TOOLS4EVER

Whitepaper V1.0 / 25.08.2022

ISO 27001

und die Rolle des Identity Management

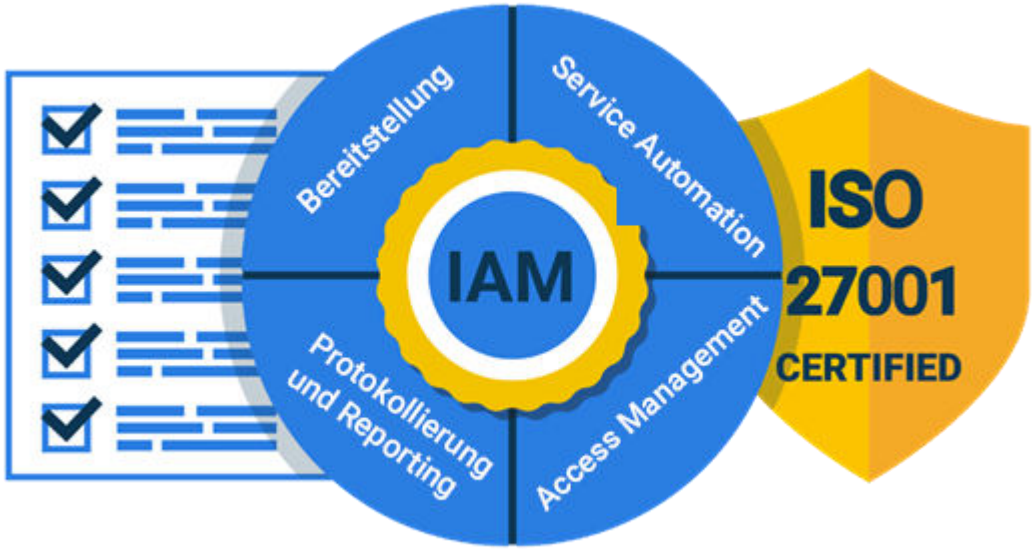
Inhalt

Einführung

Die ISO 27001 ist die maßgebliche internationale Norm für das Informationssicherheitsmanagement. Mit einem in der Norm beschriebenen Informationssicherheits-Managementsystem (ISMS) können Organisationen ihre Informationssysteme auf strukturierte, effektive und effiziente Weise absichern. Die ISO 27001 findet breite Anwendung und stellt auch die Grundlage branchenspezifischer Sicherheitsnormen dar, wie z. B. – in den Niederlanden – der „Baseline Informatiebeveiliging Overheid“ (BIO) oder der NEN 7510 (im Pflegebereich).

Die ISO 27001 nützt Organisationen auf zweierlei Weise. Zunächst stellt die Norm konkrete Richtlinien für die Einrichtung und das Management der Informationssicherheit in einer Organisation bereit. Darüber hinaus gilt eine Zertifizierung nach ISO 27001 als anerkannter Qualitätsnachweis. Damit weisen Sie gegenüber Kunden und Partnern nach, dass Ihre Organisation über ein vollständiges Informationssicherheitssystem verfügt und alle geltenden Vorschriften erfüllt. Für viele Kooperationsvereinbarungen und Verträge ist ein ISO-27001-Zertifikat daher ein „notwendiges Ankreuzfeld“.

In diesem Whitepaper wird zunächst eine Übersicht über die Norm ISO 27001 gegeben. Anschließend wird aufgezeigt, wie das Identity Management dazu beitragen kann, die ISO-27001-Konformität in einer Organisation umzusetzen.



Übersicht ISO 27001

Die ISO 27001 beschreibt keine technischen Einzelheiten zu Sicherheitsmethoden wie z. B. Multifaktor-Authentifizierung oder Verschlüsselung. Die Norm zielt auf Informationssicherheits-Managementsysteme ab und soll dabei helfen, Strukturen und Prozesse einzurichten, die die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sicherstellen. Die ISO 27001 schließt an die sogenannte ISO High Level Structure (HLS) an. Dabei handelt es sich um eine Grundstruktur für Managementsysteme mit allgemeinen Richtlinien für Bereiche wie Führung, Risikomanagement und Prozessmanagement. Spezifische Normen wie z. B. ISO 9001 (Qualität), ISO 14001 (Umwelt) und ISO 27001 (Informationssicherheit) lassen sich wie modulare Bausteine in einem Gesamtsystem zusammensetzen, sodass Sie als Organisation ein einziges, zusammenhängendes Managementsystem realisieren können.

