secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

WHITEPAPER

IT-SICHERHEITSPRÜFUNGEN FÜR PRODUKTHERSTELLER

OKTOBER 2018

secuvera GmbH
Siedlerstraße 22 – 24
71126 Gäufelden
Telefon 0 70 32 / 97 58 - 0
Telefax 0 70 32 / 97 58 - 30
info@secuvera.de
www.secuvera.de

Autoren
Sebastian Fritsch, Tobias Glemser

INHALTSVERZEICHNIS

1. PRÜFUNG DER IT-SICHERHEIT VON PRODUKT-HERSTELLERN

Hersteller von IT-Produkten werden häufig von Ihren Kunden nach einer Sicherheitsprüfung gefragt. Welche Sicherheitsprüfung exakt gemeint ist, wird dabei häufig offen gelassen.

Es können die unterschiedlichsten Aspekte eines Produkts geprüft werden:

- das ganze Produkt?
- zentrale Eigenschaften des Produkts?
- eine spezielle Eigenschaft des Produkts?
- die Entwicklung des Produkts?
- der Supportprozess des Produkts?
- die ganze Entwicklungsfirma?

Kunden sind im Regelfall an einer unabhängigen Prüfung der Sicherheitsmerkmale der verwendeten Produkte interessiert. Für den Weg dorthin können verschiedene Prüfungen durchgeführt werden.

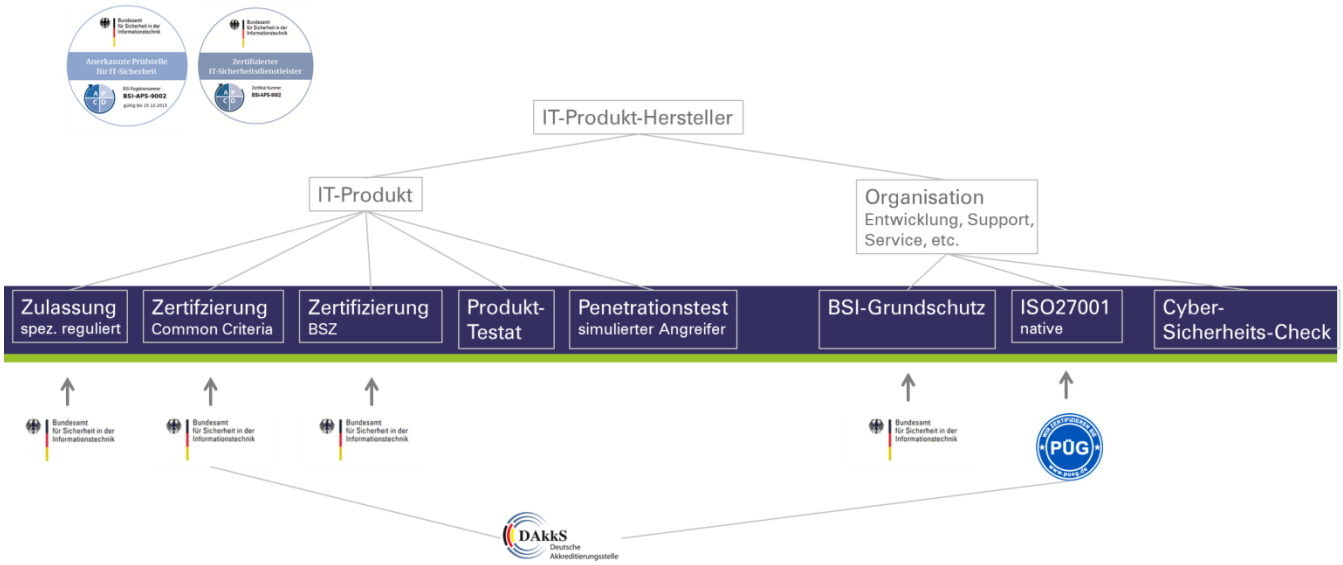
Das vorliegende Whitepaper stellt differenziert dar, in welchen Fällen das **Produkt** geprüft werden sollte und in welchen Fällen die **Organisation**.

Weiterhin soll dargestellt werden, ob das Ziel eine **Zertifizierung** oder ein **Testat** sein sollte. Da eine Zertifizierung wesentlich aufwändiger ist, werden ebenfalls die wesentlichen Abläufe beschrieben.

