QUALIFIZIERTE SICHERHEITSLÖSUNGEN

DIE ENTSCHEIDUNG FÜR EINE VERTRAUENSWÜRDIGE LÖSUNG

Julien Paffumi
Product Marketing Manager bei Stormshield

Wie viel Vertrauen haben Sie in die Sicherheitslösung, die Ihr Informationssystem schützt? Eine zentrale Frage, die jedoch viel zu wenig gestellt wird. Ob als Unternehmen oder im Bereich der Verwaltung, Sie müssen in Lösung, die Sie schützen soll, vollstes Vertrauen setzen. Was nützt es, ein Sicherheitsprodukt zu installieren, wenn es nur wenig effizient ist … oder schlimmer noch, wenn es Hintertürchen offen lässt, über die Unbefugte auf Ihre Informationen zugreifen können?

Wie kann man also in dem aktuellen Kontext zwischen Spannungen und Misstrauen und angesichts der vielen internationalen Lösungen eine sichere und zuverlässige Wahl treffen? International gibt es heute bereits mehrere Zertifizierungen, mit denen die Zuverlässigkeit der Produkte bescheinigt wird. Aber wie steht es um die Vertrauenswürdigkeit? Um dieser Unsicherheit entgegenzuwirken, haben mehrere europäische Länder nun eine weitere Kennzeichnungsstufe geschaffen: die Qualifikationen. Was aber sind nun die Unterschiede zwischen Qualifikation und Zertifizierung? Und wie findet man sich zurecht?

Zertifizierung oder Qualifikation – worin besteht der Unterschied?

Nehmen wir das Beispiel Frankreich mit seiner Agence nationale de la sécurité des systèmes d'information (ANSSI, Nationale Agentur für Sicherheit der Informationssysteme), die sich auf mehrere Jahre Erfahrung im Bereich Qualifikation berufen kann. Sie unterscheidet verschiedene Typen der Kennzeichnung: **„Certification Critères Communs" (Zertifizierung nach Common Criteria)**, „Certification de Sécurité de Premier Niveau" (CSPN, Sicherheitszertifizierung der höchsten Stufe) und Qualifikation, die wiederum in die Stufen „Elémentaire" (grundlegend), „Standard" (normal) und „Renforcée" (erweitert) unterteilt wird. Wie kann man sich da zurechtfinden?

DIE ZERTIFIZIERUNG

Mit der Zertifizierung wird die **Zuverlässigkeit** eines Sicherheitsprodukts bescheinigt. Der Herausgeber legt ein bestimmtes „Sicherheitsziel" fest, worin die bewerteten Sicherheitsfunktionen und der entsprechende Kontext der Nutzung beschrieben werden. Eine unabhängige Stelle, die als „Centre d'Évaluation de la Sécurité des Technologies de l'Information" (CESTI, Zentrum zur Bewertung der Sicherheit von Informationstechnologien) akkreditiert ist, führt eine Bewertung der Entwicklungsprozesse des Produkts sowie seiner Fähigkeit, Angriffe einer bestimmten Stärke abzuwehren, durch.

Die ***„Certification Critères Communs" (CC)*** wird in vielen Ländern anerkannt und ausgestellt.

Sie gibt an, bis zu welcher Angriffsstufe die Abwehrfähigkeit des Produkts bewertet wurde. Eine Firewall beispielsweise kann entsprechend den Stufen EAL3+, EAL4+ usw. zertifiziert werden.

COMMON CRITERIA

COMMON CRITERIA

Die ***„Certification de Sécurité de Premier Niveau" (CSPN)*** wurde von der ANSSI geschaffen, um eine Alternative zu den Bewertungen der CC-Zertifizierung zu bieten, deren Kosten und Dauer Hindernisse sein können. Die Tests werden in begrenzter Zeit und mit begrenztem Arbeitsaufwand durchgeführt (typischerweise zwei Monate, 25 bis 35 Personentage). Achtung, kleine Anmerkung zur Klassifikation: Im Gegensatz zur CC-Zertifizierung, die international anerkannt ist, handelt es sich bei der CSPN derzeit um eine rein französische Kennzeichnung. Ziel ist es jedoch, dass sie in Zukunft auch auf europäischer Ebene anerkannt wird.

Achtung – was Sie vielleicht noch nicht über die Zertifizierung wissen

- Solange die Zertifizierung anschließend nicht zu einer Qualifikation führt, wird die Zertifizierungsstelle des ausstellenden Landes bei der Festlegung des Sicherheitsziels nicht intervenieren. Der Herausgeber kann das Ziel also bis zu einem gewissen Maße nach eigenem Ermessen anpassen und möglicherweise bestimmte Sicherheitsfunktionen, die das Produkt umfasst, von den Bewertungen ausschließen.
  Daher ist es sehr wichtig, sich das vom Herausgeber bestimmte Sicherheitsziel hinsichtlich der eigenen Erfordernisse für den Schutz gut anzuschauen. Dies liegt in Ihrer Verantwortung, wenn Sie die entsprechende Sicherheitslösung auswählen.
- Im Zertifizierungsbericht können Vorbehalte oder Anwendungsempfehlungen enthalten sein, die mit Blick auf Ihren Anwendungskontext sorgfältig zu lesen sind.
- Und schließlich gilt zu beachten, dass eine Zertifizierung für spezielle Software- und Hardwareversionen gilt – versichern Sie sich also, dass sich die entsprechende Zertifizierung nicht auf Produkte oder Versionen von vor mehreren Jahren bezieht, die eventuell nicht mehr verkauft oder unterstützt werden können.

