Privilegierte Benutzerkonten im Griff

Dr. Götz Güttich

Privilegierte Benutzerkonten wie lokale Administrator-Accounts stellen ein Sicherheitsrisiko dar. Auch die Konten von Service Providern, die via Remote-Management auf die Systeme eines Unternehmens zugreifen, bringen in der Praxis Probleme mit sich. Angreifer können diese Accounts hacken und die damit verbundenen Rechte nutzen, um auf die Daten der betroffenen Organisation zuzugreifen. Diese Bedrohung gewinnt durch die ständig steigende Zahl der gezielten Angriffsversuche immer mehr an Bedeutung. Gleichzeitig steigen neben den Anforderungen an die Compliance auch die Risiken durch die zunehmende Nutzung extern gehosteter Anwendungen sowie Cloud-Dienste. Lösungen zum Management privilegierter Zugriffe nehmen sich dieser Problematik an. Wir haben uns angesehen, was die AdminBastion Suite von Wallix in diesem Zusammenhang leistet.

Bei der AdminBastion Suite (WAB Suite) von Wallix handelt es sich um eine solche Lösung zum Privileged Access Management (PAM). Sie übernimmt die Passwort-Verwaltung, sichert den Zugriff auf wichtige Daten und Systeme ab und behält die Aktivitäten, die über privilegierte Benutzerkonten ablaufen, in Echtzeit im Auge. Dabei spielt es keine Rolle, ob diese Benutzer intern arbeiten oder von extern kommen.

Konkret umfasst die WAB Suite drei Schlüsselkomponenten, den Passwort Manager, den Session Manager und den Access Manager. Diese drei Bestandteile sorgen im Betrieb dafür, dass die richtigen Anwender zum richtigen Zeitpunkt Zugriff auf die richtigen Ressourcen erhalten. Der WAB Password Manager speichert die Zugangsdaten für Administratorkonten, lokale Accounts und Datenbankadministratorkonten in einem zentralen Tresor, der in Frankreich eine ANSSI- und in Russland eine FSTEK-Zertifizierung erhalten hat. ANNSI arbeitet eng mit dem deutschen Behörden im Bereich Cybersicherheit zusammen und ist das französische Pendant zum deutschen BSI (Bundesamt für Sicherheit in der Informationstechnik). Dort lassen sie sich über eine einzelne Konsole verwalten, also erzeugen, verstecken, anzeigen oder verändern. Die Endanwender bekommen die Passwörter im normalen Betrieb nicht zu Gesicht, deswegen ist es möglich, automatisch lange, komplexe, zufällige Strings zu verwenden.

Der WAB Session Manager verwaltet und überwacht alle Zugriffe privilegierter User auf Geräte und Applikationen im Netz und stellt dabei das Auditing sicher. Das Monitoring – und damit auch das Alerting – laufen in Echtzeit ab. Jeder

Zugriff wird stets einer eindeutigen Identität zugeordnet, so dass die Möglichkeit besteht, jeden Anwender für seine Taten zur Verantwortung zu ziehen.

