Europas Unternehmen werden von Security-Daten überschwemmt

15.05.2006, 08:24 | IT, New Media & Software

Pressemitteilung von: *Micromuse*
Presseagentur: *Jürgen Saarmann PR*

Micromuse Ltd., ein IBM Unternehmen, gab jetzt die Ergebnisse einer unabhängigen Untersuchung zum Thema Security bekannt. Die Studie, die sich auf fünf Industriebereiche in Deutschland, Frankreich, England, Italien, Spanien, den Niederlanden und Schweden konzentriert, stellt fest, dass europäische Unternehmen nicht in der Lage sind, die große, von Sicherheits-Systemen wie Firewalls und Antivirus-Lösungen generierte Datenmenge sinnvoll zu handhaben.

Nahezu ein Drittel (30 Prozent) der befragten IT-Direktoren gestand, dass die Menge der genierten Security-Daten viel zu groß ist, um sie sorgfältig zu analysieren und potentielle Sicherheitsbedrohungen zu identifizieren. 72 Prozent der Unternehmen verläßt sich darüber hinaus auf die Erfahrung und Expertise von IT-Managern, um Security-Events daraufhin zu priorisieren, auf welche Ereignisse zuerst reagiert wird. Das bedeutet, dass die getroffenen Priorisierungen nicht unbedingt mit den Unternehmens-Zielen übereinstimmen. Selbst wenn die IT-Abteilung ständig über die geschäftlichen Prioritäten auf dem Laufenden gehalten wird, kann es geschehen, dass eine für die Sicherheit des Unternehmens weniger wichtige Bedrohung zuerst bereinigt wird.

Die Studie mit dem Titel „Definition und Priorisierung von Sicherheits-Bedrohungen“ wurde von Micromuse konzipiert und von dem unabhängigen Marktforschungs-Unternehmen Vanson Bourne durchgeführt. Sie stellt fest, dass viele Organisationen für Sicherheits-Bedrohungen verletzlich sind und auf die Expertise einer einzelnen Person vertrauen, obwohl diese Person nicht über die Zeit verfügt, um alle Daten zu überprüfen, und nicht immer über die wichtigsten Geschäftsprioritäten informiert ist.

Die Untersuchung fand heraus, dass der Zeitaufwand für die manuelle Sammlung, Abgleichung und Analyse von Security-Daten einen signifikanten Anteil der Ressourcen der IT-Abteilungen beansprucht. Einer von zehn Befragten (13 Prozent) gab an, dass die IT-Abteilung mehr als 60 Prozent ihrer Zeit für die Analyse von Security-Informationen aufwendet, was mehr als drei Tagen pro Woche entspricht. Bezogen auf die vertikalen Marktsektoren stellte sich heraus, dass im Handels- und im Öffentlichen Sektor die größten Schwierigkeiten bei der Identifikation und Priorisierung von Sicherheits-Bedrohungen auftreten: 44 beziehungsweise 41 Prozent gaben an, nicht in der Lage zu sein, mit der großen Datenmenge zurechtzukommen.

„Offensichtlich nehmen viele Unternehmen die Sicherheit nicht ernst genug, wenn sie sich auf das Bauchgefühl eines IT-Managers verlassen“, sagt Richard Lowe, Senior Vice President for Business Operations in Europa, dem Nahen Osten und Afrika bei Micromuse. „Durch die Verlagerung der Verantwortlichkeit auf eine Person bleiben die Unternehmen offen für Sicherheits-Bedrohungen, besonders wenn diese Person in Urlaub geht oder das Unternehmen verläßt. Solche Organisationen sollten ihre Sicherheits-Strategie überdenken, um sicherzustellen, dass die Kenntnisse des IT-Managers nicht die einzige Instanz sind, die die Sicherheit ihres Netzwerks gewährleistet. Gewöhnlich investierten Unternehmen in neue Sicherheits-Applikationen oder -komponenten, sobald neue Bedrohungen erkannt wurden. Das Ergebnis davon ist, dass derartige Sicherheitssysteme über die gesamte Organisation verteilt sind und Unmengen von Daten von sich geben, die nicht mehr zu bearbeiten sind. Bevor nicht ein besserer Weg gefunden wird, die Menge von Sicherheits-Daten zu sammeln, zu kontrollieren und zu analysieren, ist die IT-Abteilung gezwungen, sich auf die Administration zu konzentrieren anstatt strategischen Wert zu generieren.“

Das reine Datenvolumen war im Rahmen der Umfrage ein weiteres Thema. Fast die Hälfte der Befragten (45 Prozent) sprach von 4.000 Sicherheits-Events pro Sekunde, 15 Prozent sogar von mehr als 6.000. Ein Sicherheits-Event wird registriert, ob eine Aktivität gefährlich ist oder nicht, wodurch Massen von Sicherheits-Daten entstehen, die von der IT-Abteilung untersucht werden müssen – was deren Kapazität meistens überschreitet. Der Öffentliche Sektor und Finanzorganisationen erhalten mehr als doppelt so viele Events wie die anderen Sektoren: 38 beziehungsweise 39 Prozent teilten mit, mehr als 6.000 Events pro Sekunde zu verzeichnen. Das mag mit der vertraulichen und wichtigen Natur der

Daten zusammenhängen, die über diese Netzwerke transportiert werden, und könnte darauf hinweisen, dass diese Organisationen das größte Ziel für Hacker und andere Kriminelle darstellen – besonders, wenn sie ihre Sicherheitseinrichtungen nicht effektiv überwachen.

Ein anderes alarmierendes Ergebnis war, dass 69 Prozent der befragten Unternehmen sich bei der Auswertung von Sicherheits-Events auf die Expertise eines IT-Managers verlassen, um verdächtiges Verhalten oder potentielle Sicherheits-Bedrohungen zu ermitteln. Diese Zahl steigt im Öffentlichen Sektor auf 79 Prozent – eine verstörende Aussicht, da der Öffentliche Sektor sich in Richtung eGovernment bewegt und eine zunehmende Verlagerung auf Online-Services stattfindet.

„Es ist sicherlich nicht der richtige Ansatz, sich auf einen IT-Manager zu verlassen, um die täglich wachsende Menge von Sicherheitsbedrohungen auszuwerten und auf diese Weise einen ernstzunehmenden Bruch der Sicherheitsvorkehrungen zu verhindern“, sagt Lowe. „Notwendig ist gerade im Hinblick auf die Zunahme von mobilen Endgeräten, Online-Transaktionen, Intra- und Extranets ein proaktiverer Ansatz beim Security Management, um sicherzustellen, dass ernstzunehmende Sicherheits-Bedrohungen identifiziert, dem Personal angezeigt, priorisiert und schnell eliminiert werden, bevor sie Services, Kunden und Umsatz gefährden können.“

Die Studie wurde von Micromuse konzipiert, um die Frage zu beantworten, welchem Ansatz IT-Abteilungen in Europa im Hinblick auf die Sicherheit folgen. Sie wurde von dem unabhängigen Marktforschungsunternehmen Vanson Bourne durchgeführt und basiert auf der Befragung von 700 IT-Managern in Deutschland, Frankreich, England, Italien, Spanien, Schweden und den Niederlanden.

Portrait

Micromuse Ltd. – ein IBM Unternehmen
Susanne Eberhardt-Camilotti
2, Avenue de la Cristallerie
92310 Sèvres, Frankreich
Tel: 0033 – 158870013
seberhard@fr.ibm.com

www.micromuse.com

News-ID: 86728 • Views: 1610 (Stand: 05.08.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/86728/Europas-Unternehmen-werden-von-Security-Daten-ueberschwemmt.html