accenture

WEBCAST

AUTONOMOUS IDENTITY

Automatisierung als Turbo für Ihr Berechtigungsmanagement

MODERATION: DR. OLIVER JANZEN
Freier Journalist für COMPUTERWOCHE

DENNIS HAAKE
Lead Solution Architect, Forgerock

LARS ZYWIETZ
Managing Director, Accenture

LIDIYA KYURKCHIEV
Digital Identity Expert, Accenture

[00:02] OLIVER
Hallo und Herzlich Willkommen zu unserem heutigen COMPUTERWOCHE Webcast in Zusammenarbeit mit Accenture und Forgerock. Unser Thema heute: **Autonomos Identity – „Automatisierung als Turbo für ihr Berechtigungsmanagement“.** Wir sprechen heute über einen neuen Ansatz im Identitäts- und Berechtigungsmanagement: ein komplexes und oft unterschätztes Gebiet. Wir sprechen darüber, wie Machine Learning helfen kann, die Aufgaben zu automatisieren und damit Kosten und Risiken zu senken und gleichzeitig Transparenz und Compliance zu steigern. Hierzu haben wir heute drei Experten in der Konferenz, die ich jetzt gern begrüßen möchte. Zuerst begrüße ich Lidiya von Accenture: Hallo Lidiya!

[00:45] LIDIYA
Hallo Oliver! Einen schönen guten Tag!

[00:48] OLIVER
Einen wunderschönen Tag! Lidiya, du bist IT Security Manager bei Accenture. Was hast du uns heute mitgebracht? Gib unseren Teilnehmer doch mal kurzen Ausblick.

[00:57] LIDIYA
Also ich habe heute ganz aktuelle und praxisnahe Erfahrungen mit dem Einsatz von Auto ID mitgebracht. Aber auch gute Laune, weil das ein Vorsatz bei uns im Haus ist!

[01:09] OLIVER
Wunderbar! Das freut mich. Die habe ich auch! Dann begrüße ich zunächst mit guter Laune den Dennis Haake von Forgerock: Hallo Dennis. Was machst du heute hier?

[01:20] DENNIS
Hallo Oliver. Vielen Dank für die Einladung! Und ich habe heute einen technischen Einblick in die wachsende Bedeutung von künstlicher Intelligenz und Machine Learning. Für Prozessoptimierungen, Automatisierung, aber auch Risikominimierung im Berechtigungsmanagement.

[01:38] OLIVER
Okay, das klingt spannend. Last but not least begrüße ich Lars Zywietz, Hallo! Lars, du bist Managing Director für das Thema Security bei Accenture. Warum ist das Thema, was wir heute hier besprechen wichtig?

[01:57] LARS
Ich denke der Titel dieser Veranstaltung, der sagt es eigentlich schon sehr sehr gut. Es geht darum, unseren Identity und Access Management Programmen einen Turbo zu verpassen. Und genau dieser Turbo wird benötigt, um die Anforderungen, die das Business an uns richtet, zu meistern. Und darüber freuen wir uns heute, gemeinsam sprechen zu können.

[02:20] OLIVER
Perfekt! Super, dank dir! Wir machen auch gleich mit dir weiter. Aber bevor wir weitermachen: Liebe Teilnehmer, wir sind live wir sind/beziehungsweise wir haben die Gelegenheit interaktiv zu sein. Und diese Interaktivität möchten wir auch gerne ausleben.

Von daher: Sie haben in der Oberfläche die Möglichkeit Fragen zu stellen. Gehen sie davon aus, in den nächsten 43 Minuten gehören diese Experten Ihnen. Sie haben den Zugriff. Der Zugriff läuft über mich. Das heißt Sie stellen die Fragen. Ich, als der Moderator, stelle sicher, dass wir die Fragen alle bis zum Ende beantwortet haben. Die einzige Bitte, die ich in dem Zuge habe, ist: a) stellen Sie Fragen und b) stellen Sie nicht alle ganz am Ende, weil ansonsten laufen wir dann aus der Zeit. Ich kann Ihre Anliegen immer wieder mit in die Diskussion mit einfließen lassen und das mache ich auch gerne. Umgekehrt haben wir auch Fragen an Sie vorbereitet und da steigen wir auch gleich mit ein.

Und zwar haben wir eine Umfrage. Bevor wir in das Thema einsteigen und Ihren Blick auf die Dinge beeinflussen, haben wir jetzt die Frage an Sie: **Was sind denn aktuell ihre größten Herausforderungen im Bereich Identitäts- und Berechtigungsmanagement?** Sie haben mehrere Antwortmöglichkeiten: Zählt zu den wichtigsten oder größten Herausforderungen:
A) die Transparenz über die Zuweisungen von Berechtigungen
B) die Bereitstellung von Zugängen (zum Beispiel für neue Mitarbeiter)
C) die Regelkonformität oder
D) der Aufwand im Betrieb

Wir sind gespannt auf Ihre Antworten. Wir lassen es jetzt eine kleine Minute laufen.

Lidiya, was würdest du erwarten, was die größte Herausforderung ist, die wir gleich genannt bekommen?

[04:12] LIDIYA
Sehr gute Frage, Oliver. Also ich würde erwarten, dass die Transparenz im Unternehmen, in Bezug auf die Berechtigungslandschaft, eine große Herausforderung für viele Unternehmen ist.

[04:31] OLIVER
Okay prima, dann sind wir gespannt! Das läuft hier noch. Es sind auch alle schon ganz fleißig. Lars, deine Folien kommen in ungefähr 30 Se-kunden auf den Schirm. Vielleicht möchtest du beginnen, schon mal einzusteigen. Auch kurz noch zwei, drei Sätze zu dir selbst und deiner Rolle.

[04:51] LARS
Sehr gerne, Oliver! Zunächst noch mal einen guten Tag und vor allem Moin Moin aus dem hohen Norden – um genauer zu sein aus Hamburg. Herzlichen Dank an alle Teilnehmer für ihre Zeit und natürlich für ihr Interesse an unserer heutigen Veranstaltung.

Mein Name ist Lars Zywietz. Ich bin als Managing Director bei Accenture Security verantwortlich für unser sogenanntes Applied Security Services Team, zu dem auch unsere Digital Identity Practice gehört.

