Produktzertifizierungen – was bringts?

Sicherheitszertifizierungen werden kommen in der EU, so viel ist sicher. Doch allen Kritikern zum Trotz bringt das mehr Vor- als Nachteile.

Von Sebastian Fritsch und Tobias Glemser

Die chinesische Regierung macht es vor: Immer mehr Regularien zwingen Hersteller, ihre Produkte nach Standards zertifizieren zu lassen. Die EU arbeitet ihrerseits seit Jahren am Cybersecurity Act (CSA), der harmonisierte europäische Sicherheitszertifizierungen definiert. Ohne eine solche Zertifizierung werden Produkthersteller künftig keine Produkte mehr auf den Markt bringen können. Eine Zertifizierung kann andererseits auch ein deutlicher Marketingmehrwert für Hersteller sein.

An der Aussagekraft von Produktzertifizierungen gibt es seit jeher Grundsatzkritik: Da es prinzipbedingt hundertprozentige Sicherheit nicht geben kann, sind Produktzertifizierungen in den Augen einiger praktisch wertlos. Da immer nur eine spezifische Version geprüft wird, dürfe man außerdem keine Produktupdates zertifizierter Produkte einspielen. Warum gut gemachte Produktzertifizierungen nach einheitlichen Standards sinnvoll und Updates selbstverständlich nötig und möglich sind, beleuchtet der Artikel.

iX-TRACT

- Kritiker bemängeln an Zertifizierungen vieles, etwa die fehlende Garantie für eine hundertprozentige Sicherheit oder den schwierigen Umgang mit Updates.
- Wer sich für eine Zertifizierung entscheidet, profitiert in der Regel nicht nur durch sicherere Produkte, sondern letztlich auch durch ausgereiftere Prozesse.
- Aktualisierungen und Patchprozesse sind keine Hindernisse mehr: Zunehmend werden diese Aspekte in den Zertifizierungsprozess einbezogen.

Es gibt verschiedene Ansätze bei der Prüfung beziehungsweise bei Sicherheitsaussagen zu Produkten, die über die reine Selbstauskunft „Wir sind sicher“ hinausgehen. Es gibt drei Arten von Standards, die im Folgenden unterschieden werden: generelle Modelle, domänenspezifische Modelle und standardisierte Selbstauskünfte.

Die verschiedenen Ansätze

Die relevantesten generellen Modelle sind Common Criteria (CC) als internationaler Standard, die Beschleunigte Sicherheitszertifizierung (BSZ) des Bundesamts für Sicherheit in der Informationstechnik (BSI) und die Verschlusssachen-Zulassung (VS), ebenfalls beim BSI angesiedelt. Alle haben ein dokumentiertes Vorgehensmodell und sind nicht auf bestimmte Produktklassen beschränkt. So gibt es CC-Zertifikate zum Beispiel für Smartcards, Betriebssysteme, Firewalls oder Videokommunikationssoftware. Common-Criteria-Zertifikate sind aufgrund des damit verbundenen Aufwands für Hersteller eine große Herausforderung. Einerseits sind viele motiviert, einen entsprechenden Nachweis vorzeigen zu können und sich durch die Normerfüllung zu verbessern. Andererseits liegen die damit verbundenen Gesamtkosten schnell im sechsstelligen Bereich. Damit lohnt sich die Investition für viele grundsätzlich einer Prüfung nicht abgeneigter Hersteller derzeit nicht.

Das BSI hat mit der Beschleunigten Sicherheitszertifizierung eine Alternative geschaffen, die auch europäisch harmonisiert werden soll. Vor Kurzem haben der BSI-Präsident Arne Schönbohm und Guillaume Poupard, der Generaldirektor des französischen BSI-Pendants ANSSI (Agence nationale de la sécurité des systèmes d’information), ein Abkommen zur gegenseitigen Anerkennung der IT-Sicherheitszertifikate BSZ und CSPN (Certification de Sécurité de Premier Niveau) unterzeichnet. Mit Inkrafttreten des Abkommens werden bereits gültige Zertifikate in beiden Programmen als gleichwertig anerkannt. Zukünftig erteilte Zertifikate werden mit ihrer Veröffentlichung automatisch anerkannt. Weitere Schritte in Richtung Harmonisierung sind in Arbeit.

