DuD
Datenschutz und Datensicherheit

T.I.S.P. – das europäische Qualifikationszertifikat für Informationssicherheit

Bedeutung, Akteure, Profil, Perspektiven

Kai Hartwich, Christoph Weinmann

Spezialisten für IT-Sicherheit sind auf dem Arbeitsmarkt gefragt. Aber für potentielle Arbeitgeber ist es mitunter nicht einfach, die Qualifikation der Bewerber realistisch einzuschätzen, genau wie es für den Bewerber nicht immer leicht ist, seine Qualifikation nach außen glaubhaft deutlich zu machen. Expertenzertifikate können das Problem mindern. Mit diesem Anspruch wurde vor knapp drei Jahren von TeleTrusT Deutschland e.V. das T.I.S.P.-Zertifikat entwickelt – mit Erfolg: Über 130 Experten haben es seitdem erworben.

Kai Hartwich

Assistent des Geschäftsführers von TeleTrusT Deutschland e.V., Projektleiter T.I.S.P.

E-Mail: kai.hartwich@teletrust.de

Christoph Weinmann

Leiter des Schulungsanbieters Secorvo College und verantwortlich für die dortige Etablierung des T.I.S.P.

E-Mail: christoph.weinmann@secorvo.de

Einleitung

Seit 2004 gibt es das Zertifikat „TeleTrusT Information Security Professional“, kurz T.I.S.P. (auch TISP), ein deutsches Qualifikationszertifikat für Informationssicherheit. Voraussetzung für den Erwerb sind mindestens drei Jahre Berufserfahrung in der Informationssicherheit, die Teilnahme an einem fünftägigen, zusammenfassenden Training sowie das Bestehen einer anschließenden Prüfung. Training und Prüfung wurden unter der Federführung von TeleTrusT von TeleTrusT-Mitgliedsunternehmen entwickelt. Sie werden derzeit von vier zugelassenen Schulungsunternehmen angeboten. Nach gut drei Jahren und rund 130 ausgestellten Experten-Zertifikaten lohnt sich ein Blick zurück, auf den Status und die Entwicklungsperspektiven.

Die Zeit ist reif

Informationssicherheit wird heute mit Recht in allen Geschäftsbereichen von Wirtschaft und Verwaltung grundsätzlich gefordert. Allerdings sind Antworten auf diese Anforderung breit gefächert und im Allgemeinen jeweils eng auf einen bestimmten Prozess zugeschnitten. Der Anwender steht deshalb oft ratlos vor dem riesigen Angebot von Produkten, Lösungen und Dienstleistungen für IT-Sicherheit.

Noch immer ist dabei zu erkennen, dass Sicherheit zu den Geschäftsprozessen hinzugefügt werden soll, statt generisch mit ihnen verbunden zu sein. In vielen Fällen hat sich allerdings die Sicht auf den Wert der Informationssicherheit bereits entscheidend gewandelt: Im Mittelpunkt steht nicht mehr eine abstrakte Schutzfunktion einer IT-Sicherheitslösung sondern ihre Rolle als „Enabler“ von risikobehafteten Geschäftsprozessen. Dabei gewinnt auch die „Compliance“ der gesamten IT-Abläufe eine zunehmende Bedeutung.

Letzten Endes ist damit klar, dass die zielführenden Entscheidungen zur Informationssicherheit auf Geschäftsführer- oder Vorstandsebene fallen. Dort liegt natürlich die Verantwortung für die Erfüllung von gesetzlichen Vorgaben, ausdrücklich auch zu denen des Datenschutzes.

Diese Situation spiegelt sich in den Organisationen wider. Die IT-Abteilungen verantworten die operativen Funktionen, während strategische Prozesse und die Umsetzung der Sicherheitspolicy meist vom „Chief Information Security Officer (CISO)“ oder vom „Chief Security Officer (CSO)“ wahrgenommen werden. Vor diesem Hintergrund sind auch die Veränderungen der Anforderungen an IT-Security-Spezialisten zu sehen.

Viele Unternehmen suchen heute händeringend nach „den Richtigen“ für Positionen in den Bereichen IT- und Informationssicherheit. Wie soll man aber einen wirklichen Informationssicherheits-Experten von solchen unterscheiden, die sich nur dafür ausgeben? In Deutschland gibt es derzeit zwar keinen derartigen Ausbildungsberuf, jedoch viele differenzierte Schulungsangebote und in der Praxis gewachsene „Do-it-yourself-Experten“.

