ISIS 12

ISIS12 – EIN **I**NFORMATIONS**SI**CHERHEITS-MANAGEMENT**S**YSTEM IN **12** SCHRITTEN

Unterstützt durch das
Bayerische Staatsministerium des Innern, für Bau und Verkehr

Initiative Cybersicherheit Bayern

ITSECURITY
Bavarian IT Security & Safety Cluster

→ EINE MARKE
DES BAYERISCHEN
IT-SICHERHEITS-
CLUSTERS E.V.

Der Bayerische IT-Sicherheitscluster e.V.

Der Bayerische IT-Sicherheitscluster e.V. ist ein Zusammenschluss von Unternehmen der IT-Wirtschaft, von Unternehmen die IT-Sicherheitstechnologien nutzen, von Hochschulen, von weiteren Forschungs- und Weiterbildungseinrichtungen und Juristen. Der Verein fördert die Erforschung, Entwicklung, Anwendung und Vermarktung von Technologien, Produkten und Dienstleistungen, die zur Erhöhung der Informationssicherheit und der funktionalen oder physischen Sicherheit in Unternehmen beitragen.

Er unterstützt zudem die Aus- und Weiterbildung in diesem Bereich, begleitet Unternehmensneugründungen und initiiert Kooperationen, insbesondere zwischen den Mitgliedern des Vereins. Darüber hinaus informiert er Unternehmen und Privatanwender über Sicherheitsrisiken, sowie technische und organisatorische Lösungen, z.B. durch öffentliche Veranstaltungen und Workshops.

ITSECURITY
Bavarian IT Security & Safety Cluster

Sandra Wiesbeck
Clustermanagerin &
Vorstandsvorsitzende
Bayerischer IT-Sicherheitscluster e.V.

ISIS 12

Informationssicherheit für den Mittelstand und Kommunen

Mittelständische Unternehmen und Organisationen müssen sich zunehmend mit den Herausforderungen der Wirtschaftsspionage, des Datenschutzes und der Notwendigkeit hoher IT-Verfügbarkeit auseinander setzen. Die bestehenden Standardverfahren für IT-Service Management (ITSM) und für ein Informations-Sicherheitsmanagementsystem (ISMS) sind in erster Linie für große Unternehmen entwickelt worden und daher in der Anwendung zu komplex und letztendlich zu teuer.