Und wir als Accenture beschäftigen uns seit vielen, vielen Jahren mit Fragestellungen genau rund um dieses Thema und unterstützen unsere Kunden bei der Umsetzung ihrer Identity Management Programmen. Das kann in manchen Fällen eher konzeptionell oder strategisch geprägt sein – oft aber übernehmen wir hier die Gesamtverantwortung. Das beinhaltet dann auch die entsprechenden Implementierungsaufgaben. Hier arbeiten wir dann sehr sehr eng und vor allem sehr sehr gerne mit unserem Technologiepartner Forgerock zusammen. Wir können feststellen, dass das Thema Digital Identity oder Identity und Access Management sich ja momentan unglaublicher Beliebtheit erfreut. Das Thema ist derzeit so aktuell und en vogue, wie eigentlich noch nie zuvor. Diejenigen hier unter uns, die in diesem Bereich schon ein wenig länger tätig sind, die wissen natürlich, dass das nicht immer so war und vor allem auch wie stark sich die Anforderungen an das Managen von digitalen Identitäten verändert haben.

Ich weiß noch so vor 10–15 Jahren: da war das eher so eine langweilige und gut versteckte Infrastrukturkomponente. Und jetzt hat sich das aber in den letzten Jahren doch zu einem absolut kritischen Service entwickelt, der es den Unternehmen letztlich erlaubt, sicher ihre digitalen Transformationen voranzubringen. Deswegen haben wir vor zwei, drei Jahren sehr intensiv eine Bestandsaufnahme gemacht gemeinsam mit unseren Kunden. Und sind dabei auf eine Reihe von doch recht wichtigen Herausforderungen beziehungsweise Anforderungen gestoßen.

Was sind die treibenden Kräfte? Die treibenden Kräfte sind vor allem die disruptiven Geschäftsmodelle und die digitalen Services, die bekanntlich die Unternehmensagenda beherrschen. Genau das wirkt sich natürlich auch auf die Art und Weise der tatsächlichen Arbeitserbringung aus. Die kurzen Produkt- und Releasezyklen erfordern, dass Teams sich in den Unternehmen ad hoc formieren und dann aber auch genauso schnell wieder auseinander gehen. In solch einem agilen Umfeld kann ein Rollenkonzept, so wie wir es kennen, kaum noch Schritt halten.

Die Konsequenz, die wir sehen, ist häufig eine sogenannte Überprovisionierung. Da Benutzern oft ganze Rollen zugewiesen werden, obwohl sie vielleicht nur mal schnell eine einzelne Berechtigung benötigen.

Um das vermeiden, sehen wir im Umkehrschluss sehr oft, dass eine Rollenexplosion stattfindet. Nämlich als Versuch, die Rollen eben etwas schlanker zu schneiden. Beides so in der Form sicherlich nicht optimal.

Wir stellen aber auch fest, das wir immer noch nicht wirklich gut genug verstehen, warum ein Benutzer seine Berechtigung hat oder beziehungsweise eine Benutzerin ihre Berechtigungen hat. Nachlässigkeit bei Nova und Lieferprozessen, beispielsweise führt dazu, dass Berechtigungen angehäuft und eben nicht zeitgerecht entzogen werden. Wer von den Teilnehmern aber wiederum unternehmensweite Zertifizierungskampagnen durchführt, der weiß ganz sicher ein Lied davon zu singen, wie beliebt dieser innerhalb der Organisation sind und vor allem wie viel Aufwand hier investiert wird, für doch am Ende recht zweifelhafte Ergebnisse.

So aus unserer Sicht sagen wir, dass die Zuweisung von Berechtigungen (wenn man es denn treffsicher und automatisiert hinbekämen) wirklich ein großer Schritt nach vorne wäre, statt unsere Benutzer eben in überfüllten Katalogen nach häufig kryptischen Berechtigungen suchen zu lassen. Und dann langwierige und oft fehlerbehaftete Approval-workflows zu initiieren. Wir sagen, das es genau so wünschenswert wäre, auf einen Blick erkennen zu können, welches denn unsere risikobehafteten Berechtigungen und auch Benutzer sind. Und genau bei diesen Ausreißern dann ganz direkt und unmittelbar eingreifen zu können.

Mit dieser festen Überzeugung, dass die konventionellen Ansätze und Produkte auf diese beschriebenen Herausforderung nur unzureichend Lösungen anbieten können, haben Accenture und Forgerock sich entschlossen, in unserem Innovation Center in Dublin (das wir übrigens liebevoll „the Dock" nennen) eine neuartige Lösungen zu entwickeln.

Und das wirklich Spannende an diesem Prozess war, dass wir unter Anderem auch zwei Kunden mit dabei hatten, um die sogenannten „Pain points" eben aus verschiedenen Blickwinkeln aufnehmen zu können. Z.B.: aus Sicht der Benutzer; aus Sicht der Vorgesetzten; aus Sicht der Administratoren; der Applikationsverantwortlichen, aber eben auch aus der Sicht des CISOs. Auf unserer Seite wiederum hatten wir ein fachübergreifendes Team, das aber eben nicht komplett nur aus der Identity-Ecke kam, damit wir hier von vorn herein nicht wieder betriebsblind sind. Sondern wir hatten eine hohe Anzahl von Data Scientists mit an Bord. Im Peak waren es bis zu 25 Personen, die ihren Fokus von Beginn an auf der Analyse der Daten und der entsprechenden Algorithmen hatten.

Als Ergebnis kam am Ende Autonomous Identity zum Vorschein. Aus unserer Sicht eine radikal neue Lösung, die eben mit Hilfe von Machine Learning automatisiert ein Risk Scoring der Benutzer unter zugewiesenen Berechtigungen durchführt. Genau damit lässt sich die Identity Governance neu gestalten und weitestgehend automatisieren. Was letztlich dazu führt, dass Kosten und Risiken sinken, während Transparenz und Übersicht steigen.

So, und jetzt hoffe ich, dass sich Ihre Neugier etwas wecken konnte und Sie sich jetzt darauf freuen, Autonomous Identity noch etwas besser kennenzulernen. Dennis Hake von Forgerock wird jetzt im weiteren Verlauf diesen Teil sehr sehr gerne übernehmen.

