Leipzig, 01.06.2017

Sehr geehrte Damen und Herren,

damit Sie in Ihrem Unternehmen in puncto IT-Sicherheit immer den Überblick bewahren, erhalten Sie heute unser aktuelles **Security eMagazine »complexITy«.** In dieser Ausgabe haben sich unsere Consultants intensiv mit dem Thema Identity & Access Management (IAM) befasst.

Identity & Access Management ist kein konkretes Produkt, sondern ein Lösungsansatz. Durch IAM sind Benutzer effizient und nachvollziehbar verwalt- und authentifizierbar. In diesem Zusammenhang spricht man oftmals von den **vier A's – Administration, Authentifizierung, Autorisierung und Auditing**.

Für die Umsetzung dieses Lösungsansatzes ist der Einsatz unterschiedlicher Softwareprodukte und Technologien – die über definierte Schnittstellen miteinander kommunizieren – notwendig. Wir erläutern Ihnen die Rahmenbedingungen eines IAM und erklären die wichtigsten Begrifflichkeiten. Breaking News aus dem Security-Umfeld und aktuelle Veranstaltungshinweise runden dieses eMagazine ab.

Breaking News

Secure Hash Algorithm: SHA-1

Die Browser **Google Chrome**, **Mozilla Firefox** und **Microsoft Edge** vertrauen seit Anfang 2017 Webseiten nicht mehr, die **SHA-1 Zertifikate** einsetzen. Andere Browser haben schon vorher Webseiten mit diesen Zertifikaten markiert und als nicht mehr vertrauenswürdig eingestuft, also die Nutzer vor dem Besuch dieser Webseiten und Webshops gewarnt.

Haben Sie Ihr Zertifikatsmanagement im Blick und wissen Sie, ob Sie noch **SHA-1** Zertifikate nutzen? Gern beraten wir Sie zu diesem Thema.

Community Draft: Risikomanagement-Standards 200-1, 200-2 und 200-3

Der IT-Grundschutz des BSI wird modernisiert, um sich an die ISO 27001:2013 anzulehnen. Dabei werden die drei Grundschutzwerke 200-1, 200-2 und 200-3 überarbeitet. Sie liegen als Community-Draft zur Einsicht bereit – insbesondere wird sich daraus die Einreichung von Verbesserungsvorschlägen erhofft.

Der Risikoanalyseprozess aus dem BSI-Standard 200-3 wurde grundlegend umgestaltet, sodass dieser mit einem geringeren Aufwand realisierbar ist. Der IT-Grundschutz und der neue BSI-Standard zum Risikomanagement sind wichtige Grundlagen, um Gefährdungspotenziale zu untersuchen, realistisch zu bewerten und mögliche Risiken angemessen zu behandeln.

Hier geht es zum Community-Draft der BSI-Standards. >>

Gesetze und Normen

EU-Datenschutz-Grundverordnung

Am 25. Mai 2018 tritt die EU-Datenschutz-Grundverordnung (EU-DSVGO) in Kraft. Diese führt zu einer Vereinheitlichung des Datenschutzrechtes innerhalb der EU.

Ziel der EU-DSGVO ist es, den Schutz personenbezogener Daten zu stärken. Für Unternehmen und Verbraucher wird die Grundverordnung u. a. folgende Neuerung im Bereich des Datenschutzes mit sich bringen:

- Rechte von Betroffenen werden gestärkt und in manchen Bereichen erweitert.
- Unternehmen, die für die Verarbeitung personenbezogener Daten verantwortlich sind, müssen »geeignete technische und organisatorische Maßnahmen installieren«.

Berücksichtigt werden müssen dabei:

- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Unterschiedliche Eintrittswahrscheinlichkeiten
- Ausmaß der Risiken für die persönlichen Rechte und Freiheiten der Betroffenen
- Datenschutz-Folgeabschätzung

Rahmenbedingungen

Die erfolgreiche Einführung eines Identity & Access Managements (IAM) und der damit verbundene Aufwand sind abhängig von der organisatorischen sowie technischen Ausgangssituation.