Die BSZ verfolgt den Ansatz eines Produktpenetrationstests. Dabei sind vom Hersteller im Vergleich zu CC deutlich weniger formale Anforderungen zu erfüllen. Die Prüfer untersuchen mit definierten Angreifermodellen, ob sie im Produkt innerhalb der zur Verfügung stehenden

Governance	Design	Implementation	Verifications	Operations
Strategy and Metrics	Threat Assessment	Secure Build	Architecture Assessment	Incident Management
Policy and Compliance	Security Requirements	Secure Deployment	Requirements-driven Testing	Environment Management
Education and Guidance	Security Architecture	Defect Management	Security Testing	Operational Management

Das Software Assurance Maturity Model (SAMM) der OWASP berücksichtigt den gesamten Softwarelebenszyklus. Es soll eine messbare Methode zur Analyse und Verbesserung des sicheren Entwicklungslebenszyklus bieten.

Zeit Schwachstellen entdecken konnten. Für eine erfolgreiche Zertifizierung muss das geprüfte Produkt entsprechend resilient designt und entwickelt worden sein. Die Zulassung von VS-Produkten ist ein spezielles Feld für hoheitlich eingesetzte Sicherheitsprodukte und eigens reguliert.

Für verschiedene Domänen wurden eigene Standards veröffentlicht, etwa die IEC 62443 für industrielle Steuerungsanlagen. Die Norm adressiert in unterschiedlichen Teilen sowohl Hersteller als auch Integratoren und Betreiber. Der Normabschnitt 4 ist für Produkthersteller relevant und wird bereits von großen Konzernen bei der Beschaffung verlangt. Perspektivisch können Hersteller nur noch Produkte verkaufen, die den Anforderungen genügen.

Höhere Anforderungen an kritische Komponenten

Für den politisch viel diskutierten Mobilfunkstandard 5G beschrieb zuletzt die Novellierung des BSI- und Telekommunikationsgesetzes zusätzliche Sicherheitsanforderungen für Netze und Dienste mit erhöhter Kritikalität. Der Gesetzgeber fordert nun die Zertifizierung kritischer Komponenten. Dies gilt für alle Komponenten, die definierte kritische Funktionen implementieren.

Bei allen bislang beschriebenen Vorgaben ist eine Prüfung durch Dritte das Ziel. Daneben gibt es aber auch reine Selbstauskünfte wie das neue IT-Sicherheitskennzeichen des BSI. Beim Sicherheitskennzeichen muss der Hersteller im Antragsverfahren spezielle Informationen zum Beispiel über die Dauer der Verfügbarkeit von Updates angeben. Das BSI prüft lediglich die Plausibilität. Die Sicherheitskennzeichen sollen dem Verbraucher beim Kauf ermöglichen, auf Sicherheit als Qualitätseigenschaft zu achten. Ob und wie lange ein Produkt Updates vom Hersteller erhält, ist dabei ein wichtiger Baustein.

Der Bundesverband für IT-Sicherheit TeleTrusT hat mit „Security Made in Germany“ und „Security Made in EU“ zwei anerkannte Vertrauenszeichen geschaffen. Hersteller, aber auch Dienstleister bestätigen unter anderem, dass das Produkt keine Hintertüren enthält und den Datenschutzanforderungen genügt.

Durch die europäische Harmonisierung von Zertifizierungen im Rahmen des EU CSA sollen einheitliche Nachweise entstehen. Derzeit gibt es in den Mitgliedsstaaten nationale Standards, zum Beispiel in Frankreich mit der erwähnten CSPN-Zertifizierung. Die ENISA als europäisch führende Behörde schickt sich an, für verschiedene Vertrauenswürdigkeitsstufen entsprechende Zertifizierungsprogramme zu schaffen.