[11:28] OLIVER
Super, Danke Lars! Bevor der Dennis weitermacht, würde ich gerne auf der einen Seite auflösen, was denn die größten Herausforderungen unserer Teilnehmer im Bereich Identitäts- und Berechtigungsmanagement sind und dann auch gleich die zweite Frage anschließen. Und zwar als Ergebnis haben wir: größte Herausforderungen ja, Lidiya, Self-Fullfilling Prophecy als ist die Transparenz, wie du auch getippt hattest. Aber vielleicht war es dann auch der Hinweis, den du gegeben hast – werden wir nicht rausfinden. Mit 69 Prozent – zweiter Platz – der Aufwand im Betrieb mit 57 Prozent. Ich glaube das sind beides Themen, die ihr ganz klar mit eurer Lösung adressiert. Aber auch die anderen beiden Punkte: jeweils ungefähr ein Drittel der Teilnehmer haben gesagt, das es auch eine der größten Herausforderungen ist, die Bereitstellung von Zugängen und die Regelkonformität.

Damit wären wir auch schon bei der nächsten Frage an Sie. Und zwar die Frage ist: **Wie viele Zuweisungen von Berechtigungen managen Sie in Ihrem Unternehmen?** Und wir werden es, während sie die Antwortmöglichkeit haben, noch mal kurz diskutieren und näher erläutern: Sind es weniger als eine Million? Sind es zwischen einer Million und 3 Millionen? Oder mehr als drei Millionen Zuweisungen von Berechtigungen?

Lars, Lidiya – vielleicht sagt ihr noch mal kurz, was genau meinen wir mit Zuweisung von Berechtigungen. Wir haben viel miteinander gesprochen und ihr habt was von einem Kunden von euch erzählt, bei dem es knapp fünf Millionen waren oder so. Wie genau zählt man da?

[13:19] LARS
Also genau. Es gibt ja in einer Applikation beispielsweise ein Berechtigungsobjekt und dieses Berechtigungsobjekt kann jetzt mehrfach in Rollen beispielsweise auftauchen. Kann aber auch natürlich mehreren Benutzern zugewiesen werden. Also über diese tatsächliche Zuweisung von Benutzer zu Berechtigungsobjekt sprechen wir. Und eben nicht nur um die einzelnen Berechtigungsobjekte. Es geht nicht um diese Zahl, sondern es geht um die Zuweisungen.

[13:45] OLIVER
Ok, verstanden. Ja, die Umfrage läuft. Da pendelt sich auch was ein. Lassen wir es noch einen Moment laufen, während der Dennis schon mal einsteigt. Dennis, du hast uns vorhin einen Ausblick gegeben, dass du tief in die Technik guckst. Wir sind jetzt gespannt.

[14:17] DENNIS
Hallo noch mal an alle zusammen. Mein Name ist Dennis Haake und ich bin Solution Architect bei Forgerock und ich habe sehr langjährigen Machine Learning Background aus verschiedenen Branchen. Ich habe in der Pharma gearbeitet, in der Robotic und jetzt auch im Identity und Access Management – speziell im Governance Bereich. Und ich möchte einfach mal so ein bisschen in das technische konzeptionelle Konzept von Autonomous Identity, oder kurz „Auto ID", eingehen.

Zuerst „Machine Learning für Identity Governance": Aber was ist Auto Identity überhaupt von der technischen Seite? Wir sehen Auto ID als quasi den Turbo für das Berechtigungsmanagement. Und wenn wir uns mal die traditionellen Governance-Anwendungen anschauen: was die traditionelle Governance-Anwendungen tun normalerweise. Sie sind ein bisschen der mechanistische Apparat, quasi „Wie gebe ich jemanden Zugriff zu einem bestimmten System". Zum Beispiel: ein User kann kommen und er sagt: ich möchte gerne Zugriff zu System X und ein Entscheider kann dann den Zugriff gewährleisten in einem Approval Flow. Es ist nur so, dass diese Anwendungen nicht beschreiben, warum jemand Zugriff zu einem System haben soll.

Genau deswegen haben wir auch Autonomous Identity. Autonomous Identity ist eine datengetriebene und sehr skalierbare Machine Learning Anwendung, die es ermöglicht, die Millionen von Zugriffsmuster, die in einem Unternehmen existieren, zu finden. Wenn ich Zugriffsmuster sage, was ich meine ist: die Kombination von Profilattributen der User, welche im Zusammenhang mit einer Berechtigung am häufigsten auftreten. Also quasi den Root Cause of Access für eine bestimmte Berechtigung. Auto ID ermöglicht die Modellierung der Zugriffsdatenlandschaft eines Unternehmens. Und dieses Modell kann dann benutzt werden für Prozessautomatisierung, aber auch Ausreißererkennung für Risikominimierung. Die Frage ist jetzt, was macht Autonomous Identity anders als andere, traditionellere Methoden?

Das Erste ist, wir haben einen umfassenden globalen Ansatz. Das heißt: die gesamte Datenlandschaft des Unternehmens wird berücksichtigt. Um das ein bisschen im Kontrast zu traditionellen Verfahren zu erklären: nehmen wir zum Beispiel mal das traditionelle Peer-group analysis was mehr Clustering ist. Was dort passiert, ist, dass zu einem gegebenen Zeitpunkt immer nur ein Teil/eine Submenge der Daten benutzt wird. Um ein spezielles Beispiel zu geben: wir haben einen Vorgesetzten und derjenige hat 20 Mitarbeiter. Dann wird zum Beispiel diese Untermenge – diese 20 Personen + der Vorgesetzte – als „Peer-Group" bezeichnet. Und die Datenanalyse passiert nur basierend auf dieser Datenmenge hier. Das Problem dahinter ist, dass viele potenzielle Zugriffsmuster eben fehlen, dadurch, dass man nicht alle Daten mit einbezieht. Autonomous Identity im Gegensatz findet alle diese Muster. Einfach weil wir die komplette Datenlandschaft mit einbeziehen. Das bedeutet, dass wir quasi ein bisschen weg von dieser eingeschränkten, traditionellen Sichtweise wollen und ein bisschen mehr global, und auch diese Agilität in Unternehmen heutzutage einfach mit einbeziehen wollen.

Der zweite Punkt ist, dass Autonomous Identity hoch skalierbar ist. Das heißt, dass die Millionen von Zugriffen, die in einem Unternehmen existieren, können simultan und auch automatisiert – und das ist besonders wichtig – automatisiert modelliert werden. Was natürlich irgendwo dann ressourcenschonend ist, weil die manuellen Prozesse, die notwendig sind, minimiert werden.

