IT-Sicherheit aus einer Hand

cirosec

Willkommen bei cirosec – Kompetente IT-Sicherheit aus einer Hand

Wir sind ein spezialisiertes Unternehmen mit Fokus auf IT- und Informationssicherheit und beraten unsere Kunden im deutschsprachigen Raum.

Gegründet wurde cirosec im Jahr 2002 von einem erfahrenen Team aus der Sicherheitsbranche. Heute beschäftigt cirosec über 30 Mitarbeiter, darunter viele langjährig erfahrene, bekannte IT-Sicherheitsexperten, die Sie mit großem Sachverstand beraten.

Unser Ziel ist es, Ihnen fachliche Beratung und Schulungen auf höchstem Niveau zu bieten. Um den Anforderungen gerecht zu werden, sind Research-Tätigkeiten von Beratern an der Tagesordnung. Aktuelle Themen, Methoden oder Werkzeuge werden in diesem Rahmen analysiert und aufbereitet. Darüber hinaus sind wir regelmäßig auf weltweit führenden Konferenzen und IT-Security-Messen vertreten, um mit den neuesten Entwicklungen der Branche vertraut zu sein.

Mit cirosec können Sie sich sicher sein, einen kompetenten und zuverlässigen Ansprechpartner für die aktuellen und zukünftigen Herausforderungen der IT- und Informationssicherheit gefunden zu haben.

Wir sind vor allem in folgenden Bereichen tätig:

- Konzepte, Reviews, Analysen
- IT-Sicherheitsmanagement-Beratung
- Audits und Penetrationstests
- Incident Response und Forensik
- Implementierung von Produkten und Lösungen
- Trainings

KONZEPTE, REVIEWS UND ANALYSEN

Erfahrung und Herstellerneutralität ermöglichen anspruchsvolle Konzepte und Analysen.

Wir verfügen über langjährige Erfahrung in der Konzeption sowie Implementierung komplexer Sicherheitsumgebungen. Als herstellerunabhängiges Beratungsunternehmen können wir eine neutrale Konzeption gewährleisten. Zugleich unterhalten wir jedoch Beziehungen zu allen relevanten Herstellern von Sicherheitslösungen – dadurch können wir Konzepte nicht nur theoretisch, sondern auch praxisnah gestalten.

Ebenso kompetent führen wir Reviews Ihrer Konzepte und Architekturen durch, um Schwachstellen und fehlende oder auch unangemessene Maßnahmen aufzudecken und Verbesserungen zu empfehlen.

Als Grundlage für Konzepte dienen oftmals Risikoanalysen: Zunächst analysieren wir die größten Risiken und welche Maßnahmen geeignet sind, um sie auf ein akzeptables Niveau zu reduzieren.

Wo technische Maßnahmen oder Werkzeuge zur Risikoreduzierung nötig sind, helfen wir, eine Strategie unter Berücksichtigung verfügbarer Technologien festzulegen. Entscheidend dabei ist das Gesamtkonzept, sodass alle benötigten Techniken und organisatorischen Aspekte miteinander kompatibel sind, sich optimal ergänzen und zu den Prozessen und Strukturen im Unternehmen passen.

In den folgenden Bereichen führen wir nicht nur regelmäßig Risikoanalysen durch, sondern empfehlen auch Maßnahmen, erstellen Konzepte und Architekturen oder bewerten vorhandene Konzepte und Policies:

- Mobile Endgeräte und Projekte rund um „Bring your own Device“
- Interne Netzwerke, Internetanbindungen und DMZ-Strukturen
- Portale, Web-Applikationen und Web Services
- Server- und Endgerätesicherheit sowie Serverhärtung

Unsere typischen Leistungen:

- Individuelle Bedrohungs- und Risikoanalysen für IT-Vorhaben
- Gegenüberstellung von möglichen Maßnahmen zur Reduzierung von Risiken in Verbindung mit dem jeweiligen Aufwand und den Kosten
- Herstellerneutrale Erstellung von Sicherheitskonzepten
- Review existierender Konzepte und Architekturen sowie Empfehlung von Verbesserungen

INFORMATIONSSICHERHEITSMANAGEMENT-BERATUNG

ISO 27001, Risiko- und Compliance-Management, Prozesse, Policies, Richtlinien

Die meisten Informationen werden heutzutage mit Mitteln der Informationstechnik verarbeitet und gespeichert. Auch die Geschäftsprozesse im Unternehmen sind in der Regel maßgeblich von einer funktionierenden IT abhängig.