Grenzen der Prüfung

Für Produkte oder Produktklassen lassen sich vergleichsweise klare Prüf- und Messmethoden festlegen und anwenden. Für industrielle Automatisierungskomponenten wird zurzeit ein spezifischer Normteil in der IEC 62443 entwickelt, der die Prüfanforderungen enthalten wird. Ein weiteres Beispiel sind Zufallszahlengeneratoren (Random Number Generator; RNG) in Produkten. Für RNGs hat das BSI mit den AIS20/31 eine Prüfmethodik beschrieben. Die besprochenen Zertifizierungsverfahren sind für Komponenten wie Router, Firewalls oder Smartphones gedacht und werden nicht auf einzelne Elemente wie einen RNG angewendet.

Für die Prüfung von Prozessen ist eine andere Vorgehensweise notwendig. Beispielsweise kommen beim sicheren Softwareentwicklungszyklus (Security Development Lifecycle, SDL) oder bei Informationssicherheitsmanagementsystemen (ISMS) andere Verfahren zum Einsatz. Das OWASP-Projekt Software Assurance Maturity Model (SAMM) beschreibt einen SDL, wenngleich man danach nicht zertifizieren, aber durchaus prüfen kann (siehe Abbildung). Vielen Lesern dürfte die ISO 27001 oder der BSI-Grundschutz für ISMS bereits bekannt sein.

Fünf Euro für das Phrasenschwein

„Hundertprozentige Sicherheit gibt es nicht“ ist der Phrasenschweinsatz Nummer eins in der Cybersicherheit. Dies gilt selbstverständlich auch für zertifizierte Produkte. Häufig gibt es Kritik oder sogar Häme, wenn Schwachstellen in zertifizierten Produkten auftreten. Meist basiert dies auf Unverständnis, und bessere Alternativen zu einer Zertifizierung nennen die Kritiker nicht.

Ein Kritikpunkt lautet, dass veraltete Versionen eines Produkts zertifiziert werden. Bis eine Zertifizierung abgeschlossen ist, sind nicht selten bereits neuere Versionen am Markt. Das ist den zeitraubenden und arbeitsintensiven Prüfprozessen geschuldet. Die Prüfungen von IT-Produkten sind aufgrund der Individualität, der Komplexität und der Vielzahl der zu prüfenden Funktionen aufwendig. Mechanische Prüfungen hingegen sind zum Teil sehr einfach. So wird eine mechanische Belastungsprüfung als Beweis für Langlebigkeit sogar in dem ein oder andern Möbelhaus demonstriert und kann von jedem nachvollzogen werden – eine Belastungsprüfung von IT-Produkten sicherlich nicht.

Schwachstellen aus dem Nichts?

Insofern ist die Kritik zutreffend, dass nicht zwingend die aktuellste Version geprüft wurde. Es ist dennoch unwahrscheinlich, dass auf dem Weg von einer geprüften zu einer weiterentwickelten Version plötzlich Designschwachstellen auftreten.

Auch zertifizierte Produkte weisen immer wieder Schwachstellen auf, was Kritiker den Sinn des Zertifizierens bezweifeln lässt. Doch bei vielen zertifizierten Produkten gilt es, auch den Entwicklungsprozess zu betrachten: Hier zeigt die Erfahrung, dass die Hersteller durch die Zertifizierungsanstrengungen dazulernen und man davon ausgehen kann, dass, wenn Schwachstellen gefunden werden, Updates zügig bereitgestellt werden.

Einige Hersteller oder politische Parteien reagieren ja bis heute mit Klageandrohungen, wenn man auf Schwachstellen hinweist – wie geschehen bei der vulnerablen Wahlkampf-App der CDU. Hier hatte die Partei zunächst die Entdeckerin der Schwachstellen angezeigt, nach massivem Protest der Öffentlichkeit die Anzeige aber wieder zurückgezogen. Ein solcher Umgang mit reporteten Schwachstellen wird bei Herstellern mit Zertifizierungsstrategie und einem damit einhergehenden Qualitätsanspruch vermutlich nicht vorkommen.

