INCIDENT RESPONSE & PLAYBOOKS

# Im Ernstfall handlungsfähig.

Vorfallsreaktion nach NIST SP 800-61 und ISO/IEC 27035: erkennen, melden, eindämmen, beheben und daraus lernen – mit Rollen-Tracks (Ersthelfer · Responder · Krisenstab), fünf szenariobasierten Playbooks und den Meldepflichten nach § 32 BSIG, DS-GVO und DORA.

### Vom Alarm zur beherrschten Lage – entlang des sechsphasigen IR-Lebenszyklus

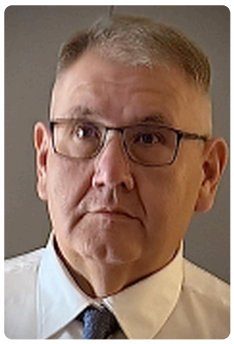
- Vorbereitung
- 5 Playbooks
- Rollen & CIRT
- Meldewege

**Incident**

Response

handeln · melden

- Erkennen
- Eindämmen
- Beseitigen
- Wiederherstellen
- Melden
- Lernen



**Heinrich Markus Schulte**
IT-Auditor · Sachverständiger

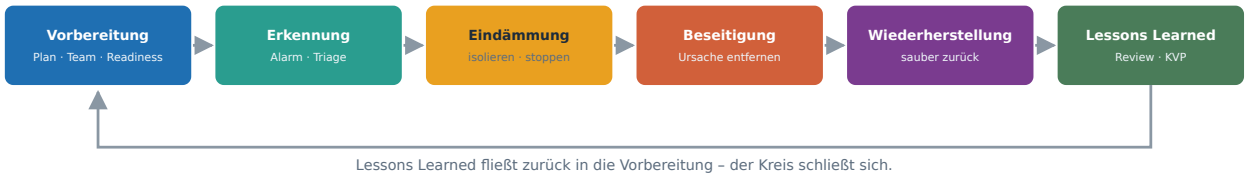
### Vom ersten Alarm bis zur Lessons-Learned-Runde

8 Module · 35 Lektionen · 189 Fragen

**Didaktisch, juristisch exakt, prüffest.**

**Erkennen. Melden. Eindämmen. Beseitigen. Wiederherstellen. Lernen.**

**Der Incident-Response-Lebenszyklus (NIST SP 800-61 · ISO/IEC 27035)**




Lessons Learned fließt zurück in die Vorbereitung – der Kreis schließt sich.

**Prozess nach NIST & ISO**
Der sechsphasige IR-Lebenszyklus nach NIST SP 800-61 und ISO/IEC 27035, eingebettet in BSI-Standard 200-4 und die BSI-Hilfsmittel (Digitaler Ersthelfer, IT-Notfallkarte).

**Meldepflichten rechtssicher**
§ 32 BSIG (24 h / 72 h / 1 Monat), Art. 33/34 DS-GVO (72 h) und DORA – Fristen, Adressaten und Zusammenspiel korrekt und aktuell (Stand Nov. 2026).

**Rollen & 5 Playbooks**
Ersthelfer, Responder und Krisenstab als umschaltbare Tracks; Playbooks für Ransomware, Phishing/BEC, Datenabfluss, DDoS & Konto und Innentäter.

| 8 | 35 | 189 | ~7,5 h | 35 | 420 min |
|---|---|---|---|---|---|
| Module | Lektionen | Quizfragen | Lernzeit | Infografiken | Mindestzeit |

**Testzugang oder Demo anfragen**

**Schulungsseite öffnen**

12 Monate Zugang einschließlich Updates · Sprache: Deutsch · DSGVO-freundlich, ohne Werbe-Tracker

# Vorfallsreaktion ist kein Zufall, sondern ein Prozess.

Warum der Ernstfall keine Improvisation verzeiht – und wie Vorbereitung, Erkennung, Meldung und Bearbeitung ineinandergreifen




Der sechsphasige Incident-Response-Lebenszyklus – von der Vorbereitung bis Lessons Learned, als Kreislauf.