Die ISO 27001 besteht aus 10 Kapiteln und einem Anhang. Die inhaltlichen Anforderungen werden in den Kapiteln 4 bis 11 beschrieben und im Folgenden zusammengefasst. In Anhang A der ISO 27001 finden sich konkrete Organisationsziele und -maßnahmen, mit denen sich, soweit für Ihre Organisation relevant, ein Informationssicherheitssystem konkret einrichten lässt. Mehr zu diesem Anhang finden Sie in einem späteren Kapitel des vorliegenden Whitepapers.

Kapitel 4-5: Kontext der Organisation

Eine wichtige Forderung in der ISO 27001 ist, dass die Informationssicherheit auf ausreichend „hohem Niveau“ in der Organisation angesiedelt ist. Es reicht nicht aus, ein einfaches „Schutzkonzept“ durch die IT-Abteilung aufstellen und verwalten zu lassen. Die Informationssicherheit muss in den Geschäftszielen und dem Geschäftsbetrieb verankert sein und auf der Agenda der obersten Führungsebene stehen. Diese Anforderungen werden in den ersten beiden Kapiteln der Norm (4 und 5) beschrieben.

H5. Führung	Die Führung ist ein wichtiger Aspekt. Nicht ohne Grund werden bei ISO-Audits auch Führungskräfte befragt, denn für die Informationssicherheit muss das Senior Management zuständig sein – nicht ein „zahnloser“ Qualitätsbeauftragter in einem Nebengebäude. Zudem müssen die einzelnen Rollen und Zuständigkeiten für die Informationssicherheit klar und deutlich definiert sein.
H4. Kontext der Organisation	Hier erfolgt eine Bestandsaufnahme des Organisationskontextes für die Informationssicherheit. Bei einem Universitätskrankenhaus gibt es offensichtlich ganz andere Sicherheitsanforderungen als bei einem Autohändler. Deshalb ist es wichtig, zu ermitteln, was die Ziele der Organisation sind, wer interne und externe Betroffene sind, welche Gesetze und Vorschriften zu beachten sind, und so weiter. So wird der Rahmen für den späteren Informationssicherheitsplan festgelegt.