In Umgebungen, in denen der Einsatz zertifizierter oder zugelassener Produk-

te regulativ vorgeschrieben ist, werden Updates teilweise nicht eingespielt, weil man sonst den „zertifizierten Betrieb“ verlasse. Das ist aus Sicherheitssicht natürlich auf keinen Fall empfehlenswert. Eine bekannt unsichere zertifizierte Version ist sicher nicht der Wunsch eines Regulierers.

Die Sache mit den Updates

Das Risikomanagement eines Betreibers hat diesem immer schon eine Entscheidung abverlangt, welche Produktversion er installieren soll. Schon der Entschluss, überhaupt ein zertifiziertes Produkt einzusetzen, sollte aus dem Prozess resultieren. Daher sollte die Frage, ob „zertifiziert“ oder „zertifizierte Basis mit Update“, auch weiterhin gemäß Risikomanagement beantwortet werden. Ein Trend in der Produktzertifizierung ist das Einbeziehen von Updatemechanismen und Patchprozessen in die Zertifizierungsaussage. Das hilft dem Betreiber in seinem Risikomanagement bei der Entscheidungsfindung. In den Common Criteria wurde 2021 erstmals für die Firewall genugate 10 das Patchmanagement (neues CC-Modul ALC_PAM) mitzertifiziert.

Bei einer Produktprüfung wird im Regelfall nicht das gesamte Produkt evaluiert, sondern relevante Teile davon. Die Beschreibung der Funktionen führt in Summe zum sogenannten Evaluierungsgegenstand (Target of Evaluation, TOE). Ein Standardrouter vereint zahlreiche Funktionen in sich, zum Beispiel Internetzugang, Firewall, VPN, Medienserver, Telefonie oder Smarthome. In der Abgrenzung zwischen Gesamtprodukt und TOE entscheidet der Hersteller, welche Sicherheitsfunktionen im Rahmen der Evaluierung überprüft werden sollen.

Diese Beschreibung findet sich üblicherweise im Security Target (ST) wieder. Bei einigen Verfahren gibt es jedoch Ausnahmen. So können Mindestfunktionen durch das Zertifizierungsschema vorgegeben sein. Es ist daher auch bei der Bewertung von Zertifizierungen sinnvoll, das jeweilige ST zu lesen. Wenn jemand ein Produkt für VPN-Einwahl sucht und ihm eine Zertifizierung wichtig ist, sollten demnach Geräte aus der Wertung fallen, bei denen das ST die VPN-Funktion nicht berücksichtigt.

Zertifizierung ist nicht gleich Zertifizierung

Für manche Komponenten sind mehrere Zertifizierungsverfahren passend. Je nach Verfahren erreicht man unterschiedliche Vertrauenswürdigkeitsstufen durch Umfang, Blickwinkel und Tiefe der Prüfungen. Innerhalb der Verfahren kann es auch noch Abstufungen geben. Sowohl Hersteller als auch Käufer, die die Vertrauenswürdigkeit eines Produktes anhand von Zertifizierungen einschätzen wollen, sollten also die TOE-Abgrenzung, das Verfahren und die Tiefe des Verfahrens berücksichtigen.

Wenn ein Hersteller beginnt, sich Gedanken zur Drittzertifizierung zu machen, sind die Zertifizierungsstellen und Prüflabore ein sinnvoller Einstieg, um eine erste Einschätzung und Beratung zu Zertifizierungsverfahren und Produktabgrenzungen zu erhalten. Die Standards bewegen sich alle in einer eigenen Sprachwelt, die es zu durchdringen gilt.

Im weiteren Verlauf arbeiten drei Instanzen zusammen: der Hersteller, das Prüflabor und die Zertifizierungsstelle. Die eigentliche Evaluierung erledigen und dokumentieren die Beschäftigten eines Labors. Die Zertifizierungsstelle definiert alle Regeln des Zertifizierungsverfahrens und bewertet, ob die Prüfungen und das Ergebnis den Anforderungen entsprechen. Abschließend bewertet sie das geprüfte Produkt.

