Sylvia Johnigk

Herausforderungen an das Identitätsmanagement, allen Rollen gerecht zu werden

Outsourcing hat in den letzten Jahren die Möglichkeiten, mittels Identitätsmanagement und Zugriffskontrolle den Zugriff auf Unternehmensdaten zu schützen, radikal verschlechtert. Der Vortrag hat sich diesem Thema gewidmet und zeigt auf, vor welchen Herausforderungen Unternehmen stehen, die im Rahmen der Digitalisierung jeden Prozess auslagern, der nicht im Fokus des Kerngeschäfts steht.

Das im Vortrag dargestellte fiktive Unternehmen steht exemplarisch für viele real existierende Unternehmen.

Ende des letzten Jahrtausends

Noch vor gut 20 Jahren hatte unser fiktiver Finanzdienstleister seine eigene IT-Abteilung. Die Hardware wie Server, Endgeräte wie Desktop-Rechner, Laptops und Mobiltelefone, und Software waren Eigentum des Unternehmens. Die Geräte wurden weitestgehend von angestelltem Personal betrieben und gewartet.

Das Personal arbeitete in Gebäuden, die Eigentum des Unternehmens waren. Zutritt zu den Gebäuden wurde anhand des Mitarbeiterausweises durch menschliche und/oder technische Einlasskontrolle überprüft. Zugriff auf die Daten bekam nur derjenige, der sich an einem Desktop-Rechner entweder mittels eindeutigen Profilen User/Passwort oder Mitarbeiterausweis/Passwort authentisieren konnte. Hinter jedem Profil waren die dedizierten erlaubten Zugriffsmöglichkeiten hinterlegt. So war mehr oder weniger gewährleistet, dass nur das Personal mit den Daten arbeiten konnte, für die es zuständig war. Hochsicherheitszonen wie das Rechenzentrum waren durch zusätzliche Schleusen besonders geschützt.

Ende des letzten Jahrtausends arbeiteten Anton, Anna, Anke, Andre und Andrea gemeinsam in einem Unternehmen. Anton, Anna und Andrea arbeiteten in der IT-Abteilung, während Anke und Andre in der Fachabteilung arbeiteten. Da das Unternehmen damals ein hohes Sicherheitsbewusstsein hatte, benutzten die Mitarbeiter für das Login Smartcards kombiniert mit einem Passwort.

Die Zeit des Auslagerns beginnt

Anfang des Jahrtausends begann das Unternehmen, seine IT auszulagern. Zu Anfang geschah dies nur, um Kosten besser skalieren zu können bzw. Einsparungspotential besser erkennen zu können. Als IT-Mitarbeiter arbeiteten Anton, Anne und Andrea nun in der neu gegründeten IT-Tochter des Unternehmens. Damit die IT-Tochter kostengünstig ihre Dienste anbieten konnte, wurden, obwohl Administratoren in besonders großem Umfang mit sensiblen Daten arbeiten, als erstes die Kosten für die Smartcards resp. den Smartcard-Leser am Endgerät eingespart. Fortan meldeten sich die Administratoren nur noch mit der unsicheren Login-Prozedur User/Passwort an. Dass dies das Sicherheitsniveau des Unternehmens senkte, interessierte das Management nur am Rande, da die Kostenersparnis im Vordergrund stand und es keine besonderen Gesetze gab, die die Anmeldung mit Smartcard forderten.

Ansonsten hatte sich wenig geändert, bei IT-Problemen konnten die Mitarbeiter des Kernunternehmens wie Anke und Andre einfach kurz anrufen, ihr Problem schildern und in der Regel konnten kleine Probleme sofort und ganz ohne formalen Prozess gelöst werden. Dies sollte sich in der folgenden Zeit ändern.