Um die aus dem Einsatz von Informationen und IT resultierenden Risiken zu erkennen, sie transparent zu machen und um ein bedarfsgerechtes Schutzniveau zu erreichen, wird ein professionelles Informationssicherheitsmanagement benötigt. Es muss von der Unternehmensführung getragen, im gesamten Unternehmen als Prozess gelebt und in das unternehmensweite Sicherheitsmanagement eingebettet sein.

Für die Einführung, Umsetzung, Kontrolle und kontinuierliche Verbesserung eines solchen Informationssicherheitsmanagementsystems (ISMS) ist es empfehlenswert, sich an anerkannten Standards wie ISO/IEC 27001:2013 zu orientieren.

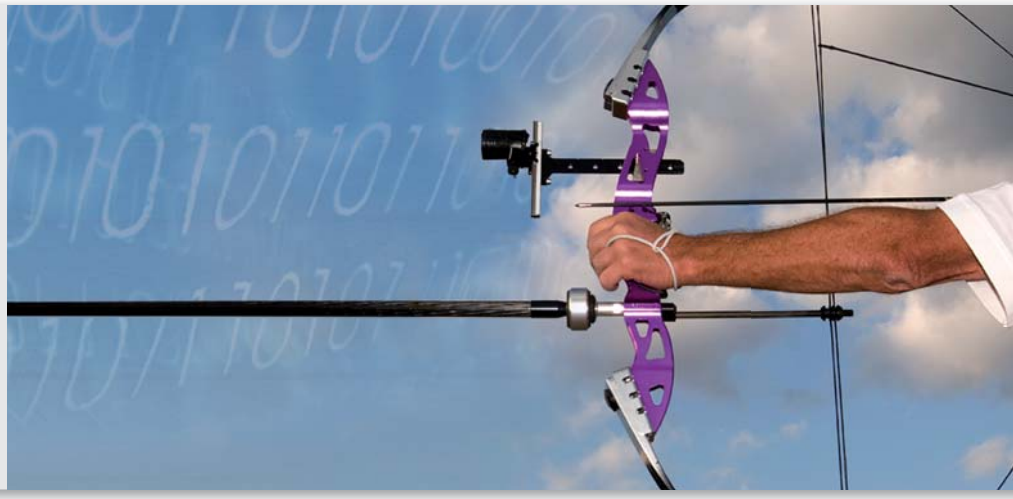
cirosec begleitet Sie bei der Einführung, Standortbestimmung, Verbesserung, Überprüfung oder Zertifizierung Ihres Informationssicherheits- und Risikomanagementprozesses. Selbstverständlich berücksichtigen wir Ihre Unternehmenskultur und die vorhandenen Prozesse sowie die für Ihr Unternehmen relevanten Standards (z.B. ISO-27000-Serie), Gesetze und branchenspezifische oder unternehmensinterne Vorgaben.

Darüber hinaus unterstützen wir Sie bei der Erstellung von Policies und Richtlinien. Gerne aktualisieren wir auch bereits vorhandene Richtlinien, um sie an neue Technologien und geänderte Bedrohungslagen anzupassen.

Ebenso beraten wir Sie zu Möglichkeiten und Einsatzbereichen, aber auch Grenzen sogenannter Governance-, Risk-Management- und Compliance-Werkzeuge in Ihrem Unternehmensumfeld. Als herstellerunabhängiger Berater unterstützen wir Sie bei der Auswahl des für Sie am besten geeigneten Produkts. Selbstverständlich können wir die Lösung auch liefern, implementieren und konfigurieren.

