



Kriterienkatalog und Vorgehensweise zur Konformitätsbewertung und Vergabe des „Pentested“-Gütesiegels

datenschutz cert GmbH
Version 1.2

Inhaltsverzeichnis

1. Konformitätsbewertung für Penetrationstests	4
2. Gegenstand der Konformitätsbewertung	5
3. Kriterienkatalog.....	6
4. Begutachtungsprozess.....	8
4.1. Laufzeiten	8
4.2. Beteiligte.....	8
4.3. Ablauf der Konformitätsbewertung	9
4.4. Konformitätsliste.....	9
4.5. Kosten und Gebühren	9
4.6. Gütesiegel.....	9
4.7. AGB und Konformitätsbewertungsordnung	10
5. Struktur des Gutachtens	11
6. datenschutz cert GmbH	12
6.1. Leitlinien.....	12
6.2. Unabhängigkeit und Unparteilichkeit	12
6.3. Vertraulichkeit	12
6.4. Datenschutz.....	13
6.5. Akkreditierungen	13

Historie

Version	Datum	Grund der Änderung	Geändert durch
0.1	22.01.2024	Erstellung erster Entwurf	Michael Cyl
0.9	31.01.2024	Redaktionelle Änderungen und Qualitätssicherung	Dr. Sönke Maseberg
1.0	26.04.2024	Finalisierung	Michael Cyl
1.1	29.10.2024	Anpassungen	Dr. Sönke Maseberg
1.2	01.11.2024	Anpassungen	Dr. Sönke Maseberg

Dokumenten-Überwachungsverfahren

Status	Prozess-/Dokumentenbesitzer	Version
Final	Michael Cyl	1.2

1. Konformitätsbewertung für Penetrationstests

Penetrationstests sind ein effektives Mittel, um die tatsächliche Sicherheit eines Systems, Netzwerks oder einer Anwendung im Hinblick auf mögliche Angriffsvektoren zu überprüfen. Dabei bedient sich ein Penetrationstester unterschiedlicher Methodiken, die denen realer Angreifer ähneln und auf den spezifischen Prüfgegenstand zugeschnitten sind. Das Ziel besteht darin, potenzielle Sicherheitslücken zu identifizieren, Verbesserungsmöglichkeiten aufzuzeigen und das Gesamtergebnis umfassend zu dokumentieren, um bei der weiteren Sicherheitsentwicklung zu unterstützen.


Aufgrund der Vielfalt an möglichen Prüfverfahren, Prüftiefen und Prüfintervallen bei Penetrationstests stellt die Bewertung der durchgeführten Tests und die Ableitung eines entsprechenden Sicherheitsniveaus sowohl für die Auftraggeber als auch für deren Kunden bzw. Nutzer oft eine Herausforderung dar.

Die datenschutz cert GmbH führt daher nicht nur Penetrationstests selbst durch, sondern validiert Penetrationstests und erteilt entsprechende Siegel für IT-Systeme, Netzwerke und Webanwendungen bzw. webbasierte Programme, die regelmäßig nach festgelegten Prüfkriterien untersucht werden.

Das Gütesiegel "Pentested" ist für Unternehmen konzipiert, die ihre IT-Sicherheit kontinuierlich durch fortlaufende Penetrationstests überprüfen sowie verbessern wollen und dies durch eine unabhängige Instanz validieren und nachweisen möchten.

Im Nachfolgenden wird vorgestellt, wie die datenschutz cert GmbH das Pentested“-Siegel vergibt und welche Kriterien dafür zugrunde liegen.

Bremen, den 29.10.2024



Dr. Sönke Maseberg/ datenschutz cert GmbH

2. Gegenstand der Konformitätsbewertung

Die datenschutz cert GmbH sowie qualifizierte externe Experten führen Penetrationstests auf IT-Systemen und Webanwendungen durch, um die Sicherheit dieser Systeme eingehend zu analysieren. Diese Tests werden sorgfältig dokumentiert, wobei der Untersuchungsgegenstand individuell nach den Anforderungen des Auftraggebers ausgerichtet wird. Der Auftraggeber entscheidet dabei selbst oder folgt der Empfehlung der Experten, wie der Prüfbereich definiert wird und auf welcher Basis der Penetrationstest durchgeführt werden soll (Black-Box, Grey-Box oder White-Box).