Zum Ende des Whitepapers stellen wir Ihnen die möglichen Dienstleistungen der secuvera in detaillierter Form vor.

2. WAS BENÖTIGEN SIE?

Nachfolgendes Bild gibt eine Übersicht, welche Optionen ein IT-Produkt-Hersteller hat, um die Qualität seiner Sicherheitseigenschaften extern bestätigen lassen zu können.



Zertifizierung (Common Criteria)

Die Common Criteria ist der internationale Prüfstandard für die Ermittlung von Vertrauenswürdigkeit von IT-Produkten. Dieser Standard ist als ISO 15408 normiert. Ausgestellte Produkt-Zertifikate werden europa- und weltweit akzeptiert. Die Common Criteria sind der klassische Standard zur **Produkt-Zertifizierung**. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) führt Zertifizierungen nach Common Criteria in Deutschland durch. Die eigentliche Prüfung, die Evaluierung, erfolgt durch eine Prüfstelle.

Details finden Sie im Kapitel *Zertifizierung nach Common Criteria*.

Zertifizierung (BSZ, Beschleunigte Sicherheitszertifizierung)

Die Beschleunigte Sicherheitszertifizierung (BSZ) ist eine Vorgehensweise, die durch das BSI aufgesetzt wurde. Die BSZ ist eine alternative **Zertifizierung von Produkten** ebenfalls angeboten durch das BSI, in welcher eine Penetrationstests getriebene Sicherheitsanalyse durchführt wird. Dabei wacht das BSI über das Verfahren. Die eigentliche Prüfung erfolgt durch eine geeignete Prüfstelle.

Details finden Sie im Kapitel *Zertifizierung durch die Beschleunigte Sicherheitszertifizierung*.

Zulassung

Des Weiteren existiert die Möglichkeit einer speziellen Zulassung von Sicherheitsprodukten für Einsatzzwecke im VS-Bereich. Dies kann nur durch das BSI erfolgen und ist speziell reguliert. Wir können Sie bei der Vorbereitung einer Zulassung unterstützen.

Details zur Zulassung finden Sie im Kapitel *Zulassung zur Verarbeitung von VS-Daten*.

Produkt-Testat

Ein Produkt-Testat enthält ist im Gegensatz zu einem Zertifikat die Aussage einer Prüfstelle ohne unabhängige Zertifizierungsinstanz. Testate sind im Regelfall im Vergleich zu einer Zertifizierung weniger aufwändig. Neben einem Testat wird ein detaillierter Prüfbericht übergeben, der zudem auch Hinweise für

zukünftige Produkt-Verbesserungen enthält. Details zu Produkt-Testaten der secuvera finden Sie im Kapitel *Produkt-Testat*.

Penetrationstest

Ein Penetrationstest ist eine Prüfung aus Sicht eines Angreifers. Meist werden Penetrationstests „Time-Boxed" durchgeführt. Sie sind also eine zeitlich beschränkte Sicherheitsanalyse, in der Schwachstellen gesucht werden. Hierbei handelt es sich um eine rein technische Analyse eines Produkts, welche sich in einer definierten Konfiguration befindet. Der Auftraggeber erhält nach der Analyse einen Bericht, der alle gefundenen Schwachstellen enthält, sowie transparent die Beschreibung zur Ausnutzung der Schwachstelle beinhaltet. Details zu Penetrationstest der secuvera finden Sie im Kapitel *Penetrationstests*.

BSI-Grundschutz

BSI-Grundschutz oder auch ISO 27001 auf der Basis von IT-Grundschutz ist ein Standard zur Prüfung des Informationssicherheitsmanagementsystems (ISMS) innerhalb eines Unternehmens. Für Produkt-Hersteller ist der BSI-Grundschutz die Möglichkeit die Prozesse zum Betrieb einer Serviceeinheit, z. B. eines Operation-Centers, auf die Einhaltung von Sicherheitsaspekten, prüfen zu lassen. Das BSI pflegt den Grundschutz inhaltlich und stellt **Zertifikate für Organisationen** aus. Grundschutz-Zertifikate werden insbesondere als Nachweis von der öffentlichen Verwaltung gefordert, da diese häufig selbst IT-Grundschutz aufgrund gesetzlicher Vorgaben umsetzen müssen. Details zu BSI-Grundschutz finden Sie im Kapitel *ISO 27001 und BSI-Grundschutz*.

