüge zu tun, empfehlen wir folgenden praktischen Ansatz: Mit einer Hardwareverschlüsselung werden die Daten auf Notebooks dem Zugriff Dritter entzogen. Die Daten auf der Festplatte des Notebooks sind dann nur mehr mit einem Schlüssel zugänglich. Damit ist im Fall der Fälle zwar ein Notebook verschwunden, ohne den Schlüssel hat aber niemand Zugriff auf die darauf enthaltenen personenbezogenen Daten. Bei einem Verlust des Notebooks entfällt dann die Verpflichtung einer Data Breach Notification an alle Betroffenen.



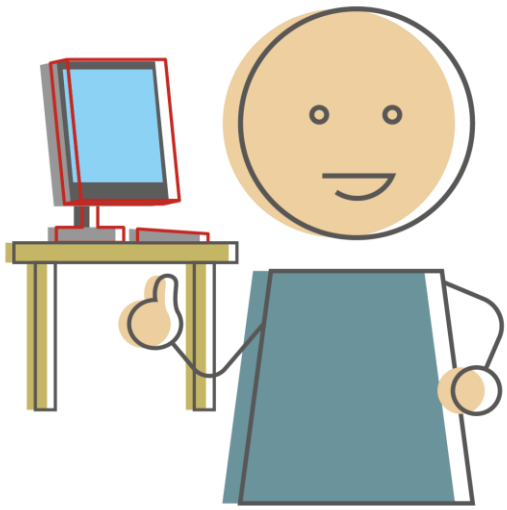
3. BEISPIEL: ZUGANG ZU APPLIKATIONSDATEN

Der Zugriff auf personenbezogene Daten in Applikationen muss ausreichend abgesichert sein.

Auch der Benutzerzugriff auf die Applikationen einer Organisation bildet einen weiteren Punkt, dem mit der DSGVO nun weit mehr Aufmerksamkeit geschenkt werden muss. Denn in Applikationen wie ERP-, CRM- oder HR-Systemen werden eine Vielzahl von personenbezogenen Daten geführt. Die DSGVO fordert, dass nur jene Benutzer Zugriff auf diese Daten haben, die sie tatsächlich für ihre Arbeit benötigen. Diese Anforderung lässt sich erfüllen, wenn mit Hilfe von entsprechenden Prozessdefinitionen ein rollenbasiertes Zugriffskonzept für die Benutzer der Applikationen erarbeitet wird. Damit wird sichergestellt, dass z.B. Vertriebsmitarbeiter keinen Zugriff auf die Personaldaten des Unternehmens haben, die sie ja für ihre Arbeit schließlich gar nicht brauchen. Und umgekehrt können dann Mitarbeiter aus der Personalabteilung keine persönlichen Daten von Kunden abfragen, die sie ihrerseits nicht benötigen.

So weit so gut. Angenommen, die oben beschriebene Anforderung wäre erfüllt und jeder User im Unternehmen hat – durch ein solides, rollenbasiertes Zugriffskonzept – nur Zugang zu genau festgelegten personenbezogenen Daten. Auch wenn das erfüllt ist, so bleibt immer noch die Frage nach der Authentifizierung der physischen Benutzer. Denn das beste Zugriffskonzept ist wertlos, wenn der Anmeldevorgang selbst ungenügend abgesichert ist. Im schlimmsten Fall kann sich dann ein User leicht für einen anderen User ausgeben; womöglich könnte sich sogar eine betriebsfremde Person Zugang zu der Anwendung verschaffen. Sofern personenbezogene Daten betroffen sind, wäre das aus dem Blickwinkel der DSGVO ein absolutes No-Go. Denn die DSGVO verlangt für diese Daten dem Stand der Technik entsprechende, angemessene Schutzmaßnahmen.

Besonders für alle Nutzungsformen von Applikationen, Diensten oder Daten über das Internet empfehlen wir daher, eine 2-Faktor Authentifizierung einzusetzen. Dabei wird eine Lösung eingerichtet, die vom Benutzer neben der Passworteingabe noch einen zweiten Faktor verlangt, wie zum Beispiel einen Hardware-Token oder ein SMS-Einmalkennwort. Die Möglichkeiten in der Realisierung sind vielfältig, entscheidend ist die doppelte Absicherung durch zwei unabhängige Faktoren. Darüber hinaus empfehlen wir, in allen Applikationen Log-Dateien der Benutzeranmeldungen mitzuführen und zu archivieren. Damit stellen Sie sicher, dass die Zugriffe auf personenbezogene Daten nachvollziehbar bleiben.



