Online-Schulung · 7 Stunden · Bescheinigung

Ein Gerät wird übernommen. Danach entscheidet das Netz.

Schutzbedarf und Datenflüsse erheben, in Zonen trennen, Kommunikation kontrollieren, Fernzugriff und Administration absichern, überwachen – und im Vorfall vorbereitet eingrenzen.

Netzwerksicherheit verhindert den Einbruch nicht. Sie entscheidet, was danach möglich ist: ob ein übernommenes Bürogerät Hunderte Systeme erreicht – oder die drei Dienste seiner Zone.

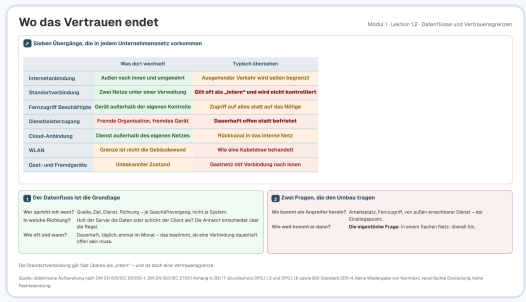
Mit 100-minütiger Architekturwerkstatt: vereinfachter Netzplan, Kommunikationsliste der Fachbereiche und ein fehlerhafter Firewall-Regelauszug – bis zum kommentierten Netzwerkzielbild mit priorisiertem Maßnahmenplan. Sechs Arbeitsaufträge mit verdeckter Musterlösung.

Vier Schritte zur belastbaren Trennung

- **Schutzbedarf erheben**
- **In Zonen trennen**
- **Verbindungen freigeben**
- **Überwachen und eingrenzen**

Netzwerk-sicherheit
8 Module
28 Lektionen
420 Minuten

- **Teilnahme-bescheinigung**
- **8 Begleit-unterlagen**
- **28 Infografiken**



Sieben Grenzen, die fast jedes Unternehmen hat. Lektion 1.2 führt von den Geschäftsvorgängen zu den Stellen, an denen Vertrauen endet. Erst wenn sie benannt sind, lässt sich sagen, wo kontrolliert werden muss.

„Erlaubt, solange nicht verboten"

In diesem Modell ist die Frage „Darf dieses System mit jenem sprechen?" nicht beantwortbar – man müsste alle Verbote kennen und ausschließen, dass eines fehlt.

Die Regel, die nie greift

Eine Sperre unterhalb einer weitreichenden Freigabe wirkt nicht. In der Dokumentation steht seitdem eine Kontrolle, die es im Netz nicht gibt.

Der Zugang, den niemand kannte

Wartungszugänge richtet oft die Haustechnik mit der Anlage ein. Sie stehen in keiner Übersicht – und damit in keiner Prüfung.

8	28	185	420	8	75 %
Module	Lektionen	Quizfragen	Minuten Mindest-bearbeitungszeit	Begleitunterlagen	Bestehensgrenze

Schulung ansehen →

Angebot anfordern →

Herausgeber: Sachverständigenbüro Schulte, Düsseldorf. Die Schulung orientiert sich an DIN EN ISO/IEC 27001 Anhang A (Netzwerksicherheit, Netzwerkdienste, Trennung in Netzwerken, Zugriffskontrolle, Protokollierung) sowie den BSI-Bausteinen NET.1.1, NET.1.2, NET.3.2, NET.2.1, OPS.1.2.5 und DER.1. **Normtexte werden nicht wiedergegeben; die Schulung nennt bewusst keine herstellerspezifischen Konfigurationen und keine allgemeingültigen Regelwerke**; maßgeblich sind Schutzbedarf und Vorgaben Ihrer Organisation. OT wird nur als Abgrenzung benannt. Rechtsstand November 2026. Keine Rechtsberatung.

Warum Netze flach bleiben, obwohl es alle besser wissen.

Das flache Netz ist der Normalzustand. Es entsteht nicht durch eine Entscheidung, sondern dadurch, dass nie eine getroffen wurde: Alles, was angeschlossen wird, kann alles erreichen – und das fällt im Betrieb nie auf, weil es immer funktioniert.