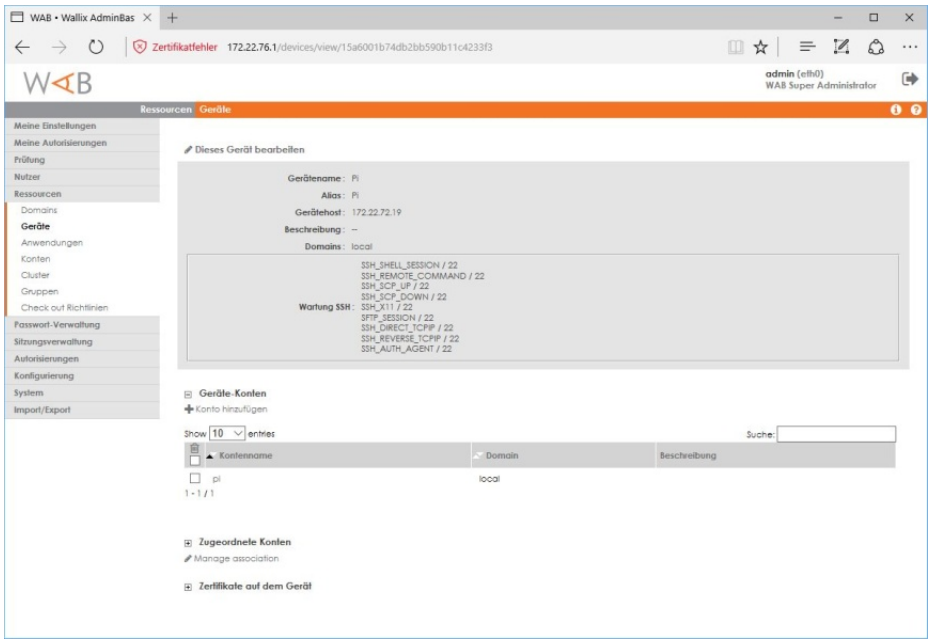
Der WAB Access Manager stellt schließlich ein Web-Portal dar, über das die Benutzer auf alle Ressourcen, die sie benötigen, zugreifen können. Das Privileged Access Management funktioniert dabei über mehrere Sites, Kunden oder auch Netzwerke hinweg. Damit eignet sich das Produkt sowohl für den Einsatz bei Cloud-Providern, als auch für die Verwendung bei End-Usern. Der Zugriff auf die gewünschten Systeme wird im Betrieb über einen einzelnen Klick hergestellt.

Der Test

Für den Test stellte uns Wallix eine Appliance zur Verfügung, auf der die WAB Suite vorinstalliert war. Wir integrierten diese Appliance in unsere Umgebung, machten uns mit dem Leistungsumfang der Lösung vertraut und verwalteten mit ihr privilegierte Benutzerkonten bei uns im Netz. Darüber hinaus zeichneten wir diverse Sitzungen bei der Nutzung dieser Konten auf und testeten die Monitoring-Funktionen.

Inbetriebnahme

Zur Inbetriebnahme des Produkts genügt es, die Appliance oder die virtuelle Appliance (in dieser Form ist das Produkt ebenfalls erhältlich) ins Netz zu integrieren und hochzufahren. Anschließend meldeten wir uns bei der lokalen Konsole des Debian-Linux an, das die Wallix-Appliance als Betriebssystem nutzt und passten die Netzwerkkonfiguration des Systems an unsere Umgebung an. Sobald das erledigt war, konnten wir uns über die neue IP-Adresse mit dem Web-Konfigurationswerkzeug der Lösung verbinden. Nach dem Login machte uns



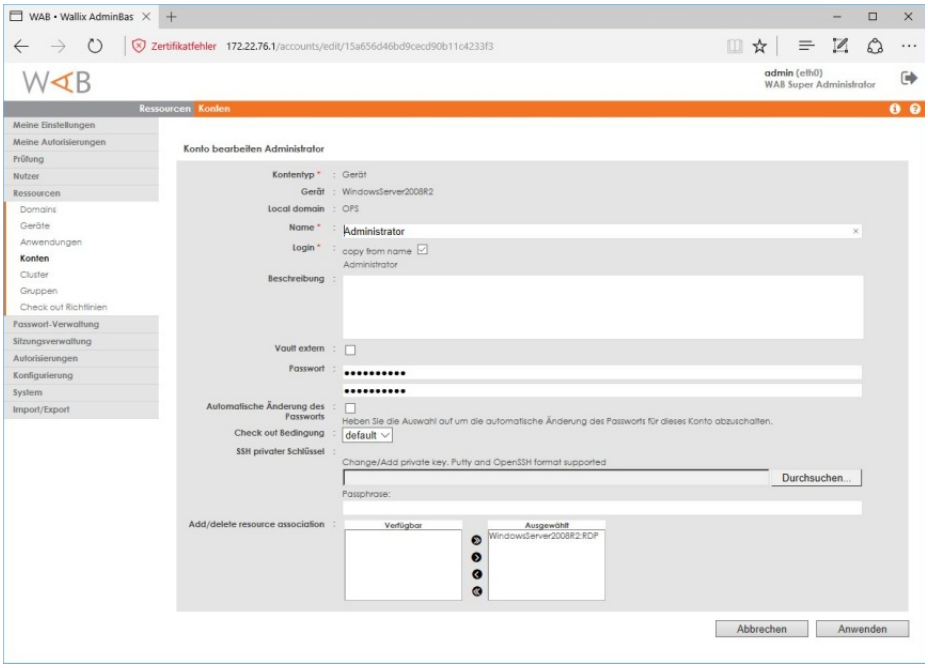
Das Gerätekonto für den SSH-Zugriff auf einen Rasberry-Pi unter Linux

