10 | 19 Sonderdruck für Ergon Informatik

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

Airlock WAF

www.it-administrator.de

Airlock WAF

Sicherheits-inspektor

von Frank-Michael Schlede und Thomas Bär

Quelle: boris15 – 123RF

Schon lange gibt es für Virenschutz & Co. neue Namen wie beispielsweise Endpoint Protection und mit einer einfachen Firewall ist auch kein IT-Profi mehr hinter dem Serverrack hervorzulocken – da muss schon mindestens eine Next Generation auftauchen. Schlussendlich schützen diese Programme aber alle vor Schädlingen. Einen Schritt weiter geht Airlock, das Admins sogar vor fehlerhaften Applikationen und unzureichender Programmierung bewahren will.

Aktuelle Entwicklungen, etwa der Einsatz von Mikroarchitekturen wie Containern, werden mittelfristig für eine Erhöhung der Betriebssicherheit sorgen, da es für Administratoren und Webentwickler – in Kombination Devops – immer einfacher wird, das unterliegende System schnell und unkompliziert auszutauschen. Die auf dem Betriebssystem aufsetzenden Webapplikationen gilt es weiterhin, zum Teil selbst zu aktualisieren. Klassische Firewalls schützen die mitunter selbst entwickelten Applikationen nur teilweise – hierfür gibt es die Spezialgruppe der Web Application Firewalls (WAF).

WAF-Systeme kontrollieren den HTTP(S)-Datenverkehr zwischen Netzwerk und dem Applikationsserver und sind in der Lage, den Inhalt zu interpretieren und im Zweifelsfall einzugreifen. Als vorteilhaft zeigt sich auch die Funktion, bei der mehrere Applikationen gleichzeitig von Administratoren mit einer WAF geschützt werden können, und selbst der Weiterbetrieb von Altanwendungen, die sich möglicherweise gar nicht mehr aktualisieren lassen, ist zumindest theoretisch möglich.

Nachteilig indes sind die Gefahren der zunehmenden Unachtsamkeit bei der Programmentwicklung, wenn sich der Developer auf den WAF-Schutz verlässt.

Eingebettet im Herstellerportfolio

Airlock WAF ist eine dieser hochspeziellen Applikationsfirewalls für den Webbetrieb. Hinter den Airlock-Produkten steht die Ergon Informatik AG, ein seit 1984 aktiver Dienstleister aus der Schweiz. Von den aktuell 280 Mitarbeitern, so ist auf der Homepage zu lesen, verfügen über 80 Prozent über einen Hochschulabschluss. Die meisten davon, so heißt es weiter, sind Informatikingenieure der ETH Zürich, einer der zehn Top-Universitäten der Welt. Airlock ist seit dem Jahr 2002 auf dem Markt und bei mehr als 500 Kunden weltweit im Einsatz.

Die Produkte mit dem Namen Airlock ergeben in ihrer Gesamtheit den "Secure Access Hub" zur Absicherung von Organisationen gegenüber Datendiebstahl, Cyberattacken und Angriffen auf Applikationen. Das Airlock API Gateway bietet Schutzmechanismen für Schnittstellen und sichert die Anbindung der unterschiedlichen Systeme. Auf diesem Gateway können IT-Sicherheitsexperten JSON-Schemata und OpenAPI-Spezifikationen hinterlegen und durchsetzen. Funktionen wie Dynamic Value Endorsement (DyVE) erlauben ein dynamisches Whitelisting von zulässigen Werten innerhalb einer API-Interaktion. Auch SOAP/XML-Requests können Administratoren gegen formale Definitionen wie zum Beispiel eine WSDL-Spezifikation automatisch prüfen. Im Zusammenspiel mit Airlock IAM lässt sich eine Zugriffskontrolle realisieren, auf Basis relevanter Standards wie beispielsweise OAuth 2.0 und OpenID Connect 1.0.

Airlock IAM stellt die zentrale Access-Management-Komponente im Secure Access Hub dar. Es ermöglicht Benutzern den sicheren Zugang zu Daten und Anwendungen – mit einmaliger Anmeldung und automatisierter Benutzeradministration. Das SSO-fähige IAM authentisiert kontextabhängig Benutzer und Clients und autorisiert Zugriffe. Neben internen Quellen unterstützt die Software auch extern verwaltete Identitäten wie Social-Login-Profile oder IDs eines Federation-Verbundes wie die in der Schweiz populäre SwissID.

