Schutz sensibler Daten im Zuge einer digitalisierten Grundversorgung

Die Auswirkung der Digitalisierung auf KRITIS- und KRITIS-nahe Unternehmen

Die Digitalisierung unserer Gesellschaft und unserer Wirtschaft bietet viele Vorzüge und verschlankt insbesondere im ökonomischen Umfeld zuvor aufwändige Prozesse. Doch wo Licht ist, gibt es bekanntlich auch Schatten und so birgt die Digitalisierung gravierende Einfallstore für Internetkriminalität.

In den letzten 12 Monaten gab es einen erheblichen Anstieg an Cyberattacken. So resultierte aus einem Hackerangriff auf SolarWinds 2020 der Zugriff auf Daten tausender Unternehmen und Behörden. Auch die Gesundheitsbranche rückt seit Beginn der Pandemie zunehmend in den Fokus von Kriminellen. So fiel die Düsseldorfer Universitätsklinik im September 2020 einem Angriff zum Opfer, der der Klink nicht einmal mehr den Notbetrieb erlaubte. Auch die Europäische Arzneimittelagentur EMA ist Ende 2020 Opfer eines Cyberangriffs geworden, bei dem die Hacker vorübergehend Zugriff auf Dokumente zu einem von BioNTech und Pfizer entwickelten Corona-Impfstoff erlangten.

Eine gern genutzte Schwachstelle von Hackern sind die Mitarbeitenden von Unternehmen. Etwa drei Viertel der Datenschutzvorfälle in Unternehmen erfolgen von innen. Zum Schutz der Unternehmensdaten bedarf es daher einer vollumfänglichen Sicherheitslösung. Dazu gehört, dass bereits bei der Zuweisung von Berechtigungen notwendige Beschränkungen und Schutzmaßnahmen integriert werden. Ebenso sind kontinuierliche und vor allem automatisierte Prüfmechanismen erforderlich.

Zur Vermeidung potenzieller Sicherheitslücken hat der Gesetzgeber umfangreiche, regulatorische Anforderungen erstellt. Sie dienen zum Schutz sensibler Daten und dazu, die Grundversorgung im Land aufrechtzuerhalten. Dazu gehören branchenübergreifende Vorgaben wie die EU-DSGVO oder auch branchenspezifische, die gezielt für spezielle Branchen gelten. Hierunter fallen beispielsweise die Ärztliche Schweigepflicht nach § 203 StGB und die Regularien der Drug Enforcement Administration (DEA) & der European Medicines Agency (EMEA) für das Gesundheits-wesen. Zudem stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Security relevante Empfehlungen zur Verfügung.

Unsere Produktsuite SecuIAM ist eine vollumfängliche Identity und Access Management (IAM) Lösung, die Unternehmen dabei unterstützt, sich vor Angriffen von innen und außen zu schützen. IAM-Lösungen ermöglichen eine strukturierte und transparente Verwaltung sämtlicher Identitäten über ihren gesamten Lebenszyklus hinweg. Sie regeln, welche Identitäten wann und wie Zugriff auf IT-Systeme und Daten haben und dass jeder Zugriff authentisiert und nachvollziehbar ist.

Dieses Whitepaper zeigt, wie die unterschiedlichen Branchen mithilfe einer IAM-Lösung einen sicheren Umgang mit sensiblen Daten in Ihre IT-Strategie einbinden, damit Sie sicher aufgestellt sind und gegenüber Wirtschaftsprüfenden und der internen Revision ad hoc auskunftsfähig sind.

Finanzsektor & Versicherungen:
Die Mindestanforderungen an das Risikomanagement (MaRisk) des Kreditwesengesetzes (KWG) und die EU-Datenschutzgrundverordnung (EU-DSGVO) sind regulatorische Anforderungen, die Unternehmen im Banken- und Finanzsektor einhalten müssen. Auch die Versicherungsbranche muss die versicherungsaufsichtlichen Anforderungen an die IT (VAIT), ein Bestandteil der MaRisk der BaFin, erfüllen. Hinzu kommen Regeln zum Umgang mit personenbezogenen Daten durch die EU-DSGVO und Telekommunikationsgesetze.

