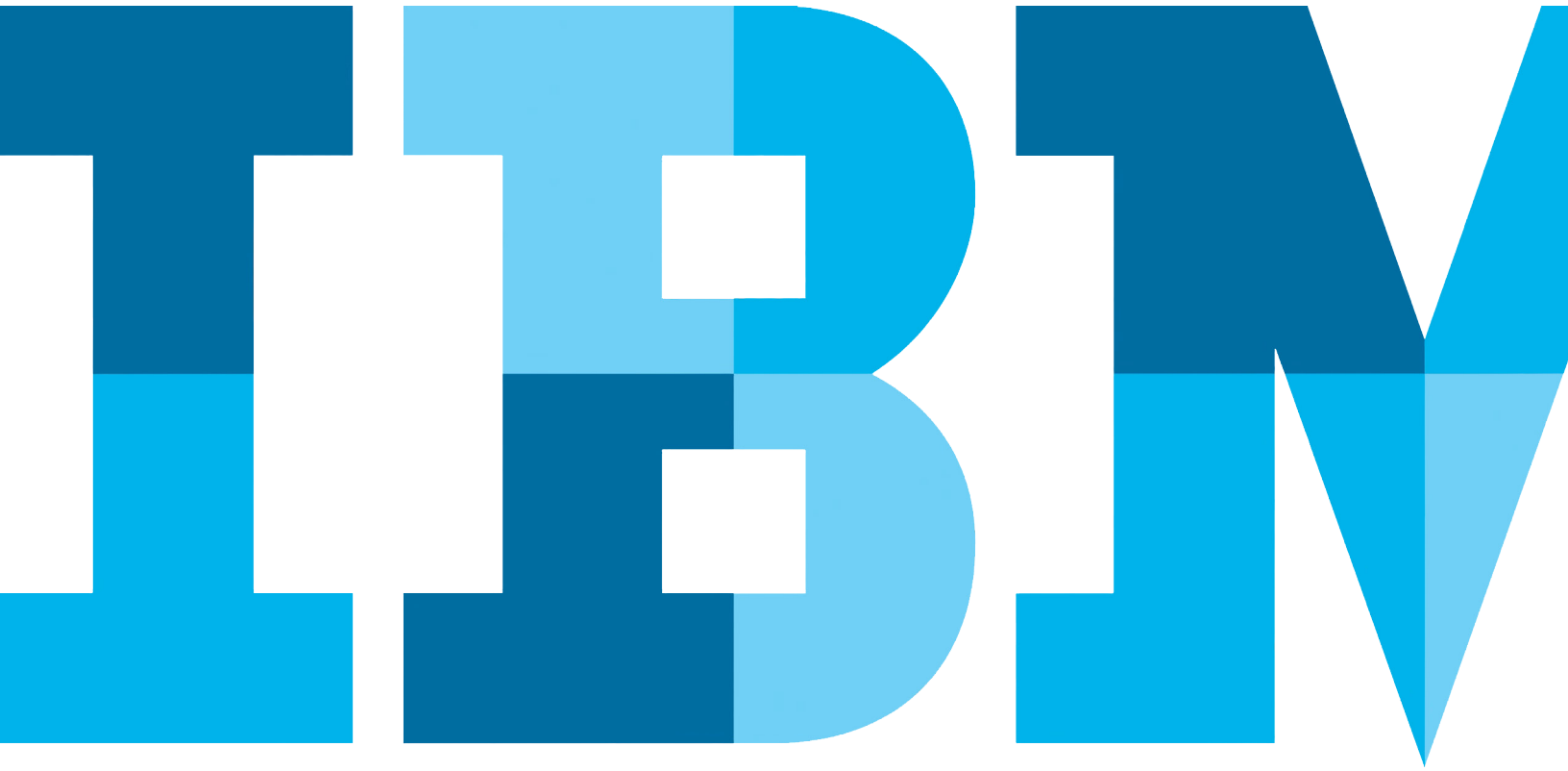
TechTarget Custom Media

Juli 2015

Thought-Leadership-Artikel

So erhält Security den richtigen Stellenwert

Autor: Oliver Schonschek



IBM

Jedes zweite Unternehmen in Deutschland ist in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden. Die Informationssicherheit muss dringend optimiert werden. 59 Prozent der Sicherheitsexperten in Deutschland gehen von steigenden bis stark steigenden Ausgaben für Datenschutz und IT-Sicherheit aus, so der eco Report „IT Sicherheit 2015".

IT-Sicherheitsverantwortliche sollten den Wert von Security deutlich machen und aufzeigen, wie sich durch die optimierte Organisation der Security mit einem Security Operations Center (SOC) von IBM das Budget erfolgreich zur Abwehr von Datenmissbrauch und Cyber-Attacken einsetzen lässt.

Kosten von Datenpannen richtig einschätzen

Wenn die Unternehmensleitung zögert, das Security-Budget den steigenden Bedrohungen entsprechend anzupassen, liegt dies oftmals daran, dass die wirtschaftlichen Vorteile von Security nicht richtig eingestuft werden.