Zentrale Durchsetzung von Sicherheitsrichtlinien

Das von uns getestete Airlock WAF analysiert den Netzwerkverkehr zu den ge-

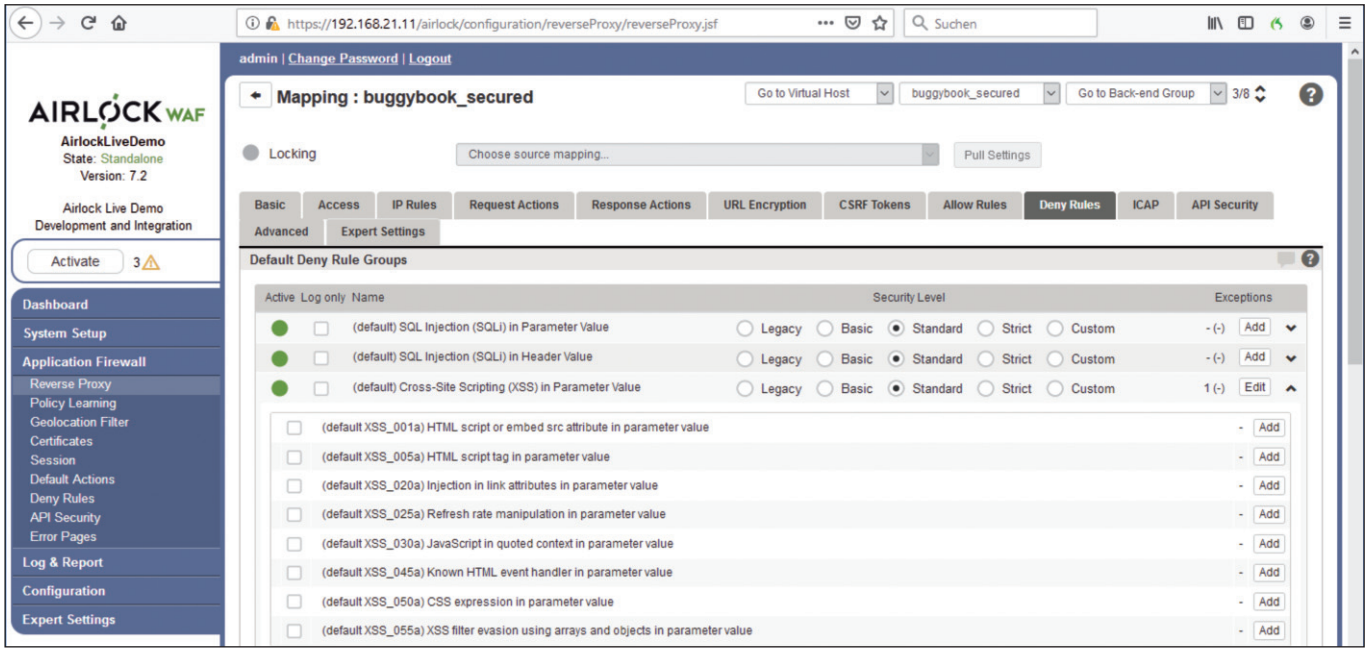

Bild 1: Airlock Web Application Firewall erlaubt umfangreiche Konfigurationsmöglichkeiten.

schützten Services und Applikationen und blockiert Angriffsversuche, ehe sie interne Dienste erreichen können. Airlock WAF bietet umfassenden Schutz gegen Schwachstellen und ermöglicht das zentrale Management von Sicherheitsrichtlinien. Der Hersteller verweist bei den Schwachstellen auf die "OWASP Top 10" – quasi eine Hitliste für Applikations-Vulnerabilitäten –, von Platz 1 heruntergezählt sind dies: Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfigurations, Cross Site Scripting (XSS), Insecure Deserialization, Using Components with known vulnerabilities, unzureichende Logging-Funktionen und fehlendes Monitoring.

Ergon Airlock WAF 7.2

Produkt
Web Application Firewall

Hersteller
Ergon Informatik AG
www.airlock.com

Preis
Airlock WAF kostet in der kleinsten Ausbaustufe 4760 Euro pro Jahr und Backend.