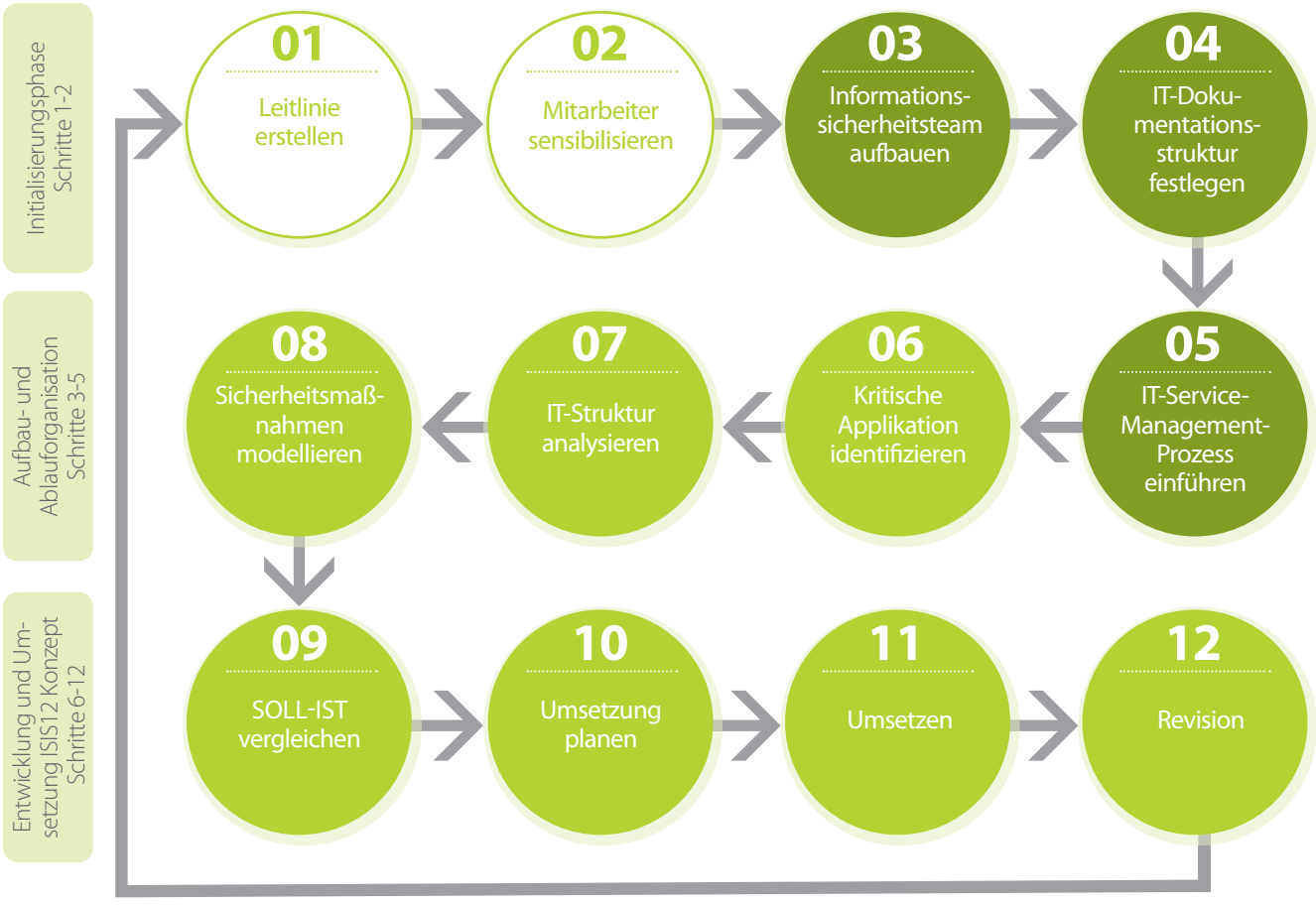
ISIS12 ist ein **I**nformations**SI**cherheitsmanage-ment**S**ystem in 12 Schritten. Es wurde in einem Netzwerk des Bayerischen IT-Sicherheitsclusters e.V. entwickelt und beschreibt ein Vorgehensmodell, welches auf die Bedürfnisse von mittelständischen Unternehmen und Kommunen zugeschnitten ist. Bei dem integrierten Management-Ansatz werden ISMS und IT SM verknüpft. Das Verfahren kann als mögliche Vorstufe zur ISO/IEC 27001- bzw. BSI IT-Grundschutz-Zertifizierung verwendet werden. Der Freistaat Bayern fördert über das Staatsministerium des Innern, für Bau und Verkehr im Rahmen der Initiative Cybersicherheit die Einführung von ISIS12 bei Kommunen.

Die insgesamt 12 Verfahrensschritte des Management-Systems sind im ISIS12-Handbuch beschrieben. Ergänzt wird dies durch den ISIS12-Katalog, der nur die relevanten Maßnahmen enthält, die für mittelständische Unternehmen und Kommunen in Frage kommen. Parallel dazu wird die Realisierung durch eine vom Netzwerk entwickelte ISIS12-Software unterstützt. Eine Möglichkeit zur anschließenden Zertifizierung durch die Deutsche Gesellschaft zur Zertifizierung von Managementsystemen (DQS) besteht. Zertifizierte Unternehmen können so höchste Qualität in ihrer Informationssicherheitspolitik nachweisen – ein Wettbewerbsfaktor, der immer wichtiger wird.