Ein IT-Sicherheitsvorfall verzeiht keine Improvisation. Wer erst im Ernstfall überlegt, wen er anruft, was er abschaltet und welche Frist läuft, verliert die ersten – entscheidenden – Minuten. Diese Schulung macht den Ablauf zur Routine: entlang des sechsphasigen Lebenszyklus von der Vorbereitung über Erkennung und Eindämmung bis zu Beseitigung, Wiederherstellung und Lessons Learned.

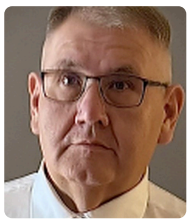
Dabei wird jeder Schritt konkret: Trennen statt ausschalten, Beweise sichern, Umfang und Schwere bestimmen, sauber erst beseitigen und dann wiederherstellen – und parallel die gesetzlichen Meldungen auslösen. Die fünf Playbooks übersetzen den Prozess in Schritt-für-Schritt-Abläufe für die häufigsten Ernstfälle.

Methodischer roter Faden sind NIST SP 800-61 und ISO/IEC 27035, eingebettet in BSI-Standard 200-4. Jede der 35 Lektionen hat eine eigene Infografik – vom Lebenszyklus-Ring über die Meldefristen bis zum Playbook-Ablauf.

### RECHTSRAHMEN & BEZÜGE

**NIST SP 800-61** · **ISO/IEC 27035** · **BSI-Standard 200-4** · **§ 32 BSIG (NIS-2)** · **Art. 33/34 DS-GVO** · **DORA**

Teilnahmeschulung zum Vorgehen, keine Rechtsberatung. „BSI“ ist ein Kennzeichen des BSI. Rechtsstand November 2026.



**PRÜFERBLICK**

**Heinrich Markus Schulte**
IT-Auditor · Sachverständiger
CISA · CISM · CIPP/E · CEH · T.I.S.P.

> *Im Ernstfall entscheidet nicht das dickste Konzept, sondern wer in den ersten Minuten das Richtige tut – und genau das lässt sich vorher üben.*

### GRUNDLAGEN & LEBENSZYKLUS

Ereignis, Vorfall, Krise; der sechsphasige IR-Lebenszyklus; Rollen und CIRT; Rechtsrahmen im Überblick.

### VORBEREITUNG

Leitlinie, IR-Plan und Playbooks; Team mit RACI und Eskalation; Readiness (Logs, Trennbarkeit, Backups); IT-Notfallkarte.

### ERKENNEN & MELDEN

Erkennungsquellen, Triage und Schweregrad, Sofortmaßnahmen und Beweissicherung – und die Fristen nach § 32 BSIG, DS-GVO und DORA.

### BEARBEITEN

Analyse und Scoping, Forensik und Chain of Custody, Eindämmung, Beseitigung, Wiederherstellung, Krisenkommunikation und Führung.

### PLAYBOOKS & ROLLEN

Fünf szenariobasierte Playbooks und drei Rollen-Tracks (Ersthelfer · Responder · Krisenstab), per Schalter umschaltbar.

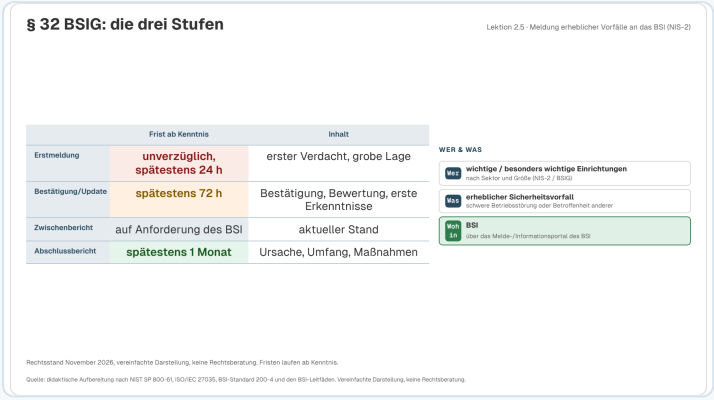
### Fragen, die Aufsicht und Prüfer stellen

