Anmeldung an
kundenservice@comconsult-research.de

Einführung von SIEM-Systemen und Mitarbeiterüberwachung nach DSGVO

Ich melde mich verbindlich für das Seminar zum Preis von 1.590,-- € netto für folgenden Termin an:

☐ **06.05. - 07.05.19 in Düsseldorf**

☐ **02.12. - 03.12.19 in Düsseldorf**

☐ **Bitte reservieren Sie für mich ein Hotelzimmer**

vom _____ bis _____19

_____
Nachname, Vorname

_____
Firma

_____
Adresse

_____
Telefon / E-Mail

Ich habe die Seminarbedingungen zur Kenntnis genommen.

_____
Unterschrift

Ort und Hotel
Leonardo Royal Hotel Düsseldorf Königsallee, Tel.: 0211/3848-0

ComConsult hat im Hotel ein Zimmerkontingent für Sie vorgebucht, nutzen Sie unsere Vorzugspreise. Das Seminar beginnt um 10:00 Uhr und endet am letzten Tag um 16:00 Uhr.

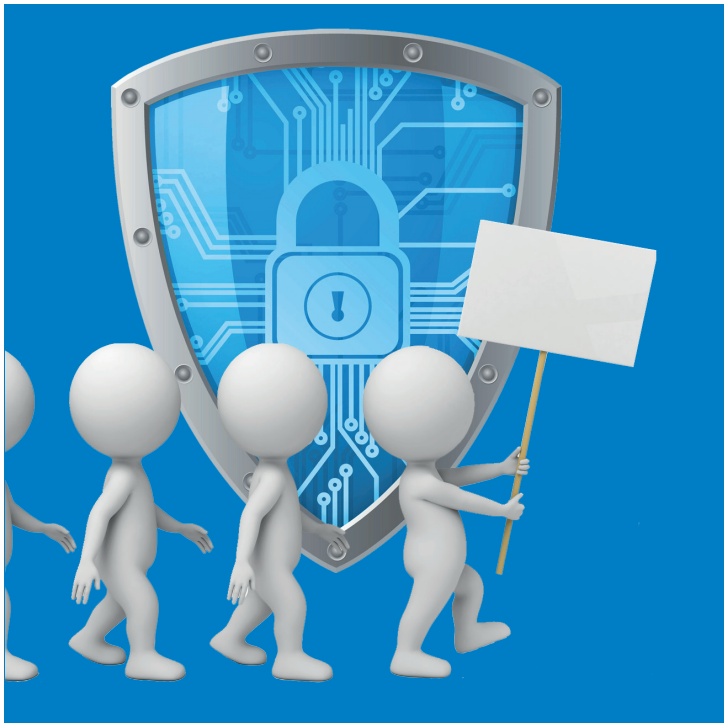
Kosten und Leistungen
Der Preis beinhaltet neben der Teilnahme die Vortragspräsentationen (auch in elektronischer Form), ein Teilnehmerzertifikat, Getränke und Mittagsmenüs an allen Tagen sowie ein Abendessen am ersten Veranstaltungstag.

Seminarbedingungen
Bis zu 14 Tagen vor Seminarbeginn behält sich der Veranstalter das Recht vor, das Seminar zu stornieren. Schriftliche Absagen von Teilnehmern sind bis 31 Tage vor Veranstaltungsbeginn kostenlos möglich. Danach sind je nach Zeitpunkt der Stornierung die Teilnahmekosten wie folgt anteilig zu zahlen: ab 30 Tage 25 %, ab 14 Tage 50 %, ab 7 Tage und bei Nichterscheinen 100 % des Veranstaltungspreises. Die Übertragbarkeit auf andere Mitarbeiter ist jederzeit kostenlos möglich. Bitte informieren Sie uns. Die Seminarkosten sind im Voraus zu entrichten. Der Veranstalter behält sich Änderungen im Programm vor.

Einführung von SIEM-Systemen und Mitarbeiterüberwachung nach DSGVO

insbesondere Umgang mit Pseudonymisierung und Verschlüsselung

Seminar



06.05. - 07.05.19 in Düsseldorf

02.12. - 03.12.19 in Düsseldorf

ComConsult Akademie

Einführung von SIEM-Systemen und Mitarbeiterüberwachung nach DSGVO

Motivation

Das Seminar zeigt, wie sich die neuen Verpflichtungen der Datenschutzgrundverordnung wie z.B. Verschlüsselung und Pseudonymisierung oder höhere Anforderungen an Einwilligungen der Mitarbeiter auf bestehende und neue Systeme, die zur Mitarbeiterüberwachung geeignet sind -insbesondere Security Information & Event Management Systeme, Logdaten und Videoüberwachung – auswirken. Jede Maßnahme, die auch zur Mitarbeiterüberwachung genutzt werden könnte und jede Einführung neuer IT- oder TK-Systeme unterliegt der vollen Mitbestimmung des Betriebs- oder Personalrats nach dem Betriebsverfassungsgesetz bzw. den Personalvertretungsgesetzen.