Auch die tatsächlichen Experten wollen sich aus der Masse herausheben und damit ihre Berufschancen verbessern – sowohl bei der Karriere innerhalb eines Unternehmens als auch bei der persönlichen Weiterentwicklung über Unternehmensgrenzen hinweg. Dies gilt insbesondere für IT-Fachleute, die sich ethischen Werten wie dem ehrenhaften, ehrlichen, sachlich richtigen und verantwortungsvollen Handeln im Rahmen der eigenen Arbeit verpflichtet fühlen

und ihrem jeweiligen Arbeit- oder Auftraggeber einen gewissenhaften und kompetenten Service bieten wollen.

TeleTrusT engagiert sich

TeleTrusT hat in den 18 Jahren seit seiner Gründung viel für die „Förderung der Vertrauenswürdigkeit“ bei elektronischen Geschäftsprozessen getan und kann auf gute Erfolge verweisen. Es ist jedoch ein Weg der vielen kleinen Schritte.

Das Wirken von TeleTrusT war während der ersten Jahren stark auf die Unterstützung der Schaffung günstiger Rahmenbedingungen fokussiert. Es wurden Chiparchitekturen bis aufs letzte Bit diskutiert und an der rechtlichen Anerkennung wesentlicher technischer Sicherheitsfunktionalitäten der elektronischen Datenverarbeitung, z. B. der digitalen Signatur, mitgearbeitet. Der Euphorie angesichts vorstellbarer Möglichkeiten folgte allerdings bald die Ernüchterung angesichts der tatsächlichen praktischen Umsetzung durch die zuständigen Stellen. Die z. B. aus der Signaturgesetzgebung Deutschlands deutlich werdende Regulierungsgewalt hinterließ statt glatter Anwendungsfelder eher nahezu unüberschaubare und unüberwindliche Anwendungshindernisse.

Den praktischen Anforderungen folgend erweiterte TeleTrusT in den vergangenen Jahren den Blick auf die Geschäftsprozesse und die Ressource Mensch in diesen Prozessen. Deshalb hat sich TeleTrusT gern zur Unterstützung bereit erklärt, als einige Schulungsanbieter unter den TeleTrusT-Mitgliedern mit ersten Ideen zu einem neuen Experten-Zertifikat auf den gemeinnützigen Verein zukamen. Kern dieser Ideen war der gezielte Zuschnitt auf die besonderen Gegebenheiten in Europa und Deutschland im Bereich IT- und Informationssicherheit. In der direkten Folge entstand so unter dem Dach von TeleTrusT der TISP.

Das TISP-Konzept sieht eine zusammenfassende Schulung und eine Prüfung vor, die nach der übereinstimmenden Meinung der Beteiligten nur von einem „wirklichen“, d. h. qualifizierten Informationssicherheitsexperten in Deutschland oder Europa bestanden werden kann.

Die Basis von TISP bildet eine Selbstregulierung. Die Qualität des TISP-Zertifikats wird durch den politisch und wirtschaftlich unabhängigen Verein TeleTrusT kontrolliert. Das geschieht insbesondere durch die Arbeit des TISP-Beirates, der vom TeleTrusT-Vorstand berufen wird und aktuell aus sechs IT- und Informationssicherheitsexperten besteht. Der Beirat unterstützt den TeleTrusT-Vorstand maßgeblich bei der inhaltlichen Entwicklung von TISP, der Zulassung weiterer TISP-Schulungsanbieter sowie bei der Betreuung der TISP-Absolventen.

TeleTrusT steht im Zusammenhang mit TISP auch für Kontinuität. Für den Verein ist es nicht damit getan, TISP-Absolventen zu zertifizieren. Sofern diese dagegen keine Einwände haben, werden ihre Namen mit elektronisch signierten Kopien ihrer Zertifikate auf der TeleTrusT-Webseite veröffentlicht. Zusätzlich wird den Absolventen mit jährlichen Angeboten der Zugang zu aktuellen Entwicklungen der IT- und Informationssicherheit ermöglicht und so eine „TISP-Familie“ begründet.

Synergien steigern die Qualität

Der grundsätzliche Inhalt der TISP-Schulung und -Prüfung ist für alle TISP-Schulungsanbieter verbindlich vorgeschrieben. In die inhaltliche Ausgestaltung von Schulung und Prüfung können und sollen die zugelassenen Anbieter allerdings ihre Erfahrung und individuelle Schwerpunkte einfließen lassen und so wesentlich zur Qualität des TISP-Zertifikats beitragen. Wichtig dabei sind die unterschiedlichen Blickwinkel, aus denen die einzelnen Anbieter das Thema IT-Sicherheit betrachten. Secorvo und Secunet können jeweils auf eine 10-jährige Beratungs- und Schulungstätigkeit im Bereich IT-Sicherheit zurückblicken. Diese Erfahrung und die damit verbundene Expertise fließen in die Bewertung und Darstellung der Trainingsinhalte ein und sorgen für den wichtigen Praxisbezug. Das Fraunhofer-Institut SIT sowie die GITS AG agieren traditionell im Forschungsumfeld sowie im universitären Bereich. Die Nähe zur aktuellen Forschung und Lehre gestattet dem TISP-Training, den Bezug zu wesentlichen aktuellen technischen Entwicklungen aktiv aufzunehmen.

