atsec the information security provider

NEWS 01/13

Common Criteria Schutzprofile – Vision und Realität

Die Entwicklung von Schutzprofilen (Protection Profiles; PPs) ist der zentrale Punkt im „Vision Statement“ des Common Criteria Management Boards vom letzten September. Besonders hervorgehoben wird dabei, dass deren Entwicklung kooperativ erfolgen soll, unter Einbeziehung von Regierungsstellen, Herstellern und Prüfstellen (liebe Anwender, ihr dürft mal wieder nur zuschauen und abnicken). Dies soll laut „Vision Statement“ eine neue Form der Anwendung der Common Criteria (CC) sein.

Ich muss gestehen, dass ich mir bei diesen Äußerungen im „Vision Statement“ ein Schmunzeln nicht verkneifen konnte. Das Konzept der PPs wurde erstmals in den amerikanischen „Federal Criteria“ 1992 vorgestellt. Für die Autoren dieser Kriterien (die in die Entwicklung der CC eingingen) war es selbstverständlich, dass PPs partnerschaftlich unter Einbeziehung von mehreren Herstellern und Anwendergruppen entwickelt werden sollen. Dies ist auch so in die CC übernommen worden, wobei alle Versionen hervorheben, dass ein PP die Anforderungen von **Anwendern** an die Sicherheitsfunktionen einer Produktklasse widerspiegeln sollen. Alle Versionen der CC erklären auch recht klar, dass die Entwicklung von PPs durch eine Gemeinschaft von Anwendern, Regierungsbehörden und Herstellern entwickelt werden sollen. Auf den ersten Blick bleibt damit unklar, warum eine solche, seit mehr als 20 Jahren gefordert Vorgehensweise nun neu als „Vision“ verkauft wird.

Um dies zu verstehen, muss man wissen, dass viele PP-Entwicklungen bisher einzig und allein durch Regierungsstellen veranlasst bzw. durchgeführt wurden – meist in einem stillen Kämmerlein, abgeschottet von der Realität. Eine ernsthafte Diskussion der Kommentare – falls überhaupt eingefordert – fand nie statt. Solche PPs habe ich schon öfter als „Wunschliste an den Weihnachtsmann“ bezeichnet: ein Satz von Sicherheitsfunktionen, der so weder von Anwendern gewünscht noch von Herstellern implementiert wurde. Entsprechend war dann auch die Nutzung: viele dieser PPs wurde nicht ein einziges Mal in einer Evaluation verwendet.

Es gibt aber auch Beispiele von PPs, die eine weite Anwendung gefunden haben. Im Smartcard-Bereich wurden PPs schon immer „collaborative“ von einer „Technical Community“ bestehend aus Herstellern, Anwendern, Regierungsbehörden und Prüfstellen entwickelt. Auch bei den Betriebssystemen ist das unter Federführung des BSI entwickelte „Operating System Protection Profile“ seit seiner Veröffentlichung 2010 in vielen Evaluationen von Betriebssystemen verwendet worden. Auch dieses PP war unter Beteiligung aller relevanten Hersteller entwickelt worden. Generell gilt dies für die meisten unter der Federführung des BSI entwickelten PPs.

Ich stelle also fest: die vom „Common Criteria Management Committee“ (CCMC) und dem „Common Criteria Development Board” (CCDB) dargestellte „Vision“ wurde in vielen Bereichen schon immer so gelebt und hat auch ohne den nun vom CCDB vorgeschlagenen administrativen Aufwand recht gut funktioniert. Anscheinend ist das einigen Personen im CCMC und CCDB bisher noch nicht aufgefallen. Wie hat unser Altkanzler Helmut Schmidt einmal gesagt: *„Wer Visionen hat, sollte einen Arzt aufsuchen.“*

Herzlichst,
Ihr Helmut Kurth

Messen und Konferenzen 2013

Die atsec information security wird in diesem Jahr auf folgenden Messen und Konferenzen vertreten sein:

- **13. Deutscher IT-Sicherheitskongress in Bonn: 14. – 16.05.2013**
  Unter dem Motto „Informationssicherheit stärken – Vertrauen in die Zukunft schaffen“ veranstaltet das Bundesamt für Sicherheit in der Informationstechnik seinen 2-jährlichen Sicherheitskongress. Wir würden uns freuen, Sie an unserem Messestand F8 begrüßen zu dürfen.
- **ICCC in USA (Orlando, FL): 10. – 12.09.2013**
  Die Internationale Common Criteria Konferenz bietet Herstellern, Prüfstellen, Anwendern sowie Behörden und Zertifizierungsstellen eine Diskussionsplattform und Informationen zu aktuellen Entwicklungen der Common Criteria.
- **ICMC in USA (Gaithersburg, MD): 24. – 26.09.2013**
  Die erste „International Cryptographic Module Conference – ICMC“ ist eine Experten-Konferenz für kryptografische Module. Für Details siehe http://www.icmc-2013.org/.
- **it-sa in Nürnberg: 08. – 10.10.2013**
  Auf der größten IT-Sicherheitsmesse im deutschsprachigen Raum wird sich atsec wie im letzten Jahr wieder mit einem eigenen Stand präsentieren.

Passwort-Sicherheit

Mittlerweile haben wir uns daran gewöhnt, dass wir regelmäßig Meldungen von Einbrüchen in große Computersysteme hören. Die typischen Schlagzeilen lauten dann: „Es wurden mehr als X Millionen Account-Daten von der Firma Y geklaut." Letztendlich unterscheiden sich diese Meldungen nur im Firmennamen (Y) und in der Menge der betroffenen Kennungen (X). Solche Schlagzeilen sind extrem geschäftsschädigend für Firmen, die auf diese Weise sehr schnell das Vertrauen ihrer Kunden verlieren. Neben einer kurzen Reaktionszeit und einem transparenten Umgang mit einem derartigen Sicherheitsvorfall spielen auch die Methoden zum Schutz der Passwörter eine erhebliche Rolle. Betrachten wir dazu verschiedene Szenarien:

Szenario 1: Die Passwörter sind im Klartext in einer Datenbank gespeichert. Dies ist unzweifelhaft das Worst-Case-Szenario. Auch weniger IT-affine Benutzer wissen dies aufgrund der Vielzahl von Vorfällen als „Mein Dienstleister/Produktanbieter ist seiner Sorgfaltspflicht nicht nachgekommen" einzuschätzen. Da der typische Anwender häufig trotz gegenteiliger Ratschläge Passwörter oft für mehrere Systeme verwendet, müssen nicht nur alle Accounts der Applikation als gebrochen angesehen werden, sondern auch Accounts der Anwender auf diversen anderen Systemen. Da der Angreifer sämtliche Zugriffsdaten direkt vorliegen hat, kann er damit direkt auf alle Funktionen und Daten zugreifen, die dem Anwender auch zur Verfügung stehen.

Szenario 2: Die Passwörter sind verschlüsselt bzw. als Hash in der Datenbank hinterlegt. Dies ist für einen Angreifer komplexer als Szenario 1, da für die Hashes erst die zugehörigen Passwörter ermittelt werden müssen. Allerdings kann man, je nach Hash-Algorithmus, davon ausgehen, dass ein Angreifer sämtliche Passwörter bis zu 8 Zeichen Länge sowie alle Passwörter beliebiger Länge, die anfällig für einen Wörterbuch-Angriff (bei dem nur häufige Passwörter, wie sie beispielsweise in einem Wörterbuch gelistet sind, geprüft werden) sind, problemlos ermitteln kann.

Szenario 3: Die Passwörter sind als Hash in einer Datenbank hinterlegt, es wird ein sog. „Pepper" verwendet. Beim Pepper handelt es sich um eine zufällig erzeugte Zeichenkette, die an das Passwort eines Nutzers angehängt wird, bevor eine Hashsumme erzeugt wird. Hierbei wird für alle Anwender die selbe Zeichenkette verwendet. Haben zwei Anwender dasselbe Passwort, dann ergeben Szenario 2 und Szenario 3 auch für beide denselben Hash-Wert. Für die Praxis ist ein Pepper relevant, weil es Angriffe erschwert, bei denen vorab der Hashwert sämtlicher möglicher Kombinationen eines Passworts berechnet werden. Der typische Anwendungsfall sind hier die sogenannten Rainbow Tables (vorab generierte Listen von Passwort-Hashes), mit denen man Passwörter ohne Pepper in der Regel innerhalb von Sekunden ermitteln kann. Wenn man zusätzlich zum Passwort noch ein zufälliges Pepper ermitteln muss, dann wird ein Einsatz von Rainbow Tables aufgrund deren Größe und der Dauer, um diese vorab zu erzeugen, erschwert.

