EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Internet of Things und Identity Management

Fachartikel von Mihael Zadro, IAM Consultant, IPG GmbH Deutschland

Braucht das Internet of Things (IoT) ein Identitäts- und Berechtigungsmanagement? Und wenn ja, können die grundlegenden Prinzipien und Prozesse des IAM auf das Internet of Things angewendet werden?

Identitäts- und Berechtigungsmanagement auch für Geräte

Als Experten für das Thema Identitätsverwaltung und Berechtigungsmanagement hat IPG schnell die Idee verfolgt, Geräte des IoT wie Identitäten in einem IDM-System zu verwalten. Es drängt sich auf, den Lebenszyklus eines Mitarbeitenden (repräsentiert durch eine Identität) in einem Unternehmen mit dem Lebenszyklus eines Gerätes zu vergleichen. Es tauchen, rein technisch gesehen, viele Gemeinsamkeiten auf und viele Workflows verlaufen ähnlich.

Doch so einfach ist es bei genauerer Betrachtung nicht. Die reine Verwaltung von Geräten im IoT ist oberflächlich gesehen zwar sehr ähnlich wie die von „normalen Identitäten“ zu verwalten, spätestens aber bei der Verwaltung von Berechtigungen werden die Unterschiede deutlich.

Der Entzug oder das Fehlen einer Berechtigung stellt für den Menschen weniger ein Problem dar, als für ein Gerät im IoT. Ein Mensch stellt fest, dass er beispielsweise nicht mehr auf einen Ordner zugreifen kann. Der Mensch kann die Situation analysieren, vielleicht hilft eine Fehlermeldung die sagt, dass er nicht berechtigt ist, auf diesen Ordner zuzugreifen. Nun kann sich ein Mensch den Zugriff darauf verschaffen, indem er die Berechtigung beantragt oder einen Administrator bittet, ihm diese einzurichten. Ein Gerät kann nur das, wozu es programmiert wurde. Sollte ein nötiger Zugriff entzogen worden sein, wird, je nach Programmierung, das Gerät im schlimmsten Fall in einer Dauerschleife hängen oder gar abstürzen und früher oder später seinen Dienst versagen. Im Besten Fall ist eine Fehlerbehandlung implementiert mit der das Gerät auf den fehlenden Zugriff aufmerksam machen kann, beispielsweise mit einer E-Mail Nachricht an den zuständigen Administrator.

Die Erteilung einer Berechtigung für ein Gerät ist insofern auch etwas anders, da einem Menschen mitgeteilt werden kann, er könne jetzt auf einen Ordner zugreifen. Einer Maschine muss das über die Programmierung mitgeteilt werden. Die Information eines erteilten Zugriffes muss also demjenigen zukommen, der die Programmierung eines Gerätes beeinflussen kann, um die neue Situation zu herbeizuführen.

Diese Tatsache, dass bei der Verwaltung einer Identität einer natürlichen Person Intelligenz vorausgesetzt werden kann und bei der Verwaltung einer Identität eines Gerätes nicht, ist nicht die einzige Besonderheit. Ein weiterer, zwingend zu beachtender Aspekt, ist die Sicherheit.

Wie selektiv handeln Geräte?

Ein Mensch sendet bewusst, wieder nur technisch betrachtet, Informationen nur an ihm bekannte Empfänger weiter. Ein Mitarbeiter würde beispielsweise den Füllstand eines Dieseltanks nur an berechtigte Empfänger weitergeben. Kriminelle Energien oder ähnliches außen vorgelassen. Ein Gerät stellt die definierten Informationen in einem bestimmten Rhythmus zur Verfügung oder versendet diese. Dies in der Regel, ohne

zu prüfen, ob der Empfänger auch berechtigt ist, diese Information zu erhalten. Gleiches gilt für einen Anwesenheits-Sensor: Die Information ob jemand zu Hause ist oder nicht, sollte nur für die Bewohner vorgehalten werden. Kriminelle Energien interessieren sich aber auch für diese Information.

Höhere Sicherheit (wie in unserem Beispiel vereinfacht gesagt eine Prüfung des Empfängers) könnte durch mehr Intelligenz oder eine intelligente Programmierung erreicht werden. Das macht ein Gerät an sich aber teurer, wenn es denn überhaupt möglich ist, einem Gerät mehr Intelligenz zu geben. Smarte Geräte müssen günstig funktionieren.