ISO 27001 (native)

Die ISO 27001 hat die gleiche Ausrichtung wie der IT-Grundschutz und ist ebenfalls ein Standard zur Prüfung der Sicherheitsprozesse in einem Unternehmen. ISO 27001 Zertifikate werden von DAkkS-akkreditierten Organisationen ausgestellt. Eine **Organisations-Zertifizierung** nach ISO 27001 wird in der Regel von der Wirtschaft gefordert. Details zu ISO 27001 finden Sie im Kapitel *ISO 27001 und BSI-Grundschutz*.

Cyber-Sicherheits-Check

Eine weitere Möglichkeit zur Bewertung des eigenen Unternehmens ist ein durchgeführter Cyber-Sicherheits-Check. Der Cyber-Sicherheits-Check ist ein vom ISACA und dem BSI entwickelter Leitfaden zur effizienten Bestimmung des Informationssicherheitsstatus eines Unternehmens. Dies wird durch einen zertifizierten Cyber Security Practitioner festgestellt. Das Vorgehen ermöglicht es im Rahmen eines Festpreisprojekts zu einer Sicherheitsaussage zu gelangen. Dabei ist kein ISMS-Prozess notwendig. Weitere Informationen zum Cyber-Sicherheits-Check finden Sie auf unserer Webseite: WWW.SECUVERA.DE

Auf den nachfolgenden Seiten werden die unterschiedlichen Prüfungen jeweils kurz vorgestellt.

Kostenfreier, individueller Workshop

Um das komplexe Themenfeld einer Produkt-Zertifizierung intensiv diskutieren zu können bieten wir Ihnen einen halbtägigen individuellen Workshop mit Einführung in die Common Criteria an.

Im Workshop erfahren Sie auch weitere Details zu den hier diskutierten alternativen Prüfungsansätzen neben einer Common Criteria Zertifizierung.

Der Workshop kann bei Ihnen oder bei uns im Haus stattfinden. Kommen Sie zu uns, ist der Workshop für Sie kostenfrei. Durch den Workshop erfahren Sie Details zu Vorgehensweise, Aufwand, Kosten, Aussagekraft und Nutzen einer Zertifizierung. Nach dem Workshop haben Sie zudem Informationen, welche Zertifizierungsstufe Sie anstreben sollten.

Sie erfahren auch, ob für Sie zunächst ein Produkt-Testat die bessere erste Zielsetzung ist. Weiteres zum Testat erfahren Sie auf der folgenden Seite.

3. ZERTIFIZIERUNG NACH COMMON CRITERIA

Eine Common Criteria Zertifizierung weist die Prüfung von Sicherheitsfunktionen in Hard- und Software nach und weist eine hohe Vertrauenswürdigkeit (high assurance level) nach.

Das zu prüfende Produkt oder ein Ausschnitt wird innerhalb einer Evaluierung **Target of Evaluation** (kurz TOE) oder auch **Evaluierungsgegenstand** genannt. Die individuellen Prüfgrundlagen, welche für das spezifische Produkt vom Hersteller definiert werden, werden **Security Target** (ST) oder **Sicherheitsvorgaben** bezeichnet. Innerhalb der Sicherheitsvorgaben werden die **umzusetzenden Sicherheitsfunktionen** oder kurz SFRs (**Security Functional Requirements**) definiert. Diese werden im Rahmen der Zertifizierung auf die korrekte Umsetzung abgeprüft.

Der Gesamtumfang der Evaluierung wird über die **Vertrauenswürdigkeitsstufe** oder **EAL-Stufe** definiert, EAL steht dabei für **Evaluation Assurance Level**. Je Stufe werden unterschiedliche **Vertrauenswürdigkeitsklassen** oder **Assurance Classes** definiert, über die Details ergibt sich die Prüftiefe. Folgende Vertrauenswürdigkeitsstufen (EAL-Stufen) existieren:

- EAL 1 – funktional getestet
- EAL 2 – strukturell getestet
- EAL 3 – methodisch getestet
- EAL 4 – methodisch entwickelt, getestet und überprüft
- EAL 5 – semi-formal entwickelt
- EAL 6 – semi-formal verifiziert und getestet
- EAL 7 – formal verifiziert und getestet

