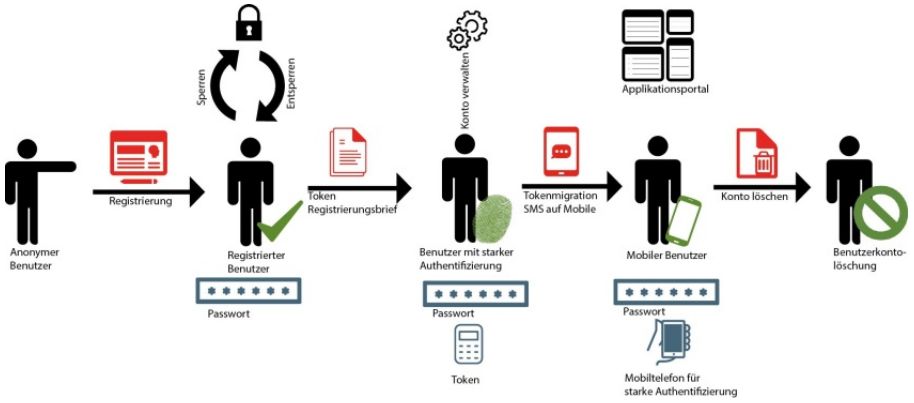
Leistungsfähige Authentifizierungslösung mit Self Service-Funktionen

Dr. Götz Güttich

Vor kurzem haben wir uns bereits im Detail mit der Airlock Web Application Firewall befasst, die dazu in der Lage ist, den Datenverkehr zwischen Anwendern und Applikationen im Unternehmen oder in der Cloud abzusichern. In vielen Fällen verwenden Unternehmen diese Web Application Firewall in Kombination mit der Identity and Access Management-Lösung des gleichen Herstellers. Das ergibt Sinn, um nicht nur die Datenübertragungen sicher zu gestalten, sondern auch die beteiligten Benutzer genau zu identifizieren. Dieser Beitrag befasst sich nun im Detail mit den Funktionen des Identity and Access Management-Produkts.



Die Airlock Identity and Access Management-Lösung (IAM) muss nicht zwangsläufig zusammen mit der Web Application Firewall (WAF) zum Einsatz kommen, sondern lässt sich bei Bedarf auch stand-alone nutzen. Für unseren Test haben wir aber beide Produkte gemeinsam in Betrieb genommen. Airlock IAM stellt den Nutzern eine zentrale Authentifizierungsplattform mit Enterprise-Funktionen zur Verfügung.

Die Lösung unterstützt eine große Zahl an Authentifizierungsverfahren, arbeitet mit Standardprotokollen und automatisiert gleichzeitig die Benutzeradministration. Umfassende Self-Service-Funktionen sorgen dafür, dass die Anwender praktisch alle Schritte, die bei der Verwaltung ihrer Benutzerkonten anfallen, selbst erledigen können, was das Helpdesk deutlich entlastet. Außerdem ermöglicht das Produkt Single Sign On (SSO) unter anderem mit SAML 2.0 IDP und SP, OAuth 2.0, OpenID Connect, Kerberos und NTLM.

Die IAM-Lösung vereint im Betrieb die Benutzerverwaltung mit der Rollenverwaltung und stellt eine vorgelagerte Authentisierung für Sessions und Requests bereit. Dank der Anbindung von LDAP-, Microsoft Active Directory- und Datenbank-Umgebungen sowie Radius-Servern und ähnlichem sind die Anwender dazu in der Lage, ihre bestehenden Benutzerverzeichnisse nahtlos weiterzuverwenden.

Alternativ steht auch eine integrierte Benutzerverwaltung mit Token- und Rollenverwaltung, Reporting und Password Policy Enforcement zur Verfügung. Eine mächtige Suchfunktion sorgt dafür, dass die Helpdesk-Mitarbeiter dazu in die Lage versetzt werden, schnell die Benutzerkonten zu finden, für die sie Support leisten sollen. Diese Suchfunktion lässt sich bei Bedarf über Plugins erweitern, falls in der jeweiligen Umgebung besondere Funktionalitäten erforderlich sind. Die Logins laufen im Betrieb über eine eigene, flexibel konfigurierbare Web-Applikation ab, auf die wir später noch genauer eingehen werden. Ein leistungsfähiges REST-API steht ebenfalls zur Verfügung. Darüber hinaus ist das Airlock IAM mandantenfähig, bietet Fail-Over- sowie Clustering-Funktionen und stellt umfassende Logging-Features beziehungsweise Statistiken bereit. Die Verwaltung erfolgt über eine browser-basierte, zentrale Management-Konsole.