Sie lernen in diesem Seminar

- Speicherfristen für Logdaten nach der neuesten Rechtsprechung vom August 2018
- Notwendigkeit der Anonymisierung oder Pseudonymisierung nach Art. 32 DSGVO
- in welchen Fällen geschäftliche Daten nach Art. 32 DSGVO verschlüsselt werden dürfen bzw. müssen
- Anforderungen an Übersichten, Live-Überwachung und Berichte von Log- und SIEM-Systemen
- Anforderungen an Videoüberwachung nach DSGVO und neuem BDSG • Mitbestimmungsrechte bei der Auswahl von IT- oder TK-Systemen
- Einbeziehung des Betriebsrates/Personalrates in IT-Projekte • Mitbestimmung bei Fragen der IT-Sicherheit und IT-Nutzung
- Anforderungen an IT-Sicherheit und IT-Sicherheitskonzepte nach der DSGVO
- Zulässigkeit von Überwachung von Gerätedaten, Kommunikationsdaten, Standortdaten, Ortung in besonderen Fällen
- wie biometrische Daten nach Art. 9 DSGVO genutzt werden dürfen
- wie private und geschäftliche Daten nach Art. 5 DSGVO / TKG getrennt werden müssen
- wie die Arbeit des Betriebsrates/Personalrates vor Überwachung geschützt werden kann
- welche Nutzungsbedingungen zulässig sind
- wann Nutzungsdaten aufbewahrt und wann sie gelöscht werden müssen
- welche Kontrollen der Betriebsrat/Personalrat bzw. der Datenschutzbeauftragte durchführen dürfen
- welche Schulungsmaßnahmen erforderlich sind
- was sich durch die neue EU-Datenschutzverordnung in diesem Bereich geändert hat

Zielgruppe

Das Seminar richtet sich an Verantwortliche für Log- oder Videoüberwachung, Betriebs- und Personalräte, Mitglieder der Geschäftsleitung, IT-Verantwortliche, Datenschutzbeauftragte von Behörden und Unternehmen, kaufmännische Leiter, Leiter der Revision und Systemadministratoren.

Zum Inhalt

- Beschränkung der Suche nach Personendaten
- Pflichten zur Verwendung von Pseudonymisierung und Verschlüsselung
- Kriterien für Pseudonymisierung und Depseudonymsierung von Logdaten
- Überwachung bei Einsatz von Datenverschlüsselung
- Standortbestimmung von Mitarbeitern
- Private Nutzung von IT und TK
- Zugriff auf Mailpostfächer
- Mithören und Aufzeichnen von Telefonaten
- Weitergabe von Verbindungsdaten von Mitarbeitern
- Videoüberwachung
- Mitschneiden von Bildschirminhalten
- Verwendung von Biometrie
- Überwachung vs. Sicherheit bei Computern des Betriebsrates
- Trennung privater Daten und geschäftlicher Daten
- Anforderungen an Einwilligungserklärungen
- Anforderungen an Ausbildung und Schulung von Mitarbeitern
- Beispiele:
  - Nutzung von Internet und E-Mail
  - Nutzung von Funknetzen
  - Regeln für Home Office Arbeitsplätze
  - Regeln für Fernwartungszugriffe
  - Einführung von VoIP Telefonanlagen oder CTI-Systemen
  - Einführung von Bring your Own Device
  - Einführung von Mobile Device Management

Der Referent

Ulrich Emmert ist Rechtsanwalt in der Kanzlei esb Rechtsanwälte. Ein Schwerpunkt seiner Tätigkeit sind Beratungen und Schulungen im Bereich des EDV-, Telekommunikations– und Online-Rechts. Dabei kommen ihm umfangreiche technische Kenntnisse im Bereich Programmierung, Datenbanken und Internet-Security zugute, die auch eine qualifizierte Beratung im Bereich Netzwerksicherheit, Softwarelizenzverträge oder Datenschutz ermöglichen.