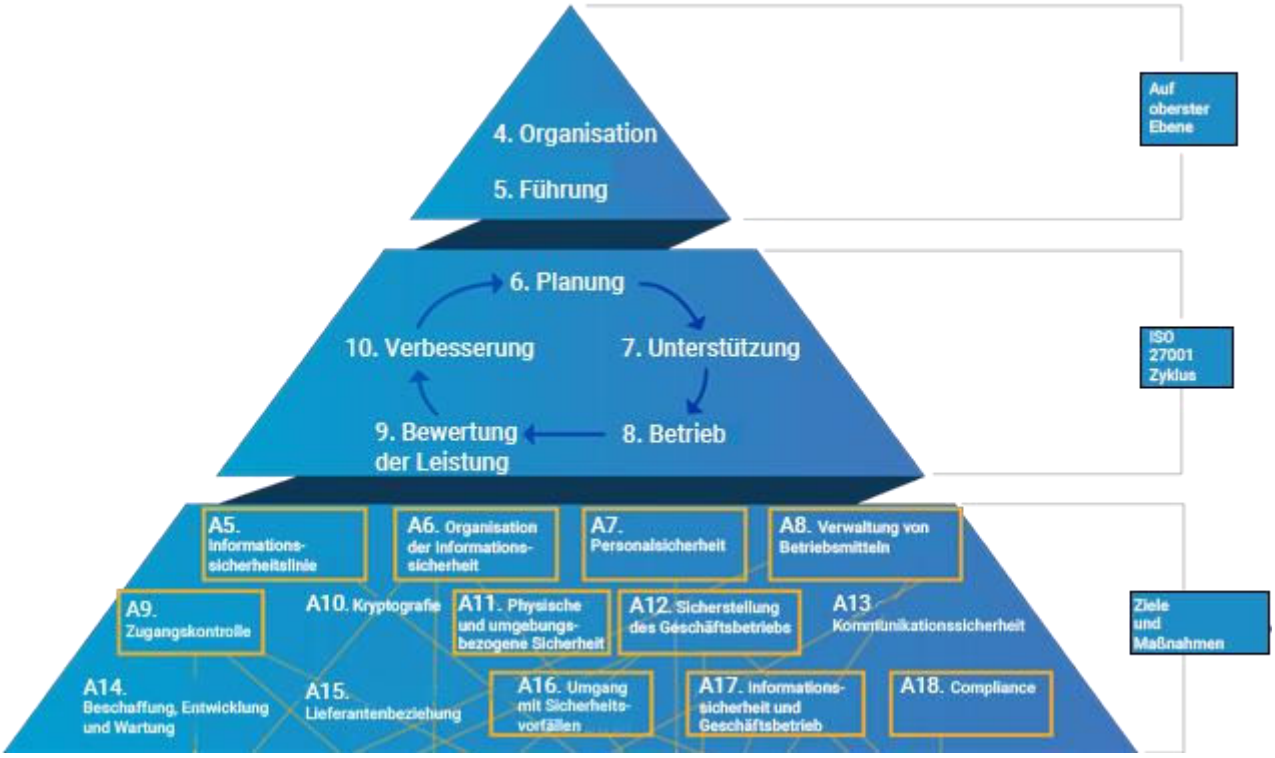
Kapitel 6-10: ISO-27001-„Zyklus“

Mit den Kapiteln 4 und 5 der Norm wird sichergestellt, dass der organisatorische Rahmen klar definiert und das Senior Management in ausreichendem Umfang eingebunden ist. In den Kapiteln 6–10 folgen Anforderungen an die Organisation, Planung, Einrichtung und kontinuierliche Anpassung des Informationssicherheitssystems.

H7. Unterstützung	Die Organisation muss selbstverständlich in der Lage sein, die Planung umzusetzen. Dazu sind entsprechende Fähigkeiten, Systeme und ein „Sicherheitsbewusstsein“ erforderlich. Daneben ist eine ausreichende und angemessene interne Kommunikation und Dokumentation wichtig.
H8. Betrieb	Zur Umsetzung der Sicherheitsprozesse werden Maßnahmen benötigt, die zur Beherrschung der Sicherheitsrisiken geeignet sind. Während der Ausführung der Planung müssen die Ergebnisse fortlaufend überwacht und die Risikoanalysen regelmäßig angepasst werden.
H9. Bewertung der Leistung	Die Ergebnisse der Sicherheitsmaßnahem müssen strukturell evaluiert werden. Dies geschieht mittels interner Audits und einer regelmäßigen sogenannten Managementbewertung, die durch die Geschäftsführung erstellt und besprochen wird.
H10. Verbesserung	Zuletzt muss neben der Behebung von Mängeln, die sich in der Bewertung der Leistung gezeigt haben, auch gewährleistet sein,
H6. Planung	Grundlage der Planung ist eine umfassende Analyse der Risiken, die für diese Organisation zutreffend sind. Für jedes Risiko werden die Wahrscheinlichkeit des Eintretens und die potentiellen Auswirkungen bestimmt. Darauf aufbauend werden Maßnahmen entwickelt, die zur Beherrschung der Risiken geeignet sind. Es werden konkrete Sicherheitsziele formuliert und wie diese realisierbar sind.

Anhang A: Organisationsziele und -maßnahmen

Damit eine Organisation eine ISO-27001-Zertifizierung erhalten kann, müssen alle Vorgaben aus den Kapiteln der ISO 27001 erfüllt sein, abhängig von dem Typ der Organisation und den Zielsetzungen. In Anhang A der ISO 27001 werden 114 verschiedene Organisationsziele und -maßnahmen in 14 Kategorien aufgeführt. Dies kann als Katalog verstanden werden, aus dem jede Organisation Maßnahmen auswählen muss, die zu ihrer Struktur und ihren Risiken passen. In der Norm ISO 27002 werden die einzelnen Maßnahmen detaillierter dargestellt. Es folgt eine kurze Übersicht über die Kategorien mitsamt Zielen und Maßnahmen aus Anhang A.