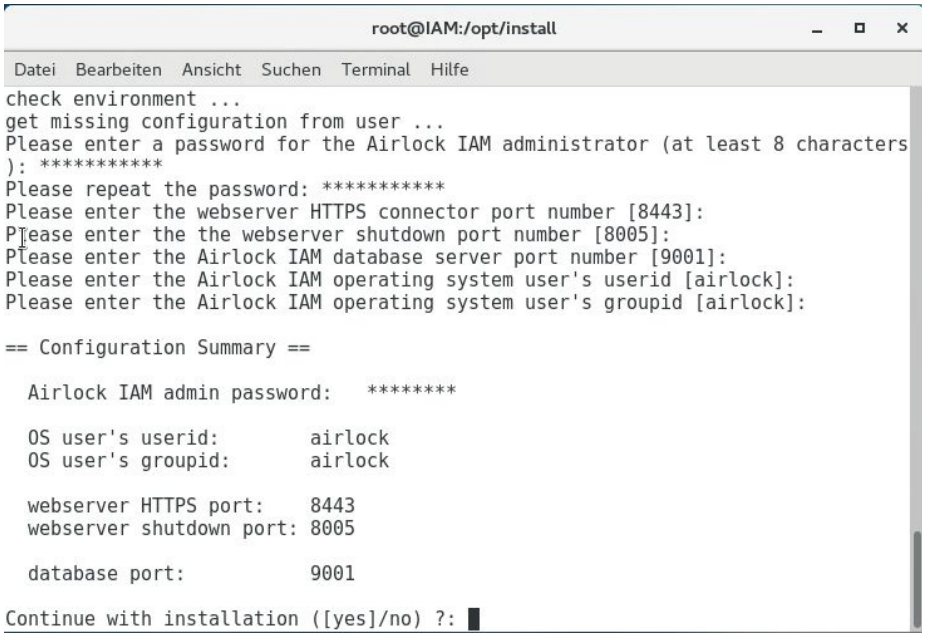
Authentifizierung und Identity Propagation

Das System unterstützt eine Vielzahl an Authentifizierungsmethoden wie unter anderem CrontoSign, mTAN/SMS, Vasco Digipass, Matrixcard, RSA SecurID und Kobil AST. Im Betrieb trennt das Produkt die Authentifizierung von der Identity Propagation. Mit letzterem ist die Vermittlung der Benutzeridentität an die abgesicherte Applikation – also praktisch nach innen – gemeint. Die Art, wie die Login-Daten übertragen werden, gestaltet sich ja je nach Anwendung unterschiedlich. In diesem Zusammenhang unterstützt die Lösung eine Vielzahl an Optionen. Die die Identity Propagation mit Hilfe von Plugins gelöst wird, lassen sich je nach Bedarf problemlos neue Anwendungen hinzufügen.

Die IT-Verantwortlichen können die IAM-Lösung zudem jederzeit flexibel erweitern und in nichtstandard Umgebungen integrieren. Durch die Anpassungen wird sie aber nicht zu einer Custom-Lösung, sondern bleibt dank ihrer Flexibilität weiter kompatibel zu den normalen, vom Hersteller bereit gestellten Update-Dateien.

Aufbau

Airlock IAM besteht insgesamt aus drei Bestandteilen. Der erste ist die genannte Login-Applikation mit Registrierung, Self Service-Funktionen (zum Beispiel zum Zurücksetzen eines vergessenen Passworts) Captchas und ähnlichem. Der zweite stellt die Administrationsoberfläche dar, über die das System verwaltet wird und der dritte nennt sich "Service Container". Er umfasst Dienste im Hintergrund, die beispielsweise Datenbanken synchronisieren, automatisch Briefe mit Authentifizierungscodes ausdrucken und vieles mehr.



Die Installationsroutine der IAM-Lösung fragt unter anderem nach den zu verwendenden Ports

Der Test

Für unseren Test spielten wir die IAM-Lösung in einer virtuellen Maschine unter Centos 7 ein. Die einzige Voraussetzung für den Betrieb des Produkts ist eine funktionierende Java-Umgebung, der Hersteller empfiehlt an dieser Stelle mindestens ein JRE mit Java 8, am besten Version 1.8u91 oder neuer von Oracle. Hardwareseitig sollte ein Rechner mit einer 2 GHz-CPU, 4 GByte RAM und 10 GByte Festplattenplatz zum Einsatz kommen.

Nach dem Abschluss des Setups richteten wir das IAM in unserem Netz so ein, dass es zusammen mit der Airlock WAF die Zugriffe auf das Web Interface des bei uns im Testlabor genutzten Network Monitoring-Produkts PRTG von Paessler absicherte. Außerdem verwendeten wir auch eine vom Hersteller bereitgestellte Testumgebung mit einem Book-Shop als Testapplikation, um anhand diverser Use Cases die Funktionalität der IAM-Lösung unter die Lupe zu nehmen.

