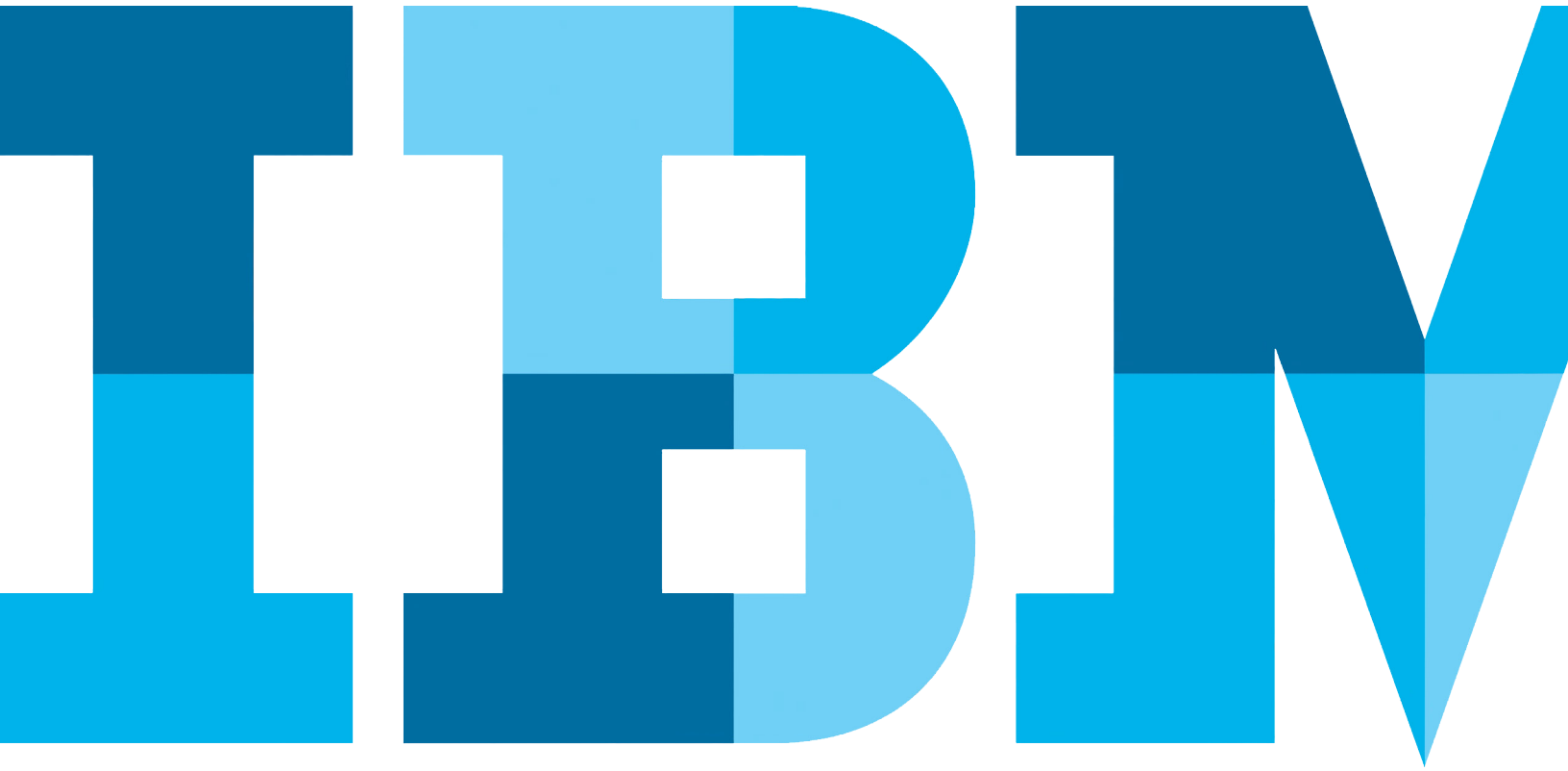
TechTarget Custom Media

August 2015

Thought-Leadership-Artikel

Unternehmen brauchen einen neuen Weg zur IT-Sicherheit

Autor: Oliver Schonschek



IBM

Das Bewusstsein für IT-Sicherheit in Unternehmen steigt, so der Digitalverband Bitkom auf Basis von Prognosen des Marktforschungsunternehmens IDC. So erfreulich eine steigende Sensibilisierung für notwendige IT-Sicherheitsmaßnahmen auch ist, so besorgniserregend ist der aktuelle Zustand der IT-Sicherheit bei Unternehmen in Deutschland.

Das Schutzschild der Unternehmen gegen die steigende Zahl an komplexen Attacken besteht mehrheitlich nur aus Virenscanner, Firewalls sowie einem Passwortschutz für IT-Geräte. Intelligente Sicherheitssysteme zur Absicherung gegen Datenabfluss nutzen lediglich 29 Prozent, nur 23 Prozent der Unternehmen in Deutschland verfügt über spezielle Systeme zur Angriffserkennung bei Attacken von außen.

Der unzureichende Schutz gegen raffinierte Angriffe wie die sogenannten Advanced Persistent Threats (APT) bleibt nicht ohne Folgen: 51 Prozent aller Unternehmen in Deutschland sind in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden, wie die Bitkom-Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter“ zeigt. Der Schaden dadurch ist enorm und liegt für Unternehmen in Deutschland bei 3,5 Millionen US-Dollar pro Datenpanne, so die Ponemon-Studie „2015 Cost of Data Breach Study“.

Es lohnt sich deshalb nicht nur für die Unternehmen in Deutschland, die eigenen IT-Sicherheitsmaßnahmen zu optimieren, sondern es ist höchste Zeit für einen neuen Weg der IT-Sicherheit. Wie dieser aussehen kann, zeigt zum Beispiel IBM Security mit einem strategischen Security-Ansatz und einem umfassenden Portfolio an Security Services und Software Solutions.