das Konfigurations-Tool als erstes darauf aufmerksam, dass wir das Default-Passwort (admin) des Admin-Kontos ändern müssten. Das ergibt Sinn, um sicher zu stellen, dass keine Produkte mit Default-Passwörtern in den Produktivbetrieb gehen. Nachdem wir das Passwort geändert hatten, konnten wir mit der praktischen Arbeit beginnen.

Die Appliance arbeitet im Betrieb als virtueller Proxy, das heißt, die Anwender greifen auf die Wallix-Lösung zu und diese stellt dann eine Verbindung zu dem jeweils gewünschten Zielsystem her. Damit eignet sich das Produkt gleichermaßen für Dienstleister und interne Administratoren in mittelständischen Betrieben. Die Konfiguration der einzelnen Zielrechner muss nicht notwendigerweise geändert werden, so dass direkte Logins auf Wunsch auch weiterhin noch funktionieren. Es gibt aber auch die eben erwähnte Möglichkeit, die Passwortverwaltung zu automatisieren und komplett in die Hände der WAB Suite zu legen, in diesem Fall funktionieren die Zugriffe nur noch über die Wallix-Lösung. Darauf gehen wir später noch genauer ein.

Im Test machten wir uns zunächst daran, den Leistungsumfang des Managementwerkzeugs unter die Lupe zu nehmen. Die Lösung arbeitet mit einer Menüstruktur auf der linken Seite, über die sich alle Funktionen des Wallix-Produkts erreichen lassen. Während wir uns mit den einzelnen Menüpunkten vertraut machten, brach plötzlich die Verbindung zur Appliance ab. Nachdem wir uns erneut bei

der lokalen Konsole des Servers angemeldet hatten, stellten wir fest, dass die Lösung



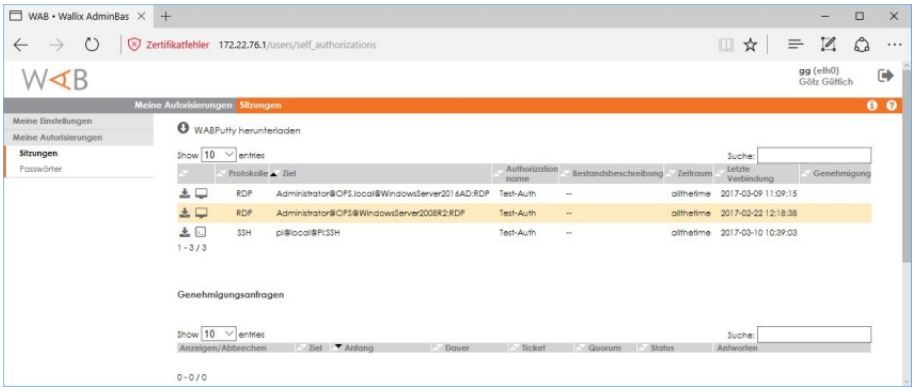
Ein Windows-Administratorkonto für RDP-Zugriffe

ihre alte Netzwerkkonfiguration, die in einem anderen Subnetz lag als unsere Testumgebung, wiederhergestellt hatte. Deswegen nahmen wir die Netzwerkkonfiguration erneut vor, verbanden uns nochmals mit dem Web-Interface und passten auch hier in den Netzwerk-Settings nochmals die Netzwerkeinstellungen an. Danach blieb die Netzwerkanbindung stabil.