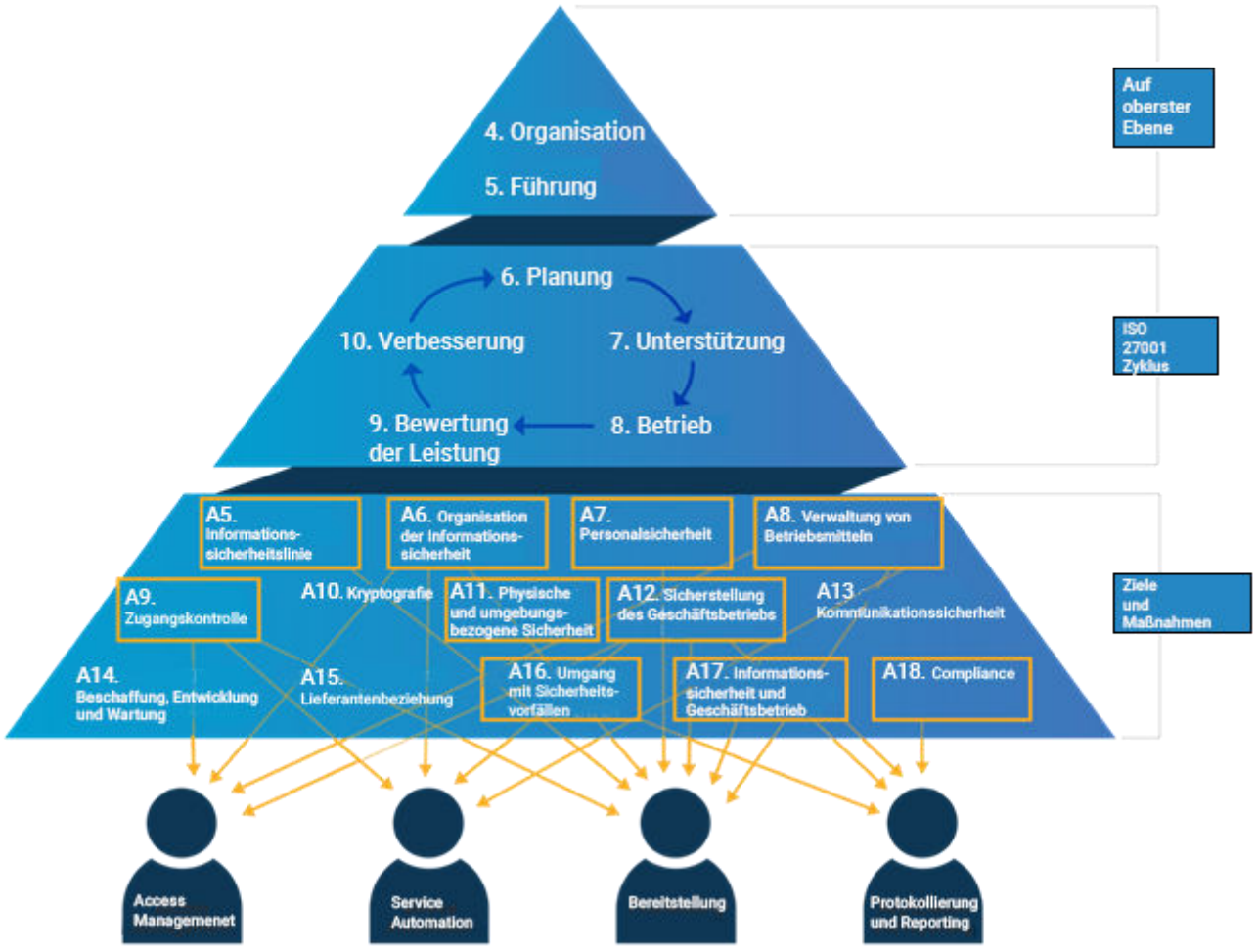


A5. Informationssicherheits-leitlinie	Zur Ergänzung der allgemeinen Organisationsrichtlinien muss eine spezifische Informationssicherheitsleitlinie erstellt und regelmäßig evaluiert werden.
A6. Organisation der Informationssicherheit	Es reicht nicht aus, eine Informationssicherheitsleitlinie zu entwickeln, sondern diese muss auch umgesetzt und gepflegt werden. Welche Rollen mit welchen Zuständigkeiten und Befugnissen sind erforderlich? Die gegenseitige Abgrenzung der Rollen ist dabei von großer Bedeutung, und auch das Online-Arbeiten und die Nutzung (eigener) mobiler Endgeräte sollten heutzutage ausreichend berücksichtigt werden.
A7. Personalsicherheit	Selbstverständlich müssen Mitarbeiter hinreichend ausgebildet und sich der Bedeutung der Informationssicherheit bewusst sein. Dies betrifft die gesamte Anstellungszeit, von der korrekten Anwerbung von Mitarbeitern bis hin zu den erforderlichen Sicherheitsmaßnahmen bei einem Austritt aus der Organisation.

