semperis

CASE STUDY UNIVERSITY OF STUTTGART

University of Stuttgart

WIE DIE UNIVERSITÄT STUTTGART DAS IDENTITY-MANAGEMENT HÄRTET

Luftfahrt, Quantentechnologie oder medizinische Robotik sind Wissenschaftsbereiche, die von höchster Relevanz sind. Insbesondere, wenn es um Forschungsergebnisse geht, die an der Weltspitze liegen – wie bei der Universität Stuttgart. Grund genug, sich um die Sicherheit der IT-Netze zu kümmern und insbesondere das Identity-Management einer gründlichen Prüfung zu unterziehen.

> “Ohne das Assessment mit Unterstützung eines kompetenten Partners hätte es für uns einen großen Aufwand bedeutet, ein Ergebnis von ähnlich hoher Qualität zu erzielen. Schon allein deshalb, weil dazu eine umfassende Schulung der Mitarbeiter erforderlich gewesen wäre.“

Mike Holz
Head of the ZVD Department

SPITZENFORSCHUNG VOR BEGEHRLICHKEITEN SCHÜTZEN

Die Universität Stuttgart ist Teil eines breitgefächerten Ecosystems und Knotenpunkt für die Forschung in einer wirtschaftsstarken Region. Rund 23.000 junge Menschen studieren an der Universität in den unterschiedlichsten Fachrichtungen. Sie werden dabei von beinahe 5.700 Mitarbeitern unterstützt, um Forschenden und Studierenden hervorragende Rahmenbedingungen zu schaffen. Dazu gehört eine digitale Infrastruktur, die den reibungslosen Zugang zu umfassenden Ressourcen garantiert – sofern die dafür notwendige Berechtigung vorliegt.

Das Management der Hardware und der umfassenden Services obliegt dem Bereich Technische Informations- und Kommunikationsdienste (TIK) als Teil des Informations- und Kommunikationszentrums der Universität (IZUS). In diesen Bereich fallen auch die Zentralen Verwaltungsdienste, die den zentralen Arbeitsplatzsupport inklusive der notwendigen File- oder Printserver, dem Patchmanagement und der Geräteverwaltung sicherstellen. Hinzu kommt die Betreuung der Fachanwendungen wie dem Dokumentenmanagement oder der Personalverwaltung.

Den Zentralen Verwaltungsdiensten (ZVD) obliegt es auch, das Active Directory zu pflegen, das den Beschäftigten sowie den Studierenden Zugriff auf die jeweils benötigten Ressourcen ermöglicht. „Wir sind im Rahmen des Identity-Managements für die Sicherheit und den Betrieb der Active Directory verantwortlich“, erläutert Mike Holz, Abteilungsleiter der ZVD.

ACTIVE DIRECTORY ALS ZENTRALE INSTANZ

In Anbetracht der Bedeutung und Sensibilität der erarbeiteten Forschungsergebnisse in Hochtechnologien und des weltweiten Interesses an derlei Daten unterliegt die Sicherung des Zugangs höchster Aufmerksamkeit. Dabei ist die besondere Umgebung zu berücksichtigen, bei der eine große Zahl von Studierenden mit Privatgeräten Zugang über ein VPN zum Universitätsnetz erhalten müssen. Auch die kontinuierliche Fluktuation stellt eine Herausforderung für die Neuprovisionierung von Rechten dar. Hierbei ist eine enge Verzahnung der IT mit dem Personalverwaltungssystem erforderlich.

„Selbstverständlich verfolgen wir kontinuierlich die aktuelle Sicherheitslage, mit besonderem Augenmerk auf öffentliche Bereiche und Universitäten“, erklärt Holz. „Dabei ist in den vergangenen Jahren auffällig geworden, dass Angriffe auf diese Bereiche kontinuierlich steigen. Es wurde uns zunehmend bewusst, dass wir hier proaktiv werden müssen.“ Dabei ist die Sicherung des Zugangs zu sensiblen Bereichen nur die eine Seite der Medaille. Hinzu kommt, dass bei einer Kompromittierung des zentralen Verzeichnisdienstes möglicherweise die Arbeitsfähigkeit der gesamten Institution für mehrere Tage eingeschränkt wird, wenn nicht sogar ganz zum Erliegen kommt.

Folgerichtig suchten Mike Holz und sein Team nach Optionen, um die Sicherheit und Funktionsfähigkeit des Identity-Managements von kompetenter Seite prüfen zu lassen. „Auch wenn wir sicher waren, das Erforderliche getan zu haben, bestand dennoch die Möglichkeit, dass Schwachstellen übersehen wurden. Und schließlich entstehen täglich neue Angriffsvektoren, zum Beispiel auf Basis neuer KI-Techniken, die wir nicht auf dem Radar haben konnten.“

SECURITY ASSESSMENT MIT KOMPETENTEM PARTNER

Es lag nahe, für ein grundlegendes Active Directory Security Assessment (ADSA) ein erfahrenes Unternehmen hinzuzuziehen, das als führender Anbieter von Sicherheitslösungen für das Active Directory über hinreichend Erfahrung und Kenntnis der aktuellen Entwicklungen verfügt. Die Entscheidung fiel zugunsten von Semperis, einem anerkannten Experten, der Organisationen dabei hilft, ihre Identitäten zu schützen und Sicherungsprozesse zu optimieren. Dazu bietet Semperis eine Reihe von Lösungen an, die auf die Schwächen und Risiken des Einsatzes des Active Directory eingehen, Änderungen am Verzeichnisdienst überwachen, mögliche Bedrohungen auch durch privilegierte Benutzer erkennen, und eine schnelle Reaktion auf Angriffe ermöglichen.

