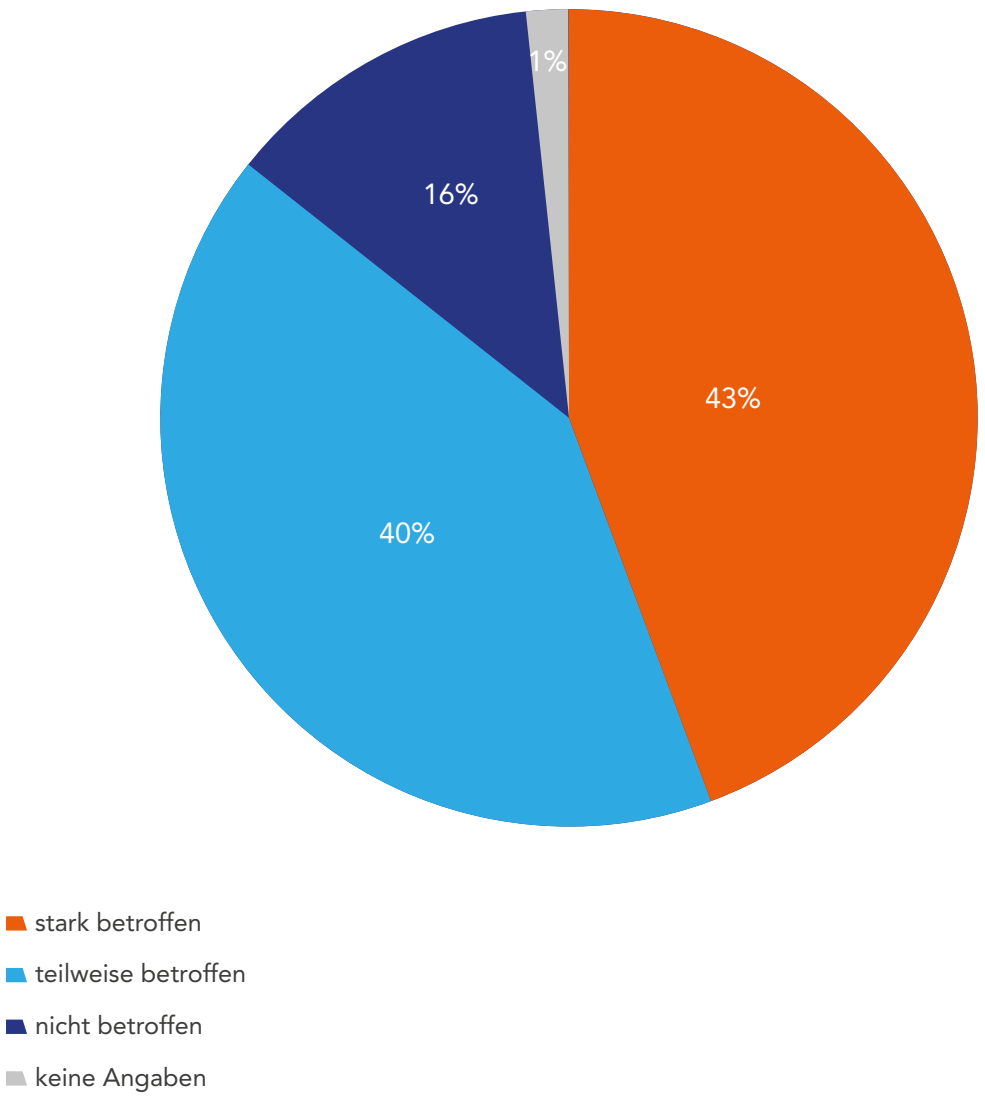
CyberDirekt

Cybersicherheit in kleinen und mittleren Unternehmen

Ergebnisse einer Befragung des Marktforschungsinstituts INNOFACT
von 305 Unternehmen im Juni 2018