A8. Verwaltung von Betriebsmitteln	Betriebsmittel zur Informationsverarbeitung wie z. B. Software und Computersysteme müssen ordnungsgemäß registriert und gepflegt werden. Wer darf Systeme nutzen? Werden Betriebsmittel und Nutzungsrechte nach Beendigung der Tätigkeiten wieder zurückgegeben? Sämtliche Informationen müssen klassifiziert und sicher gespeichert werden.
A9. Zugangskontrolle	Es sind Maßnahmen erforderlich, um sicherzustellen, dass Mitarbeiter ausschließlich auf die Netzwerke, Systeme und Daten Zugriff erhalten, die sie für ihre eigenen Tätigkeiten benötigen.
A10. Kryptografie	Daten müssen in ausreichendem Maße verschlüsselt werden, um ihre Vertraulichkeit und Integrität zu gewährleisten.
A11. Physische und umgebungsbezogene Sicherheit	Organisationen müssen verhindern, dass Unbefugte Zugang zu Computern und Datenträgern am Standort der Organisation erlangen können. Dazu zählt auch die Sicherstellung der Informationssicherheit im Falle von Stromausfällen oder Unglücken. Außerdem müssen auf Geräten vorhandene Daten vor der Entsorgung der Geräte ordnungsgemäß gelöscht werden.
A12. Sicherstellung des Geschäftsbetriebs	Es müssen klare Vereinbarungen und Vorgehensweisen eingerichtet sein, die sicherstellen, dass Informationssysteme auf sichere Weise verwendet werden können und vor Malware geschützt sind. Darüber hinaus sind angemessene Backup- und Monitoring-Maßnahmen erforderlich.
A13. Kommunikations-sicherheit	Die gesamte interne Netzwerkinfrastruktur und die externe Netzwerkkommunikation müssen gegen unberechtigten Zugriff und Missbrauch abgesichert sein.
A14. Beschaffung, Entwicklung und Wartung von Informationssystemen	Organisationen müssen bei der Beschaffung, Entwicklung und Wartung von IT-Systemen stets auf die Sicherheit der Systeme und der Daten achten. Dies schließt neben betrieblich genutzten Systemen auch Entwicklungs-, Demo- und Testsysteme usw. ein.
A15. Lieferanten-beziehungen	Organisationen sind von Lieferanten ihrer IT-Systeme abhängig. Dies gilt für On-Premise-Systeme und -Software ebenso wie für solche, die cloudbasiert sind. Es sind klare Vereinbarungen zur Gewährleistung der Informationssicherheit mit diesen Lieferanten erforderlich.
A16. Umgang mit Sicherheitsvorfällen	Trotz aller Sicherheitsvorkehrungen kann es zu Vorfällen kommen. In diesem Fall müssen angemessene Vorgehensweisen mit klaren Zuständigkeiten bestehen, welche auch Vereinbarungen bezüglich weiterer Dokumentation und Lösung des Vorfalls umfassen.
A17. Informations-sicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs	Für mögliche Vorfälle im Zusammenhang mit der IT-Ausrüstung muss insbesondere darauf geachtet werden, dass eine Fortführung des Geschäftsbetriebs jederzeit gewährleistet bleibt.
A18. Einhaltung von Vorgaben (Compliance)	Organisationen müssen jederzeit nachweisen können, dass sie alle maßgeblichen Gesetze und Vorschriften einhalten.