SecuIAM kann exakt auf die Bedürfnisse dieser beiden Branchen zugeschnitten werden, um die IT zukunftssicher aufzustellen. Die Lösung ermöglicht Unternehmen eine konforme Umsetzung des Prozessmanagements, um eine ausnahmslose Einhaltung des BSI-Gesetzes (Bundesamt für Sicherheit in der Informationstechnik) sicherzustellen. Im Vordergrund stehen hierbei nachvollziehbare User- und Role-Lifecycle, die im Rahmen von Rezertifizierungen regelmäßigen Prüfungen unterzogen werden. Ein vollumfängliches Reporting zu Rollen, Einzelberechtigungen und Zugriffen auf Ressourcen hält die Berechtigungsstruktur der Organisation sowie den Umfang der Rollen nach. Durch die kontrollierte Vergabe von Zugriffsrechten an einzelne Mitarbeitende nach dem Need-to-know-Prinzip wird auf diese Weise die unternehmensweite Durchsetzung von Segregation of Duty (SoD)-Richtlinien gewährleistet.

Gesundheitswesen:
Es gibt kaum sensiblere Daten als Patienten- und Gesundheitsdaten, die in immer größerem Umfang digitalisiert werden. Auch Kliniken und Labore setzen eine Vielzahl an IT-Systemen ein und sind untereinander stark vernetzt. Die Anforderungen an diese Branche sind entsprechend hoch:

- IT-Sicherheitsrichtlinien gemäß §75b SGB V
- IT-Grundschutz des BSI
- Bundesdatenschutzgesetz
- EU-DSGVO
- Ärztlichen Schweigepflicht nach § 203 StGB an das Gesundheitswesen

Eine Risikominimierung hinsichtlich Datenmissbrauch bzw. -diebstahl sowie die Einhaltung der IT-Compliance-Vorschriften können mit SecuIAM erzielt werden. Dabei wirken sich folgende Funktionen der Software unterstützend aus:

- Berechtigungsvergabe ausschließlich nach dem Least Privilege-Prinzip
- Automatische/r Zuweisung bzw. Entzug von Rollen und Berechtigungen im Joiner-, Mover-, Leaver-Prozess von Usern
- Sofortiges (Ent-)Sperren von Usern
- Regelmäßige Reports über User-Aktivitäten, Personalprozesse und den User-Lifecycle
- Rezertifizierung sicherheitskritischer Berechtigungen
- Strikte Einhaltung des Datenschutzes

Automobilindustrie, produzierendes Gewerbe und Handel & Logistik:
Datendiebstahl, Industriespionage, Sabotage. Das sind einige der Gefahren, denen sich die Automobilindustrie, das produzierende Gewerbe und Handel & Logistik ausgesetzt sehen. Die Lieferketten in diesen Branchen werden immer komplexer und internationaler. Die Zahl der Zulieferer und Partnerunternehmen steigt stetig.

SecuIAM schafft mehr Sicherheit bei der erforderlichen Zusammenarbeit zwischen der Produktion, ihren Schnittstellen und diversen unterschiedlichen IT-Systemen (z. B. bei der Zollabwicklung) und bietet relevante Funktionen für mehr Sicherheit in der Berechtigungsverwaltung.

Diese sind unter anderem:

- Automatisierte Zuweisung von Businessrollen und Berechtigungen im Onboarding-Prozess neuer Mitarbeitender
- Integriertes Regelwerk für automatische Beantragung und Verteilung von Rollen
- Automatische Vergabe und Entzug von Berechtigungen sowie direktes Sperren und Entsperren von Usern in Joiner-, Mover-, Leaver-Prozessen, um das unbemerkte Fortbestehen verwaister Accounts zu verhindern und das Risiko eines unerlaubten Zugriffs von internen bzw. externen Stellen zu senken
- Detaillierte sowie automatisch terminierte Reports zu diversen User-Aktivitäten, Personalprozessen, User-Lifecycle
- Sofortiges (Ent-)Sperren von Usern
- Reporting und Rezertifizierung zur regelmäßigen Prüfung sowie Bestätigung sicherheitskritischer Berechtigungen inklusive Berechtigungsanpassung, wenn notwendig
- Zentrale Verwaltung aller User und ihrer Berechtigungen entlang der gesamten Supply Chain
- Aufwandsreduktion durch die manuelle Vergabe von Zugriffsrechten (Administration sowie individuelle Abstimmung mit diversen Schnittstellen entfallen)

