



«Der Schutz von Informationen und Applikationen ist heute eine strategische Aufgabe und leistet einen zentralen Beitrag für ein erfolgreiches Risikomanagement.»

Martin Bosshardt ist CEO der Open Systems AG

Wo sehen Sie heutzutage die grössten Gefahren für die IT-Sicherheit?

Es sind aus unserer Sicht vor allem drei Bereiche. Erstens: die steigende Komplexität. Die Art der Bedrohungen und die dafür genutzten Technologien verändern sich rasant. Generalisten laufen Gefahr, den Überblick zu verlieren. Zweitens: die Ressourcenknappheit im Unternehmen, sowohl in finanzieller als auch in personeller Hinsicht. Interne IT-Teams sind gezwungen, die Anstrengungen für den Schutz der Infrastruktur aufgrund von personeller Überlastung und Budgetknappheit auf ein Minimum zu beschränken. Darunter leiden dann zum Beispiel die Reaktionsgeschwindigkeit, der regelmässige Unterhalt der Hard- und Software und die transparente und auditierbare Dokumentation. Und drittens: die fehlende Corporate Governance. Aufgrund unklarer Rollen und Verantwortlichkeiten im Bereich IT-Sicherheit sowie fehlender Gewaltentrennung bei der Umsetzung und Kontrolle der Sicherheitsrichtlinien kommt es zu Missverständnissen und Interessenkonflikten, die zu einer deutlichen Reduktion der Sicherheitsqualität führen.

Müssen Anwender heutzutage immer noch für das Thema Sicherheit sensibilisiert werden?

Auf jeden Fall, denn sie müssen verstehen, wie wichtig eine gut funktionierende IT-Infrastruktur für den Unternehmenserfolg geworden ist und inwiefern menschliches Fehlverhalten das operative Geschäft bedroht. Das Bewusstsein für die IT-Sicherheit sollte aber nicht nur bei den Anwendern geschärft werden. Der Schutz der unternehmenskritischen Informationen und Applikationen ist heute eine strategische Aufgabe und leistet einen zentralen Beitrag für ein erfolgreiches Risikomanagement. Deshalb sollte auch das

Management sensibilisiert werden, sich verstärkt mit dem Thema auseinanderzusetzen.

Welche Rolle spielt der Faktor Mensch in Sicherheitsüberlegungen?

Bedrohungen der Sicherheit und Zuverlässigkeit der IT-Infrastruktur gehen in den meisten Fällen vom Menschen aus. Die Angreifer suchen immer wieder neue Methoden und Wege, die Infrastruktur zu schwächen oder in die Netzwerke einzudringen. Deshalb kann die Netzwerküberwachung und -sicherung nicht einfach an eine Software «aus dem Regal» delegiert werden. Die Überwachung der IT-Infrastruktur muss von Spezialisten übernommen werden, die mit Expertise und Erfahrung in der Lage sind, sich in die Denkweise der Angreifer hineinzusetzen, um die von den Überwachungssystemen gewonnenen Erkenntnisse richtig zu deuten und entsprechende Massnahmen einzuleiten.

Webapplikationen bieten Angriffsflächen, die von herkömmlichen Firewalls nicht geschützt werden können.

Wie kann man sich vor solchen Angriffen schützen?

Der effizienteste Schutz gegen Attacken auf Webapplikationen bietet der Application Shield, der in den offenen Ports in der Firewall – also im Fall einer Webseite dem Port 80 – die übermittelten Inhalte in Echtzeit auf bekannte Angriffsmuster überprüft oder den Zugang – je nach Anwendung – mit starker Authentisierung zusätzlich schützt. Anfragen, die als ungefährlich eingestuft werden, verbindet der Application Shield mit der entsprechenden Anwendung. Identifiziert der Application Shield einen Angriff, blockt er den Zugriff ab. Angreifer oder automatisierte Bedrohungen aus dem Internet werden so sehr effektiv abgewehrt. ■