Es gilt die Faustregel: Je höher die EAL-Stufe ist, desto mehr und detailliertere Nachweise werden innerhalb der Evaluierung verlangt. Tiefere Nachweise bedeuten zum einen einen höheren Detailierungsgrad oder auch zusätzliche Informationen wie Bereitstellung des Quellcodes oder auch formale Definitionen. Als Hersteller sollten Sie bei höheren Evaluierungsstufen beachten, dass eine intensivere Unterstützung benötigt wird, was sich direkt auf die benötigen internen Personalressourcen auswirkt.

Üblicherweise werden Software-Produkte bis zu EAL4 zertifiziert. Hardware-Produkte werden auch häufiger bis EAL6 zertifiziert. Dies trifft z. B. auf Smartcards zu, welche häufig die vertrauenswürdige Grundlage für andere Produkte bilden.

Die Common Criteria nutzt verschiedene Prüfaspekte, um eine Vertrauenswürdigkeit feststellen zu können. Während der Zertifizierung werden Designdokumente, durchgeführte Herstellertests und weitere Aspekte mit der vorgegebenen Common Criteria-Methodik evaluiert, d.h. es finden Analysen und Bewertungen dieser Prüfaspekte statt.

Wichtig bei der Auswahl der Prüfstelle ist die Erfahrung mit den verschiedenen Prüfaspekten, denn je nach Art der Evaluierung (z. B. entwicklungsbegleitende Erst-Zertifizierung) kann die Reihenfolge der Prüfung die Zeitdauer des Gesamtablaufs entscheidend beeinflussen.

Als dienstälteste Prüfstelle des BSI können wir weitreichende Erfahrungen in der Evaluierung von Produkten aufweisen. Gerne besprechen wir mit Ihnen Möglichkeiten wie eine geplante Produktzertifizierung effizient durchgeführt werden kann.

Im eigentlichen Zertifizierungsverfahren sind verschieden Rollen zu unterscheiden, deren Aufgaben werden nachfolgend noch einmal detailliert erläutert:

- Hersteller, meist auch der Sponsor der Evaluierung
- Prüfstelle / Evaluatoren
- BSI / Zertifizierer
- ggf. Berater, häufig Mitarbeiter der Prüfstelle aber nie an der Prüfung beteiligt

Bei einer Erst-Zertifizierung ist folgender Projektablauf empfehlenswert:

- Beratungs- oder Informationsgespräch beim BSI
- Antrag auf Zertifizierung mit Abgabe eines Security Targets
- Annahme des Antrags und Eröffnung des Verfahrens mit Vergabe einer Zertifizierungs-ID mit Veröffentlichung[1]
- Kick-Off mit dem BSI und der Prüfstelle bei Verfahrensbeginn
- Evaluierung des Produkts durch die Prüfstelle
- Abnahme der Prüfberichte durch das BSI
- Abschluss der Evaluierung durch Abnahme des Abschlussberichts
- Veröffentlichung des Zertifikats mit Bereitstellung von Security Target und Certification Report[2]

Eine Produkt-Zertifizierung nach Common Criteria ist international anerkannt. Konkret bedeutet dies, dass ein in einem Land zertifiziertes Produkt von jedem anderen Land innerhalb des Abkommens ebenfalls anerkannt wird. Deutschland ist sowohl Mitglied innerhalb des weltweiten CCRA-Abkommens, welches generell bis zur Stufe EAL2 gegenseitig anerkennt, als auch im europaweiten SOGIS-Abkommen, welches bis EAL4 und in besonders geregelten Fällen bis EAL7 gegenseitig anerkennt.

4. BESCHLEUNIGTE SICHERHEITSZERTIFIZIERUNG (BSZ)

Eine Beschleunigte Sicherheitszertifizierung (BSZ)[3] prüft ein IT-Produkt darauf, ob ein Produkt frei von Schwachstellen ist. Hierdurch soll eine möglichst hohe Vertrauenswürdigkeit bei Benutzern erreicht werden.