Das primäre Ziel der Konformitätsbewertung durch die datenschutz cert GmbH ist es, zu überprüfen, ob der durchgeführte Penetrationstest den Mindestanforderungen und den aktuellen Standards im Hinblick auf Prüftiefe, Prüfkriterien und Dokumentation entspricht. Die Tests müssen mindestens eine Kombination aus automatisierten und manuellen Testphasen aufweisen. Des Weiteren sollten die obligatorischen Module der Praxisleitfäden „IS-Penetrationstest“ und „IS-Webcheck“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) berücksichtigt werden. Webanwendungen sollten zudem gemäß den OWASP-Top-10 bzw. OWASP-API-Top-10 geprüft werden, um die Abdeckung der entscheidenden Prüfkriterien sicherzustellen. Eine detaillierte und verständliche Dokumentation der Testergebnisse, einschließlich einer Bewertung der identifizierten Schwachstellen nach einheitlichen und nachvollziehbaren Standards wie dem Common Vulnerability Scoring System (CVSS) oder dem OWASP Risk Scoring, ist ebenso ein wesentlicher Bestandteil der Bewertung. Zudem wird Wert auf regelmäßige Testintervalle gelegt, um die anhaltende Sicherheit zu gewährleisten.

Es gilt zu beachten, dass durch die Konformitätsbewertung nicht die Sicherheit des getesteten Systems bzw. der getesteten Anwendung selbst validiert oder zertifiziert wird. Vielmehr wird bestätigt, dass der Penetrationstest gemäß den geforderten Standards durchgeführt wurde. Die Ergebnisse dieser Bewertung werden anschließend in einem Kurzgutachten festgehalten, das die Einhaltung der Kriterien dokumentiert und den Auftraggebern auf Wunsch eingesehen werden kann.

3. Kriterienkatalog

Für die Begutachtung ist die Vorlage des Testreports sowie ein Nachweis über die angestrebten Testzyklen (z. B. vertragliche Vereinbarungen) zwingend erforderlich. Die Art und der Umfang der Dokumentation müssen ausreichend sein, um eine fundierte Beurteilung der Prüfkriterien zu ermöglichen. Kundenbezogene Systemdaten innerhalb der Dokumente dürfen pseudonymisiert eingereicht werden.

Die vorgelegten Dokumente müssen folgende Punkte erfüllen:

I) Server-Systeme und Netzwerke (extern oder intern)

A1. Alle Zielsysteme wurden durch einen Port- und Schwachstellenscan gegenüber einer aktuellen CVE-Datenbank überprüft.

A2. Die folgenden Prüfpunkte müssen im Rahmen manueller Tests beachtet worden sein (sofern anwendbar):

- die Analyse der identifizierten Dienste und Betriebssysteme in Hinblick auf veraltete Software mit bekannten Sicherheitslücken,
- die Kontrolle der Erreichbarkeit von administrativen Zugängen bzw. Fernwartungszugängen ausgehend von unautorisierten Systemen,
- Brute-Force-Angriffe auf Authentisierungsdienste zur Überprüfung auf Standardzugangsdaten oder triviale Kennwörter,
- die gezielte Suche nach der Ausgabe von sensiblen Informationen,
- die Überprüfung der Verschlüsselung und die Angemessenheit der eingesetzten Verschlüsselungsverfahren,
- die Kontrolle, ob die identifizierten Dienste und Anwendungen eine adäquate Zugriffbeschränkung aufweisen sowie
- die generelle Analyse der Systeme im Hinblick auf potenzielle Verbesserungspotentiale und Härtungseinstellungen.

A3. Die Ergebnisse des Penetrationstests müssen in einer klaren und detaillierten Form dokumentiert werden. Schwachstellen sind entsprechend ihrer potenziellen Auswirkungen in einer Risikomatrix mit mindestens vier Abstufungen zu klassifizieren. Es sollen, soweit möglich, Empfehlungen zur Behebung der identifizierten Schwachstellen bereitgestellt werden.

A4. Außerdem muss gewährleistet werden, dass der nächste Penetrationstest für den zuvor geprüften Untersuchungsgegenstand spätestens nach 12 Monaten stattfindet.

II) Webapplikationen oder web-basierte Software

A1. Die zugrundeliegende Infrastruktur der Anwendung, wie beispielsweise Web- oder API-Server, muss mittels Port- und Schwachstellenscans gegenüber einer aktuellen CVE-Datenbank überprüft worden sein.