Doch die Qualifizierung und Expertise der einzelnen Anbieter sind nicht alleine der Grund für die Qualität von TISP. Erst Ihr synergetisches Zusammenwirken macht TISP zu dem was es heute ist. Durch einen kontinuierlichen Austauschprozess unter allen Anbietern werden die Inhalte des Trainings, die Schwerpunktsetzung und schließlich auch der Fragenpool für die Zertifikatsprüfung ständig überprüft, ergänzt und weiterentwickelt. Dieser Prozess wird durch ein Redaktionsteam gesteuert, bei dem die Verantwortung für die spezifischen Inhalte aller Vorträge liegt. Seine Aufgabe ist es, eine Plattform für die notwendige Abstimmung zwischen den verschiedenen Anbietern zu bilden sowie die Abstimmung aktiv einzufordern. Die Vorgaben der Redaktion sind für alle Referenten bindend. Damit gelingt es, die Vergleichbarkeit von Schulungen und Prüfungen sowie eine ständige Qualitätssicherung zu garantieren – ein wesentliches Qualitätsmerkmal des TISP.

Eine Schlüsselposition bei der Qualitätssicherung und Weiterentwicklung übernimmt der TISP-Beirat, dem das Redaktionsteam unterstellt ist. Hier werden die inhaltlichen Grundsätze sowie die Entwicklungsrichtung für den TISP abgestimmt und festgelegt. Er bildet auch die Basis für die erfolgreiche Koordination der Arbeit aller Beteiligten.

Zukünftig wird die Aufsicht über die TISP-Entwicklungen zusätzlich durch ein Steering Board mitgetragen, in dem Vertreter der Management-Ebene, auch aus dem Bundesamt für Sicherheit in der Informationstechnik (BSI), vertreten sein sollen.

Die Inhalte spiegeln die Praxis wider

Das TISP-Zertifikat belegt, dass sein Inhaber über ein breites Verständnis der IT-Sicherheit verfügt und in der Lage ist, die unterschiedlichen Aspekte des Themas IT- und Informationssicherheit miteinander zu vernetzen und ganzheitlich zu betrachten.

In der Praxis wird von IT-Sicherheitsverantwortlichen immer stärker Flexibilität und fortlaufende Qualifizierung gefordert, um auf die sehr differenzierten praktischen Anforderungen des Arbeitsalltages adäquat reagieren zu können. Neben der soliden fachliche Ausbildung bedarf es einer kontinuierlichen Weiterbildung, um ein breites Wissensspektrum aufbauen zu können. Ebenso ist es wesentlich, dass die Fähigkeit, in größeren Zusammenhängen denken zu können, ausgebildet und gefördert wird.

Diesem Erfordernis folgend sind die Inhalte von TISP breit gefächert. Sie beginnen mit gängigen Angriffsszenarien, behandeln kryptografische Grundlagen, auf denen die

wichtigsten Sicherheitstechnologien aufbauen und bearbeiten Sicherheitsaspekte der Betriebssysteme. Dabei spielen insbesondere die praktischen Umsetzungen im täglichen Arbeitsalltag eine wichtige Rolle, wie auch die rechtlichen Aspekte der IT-Sicherheit. Einen wesentlichen Platz und entsprechenden Raum nimmt das Thema „Information Security Management“ ein. Der Rolle von Prozessen, unterstützenden Standards und ganzheitlichen Sichtweisen wird hier ebenfalls Rechnung getragen.

Insbesondere in den Bereichen Information Security Management und rechtliche Rahmenbedingungen werden den Inhalten von TISP die europäischen Standards und Rechtssprechungen zugrunde gelegt. TISP ist ein Zertifikat, das sich vor allem an IT-Security Verantwortliche richtet, die in Europa agieren.