An der kontinuierlichen Weiterentwicklung und Vermarktung von ISIS12 arbeitet das „Netzwerk Informationssicherheit für den Mittelstand“ (NIM) des e.V. Das ISIS12-Handbuch und der ISIS12-Katalog sind gegen eine Schutzgebühr erhältliche öffentliche Dokumente. Kommunen erhalten diese kostenfrei. Empfehlenswert ist die Begleitung der Einführung von ISIS12 durch einen zertifizierten ISIS12-Dienstleister.

Weitere Informationen zu ISIS12 erhalten Sie unter:
www.isis12.de

12 INFORMATIONSSICHERHEIT IN 12 SCHRITTEN



01 Leitlinie erstellen

ISIS12 Schritt 1 beschäftigt sich mit der Erstellung einer Unternehmensleitlinie für Informationssicherheit. Die Unternehmensleitlinie ist das zentrale Strategiepapier. Darin werden die Informationssicherheitsziele sowie die daraus abgeleiteten und abzuleitenden Konzepte und Maßnahmen festgehalten. Die Mitarbeiter müssen zur Einhaltung und Umsetzung von der Unternehmensleitung motiviert werden. Zu berücksichtigen sind insbesondere auch die unternehmensspezifischen Sicherheitsziele wie z.B. Reduzierung der Kosten im Schadensfall oder Aufrechterhaltung der Produktionsfähigkeit.

INFORMATIONSSICHERHEIT IN 12 SCHRITTEN

02 Mitarbeiter sensibilisieren

In ISIS12 Schritt 2 stehen die Mitarbeiter und Führungskräfte im Mittelpunkt. Auf allen Organisationsebenen muss die Notwendigkeit des Projekts kommuniziert werden. In einem speziellen ISIS12-Vortrag sollen alle Mitarbeiter über den ISIS12-Workflow und die spezifische Bedeutung der Informationssicherheit für das Unternehmen hingewiesen werden. Neben dem Erhalt eines schriftlichen Exemplars der Leitlinie für Informationssicherheit sollen die Mitarbeiter regelmäßig über Neuerungen informiert werden.

03 Informationssicherheitsteam aufbauen

ISIS12 Schritt 3 beschreibt den Aufbau, die Zusammensetzung, die Aufgaben und Pflichten des Informationssicherheitsteams. Leiter ist der Informationssicherheitsbeauftragte (ISB), der auch für die Einführung des ISIS12 Prozesses verantwortlich ist. Die Berichterstattung erfolgt direkt an die Unternehmens- bzw. Behördenleitung.

04 IT-Dokumentationsstruktur festlegen

ISIS12 Schritt 4 beschäftigt sich mit einer zielführenden IT-Dokumentation. Absolut wichtig ist die Aktualität der Dokumente, die der IT-Verantwortliche kontinuierlich kontrollieren muss. Um Änderungen nachzuvollziehen, ist eine Versionierung der Dokumente erforderlich.

05 IT-Service-Management-Prozess einführen

In ISIS12 Schritt 5 erfolgt die Implementierung von drei fundamentalen IT-Service-Managementprozessen: Wartung, Änderung und Störungsbeseitigung. Wird im Rahmen einer Wartung eine Änderung nötig, wird diese über den Änderungsprozess eingesteuert. Final wird der Störungsbeseitigungsprozess definiert.

06 Kritische Applikationen identifizieren

Mit ISIS12 Schritt 6 beginnt die operative Phase des ISIS12 Vorgehensmodells. Dabei werden nur unternehmenskritische Anwendungen identifiziert und bewertet. Diesen werden jeweils 3 Schutzbedarfskategorien, bezogen auf die Grundwerte „Vertraulichkeit, Integrität und Verfügbarkeit“, zugeordnet.