Der dritte Punkt ist, dass das System datengetrieben ist. Was bedeutet, dass keine menschliche Beeinflussung, also kein Bias in die Analyse mit einschließt. Das bedeutet, dass Machine Learning Modell, was erstellt wird, reflektiert die Zugriffsdatenlandschaft des Unternehmens, wie sie ist. Die meisten anderen Methoden – unglücklicherweise – haben als Voraussetzung irgendwo diese Beeinflussung. Zum Beispiel die Definition dieser Peer-Groups, die ich gerade gesagt habe. In unserem Fall Autonomous Identity braucht es nicht. Es ist komplett datengetrieben ohne äußeren Bias.

Und dann um noch mal auf Transparenz, wie Lidiya das vorhin schon mal zum Teil angerissen hat, zurückzukommen: Transparenz oder Erklärbarkeit ist natürlich eine ganz wesentliche Komponente in Analyseverfahren. Das Problem ist

viele Machine Learning Algorithmen haben natürlich so ein bisschen dieses Problem, dass sie wie eine Blackbox arbeiten. Was natürlich irgendwo Risiko bedeutet. Gerade wenn man auf sensitiven Daten arbeitet, wie das bei Governance der Fall ist. Und hier kommt Autonomous Identity ins Spiel: Die Algorithmen, die benutzt werden sind klassifiziert als erklärbare, künstliche Intelligenz oder Machine Learning. Das bedeutet, dass der Entscheider, der mithilfe der Analyseergebnisse letztendlich Entscheidungen fällt, kann den Datenanalyseprozess genau nachvollziehen. Das heißt der Prozess, wie das System oder bzw. das Tool quasi zu den Ergebnissen kommt, ist komplett nachvollziehbar. Und der Entscheider mit seinem Domainwissen kann dann letzten Endes nachvollziehen, warum das Ergebnis Sinn macht oder halt nicht.

Der fünfte Punkt ist die ist dynamische Analyse. Wenn man sich überlegt, das Zugriffsmuster in Unternehmen ändert sich heutzutage beinahe täglich. Die meisten Unternehmen agieren global. Dinge ändern sich ständig. Und das Problem, wie Lars gerade schon gesagt hat, ist, dass traditionell zum Beispiel Zertifizierungskampagnen. Diese Dinge laufen normalerweise projektweise und können sehr lange dauern. Teilweise bis drei oder sechs Monate. Das Problem ist, dass die Ergebnisse dieser Projekte dann teilweise auf veralteten Daten basieren, weil eben die Datenlandschaft sich schon verändert hat und dann Dinge implementiert werden im Unternehmen, basierend auf veralteten Daten.

Autonomous Identity ermöglicht es, Updates in Echtzeit zu haben. Das heißt, wir können quasi zum Beispiel das Modell wöchentlich neu trainieren und dadurch dann eine beinahe Echtzeitanalyse haben. Wie funktioniert das Ganze jetzt? Um das Ganze mal ein bisschen konzeptioneller zu machen: wie ich schon gesagt habe, wir beziehen uns auf die komplette Zugriffsdatenlandschaft des Unternehmens. Das heißt, wir schauen uns wirklich alle Berechtigungen im Unternehmen an, die vorhanden sind, und auf der anderen Seite natürlich beziehen wir alle Mitarbeiter eines Unternehmens ein. Und wenn wir jetzt Großunternehmen haben – das können mehrere Hunderttausend sein – simultan in derselben Analyse mit ein.

Was wir machen, ist – anders als bei den traditionellen Rollen oder Rolemining ansetzen – ist, dass wir uns die Berechtigung selbst anschauen. Das heißt, wir gehen auch die Berechtigungsebene und schauen uns jede einzelne Berechtigung jedes Mitarbeiters an. Wie funktioniert das Ganze? Das Ganze funktioniert so, dass wir quasi alle User im Unternehmen finden, die Zugang zu einer bestimmten Berechtigung haben. Wir nehmen Zugang zu einem CRM Systemen zum Beispiel und wir wollen alle User die genau Zugang zu diesen System haben und wir nehmen deren Profile. Wenn wir jetzt in die Human Resource Datenbanken gehen und nehmen zum Beispiel Dinge wie Location oder Team; Dinge wie Status (also Angestelltenstatus: ist jemand ein Contractor oder Fulltime-Employee und so weiter und so fort). Und was wir machen ist: wir versuchen diese Zugriffsmuster zu finden. Und wie ich vorhin schon gesagt habe, wenn ich Zugriffsmuster sage, was ich meine ist, dass die am häufigsten auftretende Kombination von Attributen, die zum Zugriff zu einem System führt. Das ist das, was wir herausfinden wollen. Das tun wir, wie ich gerade schon gesagt habe, für jede einzelne Berechtigung.

Was wir dann machen und da kommt genau diese globale Sichtweise ins Spiel, ist, dass wir uns die gesamte Datenlandschaft zu Nutze machen. Dass wir sagen okay, wir haben jetzt einen Zugriffsmuster gefunden – das kann irgendeine Kombination von Attributen sein – und wir schauen uns an: die Mitarbeiter, die dieses Muster haben und die Berechtigung/Zugriff zur Berechtigung haben. Wir schauen, dass im Kontrast zu allen anderen Mitarbeitern, die auch dieses Muster haben. Irgendwo ist das Konzeptionell natürlich sehr schön zu visualisieren. Aber wir brauchen hier irgendetwas/irgendeine Metrik, um dem Ganzen irgendwo Gewicht zu geben.

Normalerweise hat man sowas wie ein Risiko Score (Risk Score) – in unserem Fall benutzen wir einen Confidence Score. Was ist dieser Confidence Score? Der Confidence Score repräsentiert quasi die Stärke der Korrelation zwischen eben einem gefundenen Zugriffsmuster und einer spezifischen Berechtigung. Ich würde ganz gerne mal ein kleines Beispiel geben, um es mal ein bisschen mehr zu veranschaulichen. Sagen wir mal, wir nehmen das Beispiel hier unten: unser Zugriffsmuster in dem Fall ist der Ort/das Attribut Ort ist vorhanden. In dem Fall ist es das Delaware Office in den USA. Und das Team ist das Analytic-Team in diesem Büro in den USA. Und wir haben ja einen Confidence Score von 75% und wir haben eine Team-Size oder auch Frequenz von 4. Wie berechnet sich jetzt dieser Confidence Score jetzt? Wenn wir uns überlegen: wir haben vier Personen in diesem Team. Alle vier Personen haben dieses Zugriffsmuster. Also alle vier Personen haben „Ort Delaware“ und „Team Analytic“, aber nur drei dieser Personen haben Zugriff zu diesem System. In dem Fall hier ist es eine Applikation One Drive. Es ist also ein File-sharing für einen Clinical Trial. Aber das ist nur ein Beispiel.