Installation

Die Installation des Produkts gestaltet sich vergleichsweise einfach. Es genügt, die von der Webseite des Herstellers heruntergeladene Installationsdatei unter Linux ausführbar zu machen und aufzurufen. Danach fragt die Setup-Routine nach dem Passwort für den IAM-Administrator und den für die Datenkommunikation eingesetzten Ports. Wir beließen diese für unsere Testinstallation auf den Standardwerten. Danach lief die Installation durch und wir konnten uns über die URL http://localhost:8443/auth-admin/login beim System anmelden. Nachdem das erledigt war, spielten wir zunächst unsere Lizenz ein.

Um nun die IAM-Lösung so zu konfigurieren, dass sie mit der WAF, die in unserem Netz auf einer anderen virtuellen Maschine lief, zusammenarbeitete, war es im nächsten Schritt erforderlich, die IAM in der WAF als Backend

Host einzutragen und ein entsprechendes Mapping anzulegen. Für dieses Mapping bietet der Hersteller ein Template an, so dass sich diese Arbeit relativ einfach erledigen lässt. Das ganze Vorgehen wird in der Dokumentation gut beschrieben, so dass sich beim Anpassen der Konfiguration an die jeweiligen Gegebenheiten keine Schwierigkeiten ergeben.

Die Konfigurationsoberfläche

Setzen wir uns an dieser Stelle einmal kurz mit dem IAM-Konfigurationswerkzeug auseinander. Loggt sich der Anwender bei dem Tool ein, so landet er zunächst auf einer Seite mit den aktuellen Log-Einträgen. Hier kann er nicht nur die Lizenz einspielen, sondern ist unter anderem auch dazu in der Lage, die verschiedenen Administratorkonten, die Zugriff auf das Produkt erhalten sollen, zu verwalten, die Konfiguration der Lösung anzupassen, Wartungsmeldungen einzurichten, die das System auf dem Anmeldebildschirm anzeigt, und die Benutzer zu administrieren.

Wechselt der zuständige Mitarbeiter in die Benutzerverwaltung, so landet er zunächst einmal in einer Suchfunktion, mit der sich alle vorhandenen Benutzerkonten durchsuchen lassen. Ruft er dann ein Benutzerkonto auf, so präsentiert ihn die Lösung eine Übersichtsseite mit dem Benutzernamen, der Firma, dem Token des Users (falls vorhanden), der Zahl der fehlgeschlagenen Anmeldungen, dem Datum und der Uhrzeit der letzten Anmeldung und ähnlichem.

Interessanter ist an dieser Stelle der Reiter „Profil“. Dieser ermöglicht das Ändern des Benutzernamens, das Angeben von Adressdaten, das Festlegen der Gültigkeitsdauer des Accounts, das Löschen des Kontos und das Hinzufügen des Users zu bestimmten Rollen. Bei letzterem kann es sich um „Customer“, „Employee“ oder „Administrator“ handeln. Alles ist jederzeit konfigurierbar und alle Einstellungen lassen sich on the fly ändern.

Der nächste Reiter befasst sich mit den Authentifizierungsmethoden. Hier legen die zuständigen Mitarbeiter unter anderem das aktive Authentifizierungsmittel fest. Üblicherweise kommt zuerst immer eine Authentifizierung via Benutzername und Passwort zum Einsatz. Danach kann dann das Sicherheitsniveau durch eine weitere Methode, wie zum Beispiel mTAN/SMS oder auch Kobil AST, angehoben werden.

An gleicher Stelle sind die IT-Verantwortlichen dazu in der Lage, weitere Authentifizierungsmethoden hinzuzufügen, wie etwa Matrixcard, E-Mail OTP, OATH OTP oder auch CrontoSign. Außerdem besteht auch die Option, eine Migration der Authentifizierungsmethoden anzustoßen und den betroffenen Benutzer zu zwingen, bis zu einem bestimmten Termin auf die neu eingerichtete Authentifizierung umzusteigen. Auf diese Funktionalitäten gehen wir später noch genauer ein.

Die weiteren Reiter der Benutzerverwaltung befassen sich dann mit der Konfiguration der jeweils aktiven Authentifizierungsmethoden. Hier legen die Administratoren zum Beispiel fest, ob Passwortwechsel erzwungen werden sollen, wie lang die Codes gültig sind, die sich auf per Post verschickten Aktivierungsbriefen befinden, und ähnliches. Eine Aktivitätsübersicht, die Aufschluss darüber gibt, wann sich der betroffene Benutzer angemeldet hat oder ob es fehlgeschlagene Login-Versuche gegeben hat, schließt den Leistungsumfang der Benutzerverwaltung ab.

Dank des großen Funktionsumfangs der IAM-Lösung haben die Administratoren über das eben beschriebene User Management eine große Zahl an Optionen, um die Authentifizierung der Benutzer zu beeinflussen und die Veraltung zu automatisieren. So besteht beispielsweise die Möglichkeit, den Anwendern zu erlauben, eine neue Authentifizierungsmethode wie CrontoSign zu aktivieren.