Identitäten und Zugänge müssen bekannt sein, um verwaltet werden zu können. Dies bedeutet aus organisatorischer Sicht, dass z. B. für personelle Veränderungen wie Zu- und Abgänge oder das Wechseln einer Abteilung, On- und Offboarding Prozesse definiert sein müssen. Neben personenbezogenen Daten die in den jeweiligen Prozessen erfasst werden, sind weitere Metadaten wie Abteilung, Position und Vorgesetzter ebenso relevant, wie Aufgaben und Verantwortlichkeiten. Zudem sind auch systemspezifische Identitäten nicht zu vernachlässigen.

Wenn ein System über eine Web-Schnittstelle mit einem anderen kommuniziert, verwendet dieses im Regelfall eine Identität die im IAM berücksichtigt werden sollte. Aus den Aufgaben und Verantwortlichkeiten der Identitäten ergeben sich Rollen. Zu den jeweiligen Rollen müssen notwendige räumliche und digitale Zugänge auf Ressourcen, Systeme und Daten bekannt sein. Diese sind wiederum in Vertraulichkeitsstufen (z. B. intern oder extern) zu kategorisieren.

Um diese organisatorischen Herausforderungen meistern zu können, ist eine entsprechende IT-Infrastruktur unumgänglich. Kern einer IAM IT-Infrastruktur ist ein zentraler Verzeichnisdienst. In diesem wird die erforderliche digitale Identität erstellt und verwaltet. Hier ist eine Schnittstelle zum Fachbereich Personalverwaltung von Vorteil, um zu gewährleisten, dass sich personelle Veränderungen direkt auf die digitalen Identitäten der Mitarbeiter übertragen. Damit sichergestellt wird, dass jeder Mitarbeiter der sich an einem System anmeldet, auch der ist, für den er sich ausgibt, muss sich dieser gegen seine persönliche digitale Identität authentifizieren. Methodenabhängig können hierzu weitere technische Geräte wie Kartenleser für eine Zwei-Faktor-Authentifizierung oder eine Public Key Infrastruktur (PKI) erforderlich werden. Ein zusätzliches Self-Service-System kann Zugangsanfragen teil- bis vollautomatisieren und Genehmigungs- und Freigabeprozesse technisch abbilden. Mit einem Provisionierungsdienst können auf Basis der organisatorisch erhobenen Personen-, System-, Meta- und Organisationsdaten (Bspw. Position und Abteilung eines Mitarbeiters) entsprechende Rollen mit personalisierten Zugriffsrechten vollautomatisch zugewiesen und auch entzogen werden.

IAM: Warum und Wie?

Die Verwaltung von Usern, ihrer Zugriffsrechte auf Systeme und Applikationen, und Ihrer Zutrittsberechtigungen in die Räumlichkeiten des Unternehmens, sind ein wichtiger Bestandteil des Sicherheitskonzeptes. Um diesen Prozess auch bei einer hohen Anzahl von Nutzern effektiv umsetzen zu können, hat sich die Nutzung eines Identity & Access Management etabliert. Ein auf die Bedürfnisse des Unternehmens abgestimmtes IAM ermöglicht eine Strukturierung von Nutzern und ihren Berechtigungen, die nicht nur den Verwaltungsaufwand verringert, sondern auch interne und externe Audits vereinfacht. Mit einem IAM kann die Einhaltung der Sicherheitsvorgaben von internen Gremien und dem Gesetzgeber überprüft und gewährleistet werden.

In unserem Blog-Beitrag verraten wir Ihnen, wie Identity & Access Management dies erreicht. >>

IAM: User-managed vs. Risk-based

Klassisches Identity & Access Management folgt einer klaren Struktur, die sich in der Praxis als unflexibel erweisen kann. Sollen einzelnen Nutzern kurzfristig Rechte gewährt werden, die ihnen normalerweise nicht zustehen, wird der wohlstrukturierte Ansatz vor Probleme gestellt.

Um flexibler zu sein, gibt es zwei Ansätze, die das IAM erweitern können:

- Im **User-managed IAM** kann der User bestimmte Berechtigungen selbst beantragen. Diese Anträge werden teilweise automatisiert und damit sehr zügig bearbeitet. Weiterhin kann der User selbst entscheiden, wer Zugriff auf seine Daten und Dateien erhalten kann und wer nicht.
- Das **Risk-based IAM** kalkuliert bei jeder Gewährung von Rechten, die damit verbundenen Risiken. So können Usern Berechtigungen entzogen werden, wenn der Rechner von dem der Zugriff erfolgt, nicht den Sicherheitsrichtlinien der Firma entspricht.