A2. Es ist erforderlich, dass im Rahmen manueller Tests folgende Prüfpunkte beachtet wurden (sofern anwendbar):

- die Überprüfung der Art und Qualität der Registrierung und Authentisierung für Benutzer sowie der Authentisierung auf Objektebene,
- die Ausweitung der Zugriffsrechte (vertikal und horizontal) zwischen ggf. unterschiedlichen Benutzern, Gruppen und Rollen,
- die Analyse und Manipulation des Session-Managements, inkl. Prüfung von seitenübergreifenden Aufruf-Manipulationen (Cross-Site-Request-Forgery-Angriffe),
- die Analyse und Manipulation von API- respektive Authentifizierungs-Tokens (sofern vorhanden),
- die Überprüfung der Datenvalidierung, insb. im Hinblick auf Cross-Site-Scripting (XSS)-Angriffe und die Anfälligkeit für Injections (u.a. SQL-, OS-, Header- und XML-Injections),
- die Auswertung von Fehlermeldungen im Hinblick auf die Rückgabe von sensiblen Informationen,
- die Überprüfung der Verschlüsselung und die Angemessenheit der eingesetzten Verschlüsselungsverfahren sowie
- die generelle Analyse der Sicherheitseinstellungen bzgl. Fehlkonfigurationen und Verbesserungspotenzialen.

Die geprüften Aspekte sollten dabei entsprechend die Standards der „OWASP-Top-10“ bzw. „OWASP-API-Top-10“ berücksichtigen.

A3. Die Ergebnisse des Tests müssen in einer klaren und detaillierten Form dokumentiert sein. Schwachstellen müssen entsprechend ihrer potenziellen Auswirkungen in einer Risikomatrix mit mindestens vier Abstufungen klassifiziert werden. Es sollen, soweit möglich, Empfehlungen zur Behebung der identifizierten Schwachstellen aufgeführt werden.

A4. Außerdem muss gewährleistet werden, dass der nächste Penetrationstest für den zuvor geprüften Untersuchungsgegenstand spätestens nach 12 Monaten stattfindet.

4. Begutachtungsprozess

In diesem Abschnitt wird vorgestellt, wie die datenschutz cert GmbH die Konformitätsbewertung der Penetrationstests durchführt.

4.1. Laufzeiten

Aufgrund der kontinuierlichen Veränderung der Bedrohungslandschaft sowie der fortwährenden Dynamik innerhalb von IT-Systemen und Anwendungen sollte ein Penetrationstest nach spätestens 12 Monaten wiederholt werden. Dies dient dazu, die Sicherheit kontinuierlich zu verbessern, die Maßnahmen den neuen Bedrohungen anzupassen und ein hohes Maß an Compliance und Vertrauen aufrechtzuerhalten. Somit ist auch die Konformitätsbewertung auf einen Zeitraum von maximal 12 Monaten beschränkt.

4.2. Beteiligte

4.2.1. Kunde

Der Kunde ist der Auftraggeber des Penetrationstests und der Eigentümer des Untersuchungsgegenstandes. Er stellt den Antrag auf die Konformitätsbewertung des durchgeführten Penetrationstests. Der Kunde stellt dafür die benötigten Unterlagen zur Verfügung, oder er kann sein Einverständnis zur Übergabe durch den Auftragnehmer, d. h. das mit dem Penetrationstest beauftragte Unternehmen (vgl. Abschnitt 4.2.2), erklären. Kunde oder Auftragnehmer geben, soweit von den Evaluatoren oder der Zertifizierungsstelle gefordert, weitere Informationen über den durchgeführten Penetrationstest.

4.2.2. Tester

Der Tester ist der ausführende Penetrationstester bzw. das mit dem Penetrationstest beauftragte Unternehmen. Der Tester kann mit Einverständnis des Kunden (vgl. Abschnitt 4.2.2) ebenfalls den Antrag auf die Konformitätsbewertung stellen und stellt dann die dafür benötigten Dokumente und Informationen direkt den Evaluatoren und der Zertifizierungsstelle zur Verfügung.

4.2.3. Evaluatoren

Evaluatoren prüfen die Dokumentation des Penetrationstestes sowie sonstige Nachweise auf Konformität zu den o.g. Anforderungen und erstellen ein Kurzgutachten.

Evaluatoren sind bei der datenschutz cert GmbH berufen; die Berufung umfasst u.a.:

- Erfahrung im Bereich Informationstechnik und -sicherheit;
- Kenntnisse über Penetrationstests und ihre Durchführung;
- Übung im Umgang mit Kriterienwerken.

4.2.4. Zertifizierungsstelle

Die Zertifizierungsstelle prüft das Kurzgutachten auf Vollständigkeit und Nachvollziehbarkeit der gemachten Angaben. Sie prüft dabei sowohl die formalen Anforderungen an das Kurzgutachten als auch die inhaltlichen Angaben zum Penetrationstest.

4.3. Ablauf der Konformitätsbewertung

Der Antrag auf die Konformitätsbewertung kann direkt mit der Beauftragung des Penetrationstests sowie bis zu zwei Wochen nach Abschluss des Tests gestellt werden.