Viele Begrifflichkeiten sind analog denen der Common Criteria gewählt. Im Vergleich zu Common Criteria werden aber bis auf ein Security Target (Sicherheitsvorgaben) so gut wie keine Dokumente vom Hersteller für die Prüfung gefordert. Die Prüfungen fokussieren auf die sicherheitstechnische Robustheit des Produktes. Der Umfang einer solchen Prüfung sinkt dadurch im Vergleich zu einer Common Criteria Zertifizierung erheblich. Explizit vorgedacht ist die Aufrechterhaltung eines Zertifikates bei Produktupdates.

Zunächst findet ein **Kick-Off** mit Hersteller, Prüfstelle und Zertifizierung beim BSI statt. Dabei werden die geplante Evaluierung des **TOE** und der Aufwand erörtert.

Die Prüfstelle prüft in folgendem ohne Kommunikation mit Hersteller und BSI:

- **Korrektheit** der Installationsanleitung
- **Konformität** des TOE zu den Sicherheitsvorgaben
- **Robustheitsprüfung** des TOE mittels Penetrationstests und Angriffen mit hohem Sachverstand
- Korrektheit der implementierten **Kryptographie**

[1] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ZertifizierteProdukte/inzertifizierungbefindlich.html

[2] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ZertifizierteProdukte/zertifizierteprodukte_node.html

[3] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/Beschleunigte_Sicherheitszertifizierung/BSZ_node.html

Im Anschluss wird der Ergebnisbericht an das BSI gesendet. Ein wesentlicher Bestandteil des Prozesses ist dann die **Verteidigung** der Ergebnisse durch die Prüfstelle im Rahmen eines Interviews vor BSI-Experten.

Ob eine Prüfung erfolgreich war, wird durch das BSI entschieden. Im Falle einer positiven Prüfung erhält der Hersteller das Zertifikat. Der Hersteller verpflichtet sich, das Produkt auf neue Sicherheitslücken zu überwachen und **Updates** bereitzustellen.

secuvera war bereits in der Machbarkeitsstudie der BSZ beteiligt und plant direkt in der Pilotphase BSZ-Prüfstelle beim BSI zu werden.

5. ZULASSUNG ZUR VERARBEITUNG VON VS-DATEN

Neben einer Common Criteria Zertifizierung existiert auch ein vom BSI definierter Prozess zur Zulassung von Produkten für VS-Daten, dieser Prozess nutzt zu Teilen die Common Criteria Methodik. Im Rahmen sogenannter Zulassungsverfahren findet eine direkte Kommunikation zwischen Produkt-Hersteller und BSI statt, dieser Bereich ist speziell reguliert.

Wir können Sie in diesem Prozess ebenfalls in folgenden Bereichen unterstützen:

- Evaluierung des Produkts als Ergänzung oder Kompensation von Hersteller-Tests
- Beratung zur Erstellung von Dokumenten für eine Zulassung
- Beratung im direkten Dialog mit dem BSI zur Durchführung einer zeitlich effektiven Zulassung

Für eine Zulassung ist zunächst die Anforderung durch eine Behörde, den sogenannten Bedarfsträger, notwendig. Dieser muss von dem Produkt überzeugt sein und eine Anforderung zum Einsatz für VS-Daten beim BSI stellen.

Für weitere Informationen sollte ein informelles Erstgespräch durchgeführt werden, um Ihre aktuelle Situation konkret kennenzulernen.

6. PRODUKT-TESTAT

Da der Aufwand einer formalen Zertifizierung nach Common Criteria nicht von allen Herstellern getragen werden kann, aber häufig in Ausschreibungen Sicherheitsprüfungen oder Gutachten gefordert werden, wurde von secuvera eine weitere Prüfvariante entwickelt.

Die Prüfungen für ein Produkt-Testat bewerten die Sicherheitseigenschaften eines Produkts. Die Prüfmethodik basiert auf Abläufen der Prüfstelle sowie dem Bereich Penetrationstests und wird kombiniert angeboten. Im Vergleich zu Common Criteria Evaluierungen ist die Prüfung weniger formal. In den Prüfprojekten werden die ausgebildeten Prüfstellen-Evaluatoren eingesetzt.

Nach positivem Abschluss der Prüfung wird eine Testat-Urkunde ausgestellt, welche sich auf die getestete Produktversion bezieht. Zudem erhalten Sie als Hersteller einen Prüfbericht mit transparentem Analyseergebnis und eventuell Vorschlägen für zukünftige Verbesserungen. Zusammengefasst, Sie erhalten eine testierte Prüfaussage von Sicherheitsexperten zu Ihrem Produkt.