12 INFORMATIONSSICHERHEIT IN 12 SCHRITTEN

07 IT-Struktur analysieren

Nach der Lokalisierung kritischer Applikationen steht in ISIS12 Schritt 7 die Definition des Informationsverbunds im Mittelpunkt. In diesem werden die technischen, personellen, organisatorischen und infrastrukturellen Objekte, die für die Verarbeitung von Informationen im Unternehmen benötigt werden, zusammengefasst.

08 Sicherheitsmaßnahmen modellieren

In ISIS12 Schritt 8 erfolgt die Zuordnung der empfohlenen Sicherheitsmaßnahmen zu den in Schritt 7 ermittelten Objekten. Die Bausteine, die für den gesamten Informationsverbund anzuwenden sind, lauten: Universale Aspekte, Infrastruktur, IT-Systeme / Netze und Anwendungen. Diesen Bausteinen werden die IT-Objekte zugeordnet, z.B. gehören Gebäude und Serverraum zur Infrastruktur.

09 Ist-Soll vergleichen

In ISIS12 Schritt 9 soll mit dem Ist-Soll-Vergleich ein Überblick über den Umsetzungsgrad der in Schritt 8 geforderten Maßnahmen gegeben werden. Die Erhebung kann durch die vom ISB ernannten verantwortlichen Spezialisten im Unternehmen durchgeführt werden. Die hierfür von der ISIS12-Software erstellten Erhebungsbögen können im größeren Kreis oder in Einzelinterviews abgearbeitet werden.

10 Umsetzung planen

In ISIS12 Schritt 10 wird ein Maßnahmenkatalog erzeugt und konsolidiert. Die umzusetzenden Maßnahmen werden priorisiert und zusammen mit einer Kostenabschätzung der Geschäftsleitung als Vorschlag präsentiert. Nach Festlegung der Umsetzungsreihenfolge der Maßnahmen werden diese in ISIS12 Schritt 11 final umgesetzt.

11 Umsetzen

In ISIS12 Schritt 11 werden die konsolidierten und genehmigten Sicherheitsmaßnahmen im Unternehmen umgesetzt. Für jede Maßnahme, sind die Rollen des Initiators, des Umsetzers und der Zeitpunkt der Realisierung festzulegen. Bei einer komplexen Umsetzung ist zu überlegen, ob eine Schulung der Mitarbeiter sinnvoll ist.

12 Revision

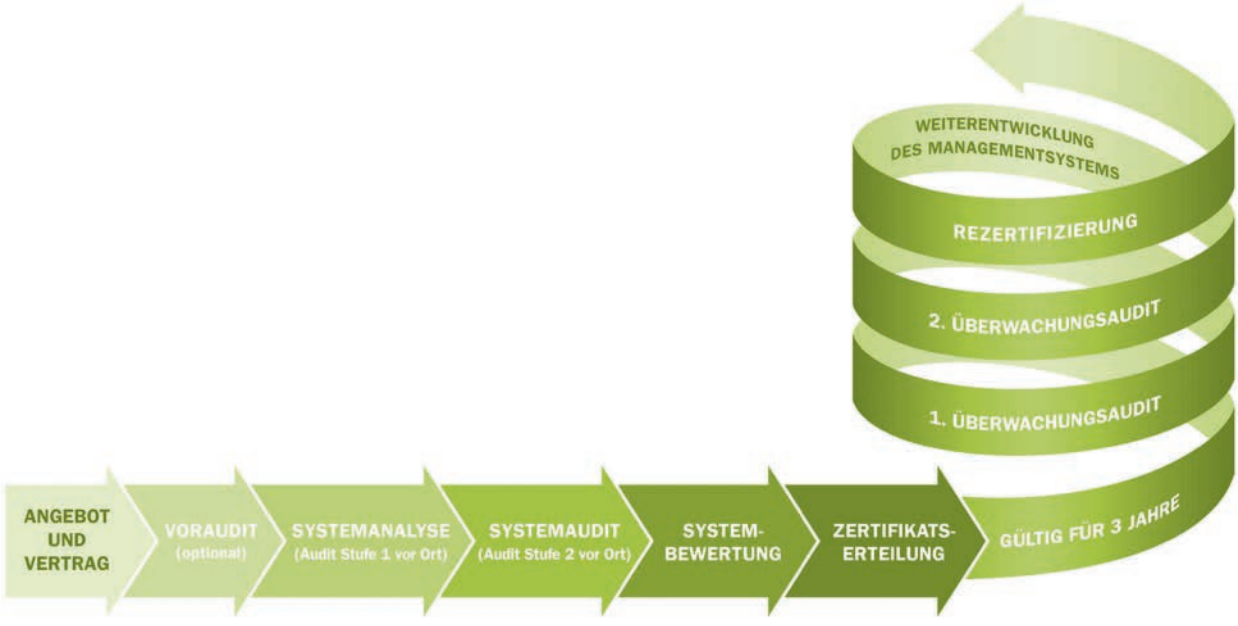
Mit dem Abschluss des Schrittes fordert die ISIS12-Software zur Eingabe eines Revisionstermins für eine oder mehrere Maßnahmen auf. Die gescannte Revisionsliste wird in Schritt 12 erzeugt.