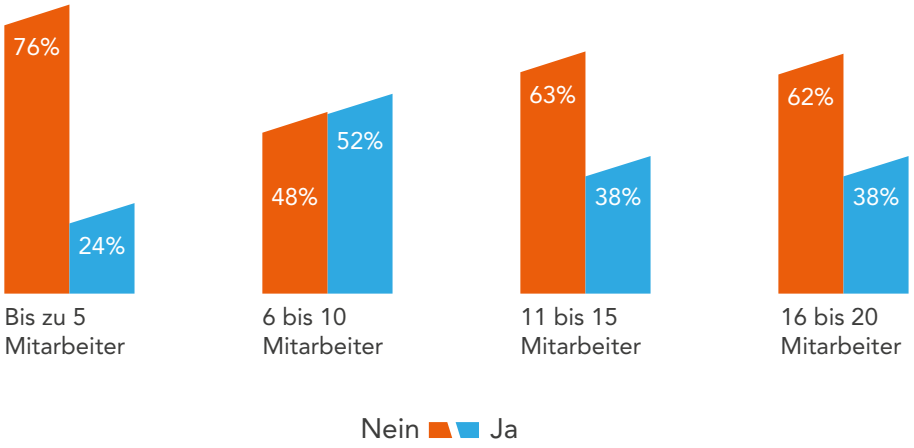
Cyberrisiken sind für Unternehmen jeglicher Größe ein allgegenwärtiges Risiko geworden. Das Ausmaß der Gefahr haben spätestens die großflächigen Angriffe wie Wannacry oder NotPetya im Jahr 2017 gezeigt. Während Konzerne sich dieser Bedrohungslage schon länger bewusst sind, ist bisher wenig über die Risikosituation bei kleineren Unternehmen bekannt. Aus diesem Grund hat CyberDirekt in Zusammenarbeit mit dem Marktforschungsunternehmen INNOFACT 305 Betriebe in einer Studie zum Thema „Cybersicherheit in kleinen und mittleren Unternehmen" befragt. Die Untersuchung analysiert sowohl die Wahrnehmung der aktuellen Bedrohungslage, als auch den Verbreitungsgrad von Präventions- und Absicherungsmaßnahmen.

1 Wie stark schätzen Sie die Bedrohungslage für Ihr Unternehmen ein, Opfer einer Cyber-Attacke zu werden?



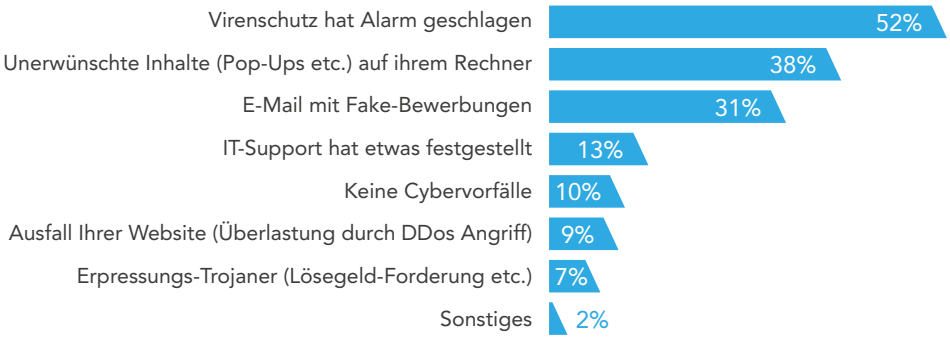
Nur ein Viertel der Kleinstunternehmer kennt aus dem direkten Umfeld mindestens einen anderen Betrieb, welcher schon von einem Cyber-Angriff betroffen gewesen ist. Bei größeren Unternehmen ist dieser Anteil deutlich höher.

2 Haben Sie in den letzten 2 Jahren in Ihrem Umfeld von einem Unternehmen gehört, das Opfer einer Cyber-Attacke geworden ist?