Shift Left jetzt

Völlig unabhängig davon, ob eine Marktbeschränkung für ungeprüfte Produkte durch den Gesetzgeber oder den Markt (zum Beispiel durch Einkaufsbedingungen) kommen wird oder nicht: Es lohnt sich immer, in die Produktsicherheit zu investieren.

Sofern ein Produkt bereits existiert oder die ersten Kunden nach Prüfergebnissen fragen, kann ein Produktpenetrationstest stattfinden. Er verursacht beim Hersteller wenig Aufwand und liefert ihm eine Sicherheitsaussage. Je nach Ergebnis und Bedarf kann man den Penetrationstest veredeln, indem man ihn um eine weitere Prüfung im Rahmen einer Beschleunigten Sicherheitszertifizierung ergänzt. Damit lässt sich sogar eine BSI-Zertifizierung erreichen.

Sofern der Druck noch nicht groß ist, genügen viele kleine Schritte, um den Entwicklungsprozess an Standards auszurichten. Sicherheit wird derzeit – wenn überhaupt – häufig erst am Ende eines Projekts berücksichtigt (also rechts im Projektplan). Um Security by Design zu erhalten, gilt es jedoch, diesen Aspekt möglichst früh, also möglichst weit links einzubeziehen: das Shift-Left-Paradigma.

Die Politik der kleinen Schritte dahin ist strategisch nachhaltig, da eine Änderung von Prozessen immer auch einen kulturellen Wandel bedeutet. Dieser braucht Zeit und kann nicht mit dem Holzhammer durchgesetzt werden. Sehr gute Erfahrungen machen dabei viele mit dem schon erwähnten OWASP SAMM. Obwohl aus der „Web-Ecke“ kommend, ist der Standard für nahezu alle Entwicklungsprozesse nutzbar. Eine Gap-Analyse kann den Ist-Stand erfassen und den Weg zu einem noch reiferen, standardorientierten Prozess ebnen.

Für einen Einstieg in den sicheren Entwicklungsprozess empfiehlt sich ein Threat Modelling (Bedrohungsmodellierung). Üblicherweise nehmen an solchen Workshops Architekten und Entwickler teil. Während des Diskussionsprozesses können die Beteiligten sinnvollerweise gleichzeitig mögliche Gegenmaßnahmen erwägen und bewerten.

Tun oder lassen?

Ob und wann eine Zertifizierung für Hersteller sinnvoll ist, ergibt sich aus einer einfachen Analyse: Eine Prüfung kostet immer Zeit und Geld. Zum einen wollen Berater, Zertifizierungsstellen und Labore bezahlt sein, zum anderen sind auch die internen Aufwände je nach Schema zu bedenken. Die Frage für Hersteller lautet immer, ob eine Zertifizierung zu einem Marktvorteil führt oder ob der Markteintritt beziehungsweise Verbleib in regulierten Märkten diese Investition rechtfertigt.

Aus Sicherheitssicht ist eine Zertifizierung immer wünschenswert. Kein Produkt ist am Ende eines solchen Verfahrens schlechter oder unsicherer als vorher. Moderne Zertifizierungsansätze, die Produktupdates und Patchmanagement mitberücksichtigen, sorgen für eine Investitionssicherheit der meist hohen initialen Aufwände für die Erstzertifizierung. In Summe steigt die Qualität eines Produkts daher erheblich. (ur@ix.de)

Sebastian Fritsch

ist Leiter der BSI-Prüfstelle der secuvera GmbH. Er ist seit mehr als 10 Jahren als Evaluator, Auditor und Berater tätig. Er hat bereits verschiedene Common-Criteria-Evaluierungen im Bereich EAL4+ durchgeführt.

Tobias Glemser

ist BSI-zertifizierter Penetrationstester und Geschäftsführer der secuvera GmbH. Seit über 20 Jahren arbeitet er in der Cybersicherheit. Privat ist er unter anderem bei OWASP engagiert.