ZERTIFIZIEREN NACH ISIS12

→ DEUTSCHE GESELLSCHAFT ZUR ZERTIFIZIERUNG VON MANAGEMENTSYSTEMEN

Die DQS mit Hauptsitz in Frankfurt am Main fokussiert als einziger großer Zertifizierer die Begutachtung und Zertifizierung von Managementsystemen und Prozessen in Unternehmen und Kommunen. Zum umfangreichen Begutachtungs-Portfolio zählen neben den Schwerpunkten Qualität, Umwelt und Energie auch Themen aus dem Service- und Risikosegment.

Sobald Sie ISIS12 erfolgreich eingeführt haben und der Schritt 12, die Revision, abgeschlossen ist, können Sie sich von der DQS als Exklusivpartner nach ISIS12 zertifizieren lassen. Das Zertifikat hat eine Gültigkeit von drei Jahren. In diesen drei Jahren finden zwei Überwachungsaudits statt. Im dritten Jahr kann durch eine Rezertifizierung das Zertifikat neu erteilt werden.



Zum Nachweis Ihrer erfolgreichen Zertifizierung können Sie zu Werbezwecken das folgende Logo nutzen, zum Beispiel auf dem Geschäftspapier, auf Broschüren oder im Internet.

DQS ISIS 12

12 ISIS12 FÜR DIE KOMMUNEN

→ IT-PLANUNGSRAT EMPFIEHLT ISIS12 FÜR DIE KOMMUNALE SICHERHEIT

Nach den verbindlichen Vorgaben der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“ des IT-Planungsrates haben auch Kommunen in Deutschland bis 2018 ein Informations-Sicherheitsmanagementsystem (ISMS) einzurichten, wenn sie Ebenen-übergreifende IT-Verfahren nutzen. Das Verfahren ISIS12 bietet Verwaltungen ein hohes Maß an Informationssicherheit mit vergleichsweise geringem Aufwand.

