

Produktion im Kontext integrierter Sicherheitskonzepte

Allgemein

Weltweit immer mehr Unternehmen stellen Produkte her, bei denen Sicherheit einen wesentlichen Aspekt darstellt. Medizintechnik, die das Überleben nach einem Unfall sichert, Kreditkarten, die sicherstellen, dass wir auch im Urlaub nicht plötzlich ohne Geld auskommen müssen oder Ausweisdokumente, die beweisen, dass wir derjenige sind, der wir zu sein vorgeben.

Aber die Sicherheit beginnt schon weit vor der eigentlichen Benutzung der Produkte. An die Hersteller dieser Produkte werden immer komplexere und anspruchsvollere Anforderungen an die Produktionssicherheit gestellt.

Im Spannungsfeld aus Kundenanforderungen, Kosten-Nutzen-Analysen und Risikoabschätzung bewegen sich die Sicherheitsexperten der Unternehmen und sind letztlich gefordert, praktikable, sichere sowie wirtschaftliche Lösungen zu entwickeln.

Die meisten Organisationen und Unternehmen, die im Umfeld der Produktion von sicherheitsrelevanten Produkten tätig sind, verwenden grundlegend die Kontrolle des Zutritts zum Schutz ihrer Produktionsumgebung. Diese Kontrollen können mittels sehr unterschiedlicher Formen von physischen und logischen Mechanismen (Berechtigungs-Token, Einsatz von PINs und biometrischen Erkennungsverfahren, Kameras, Alarmmelder usw.) umgesetzt werden.

Es wird das Ziel verfolgt, unbefugten Zutritt in zu schützende Bereiche zu verhindern oder zumindest die Folgen für den Betroffenen abzuschwächen.

Im Informationszeitalter hat sich der Fokus mittlerweile von überwachten Ein- und Ausgängen aber immer mehr hin zu integrierten Sicherheitskonzepten verschoben, welche garantieren, dass von Beginn der Wertschöpfung bis hin zum fertigen Produkt das notwendige Maß an Sicherheit vor Zugriff und Manipulation gegeben ist.

Gerade der Baustein der Zutrittskontrolle ist nur im Kontext eines übergeordneten Sicherheitssystems und im Zusammenhang mit anderen Bausteinen wie der Zugriffskontrolle oder der Weitergabekontrolle, geeignet, die Sicherheitsanforderungen der verschiedenen Beteiligten zu erfüllen und auch nur zusammen mit diesen wirklich wirksam.

Vorgehensweisen und Modelle

Erst ein vollständiges Sicherheitssystem führt im Endeffekt zu einer in Qualität und Quantität messbaren Sicherheit und ist letztendlich der Garant für zufriedene Kunden und wirtschaftlich erfolgreiche Produzenten.

Das Sicherheitskonzept, dass bei vergleichbaren Firmen wie ComCard zum Einsatz kommt, erfüllt die vielfältigen Anforderungen, die die Fertigung sicherheitssensibler Produkte wie Smartcards aus dem Identifikations- und Zahlungsverkehrsbereich an die Unternehmen stellt.

Es sollte in engem Zusammenspiel mit den Systemen von Lieferanten, Partnern wie Auftraggeber stehen, und dabei die Aufgabe erfüllen, dass entlang dieser Kette kein Sicherheitsmangel zugelassen wird, der auch nur ansatzweise zu einer Komprimierung einer Kundeninstallation beitragen könnte.

Ohne bei der dafür zum Einsatz kommenden Hard- und Softwareinstallation ins Detail gehen zu können, bedient man sich dabei natürlich aus dem Fundus, den moderne Sicherheitstechnologien heutzutage bieten.

Schematisch folgen wir intern einem Modell, das sowohl in seinem logischen Aufbau wie auch der physischen Umsetzung als Schalenmodell umgesetzt wurde. Das logische Modell folgt dem Prinzip, dass die Konzepte von der äußeren Schale einer unternehmensweiten Sicherheitspolitik bis zum Kern einer produktbezogenen Handlungsanweisung immer spezialisierter werden, dabei aber immer alle darüber liegenden Anforderungen zu erfüllen haben. Das physische Modell folgt der Tatsache, dass z.B. der Zutritt zu den äußeren Bereichen geringeren Restriktionen unterliegt, zum Kern hin die Zutrittsberechtigungen immer mehr eingeschränkt werden. Der Wert der zu schützenden Objekte für das Unternehmen oder einen Angreifer steigt danach immer weiter an, je mehr ein potentieller Eindringling sich dem Kern nähert.

