Umfrage zu Cyber- und Cloud-Sicherheit in deutschen Unternehmen

Firmen verschlafen Cyber-Risiken

06.01.15 | Redakteur: Peter Schmitz

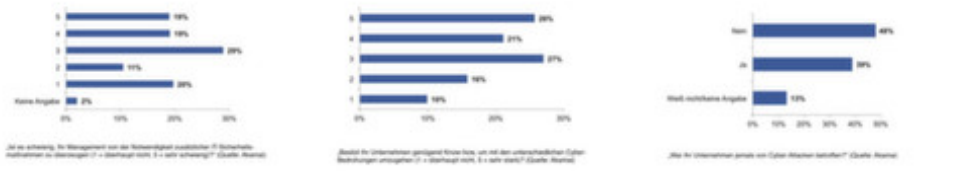
Obwohl viele Unternehmen die Gefahren von Cyber-Attacken kennen und sogar schon Opfer wurden, tun sie zu wenig, um sich ausreichend zu schützen. Das ist das Ergebnis einer Umfrage des Cloud-Sicherheitsexperten Akamai.

Cyber-Attacken, die auf den Ausfall von Websites oder das Ausspionieren von Firmengeheimnissen zielen, sind mittlerweile in der Alltagsrealität angekommen und in der breiten Öffentlichkeit bekannt.

In Unternehmen schätzten 61 Prozent der Befragten aus 150 Unternehmen das Bedrohungsrisiko als "hoch" oder "sehr hoch" ein; eine beachtlich hohe Zahl konnte überdies aus erster Hand berichten, denn 39 Prozent aller Befragten gaben an, dass ihr Unternehmen selbst schon Opfer von Cyber-Attacken geworden ist.

Konsequenzen werden daraus aber nicht immer gezogen, denn es besteht ein deutliches Missverhältnis zwischen Gefahrenbewusstsein und Handlungsbereitschaft. Erstens beklagte mehr als die Hälfte (53 Prozent), dass das eigene Unternehmen

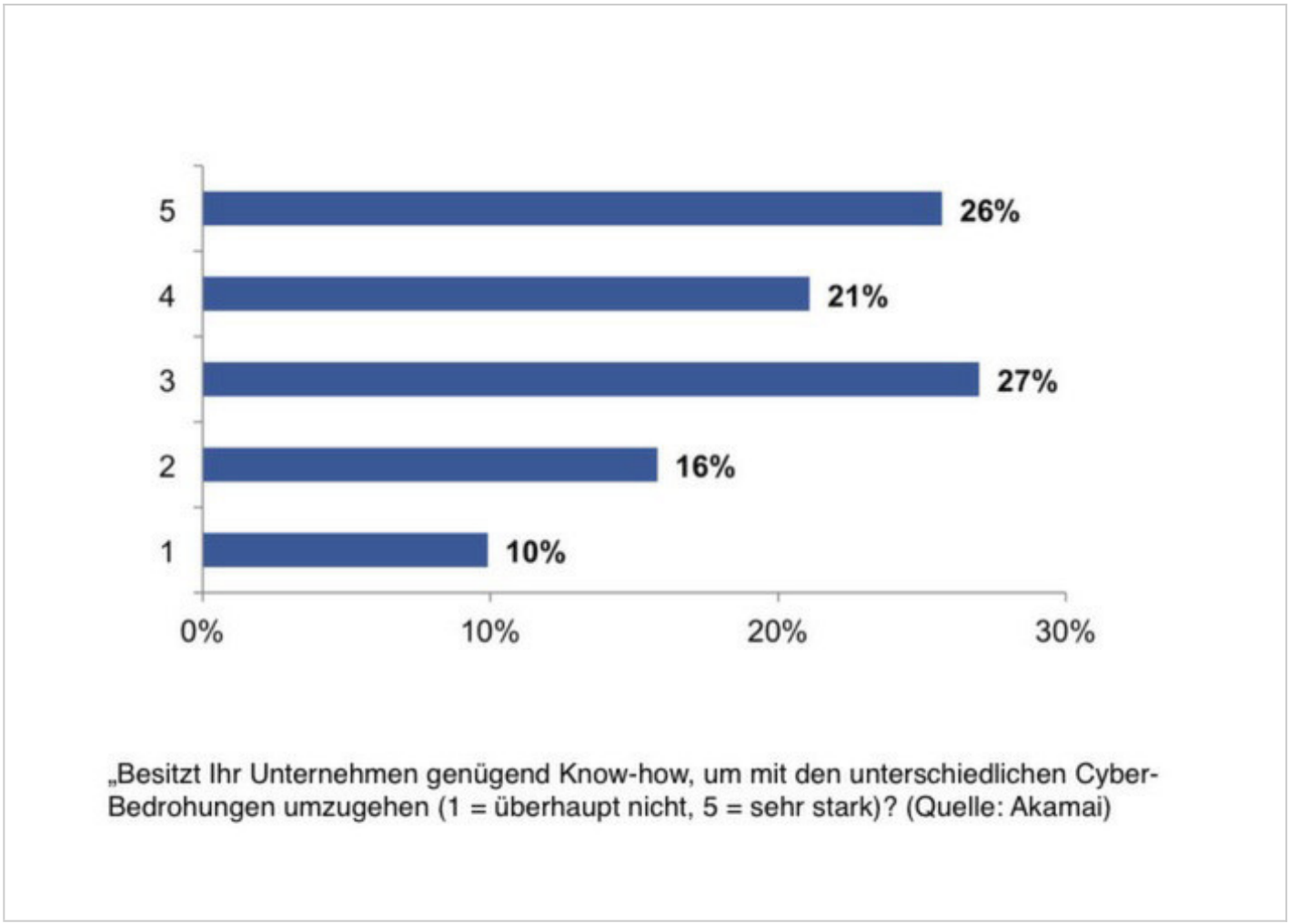
nicht genügend Know-how besitzt, um mit Cyber-Bedrohungen umzugehen. Zweitens bedauerten nahezu 40 Prozent der Befragten, es sei "schwierig" oder "sehr schwierig", das Management für Investitionen in IT-Sicherheit zu gewinnen.