Die Art und Weise, wie wir jetzt diesen Confidence Score berechnen ist einfach: wir dividieren quasi die Personen, die das Zugriffsmuster haben und Zugang zum System haben durch die Anzahl der Mitarbeiter, die das Profil haben. Das heißt wir haben 3:4=75 Prozent. Jetzt zu der Frage: (wir haben diese Zugriffsmuster und wir haben diese Confidence Scores für jedes Zugriffsmuster). Was können wir damit machen?

Wir können und wollen auf der einen Seite: Automatisierung. Wie wir eben schon gesagt haben, haben wir Zertifizierungskampagnen. Die sind meistens sehr langwierig, fehlerbehaftet usw. Und da wir hier auf komplett datengetriebenes Analyseverfahren setzen, können wir die Ergebnisse benutzen um automatische Rezertifizierungen durchzuführen für die Berechtigungen, wo wir einen sehr hohen Confidence Score haben.

Das heißt, man kann zum Beispiel sagen: ich setze ein Threshold von 85 Prozent oder 90 Prozent. Das heißt, alles, was einen Confidence Score über 90 Prozent hat, wird automatisch rezertifiziert. Und was wir in der Praxis sehen ist, dass das eben sehr sehr viele Berechtigungen im Unternehmen betrifft. Wenn es Automatisierung geht, dann können wir natürlich auch über das Onboarding sprechen. Das heißt, wenn neue Mitarbeiter ins Unternehmen kommen. Und basierend auf deren Profilen (wenn wir das mit den Profilen mit diesen Zugriffsmustern vergleichen), können wir natürlich herausfinden, wo können wir sehr viel Sicherheit von vorn herein irgendwo haben, um einem Mitarbeiter Zugriff zu einem System zu geben. Wo wir davon ausgehen können, dass dieser Mitarbeiter eben Zugriff auf das System braucht.

Und genau diese beiden Komponenten für Automatiserung werden erleichtert durch Automonous Identity. Aber natürlich geht es im Governance Bereich nicht nur um Automatisierungen, sondern natürlich auch um Risikominimierung. Und wenn es um Risikominimierung geht, wollen wir natürlich Ausreißer erkennen.

Genau das ist der zweite große Punkt, der Autonomous Identity ermöglicht. Und zwar, dass wir unseren Fokus ein bisschen weg von den hohen Kompetenzberechtigungen einfach auf die Berechtigungen oder die User fokussieren können, wo wir eben nur sehr geringe Confidence haben. Das bedeutet: alles was irgendwo Risiko für das Unternehmen bedeuten könnte, wir können wir genau nur auf diese Weise fokussieren und da manuell Reviews machen, usw.

Und das sind diese beiden große Bereiche, die das Tool einfach ermöglicht.

[26:39] OLIVER
Dennis, hörst du mich? Ich weiß, dass du jetzt noch auf die unterschiedlichen Perspektiven eingehen willst. Aber wir haben ein paar Fragen reinbekommen und ich glaube es ist gut und einfacher, wenn wir sie jetzt direkt beantworten. Eine Frage: **Wie werden die existierenden Berechtigungen in einem Unternehmen gefunden, wenn sie zum Beispiel nur in den Applikationen selbst definiert sind? Wie kriegt ihr die?**

[27:10] DENNIS
Genau, das ist quasi der Data Ingestion Punkt am Anfang. Das heißt, das System ermöglicht die Vernetzung zu all diesen Systemen und zieht die Berechtigungen aus dem System raus. Das heißt zum Beispiel: wir haben sieben verschiedene Applikationen laufen, die alle unterschiedliche Logik haben in den Applikationen selber, wie Berechtigungen ausgeführt sind. Wir haben also Kontaktstellen zu diesen Systemen, die wir herstellen können und dann wird am Ende quasi ein Datenformat benutzt, was dann letzten Endes in das Auto ID System reingeht. Das heißt: es ermöglicht die Verbindung zwischen Auto ID und diesem System, die Berechtigungen herauszubekommen.

[27:52] OLIVER
Nächste Frage: **Spielt eure Auto ID Plattform mit jeder IAM/IGA Lösung zusammen? Beispielsweise mit Salepoint oder IBM?**

[28:06] DENNIS
Sehr gute Frage! Ja, tut sie. Also unser Autonomous Identity System ist so wirklich designt, dass sie mit jeder Government Solution/IGA Solution zusammenarbeiten kann. Wir sehen das so Augmented. Wir können das System quasi als intelligentes System auf jede Government Solution draufsetzen. Auf der einen Seite müssen die Daten ins System rein, auf der anderen Seite wollen wir mit den Ergebnissen etwas antriggern in der Government Solution. Und das ist genau für jedes System auf dem Markt möglich.

[28:47] OLIVER
Die letzte Frage bevor es weiter geht: **Um einen Confidence Score zu ermitteln, werden bestehende Berechtigungsvorgaben und Prozesse benötigt? Ist das Verfahren also nur bei Umstrukturierungen oder Neustrukturierungen sinnvoll einsetzbar? Oder ist es auch einsetzbar bei Neueinführungen?**

[29:12] DENNIS
Okay, also wenn ich es richtig verstehe. Was natürlich wichtig ist/was vorhanden sein muss sind die Daten letzten Endes. Die Berechtigungsdaten und die Profildaten müssen natürlich da sein, um das initiale Machine Learning Modell zu erstellen.

Wenn keine Daten vorhanden sind, dann kann natürlich nichts berechnet werden. Aber solange in irgendeiner Form Daten vorhanden sind (für Berechtigungen und Profile der User), kann das System trainiert werden, ja.