Optimierung der IT-Sicherheit mit Security Intelligence

Unternehmen und Organisationen müssen gegenwärtig durchschnittlich 91 Millionen potentielle Security-Vorfälle pro Jahr abwehren. Wie IBM-Studien zeigen, dauert es in 75 Prozent der Sicherheitsvorfälle Tage, Wochen oder gar Monate, bis diese in Unternehmen entdeckt werden. Das Ponemon-Institut ermittelte, dass die Unternehmen durchschnittlich rund ein dreiviertel Jahr (256 Tage) benötigen, um Hackerangriffen auf die Schliche zu kommen.

Die Erkennung der Angriffe ist deshalb so schwierig, weil die Datendiebe und Internetkriminellen immer raffiniertere Methoden einsetzen, die mit klassischen Verfahren der IT-Sicherheit nicht schnell genug oder überhaupt nicht mehr festzustellen sind. Unternehmen brauchen neuartige, intelligente Sicherheitslösungen und Zugang zu dem notwendigen Security-Know-how, das in vielen Unternehmen nicht vorhanden ist.

Über 70 Prozent der von IBM befragten IT-Sicherheitsverantwortlichen gaben an, dass die Nutzung von Security Intelligence in Echtzeit immer wichtiger wird. Die Vielfalt an Bedrohungen und die Komplexität der Attacken übersteigt oftmals die Möglichkeiten eines einzelnen Unternehmens, so dass Security-Intelligence-Lösungen wie die von IBM sowie die Erfahrung und personelle Unterstützung aus einem professionellen

Security Operations Center (SOC) und von Security Consultants als die richtige Antwort auf die Risiken erscheinen.