Systemvoraussetzungen
Airlock WAF basiert auf CentOS 7.5. Der Hersteller verweist für die Hardware-Auswahl auf die Red Hat HCL. Für eine Demo-Installation ist eine virtuelle Maschine mit 3 GByte RAM und 18 GByte Festplattenspeicher ausreichend. Eine mittelgroße Einrichtung mit 9000 HTTPS-Sessions erfordert eine 8-Core-CPU mit 2,5 GHz, 32 GByte RAM, zwei 1GBit-NICs und mindestens 200 GByte Festplattenspeicher im RAID-Ausbau. Die Software skaliert bis zu einer RAM-Größe von 256 GByte verfügbaren Arbeitsspeicher.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

Im Zusammenspiel mit IAM übernimmt Airlock WAF die Rolle des zentralen Durchsetzungspunkts für Sicherheitsrichtlinien und stellt sicher, dass jeder Zugriff authentisiert und autorisiert erfolgt. Die vielen Schnittstellen zu Security-Werkzeugen wie SIEM-Systemen, Virenscannern, Threat Intelligence, Fraud-Prevention-Systemen oder HSMs machen Airlock WAF zur zentralen Drehscheibe in jeder Sicherheitsarchitektur.

Testumgebung unter VMware Workstation 15

Ein solch umfassendes System in einer Testumgebung bereitzustellen und sinnvolle Aussagen über die Sicherheitsfunktionen zu treffen, ist nicht ganz einfach. Neben den Schutzsystemen selbst mussten wir eine an sich fehleranfällige Applikation, sinnvollerweise als Web-Lösung, einbinden und Angriffsvektoren erarbeiten und durchspielen. Glücklicherweise unterstützt der Hersteller Evaluierungsinstallationen dieser Art durch ein Gespann von zwei virtuellen Maschinen. Das erspart dem Interessenten, den eigentlichen Installationsvorgang mit Linux aufzusetzen, das Setup der Airlock-Produkte über Anaconda und die Zertifikatspflege.

Unsere Testumgebung ließ sich problemlos unter VMware Workstation 15 auf einem Windows-10-Host in Betrieb nehmen. Einzig ein zusätzliches "Host-Only"-Netzwerk gilt es im virtuellen Netzwerk anzulegen. Alle Zugriffe auf die Managementoberfläche und auf die bewusst mit Lücken und Fehlern geradezu gepflasterte Beispiel-Webseite "Buggy Book Store" erledigt der Nutzer per Browser. Neben einer Zugriffsvariante durch Airlock WAF, bei der sicherheitsrelevante Vorkommnisse lediglich durch die Software zu protokollieren sind, gibt es mit dem "buggybook-secured" eine Konfigurationsvariante, bei der die WAF-Software ihre Schutzfunktion unter Beweis stellt und Missbrauch verhindert.

Dashboard mit Kibana-Grafik

Das AirlockLiveDemo mit der aktuellen Version 7.2 von WAF öffnet der Administrator ganz einfach per Browser. Erwartungsgemäß findet sich ein Dashboard mit grafischen Auswertungen zum Systemzustand, Proxy-Statistiken bezüglich der Sessions und der ein- und ausgehenden Bandbreite. Der Bereich "System Setup" mit Lizenzen, Routing und