- Gibt es einen IR-Plan mit klaren Rollen, Erreichbarkeiten und Eskalationswegen?
- Ist bekannt, welche Fristen (§ 32 BSIG, DS-GVO, DORA) ab wann laufen und wer meldet?
- Sind Backups getrennt und unveränderlich (immutable) und ist der Wiederanlauf geübt?
- Werden Vorfälle ausgewertet (Lessons Learned) und die Playbooks gepflegt?

INCIDENT RESPONSE & PLAYBOOKS

# Ablauf, Nutzen und Inhalte

Acht Module – von den Grundlagen über die fünf Playbooks bis zum Abschluss




§ 32 BSIG: die drei Stufen – Erstmeldung 24 h, Bestätigung 72 h, Abschlussbericht 1 Monat.

## Was Sie lernen

1. **Grundlagen & Bedrohungslage**
   Ereignis/Vorfall/Krise, IR-Lebenszyklus, Rollen & CIRT, Rechtsrahmen
2. **Vorbereitung**
   Leitlinie, IR-Plan, Playbooks, Team/RACI, Readiness, IT-Notfallkarte
3. **Erkennen & Melden**
   Triage & Schweregrad, Beweissicherung, § 32 BSIG, DS-GVO, DORA
4. **Bearbeiten**
   Forensik & Chain of Custody, Eindämmung, Beseitigung, Wiederherstellung
5. **Die fünf Playbooks**
   Ransomware, Phishing/BEC, Datenabfluss, DDoS & Konto, Innentäter
6. **Rollen-Vertiefung, Üben & Abschluss**
   Ersthelfer/Responder/Krisenstab, Lessons Learned, Kennzahlen, Abschluss-Quiz

**FÜR WEN** **IT-Notfallteam / CSIRT · IT-Service & digitale Ersthelfer · IT-Leitung / CISO · Krisenstab & Geschäftsleitung · Datenschutzbeauftragte**

## IHR MEHRWERT

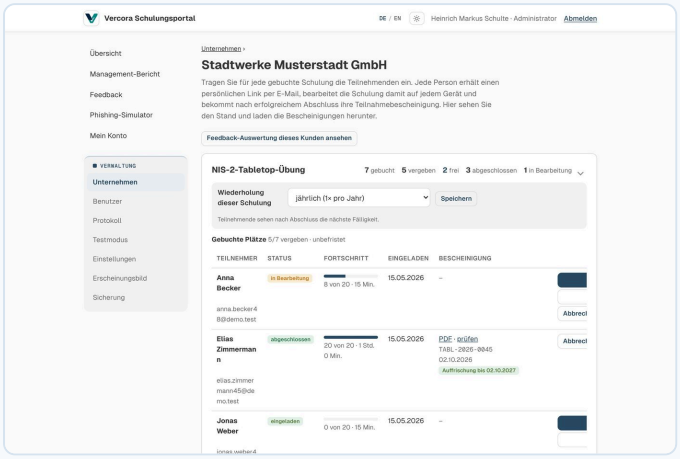
- **Sehr ausführlich**
  ~7,5 Stunden Lernzeit über den kompletten Vorfallsprozess – vom Alarm bis Lessons Learned.
- **35 Infografiken**
  Je Lektion eine – Lebenszyklus-Ring, Meldefristen, RACI/Eskalation und je Playbook ein Ablauf.
- **Rechtssichere Meldepflichten**
  § 32 BSIG (24 h/72 h/1 Monat), Art. 33/34 DS-GVO und DORA – Fristen und Adressaten korrekt.
- **5 szenariobasierte Playbooks**
  Ransomware, Phishing/BEC, Datenabfluss, DDoS & Konto und Innentäter – Schritt für Schritt.
- **Rollen-Tracks**
  Ersthelfer, Responder und Krisenstab – per Schalter umschaltbar, Modul 5 vertieft jede Rolle.
- **Prüffest**
  75 % Bestehensgrenze, Teilnahmebescheinigung IR-..., online verifizierbar.
- **10 Begleitunterlagen**
  Ausfüllbare Vorlagen (RACI, Meldeformular, Vorfalls-Log, Playbook …), Kurzreferenz/IT-Notfallkarte und Glossar.
- **Üben statt nur lesen**
  Tabletop-Durchlauf und Post-Incident-Review machen den Ablauf zur Routine.

