aldb
wir vernetzen deutschland

BERATUNGS-LEISTUNGEN

für die Beteiligten des Digitalfunk BOS und Netze des Bundes

„Unsere Beratungskompetenz für Ihre Qualität“

LIEBE LESERINNEN UND LESER,

es ist Zeit, neue Wege zu gehen und unser Angebot gezielt zu erweitern. Mit großer Freude präsentieren wir Ihnen unsere neue Beratungsrichtung, die sich auf Sicherheitsthemen für Organisationen mit systemkritischen Infrastrukturen spezialisiert hat. Diese Ausrichtung basiert auf unseren einzigartigen Fachkompetenzen und wurde entwickelt, um Qualität und Effizienz in diesen essenziellen Bereichen nachhaltig zu steigern.

Der Aufbau des Beratungsportfolios befindet sich derzeit noch in Entwicklung. Mit diesem Schritt legen wir die Grundlage für ein umfassendes und vielseitiges Angebot, das künftig weitere zentrale Themen aufnehmen und die Beratung auf eine noch breitere Basis stellen wird.

Wir laden Sie ein, sich mit uns auf diese spannende Reise zu begeben, um gemeinsam neue Maßstäbe in der Beratung zu setzen. Mit Begeisterung und Engagement arbeiten wir daran, Ihre Herausforderungen mit Lösungen zu begegnen, die Sicherheit, Effizienz und Vertrauen stärken.

Herzliche Grüße,

Ihre ALDB

INHALT

WISSENSWERTES ZUR BERATUNGSPLANUNG 6
Formate und Kosten 6
Zielgruppe und Voraussetzungen 7
ÜBER UNS 8
AUFNAHME IN UNSEREN NEWSLETTER 9
KONTAKT ZU UNS 9

UNSERE BERATUNGSANGEBOTE

BSI IT-GRUNDSCHUTZ 12
PENETRATIONSTESTS 14
LOGSOURCE 16
NETZMODERNISIERUNG 18
IPV6-NETZWERK 20

WISSENSWERTES ZUR BERATUNGSPLANUNG

Beratungsformate

Um sicherzustellen, dass unsere Beratungsleistungen bestmöglich auf Ihre Bedürfnisse abgestimmt sind, bieten wir **flexible Formate** an. Je nach Inhalt und Anforderungen kann die Beratung sowohl online als auch vor Ort erfolgen. Die **Online-Beratung** ermöglicht eine schnelle, unkomplizierte und ortsunabhängige Kommunikation und bietet ein hohes Maß an Flexibilität.

Für komplexere Fragestellungen oder wenn der direkte **Austausch vor Ort** erforderlich ist, stehen wir Ihnen selbstverständlich auch persönlich zur Verfügung. Die Präsenzberatung ermöglicht ein noch tieferes Verständnis Ihrer spezifischen Anforderungen.

Beratungskosten

Ein initiales Gespräch sowie eine **Erstberatung** sind in der Regel **kostenfrei**. Dies gibt uns die Möglichkeit, Ihre individuellen Anforderungen zu verstehen und gemeinsam erste Lösungsansätze zu entwickeln.

Basierend auf dem identifizierten Bedarf erstellen wir ein **maßgeschneidertes Kostenangebot**. Die Abrechnung erfolgt auf Grundlage eines Beratertagessatzes. So können wir sicherstellen, dass unsere Leistungen optimal auf Ihre Bedürfnisse abgestimmt sind und Sie maximale Wertschöpfung erhalten.

Zielgruppe und Voraussetzungen

Mit unserem Beratungsangebot sprechen wir **sowohl öffentliche Einrichtungen als auch private Unternehmen** an, die in den essenziellen Bereichen systemkritischer Infrastrukturen tätig sind.
Die Voraussetzungen für eine Beratung variieren je nach Beratungsinhalt. Gemeinsam evaluieren wir Ihren individuellen Bedarf und klären, welche Rahmenbedingungen erforderlich sind, um die Beratung optimal auf Ihre Ziele abzustimmen. Unser Fokus liegt darauf, Lösungen zu entwickeln, die Ihren spezifischen Anforderungen entsprechen und nachhaltigen Mehrwert schaffen.

ÜBER UNS

UNSERE LEISTUNGEN

Maßgeschneiderte Schulungen

Wir vermitteln praxisnahes Wissen zu aktuellen technischen Standards und Best Practices.

Individuelle Beratung

Wir analysieren Ihre spezifischen Anforderungen und entwickeln maßgeschneiderte Beratungskonzepte.

Expertenwissen aus erster Hand

Profitieren Sie von der langjährigen Erfahrung unserer Fachleute und deren einzigartigem Know-how.