Szenario 4: Im Gegensatz zu Szenario 3 kommt anstatt eines Peppers „Salt" zum Einsatz. Salt ist wie Pepper eine zufällige Zeichenfolge, allerdings wird diese pro Account vergeben. Zwei Anwender mit dem selben Passwort hätten also unterschiedliche Hashes (wenn nicht gerade zufällig das Salt identisch ist). Wie Pepper ist Salt eine Maßnahme um Angriffe mit Rainbow Tables zu erschweren.
Je nach Größe des Salts sind damit nur relativ kurze Passwörter in Gefahr, per Brute Force (also durch Ausprobieren aller möglichen Kombination bis zu einer gewissen Passwortlänge) gebrochen zu werden. Klassische Wörterbuch-Angriffe sind nicht mehr mit vorab generierten Rainbow Tables umzusetzen, da das Salt dies verhindert. Das direkte Ermitteln des Passworts mit einem Passwort-Knacker wie z.B. John the Ripper oder hashcat, wird kaum behindert, da das Salt bei einem Einbruch in der Regel direkt mit kopiert wird (da die Applikation das Salt ja selbst braucht, wenn ein Passwort des Anwenders geprüft werden soll). Allerdings dauert ein Angriff gegen sämtliche Anwender-Accounts erheblich länger, da bestehende Passwortlisten pro Anwender geprüft werden müssen, anstatt einfach alle Anwenderkonten gleichzeitig zu prüfen. Der Aufwand zum Ermitteln des Passworts eines einzelnen Accounts bleibt allerdings nahezu derselbe wie in den Szenarios 2 und 3.

Szenario 5: Anstatt einen „einfachen" Hash-Algorithmus wie MD5 oder SHA1 zu verwenden kommt ein spezieller Algorithmus zum Einsatz, der für das Hashing von Passwörtern optimiert ist. Diese Optimierung wird erreicht, indem man das Hashing eines Passworts sehr aufwändig gestaltet. Die „üblichen Verdächtigen" sind hier die Algorithmen bcrypt, PBKDF2 und scrypt. Grundsätzlich wird bei diesen Algorithmen das Passwort mehrfach gehasht, über die Anzahl der Hash-Runden lässt sich der Aufwand steuern. Dies sollte wieder mit einem Salt, wie in Szenario 4 beschrieben, kombiniert werden, um Angriffe mit Rainbow Tables zu verhindern.

Szenario 6: Die ultimative Antwort auf Passwort-Angriffe ist Mehrfaktor-Authentisierung. Klassische Passwort-Authentisierung ist eine sog. 1-Faktor Authentisierung, weil nur ein Faktor (Wissen) zum Einsatz kommt. Bei Mehrfaktor-Authentisierung kommen noch weitere Faktoren hinzu: Besitz oder

biometrische Merkmale. Viele große Dienstanbieter haben dies mittlerweile auch erkannt (meist nach verheerenden Sicherheitsvorfällen); so wurde 2-Faktor Authentisierung beispielsweise bei Google, Facebook und Dropbox eingeführt, Twitter und Evernote planen demnächst eine Einführung. Die Herausforderung für Firmen und Dienstanbieter ist hierbei, ein Modell zu finden, das an das jeweilige Geschäftsmodell angepasst ist. Die internen Mitarbeiter einer Firma alle mit Access Tokens für Remote Access auszustatten ist eine Sache, eine ganz andere ist es, wenn 250.000 User eines Portals, die über die gesamte Welt verstreut sitzen, Zugriff benötigen. Für letzteren Fall skaliert eine Hardware-Lösung meist weder finanziell noch logistisch.