Wenn IAM entsprechend konfiguriert wurde, druckt das System, sobald der User aktiv geworden ist, einen Aktivierungsbrief mit einem Authentifizierungscode aus und schickt ihn an den betroffenen Anwender. Sobald dieser den Brief erhält, ist sichergestellt, dass seine Adressangabe stimmt.

Wenn er den Code mit seinem Smartphone scannt, wird die neue Authentifizierungsmethode freigeschaltet und kann anschließend zum Einsatz kommen. In diesem Zusammenhang können die Administratoren, wie bereits gesagt, auch einstellen, dass der Code innerhalb eines bestimmten Zeitraums gescannt werden muss, um die Umstellung auf eine andere Authentifizierungsmethode zu forcieren. Alternativ besteht auch die Option, Benutzern, die

sich erfolgreich angemeldet haben, direkt zu erlauben, eine neue Authentifizierungsmethode zu aktivieren, ohne dass dazu weitere Maßnahmen erforderlich sind. Das System ist folglich sehr flexibel.

Die Konfiguration der Login-Applikation

Ebenfalls interessant: die Konfiguration der Login-Applikation. Hier lassen sich IP-Address Restrictions einrichten und Spracheinstellungen vornehmen. Außerdem legen die zuständigen Mitarbeiter an dieser Stelle bei Bedarf fest, dass Logins verzögert durchgeführt werden sollen, um Brute Force-Angriffe zu erschweren. Darüber hinaus haben die zuständigen Mitarbeiter bei der Konfiguration der Login Applikation auch die Option, sämtliche Einstellungen zu den Self Services vorzunehmen und so beispielsweise den Anwendern zu erlauben, Login-Informationen zu ändern, ihr Passwort anzupassen und so weiter.

Die Admin-Applikation

Kommen wir jetzt noch einmal kurz auf die zuvor bereits angesprochene IAM-Konfigurationsoberfläche zurück. Diese bietet unterschiedliche Rollen für einzelne Administratorkonten, über die sich die Zugriffsrechte auf die Funktionen innerhalb der Administrationsanwendung granular vergeben lassen. So stehen beispielsweise die Rollen „useradmin“, „tokenadmin“, „helpdesk“, „sysadmin“ und „superadmin“ und diverse Kombinationen daraus zur Verfügung. Das macht es einfach, dafür zu sorgen, dass nur die Anwender Zugriff auf die jeweiligen Funktionen der IAM-Lösung erhalten, die diesen auch wirklich brauchen.

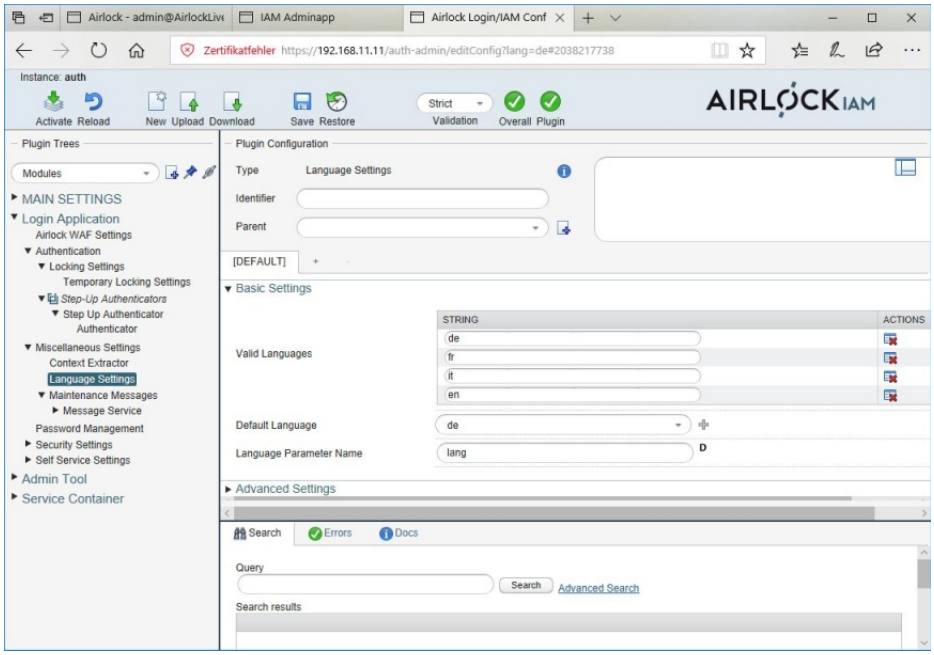
Der Life Cycle eines Benutzerkontos

Gehen wir nun exemplarisch auf die Verwaltung eines Benutzerkontos über seine gesamte Lebensdauer hinweg ein. Zunächst einmal haben die Benutzer (wenn das System entsprechend konfiguriert wurde) die Möglichkeit, über die Login-Applikation selbst ein Konto anzulegen, indem sie sich beispielsweise mit ihrem Benutzernamen oder ihrer E-Mail und einem Passwort registrieren. Im Test funktionierte das ohne Probleme. Die Selbstregistrierung ist sehr flexibel konfigurierbar, da alle Organisationen andere Anforderungen für ihre Benutzerkonten haben. Manche verlangen neben dem Namen auch eine Adresse oder eine Firma und ähnliches.