WARUM WIR

Spezialisierung

Wir konzentrieren uns ausschließlich auf die Sicherheit kritischer Infrastrukturen.

Kompetenz

Unser Team verfügt über umfassende Expertise in allen relevanten Bereichen.

Expertenwissen aus erster Hand

Wir entwickeln Lösungen, die exakt auf Ihre Bedürfnisse zugeschnitten sind.

AUFNAHME IN UNSEREN NEWSLETTER

Melden Sie sich für unseren Newsletter an!

Gern informieren wir Sie regelmäßig über unsere neuesten Einblicke, Veranstaltungen und Angebote aus dem Bereich „Schulung und Beratung“.

Schreiben Sie uns hierfür eine E-Mail an schulung@aldb.org.

Wir freuen uns auf Ihre Teilnahme!

KONTAKT ZU UNS

E-Mail
schulung@aldb.org

Telefon
030 565555-150

Standort
Dernburgstraße 50
14057 Berlin

www.aldb.org/schulung-und-beratung

designed by freepik

BSI IT-GRUNDSCHUTZ

Umsetzung nach BSI Standard 200-x in Sicherheitsnetzen

Der BSI-Grundschutz ist eine Methodik des Bundesamts für Sicherheit in der Informationstechnik (BSI), die darauf abzielt, ein hohes Maß an Informationssicherheit in Organisationen zu gewährleisten.

Nutzen Sie unsere umfassenden Kompetenzen und Erfahrungen im Umfeld von Hochsicherheitsnetzwerken!

Wir beraten Sie!

Unsere Fachexperten geben Ihnen einen umfassenden Überblick über die notwendigen Grundlagen des BSI IT-Grundschutz-Standards sowie wertvolle Empfehlungen zur praktischen Umsetzung des IT-Grundschutz Kompendiums.

Wir unterstützen Sie dabei, maßgeschneiderte IT- Sicherheitskonzepte zu entwickeln und organisationseigenen Anforderungen entsprechend zu implementieren. Gemeinsam prüfen wir, welche Voraussetzungen zur Anbindung an behördliche Sicherheitsnetze bereits vorhanden sind oder noch erfüllt werden müssen.
Bitte beachten Sie: Eine Begleitung oder Durchführung einer IT-Grundschutzzertifizierung ist von dem Beratungsangebot ausgeschlossen.

Beratungsmodule

1 ALLGEMEINES

Überblick und Bedeutung zum BSI IT-Grundschutz

Zielsetzung und Rahmenbedingungen des Projekts

2 IST-ANALYSE

Analyse der bestehenden IT-Infrastruktur und Sicherheitsmaßnahmen

Identifikation von Schutzbedarfen und Sicherheitsanforderungen

3 RISIKOBEWERTUNG

Durchführung einer Risikoanalyse gemäß BSI-Standards

Identifizierung und Bewertung möglicher Bedrohungen und Schwachstellen

4 MASSNAHMEN-KATALOG PLANEN

Erarbeitung basierend auf BSI IT-Grundschutz

Priorisierung und Planung konkreter Schutzmaßnahmen

5 IMPLEMENTIERUNG UND INTEGRATION

Einführung technischer, organisatorischer und personeller Maßnahmen

Integration der Sicherheitsmaßnahmen in bestehende Prozesse

6 SENSIBILISIERUNG

Sensibilisierung der Mitarbeiter für IT-Sicherheitsmaßnahmen im täglichen Betrieb

7 ÜBERWACHUNG UND KONTINUIERLICHE VERBESSERUNG

Etablierung eines Prozesses zur regelmäßigen Überprüfung und Aktualisierung der Sicherheitsmaßnahmen

Sicherstellung der Compliance und Anpassung an neu Bedrohungslagen

8 ABSCHLUSS UND ÜBERGABE

Zusammenfassung der Ergebnisse und Abschlussbericht

Übergabe von Dokumentation und ggf. Zertifizierungsvorbereitung

Informationen zur Schulung

Zielgruppe: Betriebliche Mitarbeiter der Autorisierten und Koordinierenden Stellen, Behörden und Ministerien

Format: Vor-Ort-Beratung am ALDB Standort, Online-Beratung

Produktnummer: B-401

PENETRATIONSTESTS

Unterstützung und Durchführung zur Netzabsicherung

Die Sicherheit von Netzwerken und Systemen ist in Zeiten von Cyberangriffen und Sicherheitslücken von höchster Bedeutung. Penetrationstests, auch Pentests genannt, sind eine proaktive Methode zur Bewertung der Sicherheit eines Netzwerks oder Systems. Dabei werden reale Angriffe simuliert, um Schwachstellen aufzudecken und Angreifern entgegenzuwirken.

Wir beraten Sie!