**PAKET & BUCHUNG** Einzelplatz mit 12 Monaten Zugang oder im Unternehmens-Portal mit Einladungslinks · ergänzt die NIS-2-, CRA- und BCM-Schulungen · Bescheinigung IR-...

# So läuft es ab

Von der Buchung zum einsatzbereiten Vorfallsmanagement

## Im Vercora Schulungsportal inklusive




- **Teilnehmerverwaltung:** Plätze buchen, Personen anlegen, persönliche Einladungslinks ohne Passwort
- **Fortschritt & Management-Bericht:** Teilnahme, Abschlüsse und fällige Auffrischungen als PDF für die Leitung
- **Nummerierte Bescheinigung:** PDF mit Online-Echtheitsprüfung, Protokoll und eigenem Nummernkreis (IR-…)
- **Wiederholungsintervall:** je Schulung 6, 12, 24 oder 36 Monate – das Portal zeigt, wann nachgeschult wird
- **Ihr Erscheinungsbild:** auf Wunsch mit Ihrem Logo und Ihrer Farbe – auch auf Bescheinigung und Bericht
- **Sicher & datensparsam:** Anmeldung mit zweitem Faktor, Hash-Ketten-Protokoll, keine Werbe-Tracker

## Der Schulungsprozess im Überblick

**1 Buchen**
**Einzelplatz oder Portal-Zugang**

**2 Lernen**
**35 Lektionen mit Abschluss-Quiz**

**3 Anwenden**
**Playbooks & IT-Notfallkarte im eigenen Haus**

**4 Nachweisen**
**Bescheinigung IR-… erhalten**

**5 Üben**
**Tabletop & Lessons Learned**

## Was Sie erhalten

### Der komplette Vorfallsprozess
Alle sechs Phasen des IR-Lebenszyklus, didaktisch aufbereitet – vom Alarm bis Lessons Learned

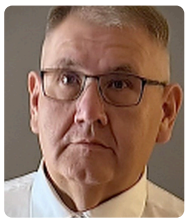
### Fünf szenariobasierte Playbooks
Ransomware, Phishing/BEC, Datenabfluss (DS-GVO), DDoS & Konto und Innentäter – Schritt für Schritt

### Rollen-Tracks
Ersthelfer, Responder und Krisenstab – per Schalter umschaltbar, mit eigener Vertiefung

### Zehn Begleitunterlagen zum Ausfüllen
RACI, Kontaktliste, Meldeformular, Meldepflichten-Checkliste, Vorfalls-Log, Playbook-Vorlage, Review, Tabletop, Kurzreferenz/IT-Notfallkarte, Glossar

### 35 Infografiken & prüfbarer Abschluss
Je Lektion eine Grafik; 75 % Bestehensgrenze, Teilnahmebescheinigung IR-…, online verifizierbar

## PRÜFERBLICK



**Heinrich Markus Schulte**
IT-Auditor · Sachverständiger
CISA · CISM · CIPP/E · CEH · T.I.S.P.

> *Wer den Ablauf einmal geprobt hat, greift im Ernstfall zum Playbook statt zur Improvisation – das verkürzt jede Reaktionszeit.*

**Demo oder Testzugang anfragen**

**itschulte.de/schulungen.html**

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