VORLAGE ZU ABSCHNITT 3.5 DES BANDES 5B

Der digitale Beinaheunfall und seine Bewertung

Fünf Fragen an jede Meldung, und die Frage, ab wann die Uhr läuft: nicht «wann ist es passiert», sondern «wann haben wir es gewusst».

Kategorie: Prüfliste (mit Anwendung in Schritten und häufigen Fehlern). Bezug im Buch: Abschnitt 3.5 (Das Prinzip, Der Rahmen in Deutschland, Österreich und der Schweiz); Norm: Klauseln 7.3, 9.1, 10.1 und 10.2 sowie Maßnahmen A.5.25, A.5.26, A.5.27, A.6.8 und A.8.16 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Buches. Rechtsstand des Bandes: 28. September 2026.

Haus / Standort		**Bewertende Rolle**	
Datum		**Land (DE / AT / CH)**	

So nutzen Sie diese Vorlage

1. Prüfen Sie zuerst das Thermometer: Ein leeres Ereignisregister ist ein Befund, kein Ergebnis. Fragen Sie nie zuerst, wie viele Vorfälle es gab, sondern woher das Haus es wüsste (3.5).
2. Prüfen Sie in drei Schritten: die technischen Quellen abfragen, die menschlichen Quellen befragen, beide gegen das Register halten und die Differenz benennen (Teil 1).
3. Bewerten Sie jede Meldung mit den fünf Fragen (Teil 2) und halten Sie Datum und Uhrzeit der Kenntnis fest (Teil 3). Die Bewertung ist Sache der benannten Rolle, nicht des Melders.

Spalte «Im Buch»: verlangt = von der Norm oder vom Recht verlangt, wie das Buch es in eigenen Worten wiedergibt (Klausel oder Quelle in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Prüfung in drei Schritten: Quellen gegen das Register

Quelle	Auswertung, die jedes System ohne Aufwand liefert	Zahl	Im Register?
Technisch: Gateway	Zurückgewiesene Nachrichten als Betrugsversuch oder Schadsoftware; darunter an namentlich genannte Personen gerichtete		
Technisch: Verzeichnisdienst	Fehlgeschlagene Anmeldungen je Konto, aus wechselnden Netzen		
Technisch: Postfachregeln aller Konten	Weiterleitungsregeln an externe Adressen, Anlagedatum		
Technisch: Firewall, Verwaltungssystem	Was das Haus dort ohnehin zählt		
Menschlich: Rezeption, Reservierung, Buchhaltung, Etage	Anrufe, die nach Zugängen fragen; Mails, die zur Änderung von Bankdaten auffordern; was keine E-Mail ist		

Grund: Technik zählt, Menschen erkennen (A.8.16 und A.6.8 gehören zusammen). Vorhandene Protokolle sind keine Überwachung: Die Maßnahme setzt eine Person, eine Frequenz und ein Kriterium voraus (9.1 und A.8.16: verlangt; die Prüfung in drei Schritten: Methode dieses Bandes).

2 Fünf Fragen an jede Meldung

Frage	Antwort	Grund (aus dem Band)	Im Buch
1. Was wurde beobachtet, wann, von wem, und wann wurde es gemeldet (Datum und Uhrzeit)?		Wer eine Meldung entgegennimmt, hält Datum und Uhrzeit fest; ohne Zeitstempel lässt sich der Beginn der eigenen Frist nicht belegen.	Methode dieses Bandes
2. Deutet es auf einen möglichen Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit hin?		Ein Ereignis ist eine Beobachtung, die auf einen solchen Verlust hindeutet und beurteilt werden muss, bevor man weiß, was sie ist.	Methode dieses Bandes
3. Steht es auf der Seite «Was bei uns kein Ereignis ist» (vergessene Passwörter, klemmende Türen)?		Ohne diese zweite Seite füllt sich das Register mit Rauschen, und die bewertende Rolle verliert in drei Monaten die Lust.	Methode dieses Bandes
4. Bedeutet es nach Beurteilung Schaden oder kann es Schaden bedeuten: ist es ein Vorfall?		Ein Vorfall ist ein Ereignis, das nach Beurteilung Schaden bedeutet oder bedeuten kann. Es braucht ein vereinbartes Schema und eine benannte Rolle; in einem Haus mit zweihundertvierzig Zimmern eine Person mit Stellvertretung und eine Seite Papier.	verlangt (A.5.25); Form: Methode
5. Sind personenbezogene Daten betroffen, und seit wann hat das Haus Kenntnis davon?		Ein abgewehrter Angriff, ein blockierter Zugriff und ein Beinaheunfall sind für sich keine Verletzung des Schutzes personenbezogener Daten; ins Ereignisregister gehören sie trotzdem.	verlangt (Recht des Landes); Frage: Methode

Melden ist niedrigschwellig; bewerten ist Sache der benannten Rolle. Der Filter liegt nicht beim Melder. In Häusern mit funktionierender Meldekultur liegt das Verhältnis von Meldungen zu Vorfällen etwa zwischen zehn zu eins und zwanzig zu eins: Neun von zehn Meldungen werden nach kurzer Bewertung geschlossen.