Wurde das Konto angelegt, so erhält der User bei einer typischen Konfiguration erst einmal einen Basiszugang. Gleichzeitig schickt ihm IAM einen Brief mit einem zu scannenden Code. Nachdem über diesen Scan die Richtigkeit der Adresse bestätigt wurde, hat er die Option, mit seinem Konto voll auf die bereitgestellten Anwendungen zuzugreifen. All diese Schritte lassen sich ohne Unterstützung durch das Helpdesk automatisch durchführen.

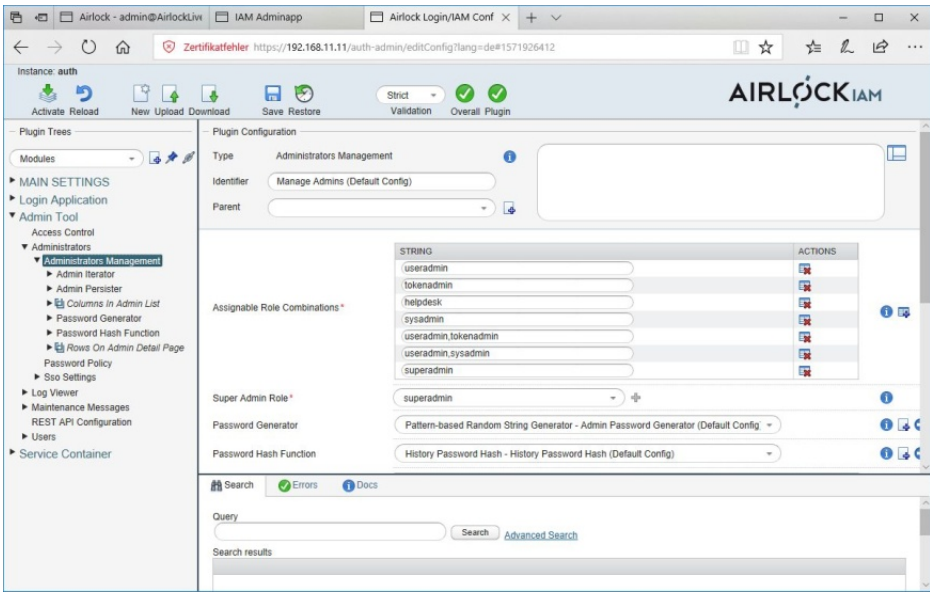
In diesem Zusammenhang ist auch die Self Unlock-Funktion von Interesse: Hier kann sich der Anwender mit dem zweiten Authentifizierungsfaktor einen zusätzlichen Versuch freischalten lassen, um sein zuvor vergessenes Passwort einzugeben. Damit lässt sich ein – etwa wegen drei falschen Passworteingaben – gesperrtes Konto wieder freischalten, wenn dem Benutzer sein Passwort später wieder einfällt, ohne dass das Helpdesk dazu aktiv werden muss.

Wird eine Passwort-Policy geändert, so können die Verantwortlichen die Benutzer nachträglich jederzeit zwingen, ihre Passwörter so zu ändern, dass sie der neuen Policy entsprechen. Wie angesprochen, besteht auch die Option, die Benutzer zum Wechsel ihrer Authentifizierungsme-



Das Konfigurationsinterface für die Login-Applikation

thoden zu zwingen oder ihnen die Möglichkeit zu geben, selbst Authentifizierungsmethoden zu ihrem Konto hinzuzufügen. Bei Bedarf stehen auch Funktionen für die Token Migration zur Verfügung. Auf diese Weise lassen sich die Konten immer an die aktuellen Gegebenheiten anpassen und praktisch alle Aktionen laufen ohne die Belastung des Helpdesks und seiner Mitarbeiter ab. Abgesehen davon bietet das Self Service-Portal den Nutzern noch eine Vielzahl anderer Funktionen, beispielsweise zum Ändern ihrer persönlichen Daten oder auch zum Löschen ihres Kontos. Im Test ergaben sich dabei keinerlei Schwierigkeiten.



Das Konfigurationsinterface für die Administrationsoberfläche

Weitere wichtige Funktionen

Gehen wir nun noch etwas genauer auf einige der wichtigsten Features der IAM-Lösung für Administratoren ein. Das Tool stellt unter anderem unterschiedliche Konfigurationskontexte zur Verfügung. Damit lassen sich innerhalb der Konfiguration verschiedene Verhaltensweisen abbilden.