Praxis

Was heißt das in der Praxis? Ein Unternehmen aus der Smartcard-Branche muss ein sicherheitsrelevantes Produkt, sagen wir eine Prozessorchipkarte, im betrieblichen Durchlauf in mehreren Schritten produzieren.

Der Zusammenbau der Karte und elektrische Initialisierungsschritte des Chipmoduls erfolgen zwingend räumlich getrennt von der Personalisierung. Hier befinden sich höchst sensible Bereiche wie Sicherheits-Server für geheime Informationen und Systeme mit Master-Schlüsseln, die für die Kunden, das Unternehmen und damit auch für Unberechtigte beträchtliche Werte darstellen.

Die an der Produktion beteiligten Mitarbeiter besitzen differenzierte Zugangsberechtigungen zu den einzelnen Unternehmensbereichen. Die zur Produktion eingesetzte Software bedarf besonderem Schutz, hier wird mit zur Außenwelt abgegrenzten Netzwerken gearbeitet. Der Zugriff auf sensible Daten geschieht durch Rollen, die die Rechte zum Zugriff auf Ressourcen des betreffenden Auftrags regeln. Dadurch kann genau bestimmt werden, dass z.B. nur ein Qualitätsbeauftragter des Unternehmens Statistiken für ein Reporting an den Auftraggeber abrufen darf, dem Operator in der Produktionsumgebung kann wiederum nur mittels Leserechten aktuell eingestellte Aufträge zur Produktion bringen.

Im Gegensatz dazu sind zum Beispiel Besucher- und Besprechungsräume außen angesiedelt und unterliegen den geringsten Restriktionen.

Nach extern müssen Schnittstellen zu Kunden und Firmen, die z.B. ein externes Datenprozessing durchführen, aufgebaut werden, die den sicheren Datenaustausch gestatten. Hier wird nach dem Zonenprinzip gearbeitet, das durch diverse Vorkehrungen an den Zonenübergängen entsprechend hohe Hürden vorgibt.

Die organisatorischen Maßnahmen sollten sich durch exakte Handlungsanweisungen und einer konkreten Planung jedes Auftrags auszeichnen. Dabei gelten dann die internen Festlegungen des Unternehmens, es sind aber weiterhin IT-Sicherheitskonzepte und Eskalationspläne auftragspezifisch mit dem Kunden festzulegen.

Die Auditierbarkeit im Sinne der Zertifizierung für z.B. Kreditorganisationen spielt beim Aufsetzen des Gesamtsystems für den Dienstleister eine wesentliche Rolle.

Resume

Unternehmen wie ComCard hoffen in diesem Zusammenhang einen wesentlichen Grundstein dafür gelegt zu haben, auch in Zukunft das Vertrauen ihrer Kunden zu genießen, um erfolgreich Produkte für den Bankenbereich sowie Ausweissysteme von Unternehmen anzubieten oder im eTicketing tätig zu sein.

Die Arbeit mit persönlichen Daten von Kunden und Verbrauchern stellt eine stetige Verpflichtung zum verantwortungsvollen Umgang dar und ist damit zu Recht in diesen Tagen mehr denn je im Fokus der Öffentlichkeit.

Die ComCard GmbH wurde 1991 gegründet und konnte seither ihre Marktposition als moderner Anbieter von Smartcard-Systemen kontinuierlich festigen und ausbauen. Die Firma mit Sitz in Falkenstein/ Vogtland fertigt und personalisiert Chipkarten der verschiedenen technischen Ausführungen für die Bereiche Zahlungsverkehr, Gesundheitswesen, Identifikation und Kundenbindung. Der Kundenkreis umfasst weltweit Kreditinstitute, Versicherungen und Handels- und Systemhäuser. Eine günstige Gelegenheit das Unternehmen kennen zu lernen bietet sich vom 03.03. bis 08.03. auf der CeBIT in Hannover in der Halle 11 am Stand A16.