[29:37] OLIVER
Ja, Okay. Die weiteren Fragen machen wir später. Ich habe noch die so früh so viele Fragen in so einem Webcast gehabt. Super! Ich finde das klasse, liebe Teilnehmer. Aber wir wollen den Dennis jetzt nicht bremsen.

[29:56] DENNIS
Ich wollte noch kurz einen kleinen Überblick geben, wie das Ganze dann in der Praxis aussieht. Wir haben verschiedene Perspektiven.

Die drei Großen sind:
Die globale Perspektive. Das heißt die Unternehmensperspektive, welche zum Beispiel aus CISO Sicht oder Adminsicht wichtig sind. Und hier kann man eben das Machine Learning Modell selber verfolgen, aber zum Anderen auch die globale Sicht auf das Unternehmen bekommen. Man hat eine History irgendwo, wie sich das Risiko verhält im Unternehmen und wie sich die Berechtigungsanalysen verhalten. Man sieht auch die kritischsten Berechtigungen im Unternehmen.

Das Zweite ist dann Berechtigungsveranwortliche (Entitlement Owner), was zum Beispiel ein Application Owner sein kann. Hier ist der Fokus auf den Berechtigungen selber. Die Analyse, das was derjenige sieht, sind die Berechtigungen. Die Confidence Scores beziehen sich auf die Berechtigungen selber. Das heißt, man möchte als Entscheider wissen: okay, ich habe die Verantwortung für verschiedene Systeme und ich möchte gerne wissen, welches System ist am größten risikobehaftet oder welche Ergebnisse aus dem System kann ich am meisten automatisieren. Das Ganze können wir uns hier auch für jede einzelne Berechtigung anschauen. Und genau das sind die Zugriffsmuster, die wir hier auf der rechten Seite sehen. Die werden unterteilt mit den verschiedene Conference Scores und wir bekommen ein sehr übersichtliches Dashboard, auf dem wir auf einem Blick sehen können wie sich das Ganze global verteilt, aber was wir vielleicht auch automatisieren wollen und in Sicht auf Risikomanagement betrachten wollen.

Und als letzten Punkt haben wir dann die Vorgesetzten- oder Managerperspektive, wo wir den Fokus mehr auf die User richten. Das heißt zum Beispiel: alle Angestellten unter einem speziellen Manager. Und der Manager, als Entscheider, möchte gerne wissen, welche User haben einen sehr hohen Confidence Score für die verschiedenen Berechtigungen, wo wir zum Beispiel automatisieren können für Rezertifizierungen. Und auf der anderen Seite möchten wir wissen, welche User haben Zugriff zu Systemen, wo sie vielleicht nicht Zugriff haben sollten, um irgendwo das Risiko zu minimieren. Genau wie für die Berechtigungen auch, können wir uns die einzelnen Nutzer im Detail anschauen und für welche Berechtigungen der User die entsprechenden Confidence Scores hat.

Ja, Oliver, damit gebe ich an dich zurück.

[32:12] OLIVER
Super, das ist Klasse! Jetzt muss ich mal eben auf unsere Umfragen schauen. Wir wollen auflösen: Wie viele Zuweisungen haben Sie in ihrem Unternehmen? Ja, interessanterweise zwei Drittel (65 Prozent) von Ihnen, liebe Teilnehmer, haben weniger als 1 Millionen Zuweisungen von Berechtigungen. Ungefähr ein Sechstel (13 Prozent) zwischen 1 und 3 Millionen. Aber es gibt auch in Etwa ein Viertel (23 Prozent), die mehr als 3 Millionen Zuweisungen von Berechtigungen in ihrem Unternehmen sehen.

Damit kommen wir zur letzten Frage an Sie. Nachdem der Dennis das so schön vorgestellt hat, stellt sich jetzt die Frage: **Würden Sie Machine Learning im Bereich Identitäts- und Berechtigungsmanagement vertrauen?** Die Antwortmöglichkeiten sind: Ja – ich weiß nicht – nein. Wir haben noch die zeitliche Komponente mit einfließen lassen. Die da heißt: noch nicht.

Während Sie jetzt eine gute Minute zum Beantworten haben, haben wir noch weiter Fragen schon mal abarbeiten können. Und zwar: **Was ist mit extern gehosteten Anwendungen (von Dienstleistern)? Wie können diese eingebunden werden?**

[33:53] DENNIS
Sehr gute Frage. Das kommt natürlich drauf an, wie man das Ganze aus Compliance-Sicht strukturiert. Man kann es so machen, dass man die Prozesse teilt. Das heißt, man sieht sie als individuelle Prozesse und möchte wissen: ich möchte nur den Fokus auf diese externe Komponente richten. Oder man bezieht das Ganze in das Modell des Unternehmens mit ein. Man fusioniert, zum Beispiel, extern und intern zusammen und bekommt die Übersicht und bezieht quasi die Businesslogik aus dem Externen mit hinein.

Das kann man ganz flexibel organisieren und kann verschiedene Modelle/Vorhersagen herstellen.

[34:38] OLIVER
Okay. Und dann eine Frage, wo ich mir vorstellen könnte, das Lidiya gleich weitermacht und sehr gut beantworten könnte: **In welchen Branchen waren die Kunden, die an der Lösung beteiligt waren?**

[34:55] LIDIYA
Das ist auch eine gute Frage, Oliver. Ganz lieben Dank. Also bis jetzt haben wir Auto ID in verschiedenen Branchen zum Einsatz gebracht. Die Ergebnisse sind jetzt nicht so relevant für die Auswertungen. Aber für die Information: wir waren dann eigentlich in Resources unterwegs und hauptsächlich in Products.

[35:25] OLIVER
Okay, Prima. Lidiya, du hast uns noch etwas zur Kundenreise mitgebracht.

[35:26] LIDIYA
Herzlichen Dank, Oliver. Ja, wie ich am Anfang schon ein bisschen angedeutet habe, möchte ich gern noch mal über eine ganz aktuelle Kundensituation sprechen, in der Auto ID zum Einsatz kommt. Die Zeit möchte ich aber auch gerne nutzen, um Ihnen einige Take Aways mit auf den Weg zu geben.

Also unser Kunde plant gerade die Modernisierung seiner Identity Governance Platform und möchte genau diesen Wendepunkt nutzen, um die gesamte Berechtigungslandschaft zu analysieren und entsprechend Komplexität herauszunehmen.