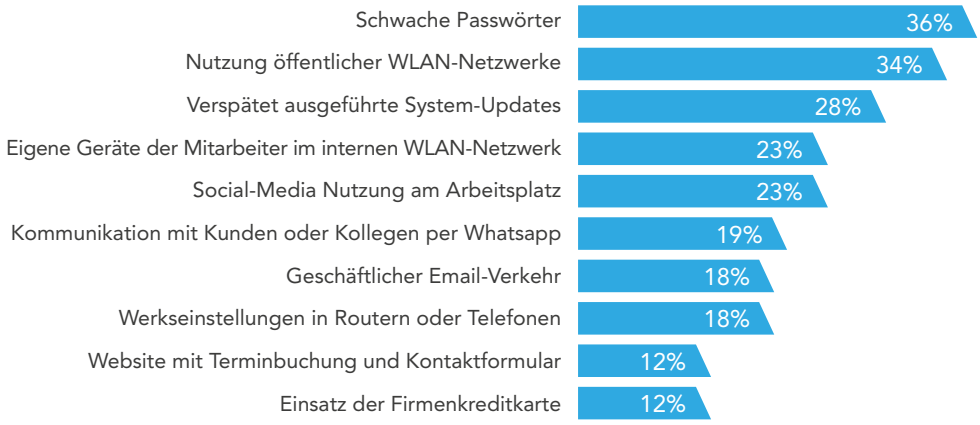
Im eigenen Unternehmen ist die Bedrohungslage fast allgegenwärtig. Nur 10% der kleinen und mittelständischen Unternehmen waren in den letzten 2 Jahren überhaupt nicht von einem Cyber-Vorfall betroffen.