Wer vermitteln Ihnen die notwendigen Grundlagen zum Thema. Gerne begleiten wir Sie bei der Vorbereitung und Planung von Pentests sowie deren erfolgreiche Durchführung. Ebenfalls unterstützen wir auch gern bei der Analyse und Nachbereitung von Ergebnissen und beraten Sie hinsichtlich aufkommenden Schwachstellen, wie mit diesen umzugehen ist und verhindert werden können.

Beratungsmodule

1 ZIELSETZUNG

Umfang und Ziel definieren

Identifikation der zu schützenden Werte und Testziele

Abgleich mit Unternehmenssicherheitsrichtlinien und Compliance-Anforderungen

2 PLANUNG

Testumfang und Testarten bestimmen

Ressourcen und Zeitaufwand festlegen

3 RECHTLICHES

Dokumentation des Vorgehens

Vertraulichkeits- und Haftungsklärungen (Geheimschutz, Genehmigungen)

Festlegung der Eskalations- und Notfallprozesse

4 INFORMATIONSBESCHAFFUNG UND -ANALYSE

Sammlung von Informationen über Zielsysteme (OSINT, Netzwerkstrukturen)

Identifikation von Schwachstellen und potentiellen Angriffspunkten

Erstellung eines Testplans

5 DURCHFÜHREN DES PENTESTS

Phase 1: Identifikation und Scanning (Port-Scans, Schwachstellenscans)

Phase 2: Exploitation (Test von Schwachstellen, Proof-of-Concept-Angriffe)

Phase 3: Post-Exploitation (Analyse von Zugriffsmöglichkeiten und Datenzugriff)

6 ERGEBNISSE UND RISIKOBEWERTUNG

Auswertung von Schwachstellen und Sicherheitslücken

Risikobewertung gemäß Unternehmensstandards und Compliance-Anforderungen

Entwicklung von Handlungsempfehlungen

7 ABSCHLUSSBERICHT

Erstellung eines detaillierten Berichts mit Ergebnissen, Risiken und Maßnahmenvorschlägen

Entwicklung von Handlungsempfehlungen

8 NACHBEREITUNG UND VERBESSERUNG

Erstellung eines Maßnahmenplans zur Behebung gefundener Schwachstellen

Informationen zur Schulung

Zielgruppe: Betriebliche Mitarbeiter der Autorisierten und Koordinierenden Stellen
Format: Vor-Ort-Beratung am ALDB Standort

Produktnummer: B-402

LOGSOURCE

Analyse und Identifikation von technischen Problemstellungen

Das SOC meldet oftmals und insbesondere Sicherheitsvorfälle aus dem ZTB, welche durch das Wirknetz Digitalfunk BOS kommen und ihren Ursprung in den ASen haben. Aktuell werden diese Informationen auf technischem Wege an die BDBOS kommuniziert für die Beseitigung, die wiederum die Aufgaben oftmals unmittelbar weiterleiten. Die nachfolgenden Rückfragen und außergewöhnlich hohen Reaktionszeiten zeigen jedoch, dass kein greifbares Verständnis existiert, wie man strukturiert die Meldungen annimmt und mit deren Hilfe man Fehlerquellen findet.
Ziel soll die Förderung von analytischen Vorgehensweisen und -Verständnis sein.

Wir beraten Sie!

Gern bieten wir Ihnen eine „Vorort“-Beratung an. Dabei bedarf es entsprechender Berechtigung und Kenntnisse seitens verantwortlicher IT-Mitarbeiter Ihrer Organisation. Es bedingt umfangreiche Erfahrungen und Kenntnisse der Informatik im Allgemeinen sowie lokale Kenntnisse der Infrastruktur inkl. Berechtigung.

Beratungsmodule

1 FUNKTIONS-WEISE DES SOC

2 ERKENNTNISSE DES SOC

3 PROZESSE UND MELDEKETTEN

4 LESEN UND INTERPRETIEREN VON ÜBERMITTEL-TEN SICHERHEITS-VORFÄLLEN

5 ANWENDEN AUF IT-NETZWERKE UND -SYSTEME

Informationen zur Schulung

Zielgruppe: Betriebliche Mitarbeiter der Autorisierten und Koordinierenden Stellen, Behörden und Ministerien, sowie weitere Teilnehmer an den vom SOC überwachten Netzen

Format: Vor-Ort-Beratung beim Nutzer

Zu beachten: dient als theoretische/ praktische Ergänzung zu: Administrative-/IT Security Tätigkeiten; entsprechende Berechtigung und Kenntnisse notwendig, sowie umfangreiche Erfahrungen und Kenntnisse der Informatik im Allgemeinen und lokale Kenntnisse der Infrastruktur inkl. Berechtigung

Produktnummer: B-403

NETZMODERNISIERUNG

Betriebliche Änderungen durch die Netzmodernisierung

Die ALDB ist einziger Betreiber im Digitalfunknetz!