Detaillierte Informationen über die Erweiterungen des IAM erhalten Sie auf unserem Blog. >>

Softline Services

So wie das Identity & Access Management eine immer größer werdende Rolle in modernen IT-Infrastrukturen einnimmt, wird auch der Einsatz einer unternehmensweiten Public Key Infrastructure (PKI) immer bedeutsamer. Es werden Zertifikate für unterschiedliche Anforderungen benötigt bspw. öffentliche Zertifikate für die Kommunikation mit externen Partnern über Webserver (SSL/ TLS), VPN Gateways (IPSec) oder zur Email-Verschlüsselung (S/ MIME Nutzung).

Auch für interne Ressourcen sind vertrauenswürdige Zertifikate zur Absicherung unterschiedlicher Prozesse notwendig. Dazu gehören neben starken passwortunabhängigen Authentifizierungs-möglichkeiten (mittels SmartCards), auch andere zertifikatsbasierte Authentifizierungsmethoden in IT-Infrastrukturen sowie digitale Signaturen oder Maschinenzertifikate für eine Geräteauthentifizierung.

Gern unterstützen wir Sie bei der Entwicklung Ihrer PKI oder Ihres Identity & Access Managements. In unseren **Security@Softline Workshops** stellen wir die Weichen für Ihre IT auf Zukunft. Wir informieren Sie, evaluieren Ihre Ausgangssituation, definieren Lösungen und beraten Sie ganzheitlich zu den Themen IT-Sicherheit, Compliance und Datenschutz.
Informieren Sie sich dazu auf unserer Webseite unter www.softline-solutions.de, kontaktieren Sie uns unter it-sicherheit@softline-group.com oder telefonisch unter +49 341 24051-0

FAQ – Was bedeutet eigentlich…?

Privileged Identity Management (PIM)

Hierbei handelt es sich um privilegierte Benutzerkonten (Administration Accounts), die nicht personalisiert sind.

Identity Management (IDM)

Ist die Verwaltung von Identitäten, Rollen und Berechtigungen von Personen.

Access Management (AM)

Befasst sich mit der Authentisierung (z. B. per Passwort) und der Autorisierung (anhand von Rollen/ Berechtigungen) von Benutzern.

Role Based Access Control

Ist in Rechnernetzen ein Verfahren zur Zugriffssteuerung und -kontrolle auf Dateien oder Dienste. Das Konzept basiert auf Benutzerrollen und soll die Rechte anhand von Arbeitsprozessen abstrahieren. Ein Benutzer kann dabei mehrere Benutzerrollen besitzen.

Segregation of Duties (SoD)

Ist die organisatorische Trennung zwischen Bereichen oder Organisationseinheiten zur Vermeidung von möglichen Interessenskonflikten.

Public Key Infrastructure (PKI)

Eine zentrale Infrastruktur, die neben einer Zertifizierungsstelle (CA) zur Signatur von Zertifikaten auch Validierungsdienste bereitstellt, um den Lebenszyklus von Zertifikaten vollständig abzubilden. (Ausstellung → Prüfung → Rückruf → Ablauf ↻)

Allgemeines zur IT-Sicherheit

Breaking News:

»Computersabotage und Erpressung nehmen deutlich zu. Immer mehr Unternehmen müssen sich mit den Folgen von Angriffen auf ihre IT-Infrastruktur herumschlagen. Zwar hat das Bewusstsein um die Gefahren zugenommen, allerdings auch die Bösartigkeit der Attacken.«

Mehr dazu unter: www.heise.de

Veranstaltungshinweis:

- **KOGIT Compliance Identity Forum**
  26. September 2017, Frankfurt am Main
  http://www.compliance-identity-forum.com/

Falls Sie Fragen oder Hinweise zu gewünschten Magazininhalten haben oder unsere Unterstützung in IT-Sicherheitsprojekten benötigen, dann kontaktieren Sie uns unter it-sicherheit@softline-group.com oder telefonisch unter +49 341 24051-0.

Mit freundlichen Grüßen
Ihr Softline Team

Softline Solutions GmbH // Geschäftsführer: Martin Schaletzky // Sitz der Gesellschaft: Leipzig // Handelsregister Leipzig: HRB 26058 // Steuer Nr.: 232/118/06001 // USt ID: DE270894910