Die Verbindung zu einem Windows-Server

Nachdem alles wie gewünscht lief, gingen wir daran, zwei Verbindungen zu einem System unter Debian-Linux und einem Rechner, der mit Windows Server 2016 lief, einzurichten. Der Windows Server sollte über RDP angesprochen werden, der Linux-Rechner mit Hilfe von SSH.

Um die RDP-Verbindung einzurichten, wechselten wir zunächst nach "Nutzer/Konten" und fügten der Appliance ein Benutzerkonto mit normalen User-Rechten hinzu. Über dieses Konto konnten sich die Anwender später bei dem Wallix-System anmelden um



Nach dem Login als User erhält man eine Liste der freigebenen Client-Systeme

auf die für sie freigegebenen Rechner zuzugreifen. Danach legten wir gleich auch eine Gruppe an, in die unsere lokalen Nutzerkonten eingeordnet werden sollten. Mit Hilfe der Gruppen ist es möglich, bestimmten Anwendern – beispielsweise den Mitarbeitern der IT-Abteilung oder auch externen Usern – im Netz andere Rechte zuzugestehen als anderen.

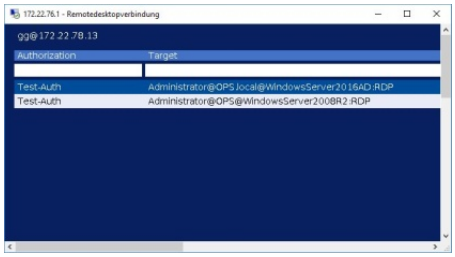
Anschließend gingen wir nach "Ressourcen/Geräte" und legten dort ein neues Gerät an. Diesem gaben wir den Namen "Windows2016AD", da es sich um einen Active Directory-Controller handelte. Außerdem trugen wir die IP-Adresse und die Domäne ein.

Als nächstes wählten wir das benötigte RDP-Protokoll aus. An dieser Stelle unterstützt das System neben RDP und SSH auch Telnet, RLOGIN und VNC. Falls erforderlich sind die zuständigen Mitarbeiter bei der Konfiguration der Protokolle dazu in der Lage, die verwendeten Ports und ähnliches anzugeben.

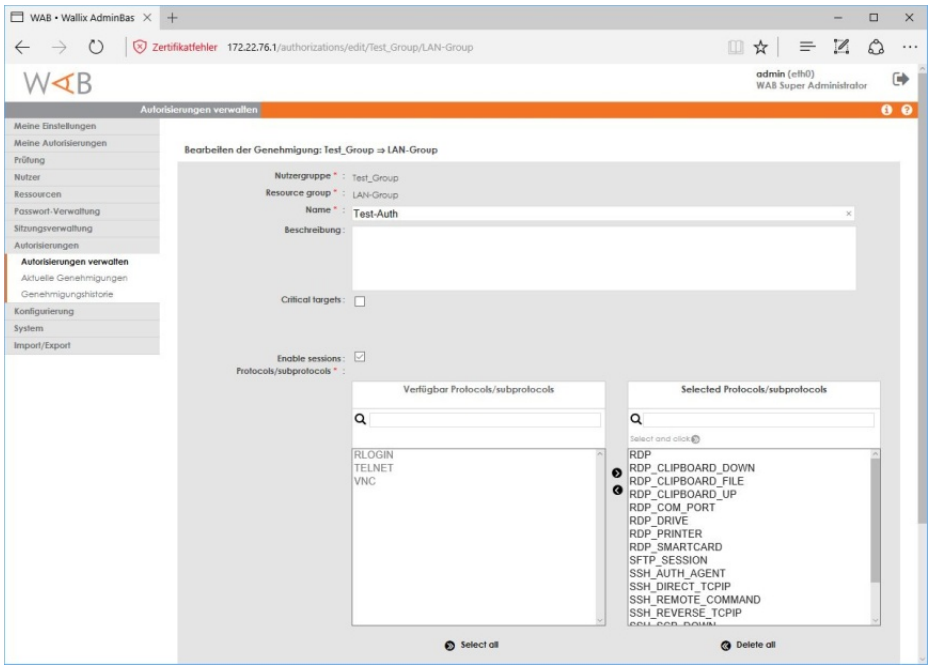
Sobald das Gerät existierte, konnten wir uns daranmachen, nach "Ressourcen/Konten" zu wechseln und dort für das neue Gerät ein Gerätekonto anzulegen. Dieses kam zum Einsatz, um den Login beim Endgerät durchzuführen. Da wir ja mit der Wallix-Lösung unsere privilegierten Konten absichern wollten, verwendeten wir zu diesem Zweck das Administrator-Kon-