Was bedeuten diese Szenarien nun für die Praxis? Um als Unternehmen seiner Sorgfaltspflicht gerecht zu werden, sollte man mindestens Szenario 5 ins Auge fassen. Dazu gilt es, sich einen passenden Algorithmus auszuwählen, der in der eigenen Umgebung einsetzbar ist. Der Grad des Schutzes durch solch einen Algorithmus hängt im Wesentlichen von der Anzahl der Hash-Zyklen ab, die ausgeführt werden. Wieviele Operationen für die eigene Umgebung machbar sind, lässt sich relativ einfach ermitteln: Basierend auf der maximalen Anzahl von Anwendern, die sich gleichzeitig authentisieren sollen, prüft man, wie lange eine einzelne Authentisierung maximal dauern darf. Danach misst man die Anzahl der Hash-Zyklen, die in dieser Zeit durchlaufen werden können. Dies liefert das maximal machbare Limit an Zyklen, die mit bestehender Hardware umgesetzt werden können. Dies sollte man durch eine Risiko-Analyse ergänzen, die feststellt, ob die Anzahl der Zyklen den eigenen Sicherheitsbedarf abdeckt. Sollte dies nicht der Fall sein, muss man wohl oder übel die Hardware ausbauen oder einen speziellen Crypto-Beschleuniger einsetzen.

Szenario 6 sollte man ins Auge fassen, wenn man das Thema „Passwörter“ langfristig lösen möchte, da Szenario 5 schon allein basierend auf Moore’s Law in jedem Jahr eine Anhebung der Zyklen notwendig macht. Ein Beispiel für eine Softwarelösung ist Google Authenticator, wo man zusätzlich zum Passwort noch entweder eine feste Liste von Einmal-Passwörtern oder ein per App generiertes Passwort zur Authentisierung benötigt. Ein anderer Ansatz ist die Nutzung von mTANs, wobei via SMS eine einmalig nutzbare TAN (Transaktionsnummer) an den Anwender gesendet wird. Ob eine solche Lösung dem eigenen Schutzbedarf entspricht, sollte dann ebenfalls wieder über eine Risikoanalyse ermittelt werden.

Unabhängig von den Szenarien sollte bedacht werden, dass die Güte der Passwörter immer Einfluss auf ihre Angreifbarkeit haben wird. Auch bei Szenario 4 wird die Wirksamkeit des Passwortschutzes entscheidend von der minimal erlaubten Passwort-Länge und den Anforderungen an die Passwort-Komplexität abhängen. Ein simples Passwort, das in einem Wörterbuch zu finden ist, lässt sich auch in Szenario 4 nicht effektiv schützen. Daher sollte man vor der Umsetzung potenziell teurer technischer Maßnahmen immer sicherstellen, dass die Passwortqualität für den eigenen Schutzbedarf angemessen ist.

Datenschutz – Ein Lösch- und Sperrkonzept

Eine der großen Herausforderungen beim Datenschutz ist die Erstellung eines vernünftigen Lösch- und Sperrkonzepts. Das Bundesdatenschutzgesetz (BDSG) macht in § 35 Vorgaben zum Löschen und Sperren von personenbezogenen Daten für nicht-öffentliche Stellen. Personenbezogene Daten müssen grundsätzlich gelöscht oder gesperrt werden, wenn es keine rechtliche Grundlage für deren Speicherung mehr gibt oder wenn der Eigentümer dieser Daten der Speicherung widerspricht.

In der Regel löst man dies so, dass man im Verfahrensverzeichnis eine Aufbewahrungsfrist definiert, nach deren Ablauf diese Daten gelöscht werden. In der Praxis gestaltet sich dies allerdings häufig schwierig. Aussagen der Art „Löschung gemäß den gesetzlichen Vorgaben“, wie sie häufig vorzufinden sind, helfen hier wenig. Die Erfahrung zeigt, dass es sinnvoll ist, ein Lösch- und Sperrkonzept zu erstellen, um sich systematisch mit diesem Thema auseinanderzusetzen.

Voraussetzung für ein Lösch- und Sperrkonzept (LuSK) ist ein vollständiges Verfahrensverzeichnis. Ebenso sollte man bereits im Vorfeld die für das eigene Unternehmen relevanten gesetzlichen Vorgaben für Aufbewahrungsfristen recherchieren. Diese werden idealerweise zu Aufbewahrungsklassen zusammengefasst, die man dann später den Daten pro Verfahren zuordnet.