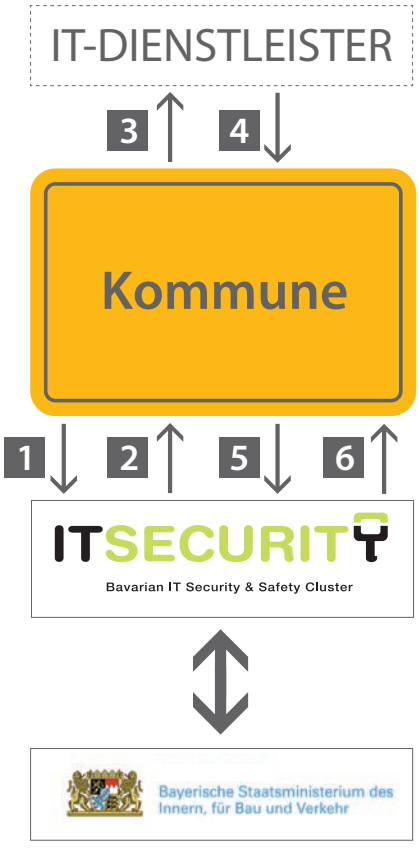
Ein vom Freistaat Bayern bei Fraunhofer AISEC in Auftrag gegebenes Gutachten bestätigt ebenfalls, dass sich ISIS12 an der BSI IT-Grundschutzmethodik orientiert und die Mindestanforderungen des IT-Planungsrats an ein ISMS erfüllt. Die erforderlichen Sicherheitsmaßnahmen können mit ISIS12 bei kleineren und mittleren Kommunen als Einstieg in ein ISMS vergleichsweise leicht umgesetzt werden. Insbesondere eigne sich ISIS12 auch als Grundlage für die spätere Einführung eines ISMS auf Basis von ISO 27001 oder des BSI IT-Grundschutzes.

Auch die Kommunalen Spitzenverbände kommen in ihrer „Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen“ zu dem Ergebnis, dass ISIS12 eine Grundlage für den Ausbau eines Leitlinien-konformen ISMS in Kommunen darstellt.

Alexander Schmidlkofer, Systemadministrator der Stadt Dingolfing:

> ***„Gerade Kommunalverwaltungen sind es den Bürgern schuldig, sich beim Thema Datensicherheit regelmäßig auf den Prüfstand zu stellen. Das ISIS12-Verfahren ist für eine Verwaltung unserer Größe kosten-, zeit- und ressourcenschonend umsetzbar. Vor allem bekommt man durch die externen Berater einen anderen Blick auf das Thema.“***

FÖRDERUNG DER INFORMATIONSSICHERHEIT BEI KOMMUNALEN GEBIETSKÖRPERSCHAFTEN



1. Elektronischer formgebundener Antrag
2. Bestätigung der Förderfähigkeit und Abschluss des Fördervertrags
3. Beauftragung eines lizensierten IT-Dienstleisters
4. Rechnungsstellung an die Kommune
5. Auszahlungsantrag mit Verwendungsnachweis
6. Auszahlung der Förderung

Bewilligung und Auszahlung gemäß Zuwendungsvereinbarung

Zur Erhöhung des IT-Sicherheitsniveaus in der bayerischen Verwaltung werden Kommunen durch die Förderung bei der Implementierung eines Informations-Sicherheitsmanagementsystems durch das Bayerische Staatsministerium des Inneren, für Bau und Verkehr unterstützt. Dieses dient der Entwicklung einer Schutzstrategie und der Umsetzung entsprechender Maßnahmen zur Sicherung der Verfügbarkeit, der Vertraulichkeit und der Integrität von IT-Systemen und Daten. Einmalig förderberechtigt sind alle bayerischen kommunalen Gebietskörperschaften und deren Zusammenschlüsse sowie die von ihnen in öffentlich-rechtlicher Form geführten Unternehmen und Einrichtungen mit Sitz in Bayern mit bis zu 500 (IT-) Arbeitsplätzen. Förderfähige Ausgaben in Rahmen einer Einführung von ISIS12 sind:

- Beratungsdienstleistungen bei der Implementierung von ISIS12
- Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter
- Erstzertifizierung des Managementsystems zur Informationssicherheit nach ISIS12

Die Förderung erfolgt in Form einer Anteilsfinanzierung in Höhe von bis zu 50 % der zuwendungsfähigen Ausgaben, maximal 15.000 EUR.

Interessierte Kommunen wenden sich direkt an den Projektträger, den Bayerischen IT-Sicherheitscluster e.V. in Regensburg.