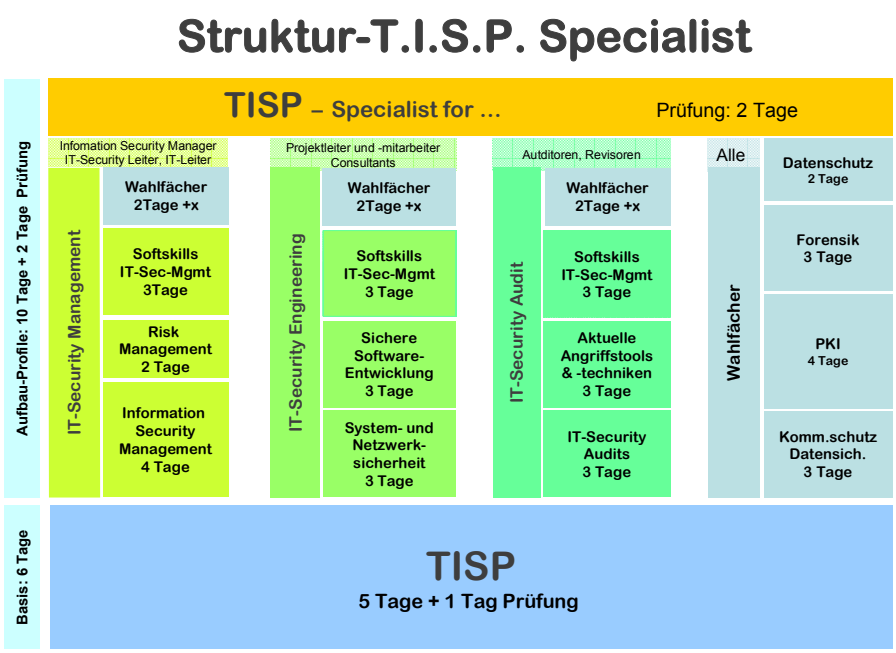
Der nächste Schritt: Zertifikate für Spezialisten

Der TISP-Beirat ruht sich auf dem Erreichten nicht aus. TISP ist ein Zertifikat, das sich an den sehr differenzierten Erfordernissen des Arbeitsalltages ausrichtet. In seiner jetzigen Form gibt er IT-Sicherheits-Verantwortlichen die Möglichkeit zu belegen, dass sie eine breit angelegte fachliche Qualifikation besitzen.

Auf dieser Basis möchte der TISP ab 2008 für bestehende spezialisierte Tätigkeitsfelder in der IT-Sicherheit spezifische Ausbildungsgänge mit einer Profil-Zertifizierung anbieten: den „TISP Specialist“. Im Fokus stehen dabei drei Themenfelder:

- Information Security Management,
- IT-Security Engineering und
- IT-Security Auditing.

Für jeden Ausbildungsgang werden spezifische Pflichtveranstaltungen angeboten sowie die Möglichkeit, ein oder zwei Wahlthemen zu belegen, die zusammen ein Volumen von mindestens 10 Schulungstagen haben. Dabei werden die Kurse durch



Hausarbeiten ergänzt, die den Teilnehmern die Möglichkeit geben, wesentliche Aspekte der Schulungen zu vertiefen. Alle Veranstaltungen zusammen sollen in einem Zeitraum von zwei Jahren besucht werden. Die abschließende zweitägige Prüfung wird im Wesentlichen aus der Bearbeitung einer individuellen Aufgabenstellung bestehen, deren Ergebnis in einem Kolloquium vorgestellt und verteidigt werden soll.

Damit ist „TISP Specialist“ ein Lehrgang, der nicht nur bestehende Qualifikation bestätigt, sondern hochgradig spezialisiertes Know-how in hochwertigen Schulungen vermittelt und damit zum IT-Sicherheitsspezialisten ausbildet. Die erreichte Qualifikation wird nach der bestandenen Prüfung mit einem speziellen TISP-Zertifikat belegt.

Fazit

Die Erfahrungen der letzten drei Jahre haben gezeigt, das Qualifikationszertifikate für IT-Sicherheitsexperten gefragt sind und das TISP-Zertifikat als solches anerkannt und akzeptiert wird. TeleTrusT und die TISP-Anbieter haben bis heute viel investiert, um die hohe Qualität des Trainings und der Prüfung sicherzustellen und weiter zu entwickeln. Damit wurde erheblich dazu beigetragen, das Vertrauen in TISP aufzubauen und zu stärken. Mit den vorgesehenen zukünftigen Investitionen könnte sichergestellt werden, dass dieser Vertrauensvorsprung stabilisiert und ausgebaut werden kann.

> TeleTrusT und die TISP-Anbieter sind überzeugt, dass sie mit der Mischung aus einem Zertifikat zu breitem IT-Security Wissen sowie den drei Spezialistenzertifikaten sehr spezifisch und angemessen auf die Erfordernisse des Marktes reagieren.

Wenn dem so ist, könnte es gelingen ein allgemein anerkanntes Qualifizierungsniveau zu etablieren und eine „Expertengemeinde“ der Informationssicherheit aufzubauen.