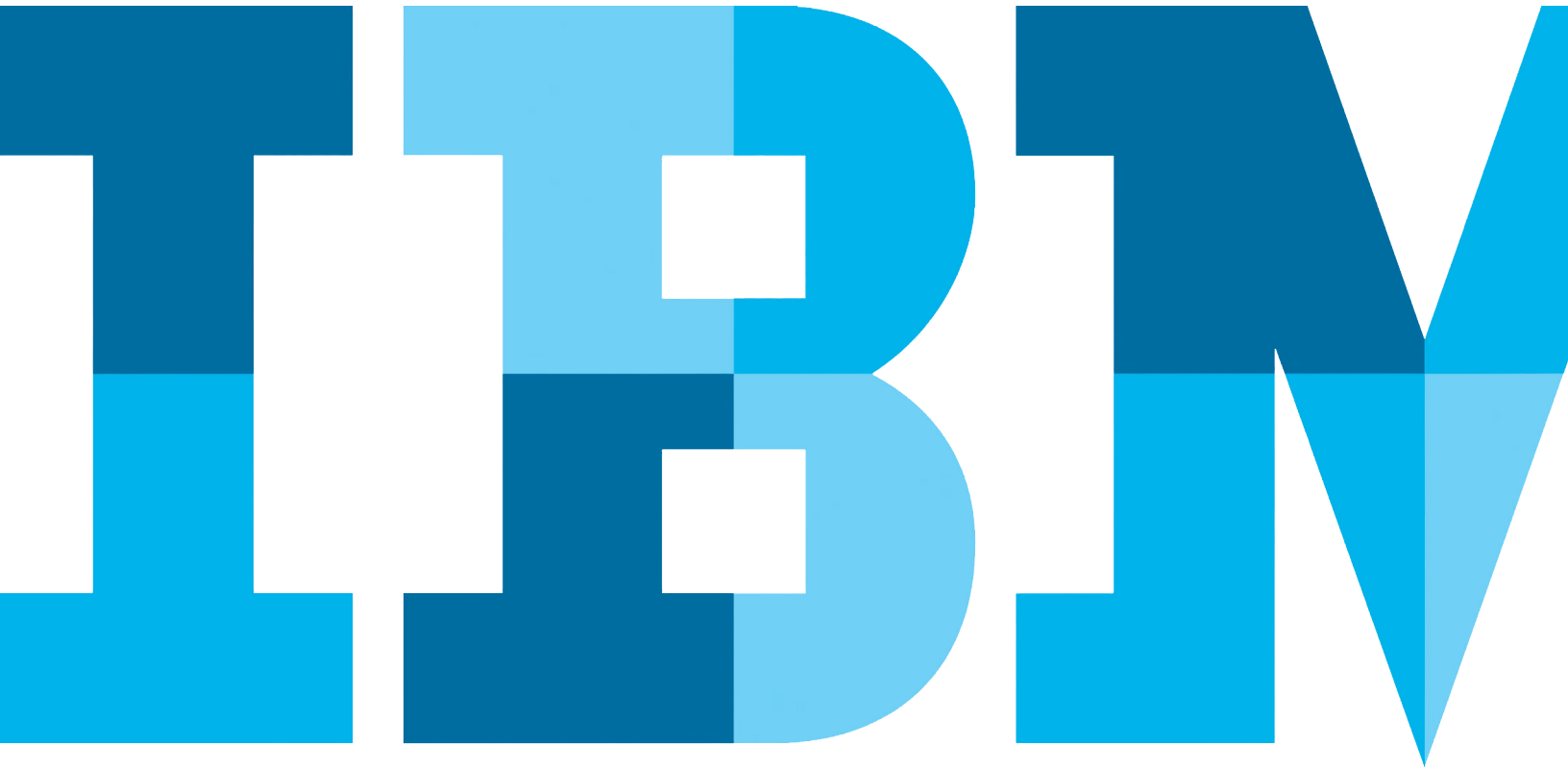
TechTarget Custom Media

Juli 2015

Thought-Leadership-Artikel

Der Weg zum eigenen Security Operations Center

Autor: Oliver Schonschek



IBM

81 Millionen echte Sicherheitsvorfälle in 2014, darunter rund 12.000 Cyberattacken und knapp über 100 Ereignisse pro Unternehmen, diese Zahlen aus dem IBM 2015 Cyber Security Intelligence Index machen mehr als deutlich, dass sich Unternehmen nicht fragen sollten, ob sie angegriffen werden, sondern wann der nächste Angriff kommt.

Unternehmen benötigen eine IT-Sicherheitsstrategie, die die zunehmenden, sich dynamisch ändernden Bedrohungen berücksichtigt. Ein zentrales Element dabei ist der Aufbau und Betrieb eines Security Operations Center (SOC). Aus der Vielzahl der Sicherheitsmeldungen, die in den Systemprotokollen der IT auftauchen, gilt es diejenigen Sicherheitsereignisse zu erkennen, die unmittelbare Gegenmaßnahmen erfordern, insbesondere also die Erkennung und Abwehr echter Attacken. Dazu werden in einem SOC die Sicherheitsmeldungen zentral ausgewertet und analysiert, erkannte Ereignisse werden bewertet und priorisiert. Das SOC-Team leistet Support in der Umsetzung der IT-Sicherheitsstrategie und bei der Kontrolle, ob die internen Sicherheitsrichtlinien und relevanten Compliance-Vorgaben eingehalten werden.