Um weitere Kosten zu sparen, wurde als nächstes versucht, die Kosten für die Endgeräte der Mitarbeiter zu reduzieren. Die Lösung war, dass neue Endgeräte (Desktop-Rechner bzw. Laptops) nicht gekauft, sondern geleast wurden. Zudem wurde der First Level Support an denselben IT-Dienstleister ausgelagert. Im Laufe der Zeit wurden immer mehr Service-Dienstleistungen rund um die Endgeräte ausgelagert. Arbeiteten die externen Service-Mitarbeiter anfangs noch in den Räumen des Unternehmens mit geleasten Endgeräten und verfügten wie interne Mitarbeiter über eine User/Passwort-Kombination zum Einloggen in das Firmennetzwerk, so benutzten sie zunehmend die Möglichkeit, sich via VPN und RSA Token in das Unternehmensnetzwerk einzuloggen. So wurden die Kosten für Arbeitsplätze und Endgeräte eingespart. Zusätzlich wurden interne Mitarbeiter, die bisher den Service geleistet hatten, entweder in vorzeitigen Ruhestand geschickt oder an den externen Dienstleister ausgelagert. Anna nahm das Angebot an und arbeitete fortan als externe Mitarbeiterin weiter im alten Unternehmen. Man konnte Anna zwar immer noch anrufen, aber Anna war nun nur noch gegenüber ihrem neuen Arbeitgeber weisungsgebunden. So konnten selbst kleine Probleme nur im Rahmen eines formalen Prozesses gelöst werden.

Obwohl keine (nennenswerten) Kosten eingespart wurden, wurden als nächstes die Server nicht mehr gekauft, sondern ebenfalls geleast. Weitere First- und Second-Level-Services wurden ebenfalls an den externen Server-Dienstleister ausgelagert. Wie schon zuvor wurden interne Mitarbeiter in den Vorruhestand geschickt, oder konnten fortan in dem externen Unternehmen arbeiten. Anton arbeitete nun bei dem externen Server-Dienstleister, wie Anne loggte er sich nun via VPN und RSA Token ein.

Obwohl weiterhin keine nennenswerten Kosten eingespart wurden, wurde als nächstes die Software (z. B. Betriebssysteme, Office, Virensoftware, Firewalls etc.) nicht mehr gekauft, sondern geleast, und wieder schieden Mitarbeiter aus dem Unternehmen aus, da auch die Services rund um die Installation und Wartung ausgelagert wurden. Mit der Zeit verlor das Unternehmen nicht nur immer mehr IT-Wissen, sondern auch den Überblick, da die Zahl der involvierten Firmen immer größer wurde.

Da die RSA Token vom Unternehmen herausgegeben und verwaltet wurden, konnten nur externe Mitarbeiter auf die Unternehmensdaten zugreifen, wenn die externen Mitarbeiter im Unternehmen bekannt waren. So war das Unternehmen bei-

spielsweise 2011 noch im Bilde, als es Sicherheitsprobleme mit den RSA Token gab. Damals war die Technologie der RSA Token gehackt worden, und RSA benötigte mehr als drei Monate, bis sie die Sicherheitslücke schließen konnten. Zu diesem Zeitpunkt war man sich zumindest des Risikos bewusst, da man den Umfang der RSA-Zugänge zahlenmäßig erfassen konnte und auch wusste, auf welche Daten die externen Mitarbeiter zugreifen durften. So war man in der Lage, Zugriffe auf besonders sensible Daten via RSA-Zugängen zu kappen und die Mitarbeiter wieder über die konservativen Zugänge arbeiten zu lassen, sprich, diese Mitarbeiter mussten wieder Arbeitsplätze im Unternehmen nutzen.

Das international agierende Unternehmen betreibt auch kein eigenes WAN (Netzwerk), um ihre einzelnen Lokationen miteinander zu verbinden, sondern setzt auf Telco-Provider, und auch vor Ort für das LAN wird auf ausgewiesene Provider zurückgegriffen. Diese Zugriffsmöglichkeiten auf Netzwerkebene erfolgen bereits unter dem Radar des Finanzdienstleisters. Aus dem verteilten Arbeiten in internationalen Teams ergibt sich die Herausforderung, wie man die Daten so speichert, dass Mitarbeiter kostengünstig rund um die Uhr darauf zugreifen können.

Ab in die Cloud

Hatte das Unternehmen bislang noch halbwegs einen Überblick über sein Identitätsmanagement und die Zugriffskontrolle und damit darüber, wer alles auf die Unternehmensdaten zugreifen kann, so geht dieser mit dem Zeitalter des Cloudcomputing völlig verloren.