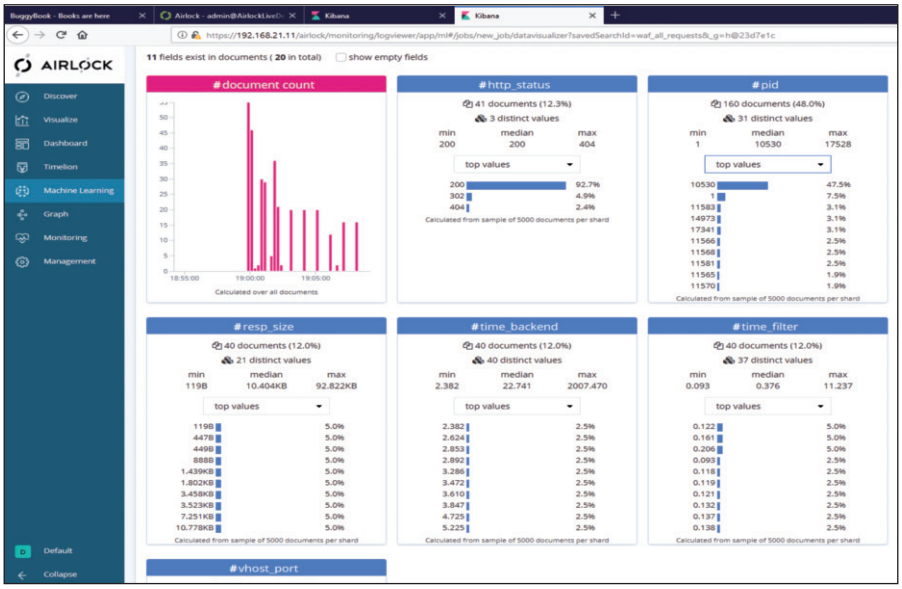

Bild 2: Die enthaltene Kibana-Analyseplattform bietet eine automatische Datenauswertung, um beispielsweise bisher unbekannte Risikobereiche zu identifizieren.

Interfaces sowie dem Zugriff auf den integrierten Software-Update-Mechanismus ist für unsere Testbetrachtung nicht erforderlich.

Im Abschnitt "Log & Report" warten weitere grafische Analysen auf Basis der Open-Source-Plattform Kibana, die die Verarbeitung der gesammelten Mess- und Protokolldaten in allen erdenklichen Qualitäten und Formen erlaubt. Besonders beeindruckend sind die in Kibana enthaltenen "Machine Learning"-Konzepte. Die Lernfunktion wird einfach auf verschiedene Datenbereiche angewandt und mit der Zeit versucht der Server selbstständig, Anomalien in den komplexen Datenstrukturen zu entdecken. Eine solche Untersuchung dauert jedoch seine Zeit, ist aber eine intelligente Erweiterung des Sicherheitskonzepts in Airlock. Kommen beispielsweise immer wieder schädliche Zugangsversuche aus einem bestimmten Netzwerkbereich, macht maschinelles Lernen diese Information möglicherweise sichtbar.

Der sicherlich interessanteste Menüpunkt ist der Abschnitt "Application Firewall". Hier findet der Administrator den Zugang zu den Bereichen Reserve Proxy, Policy Learning, Geolocation Filter, Zertifikate, Sitzungen, Standardreaktionen, "Deny"-Regeln und API-Sicherheit. Außerdem hat er die Möglichkeit, eigene Designs für die Fehlerwebseiten zu hinterlegen.

Komplexe Regelwerke möglich

Der grundlegende Aufbau von Airlock WAF ist logisch nachzuvollziehen. Zunächst gilt es, der WAF eine Webapplikation bekanntzumachen. Dies geschieht durch die Eingaben der IP- und Port-Adresse und der DNS-Namen im Abschnitt "Reverse Proxy". Es folgt die Einrichtung eines virtuellen Hosts, der die Anfragen anstelle der eigentlichen Applikation entgegennimmt.

Danach folgt das Mapping zwischen dem virtuellen Host und dem Backend-Server selbst, dies gelingt durch einfache Mausklicks und die Eingabe der sogenannten Entry- und Backend-Pfade. Insgesamt ist die so entstehende Zuordnung recht flexibel und erlaubt auch den Aufbau asymmetrischer Sicherheitseinstellungen, bei denen untergeordnete Webseiten von der WAF anders zu behandeln sind als beispielsweise übergeordnete Strukturen.

Anschließend folgen 13 Untermenüpunkte mit allen erdenklichen Sicherheitsmöglichkeiten zur Definition von IP-White- und -Black-Lists, unterschiedliche Protokollfunktionen für verschiedene Webroot-Threat-Kategorien, beispielsweise für Tor-Proxy-Interaktionen, Funktionen zur Behandlung von URL-Verschlüsselungen und Allow-Rules-Regelwerke mit der Definition von Parametergrenzwerten für Formulareingaben. Das für unsere Testbetrachtung entscheidende Dialogfenster ist jedoch "Deny Rules" zur Anpassung und Zuweisung von Einstellungen für SQL-Injektion für Parameter, Header, Cross-Site-Scripting, HTML-Injektion, UNIX-Command-Injektion, LDAP-Injektionen, unsichere direkte Objektreferenzen und die Parameter Sanity für Namen und Werte.