Die Konformitätsbewertung des Penetrationstests erfolgt allerdings frühestens nach Abschluss und Dokumentation des Tests. Der Penetrationstester führt daher unter Beachtung der geforderten Dokumentationspflichten den Penetrationstest in gewohnter Weise durch.

Die Zertifizierungsstelle benennt einen Evaluator, welcher vom Kunden oder vom Tester die benötigten Unterlagen (Testreport und Nachweise über Prüfintervalle) erhält. Auf der Basis dieser Unterlagen und evtl. Rückfragen wird das Kurzgutachten erstellt. Nach einer Prüfung des Kurzgutachtens durch die datenschutz cert GmbH wird das Gütesiegel „Pentested“ erteilt.

4.4. Konformitätsliste

Eine Liste der von der datenschutz cert GmbH erteilten Siegel kann abgerufen werden unter: <https://www.datenschutz-cert.de/zertifikatslisten/>

Aus der Liste sind der Antragsteller, der Geltungsbereich, die Siegel-ID sowie die Gültigkeit der Konformitätsbewertung ersichtlich.

4.5. Kosten und Gebühren

Es fallen Kosten für die Konformitätsbewertung an; dies beinhaltet konkret:

- Prüfung und Bewertung durch einen Evaluator;
- Erstellung eines Kurzgutachtens;
- Konformitätsbewertung mit Ausstellung des Gütesiegels;
- Listung des Siegels (12 Monate).

4.6. Gütesiegel

Im Anschluss an die Konformitätsbewertung wird ein Siegel an den Kunden ausgeben, welches die folgenden Inhalte enthält:

- Bezeichnung des Siegels: „Pentested“;
- Logo/Name der Zertifizierungsstelle;
- ID des Siegel, evtl. mit Jahreskennung;
- Gültigkeitszeitraum des Siegels

4.7. AGB und Konformitätsbewertungsordnung

Es gelten unsere Allgemeinen Geschäftsbedingungen (AGB) sowie unsere Konformitätsbewertungsordnung (KBO), die Sie unter <https://www.datenschutz-cert.de> abrufen können.

5. Struktur des Gutachtens

Kunde: xxx

Penetrationstester: xxx

Evaluator: xxx

Zeitraum des Penetrationstests: xxx

Gültigkeit:

- Dieses Gutachten gilt für den Penetrationstest des o.g. Testzeitraumes.
- Beschreibung des Testgegenstandes:
- Bei dem Testgegenstand handelt es sich um die Systeme xxx / das Netzwerk xxx
- Die Systeme/die Anwendung sind/ist gekennzeichnet durch die Nutzung als xxx

Feststellungen:

Die Anforderungen an den Penetrationstest werden umgesetzt:

- A1. Alle Zielsysteme wurden durch einen Port- und Schwachstellenscan gegenüber einer aktuellen CVE-Datenbank überprüft.

Umgesetzt durch: xxx

- A2....

Ergebnis der Evaluierung:

Die Anforderungen zur Konformitätsbewertung eines Penetrationstests gemäß den Kriterien des Gütesiegels „Pentested“ sind umgesetzt.

6. datenschutz cert GmbH

Die datenschutz cert GmbH bietet Konformitätsbewertungen auf dem Gebiet des Datenschutzes und der Informationssicherheit an. Diese Konformitätsbewertungen schließen sowohl Prüfaktivitäten als auch Zertifizierungstätigkeiten ein – einerseits für IT-Systeme und -Produkte und andererseits für Verfahren und Managementprozesse.

Die datenschutz cert GmbH ist ein Unternehmen der DSN Group. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg. Die Unternehmen der DSN Group sind inhabergeführt.

6.1. Leitlinien

Die datenschutz cert GmbH bietet Konformitätsbewertungen unter folgenden grundsätzlichen Leitlinien an:

6.2. Unabhängigkeit und Unparteilichkeit

Wir sind unabhängig und unparteilich. Es gilt das übergeordnete Interesse und die vorrangige Pflicht, Auditierungen, Evaluierungen, Zertifizierungen und Bestätigungen entsprechend den Vorgaben frei von internen und externen kommerziellen, finanziellen und sonstigen Zwängen durchzuführen. Maßstab ist das jeweilige Kriterienwerk. Zudem führen wir keinerlei Beratung durch.