So ist es beispielsweise möglich, bei einer Benutzeranmeldung mit E-Mail-Adresse und Passwort anhand des Mail-Suffixes das Unternehmen zu bestimmen, bei dem der Benutzer, der sich gerade anmeldet, arbeitet und dann von dieser Information die Login-Methode abhängig zu machen, beispielsweise mit oder ohne einen zweiten Authentifizierungsschritt. Bei Bedarf lässt sich auch eine so genannte Step-Up-Authentifizierung einrichten. Sind beispielsweise über eine WAF mehrere unterschiedliche Anwendungen verfügbar, die verschiedene Authentifizierungsanforderungen haben, so sind die Administratoren dazu in der Lage, dafür zu sorgen, dass das System nach dem Login den Zugriff auf die nicht besonders geschützten Applikationen direkt freigibt. Die anderen erscheinen erst dann im Interface, wenn der betroffene Anwender einen zusätzlichen Authentifizierungsschritt durchlaufen hat.

Risiko-basierte Authentifizierung

Interessant ist auch die risiko-basierte Authentifizierung. Die Software sammelt bei Login-Vorgängen eine große Zahl an Daten, wie die Geolocation, den verwendeten Browser, die vorhandenen Cookies, die Zeit und vieles mehr. Anhand dieser Informationen lassen sich die Logins zusätzlich absichern, zum Beispiel fügt das System – wenn entsprechend konfiguriert – einen zweiten Login-Schritt zu einer Anmeldung hinzu, wenn der letzte erfolgreiche Login erst vor kurzer Zeit, aber auf einem anderen Kontinent erfolgte.

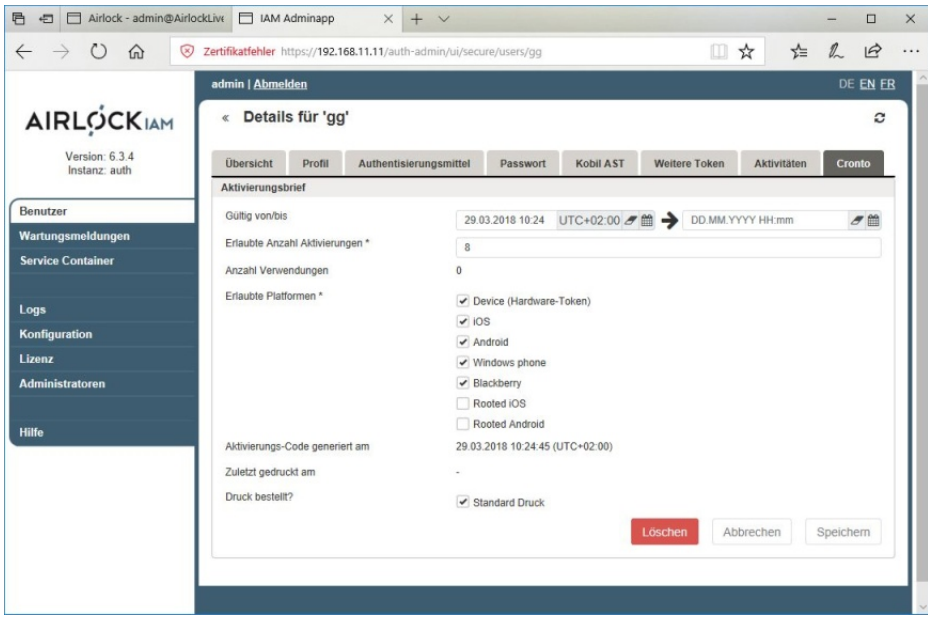
Ebenfalls von Interesse: der so genannte Stealth Mode. Oftmals kommt es vor, dass Login-Anwendungen unfreiwillig Hackern interessante Informationen liefern. Versucht beispielsweise ein Hacker, sich mit einer gültigen E-Mail-Adresse und einem falschen Passwort bei einem Web-Interface anzumelden, so schlägt der Login fehl und das Interface gibt in vielen Fällen die Meldung „Falsches Passwort“ aus.

In diesem Fall weiß der Hacker, dass die E-Mail-Adresse im System existiert und kann sich auf Login-Versuche mit dieser konzentrieren. Deswegen verfügt IAM über einen so genannten „Stealth Mode“, der – falls aktiv – keinerlei Informationen bei fehlerhaften Login-Versuchen zurückgibt. Das ist zwar nicht besonders nutzerfreundlich, erhöht aber das Sicherheitsniveau zusätzlich. Im Test funktionierte es einwandfrei.