Trennen scheitert an der Unkenntnis. Niemand weiß vollständig, welche Verbindungen gebraucht werden. Wer ohne Erhebung schließt, erzeugt Störungen; wer deshalb nicht schließt, bleibt flach. Die Schulung löst das über eine Beobachtungsphase mit offenen, protokollierten Übergängen.

Das Regelwerk wächst, ohne zu wirken. Eine „vorläufige" Freigabe aus einem Projekt von 2021 hebt die Grundentscheidung für ein ganzes Netz auf. Darunter stehen Sperren, die nie greifen – und in jeder Übersicht als Kontrolle geführt werden.

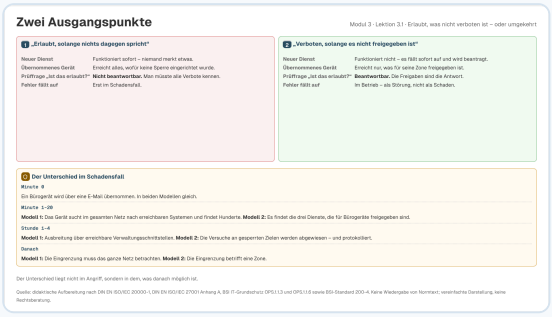
Zugänge überleben ihre Aufträge. Der Auftrag endet beim Einkauf, der Zugang bleibt in der IT. Zwei Stellen, die nicht automatisch voneinander erfahren – deshalb endet ein Zugang technisch, nicht per Erinnerung.

Was die Schulung dagegen setzt

Schutzbedarf je System statt „alles kritisch". Datenflüsse je Geschäftsvorgang. Zonen nach gleichem Schutzbedarf. Ein grundsätzliches Verbot mit begründeten Freigaben. Ein Sprungsystem für Verwaltungszugänge. Vier Wege von außen, vier Behandlungen. Abgewiesene Verbindungen als wichtigste Protokollquelle. Und drei vorbereitete Eingrenzungsstufen mit benannter Befugnis.

BEZUGSRAHMEN

ISO/IEC 27001 Anhang A · **BSI NET.1.1** · **BSI NET.1.2** · **BSI NET.3.2** · **BSI NET.2.1** · **BSI OPS.1.2.5** · **BSI DER.1**



Lektion 3.1: Derselbe Einbruch, zwei Modelle. Im einen findet das übernommene Gerät Hunderte erreichbare Systeme, im anderen die drei Dienste seiner Zone – und jeder abgewiesene Versuch ist zugleich das Signal, dass etwas nicht stimmt.

Fragen, die nach einem Vorfall kommen

1. Was konnte das übernommene Gerät erreichen – und warum?
2. Wer hatte von außen Zugriff, mit welcher Kennung, bis wann?
3. Warum greift die Sperre nicht, die seit 2023 dokumentiert ist?
4. Wer durfte entscheiden, das Netz zu trennen – und wie lange hat es gedauert?
5. Wann wurde zuletzt geprüft, ob die Freigaben noch gebraucht werden?

Die Schulung beantwortet jede dieser Fragen mit einer Vorlage – und mit geschulten Beteiligten, deren Teilnahme dokumentiert ist.

✓ **Die Richtung ist Teil der Regel**
„Arbeitsplatz darf zum Server" ist etwas anderes als die Rückrichtung – und die wird oft „zur Sicherheit" mitgegeben.

✓ **Zwei Geräte im selben Schrank**
teilen Strom, Kühlung und Softwareversion. Das ist keine Redundanz, sondern ein gemeinsamer Ausfallpunkt.

✓ **Trennen will geübt sein**
Ein Gerät in Quarantäne zu verschieben klingt einfach und dauert beim ersten Mal eine Stunde – im Vorfall ist das die falsche Zeit zum Üben.

Ablauf, Nutzen und Inhalte

Die acht Module

1 Schutzbedarf und Netzwerkübersicht
Schutzbedarf je System, Datenflüsse je Geschäftsvorgang und die sieben wiederkehrenden Vertrauensgrenzen. · 35 Min.

2 Zonen und Segmentierung
Was eine Zone ist, der Umbau in vier Schritten, WLAN und Gäste, Cloud, Standorte und die OT-Abgrenzung. · 60 Min.