Damit das SOC diese wichtigen Leistungen für das Unternehmen erbringen kann, muss die Konzeptionierung des Security Operations Centers professionell durchdacht sein. IBM bietet entsprechende Unterstützung durch sein Security Operations Center Consulting und begleitet Unternehmen auf dem Weg zum eigenen SOC.

Am Anfang steht die Ist-Analyse

Die Spezialisten von IBM helfen Unternehmen dabei, die vorhandene IT-Sicherheitslandschaft zu bewerten und mit der tatsächlichen Bedrohungslage des jeweiligen Unternehmens abzugleichen (Information Security Assessment). Ermittelt werden zum Beispiel die derzeitige Risikosituation in der Informationssicherheit, Schwachstellen der Netzinfrastruktur sowie die notwendigen Schritte zur Optimierung der Sicherheitssituation, basierend auf den jeweiligen Geschäftsanforderungen.

Die IT-Sicherheitsstrategie des Unternehmens wird überprüft, bevor diese zur Basis des geplanten Security Operations Center wird. Mit der angepassten Sicherheitsstrategie und dem aufzubauenden SOC wird es möglich, noch besser auf Sicherheitsvorfälle zu reagieren, das Security-Budget optimal einzusetzen und die Security in eine aktive Rolle zu versetzen.

In Workshops und Assessments arbeiten die IBM Security Consultants gemeinsam mit den verantwortlichen Stellen im Unternehmen an einer umfassenden Optimierung des Security-Betriebs. Abläufe und Richtlinien werden ebenso überprüft wie die genutzten Lösungen und Werkzeuge für das Security-Monitoring und die Angriffserkennung (IBM Security Governance Services). Das vorhandene Reporting wird untersucht und auf den tatsächlichen Bedarf der verantwortlichen Stellen angepasst. Ebenso werden Metriken definiert, mit deren Hilfe sich der Erfolg von Security-Maßnahmen und des geplanten Security Operations Center messen lässt.

Interne Security Intelligence wird ausgebaut

Die Schritte zum Aufbau eines eigenen SOCs werden individuell auf das jeweilige Unternehmen abgestimmt. Kernelement ist aber immer der Ausbau der vorhandenen

Fähigkeiten im Bereich Security Intelligence. Aus den sicherheitsrelevanten Informationen und den Security-Analysen müssen Einsichten gewonnen werden, welche Bedrohungen vorliegen, wie hoch das betriebliche Risiko jeweils ist, welche Compliance-Vorgaben und internen Richtlinien bestehen und welche Security-Maßnahmen in welcher Reihenfolge ergriffen werden müssen.

Fehlende Ressourcen im Unternehmen können von IBM geliefert oder beigestellt werden. Dazu gehören Security Analysten, die die Sicherheitsfunktionen überwachen und IT-Bedrohungen analysieren, bei Bedarf auch eine personelle Unterstützung rund um die Uhr für das Security-Monitoring. Ebenso steht Unterstützung bereit, um die notwendigen operationellen Prozesse zu entwickeln und einzuführen, die für ein eigenes SOC notwendig sind.

Fehlende technische Lösungen zum Beispiel aus dem Bereich SIEM (Security Information and Event Management) oder Ticket-Management zur Bearbeitung von Sicherheitsvorfällen können ebenfalls von IBM bezogen und durch IBM implementiert werden. Bei Bedarf können auch bestimmte Lösungsbausteine durch IBM betrieben werden. Dadurch ergänzt das IBM Security Hosting die im SOC des Unternehmens vorhandenen Lösungen.

Aufgaben im SOC können aufgeteilt werden

Mit der Unterstützung bei dem Aufbau eines eigenen SOCs als zentrale Überwachungs- und Steuerungsinstanz der Security enden die IBM Security Services also nicht. Der eigentliche Betrieb des Security Operations Center kann zwischen dem Unternehmen und IBM individuell aufgeteilt werden. Dazu werden die Aufgaben und Rollen sowie die Abläufe und Schnittstellen zwischen IBM und dem jeweiligen Unternehmen definiert. So kann das Unternehmen alle Bausteine des SOC-Betriebs, die selbst geleistet werden können, übernehmen und individuell die noch notwendigen Leistungen für das SOC von IBM beziehen. Die Begleitung durch IBM geht auf Wunsch über den Start des eigenen SOC hinaus und umfasst neben Betriebsleistungen auch eine regelmäßige Auditierung der SOC-Prozesse, damit diese auf Dauer dem Schutzbedarf des Unternehmens entsprechen.

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

TechTarget Custom Media