Ausrichtung der Abwehr auf raffinierte Attacken

Wie raffiniert die neuartigen Angriffsmethoden sind, zeigt zum Beispiel die von IBM aufgedeckte Cybercrime-Attacke Dyre Wolf. Bei diesem Angriff wird die Verteilung eines Trojaners als Mail-Anhang verknüpft mit dem Einsatz manipulierter Banking-Webseiten und der geschickten Täuschung der Nutzer mittels Social Engineering: Sobald der Trojaner ein System infiziert hat, leitet er den Nutzer auf eine fingierte Website anstelle der echten Online-Präsenz der hauseigenen Bank. Der Nutzer wird, unter dem Vorwand technischer Schwierigkeiten, aufgefordert, sich telefonisch an einen Servicemitarbeiter zu wenden. Hinter der angezeigten Telefonnummer stecken die Hacker selbst. Sie bringen die ahnungslosen Mitarbeiter dazu, die Kontoinformationen und Zugangsdaten ihres Arbeitsgebers preiszugeben. Laut den Sicherheitsforschern von IBM ist es den Cyberkriminellen so gelungen, einzelne Unternehmen teils um über eine Million US-Dollar zu erleichtern.

Um solche Attacken rechtzeitig zu erkennen und den immensen Schaden zu vermeiden, reichen herkömmliche IT-Sicherheitsmaßnahmen alleine nicht aus. Erst auf Basis von Security-Intelligence-Verfahren lassen sich die Bestandteile der raffinierten Attacken im Zusammenhang erkennen und abwehren.

Fokus auf Identitäten und Berechtigungen

Viele Angriffe beginnen damit, legitimen Nutzern Zugangsdaten zu stehlen. Da viele Nutzer weitaus mehr kritische Berechtigungen haben, als sie für ihre Aufgabenerfüllung benötigen, gelten die Versuche, Passwörter zu stehlen, nicht nur den Anwendern mit hohen Systemprivilegien, sondern allen Nutzern. Lösungen zur Vergabe und Kontrolle von Identitäten und Berechtigungen kommt deshalb eine große Rolle bei der Optimierung der IT-Sicherheit zu.

Ein weiterer Grund für zusätzliche Maßnahmen im Bereich Identity and Access Management (IAM) ist, dass „unbefugte Zugriffe“ die Rangliste der Sicherheitsvorfälle im Jahr 2014 anführten und 31,5 Prozent aller Attacken durch Innentäter erfolgte, darunter ehemalige Angestellte, die noch über Passwörter verfügten oder Zugänge einrichteten, bevor sie das Unternehmen verließen. Nur ein professionelles, intelligentes Identitäts- und Zugriffsmanagement hilft gegen solche Angriffe aus den eigenen Reihen.

Implementierung moderner IT-Sicherheit für moderne Technologien

Eine weitere Entwicklung macht neue Wege in der IT-Sicherheit erforderlich: Unternehmen führen neue Technologien wie mobile Apps und Cloud-Services ein, ohne die IT-Sicherheit auf die damit verbundenen Risiken anzupassen. In der IBM CISO-Studie bestätigen nur 45 Prozent der Sicherheitsverantwortlichen, dass sie für mobile Apps und Geräte spezifische Sicherheitskonzepte im Einsatz haben.

85 Prozent der von IBM befragten IT-Sicherheitsverantwortlichen gab an, dass die IT ihrer Unternehmen sich weiter in Richtung Cloud entwickelt, fast die Hälfte erwartet dabei aber Sicherheitsprobleme bei Cloud-Anbietern.

Der neue Weg zur IT-Sicherheit bedeutet deshalb: Die IT-Sicherheit muss sich fortentwickeln, wenn neue Technologien eingeführt werden und neuartige Bedrohungen auftreten. Damit die IT-Sicherheit aber dem Schutzbedarf nicht nachhinkt, sind intelligente Sicherheitslösungen und ein reicher Erfahrungsschatz erforderlich, der Bedrohungen sehr schnell sichtbar werden lässt und die geeigneten IT-Sicherheitsmaßnahmen frühzeitig vorsieht.

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