COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/sicherheitsgefahren-werden-falsch-eingeschaetzt,2558001

IT-Security

Sicherheitsgefahren werden falsch eingeschätzt

Datum: 21.04.2014
Autor(en): Holger Eriksdotter

Die Mehrzahl der europäischen Unternehmen schätzt die Bedrohung durch externe Angriffe auf ihre IT falsch ein. Während sich die Aufmerksamkeit der IT-Abteilungen vor allem auf interne Sicherheitslücken richtet, wird die Gefahr durch Angriffe von Außen oft übersehen.

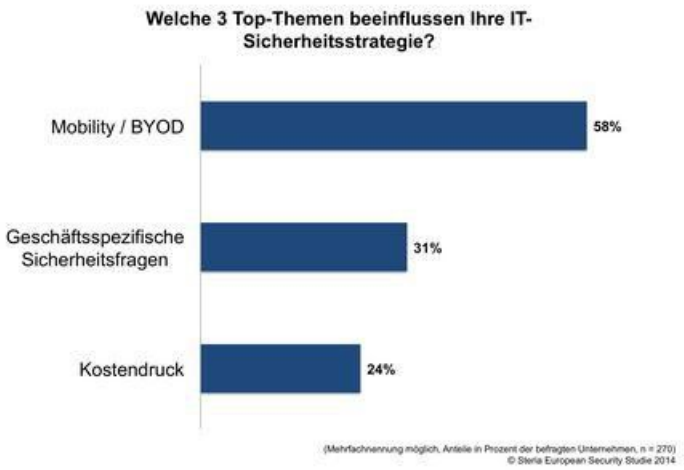
Mit der zunehmenden IT-Durchdringung aller Branchen und Industriezweige steigt auch das Risiko externer Cyber-Attacken. Dennoch steht das Thema laut einer Studie der Unternehmensberatung Steria und der Markforscher von Pierre Audoin Consultants (PAC) nur bei einer Minderheit der Unternehmen auf der Agenda.

Die mittel- und langfristigen Security-Planungen der meisten europäischen Unternehmen richten sich vor allem auf den Schutz vor internen Angriffen. So rechnet mehr als die Hälfte der für die Studie befragten europäischen Unternehmen nur 20 Prozent der Angriffe externen Quellen zu. Vor allem die Bedrohung durch das organisierte Verbrechen und die Spionage staatlicher Institutionen wird als äußerst gering eingeschätzt: Weniger als 15 beziehungsweise sechs Prozent wollen hier überhaupt ein Risiko erkennen.

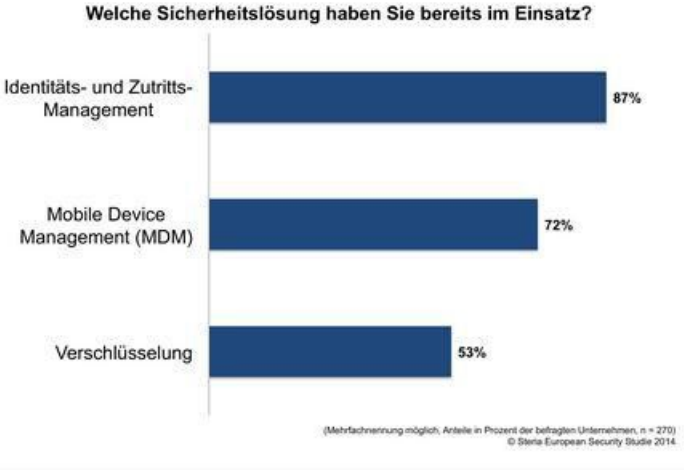
Gerald Spiegel, Leiter Information Security Solutions bei Steria Mummert Consulting
Foto: Steria Mummert Consulting

"Dass europäische Unternehmen Cyber-Attacken kaum Bedeutung beimessen, ist besorgniserregend, kommentiert Dr. Gerald Spiegel, Leiter Information Security Solutions bei Steria Mummert Consulting, die Ergebnisse. "In der Folge führen sie nicht die erforderlichen und angemessenen Sicherheitsprozesse und -technologien ein, um gegen aktuelle und zukünftige Risiken gewappnet zu sein."

Zwar hat unter dem Einfluss der Debatte um Spähprogramme wie Prism und Tempora die Sensibilität für externe Bedrohungen zugenommen. Die Ausspähung von Daten wird zunehmend als Gefahr eingeschätzt, 60 Prozent der Unternehmen bezeichnen Datenklau sogar als eine der drei größten Bedrohungen. Dabei schätzen sie Hackerangriffe als größte Gefahr ein, 22 Prozent verdächtigen sogar die Konkurrenz, sich mit kriminellen Mitteln Zugang zu ihrem Know-how verschaffen zu wollen.



Mobiltiy/ByoD ist das dominierende Thema für die IT-Sicherheitsstrategien der Unternehmen.
Foto: Steria Mummert Consulting



Um sich vor Angriffen zu schützen, setzen 77 Prozent der Unternehmen in Deutschland Authentifizierungs- und Zugriffsmanagement-Lösungen ein. Allerdings plant nur ein Fünftel die Einführung von Verschlüsselungstechnologien in den kommenden drei Jahren. Lediglich 14 Prozent der Unternehmen mit weniger als 5.000 Mitarbeitern haben ein sogenanntes Security Operation Center eingerichtet, um Abläufe und Ereignisse zu überwachen und um sicherzustellen, dass Anomalien aufgedeckt, identifiziert und klassifiziert werden, so dass mit geeigneten Maßnahmen reagiert werden kann.

"Unsere Studie belegt, dass viele Unternehmen Sicherheitsrisiken falsch einschätzen" beurteilt der Steria-Sicherheitsexperte Spiegel die Ergebnisse der Befragung, "Unternehmen müssen ihr IT-Sicherheitsniveau auf eine deutlich komplexere Bedrohungssituation einstellen, hier besteht dringender Handlungsbedarf."

Die Unternehmensberatung Steria hat in Zusammenarbeit mit dem Beratungs- und Analystenhaus Pierre Audoin Consultant (PAC) 270 Entscheider in europäischen Unternehmen verschiedener Branchen mit 500 bis über 5000 Mitarbeitern befragt, 72 davon aus Deutschland. Im Mittelpunkt der Befragung standen die Strategien der Unternehmen im Hinblick auf aktuelle und zukünftige IT-Bedrohungen.