Allein für das Dialogfenster "Application Firewall" ist sicherlich eine mehrtägige Schulung vonnöten, um die Tragweite aller Funktionen überhaupt zu erfassen, und dann würden Themen wie Load Balancing und Ausfallsicherheit der Serverstruktur wahrscheinlich noch gar nicht angesprochen. Betrachten wir nun aber die Sicherheitsfunktion in einem praktischen Kontext.

Cross-Site-Scripting verhindern

Unter XSS, der gängigen Abkürzung für das webseitenübergreifende Scripting, bezeichnen Sicherheitsexperten das Ausnutzen einer Computersicherheitslücke in einer Webanwendung, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig gelten. Aus diesem vertrauenswürdigen Kontext lässt sich dann ein Angriff starten. Praktischerweise handelt es sich häufig um die Verwendung von JavaScript-Kommandos, die über Formularfelder zur Ausführung gebracht werden können.

In dem exemplarisch von Ergon verwendeten "Bookstore" gibt es die Möglichkeit, dass sich Benutzer gegenseitig Nachrichten zuschicken können. Nach der Anmeldung und dem Aufruf des entsprechenden Dialogfelds ergänzten wir die Titelzeile unserer Nachricht durch ein Skript-Kommando wie *prompt("Bitte Passwort eingeben")* und sendeten diese Nachricht an einen fiktiven Kollegen. Meldet sich dieser an und verwendet die Nachrichtenfunktion, so erscheint der Eingabedialog nach dem Öffnen der Nachricht. Zugegeben, ein einzelnes Kommando dieser Art stellt kein Sicherheitsrisiko dar, zeigt jedoch, dass es möglich ist, JavaScript-Befehle so aufzurufen, wie es eigentlich nicht möglich sein sollte.

In der geschützten Variante des Buchladens wird nicht der Aufruf der mit dem Skript-Code versehenen Nachricht auf der Empfängerseite verhindert, sondern die Eingabe einer Nachricht unter Verwendung von Skript-Kommandos geblockt. Erst wenn die Nachricht, in unserem Fall die Betreffzeile, frei von aktiven Codes ist, erlaubt Airlock WAF die Weitergabe der Eingabe auf dem Applikationsserver. Im Datenstrom ermittelt der als Reserve Proxy aufgebaute WAF-Service die unerwünschten Eingaben und blockiert diese. Die dahinterstehende Applikation, bei der der Entwickler die Eingabeüberprüfung aus Unwissenheit oder Schludrigkeit wegließ, bemerkt von diesen vorgelagerten Aktivitäten nichts. Im Dashboard und auf der Konsole von Airlock WAF wurden indes die Ereignisse sehr wohl protokolliert und festgehalten.

Tampering erfolgreich unterdrücken

Das Tampering ist die gezielte Manipulation von Daten - hierfür gibt es verschiedene kleine Erweiterungen für Browser. Programme dieser Art unterbrechen beispielsweise den POST-Sendevorgang vom Browser zum Applikationsserver und erlauben die gezielte Manipulation von Eingaben. In unserem Testszenario ließ sich ein Voucher-Code mit einem Gegenwert von 50 über diesen Weg auf 500 erhöhen. Nach der Aktivierung der Funktion "Protect request for tampering" war hingegen keine sinnvolle Anpassung eines Werts mehr möglich.

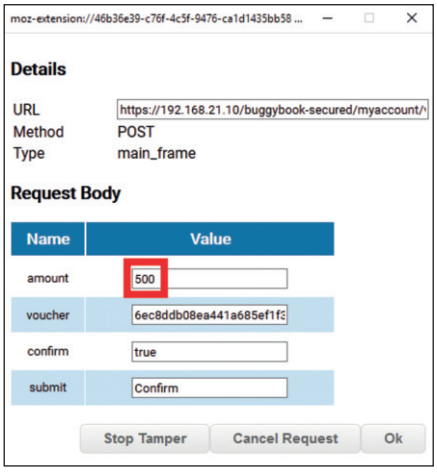

Bild 3: Airlock WAF ist in der Lage, das Tampering von Webseiten gezielt zu unterdrücken, damit aus einem 50-Euro-Gutschein nicht plötzlich eine Gutschrift von 500 Euro wird.