Environment Staging

Mit dem Environment Staging sind die Administratoren dazu in der Lage, verschiedene Konfigurationen mit identischen Parametern zu verwenden. Das ergibt unter anderem Sinn, wenn eine bestehende Konfiguration aus ei-

ner Testumgebung in eine Produktivumgebung übergehen soll. In diesem Fall kann ein Großteil der Parameter gleichbleiben, in der Regel ändern sich aber ein paar Einstellungen wie die URLs oder auch die Adressen der Datenbank-Server, da diese in der Testumgebung anders lauten als in der Produktion. Das Environment Staging bringt hier eine große Arbeitserleichterung, da nicht alle Konfigurationsparameter manuell angepasst werden müssen. Bei Bedarf besteht sogar die Option, die nicht zu modifizierenden Parameter zu "locken" (also „abzusperren“), was Änderungen an ihnen unmöglich macht. Auf diese Weise schließt das System viele Fehlerquellen aus und erhöht das Sicherheitsniveau. Es gibt auch die Möglichkeit, ganze Konfigurationen als Zip-Dateien zu exportieren und dann an anderen Orten einzuspielen. Im Test traten bei der Arbeit mit dem Environment Staging keinerlei Probleme auf.



Die Managementoptionen für die CrontoSign-Authentifizierung mit Gültigkeitsdauer des Aktivierungsbriefs, den erlaubten Plattformen und ähnlichem

Use Cases

Im nächsten Schritt des Tests verwendeten wir die vom Hersteller bereitgestellte Demoinstallation mit dem Online Bookshop „BuggyBook“. Für unseren ersten Use Case wechselten wir in dieser Testinstallation auf die Seite https:// {IP-Adresse des Servers} / buggybook-withlogin, die es uns ermöglichte, uns über die Login-Anwendung von IAM bei dem Bookstore anzumelden.

Zunächst versuchten wir nun einen Login mit Benutzername und Passwort und verwendeten dazu folgerichtig einen Test-Account, den wir zuvor über das Web-Interface nur für diese Login-Methode konfiguriert hatten. Das funktionierte einwandfrei.

Nachdem wir auf diese Weise die Funktionsfähigkeit unserer Testinstallation sichergestellt hatten, wandten wir uns etwas komplizierteren Login-Methoden zu. Im zweiten Use Case wollten wir einen Login mit Benutzername und Passwort durchführen, der zusätzlich durch den Google Authenticator geschützt wurde.

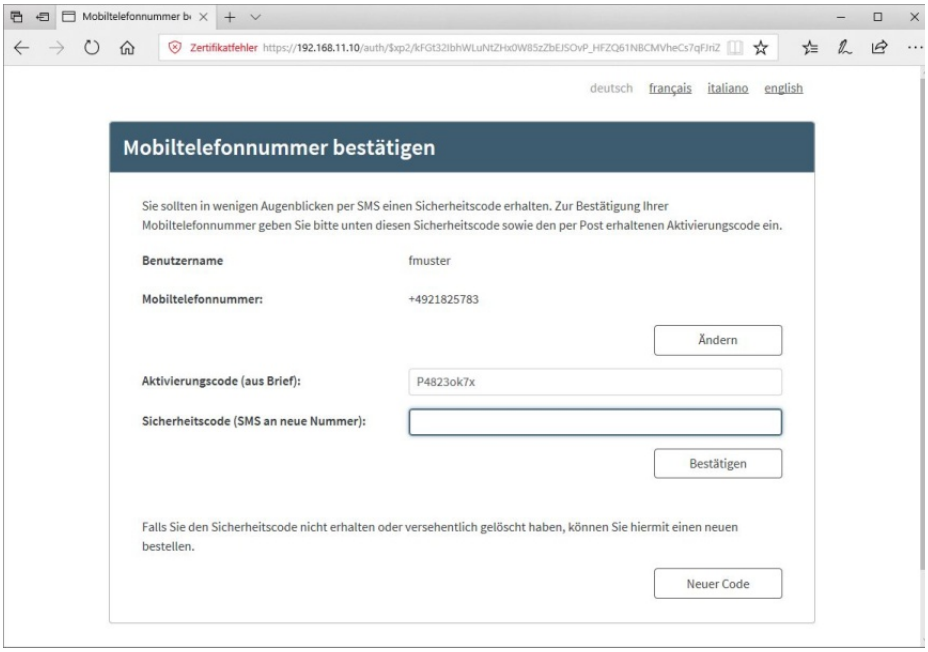
Dazu installierten wir zunächst einmal die Google Authenticator-App auf einem Android Smartphone vom Typ Huawei P9. Danach loggten wir uns wieder bei dem Bookstore ein, landeten aber, da wir ein Konto verwendeten, das wir für die Arbeit mit dem Google Authenticator konfiguriert hatten, nicht gleich im Buch-Geschäft, sondern auf einer Seite mit einem QR-Code.