Zudem ist durch cirosec eine Ausbildung zum Lead Implementer, Lead Auditor oder Lead Incident Manager möglich.

AUDITS UND PENETRATIONSTESTS



Schwachstellen finden und angemessen bewerten

Durch unsere fundierten Kenntnisse der aktuellen Angriffstechniken und Methoden und unsere langjährige Erfahrung im Bereich von Audits und Penetrationstests können wir Ihre IT-Lösungen nicht nur auf der konzeptionellen Ebene auf potentielle Sicherheitsrisiken hin untersuchen, sondern auch tatsächlich vorhandene technische und organisatorische Schwachstellen finden und angemessen bewerten.

Entscheidend für erfolgreiche Audits und Penetrationstests sind einerseits die kompetente und professionelle Durchführung der Prüfungen und andererseits die angemessene Bewertung und Präsentation der Ergebnisse für die jeweilige Zielgruppe.

Unser Unternehmensfokus auf Sicherheitsüberprüfungen, die Größe unseres Prüfer-Teams, die Erfahrung und Kompetenz der einzelnen Prüfer, die kontinuierliche Verbesserung unserer Prüfmethoden und Werkzeuge, unsere zielgruppenspezifischen und hochwertigen Auditberichte sowie unsere internen Qualitätssicherungs- und Qualitätsmanagementprozesse gewährleisten erfolgreiche und professionelle Prüfungen.

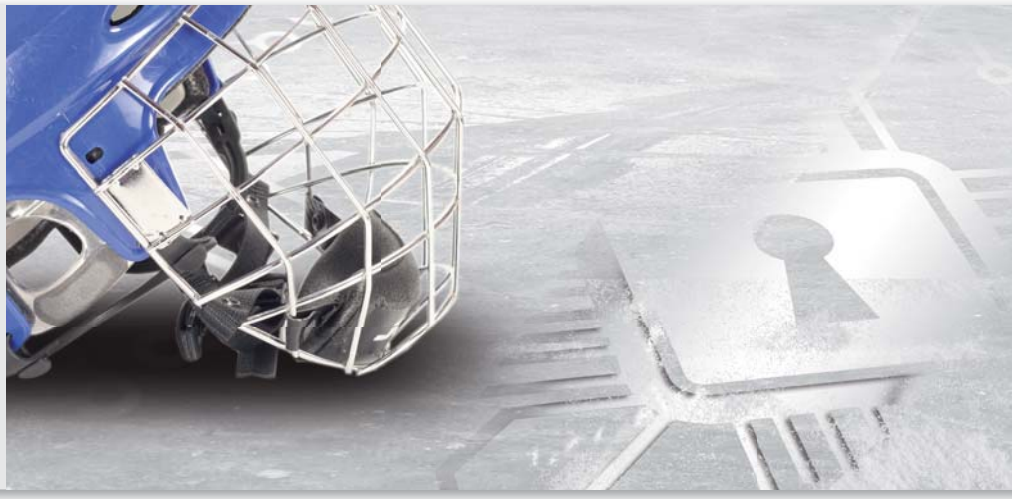
Erfahrung, Orientierung an relevanten Standards und eigene Qualitätsziele sorgen dafür, dass die Ergebnisse verständlich, nachvollziehbar und für das Management verwertbar dargestellt werden.

Wir beraten Sie gerne bereits im Vorfeld, welche Bereiche und Prüfungen im Einzelfall für Sie sinnvoll sind.

Beispiele für Prüfungsaspekte:

- Sicherheit von Web-Applikationen, Web Services und Portalen
- Prüfung mobiler Apps und Embedded Devices am Quellcode oder mit Reverse-Engineering-Techniken
- Netzwerk-Reviews/-Audits
- WLAN-Reviews/-Audits
- Innentäter-Analysen
- Prüfung des ISMS, Überprüfung von Prozessen oder Richtlinien
- Analyse von DMZ-Strukturen
- Systemsicherheit und Härtung von Servern und Endgeräten
- Datenschutz-Audits im Kontext der IT-Sicherheit
- Social Engineering
- Prüfung von Spezialgeräten, Embedded-Systemen oder eigenen Produkten des Kunden

INCIDENT RESPONSE UND FORENSIK



Die Untersuchung möglicher Fälle von Computerkriminalität im eigenen Unternehmen stellt die meisten Organisationen vor große Herausforderungen, denn die technischen, organisatorischen und rechtlichen Rahmenbedingungen sind alles andere als trivial.