Die Netzmodernisierung bringt umfangreiche Änderungen im Digitalfunk mit sich. Nicht nur die System- und Anbindungstechnik ändert sich, auch die Werkzeuge zum Betreiben des Netzes werden kontinuierlich weiterentwickelt.

Wir beraten Sie!

Diese Modernisierungsmaßnahmen im Digitalfunk im Kern- und Zugangsnetz beeinflussen das Arbeitsumfeld und die Arbeitsweise der Autorisierten Stellen der Länder. Wesentliche Auswirkungen gibt es auf die verschiedenen betrieblichen Tools des Digitalfunk. Um Ihnen Sicherheit im Umgang mit den neuen Systemen zu geben, möchten wir Sie gezielt über die Änderungen informieren und Ihnen beratend zur Seite stehen.

Unser Angebot richtet sich insbesondere an die Nutzer, die Fragen rund um die Zugangsnetzmigration haben. Wir werden diese Beratungsleistung speziell auf Ihre Bedürfnisse ausrichten.

Beratungsmodule

1 TECHNISCHE MASSNAHMEN DER NETZMODERNISIERUNG

Umsetzung in der Praxis

Neue Netzarchitektur/Netzelemente

Änderungen in der Leitstellenanbindung

Landespezifische Besonderheiten

2 BETRIEBLICHE ÄNDERUNGEN UND HERAUSFORDERUNGEN

Spezifische und bekannte Fehlerbilder

Auswirkungen von Funkschutz in der neuen Netzinfrastruktur

Überblick Notfall- und Ausfallkonzept

3 ÄNDERUNGEN IN DEN TOOLS

Umbrella Management System

Tactilon

Nutzerbezogene Fragen zu spezifischen Tools

Informationen zur Schulung

Zielgruppe: Betriebliche Mitarbeiter der Autorisierten Stellen
Format: Vor-Ort-Beratung beim Nutzer

Produktnummer: B-404

IPV6-NETZWERK

Test von Fachanwendungen zur Funktion mit IPv6

Die Einführung von IPv6 eröffnet zahlreiche neue Möglichkeiten in der Netzwerktechnologie. Funktionen wie automatisches Adressmanagement, integrierte Sicherheit durch IPsec und erweiterte Unterstützung für mobile Endgeräte machen IPv6 zu einer Schlüsseltechnologie für die Weiterentwicklung von Netzwerkinfrastrukturen. Mit diesen Vorteilen können die steigenden Anforderungen der digitalen Welt optimal bedient werden.

Wir beraten Sie!

Sie erhalten eine präzise Übersicht über die Unterschiede zwischen den beiden Protokollen IPv4 und IPv6. Wir unterstützen Sie bei der Bewertung des Einflusses der Protokollumstellung auf die Funktion bestehender Fachverfahren. Für die Überprüfung der Funktionalität wird gemeinsam ein Konzept für eine Testumgebung erarbeitet und ein Testplan erstellt. Wir begleiten Sie bei der Durchführung Ihrer Testfälle und unterstützen Sie bei der objektiven Bewertung der Testergebnisse, um fundierte Entscheidungen treffen zu können.

Beratungsmodule

1. BUSINESS ANALYSE

Erörterung des Fachverfahrens und der zugrunde liegenden Netzarchitektur

Austausch zum Migrationsvorhaben

Erarbeitung von Herausforderungen für die Migration

2. BESONDERHEITEN VON IPV6

Welche Fallstricke gibt es bei eine reinen IPv6-Netzarchitektur?

Ist die für das Fachverfahren eingesetzte Software IPv6-ready?

Gibt es Beispielansätze, die für den konkreten Fall passen und verwendet werden können?

3. UNTERSTÜTZUNG BEI DER TESTPLANUNG

Welche Komponenten hat das IPv6 Testlabor?

Wie kann das Fachverfahren in der Laborumgebung realisiert werden?

Wie muss der Testkatalog gestaltet sein, dass die Fachanwendung umfassend geprüft wird?

4. UNTERSTÜTZUNG BEI DER TESTDURCHFÜHRUNG

Gemeinsame Testdurchführung

Gemeinsame Testauswertung

Informationen zur Schulung

Zielgruppe: Behörden und Bundesministerien
Format: Online-Beratung

Produktnummer: B-405

IHRE GESPRÄCHSNOTIZEN

Herausgeber
ALDB GmbH
Fehrbelliner Platz 3
10707 Berlin

Besucheranschrift
ALDB Schulungscenter
Dernburgstraße 50
14057 Berlin

aldb
wir vernetzen deutschland