IDM-Prozesse für Geräte

Die Idee, Geräte als Identitäten zu behandeln, muss zwingend dem Sicherheits-Aspekt gerecht werden. Technisch lässt sich eine Blockade der gesendeten Informationen relativ einfach mit einer Firewall lösen. Der Sicherheits-Aspekt muss aber neben der technischen Sicht auch in allen IDM-Prozessen betrachtet werden. Reicht es bei einem Ausscheiden eines Mitarbeitenden in der Regel alle Accounts zu sperren und die Identitäten zu löschen, muss bei Geräten unter Umständen mehr betrachtet werden. Ein Mitarbeiter hat ohne Accounts wenig Potential Schaden anzurichten. Ein Gerät, das neben seiner eigentlichen Aufgabe, den Diesel-Füllstand zu melden, noch weitere Dinge könnte, wie E-Mails zu versenden, kann mehr Schaden anrichten. Die einfache Deaktivierung der Melde-Funktion reicht nicht aus. Zusätzlich sollte zum Beispiel das Versenden von E-Mails durch das Gerät technisch unterbunden werden oder der Zugang zum eigenen Netzwerk für das Gerät gänzlich abgestellt werden. Es müsste auch analysiert werden, ob Prozesse betroffen sind, und allenfalls angepasst werden müssten.

An sich sind der Kreativität der Programmierungen von Geräten des IoT und auch den möglichen Szenarien, die eine (schlechte) Programmierung als Ursache haben könnten, keine Grenzen gesetzt. Sicher ist, dass mit der Verwaltung von Geräten in einem IDM das Thema Security etwas mehr im Vordergrund steht als die reine „Verwaltung“ der Geräte. Das ist bedingt durch die Hersteller der Geräte, die meist eigene Software-Lösungen zur Verwaltung der Geräte mitliefern. Wenn sich in Ihrem Portfolio allerdings viele Geräte von eventuell verschiedenen Herstellern befinden, die verschiedenen Aufgaben dienen, gewinnt die Idee einer zentralen Verwaltung durch ein IDM-Tool, trotz höherem Aufwand, wieder an Attraktivität.

Dazu tragen auch standardisierte Workflows, beispielsweise der „Eintritt“ eines Gerätes in ein Unternehmen, bei. Warum sollte man nicht auch für Geräte ein standardisiertes Vorgehen entwickeln, wie man es für seine Mitarbeiter tut? Geräte erhalten eine eindeutige Identität, werden erfasst und erhalten eine verantwortliche Stelle. Insbesondere bei einer großen Menge an vielleicht verschiedenen, smarten Geräten würde ein solches Vorgehen den administrativen Aufwand durch Tool-Unterstützung verringern und gleichzeitig die Sicherheit im Unternehmen erhöhen.

Wie unterstützt IPG?

Alles in allem ist die Idee, Geräte des IoT mit einem IDM-System zu verwalten, umsetzbar, setzt aber einen starken Partner voraus, der sich sowohl in der Identitäten- und Zugriffs-Verwaltung bestens auskennt, als auch in der Welt des IoT zurechtfindet. Fehlende Standards müssen durch Erfahrung und Expertise geschaffen werden. Nur so kann für den jeweiligen Einsatzzweck die beste Lösung gefunden und vielleicht eine eigene Definition von IoT formuliert werden.

EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Wie viel IAM braucht Ihr Unternehmen für IoT? Die Berater der IPG Adivsory Services unterstützen Sie als Partner in Fragen zur Verwaltung von Geräten und erarbeiten für Ihre Bedürfnisse maßgeschneiderte Lösungskonzepte.

Kontaktieren Sie uns und erfahren Sie mehr über Geschäftsrollen.

Christian Rückert: Sales Manager Germany and Austria
christian.rueckert@ipg-group.com; Telefon +49 170 908 03 53

Arne Vodegel: Sales Manager Germany
arne.vodegel@ipg-group.com; Telefon +49 170 908 04 32

Marcel Weber: Sales Manager Switzerland
marcel.weber@ipg-group.com; Telefon +41 79 907 84 47