Chemie- & Pharmaindustrie:
Die Chemie- und Pharmaindustrie verarbeitet Werkstoffe, für die sehr hohe regulatorische Anforderungen gelten:

- Die Vorschriften der Food and Drug Administration (FDA), die Regulatorien der Drug Enforcement Administration (DEA) und der European Medicines Agency (EMA)
- Compliance Anforderungen aus 21 CFR Part 11, HIPAA, SOX, GMP, GLP und ISO Standard
- Einhaltung von SoD- Richtlinien (Segregation of Duties)

Ein Angriff oder eine Manipulation hätten fatale Folgen. Mit SecuIAM kann das Security-Level von Unternehmen in diesen Branchen erhöht werden. Der Einsatz der Lösung garantiert einen nachvollziehbaren Lifecycle von Usern und Rollen, die Rezertifizierung sicherheitskritischer Berechtigungen (u. a. zur Wahrung der HIPAA-Vorgaben) und vollumfängliche, automatisierte Reports über die gesamte Berechtigungsstruktur der Organisation. Zudem werden die SoD-Richtlinien in den Prozessen zur Vergabe von Berechtigungen berücksichtigt und die Zugriffe erfolgen ausschließlich nach dem Need-to-know-Prinzip.

Schutz sensibler Daten im Zuge einer digitalisierten Grundversorgung

Öffentliche Auftraggeber:
Komplexe Strukturen, viele Altsysteme, die verbindliche Umsetzung von IT-Projekten nach dem V-Modell XT sowie eine sehr hohe Zahl an jährlichen Zu- und Abgängen: Das sind einige der Herausforderungen, mit denen sich Unternehmen im Öffentlichen Dienst und Bildungsreinrichtungen konfrontiert sehen. Hinzu kommt das Onlinezugangsgesetz, welches verlangt, dass Verwaltungsleistungen bis 2022 auch in digitaler Form angeboten werden.

Für die Einhaltung der IT-Compliance-Vorschriften und die Minimierung der Risiken für Betrug und Datenmissbrauch sorgt SecuIAM. Durch das Least-Privilege-Prinzip und die automatisierte Berechtigungsvergabe wird die Sicherheit erhöht und der Zugang zu digitalen Verwaltungssystemen beschleunigt. Das Self-Service-Portal bietet Mitarbeitenden zudem die Möglichkeit, Anträge für Berechtigungen oder Ressourcen zu stellen. Diese Anträge werden anhand vordefinierter Berechtigungs- und Rollenkonzepte, die die Mitarbeitenden im Joiner-Mover-Leaver-Prozess erhalten haben, bewilligt oder abgelehnt. Durch das vollumfängliche Reporting dieser Berechtigungsverwaltung ist jederzeit nachvollziehbar, wer über welche Berechtigungen verfügt.

Sicherheit mit vielen Facetten

Es wird deutlich, dass die verschiedenen Branchen teilweise den gleichen Vorgaben unterliegen, es zum Teil jedoch auch mit branchenspezifischen Herausforderungen zu tun haben.

Die in Deutschland entwickelte und qualitätsgesicherte IAM-Software SecuIAM hilft Ihnen dabei, den Zugriff auf Unternehmensdaten unter Berücksichtigung branchenspezifischer, regulatorischer Anforderungen umzusetzen.

Mit SecuIAM und unserer langjährigen Erfahrung im Bereich Identity & Access Management sowie Governance, Risk & Compliance unterstützen wir Sie beim Aufbau oder der Optimierung Ihrer IT-Security-Strategie.

Zu unserem Leistungsumfang gehören die folgenden Bestandteile:

- Analyse
- Beratung
- Konzeption & Design
- Implementierung einer IAM-Lösung
- Hosting der benötigten Infrastruktur in der OEDIV private Cloud
- Betrieb und Support

Sprechen Sie uns an:

KOGIT GmbH
Rheinstraße 40 - 42
D-64283 Darmstadt
Tel.: +49 6151 7869-0
E-Mail: sales@kogit.de
Web: www.kogit.de

OEDIV SecuSys GmbH
Brückenweg 5
D-18146 Rostock
Tel.: +49 381 37573-0
E-Mail: info@secusys.de
Web: www.secusys.de