Anhand des Verfahrensverzeichnisses beginnt man dann, systematisch sämtliche Verfahren und die pro Verfahren verarbeiteten personenbezogenen Daten zu analysieren. Dies läuft etwa wie folgt ab:

- Die jeweiligen Daten werden einer Aufbewahrungsklasse zugeordnet. Damit ist geklärt, wie lange diese Daten aufbewahrt werden müssen. Hierbei gilt es, den Starttermin zu beachten (z. B. „am Ende des Jahres“ vs. „nach Erhebung“).
- In Interviews mit dem Fachbereich werden die Prozesse des Verfahrens besprochen, um zu ermitteln, wie lange der Fachbereich die Daten benötigt und wie die Daten am besten gelöscht werden können.
- In Interviews mit der IT wird geklärt, ob und wie diese Daten gelöscht werden können. Falls eine Löschung nicht möglich ist, muss alternativ eine Sperrung erfolgen.
- Abgeleitet aus den Ergebnissen der Interviews dokumentiert man die Aufbewahrungsfristen, den Lösch-/Sperr-Prozess und die Lösch-Methode. Daraus ergibt sich der Plan für technische und organisatorische Maßnahmen, den es umzusetzen gilt.

Was hier in der Aufzählung einfach aussieht, kann sich in der Praxis als schwierig erweisen. Häufig kommen Anwendungen zum Einsatz, bei denen weder eine Löschung noch eine Sperrung von Daten jemals vorgesehen war. Hier helfen dann nur hartnäckige Verhandlungen mit dem Hersteller oder (worst case) ein Austausch des Systems. Bei eigenentwickelten Applikationen ist es oft nicht besser: Hier hat man zwar die Anpassung in eigener Hand, allerdings kann sich diese bei komplexen Anwendungen mit Upstream- und Downstream-Abhängigkeiten sehr schwierig gestalten. Langfristig hilft in beiden Fällen nur, die Checklisten für den Einkauf von Applikationen bzw. für die Programmierung neuer Anwendungen um entsprechende Prüfpunkte zu ergänzen.

Analog zu den internen Verfahren sollten für ein LuSK auch die ausgelagerten Auftragsdatenverarbeitungen nach §11 BDSG geprüft werden. Das auslagernde Unternehmen ist hier weiterhin die verantwortliche Stelle für die Einhaltung der TOMs (technischen und organisatorischen Maßnahmen), dies umfasst dann auch das Thema „Löschen und Sperren“. Gemäß §11 BDSG sollte es dazu für bestehende Auslagerungen bereits entsprechende Verträge geben, in denen dieses Thema behandelt wird. Im besten Fall ist hier also nichts weiter zu tun. In der Praxis findet man hier allerdings auch häufig noch offene Themen, so dass man die Vorgaben zusammen mit den internen Verfahren nochmals verifizieren sollte.

Eine Erkenntnis aus mehreren durchgeführten Projekten ist, dass die Güte des bestehenden Verfahrensverzeichnisses den Projektaufwand enorm beeinflusst. Wenn die Verfahren bereits hinreichend beschrieben und die verschiedenen Arten personenbezogener Daten schon analysiert und klassifiziert sind, dann lässt sich ein derartiges Projekt relativ einfach durchführen. Probleme treten meistens dann auf, wenn im Projekt laufend neue Verfahren identifiziert werden und die genauen Daten pro Verfahren letztendlich unbekannt sind. In diesem Fall sollte man ein Projekt zur Erstellung eines Lösch- und Sperrkonzepts sinnvollerweise mit der Überarbeitung des bestehenden Verfahrensverzeichnisses koppeln, da für beide Projektteile faktisch dieselben Personen aus IT und Fachbereich benötigt werden.

atsec it security blog

Verfolgen Sie brandaktuell Diskussionen und Erlebnisse unserer Mitarbeiter auf http://atsec-information-security.blogspot.com

IMPRESSUM

atsec information security GmbH
Steinstr. 70
81667 München
Deutschland
Telefon: +49-89-442-49-830
Telefax: +49-89-442-49-831
E-Mail: info@atsec.com

Vertretungsberechtigte Geschäftsführer:
Salvatore la Pietra
Staffan Persson
Registernummer: HRB 129439
Registergericht: Amtsgericht München
UST-ID-Nr. gemäß § 27a UStG: DE205370914
Verantwortlich für den Inhalt:
Staffan Persson (Anschrift s.o.)