to des Windows Servers. An dieser Stelle ist es auch möglich, neben Passwörtern private Schlüssel, beispielsweise für SSH-Konten, oder auch Passphrasen zu hinterlegen. Nachdem wir unser Konto mit Passwort und Beschreibung eingerichtet hatten, wiesen wir es direkt unserem Gerät zu.

Im Rahmen der Gerätekontenkonfiguration besteht auch die Option, die bereits erwähnte automatische Passwortänderung zu aktivieren. Damit ist es möglich, der Wallix-Lösung die Passwort-Verwaltung für die privilegierten Konten (oder auf Wunsch auch für alle Konten, bei den privilegierten Accounts ergibt es aber am meisten Sinn) komplett zu überlassen. Dazu müssen lediglich die Komplexität der Passwörter konfiguriert und die automatische Passwort-Änderung aktiviert werden. Danach erzeugt AdminBastion für alle betroffenen Konten in regelmäßigen Abständen – das Intervall ist dabei definierbar – entsprechende Passwörter, legt sie in seinem Passwort-Vault ab und aktiviert sie auf den betroffenen Zielsystemen. In diesem Fall sind die Passwörter den Nutzern nicht mehr bekannt und sie können ausschließlich über das Wallix-Produkt auf ihre Rechner zugreifen.



Greift man per RDP-Client auf die WAB Suite zu, so erhält man eine Liste der für das jeweilige Konto freigegebenen RDP-Clients



Für unsere Test-Gruppe gaben wir die Protokolle RPD und SSH frei

Nach dem Definieren des Gerätekontos legten wir unter "Ressourcen/Gruppen" eine neue Gruppe an und fügten ihr den neuen Account hinzu, um ihn für die User nutzbar zu machen. Zum Schluss wandten wir uns noch dem Punkt "Autorisierungen/Autorisierungen verwalten" zu, erzeugten auch hier eine Gruppe und schalteten für diese das RDP-Protokoll frei. Gleichzeitig aktivierten wir mit dem Session-Recording eines der Highlights des Wallix-Produkts, auf das wir später noch genauer eingehen werden. Damit war die erste Verbindung einsatzbereit.

Der erste Zugriff

Um die neue Verbindung zu nutzen, loggten wir uns nun mit unserem zuvor angelegten Benutzerkonto bei der Appliance ein und landeten in einem Web-Interface, das über zwei Menüpunkte verfügte. Der erste nennt sich "Meine Einstellungen" und ermöglicht es, die Sprache, die für das jeweilige Konto Verwendung finden soll, festzulegen und die E-Mail-Adresse des Anwenders anzugeben. Außerdem lassen sich hier auch SSH- und GPG-Keys hinterlegen.

