

Link: <https://www.computerwoche.de/a/automatisiertes-risikomanagement-verspricht-effizienz,1884244>

80 Prozent Ersparnis

Automatisiertes Risikomanagement verspricht Effizienz

Datum: 16.01.2009
Autor(en): Uli Ries

IT-Risikomanagement ist ein überaus zeitraubendes Geschäft - wenn es händisch erledigt wird. Anbieter von Software zum automatischen Risikomanagement versprechen eine Zeiteinsparung von bis zu 80 Prozent - angesichts knapper Ressourcen ein verlockendes Angebot. Glaubt man den Herstellern wie Skybox Security, stellt sich der ROI bereits binnen weniger Monate ein.



Goldener Mittelweg: Dank automatischer Risikoanalyse sollen sich kontinuierliche Tests zu geringen Kosten umsetzen lassen.

Foto: Skybox Security

ARCM nennt sich die Wunderwaffe gegen ausuferndes **IT-Risikomanagement**¹ – Automated Risk and Compliance Management. ARCM soll in Zeiten komplexer Richtlinien wie **Basel II**², **Sarbanes-Oxley**³, **ITIL**⁴, **Cobit**⁵, **HIPAA**⁶ oder **PCI**⁷ dafür sorgen, dass auch komplexe und sich ständig verändernde IT-Infrastrukturen sicher und Konform zu den Regularien bleiben.

Anbieter von ARCM-Produkten wie **Skybox Security**⁸ versprechen das Ende der mit großem Personalaufwand meist nur einmal pro Jahr umgesetzten IT-Risk-Audits. Mit Hilfe ihrer Software sollen sich solche Audits auf Knopfdruck binnen weniger Stunden auch in der komplexen IT-Landschaft eines Großunternehmens erledigen lassen. ARCM-Produkte ersetzen aber keine der vorhandenen IT-Sicherheitskomponenten, sie stützen sich aber auf diese und beziehen die zur Analyse notwendigen Daten von ihnen.

ARCM soll insbesondere dabei helfen, binnen weniger Minuten zu erkennen, ob eine geplante Änderung – zum Beispiel neue **Firewall**⁹-Regeln – die Compliance gefährdet. Der Gründer von Skybox Security, Gidi Cohen, schätzt, dass eine Enterprise-Firewall zwischen 200 und 1000 Regeln kennt. Bei 100 bis 1000 Firewalls pro Unternehmen und ein bis zwei Regeländerungen pro Monat könne laut Cohen kein IT-Team mehr den Überblick behalten.

Ein Mensch benötigt laut Cohen pro zu überprüfender Regel zwei Stunden und länger. Daher würden die Checks nur einmal jährlich gemacht, wodurch große Zeitfenster mit unklarem Zustand entstehen. Die Skybox-Software klopft die Regeländerung binnen zehn Minuten ab, 400 Firewalls sollen sich in zwei Tagen checken lassen. Außerdem liegt der Analyst aus Fleisch und Blut nur in 70 Prozent aller Fälle richtig mit seiner Einschätzung, die Software jedoch zu 99 Prozent.

Außerdem kann **Skybox Secure**¹⁰ laufend Risk Assessments machen, in dem es Attacken gegen die real vorhandene Infrastruktur simuliert – freilich ohne den Geschäftsbetrieb zu stören. Die Ergebnisse der Tests werden übersichtlich und samt Handlungsvorschlägen dargestellt. Laut Skybox bewertet die Software gefundene Risiken nicht anhand eines abstrakten Klassifizierungssystems wie **CVSS**¹¹, sondern knüpft die Einschätzung der Relevanz an die tatsächlich vorhandene **Netzwerk**¹²-Infrastruktur.

Ohne Fleiß gibt es aber auch bei ARCM keinen Preis. Damit das Tool effizient arbeiten kann, müssen erst einmal alle relevanten Konfigurations- und Infrastrukturdaten eingepflegt werden. Außerdem gebe es laut Gidi Cohen „keinen Freifahrtschein“, da sich auch die bestehenden Prozesse ändern und an die neuen Möglichkeiten anpassen müssen, die durch ARCM entstehen. Nur dann lässt sich der maximale **Return on Invest**¹³ heraus holen.

Links im Artikel:

¹ <https://www.computerwoche.de/subnet/hp-intel/1879636/>

² <https://www.computerwoche.de/schwerpunkt/b/Basel-II.html>

³ http://de.wikipedia.org/wiki/Sarbanes-Oxley_Act

⁴ https://www.computerwoche.de/knowledge_center/software_infrastruktur/1875989/

⁵ <http://de.wikipedia.org/wiki/Cobit>

⁶ http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

⁷ http://de.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

⁸ <http://www.skyboxsecurity.com/>

⁹ <https://www.computerwoche.de/schwerpunkt/f/Firewall.html>

¹⁰ <http://www.skyboxsecurity.com/?CategoryID=238&ArticleID=135>

¹¹ <http://www.first.org/cvss/>

¹² https://www.computerwoche.de/knowledge_center/netzwerke/

¹³ https://www.computerwoche.de/knowledge_center/security/1878479/index4.html

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.