3 Hat es auf Ihr Unternehmen in den letzten 2 Jahren bereits einen oder mehrere Cyberangriffe gegeben?



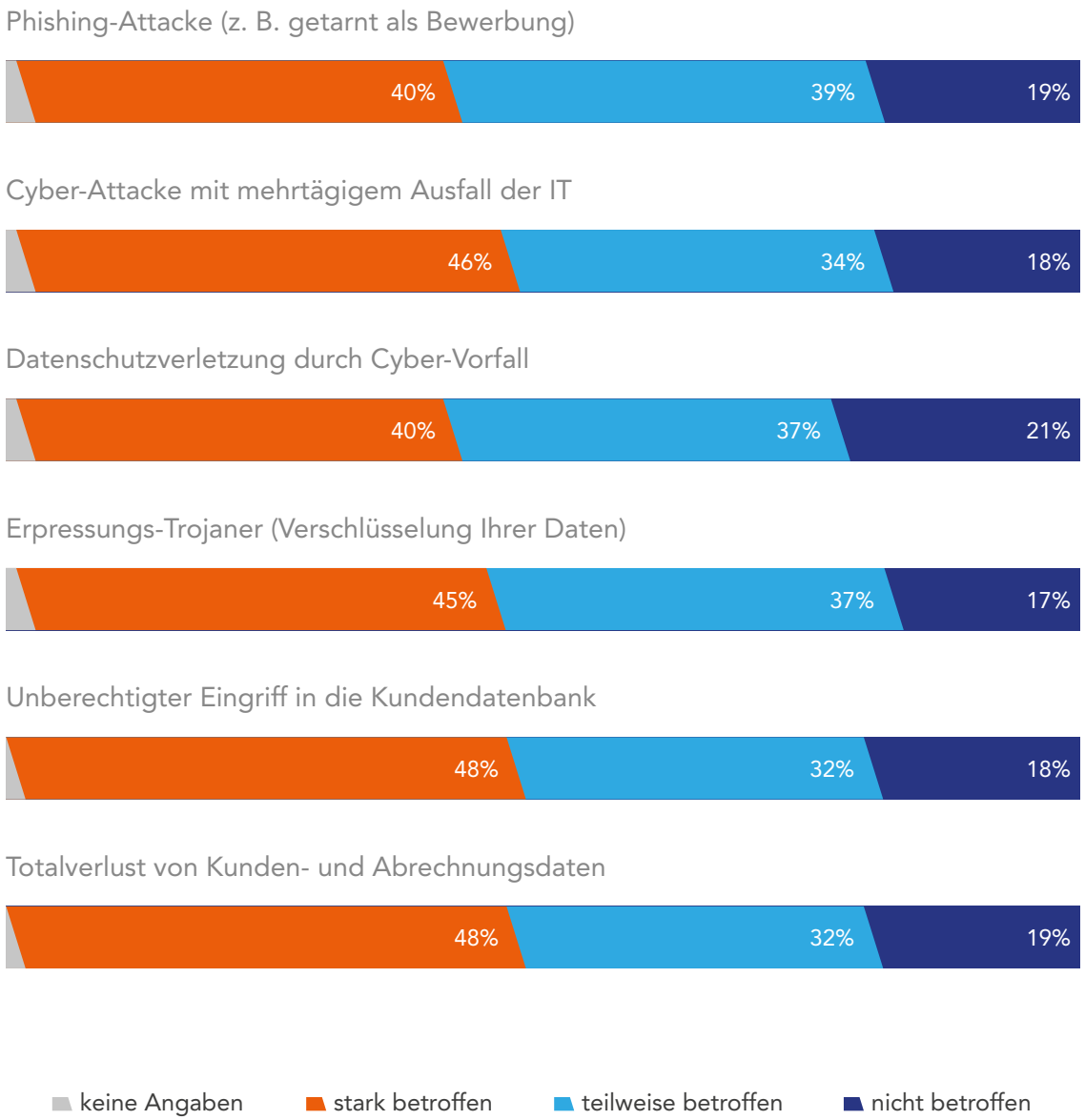
Im direkten Arbeitsumfeld werden viele Gefahrenquellen als bedrohlich angesehen, die mit menschlichen Verhaltensweisen zusammenhängen (z.B. „Schwache Passwörter" bzw. „Social-Media Nutzung am Arbeitsplatz"). „Geschäftlicher Email Verkehr" wird jedoch nur von 18% der Befragten als größte Bedrohung eingeschätzt. Dies ist bemerkenswert, da nahezu jedes Unternehmen Emails zur betrieblichen Kommunikation verwendet und infolge dessen von daraus resultierenden Gefahren wie Phishing oder Anhängen mit versteckter Schadsoftware betroffen sein kann.

4 Was ist Ihrer Meinung nach die größte Gefahrenquelle in Ihrem Arbeitsumfeld?



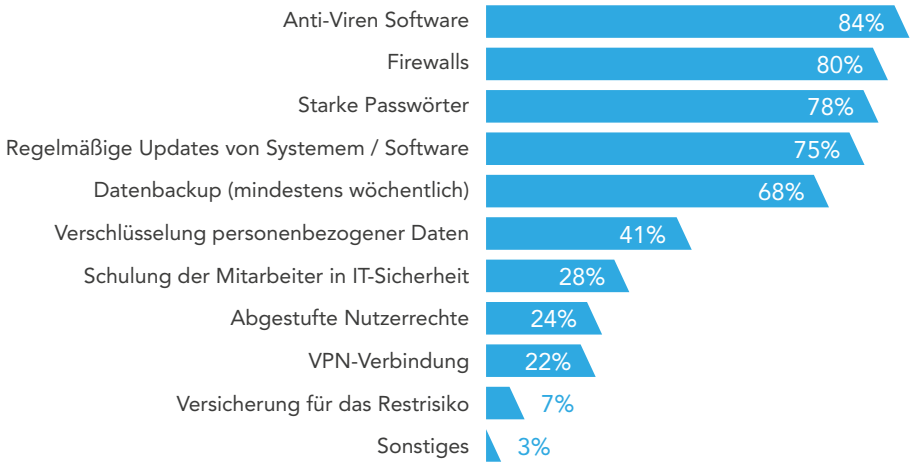
Die Bedrohungslage konzentriert sich nicht nur auf ein einzelnes Angriffsmuster, sondern verteilt sich auf mehrere potentielle Risikoszenarien einer Cyberattacke. Insbesondere ein unberechtigter Eingriff in die Kundendatenbank bzw. ein Totalverlust ebendieser Daten wird als schwerwiegendes Risiko angesehen.