Ein weiteres Anwendungsbeispiel von Airlock WAF betrifft die unerwünschte Ausgabe von Serverinformationen. Im Fall des schlecht konfigurierten Web-Buchhandels ließ sich durch das bewusste Setzen von Verzeichnisbefehlen im Stil von ".../ help/ index.html?page= ../ ../ WEBINF/ web.xml;" die Ausgabeseite für den Entwicklungsmodus der Webseite ausgeben. Derselbe Versuch in der Bookstore-Variante mit aktiviertem "Protect the web application from forceful browsing" führte lediglich auf die normale Menüwebseite.

Insgesamt bewies die Airlock-Software, dass sie die Mehrzahl der Angriffsversuche identifiziert und auch abzuwehren weiß. Ausgestattet mit dem Nexpose-Scanner von Rapid7 unterzogen wir den Buggy Bookstore einem genauen "Web Audit". Dieser ergab, neben einigen Meldungen, die der reinen Teststellung geschuldet waren, dass unser System anfällig für Cross Site Scripting ist und dass der Status von "Autocomplete for sensitive HTML form fields" auf "enabled" steht. Auf der anderen Seite realisierte die WAF, dass von dem Nexpose-Server aus versucht wurde, Sicherheitslücken auszunutzen.

Lückenlose Schwachstellenauflistung

Wenn ein Hersteller eine Sicherheitssoftware auf den Markt bringt, deren primäre Aufgabe es ist, andere Systeme gegen diverse Angriffsvektoren zu wappnen, ist es zwingend erforderlich, dass auch diese Software selbst ganz besonders geschützt sein muss. Eine hundertprozentige Sicherheit, so die landläufige Binsenweisheit der IT-Branche, wird es kaum geben und da stellen die Lösungen aus dem Airlock-Umfeld keine Abweichung dar. Die Art und Weise, wie der Hersteller mit bekanntgewordenen Sicherheitsrisiken umgeht, dürfte aber eine wahre Seltenheit darstellen: Im passwortgeschützten Bereich der Webseite finden Kunden und Partner im Menüpunkt "Vulnerabilities" eine seit 2007 geführte Liste mit Lücken und Suchschlüsselwörtern, CVE-Identifikationsnummern, Aktualisierungsdatum und einer farbigen Aufschlüsselung, ob die geschützten Systeme für die Lücke mit oder ohne Airlock angreifbar wären.

So urteilt IT-Administrator

Schutz vor XSS	8
Reverse Proxy	8
Filterfunktionen	8
Richtlinien lernen	7
Auswertung und Reporte	8

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für größere Unternehmen, die ihre Applikationssysteme maximal absichern müssen.

bedingt für kleine Unternehmen mit geringeren Sicherheitsanforderungen.

nicht für kleine Firmen ohne ausreichendes Security-Know-how.

Eine andere Spalte zeigt an, ob Airlock selbst für das Sicherheitsproblem anfällig ist, beispielsweise bei CVE-2018-5390 oder CVE-2019-7317. Praktischerweise führt ein Klick auf die Beschreibung auf eine Webseite mit einer genauen Problembeschreibung und, sicherlich noch wichtiger, was der Administrator dafür tun könnte, um das Problem für seine Systeme zu lösen. Üblicherweise – und das dürfte die IT-Profis freuen – ist eine Aktualisierung per Hotfix auf die neueste Version die Lösung, um eine mögliche Sicherheitslücke im Schutzsystem selbst zu schließen.

Fazit

Airlock WAF überzeugte uns in der Testbetrachtung durch den hohen Funktionsumfang, den Grad der Absicherung und die übersichtliche Managementoberfläche. In unseren Angriffsszenarien wurde auf Applikationsseite die Attacke überhaupt nicht registriert – was für eine Schutzsoftware wohl die höchste Form der Anerkennung darstellt. Losgelöst davon handelt es sich um ein Werkzeug für sattelfeste Security-Experten. Wer einen solchen nicht im Team hat, sollte bei der Einrichtung und im Betrieb auf entsprechende Unterstützung setzen. *(ln)*