3 Kommunikationskontrolle
Grundsätzliches Verbot, Regelantrag und Begründung, weitreichende und verdeckte Regeln, Regelpflege und Überprüfung. · 55 Min.

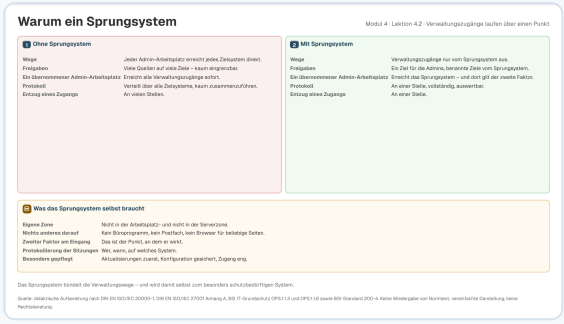
4 Fernzugriff und sichere Administration
Vier Gruppen und vier Wege, Sprungsystem und getrennte Kennungen, Dienstleisterzugänge von Anfang bis Ende. · 50 Min.

5 Sicherer und verfügbarer Betrieb
Härtung und Standardzugänge, Aktualisierung von Netzkomponenten, Konfigurationssicherung, Redundanz und zentrale Dienste. · 55 Min.

6 Überwachung und Reaktion
Was aufgezeichnet wird, wie auffällige Kommunikation erkennbar wird, drei vorbereitete Eingrenzungsstufen. · 40 Min.

7 Architekturwerkstatt
Ein Fall über sechs Lektionen: Netzplan, Kommunikationsliste, Regelauszug, Zonenschnitt, Zugangswege und Maßnahmenplan. · 100 Min.

8 Steuerung und Abschluss
Verantwortlichkeiten, wiederkehrende Prüfungen, Ausnahmen und der Transfer in die eigene Organisation. · 25 Min.



Lektion 4.2: Ohne Sprungsystem erreicht jeder Administrationsarbeitsplatz jedes Zielsystem – die Freigaben sind nicht eingrenzbar, die Protokolle liegen verteilt, und der Entzug eines Zugangs muss an vielen Stellen erfolgen.

Die Architekturwerkstatt

Ein Unternehmen mit zwei Standorten, mobilen Arbeitsplätzen, zentraler Geschäftsanwendung, Cloud-Diensten und einem externen Wartungszugang. Gäste, Bürogeräte und technische Systeme sind unzureichend getrennt. Das Fallpaket enthält einen vereinfachten Netzplan, die Kommunikationsliste der Fachbereiche und einen fehlerhaften Firewall-Regelauszug. Am Ende steht ein kommentiertes Netzwerkzielbild mit priorisiertem Maßnahmenplan – sechs Lektionen, sechs Arbeitsaufträge mit verdeckter Musterlösung.

Für wen

Betrieb: Netzwerk-, System- und Cloud-Administration, Verantwortliche für Firewalls und Fernzugriff, Anwendungsbetreuung mit Netzbezug, Beauftragte für Informationssicherheit. Führung: IT-Betriebsleitung und Teamleitungen, Verantwortliche für Dienstleistersteuerung, IT-Budget und Investitionsentscheidungen.

Acht Begleitunterlagen – dazu 185 Lernkontrollfragen, bestanden ab 75 %

Netzwerkübersicht und Datenflüsse — B1
Modul 1
Was angeschlossen ist, wer von außen hereinkommt – und wo heute tatsächlich kontrolliert wird.

Zonen- und Kommunikationsmatrix — B2
Modul 2/3
Je Verbindung: Quelle, Ziel, Dienst, Richtung, Zweck, Befristung und Freigabe.

Regelantrag und Überprüfung — B3
Modul 3
Sechs Felder je Antrag, die Prüfpunkte vor dem Eintrag – und die vier wiederkehrenden Befunde.

Fernzugriff und Dienstleister — B4
Modul 4
Vier Gruppen, vier Behandlungen – und der bestätigte Entzug, der am häufigsten fehlt.

Administration und Konfiguration — B5 · B6
Modul 4/5
Härtung vor dem Anschluss ans Netz, getrennte Kennungen – und die gemessene Wiederherstellungsdauer.