Wir haben einen "Ausschuss zur Sicherstellung der Unparteilichkeit der datenschutz cert GmbH" (Ausschuss) etabliert, mit dem die grundsätzlichen Regelungen zur Unabhängigkeit und Unparteilichkeit der Zertifizierungstätigkeiten diskutiert und durchgeführte Zertifizierungsprozesse auf ihre Unabhängigkeit hin überprüft werden.

Zur Gewährleistung der Unabhängigkeit und Unparteilichkeit unserer erteilten Zertifikate setzen wir für den Auditierungs- und Zertifizierungsprozess darüber hinaus regelmäßig externe Fachbegutachter ein.

6.3. Vertraulichkeit

Wir sichern Ihnen Vertraulichkeit zu.

6.3.1. Offenheit und Transparenz

Wir sind offen und transparent hinsichtlich unserer Tätigkeiten, d.h.

- wir kommunizieren klar und unmissverständlich, was und nach welchen Regeln geprüft und zertifiziert wird;
- unsere Zertifikate und Auditreports sind klar und verständlich formuliert;
- wir veröffentlichen die zugrundeliegenden Regelwerke - sofern nicht durch Copyright geschützt -;
- wir benennen klar, wofür wir akkreditiert sind;
- wir lassen uns selber regelmäßig auditieren;

- wir sind offen für alle Anfragen und Beschwerden: Wenn Sie Fragen zu einem von uns erteilten Zertifikat haben oder potentiell den Missbrauch eines Zertifikats vermuten: Bitte sprechen Sie uns an. Wir sichern Ihnen Vertraulichkeit zu und gehen der Sache nach. Wir informieren Sie über den Stand der Untersuchung sowie den Abschluss.

6.4. Datenschutz

Wir kommen aus dem Datenschutz. Jede Art von Konformitätsprüfung wird - im Rahmen des jeweiligen Untersuchungsgegenstands - unter den besonderen Aspekten des Datenschutzes beleuchtet. Dadurch stellen wir sicher, dass die von uns geprüften und bewerteten IT-Produkte und -Systeme den Anforderungen des Datenschutzes genügen.

Unser Anspruch ist, dass sich "datenschutz zertifizierte" Produkte und Prozesse etablieren und für unsere Kunden einen Mehrwert zu einem besseren Datenschutz darstellen und dass unser Zertifikat eine entsprechende Anerkennung genießt.

6.5. Akkreditierungen

Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle GmbH (DAkKS) gemäß ISO/IEC 27006 akkreditierte Zertifizierungsstelle und darf danach international gültige Zertifikate für ISO/IEC 27001-konforme Informationssicherheits-Managementsysteme (ISMS) erteilen. Darüber hinaus umfasst die DAkKS-Akkreditierung das Regelwerk „IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG“ für Strom- und Gasnetzbetreiber sowie das Regelwerk „IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG“ für Energieanlagenbetreiber.

Ferner ist die datenschutz cert GmbH bei der DAkKS für Produkte und Dienstleistungen gemäß ISO/IEC 17065 akkreditiert und darf danach als Konformitätsbewertungsstelle Vertrauensdienste gemäß eIDAS prüfen und bewerten. Die Akkreditierung gem. ISO/IEC 17065 umfasst auch Videosprechstunden (ips-VSS-IT).

Auditoren der datenschutz cert GmbH sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Auditoren für die TR-03109-6 (Smart Meter Gateway Administratoren) sowie BSI TR-03145 (Secure CA Operation) zertifiziert.

Die datenschutz cert GmbH ist als Prüfstelle für IT-Sicherheit und IT-Sicherheitsdienstleister beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt.

Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-Auditoren und IS-Revisionen. Die datenschutz cert GmbH stellt eines der beiden GS-Zertlabs, die für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfbegleitung in den IT-Grundschutz-Verfahren durchführt.

Die datenschutz cert GmbH ist bei der Bundesnetzagentur anerkannte Zertifizierungsstelle nach eIDAS gem. Vertrauensdienstegesetz (VDG).

Aufgrund der Akkreditierung bei der DAkKS und der Anerkennung beim BSI darf die datenschutz cert GmbH im Kontext von §8a BSIG/KRITIS-VO-Verfahren die Rolle der „prüfenden Stelle“ einnehmen. Ferner sind die Auditoren der datenschutz cert GmbH

beim BSI als Prüfer für § 8a BSIG anerkannt; dies umfasst auch die Prüfung von Systemen zur Angriffserkennung (SzA).

datenschutz



datenschutz cert GmbH

Hauptsitz Bremen

Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: +49 421 69 66 32-550

Standort Offenbach

Mainstraße 143
63065 Offenbach am Main
Tel.: +49 69 870 07 83-580

office@datenschutz-cert.de

www.datenschutz-cert.de