Diesen Scannten wir mit unserem Smartphone, um den User auch in der Google Authenticator App anzulegen. Danach zeigte uns diese App einen Sicherheits-Code an, den wir im Web Interface der IAM-Lösung eingaben, anschließend waren wir authentifiziert. Es ist übrigens nicht nötig, bei jedem Login den Weg über den QR-Code zu gehen. Kennt die Authenticator App den User bereits, so verlangt das System direkt nach dem Abfragen von Benutzernamen und Passwort nach dem Sicherheitscode. In diesem Fall ist es nur noch erforderlich, den gerade gültigen in der App nachzusehen (er wechselt in kurzen Abständen) und auf der Webseite einzutragen, danach funktioniert der Zugriff auf den Bookstore.

Der dritte Use Case befasste sich mit Logins mit mTAN und Aktivierungsbrief. Dazu kam ein anderes Benutzerkonto zum Einsatz, das wir zuvor für diese Authentifizierungsart eingerichtet hatten. Der Aktivierungsbrief lag uns als PDF vor und wir loggten uns zunächst mit Benutzernamen und Passwort ein. Danach forderte uns das System auf, eine Handy-Nummer anzugeben und auf "Registrieren" zu klicken. An diese Handy-Nummer würde nun in einer Produktivumgebung eine SMS mit einem Code geschickt, den die Benutzer später mit an-

geben müssten. Da wir in unserer Testumgebung keinen SMS-Gateway hatten, mussten wir uns anders behelfen, um diesen Code in Erfahrung zu bringen.

Wir meldeten uns als Administrator beim IAM-Konfigurationswerkzeug an und schauten im Log der Admin-App nach, welcher Code erwartet wurde. Danach wechselten wir wieder zur Login-Anwendung. Diese fragte uns jetzt nach dem Code aus dem Aktivierungsbrief und dem Sicherheitscode aus der SMS.



Nach dem Versenden der SMS fragt das System nicht nur nach dem Code aus dem Aktivierungsbrief, sondern auch nach dem per SMS übermittelten Sicherheitscode. So sorgt das System für eine Validierung der Adresse, an die der Brief ging und der Mobilfunknummer, an die die SMS geschickt wurde.

Danach war unsere Telefonnummer im System registriert und wir konnten uns normal anmelden. Dazu war es nur noch erforderlich, uns mit Benutzernamen und Passwort einzuloggen und den SMS-Code einzugeben, den das System anschließend verschickte. Anschließend konnten wir auf den Bookstore zugreifen. Diese Funktionalität ermöglicht es den Verantwortlichen, die Validität sowohl der Mobilfunknummer als auch der Adresse zu überprüfen.

Der letzte Use Case befasste sich mit einer Stepup Authentifizierung. Das ergibt Sinn, wenn zusätzliche Sicherheit bei bestimmten Aktionen gewünscht wird. In unserem Fall verwendeten wir eine Stepup Authentifizierung mit Google Authenticator, um den Checkout des virtuellen Einkaufswagens des Book Stores zusätzlich zu sichern.

Dazu passten wir zunächst einmal das Mapping innerhalb der WAF-Konfiguration an, da diese die Stepup Authentifizierung starten muss, wenn die Checkout-Seite des Buchladens aufgerufen wird. Danach meldeten wir uns bei dem Bookstore an, fügten ein Buch zu unseren Einkäufen hinzu und wechselten zum Checkout. Daraufhin fragte uns das System nach einem Token. Wir sahen zu diesem Zeitpunkt in der Authenticator App nach, welches Token gerade gültig war, gaben dieses ein und hatten daraufhin das Buch gekauft.

Diese Beispiele zeigen, dass sich das IAM-System in Verbindung mit der WAF nutzen lässt, um viele Aktionen bei der Arbeit mit Web-Anwendungen abzusichern und sogar um für kritische Tätigkeiten nochmals extra Authentifizierungsschritte durchzuführen. Das alles funktioniert, ohne dass dazu die Konfiguration der geschützten Applikationen selbst modifiziert werden muss.

Fazit

Das IAM-System von Airlock lässt sich sehr flexibel einsetzen. Es unterstützt eine große Zahl an Authentifizierungsmethoden, die sich beliebig kombinieren lassen und verfügt zudem über einen sehr großen Funktionsumfang.

Insbesondere die Self Service-Funktionen sind positiv zu erwähnen, da sie dem Helpdesk viel Arbeit abnehmen. Aber auch die REST-API-Unterstützung sollte auf keinen Fall vergessen werden.

Schließlich spielt die Automatisierung heutzutage auch im IT-Umfeld eine immer größere Rolle und die Entwicklung geht immer mehr von grafischen Benutzeroberflächen zu DevOps und von traditionellen Anwendungen zu APIs. Die IAM-Lösung deckt praktisch alle in diesem Zusammenhang auftretenden Szenarien ab und sorgt gemeinsam mit der WAF des gleichen Herstellers für eine umfassende Applikationssicherheit.

Dr. Götz Güttich leitet das Institut zur Analyse von IT-Komponenten (IAIT) in Korschenbroich. Sein Blog: http://sysbus.eu.