5 Wie stark fühlen Sie sich von den folgenden Risiken in Bezug auf Ihr Unternehmen betroffen?



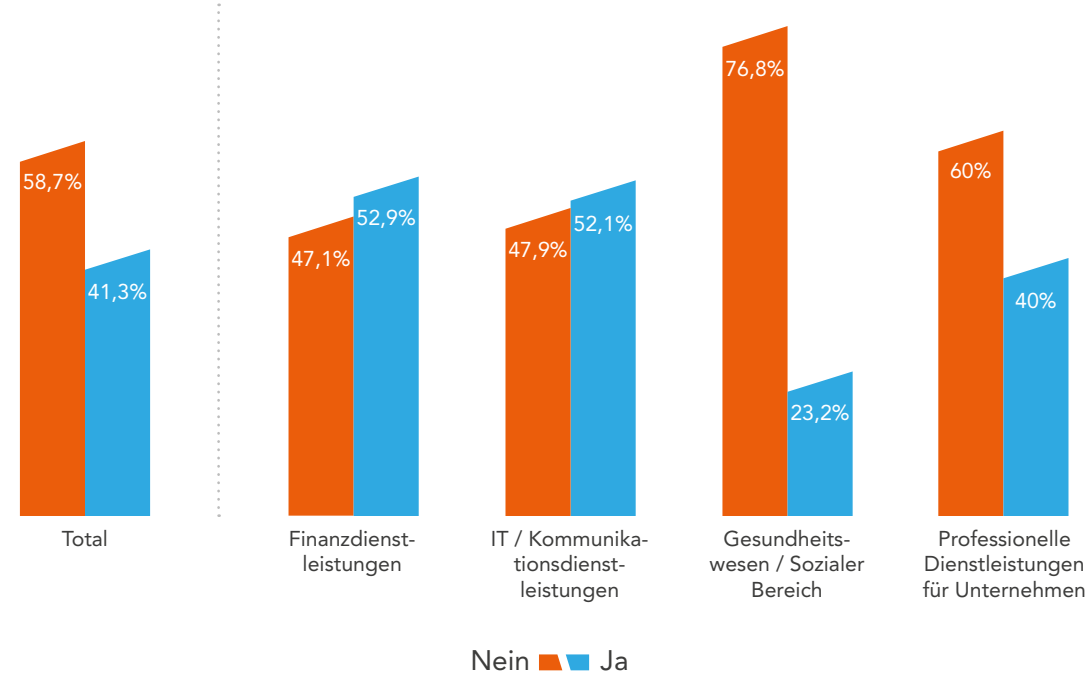
Während gängige technische Schutzmaßnahmen wie Firewalls und starke Passwörter von den meisten Unternehmen genutzt werden, führen nur zwei Drittel der Befragten regelmäßig ein Datenbackup durch. Ebenfalls sensibilisieren und schulen deutlich weniger als ein Drittel der befragten Betriebe Ihre Mitarbeiter. Dies ist umso bemerkenswerter, als menschliche Verhaltensweisen mit vielen Gefahrenquellen am Arbeitsplatz eng verknüpft sind (siehe Grafik 4).

6 Welche Maßnahmen zur Absicherung gegen die Folgen von Cybercrime (Hackerangriffe, Datendiebstahl etc.) nutzen Sie in Ihrem Unternehmen?