Und hier der erste wichtige Take Away an dieser Stelle: Autonomous Identity ist kein Ersatz für Identity Governance Solution, sondern eine Turboergänzung, die Sie bereits am Anfang ihrer Effizienzreise unterstützt. Es ist oft ein Missverständnis, dass die Daten höchste Qualität erfüllen müssen, um Machine Learning überhaupt ins Spiel zu bringen. Ganz im Gegenteil: Machine Learning beschleunigt die Bereinigungsaktivitäten, liefert von Tag 1 dann auch bereits Kosten- und Zeitersparnisse.

Gerne möchte ich nochmal kurz verdeutlichen, mit welchen Identity und Access Management Herausforderungen unser Kunden konfrontiert ist. Und dazu gebe ich noch mal ein paar Beispiele:

- Rollenüberflut mit über 150.000 Rollen
- Rollenkomplexität mit Tausenden von Rollen. Mit über 400 einzelnen unklaren Berechtigungen.
- Erhöhter administrativer Aufwand für das Senior Management mit mehr als 1 Millionen manuellen Workflows in den letzten 8 Monaten.
- und die fehlende holistische Transparenz über die Identitäten und deren Berechtigungen im Unternehmen.

Unsere Aufgabe war dabei, die Rolle um 50 Prozent zu reduzieren, diese effizienter zu gestalten und Transparenz über die gesamt Berechtigungslandschaft innerhalb von sieben Wochen zu verschaffen. Aufgrund der enormen Datenmengen ist die manuelle Analyse von Anfang an keine Option für uns gewesen. Doch durch den Einsatz von Auto ID haben wir es aber nur in wenigen Wochen geschafft, die enorme Optimierungspotenziale in Bezug auf die Automatisierung, aber auch Risikominimierung, so zu entdecken.

Und gerne möchte ich Ihnen noch zeigen, wie wir dabei vorgegangen sind:
In erster Linie haben wir sichergestellt, dass die notwendige Infrastruktur und die Umgebung aufgebaut sind. Unser Deployment Process für Accenture ist dabei zu 90 Prozent automatisiert und erfolgt innerhalb weniger Tage. Parallel dazu haben wir Identitäts- und Berechtigungsdaten aus mehreren Quell- und Zählsystemen analysiert, aggretiert und durch das Auto ID/Audit Report qualitativ zu Machine Learning aufbereitet.

Das heißt: wenn wichtige organisatorische Daten, zum Beispiel, bei einer Identität, gefallen haben, haben wir diese von seinem Vorgesetzten übernommen. Basis für das Training waren die 5,3 Millionen Berechtigungsvergaben, inklusive der variablen Parametern (falls diese vorhanden waren). Diese brachten 60.000 Rollen in die Analyse ein. Weiterhin haben wir gemeinsam mit unseren Kunden, die stabilsten oder sozusagen, die am wenigsten dynamischen, organisatorischen Attribute definiert.

Und da sind die sogenannten Training Parameter. An dieser Stelle möchte ich einen kleinen Exkurs geben und kurz erklären, was das Training im Sinne von Machine Learning bedeutet. Auch im Sinne von Identity und Access Management. Also das Training an sich ist der Lernprozess zur Erkennung von Mustern für die Berechtigungen, basierend auf vordefinierten, organisatorischen Attributen.

Wie sieht das konkret aus? Also für jede Berechtigung werden im ersten Schritt alle ihr zugewiesenen Personen identifiziert. Für diesen Personenkreis werden die organisatorischen Muster abgeleitet und der Berechtigung wird ein Confidence Score vergeben. Die Kombination von organisatorischen Mustern (Confidence Score)

und die Berechtigung an sich, sind nämlich essentiell für die Rollen und für die Regeldefinition. An der Stelle, damit die essentiellen Aufbereitung und die Datenkonfiguration Erfolg haben, haben wir den ersten Machine Learning Gedanken auch gestartet. Währenddessen kamen noch Anforderungen auf uns zu, so wie es halt im echten Leben ist und die variablen Parametern sollten kein Teil der Zukunftsberechtigungslandschaft mehr sein.
Dementsprechend haben wir die Datenkonfiguration angepasst und das Berechtigungsobjekt (ohne variable Parameter) als Basis für das Training eingesetzt.

Für den zweiten Machine Learning Vorgang wurden die Daten außerdem in zwei Datensätze aufgeteilt. Um konkrete Aussagen bezüglich bereits automatisierter und manueller Berechtigungsvergaben treffen zu können.

Und an dieser Stelle der zweite wichtige Take Away von mir heute: Machine Learning ist ein interaktiver Prozess. Und auf dem Weg zum Ziel müssen mehrere Algorhythmuskriterien ausprobiert werden, um den am bestgeeigneten für den Fall herauszufinden.

Wir sehen hier die konkreten Zahlen hier in unserem Fallbeispiel: Also für die 5,3 Millionen Berechtigungsvergaben an die 100.000 Mitarbeiter, haben wir in einer Woche Transparenz geschaffen und neue effizientere Rollen gebaut. Gerne teile ich an dieser Stelle die Ergebnisse in zwei Kategorien auf. Die Eine, die Automatisierungspotenzial mit sich bringt, und die Zweite, die die risikobehafteten Berechtigungen transparenter macht.

Wie sieht das konkret aus? Also als bestgeeignetes Kriterien für einen sieghaften Automatisierungsgrad ergaben sich in erster Stelle, für die beiden Datensätze, ein hohen Confidence Score von 85 Prozent. Und eine Frequenz (Teamgröße) von 100. Auf dieser Basis haben wir zum Einen die 4,5 Default Rollen auf knapp 1000 Rollen reduziert und diese dabei effizienter gestaltet. Das heißt, trotz der knapp 80 Prozent Reduktion der Default Rollen, decken diese weiterhin über 82 Prozent der bereits bestehenden Berechtigungsvergaben. Doch der größte Anteil von Rollen stellen die Non-Default Rollen dar. Im Kontext unseres Kunden bedeutet das, dass diese Rollen momentan manuell beantragt und vergeben werden.

Durch die Analyse der Default Rollen wurden 602 neue Rollen definiert, die zukünftig, anstatt manuell, automatisch vergeben werden können. Diese 602 neue Rollen decken 25 Prozent der zurzeit manuellen Berechtigungsvergaben und decken ein enormes Automatisierungspotenzial auf. So geben wir signifikant wertvolle Zeit für businesskritische Aktivitäten an das Unternehmen zurück und das ist nämlich unser Hauptziel.