Als Methodik wurden folgende vier Schritte aufgestellt:

1. Workshop mit Hersteller

   Im Rahmen eines Workshops werden mit Ihnen als Hersteller die zu prüfenden Sicherheitsfunktionen ausgewählt. Hiermit wird der Fokus definiert.

2. Bedrohungsanalyse

   Identisch zur Vorgehensweise in einer Common Criteria Evaluierung wird eine Bedrohungsanalyse durchgeführt. Dabei werden mögliche Angriffsszenarien identifiziert.

3. Schwachstellenanalyse mit Penetrationstests

   Die im vorherigen Schritt herausgearbeiteten Angriffsszenarien werden skizziert und mögliche Schwachstellen identifiziert. Hier startet die technische Analyse, welche das Knowhow der Prüfstelle sowie des Bereichs Penetrationstests nutzt. Die Ergebnisse der Analysen und Tests werden für eine Bewertung der zuvor definierten Angriffsszenarien genutzt. Es kann entweder eine Durchführung in Form einer Blackbox oder Whitebox Vorgehensweise angewandt werden.

4. Übergabe Testats und Prüfbericht

   Sie erhalten das Testat und den detaillierten Prüfbericht mit allen Detailergebnissen.

Die Schritte zur Durchführung der Testats-Prüfung sind überschaubar und stellen sich wie folgt dar:

- Workshop zur Initialisierung (Definition von Sicherheitsfunktionen, Selbsteinschätzung)
- Übergabe des Produkts in zu testender Version
- Bewertung des Produkts
- Erstellung Prüfbericht, ggf. mit Handlungsempfehlungen
- Durchsprache der Ergebnisse mit Hersteller
- Übergabe Testats mit Prüfbericht

Eine Testats-Prüfung kann auch als Einstieg in eine spätere Produkt-Zertifizierung genutzt werden. Insbesondere die beschleunigte Sicherheitszertifizierung (BSZ) bietet sich als aufbauende Zertifizierung an, siehe Kapitel zuvor. Sie haben bereits die Prüfstelle kennengelernt, Sie haben Information zum Sicherheitszustand Ihres Produkts erhalten und bereits eine Abgrenzung der zertifizierbaren Sicherheitsfunktionen vorgenommen. Damit haben Sie schon wichtige Schritte für den Beginn einer Zertifizierung vorgenommen.

7. PENETRATIONSTEST

Ein Penetrationstest (kurz Pentest) ist meist ein „Time-Boxed" Ansatz, d.h. es wird ein zeitlicher Rahmen vereinbart, in dem eine Suche nach technischen Schwachstellen bei möglichst hohem Abdeckungsgrad der Prüfungen durchgeführt wird. Im Rahmen einer Produktprüfung muss eine definierte Konfiguration vorgegeben werden, welche über den Zeitraum der Prüfung nicht oder nur kontrolliert geändert wird.

Detaillierte Informationen zu der prinzipiellen Vorgehensweise und den damit geltenden Durchführungsstandards finden Sie im Whitepaper-Penetrationstest[4], welches von uns bereits im Jahr 2003 entwickelt wurde und seitdem ständig fortgeschrieben wird. Die Methodik bei der Durchführung von Penetrationstests wird von uns stets aktualisiert und optimiert, so dass wir ein hoch-spezialisiertes und ein auf Kundensituationen hin angepasstes Vorgehensmodell vorweisen können. Sicherheitsüberprüfungen wie ein Penetrationstest müssen Grundsätzen genügen, um für die geprüfte Organisation ein nutzbares Ergebnis zu erzielen. secuvera verfolgt dazu folgende Qualitätsansätze:

- Nachvollziehbarkeit
  „Sicherheit ist kein Voodoo" – dies gilt auch und insbesondere für Penetrationstests. Im Gegensatz zu einigen Marktbegleitern legt secuvera die gesamte Prüfmethodik inklusive der verwendeten Prüfwerkzeuge bei jedem Penetrationstest dem Kunden gegenüber offen.
- Wiederholbarkeit
  Um überhaupt in die Lage versetzt zu werden, die erfolgreiche Behebung von Schwachstellen zu prüfen, muss die Art der Prüfung und wie das Ergebnis in einem Penetrationstest gewonnen wurde, jederzeit transparent sein. Daher werden die hierfür relevanten Informationen vollständig zur Verfügung gestellt.
- Qualifikation
  „A fool with a tool is still a fool". Unser Know-How wird durch interne Fortbildungen, externe Schulungen und die Dokumentation von Abläufen sowie die definierte interne Kommunikation stets weiterentwickelt und gleichzeitig bewahrt. Es genügt nicht, die vermeintlich besten Prüfwerkzeuge einzusetzen und sich auf diese zu verlassen. Jedes Prüfwerkzeug unterliegt prinzipbedingten Schwächen, die ein Prüfer kennen muss, um diese durch händische Prüfungen bei der Durchführung des Penetrationstests auszugleichen und zu ergänzen.
  Die Qualifikation unserer Penetrationstester ergibt sich unter anderem durch
  - die unabhängige fachliche Prüfung als BSI-zertifizierter Penetrationstester,
  - die Veröffentlichung von Fachartikeln zu Schwerpunktthemen in der einschlägigen Presse,
  - als auch durch die Veröffentlichung von neu gefundenen Schwachstellen in Produkten.
- Standards
  Es existieren diverse Standards für die Durchführung von Penetrationstests. Die im Folgenden beschriebene Methodik eignet sich, um Prüfungen konform zu verschiedenen etablierten Prüfstandards vorzunehmen. Zu nennen sind hierbei insbesondere:
  - das Modell des BSI, welches in der Studie „Durchführungskonzept für Penetrationstests" beschrieben ist,
  - das Open Source Security Testing Methodology Manual (OSSTMM)
  - für Webanwendungen der OWASP Testing Guide
- Der Tellerrand
  Technische Prüfungen wie ein Penetrationstest zeigen technische Schwachstellen auf. Darüber hinaus kann aus diesen technischen Schwachstellen auch auf mögliche Schwächen in internen Prozessen abgeleitet werden. Hierfür benötigen die Prüfer ein Grundverständnis dieser organisatorischen Abläufe. Ebenso lassen sich diese Erkenntnisse vor etablierten Standards spiegeln. Daher sind alle unsere Penetrationstester auch mit Standards wie ISO 27001 auf der Basis von IT-

[4] https://www.secuvera.de/download/whitepaper-penetrationstest/

Grundschutz oder den PCI-DSS vertraut und kennen daher die Anforderungen dieser Standards, die nicht direkt im Bezug zu Penetrationstests stehen.

8. ISO 27001 UND BSI-GRUNDSCHUTZ

Müssen Sie als Produkthersteller einen Nachweis zur Sicherheit Ihres Unternehmens gegenüber der Wirtschaft, z. B. als Zulieferer, erbringen, dann wird meistens die Forderung nach einem ISO 27001 Zertifikat aufkommen.

Sie haben dabei die Möglichkeiten die Prozesse zum Betrieb einer Serviceeinheit, z. B. eines Operation-Centers, prüfen zu lassen. Im Aufbau eines Managementsystems nach ISO 27001 gilt es die zu schützenden Werte des Unternehmens oder des Organisationsbereiche zu identifizieren und ein adäquates Sicherheitskonzept aufzubauen.

Der ISO 27001 Standard kann dabei relativ frei umgesetzt werden. Wir unterstützen Sie gerne bereitend bei Aufbau und Umsetzung, aber auch später im Rahmen der Zertifizierung. secuvera beschäftigt drei Auditoren, welche Zertifizierungsaudits durchführen. Ein ausgestelltes ISO 27001 Zertifikat wird international anerkannt.

Wenn Sie Ihre Produkte direkt oder indirekt an eine Behörde verkaufen, kann es sein, dass Sie die Anforderung einer BSI-Grundschutz Zertifizierung erfüllen müssen. Viele Aspekte sind ähnlich zu ein einer ISO 27001-Zertifizierung, aber eine ganze Reihe von Anforderungen ist auch unterschiedlich. Insbesondere sind die Freiheitsgrade in der Umsetzung deutlich geringer.