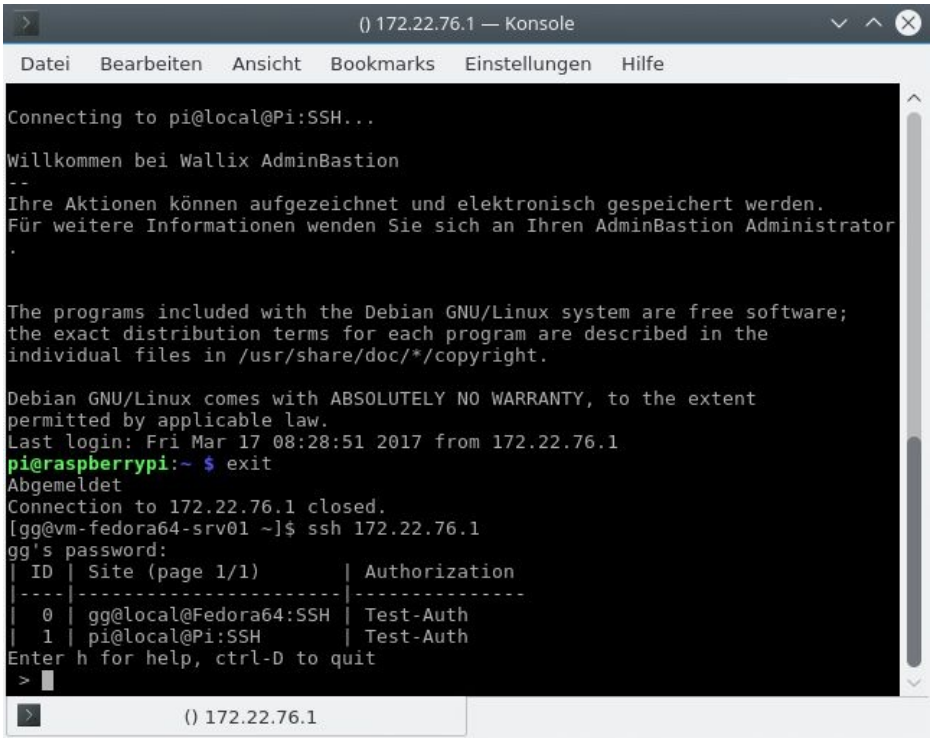
Interessanter ist der Punkt "Meine Autorisierungen", denn dieser enthält in Form einer Liste alle Systeme, auf die das jeweilige Benutzerkonto zugreifen darf, in unserem Fall war das zu diesem Zeitpunkt logischerweise nur der Windows Server.

Die genannte Liste umfasst neben dem Namen des Systems auch Informationen wie beispielsweise das zu verwendende Protokoll und die letzte Verbindung. Außerdem stellt es für jedes Zielsystem zwei Icons bereit. Das eine ermöglicht den Download einer RPD-Konfigurationsdatei, über die sich die Verbindung über einen einfachen Klick

aufrufen lässt. Verwendet ein User diesen Weg, muss er aber immer sein Passwort eingeben, um die Verbindung aufzubauen. Alternativ können die Verantwortlichen auch über das zweite Icon eine Sofortverbindung herstellen. Dazu wird kein Passwort gebraucht, der Zugriff funktioniert aber nur innerhalb von 30 Sekunden, danach verliert er seine Gültigkeit. Im Test funktionierten beide Methoden auf Anhieb.

RDP-Zugriffe lassen sich übrigens nicht nur über das Web-Interface realisieren. Es besteht auch die Möglichkeit, sich mit einem RDP-Client direkt bei der Appliance einzuloggen.