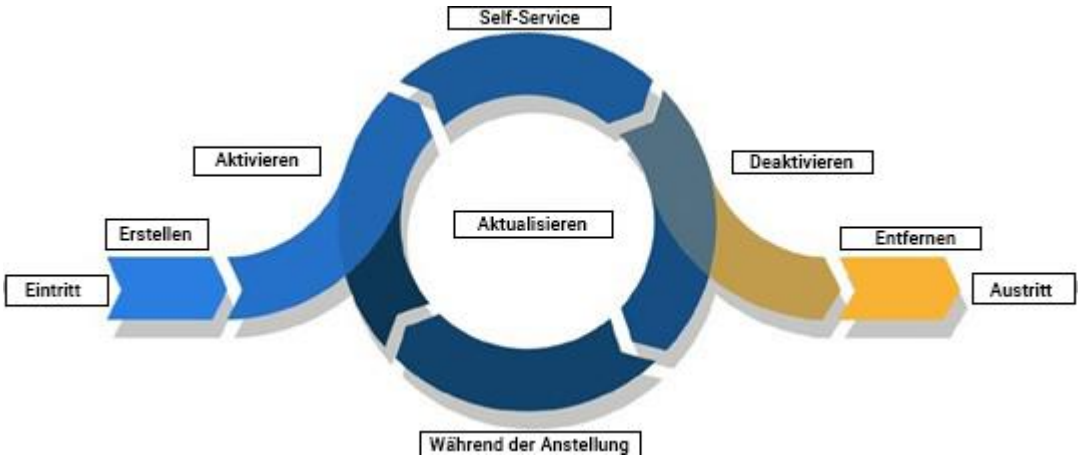
Identity Management und ISO 27001

Wie beschrieben, werden in Anhang A der ISO 27001 einige Maßnahmen detaillierter vorgestellt, mit denen eine Organisation ihre Informationen ausreichend absichern kann. Benutzerverwaltung und Berechtigungsmanagement werden dabei immer wichtiger. Für den Zugriff auf Daten durch Mitarbeiter, Partner und Kunden sollte grundsätzlich das „Need-To-Know-Prinzip“ (Kenntnis nur wenn nötig) gelten. Außerdem müssen sämtliche IT-Aktivitäten bis auf Benutzerebene nachvollziehbar bleiben. Dadurch wird das Identity Management zu einem mächtigen und wichtigen Werkzeug für die Umsetzung einer ISO-27001-konformen Informationssicherheit. In diesem Kapitel werden wir sehen, wie sich die Anforderungen aus den Kategorien und Maßnahmen aus Anhang A der Norm mithilfe einer modernen Identity-Management-Lösung erfüllen lassen. Zur Illustration dient HelloID, unsere eigene cloudbasierte Identity-&-Access-Management-Plattform.



Bereitstellung von Benutzerkonten und -rechten

Gruppenkonten sind in der ISO 27001 nicht vorgesehen, ebenso wenig wie das Prinzip „vorhandenen Benutzer kopieren“ für neue Mitarbeiter. Stattdessen müssen Zugriffsrechte eindeutig mit einem individuellen Benutzerkonto verknüpft sein. Es muss zu jedem Zeitpunkt ersichtlich sein, wer Zugriff auf Daten und Anwendungen hat und wer bestimmte Tätigkeiten ausführt. Und selbstverständlich müssen die Benutzerkonto-Informationen und die Zugriffsrechte jederzeit auf aktuellem Stand sein, d. h. der aktuellen Rolle und Position des Anwenders in der Organisation entsprechen. Dafür ist ein professionelles, automatisiertes Benutzerkonto-Management von zentraler Bedeutung.



In HelloID werden diese Anforderungen mit einem automatisierten User Provisioning sichergestellt. Damit sind die digitale Identität und die Zugriffsrechte jederzeit auf demselben Stand wie die Angaben im Personalsystem. Durch die direkte Verknüpfung zwischen HR- und HelloID-System erhalten neue Mitarbeiter sofort ein Benutzerkonto, das alle zur Rolle gehörigen Eigenschaften und Zugriffsrechte hat. Und auch während der Anstellung bleibt alles auf aktuellem Stand. Sobald sich eine Rolle ändert, werden die Zugriffsrechte durch HelloID sofort angepasst. Und wenn ein Mitarbeiter die Organisation verlässt, sperrt HelloID das Benutzerkonto und alle Zugriffsrechte automatisch. Die Anhäufung von Berechtigungen oder versehentlich bestehen bleibende Zugangsrechte gehören so der Vergangenheit an.