Aufbauend auf umfassender Erfahrung aus weltweiten Kundenprojekten bietet Semperis das Active Directory Security Assessment (ADSA) an. Diese Analyse liefert eine detaillierte Bewertung der Sicherheitslage der Active-Directory-Umgebung, gibt Organisationen ein fundiertes Verständnis über identifizierte Risiken und bietet gezielte Handlungsempfehlungen zur Stärkung der Active-Directory-Sicherheit.

Neben der Identifizierung gefährlicher Fehlkonfigurationen und der damit verbundenen Risiken liegt ein weiterer Fokus darauf, Angriffswege innerhalb der AD-Umgebung zu erkennen, die es einem Angreifer ermöglichen könnten, kritische (Tier-0-) Ressourcen zu kompromittieren.

Ein Review der Sicherheitsarchitektur und der operationalen Prozesse vervollständigt die Analyse des Assessments. Es dient dazu, Abweichungen von Best Practices zu identifizieren. In Interviews mit Schlüsselpersonen und Experten werden zentrale Bereiche wie Security Governance, Netzwerkarchitektur, Domain Trusts, Systemadministration und Sicherheitsüberwachung hinterfragt, um potenzielle Schwachstellen aufzudecken und geeignete Empfehlungen abzuleiten.

Das Ergebnis sind maßgeschneiderte Empfehlungen zur Stärkung der Sicherheit, einschließlich Best Practices für die sichere Konfiguration des Active Directory. Die Umsetzung dieser Maßnahmen liegt in der Verantwortung der Organisation.

Nachdem die Entscheidung gefallen war, das Projekt anzugehen, wurden die entsprechenden Teams zusammengestellt und ein strukturierter Fragenkatalog erarbeitet. Die Zeitspanne von der Zieldefinition und Klärung der zu bewertenden Domänen über die Inventarisierung der Struktur bis hin zur Analyse der gesamten Umgebung und deren Risiko-Bewertung betrug etwa sechs bis acht Wochen, wobei der Netto-Zeitaufwand für die Mitarbeiter der Zentralen Verwaltungsdienste der Universität lediglich bei einigen Tagen lag. Gesteuert durch die Projektleitung waren Semperis-Experten weltweit beteiligt, um das Assessment mit ihrer Expertise zu begleiten. Dazu kamen Tools zum Einsatz, um die Active-Directory-Konfiguration sowie ergänzende Informationen, die für die Analyse erforderlich sind, effizient und automatisiert zu erfassen. Auf dieser Basis wurde die zeitliche Belastung für die universitätseigene IT minimiert.

Als Ergebnis erhielt die Universität eine umfassende Analyse der bestehenden Infrastruktur und Prozesse. „Tatsächlich sind nur wenige kritische Probleme aufgefallen", resümiert Mike Holz das Ergebnis. „Vor allem im Vergleich mit anderen Institutionen unserer Größe und mit vergleichbaren Sicherheitsanforderungen war das Resultat durchaus positiv." Was allerdings nicht meint, die bisherige Praxis nun beruhigt weiterzuverfolgen. „Manches hat Anlass gegeben, über gewisse Punkte nachzudenken, die unter Berücksichtigung des gegebenen Potenzials nun sukzessive anzugehen sind."

KNOW-HOW-TRANSFER INKLUSIVE

Auch wenn das Resultat des Assessments in weiten Teilen die erfolgreiche Arbeit des Teams attestierte, so hat dessen Durchführung eine Reihe von weiteren positiven Einflüssen: Es verstärkt das Vertrauen in die etablierten Mechanismen und die handelnden Personen, was die Reputation der Universität im internationalen Ecosystem verstärkt und die Grundlage für eine vertrauensvolle Zusammenarbeit mit anderen wissenschaftlichen Institutionen und Partnern aus der Wirtschaft bildet. Zudem helfen die Ergebnisse der Analyse dabei, die zur Verfügung stehenden Human Resources gezielter einzusetzen.

Gerade in dieser Hinsicht darf ein weiterer Effekt nicht vernachlässigt werden: „Ohne das Assessment mit Unterstützung eines kompetenten Partners hätte es für uns einen großen Aufwand bedeutet, ein Ergebnis von ähnlich hoher Qualität zu erzielen. Schon allein deshalb, weil dazu eine umfassende Schulung der Mitarbeiter erforderlich gewesen wäre", erklärt Holz. Tatsächlich ist die Kompetenz des eigenen Teams durch die Zusammenarbeit mit den Experten von Semperis im Hinblick auf die Funktion und Schwachstellen des Active Directory erheblich gewachsen – auch eine Art gelungenen Know-how-Transfers.

Perspektivisch gesehen sieht sich das AD-Team der Universität mit den nun optimierten Prozessen gut gerüstet, wobei auch die Erkenntnis mitschwingt, dass eine absolute Sicherheit in einem hochdynamischen Umfeld nicht garantiert werden kann. „In Anbetracht des Aufwandes, den interessierte Kreise entwickeln, um an entsprechende Forschungsergebnisse zu gelangen, auch mit Unterstützung geeigneter Technologien aus dem Bereich der Künstlichen Intelligenz, bleibt es unsere Aufgabe, sich kontinuierlich mit neuen Angriffsvektoren auseinanderzusetzen."

Tatsächlich bestehen bei der Verwaltung von Identitäten immer Risiken, die allerdings durch den Einsatz von Methoden wie etwa Change-Tracking und Auto-Remediation minimiert werden können. Und letztlich kommt es auch darauf an, selbst in einem Worst-Case-Szenario in der Lage zu sein, das AD binnen Minuten wiederherzustellen. Entsprechende Tools wie die Active Directory Forest Recovery stehen dazu zur Verfügung und lassen sich mit minimalem Aufwand implementieren.