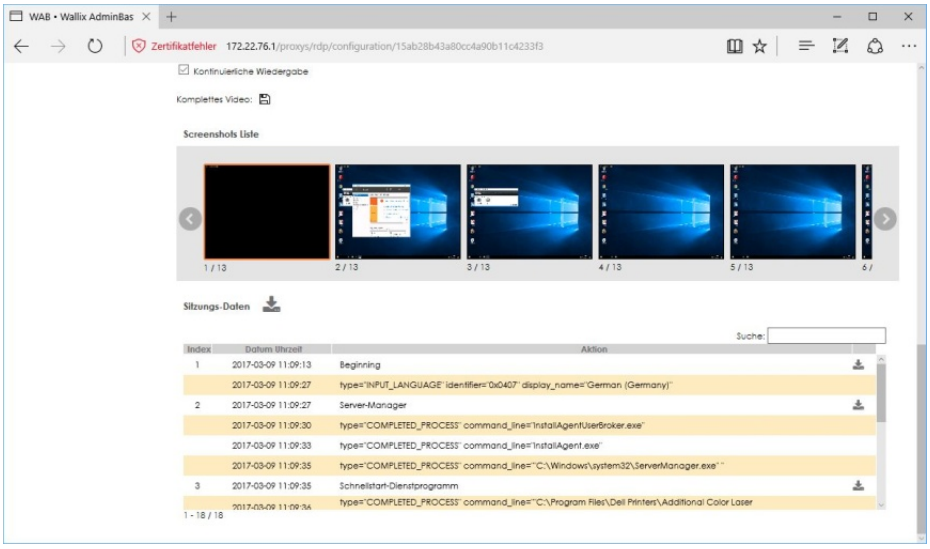
Die Wallix-Lösung bietet dann in einer Liste die RDP-Zielsysteme an, auf die das betroffene Konto zugreifen darf und stellt per Tastendruck die Verbindung her. Bei Bedarf besteht auch die Option, über einen Windows-Jump-Server mit installierten Terminaldienste- oder Remote Desktop-Rollen mit der WAB Suite einzelne Applikationen via RDP im Netz verfügbar zu machen.



Nach dem SSH-Login bei der Appliance von Linux aus zeigt das System eine Liste der freigegebenen SSH-Targets und ermöglicht so den Verbindungsaufbau

Die Konfiguration des SSH-Zugriffs

Als nächstes machten wir uns an die Konfiguration des SSH-Zugriffs auf unseren genannten Debian-Server. Das läuft ähnlich wie bei der RDP-Konfiguration. Zuerst legten wir das Gerät mit IP-Adresse und Namen an. Hier aktivierten wir anstelle des RDP-Protokolls aber natürlich SSH. Danach ging es daran, das Gerätekonto mit Passwort und ähnlichem zu definieren, an dieser Stelle verwendeten wir dazu den root-Account des Servers und deaktivierten auch gleich wieder die automatische Passwortänderung. Nachdem wir das neue Konto zu dem Debian-Gerät hinzugefügt und in die Gruppe aufgenommen hatten, schalteten wir in den Autorisierungen noch das SSH-Protokoll frei, danach war die Verbindung verfügbar.

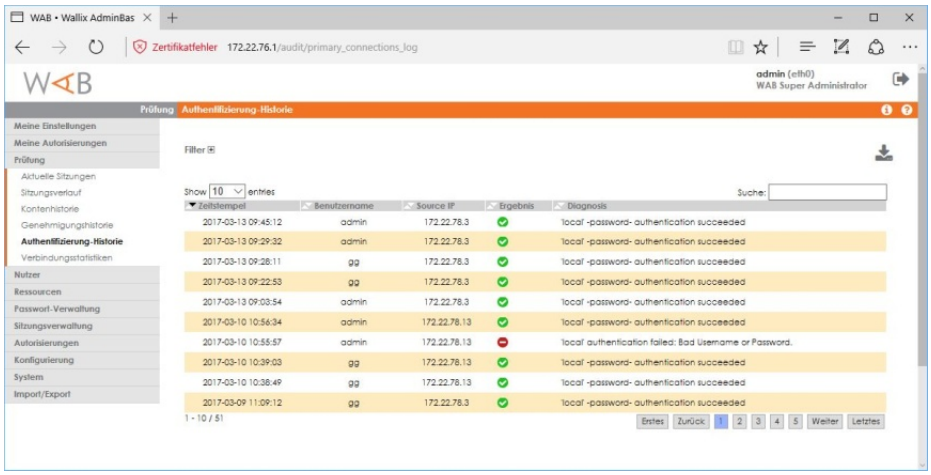


Eine aufgezeichnete RDP-Sitzung

SSH-Zugriff als Benutzer

Der SSH-Zugriff erfolgt in der Praxis etwas anders als die Arbeit mit RDP. Die Anwender können über die Liste ihrer Autorisierungen das SSH-Zielsystem zwar ganz normal aufrufen, der Verbindungsaufbau funktioniert unter Win-

dows aber nur mit einer speziellen Version des putty-Clients, die sich WABputty nennt und die direkt aus dem Benutzerinterface der Appliance heruntergeladen werden kann. Sobald diese auf dem verwendeten Client-Rechner installiert wurde, sind SSH-Zugriffe problemlos möglich.