Service Automation: Standardisierung mit Spielraum für Ausnahmen

Ein gutes Informationssicherheitssystem basiert auf klaren Richtlinien, eindeutigen Prozessen und erlaubt nur wenig individuelle, unkontrollierte Anpassungen. Dementsprechend sind die Identity-Management-Prozesse in HelloID so weit wie möglich standardisiert und automatisiert. Zugleich müssen Konzepte wie die rollenbasierte Zugriffskontrolle unterstützt werden und Prozesse implementierbar sein, mit denen sich Rollen eindeutig voneinander abgrenzen lassen. Trotzdem werden Ausnahmen immer notwendig sein, und jede Organisation muss einen für sie passenden Ausgleich zwischen Benutzerfreundlichkeit und betrieblicher Sicherheit finden. Falls automatisch zu viele Rechte erteilt werden, entstehen unerwünschte Sicherheitsrisiken. Andererseits beeinträchtigt es die Arbeit, wenn Mitarbeiter regelmäßig unnötig lange auf ihre Zugangsberechtigungen warten müssen.

HelloID bietet die gewünschte Kombination aus Standardisierung und Ausnahmen:

- Mittels der „Attribute Based Access Control“ (attributbasierte Zugriffskontrolle, ABAC) werden Standardrechte in HelloID zugewiesen. Die jeweilige Organisationsstruktur mit Rollen und zugehörigen Aufgaben wird in HelloID zu Geschäftsregeln, die automatisch und dynamisch bestimmen, welche Zugriffsrechte ein Mitarbeiter hat – vom automatisierten Onboarding neuer Mitarbeiter bis zum Ausscheiden aus der Organisation.

- Auch wenn die meisten Rechte komplett automatisiert vergeben werden, sind doch fast immer Anpassungen an der Standard-Rollenmatrix nötig. Daher bietet HelloID Spielraum für Ausnahmen. Für spezifischere Rechte, die sich nur schwer automatisch vergeben lassen, lassen sich Self-Service-Prozesse einrichten. Damit können Anwender selbstständig Zugang

zu Anwendungen oder Dateifreigaben beantragen, wobei die erforderlichen Freigabeschritte automatisch eingeleitet werden. Nach erfolgter Freigabe geschieht die Aktivierung ebenfalls auf automatisierte Weise, sodass gefährliche Ausnahmen oder Fehler vermieden werden.

Dank automatisierter Konfigurationsregeln bleibt der Katalog der Dienstleistungen immer aktuell. Neue Freigaben werden beispielsweise direkt im Katalog angezeigt. Im System ist jederzeit ersichtlich, welche Mitarbeiter aktiv sind und welche Lizenzen, Anwendungen oder Freigaben sie nutzen.

Zugangsmanagement

Ein modernes Zugangsmanagement stellt sicher, dass Mitarbeiter – und ggf. auch Partner und Kunden – auf einfache und einheitliche Weise Zugang zu Anwendungen und Daten erhalten. Wie oben erläutert, ist die Grundlage, dass jeder Anwender ein eigenes, persönliches Benutzerkonto hat. Das Konzept des Single Sign-On (SSO) ermöglicht, dass sich jeder Anwender nur einmal anmelden muss. Mit dieser Kombination aus benutzerfreundlichen und zugleich sicheren Lösungen für die Zugangskontrolle werden unsichere Behelfslösungen vermieden.

HelloID unterstützt alle gängigen Single Sign On-Protokolle, mit denen Benutzer bei den unterschiedlichen Anwendungen authentifiziert werden. Für Anwendungen ohne integrierte SSO-Funktionalität bietet HelloID außerdem weitere Zugangsmethoden. Zur primären Authentifizierung kann HelloID nicht nur mit Active Directory integriert werden, sondern auch mit anderen Identity Provider wie Azure, Google, Salesforce, SAML oder OpenID. Die Plattform unterstützt außerdem zusätzliche Sicherheitsoptionen, wie z. B. die Zwei-Faktor-Authentifizierung (2FA). HelloID erkennt kontextuale Faktoren wie den Standort und den Zeitpunkt der Anmeldung, um abhängig davon eine zusätzliche Authentifizierung vom Anwender zu verlangen. Als zweiten Faktor bietet HelloID neben Hard- und Software-Token auch die Optionen SMS oder Einmalpasswort (OTP).