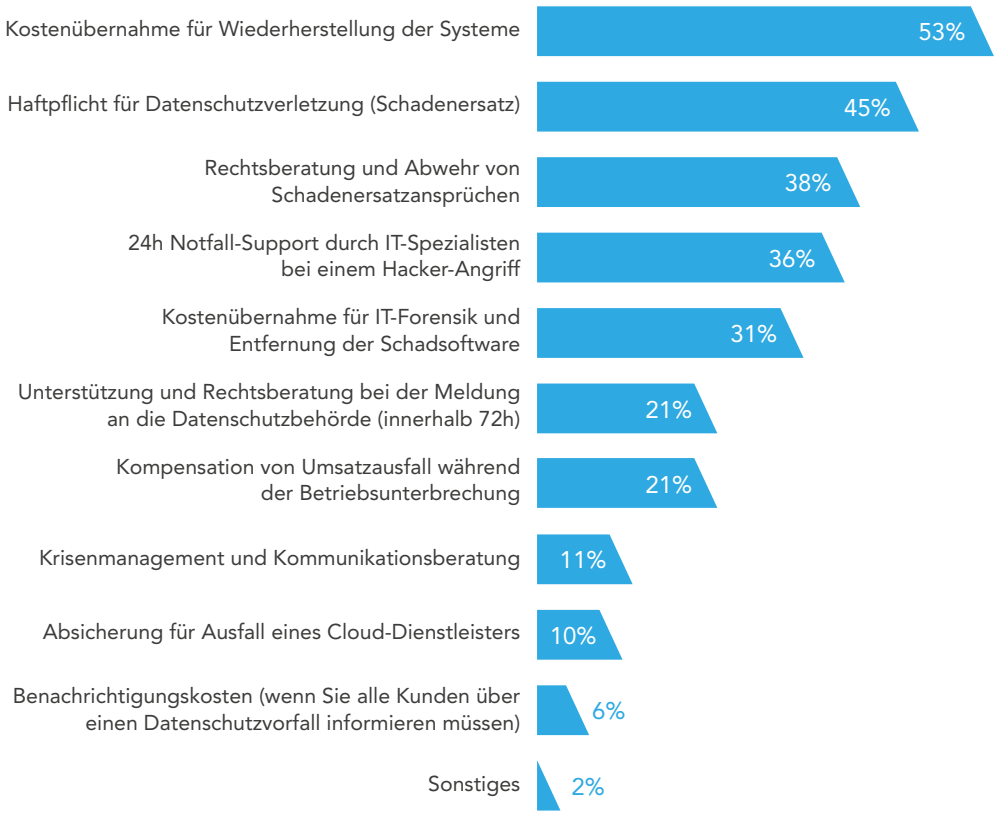
Die überwiegende Mehrheit der kleinen und mittelständischen Unternehmen nutzt Präventionsmaßnahmen technischer Natur (vgl. Grafik 6). Im Gegensatz dazu ist nur 40% der Befragten überhaupt bekannt, dass sich Betriebe mit einer Cyber-Versicherung ökonomisch gegen die Folgen eines Hacker-Angriffs absichern können.

7 Haben Sie schon einmal von der Möglichkeit gehört, gegen die Folgen eines Hacker-Angriffs eine Versicherung abzuschließen?



Obwohl die Cyber-Versicherung als Instrument des Risikomanagements bei kleineren Unternehmen noch überwiegend unbekannt ist, werden einzelne Bausteine der Deckung als sehr sinnvolle Dienstleistungen angesehen. Dies gilt insbesondere für die Kostenerstattung zur Wiederherstellung der IT-Systeme des Betroffenen.

8 Welche der folgenden Leistungen wären für Sie am wichtigsten?



Wir freuen uns von Ihnen zu hören!

www.cyberdirekt.de

CyberDirekt
Ihr Schutz gegen digitale Risiken

Cari GmbH
Köpenicker Str. 154A
Aufgang D
10997 Berlin

E-Mail: info@cyberdirekt.de
Telefon: 030 403660 36