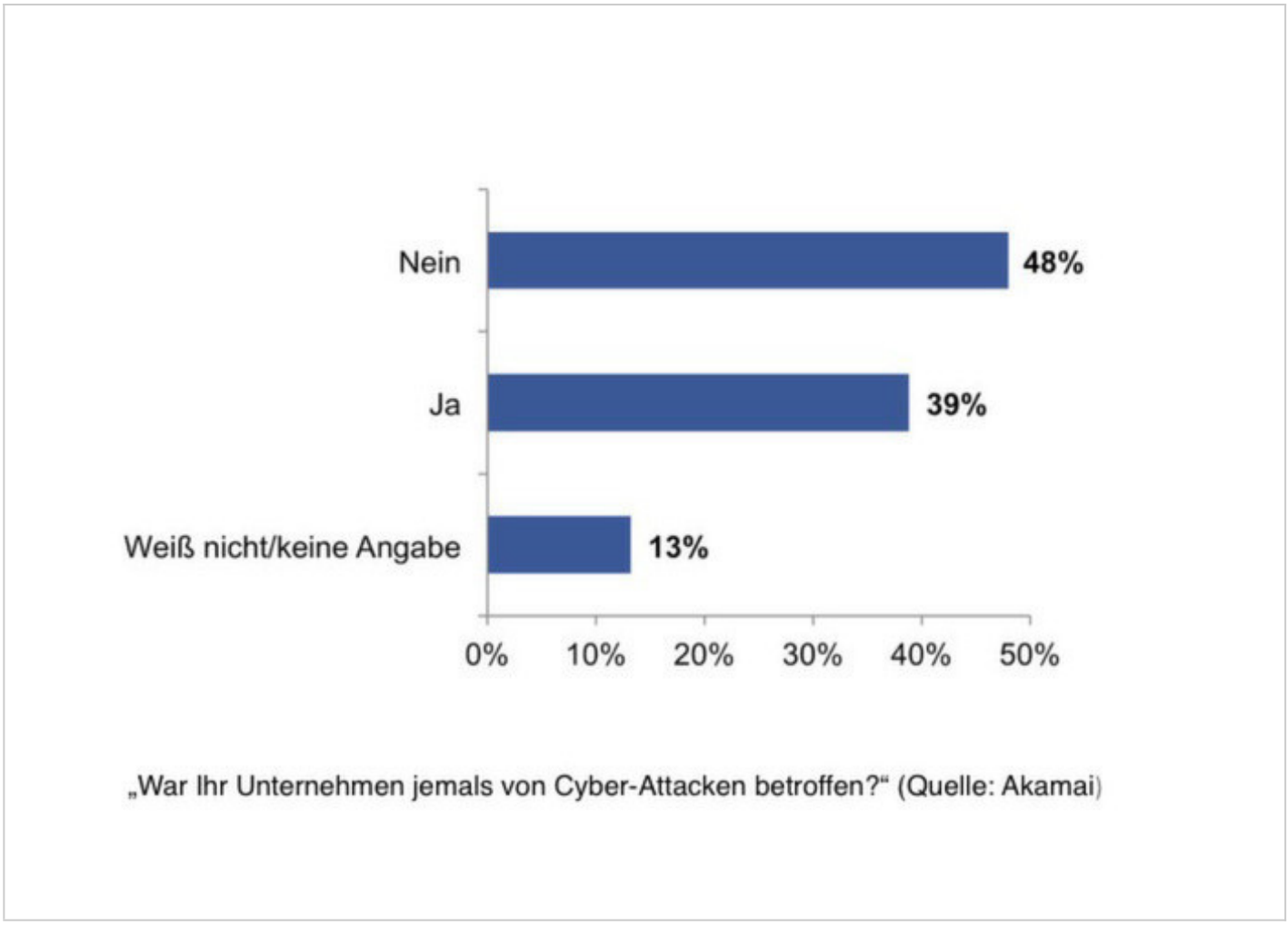
Fotostrecke starten: Klicken Sie auf ein Bild (4 Bilder)