HelloID stellt Identity & Access Management aus der Cloud bereit. Dies senkt die Investitionskosten und beschleunigt die Installation und Konfiguration, während sich Tools4ever um die technische Einrichtung kümmert, einschließlich automatischer Updates. Die Lösung läuft in einer vollständig abgesicherten Microsoft Azure- und Google-Cloud-Umgebung, die außerdem alle sechs Monate umfassend von Deloitte Risk Services überprüft wird. Die gesamte Lösung erfüllt dadurch die strengsten Sicherheitsanforderungen. Dank eingebauter Redundanz ist eine sehr hohe Verfügbarkeit gewährleistet.

Reporting

Für die ISO-27001-Konformität sind Protokollierung und Reporting von grundlegender Bedeutung. Organisationen müssen nachweisen können, dass ihre Prozesse den maßgeblichen Gesetzen und Vorschriften entsprechen. Kommt es zu einem Sicherheitsvorfall, z. B. einem Datenleck, muss nachvollziehbar sein, welche Nutzer welche Tätigkeiten im Netzwerk ausgeführt haben.

Als cloudbasierte Lösung muss HelloID immer strengere gesetzliche Vorschriften in Bezug auf Audits und Sicherheitsmechanismen erfüllen. Jeder Zugriffsversuch, jeder automatisierte und jeder manuelle Vorgang und die gesamte Nutzung unserer Plattform werden aufgezeichnet und verfügbar gemacht. Dank automatischem Monitoring der Authentifizierungsprozesse und umfangreicher Berichte und Auswertungen ist immer eindeutig nachvollziehbar,
wer welche Anwendungen von wo aus und zu welcher Zeit genutzt hat. Neben einer ausführlichen Übersicht über jeden Anmeldevorgang lassen sich so z. B. auch die IP-Adressen verdächtiger Anmeldeversuche identifizieren. Potentielle Gefahren können rechtzeitig erkannt und behandelt werden.

Ein besonderes Merkmal von HelloID ist die Auditfähigkeit des gesamten Identity Lifecycle pro System wie auch pro Benutzer. Alle ausgeführten Aktionen werden protokolliert, wie z. B. das Erstellen, Aktivieren, Aktualisieren, Verschieben, Deaktivieren und Löschen von Benutzerkonten, ebenso wie das Erteilen und Entziehen von Zugriffsrechten. Beim spontanen Vergeben von Rechten (außerhalb der regulären Rollenmatrix) wird in HelloID ebenfalls detailliert angezeigt, wer die Anfrage gestellt und wer sie bestätigt hat, und welche Änderungen in jedem System durchgeführt wurden. So werden alle HelloID-Prozesse vollständig transparent, auditfähig und anpassbar.

Weitere Informationen

Das Identity Management ist heute in der IT-Sicherheit von zentraler Bedeutung. Mitarbeiter, Partner und Kunden erhalten nur noch mit eigenen Benutzerkonten Zugriff auf Daten und Anwendungen. Zugriffsrechte werden ausschließlich nach dem „Need-To-Know-Prinzip“ (Kenntnis nur wenn nötig) vergeben. Des Weiteren müssen alle IT-Aktivitäten bis auf die Benutzerebene herunter nachverfolgbar sein. Diese Merkmale machen Ihre Identity-Management-Plattform zu einem wichtigen Werkzeug für den Aufbau eines ISO-27001-konformen Informationssicherheitssystems.

Wollen Sie mehr darüber erfahren, wie das Identity Management dazu beitragen kann, die ISO-27001-Konformität Ihrer Organisation zu realisieren? Und wie Sie Ihre IT-Umgebung absichern, ohne die Benutzerfreundlichkeit zu beeinträchtigen? Gerne erzählen wir Ihnen mehr, zum Beispiel anhand unserer Checkliste ISO 27001 – HelloID. Mit dieser Liste gehen wir sämtliche Maßnahmen aus Anhang A der ISO 27001 durch und erläutern, ob – und falls ja, auf welche Weise – diese mittels HelloID Identity Management umsetzbar sind.

TOOLS4EVER

Adresse	Hauptstr. 145-147 51465 Bergisch Gladbach Deutschland
Telefon	+49 2202 2859290
Website	Tools4ever.de
E-Mail	info@tools4ever.de
Vertrieb	sales@tools4ever.de
Support	tools4ever.de/support