Egal, ob es sich um externe Angriffe oder um Innentäter handelt: Oftmals wird den Verantwortlichen nach kurzer Zeit bewusst, dass sie bei der Handhabung des Vorfalls vieles falsch gemacht haben, dass wichtige Spuren bei der Untersuchung vernichtet wurden oder dass aufgrund von Fehlern im Ablauf eine rechtliche Verwertung gefundener Spuren nicht mehr möglich ist.

Wir bieten Ihnen unsere Unterstützung im gesamten Bereich der Behandlung von Sicherheitsvorfällen an.

Wir helfen Ihnen bei der Definition und Implementierung von Prozessen und Richtlinien oder bei der Festlegung sinnvoller Protokollierungseinstellungen für Ihre Systeme. So sind die Abläufe und Verantwortlichkeiten klar geregelt und Sie sind für den Ernstfall gut vorbereitet. Auch können wir Sie bei der Auswahl geeigneter Werkzeuge beraten und Ihnen diese liefern.

Im technischen Bereich unterstützen wir Sie beginnend bei Sofortmaßnahmen, Spurensicherung, Analyse des Tathergangs bis hin zur gerichtsfesten Durchführung und Aufbereitung forensischer Analysen.

Mit unserem Training Forensic Extrem sorgen wir für eine umfangreiche Weiterbildung im Bereich Incident Response und IT-Forensik. Das Training ISO 27035 Lead Incident Manager ermöglicht eine Zertifizierung in diesem Bereich.

IMPLEMENTIERUNG VON PRODUKTEN UND LÖSUNGEN

Technische Sicherheitsmaßnahmen sind häufig an kommerzielle Produkte oder Werkzeuge gekoppelt. Durch unsere langjährige Erfahrung und Herstellerunabhängigkeit garantieren wir nicht nur kompetente Unterstützung bei der Produktauswahl, sondern auch eine reibungslose Umsetzung und Konfiguration in Ihrer Umgebung.

Ziel ist es, die richtige Balance zwischen der bestmöglichen Sicherheit und einem einfachen Betrieb zu erreichen.

Unsere typischen Leistungen sind:

- Herstellerneutrale Konzeption und Beratung bei der Auswahl der Produkte
- Verkauf und Lieferung von Produkten
- Implementierung und Konfiguration
- Erstellen von Betriebskonzepten und Betriebshandbüchern
- Telefonsupport, Troubleshooting und Betriebsunterstützung

TRAININGS & SEMINARE

Wir bieten Ihnen Seminare und Trainings, in denen Ihnen unsere erfahrenen Berater den richtigen Umgang mit den modernen Technologien und neuen Sicherheitsthemen vermitteln.

Bei allen Trainings steht der Praxisbezug im Vordergrund. So steht jedem Teilnehmer jeweils ein Notebook mit zahlreichen Werkzeugen zur Verfügung, sodass er das vermittelte Wissen direkt anhand vieler Übungen und Beispielszenarien praktisch umsetzen kann.

Die Trainings und Workshops finden sowohl in Stuttgart, Köln, München und Hamburg als auch bei Kunden direkt vor Ort als Inhouse-Schulungen statt.

Die Vorteile eines Trainings bei cirosec liegen auf der Hand:

- Erfahrung und Wissen aus erster Hand
- Praxisnahe Schulung durch Berater von cirosec
- Lösungsorientierte Vorgehensweise

v02CRS-14-1929-DE141209 · Bildquellen: istockphoto, shutterstock

cirosec GmbH
Ferdinand-Braun-Straße 4 | 74074 Heilbronn | Deutschland
T +49 7131 59455-0 | F +49 7131 59455-99 | www.cirosec.de

cirosec