3 Wann die Uhr läuft

Frage	Antwort	Grund (aus dem Band)	Im Buch
Wann haben wir es gewusst (Datum, Uhrzeit)?		Rechtlich beginnt die Uhr nicht beim Ereignis, sondern bei der Kenntnis von einer Verletzung des Schutzes personenbezogener Daten. Im Zweifel rechnet die Behörde ab dem frühestmöglichen Zeitpunkt.	verlangt (DSGVO Art. 33; revDSG Art. 24)

Frage	Antwort	Grund (aus dem Band)	Im Buch
Welche Frist gilt an diesem Standort?		DE und AT: unverzüglich und möglichst binnen zweiundsiebzig Stunden nach Kenntnis an die Aufsichtsbehörde, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko; Benachrichtigung der Betroffenen nur bei voraussichtlich hohem Risiko (Art. 34), diese Schwelle liegt höher. CH: so rasch als möglich an den Beauftragten, wenn voraussichtlich ein hohes Risiko; die betroffene Person wird informiert, wenn es zu ihrem Schutz erforderlich ist oder der Beauftragte es verlangt. Rechtsstand: 28. September 2026.	verlangt (DSGVO Art. 33, 34; revDSG Art. 24)
Wer meldet an die Behörde: das Haus als eigene Gesellschaft oder die Gruppe?		Maßgeblich ist, wer über Zwecke und Mittel entscheidet; das ist in Hotelgruppen selten einheitlich. Ein Satz im Handbuch je Gesellschaft erspart im Ernstfall eine Telefonkonferenz.	Methode dieses Bandes
Wie lange bewahren die Systeme ihre Protokolle auf, und ist das festgelegt?		Protokolle rollieren, oft nach dreißig oder neunzig Tagen; ihre Dauer ist die Grenze der Aufklärbarkeit.	Methode dieses Bandes
Gibt es dienstleistende Unternehmen, die selbst meldepflichtig sind, und weiß das Haus, welche Informationen sie im Ereignisfall verlangen?		Klassische Hotels fallen in der Regel nicht unter die europäische Richtlinie der zweiten Generation, wohl aber Anbieter, von denen sie abhängen (Rechenzentren, Cloud-Dienste, verwaltete IT-Dienstleister). Nationale Umsetzung und Schweizer Meldepflicht für kritische Infrastrukturen sind an der geltenden Fassung zu prüfen.	verlangt (Recht des Landes)

4 Die Definition des Hauses: was ist, und was ist kein Ereignis

Bei uns ein meldepflichtiges Ereignis	Bei uns kein Ereignis
Ein Anruf, der nach Zugängen fragt	Vergessene Passwörter
Eine Mail, die zur Änderung von Bankdaten auffordert	Klemmende Türen
Ein verlorenes Gerät	
Eine offene Tür, die geschlossen sein sollte	
Ein Gast, der die Daten eines anderen sieht	

Die Beispiele stammen aus dem Abschnitt; die Definition ist kurz und nennt Beispiele aus dem Hausalltag, und das Haus schreibt sie in seiner Sprache. Dass es eine solche Definition gibt, ist Methode dieses Bandes; die Bewertung nach einem vereinbarten Schema durch eine benannte Rolle ist verlangt (A.5.25).