[43:36] OLIVER
Wunderbar! Das klingt fast nach einem tollen Schlusswort und ich sehe gerade auf der Uhr, wir haben noch eine Minute. Wir werden 2–3 Minuten überziehen, um noch ein paar Fragen zu beantworten. Und zwar, Lidiya, ich habe dir jetzt nicht das Wort abgeschnitten, oder?

[44:05] LIDIYA
Nein, alles gut.

[44:07] OLIVER
Eine Frage haben wir noch. Ich glaube, die ging in Richtung Dennis. **In welcher Tiefe sind Analysen machbar (am Beispiel SAP)? Nur Transaktionszugriffe oder auch tieferliegende Berechtigungen wie zum Beispiel Werteberei-che, Organisationsebenen, Buchungskreise?** Könnt ihr dazu was sagen, in welcher Tiefe die Analysen möglich sind?

[44:46] LIDIYA
Ich kann jetzt unsere Erfahrungen aus dem Fallbeispiel geben, sehr gerne. Ich bin aber allerdings auch keine SAP-Expertin, also kannst du mich gerne noch ergänzen.

Was wir hier jetzt bei dem SAP Komponenten zum Beispiel gemacht haben: also unser Kunde geht dann auch mit Composit Rollen um. Das heißt, Composit Rollen sind eine Zusammenfassung von einzelnen Rollen. Und unter diesen einzelnen Rollen gibt es natürlich dann auch die Autorisationsobjekte (T-Codes). Die Information, die wir in unserem Beispiel bekommen haben, war eigentlich auf Basis von Autorisation Object (T-Codes) auf den einzelnen Rollen.

[45:36] OLIVER
Okay, Prima. Noch eine Frage, die gerade reingekommen ist: **Wie gehen sie mit häufigen Umstrukturierungen in Unternehmen um, mit Blick auf Machine Learning?** Meine Vermutung wäre jetzt, dass es gerade da unterstützt, wenn es Umstrukturierungen gibt. Liege ich damit richtig?

[45:56] DENNIS
Ganz genau! Das ist genau die Stärke und vor allem diese dynamische Analyse, dass das Modell auch wöchentlich oder mehrmals die Woche retrained werden kann. Um genau diese schnelle, agile Veränderung im Unternehmen einfach zu reflektieren und halt auch dem Entscheider zu ermöglichen zu agieren, basierend auf den Ergebnissen.

[46:21] OLIVER
Ja, allerletzte Frage. Die kam ganz am Anfang rein. Ich habe ein bisschen gewartet und müsste jetzt eigentlich schon relativ klar sein: **Forgerock ist ja eher im SIAM Umfeld bekannt. Access Governance ist eher ein internes Thema. Wo liegt bei Auto ID der Fokus?**

[46:37] DENNIS
Genau. Also Auto ID bezieht sich natürlich ein bisschen mehr auf die interne Seite. Das heißt, wie haben den Identity Manager mit dem Governance dahinter. Das bezieht sich nämlich in erster Linie auf intern. Kann natürlich auch, wenn man zum Beispiel über Partnerorganisationen sprechen, die verbunden sind. Aber auch natürlich Kunden. Je nachdem, wie es halt strukturiert ist, kann es benutzt werden. Natürlich, der Fokus ist auf internal Workforce. Tatsächlich, ja.

[47:10] OLIVER
Prima! Bevor wir den Webcast schließen. Wir hatten die Frage gestellt: würden Sie Machine Learning in diesem Bereich vertrauen? 36 Prozent der Teilnehmer sagen „Ja“. 31 Prozent der Teilnehmer sagen „Noch nicht“. 26 Prozent wissen es nicht und es gibt auch 8 Prozent, die sagen klar „nein“.

Bevor wir schließen, Dennis. Wie können sich die Teilnehmer weiter informieren?

[47:43] DENNIS
Also für individuelle Fragen oder bei Interesse an einer Demo von mir, einfach eine E-Mail an die Nicola (nicola.paira@forgerock.com) schreiben. Aber wir haben auch sehr viel mehr auf unserer Webseite www.forgerock.com.

Wir haben Videos, Whitepapers und mehr Informationen. Also wenn weitergehendes Interesse besteht, melden Sie sich und wir freuen uns darauf, von Ihnen zu hören und Ihnen mehr zu zeigen.

[48:10] OLIVER
Superklasse! Eigentlich hatte ich jetzt, liebe Teilnehmer, alle drei Experten noch nach einem final Statement zu fragen, aber wir sind schon drei Minuten darüber. Lars, dich haben wir schon ein paar Minuten nicht gehört. Hast du noch Abschlussworte aus Hamburg?

[48:28] LARS
Also mir ist wichtig, dass wir verstehen, dass wir mit unseren Identity und Access Management Programmen eben eine zentrale Rolle auch in diesem größeren Kontext der digitalen Transformation spielen. Und ich bleibe gerne bei meiner Turbo-Analogie. Ich glaube, es braucht jetzt diesen Turbo genau aus diesem Grund.

Damit wir diesen Anforderungen, die wir jetzt hinreichen diskutiert haben, heute in diesem Call, dass wir diesen gerecht werden. Die neuen Technologien, die sich hier bieten und die ja auch unterstützt werden von den Zuhörern, eröffnet genau diese Möglichkeit. Deswegen freuen wir uns, das wir hier diese Resonanz erfahren haben und vielen, vielen Dank noch mal von mir aus Hamburg.

[49:16] OLIVER
Ich unterstütze dich, was du sagst, lieber Lars mit den Worten: Homeoffice ist noch lange nicht Digitalisierung. Da gehört ein bisschen mehr dazu. Ein Teil davon haben wir heute gesehen.

Ich fand es hochspannend. Von daher vielen, vielen Dank an dich Lidiya, an dich Dennis, an dich Lars! Es war ein wirklich ein interessanter Webcast. Wir bekommen hier auch schon ein Dankeschön von einem Teilnehmer rein. Ja, liebe Teilnehmer. Sorry für das Überziehen! Danke, dass sie dabei waren! Danke, dass Sie es mit uns so aktiv gestaltet haben und mir bleibt jetzt nur zu sagen: Tschüss und bis zum nächsten Mal!