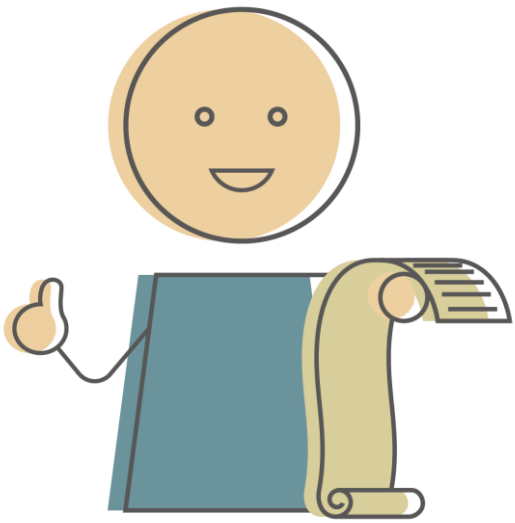
4. BEISPIEL: UMGANG MIT LOGFILES

Logfiles ermöglichen die geforderte Nachvollziehbarkeit, enthalten aber oft selbst personenbezogene Daten.

Auch die Protokollierung von Benutzeraktivitäten mit Log-Files ist ein Thema, das mit der DSGVO nun noch mehr Brisanz erfährt. Während große Organisationen schon jetzt sehr professionell damit umgehen, wird das Thema in KMU bislang meist nur stiefmütterlich behandelt. Die DSGVO sollte nun auch für mittelständische Unternehmen eine starke Motivation bieten, sich gezielt damit auseinanderzusetzen, wo und wie Logs angelegt und abgefragt werden. Denn aus dem Blickwinkel der DSGVO ist es in doppelter Hinsicht notwendig, dafür klare Prozesse und Regelungen zu schaffen.

Log-Files sind deshalb DSGVO-relevant, weil sie sehr oft benutzerbezogene Informationen enthalten. Im Serverlog eines Webservers wird zum Beispiel der Traffic aller Benutzer protokolliert. Ein weiteres Beispiel bildeten Firewalls, die ebenfalls umfangreiche Log-Dateien anlegen und damit auch Informationen über Benutzer enthalten. Ereignisprotokolle des Betriebssystems wiederum dokumentieren An- und Abmeldungen von Benutzern am System. Spezielle Log-Dateien einzelner Applikationen können einen Detaillierungsgrad bis zur minutiösen Auflistung aller Benutzeraktivitäten aufweisen. Und auch Datenbanken legen Logs in Form von Transaktionsprotokollen an, die ebenfalls Angaben über Benutzeraktivitäten enthalten können.

Alle diese Protokolldateien erfüllen aus der Sicht der DSGVO eine wichtige Funktion: Sie liefern Antworten auf die Frage, welche Benutzer wann auf welche personenbezogenen Daten Zugriff hatten. Durch die von der DSGVO geforderte Nachvollziehbarkeit ist es daher notwendig, die notwendigen Log-Files zu definieren, ihre Erstellung sicherzustellen und die resultierenden Logs zu archivieren. Da die Log-Dateien Informationen enthalten, wer auf welche Daten zugegriffen hat, sind sie aber selbst ebenfalls als personenbezogene Daten zu behandeln und entsprechend abzusichern. Außerdem besteht dadurch gegenüber Mitarbeitern eine Auskunftspflicht, wer unternehmensintern Zugriff auf diese Informationen hat.



Unsere Empfehlung zum Thema Log-Files lautet daher: Nehmen Sie die DSGVO zum Anlass, in diesem Bereich Ordnung zu schaffen. Finden Sie heraus, welche Ihrer Systeme zurzeit welche Logs anlegen und wie Sie diese ggf. erweitern müssen, um der DSGVO Forderung nach Nachvollziehbarkeit entsprechen zu können. Stellen Sie darüber hinaus sicher, dass nur ein eingeschränkter und klar definierter Personenkreis Zugriff auf die Log-Dateien hat.

5. ZUSAMMENFASSENDE EMPFEHLUNG

Wir zeigen in diesem Beitrag an Hand von vier einfachen Beispielen, wie die DSGVO die gesamte Informationsverarbeitung einer Organisation betrifft. Die angeführten Beispiele sollen auch demonstrieren, wie viele Details von der DSGVO betroffen sind, an die man auf den ersten Blick gar nicht denken würde. Wie wir zum Beispiel herausgearbeitet haben, auch die Log-Datei einer Firewall fällt in die Kategorie „personenbezogene Daten".