Im Fall des BSI-Grundschutzes wird die Zertifizierung durch das BSI durchgeführt. Die Auditierung findet durch vom BSI anerkannte Grundschutz-Auditoren statt. secuvera beschäftigt zwei Grundschutz-Auditoren.

Im Rahmen eines Kennenlerngesprächs erläutern wir Ihnen die Unterschiede zwischen einer ISO 27001 und einer BSI-Grundschutz Zertifizierung und die wesentlichen Unterschiede für den Umsetzungsprozess.

9. DIENSTLEISTUNGEN DER SECUVERA

Die secuvera GmbH ist BSI-Prüfstelle und BSI-zertifizierter IT-Sicherheitsdienstleister. secuvera ist in drei Geschäftsbereiche thematisch organisiert:

- Prüfstelle für Common Criteria/ITSEC
- IT-Sicherheitsdienstleister für Penetrationstests
- IT-Sicherheitsdienstleister für BSI-Grundschutz

In allen drei Bereichen ist secuvera vom BSI anerkannt, wobei hierdurch die Qualifizierung, die Prozesse und weitere Forderungen unabhängig und regelmäßig bestätigt werden.

9.1.Prüfstelle für Common Criteria/ITSEC

Die Prüfstelle der secuvera bietet Evaluierungen in allen EAL-Stufen an. Thematisch ist die Prüfstelle spezialisiert auf folgende Produkttypen:

- Firewalls
- VPN-Lösungen
- mobile Systeme, z. B. Smartphones
- Kommunikationssysteme
- Betriebssysteme
- Datenbanksysteme
- Smart-Meter Gateways mit Konformitätsprüfung zu TR-03109
- Signaturanwendungen
- zusammengesetzte Systeme, z. B. Rechner + Betriebssystem + Anwendungen

Neben der Evaluierung für Common Criteria bieten wir auch die Erstellung von Produkt-Testaten an.

Folgende Unternehmen des Who-Is-Who der deutschen IT-Sicherheitsbranche zählen wir zu unseren Referenzkunden:

- genua gmbH
- T-Systems GmbH
- secunet AG
- Airbus Defence and Space

Neben der Durchführung der Prüfung bieten wir Ihnen auch unsere Beratungsleistung an. Eine Beratung ist beispielsweise in folgenden Fällen sinnvoll:

- Beratung im Vorfeld einer Erst-Zertifizierung
- Coaching von Autoren für Common Criteria Dokumentation
- Externe Autoren für das Verfassen von Common Criteria Dokumentation
- Unterstützung bei Zulassungs-Verfahren mit dem BSI

Sprechen Sie uns für einen kostenfreien Workshop zum Thema Zertifizierung an, im Nachgang erstellen wir Ihnen gerne ein detailliertes Angebot.

9.2. IT-Sicherheitsdienstleister für Penetrationstests

Wir bieten Ihnen die Durchführung von Penetrationstests an. Um Ihnen ein konkretes Angebot erstellen zu können, benötigen wir einen detaillierten Hintergrund zu Ihrer Problemstellung. Sprechen Sie uns hierzu an.

Folgende Unternehmen zählen wir unter Anderem zu unseren Referenzkunden im Bereich Penetrationstests:

- Atos Worldline
- E.ON Hanse
- Freenet
- F.I.S. Kordoba
- Otto
- Siemens
- Toto-Lotto Niedersachsen

9.3.IT-Sicherheitsdienstleister für BSI-Grundschutz / ISO 27001

Wir bieten Ihnen die Durchführung von folgenden Auditarten an:

- ISO 27001 auf der Basis von IT-Grundschutz (Zertifizierungs-Audit)
- ISO 27001 (native) (Zertifizierungs-Audit)
- IS-Revision (nach BSI Leitfaden)
- Cyber-Sicherheits-Checks (zum Festpreis)

Ebenfalls bieten wir Ihnen eine umfängliche Beratung an, sowohl zur Vorbereitung einer geplanten Zertifizierung als auch im Rahmen kontinuierlicher oder sporadischer Beratung an. Sprechen Sie uns hierzu an.

secuvera GmbH
Siedlerstraße 22 – 24
71126 Gäufelden
Telefon 0 70 32 / 97 58 - 0
Telefax 0 70 32 / 97 58 - 30
info@secuvera.de
www.secuvera.de