Entscheidungen und Maßnahmenplan — B7 · B8
Modul 7/8
Die begründete Architekturentscheidung, die befristete Ausnahme und die Reihenfolge nach Wirkung.

So läuft es ab

1 Plätze buchen
Sie teilen uns die Zahl der Teilnehmenden mit; wir richten Ihr Unternehmen im Schulungsportal ein.

2 Einladen
Teilnehmende werden im Portal angelegt und erhalten ihren persönlichen Zugang per E-Mail.

3 Lernen
Acht Module, empfohlen als ein Schulungstag oder zwei halbe Tage.

4 Entwerfen
Hundert Minuten Architekturwerkstatt mit Netzplan, Kommunikationsliste und Regelauszug.

5 Nachweisen
Abschlussprüfung ab 75 Prozent, Bescheinigung als PDF, Auswertung im Portal.

Was Sie erhalten

Zugang je Teilnehmer
Persönlicher Link, Fortschritt wird gespeichert, Bearbeitung in mehreren Sitzungen möglich.

Teilnahmebescheinigung
PDF mit fortlaufender Nummer, Inhalten, Dauer und Prüfadresse zur Online-Verifikation.

Acht Begleitunterlagen
Netzwerkübersicht, Zonenmatrix, Regelantrag, Fernzugriff, Administration, Konfigurationssicherung, Architekturentscheidung, Maßnahmenplan.

Auswertung im Portal
Stand je Teilnehmer, Abschlüsse, Bescheinigungen und Wiederholungsintervalle auf einen Blick.

Erst selbst entwerfen, dann vergleichen

Die Architekturwerkstatt stellt sechs Arbeitsaufträge – von der Ergänzung des vorhandenen Netzplans bis zum priorisierten Maßnahmenplan. Die Musterlösung öffnet sich erst auf Klick, sodass der Entwurf tatsächlich entsteht, bevor er nachgelesen wird. Jeder Auftrag verweist auf die Begleitunterlage, mit der er bearbeitet wird.

Ihr Ansprechpartner

Herausgeber

Heinrich Markus Schulte

IT-Sachverständiger · CISA, CISM, CIPP/E, CEH
Schwerpunkte: NIS-2, DORA, CRA, ISMS

> *„Netzwerksicherheit verhindert den Einbruch nicht. Sie entscheidet, ob daraus ein Vorfall wird oder eine Katastrophe."*

Angebot anfordern →

Schulung ansehen →

Sachverständigenbüro Schulte
Grünberger Weg 9 · 40627 Düsseldorf
+49 211 93375777
sachverstaendiger@itschulte.de
itschulte.de

Weitere Schulungen aus demselben Haus

Schwachstellenmanagement — 240 Min.
ISO/IEC 27001 Anhang A · BSI OPS.1.1.3
Bevor aus der Schwachstelle eine Störung wird: verifizieren, priorisieren, behandeln.

Berechtigungsmanagement — 180 Min.
ISO/IEC 27001 Anhang A · BSI ORP.4
Wer darf was – und wer hat es noch, obwohl er es nicht mehr braucht?

Incident Management — 420 Min.
ISO/IEC 20000-1 · BSI DER.1
Wenn die Eingrenzung zum Vorgang wird: erkennen, priorisieren, steuern, abschließen.

SIEM Use-Cases — rund 4,5 Std.
ISACA-Leitfaden · MITRE ATT&CK® · BSI
Die Erkennungsseite: Warum vier Stunden Störung keinen einzigen Alarm erzeugten.

Die Schulung vermittelt die betriebliche Praxis der Netzwerksicherheit in der Unternehmens-IT. **Normtexte werden nicht wiedergegeben**; maßgeblich sind die gültigen Originaldokumente sowie Schutzbedarf, Zonen und Entscheidungsbefugnisse Ihrer Organisation. Herstellerspezifische Konfigurationen und allgemeingültige Regelwerke werden bewusst nicht angegeben; OT wird nur als Abgrenzung benannt. Die Bescheinigung bestätigt die Teilnahme; sie ist keine Zertifizierung und kein Prüftestat. Rechtsstand November 2026. Keine Rechtsberatung.