Zusammenfassend lässt sich festhalten, die Forderung der DSGVO nach dem sorgfältigen Umgang mit personenbezogenen Daten hat es also wirklich in sich. Sie trifft auf so viele Stellen und so viele Anwendungen zu, dass es eine große Herausforderung werden wird, ihr zu entsprechen. Um ein letztes Beispiel zu bringen, das die Thematik wirklich zuspitzt: Nehmen wir an, Ihr Unternehmen verwaltet – so wie viele andere – seine Kundendaten in einem CRM. Und nehmen wir weiter an, dass einer Ihrer Außendienstmitarbeiter aus dem CRM eine einfache Geburtstagsliste der von ihm betreuten Kunden exportiert. Dann ist damit eine neue, eigene DV-Anwendung entstanden, die von Ihrem Unternehmen zu definieren und zu verwalten wäre, sprich voll inhaltlich im Rahmen der DSGVO zu behandeln wäre. Wie dieses letzte Beispiel verdeutlicht, werden technische Maßnahmen allein nicht ausreichen, um die Forderungen der DSGVO abzudecken. Vielmehr geht es darum, im Unternehmen auch eine Bewusstseinsbildung einzuleiten. Eine unverzichtbare Maßnahme dafür ist die Schulung der Mitarbeiter des Unternehmens.

Unsere Empfehlung lautet daher: Fassen Sie die DSGVO ist nicht als Qual, sondern als Chance auf. Eine Chance auf sinnvolle organisatorische und technische Änderungen in Ihrem Unternehmen, die einen besseren und sichereren Umgang mit Daten einleiten. Damit machen Sie sich nicht nur DSGVO-fit, sondern leiten einen Verbesserungsprozess ein, der ganz allgemein Ihre IT-Sicherheitsrisiken signifikant reduzieren wird. Wir unterstützen Sie gerne.

Zu den Autoren

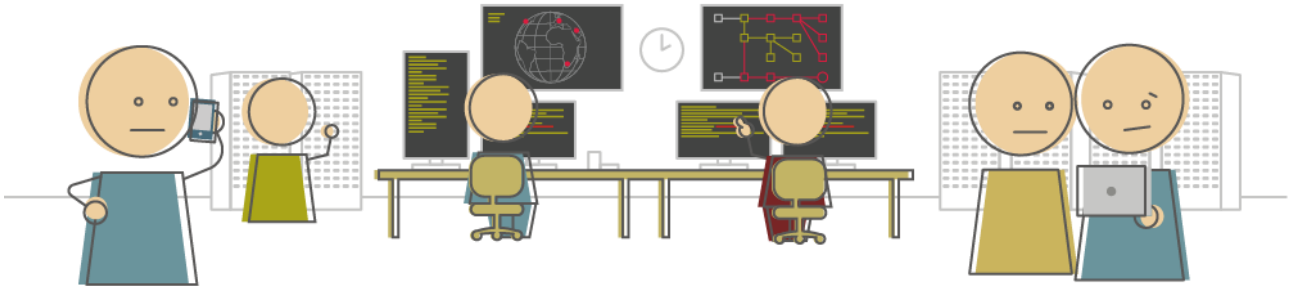
David Rosenberg ist Project Manager bei d-con.net und verfügt über langjährige IT-Erfahrungen, die er unter anderem als Leiter von europaweiten Großprojekten sammeln konnte. David Rosenberg beschäftigt sich intensiv mit dem Thema Informationssicherheit und dem Aufbau entsprechender IT-Infrastruktur.

david.rosenberg@d-con.net
d-con.net GmbH
Johannesstraße 50, AT-2371 Hinterbrühl
+43 1 616 32 17 – 0

Roman Rathler ist IT-Security Experte, CTO und Lead Consultant bei d-con.net. Neben seiner Projekttätigkeit bei Auftraggebern ist er auch für das Business Development des Unternehmens zuständig. Roman Rathler ist seit über 20 Jahren im Netzwerk- und Security-Bereich tätig und verfügt über tiefgehendes praktisches Know-how im Aufbau sicherer Infrastruktur.

roman.rathler@d-con.net
d-con.net GmbH
Johannesstraße 50, AT-2371 Hinterbrühl
+43 1 616 32 17 – 0

d-con.net ist ein strategisches Asset



d-con.net ist ein strategischer Dienstleistungspartner. Wir arbeiten laufend daran, unseren Auftraggebern Hochtechnologie zu erschließen und in Best Practices IT-Lösungen verfügbar zu machen. Bei uns erhält man hochmoderne Systeme und leistungsfähige Managed Services, immer am Puls der Zeit. Da unsere Auftraggeber oft international agierende Unternehmen sind, werden unsere Kunden rund um den Globus in ihren Landesniederlassungen auf allen Kontinenten unterstützt.

d-con.net GmbH
Johannesstraße 48a
2371 Hinterbrühl, Österreich
+43 1 616 32 17 – 0
www.d-con.net
office@d-con.net