12 ISIS12 FÜR KLEINE UND MITTELSTÄNDISCHE UNTERNEHMEN

Informationen sind ein wesentlicher Unternehmenswert und müssen entsprechend abgesichert werden – am besten ganzheitlich, in einem so genannten Informations-Sicherheitsmanagementsystem. Diese Forderung gilt auch für kleine und mittelständische Unternehmen, für die jedoch die bestehenden Standardverfahren wie der BSI IT-Grundschutz oft zu komplex und zu teuer sind. Mit „ISIS12" bietet der Bayerische IT-Sicherheitscluster e.V. eine neue, einfachere Lösung, um das IT-Sicherheitsniveau in Unternehmen zu erhöhen.

Quirin Pasquay, Geschäftsführer pascom Netzwerktechnik GmbH & Co. KG:

> ***ISIS12 überzeugt durch seine sehr praxisnahe Vorgehensweise. Somit konnten wir nicht nur den Anforderungen als Telekommunikationsanbieter gerecht werden, sondern auch den Betrieb unserer IT nachhaltig verbessern. Dadurch steht auch dem weiterem Wachstum der IT und folglich auch des Unternehmens nichts mehr entgegen.***

Besondere Empfehlung von ISIS12 auch für mittelständische Unternehmen

In einem Schreiben an den Präsidenten des Bayerischen Handelskammertags spricht sich Innenminister Joachim Herrmann ausdrücklich für das Informationsmanagementsystem ISIS12 für kleine und mittlere Unternehmen aus. Der Bayerische IT-Sicherheitscluster e.V. habe mit nur 12 konkreten Schritten ein ISMS entwickelt, das es ermöglicht, die Informationssicherheit durch klare Handlungsempfehlungen auf ein hohes, aber dennoch vom Aufwand leistbares Maß zu steigern. Herrmann plädiert daher für die Verbreitung von ISIS12 im bayerischen Mittelstand: „Bayern soll auch digital das sicherste Bundesland bleiben und ich bitte Sie, sich für die Umsetzung von ISIS12 in Ihren Unternehmen einzusetzen", so der Minister in dem Schreiben.

ISIS12 FÜR DIENSTLEISTER

Sie wollen ISIS12 in das Dienstleistungsportfolio Ihres Unternehmens aufnehmen? Dann bewerben Sie sich als ISIS12-Lizenznehmer beim Bayerischen IT-Sicherheitscluster e.V. Die dafür notwendigen Kriterien finden Sie auf unserer Webseite. Als ISIS12-Lizenznehmer besitzen Sie das Recht, ISIS12 in Unternehmen und Kommunen einzuführen. Hierfür werden Ihnen das ISIS12-Handbuch, der ISIS12-Katalog, sowie die ISIS12-Software zur Verfügung gestellt. Sie werden speziell für ISIS12-Verfahren geschult. Des Weiteren bieten wir Ihnen jährlich ein Treffen an, bei dem Sie sich zu Ihren Erfahrungen mit den zertifizierten ISIS12-Beratern austauschen können. Das Bayerische IT-Sicherheitscluster e.V. vermarktet für Sie ISIS12 bei Veranstaltungen, über Pressepublikationen und über die ISIS12-Website.

Neben der Unternehmenslizenzierung erfolgt auch die Ausbildung zum zertifizierten ISIS12-Berater. Für die Personenzertifizierung nach ISIS12 müssen Sie eine ISIS12-Schulung besuchen. Als Voraussetzung dafür müssen Sie bestimmte Qualifikationen nachweisen, die Sie auf unserer Webseite einsehen können.

Haben wir Ihr Interesse geweckt? Dann nehmen Sie gerne Kontakt mit uns auf.

Herausgeber
Bayerischer IT-Sicherheitscluster e.V.

info@it-sec-cluster.de
www.isis12.de
www.it-sicherheit-bayern.de

Redaktion
Tanja Braun
Sandra Wiesbeck

Titelbilder
www.fotolia.de
www.shutterstock.com

Konzept & Gestaltung: www.valentum-kommunikation.de