Die Ponemon-Studie „2015 Cost of Data Breach Study" macht deutlich, was Unternehmen durchschnittlich ausgeben, um ihre Datenpannen zu beheben: In Deutschland sind es rund 3,5 Millionen US-Dollar pro Vorfall. Seit 2013 sind die Kosten durch Datenpannen um 23 Prozent angewachsen. Jeder einzelne verlorene oder gestohlene Datensatz schlägt für ein deutsches Unternehmen mit Kosten von 152 US-Dollar zu Buche. Je nach Branche kann der wirtschaftliche Schaden pro Datensatz noch deutlich höher sein. Im Gesundheitswesen zum Beispiel sind die durchschnittlichen Kosten pro gestohlenen oder verlorenen Datensatz 363 US-Dollar. Wie die Studie betont, schlagen sich Datenpannen auch im Verhalten von Kunden betroffener Unternehmen nieder: Das Vertrauen sinkt und damit auch die Zahl der Kunden sowie der Umsatz.

Budget gezielt nutzen, Security zentral steuern

Die verschiedenen Bereiche der IT-Infrastruktur und IT-Nutzung werden sehr unterschiedlich bei der Budgetplanung für Security bedacht. Während die Sicherheit mobiler Apps bei der Budgetierung wenig Beachtung findet, sieht es für die Sicherheit von Cloud Computing finanziell besser aus: Laut der aktuellen IBM CISO-Studie haben 90 Prozent der befragten Unternehmen Cloud-Lösungen eingeführt oder sind gerade in der Planungsphase. Aus dieser Gruppe wiederum gehen 75 Prozent davon aus, dass ihr Cloud-Sicherheits-Budget in den nächsten drei bis fünf Jahren steigen oder sogar erheblich steigen wird.

So wichtig Cloud-Sicherheit auch ist, sollten sich IT-Sicherheitsverantwortliche mit der Förderung einiger, weniger Sicherheitsbereiche nicht zufrieden geben. Bekanntlich suchen und nutzen die Angreifer jede Lücke in der Verteidigung. Ziel muss es also sein, das Security-Budget entsprechend der tatsächlichen, aktuellen Bedrohungslage zu planen und die Prioritäten bei der Finanzierung von Security-Maßnahmen anzupassen. Bei der Security-Budgetierung helfen Ansätze wie Security Operations Center.

SOCs ermöglichen eine optimierte Security-Organisation

Durch die zentrale Überwachung der aktuellen IT-Bedrohungslage und die Steuerung der Security-Maßnahmen über ein Security Operations Center können Unternehmen für die richtigen Prioritäten und damit für die erfolgreiche Nutzung des Security-Budgets sorgen. Die Berichte zur aktuellen Bedrohungslage helfen bei der Definition und Durchsetzung des Security-Budgets.

Zudem kann über ein Security Operations Center als zentrale Schaltstelle der Informationssicherheit auch dafür gesorgt werden, dass das Security-Budget entsprechend des tatsächlichen Schutzbedarfs eingesetzt wird. Mögliche Angriffe lassen sich schneller erkennen und gezielt abwehren. Die Wahrscheinlichkeit für Datenpannen und Datenmissbrauch wird minimiert, die möglichen Kosten durch Datenpannen sinken entsprechend. Durch den Einsatz und die Lernfähigkeit eines SOCs kann sichergestellt werden, dass die Security-Organisation auf Basis der Security-Analysen fortlaufend optimiert wird.

IT-Sicherheitsverantwortliche sollten deshalb den Aufbau oder die Nutzung eines Security Operations Centers prüfen und bei der Unternehmensleitung vorschlagen. Wie die IBM CISO-Studie zeigt, hat die Zunahme von Cyberattacken und staatlichen Regulierungen in vielen Unternehmen die Rolle der IT-Sicherheitsverantwortlichen gestärkt, der Einfluss ist gewachsen: 90 Prozent der befragten IT-Sicherheitsverantwortlichen gaben an, dass sie einen erheblichen Einfluss in ihrem Unternehmen haben. 76 Prozent sagten, dass ihr Einfluss sich in den letzten drei Jahren erheblich vergrößert hat. Diesen Einfluss sollten IT-Sicherheitsverantwortliche geltend machen, um ein der Bedrohungslage entsprechendes Security-Budget zu erhalten und dieses auch so einzusetzen. Security Operations Center sind dabei eine zentrale Unterstützung.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Produziert in Europa
Juli 2015

Die IBM Homepage finden Sie unter:
ibm.com

IBM, das IBM Logo und ibm.com sind eingetragene Marken der International Business Machines Corporation. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Herstellern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter: **ibm.com**/legal/copytrade.shtml

Dieses Dokument ist zum Datum der Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle Angebote sind in jedem Land, in welchem IBM tätig ist, verfügbar.

Die Informationen in dieser Veröffentlichung werden auf der Grundlage des gegenwärtigen Zeitpunkts (auf „as-is“ Basis) und ohne ein ausdrückliche oder stillschweigende Gewährleistung zur Verfügung gestellt. Für IBM Produkte gelten die Gewährleistungen, die in den Vereinbarungen vorgesehen sind, unter denen sie erworben werden.

Jeder Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. Es obliegt allein dem Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Einhaltung aller relevanter Gesetze und gesetzlichen Bestimmungen betreuen zu lassen, die sich auf seine Geschäftstätigkeit und alle Maßnahmen auswirken können, die er im Hinblick auf die Einhaltung solcher Bestimmungen durchführen muss. IBM erteilt keine Rechtsberatung und gibt keine Garantie bzw. Gewährleistung bezüglich der Konformität von IBM Produkten oder Services mit geltenden Gesetzen.

© Copyright IBM Corporation 2015

Bitte der Wiederverwertung zuführen

TechTarget Custom Media