5 Kennzahlen und Reihenfolge im Ereignisfall

Kennzahl oder Regel	Wert / Antwort	Grund (aus dem Band)	Im Buch
Meldungen je hundert Beschäftigte, monatlich		Nicht die Zahl der Vorfälle: Steigt die erste Zahl, ist das ein gutes Zeichen. Die Zahl der Vorfälle allein wird nicht mehr berichtet.	Methode dieses Bandes
Mittlere Zeit von der Beobachtung bis zur Meldung, gemessen an den Einträgen des Registers		Sinkt sie, ist das ein besseres Zeichen. «Zahl der Vorfälle» und «Anteil geschulter Beschäftigter» lassen sich durch Nichtstun verbessern.	Methode dieses Bandes
Rückrufregel: Zahlungsdaten werden nie auf Zuruf aus einer E-Mail geändert, sondern nur nach Rückruf an eine hinterlegte Nummer. Schriftlich, ja oder nein?		Kein Gesetz schreibt sie vor, jeder Versicherer erwartet sie; sie verhinderte in Nürnberg die dritte Zahlung. Die Obliegenheiten der Cyberpolice gehören in die Liste der eigenen Anforderungen.	Methode dieses Bandes
Reihenfolge im Ereignisfall: eingrenzen (Konto sperren, Sitzungen beenden, Passwörter zurücksetzen), sichern (Protokolle exportieren, bevor sie rollieren), bewerten und melden, kommunizieren		Häuser, die zuerst kommunizieren, verlieren Beweise; Häuser, die zuerst bewerten, verlieren Zeit.	Methode dieses Bandes
Ist die Rezeption als Meldeweg so gebaut, dass die Nachtschicht ihn nutzen kann?		Die Rezeption ist die wichtigste Sensorik des Hauses und die einzige Abteilung, die rund um die Uhr besetzt ist.	Methode dieses Bandes

6 Anwendung in Schritten

Schritt	Was zu tun ist (Operative Synthese des Abschnitts)	Erledigt
1 Sofort	Die drei technischen Auswertungen anfordern, die Postfachregeln aller Konten auflisten und beides gegen das Ereignisregister halten.	☐
2 Planen	Eine Seite «Was bei uns ein Ereignis ist» mit Hotelbeispielen, eine benannte Rolle für die Bewertung, eine Meldeadresse, die auch Anrufe erfasst, und die Rückrufregel für Änderungen von Zahlungsdaten.	☐
3 Überwachen	Meldungen je hundert Beschäftigte und mittlere Zeit bis zur Meldung monatlich führen und in die Managementbewertung nehmen.	☐
4 Regel für das Programm	Ein leeres Register führt in jedem Audit zu einer Prüfung der technischen Quellen, bevor irgendetwas anderes geprüft wird.	☐

7 Häufige Fehler

Fehler (wie der Band ihn nennt)	Was der Band dagegen zeigt
Ereignis und Vorfall werden gleichgesetzt.	Ein Haus, das nur Vorfälle kennt, hat keine Vorstufe und keine Chance, vor dem Schaden zu handeln.
Die Grenze des Dienstleisters: Er meldet Störungen, abgewehrte Angriffe sind keine Störungen.	Niemand hatte je gefragt, was er sieht und nicht meldet.
Gewöhnung: «Merkwürdige Mails bekommt man eben».	Ein System, das auf die Empörung Einzelner baut, verliert sie nach spätestens einem Jahr.
Kein Meldeweg für das, was keine E-Mail ist: zwei Anrufe an der Rezeption.	Es gab keine Stelle und keine Frage im Dienstübergabebuch, die danach gefragt hätte. Gastfreundschaft ist trainierte Hilfsbereitschaft.
Weiterleitungsregeln unbekannt.	Sie sind in jedem System mit zwei Klicks auflistbar.

Fehler (wie der Band ihn nennt)	Was der Band dagegen zeigt
Die Kennzahl «Zahl der Vorfälle» steht auf null.	Eine Kennzahl, deren guter Wert durch Nichtstun entsteht, ist eine Einladung; nicht der Direktor ist schuld, sondern die Konstruktion der Kennzahl.
«Wir hatten nie einen Vorfall.»	Wahr, beruhigend und ohne Aussage über die Wirksamkeit der Vorkehrungen.
Die Feststellung ist nur systemisch formuliert.	Beides gehört in den Bericht, in dieser Reihenfolge: das konkrete Risiko («dieses Konto wird angegriffen, und es hat keine zweite Sicherung»), dann das System.
Das Haus hat nie geübt.	Eine Übung von neunzig Minuten im Jahr hätte die Lücken gezeigt, die der Ernstfall in vierzehn Stunden aufdeckte.
Die Bewertung dem Melder überlassen («nur melden, wenn sicherheitsrelevant») oder dem IT-Dienstleister übertragen.	Das Register enthielt danach fast nur IT-Meldungen; der IT-Dienstleister sieht die Technik, nicht das Haus.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch das Recht, das für Ihr Haus gilt; ob eine Meldung an eine Behörde zu erstatten ist, beurteilt sie nicht. Sie bewertet keine Angriffe, sondern die Fähigkeit des Hauses, sie zu bemerken. Ein ausgefülltes Blatt ist kein Nachweis: Es zeigt, dass jemand bewertet hat, nicht dass das Haus sieht. Ein volles Register beweist noch keine Sicherheit. Rechtsstand des Bandes: 28. September 2026.