DIE QUALIFIKATION

Über die einfach Zertifizierung hinausgehend ist die Qualifikation mit einer **Empfehlung** der ANSSI verbunden und attestiert die **Vertrauenswürdigkeit**, die der französische Staat einem Sicherheitsprodukt und seinem Herausgeber bescheinigt.

Die erste Voraussetzung besteht darin, eine Zertifizierung einer ausreichenden Stufe zu erhalten, und zwar mit einem **von der ANSSI anerkannten Sicherheitsziel**. Außerdem führt die ANSSI neben dem Zertifizierungsverfahren zusätzliche Analysen durch, unter anderem eine **Prüfung des Quellcodes des bewerteten Produkts**. Achtung bei reinen Ankündigungen. Vorsicht ist geboten, wenn ein Herausgeber versichert, bald eine Qualifikation zu erhalten, dabei aber nicht mittels eines offiziellen Schreibens nachweisen kann, dass das Verfahren zur Qualifikation tatsächlich begonnen hat.

Diese **Qualifikation eines Produkts** wird in Frankreich und in bestimmten Fällen auch in anderen europäischen Ländern anerkannt. Sie ist auch eine Voraussetzung dafür, dass ein Produkt für den Schutz von Informationen zugelassen wird, die als „NATO Restricted“ oder „EU Restricted“ eingestuft sind.

NATO OTAN

NATO RESTRICTED

Die Kennzeichnung „NATO Restricted“ (NATO – VS – Nur für den Dienstgebrauch)

Informationen werden als „NATO Restricted“ eingestuft, wenn sich ihre unbefugte Weitergabe nachteilig auf die Interessen der NATO oder bestimmter NATO-Mitgliedstaaten auswirken könnte.

Um in den Katalog der Lösungen aufgenommen zu werden, die offiziell für den Schutz dieser Informationen akkreditiert sind, reicht die Zertifizierung nicht aus. Das Produkt muss eine „Standard“-Qualifikation erhalten.

EU RESTRICTED

Die Kennzeichnung „EU Restricted“/ „Restreint UE“ (EU-VS – Schutz von Verschlusssachen der EU)

Informationen werden als „EU Restricted“ eingestuft, wenn sich ihre unbefugte Weitergabe nachteilig auf die Interessen der Europäischen Union oder bestimmter EU-Mitgliedstaaten auswirken könnte.

Um in den Katalog der Lösungen aufgenommen zu werden, die von der EU für den Schutz dieser Informationen zugelassen sind, muss das Produkt die Qualifikation von zwei Behörden von EU-Mitgliedstaaten erhalten haben (in Frankreich die „Qualification Standard“). Auch in diesem Fall ist die Zertifizierung allein nicht ausreichend.

Warum lohnt es sich, außerhalb von Frankreich ein von der ANSSI qualifiziertes Produkt zu verwenden?

In Frankreich ist es für bestimmte regulatorische Umfelder verpflichtend, die von der nationalen französischen Agentur qualifizierten Lösungen anzuwenden. Sie sind aber gewiss nicht nur auf französische Unternehmen und Organisationen beschränkt! Mit der Entscheidung für eine von der ANSSI qualifizierten Lösung erhält man ein Produkt, das von einer anerkannten und vertrauenswürdigen Behörde eines Mitgliedsstaates der Europäischen Union empfohlen wird.

- Damit nutzen Sie also **ein Produkt, dessen Zuverlässigkeit im Rahmen eines Zertifizierungsverfahrens geprüft** wurde
- Mit einem von der ANSSI b**estätigten Bewertungs- und Anwendungsziel**
- Dessen **Quellcode geprüft** wurde
- Und das von **einem Unternehmen hergestellt wurde, dessen Verfahren** der Entwicklung, Lieferung und Unterstützung von einem EU-Mitgliedsstaat **als vertrauenswürdig anerkannt wurden**

Um die französischen Unternehmen bei ihrer Wahl zu unterstützen, stellt die ANSSI seit Kurzem einen Katalog qualifizierter Lösungen zur Verfügung, die eine neue Kennzeichnung tragen: **das Sicherheitssiegel „Visa de Sécurité“**. Dieses Siegel wird für Lösungen ausgestellt, die vom französischen Staat nach strengen Tests und einer genauen Analyse als zuverlässig und vertrauenswürdig anerkannt werden. Mit diesem Siegel und der Unterstützung durch das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** setzt sich die ANSSI so weiterhin für strenge Sicherheitsanforderungen in Europa ein.

Und Sie? Haben Sie konkrete Anhaltspunkte dafür, dass Sie Ihrer aktuellen Sicherheitslösung und dem Unternehmen, das sie herausgebracht hat, vertrauen können? Vertrauen Sie den Kennzeichnungen und Zertifizierungen, mit denen es ausgezeichnet wurde?

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security).

www.stormshield.com