Der wesentliche Unterschied ist vor allem, dass nun die Daten außer Haus gespeichert und verarbeitet werden in der Cloud. Selbst personenbezogene Daten, die „eigentlich" gemäß dem BDSG oder zukünftig gemäß der EU-Datenschutzgrundverordnung zumindest innerhalb der EU gespeichert und verarbeitet werden müssen, werden schlussendlich irgendwo verarbeitet.[1]

Das Unternehmen nimmt einen Clouddienstleister in Anspruch. Es muss sich bei Vertragsabschluss und in den folgenden Jahren davon überzeugen, dass der Clouddienstleister die in der EU geltenden Gesetze auch einhält.

Bezogen auf das Identitätsmanagement und Zugriffsmanagement heißt das, dass unser fiktiver Finanzdienstleister sich davon überzeugen muss, dass sein IT-Dienstleister sich davon überzeugt, dass der gewählte Cloudprovider hinsichtlich des Identitätsmanagements dasselbe Schutzniveau bietet, wie er selbst es nach EU-Recht erbringen muss. Der Cloudanbieter greift auf Subprovider zu, um einen 7*24-Stunden-Service anbieten zu können. In dem Outsourcing-Vertrag bzw. in dem Auftragsdatenschutzvertrag werden 20 weitere Subprovider vereinbart (deren Unternehmen in den USA, Kanada, Brasilien, Singapur, Indien, der Türkei etc. ansässig sind), die ebenfalls auf die Daten Zugriff haben. Zusätzlich lässt sich der Cloudanbieter vertraglich festschreiben, dass er jederzeit neue Subprovider beauftragen kann, solange sich das Subunternehmen vertraglich verpflichten lässt, sich an die EU-Gesetzgebung zu halten. Dies muss der Cloudanbieter dem Kunden zwar mitteilen, aber unser Finanzdienstleister kann de facto nicht widersprechen, sondern lediglich den Vertrag kündigen. Dass auch die Subprovider Verträge mit weiteren Subprovidern schließen, und diese ebenfalls mit Subprovidern arbeiten, und die wiederum ... macht dies nicht einfacher.

Konsequenzen aus dem Cloudcomputing

Fakt ist, dass unser fiktives Unternehmen nicht mehr weiß, wer auf die Daten zugreifen kann. Es weiß auch nicht mehr, mit welchen Verfahren (User/Passwort, RSA Token/Passwort etc.) zugegriffen wird. Anton arbeitet übrigens derzeit bei einem dieser Subprovider in Estland, seiner alten Heimat. Estland ist ein modernes EU-Land, deshalb gibt es Personalausweise mit Chip und digitaler Signatur. Damit meldet sich Anton jeden Morgen aus seinem Home-Office an und hat so als Superadmin Zugriff auf die Unternehmensdaten. Bis zum September 2017 war dieses Verfahren mindestens so sicher wie gefordert. Nach dem Hack[2] des estnischen Chipkartensystems im September wäre zumindest eine Überprüfung des Verfahrens notwendig. Der Finanzdienstleister hat dazu de facto keine Chance. Das Unternehmen muss sich darauf verlassen, dass die Prüf-Kette über alle Subprovider funktioniert. Die fehlende Möglichkeit der Kontrolle aller Dienstleister und Subdienstleister ist im Übrigen nicht nur beim Identitäts- und Zugriffskontrollmanagement ein Problem, sondern bei allen Sicherheitsthemen.

Anmerkungen

1 *Dies geht für den Cloudprovider deshalb, weil der Gesetzgeber die Möglichkeit gibt, dies über die EU Standard Clauses, Privacy Shield bzw. Binding Corporate Rules absichern. Diese Verfahren sind Nachfolger des Safe-Harbor-Abkommens, das im Oktober 2015 vom Europäischen Gerichtshof kassiert wurde. Jedes stellt einen Vertrag zwischen Unternehmen dar, wobei sich beteiligte Unternehmen in Drittstaaten verpflichten, die europäischen Gesetze einzuhalten., aber keines bietet einen besseren Schutz als das Safe-Harbor-Abkommen.*

2 *heise online, Estland: Sicherheitslücke in fast 750.000 ID-Cards, https://www.heise.de/newsticker/meldung/Estland-Sicherheitsluecke-in-fast-750-000-ID-Cards-3822597.html*

Sylvia Johnigk

Sylvia Johnigk forscht und arbeitet seit über 25 Jahren im Bereich IT-Sicherheit, seit 2009 ist sie selbständige Beraterin in Großkonzernen. Ebenfalls seit 2009 ist sie im Vorstand des FIfF e. V.