Umfassende Statistiken, wie hier die Geschichte der Logins und Login-Versuche, helfen dabei, sämtliche Aktivitäten im Auge zu behalten

Ansonsten haben die Anwender auch noch die Option, sich per SSH mit der Wallix-Appliance zu verbinden. Das funktioniert sowohl von Linux aus, als auch mit putty unter Windows. Ähnlich wie bei Zugriffen mit dem RDP-Client präsentiert die Appliance den Anwendern dann eine Liste mit den verfügbaren Zielsystemen und stellt nach der Selektion eines Eintrags die Verbindung her.

Der weitere Test

Im weiteren Verlauf des Tests machten wir uns mit der Funktionalität der Wallix-Lösung im Detail vertraut, arbeiteten mit den Aufzeichnungsmöglichkeiten für die Sitzungen und fügten unserer Umgebung noch weitere Zielsysteme, beispielsweise unter Windows Server 2008 R2 und Fedora Linux, hinzu.

Es würde den Rahmen des Tests sprengen, genau auf jedes einzelne Feature der Lösung einzugehen, es ergibt an dieser Stelle aber Sinn, nochmals auf die Recording-Features des Produkts hinzuweisen. Loggt sich ein berechtigter User bei der Appliance ein, so hat er die Möglichkeit, in den Bereich "Prüfung" zu wechseln und dort eine Liste der aktuellen Sitzungen und den Sitzungsverlauf in der Vergangenheit einzusehen.

Dabei besteht – falls die entsprechende Funktion aktiviert wurde – die Option, für jede Sitzung den Verlauf im Detail zu analysieren. Bei SSH-Sitzungen steht dieser in Form von Text- und ttyrec-Dateien zur Verfügung. In diesem Zusammenhang müssen wir die Unterstützung von ttyrec besonders positiv hervorheben, da dieses Tool es nicht nur möglich macht, die eingegebenen Befehle zu lesen, sondern sie auch in Echtzeit auf einer Konsole ausgeben kann, so dass der Administrator jederzeit sieht, was wann genau geschehen ist.

Für RDP-Verbindungen legt die WAB-Suite Flash-Videos an, die sich direkt im Web-Interface einsehen und auch herunterladen lassen. Darüber hinaus stellt sie auch aus den Videos generierte Screenshots zur Verfügung, die anhand erkannter Aktionen erstellt werden. Auch hier ist also jederzeit klar, welche Aktionen wann durchgeführt wurden, was dabei hilft, Auditings durchzuführen und die Compliance sicher zu stellen. Umfassende Statistiken zu den Verbindungen, die beispielsweise die Zahl der WAB-Connections pro Benutzer sowie die Zielverbindungen nach Dauer oder auch nach Datum visualisieren, runden das Informationsangebot der Appliance ab.

Fazit

Im Test hinterließ die Wallix AdminBastion einen ausgesprochen guten Eindruck. Das Produkt ermöglicht nicht nur den problemlosen uns sicheren Zugriff auf die privilegierten Benutzerkonten der vorhandenen Netzwerkkomponenten, sondern übernimmt auch das Passwort Management und stellt auf Wunsch Anwendungen im Netz bereit. Umfassende Funktionen zum Auditing, die genau belegen, wer wann was getan hat, runden den Leistungsumfang der WAB-Suite ab.

Dr. Götz Güttich ist Chefredakteur von Sysbus.eu. Außerdem leitet er das Institut zur Analyse von IT-Komponenten (IAIT).