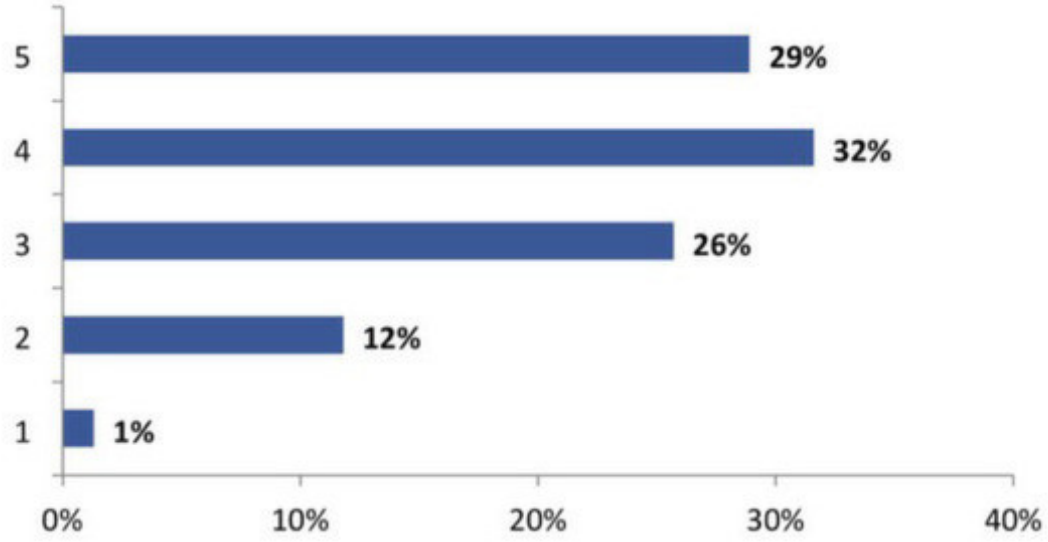
"Das Missverhältnis zwischen den Gefahren, die von Hackerangriffen und Industriespionage ausgehen, und tatsächlichen Maßnahmen zum Schutz vor Datendiebstahl ist überraschend", sagt Jürgen Metko, Regional Sales Director Central Europe bei Akamai in Garching bei München. "Viele Unternehmen waren bereits Opfer von Cyber-Angriffen, die voraussichtlich einen hohen materiellen und Imageschaden angerichtet haben. Der Aufbau eines effektiven Schutzwalls, um Angriffe rechtzeitig abzuwehren, ist daher empfehlenswert."

Handlungsbedarf besteht also. Erstens sollte die IT stärker als bislang darauf achten, Sicherheits-Expertise aufzubauen – sei es durch organisatorische oder Weiterbildungsmaßnahmen oder über den Ausbau der Belegschaft. Zweitens müsste das Management Mittel einfacher zur Verfügung stellen – für den Wissensausbau einerseits und für wirkungsvolle Abwehrmaßnahmen gegen Cyber-Angriffe andererseits.


5
4
3
2
1
26%
21%
27%
16%
10%
0%
10%
20%
30%
„Besitzt Ihr Unternehmen genügend Know-how, um mit den unterschiedlichen Cyber-Bedrohungen umzugehen (1 = überhaupt nicht, 5 = sehr stark)? (Quelle: Akamai)

(Bild: Akamai)


Nein
48%
Ja
39%
Weiß nicht/keine Angabe
13%
0%
10%
20%
30%
40%
50%
„War Ihr Unternehmen jemals von Cyber-Attacken betroffen?“ (Quelle: Akamai)
(Bild: Akamai)



„Wie schätzen Sie das Risiko von Cyber-Angriffen wie Advanced Persistent Threats (APTs), DDoS- und Web-Applikations-Attacken auf einer Skala 1 bis 5 ein (1 = sehr niedrig, 5 = sehr hoch)?“ (Quelle: Akamai)

(Bild: Akamai)

Bei deutschen Unternehmen gibt es ein klares Missverhältnis zwischen den Gefahren, die von Hackerangriffen und Industriespionage ausgehen, und tatsächlichen Maßnahmen zum Schutz vor Datendiebstahl. (Bild: apops - Fotolia.com)

Bei deutschen Unternehmen gibt es ein klares Missverhältnis zwischen den Gefahren, die von Hackerangriffen und Industriespionage ausgehen, und tatsächlichen Maßnahmen zum Schutz vor Datendiebstahl. (Bild: apops - Fotolia.com)