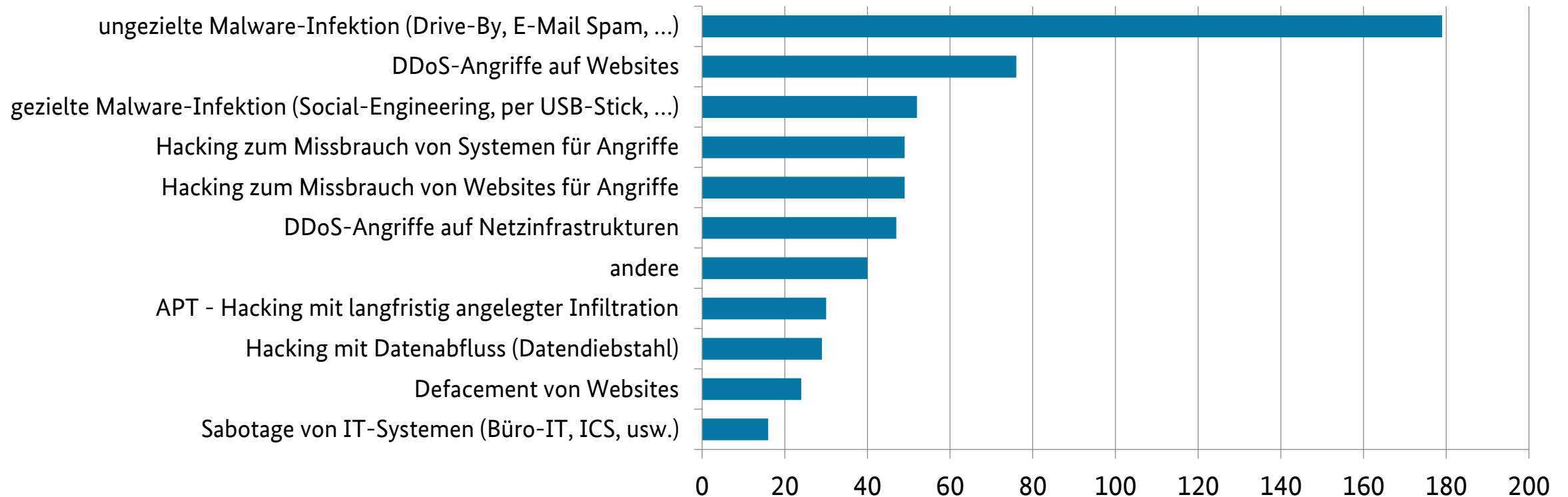
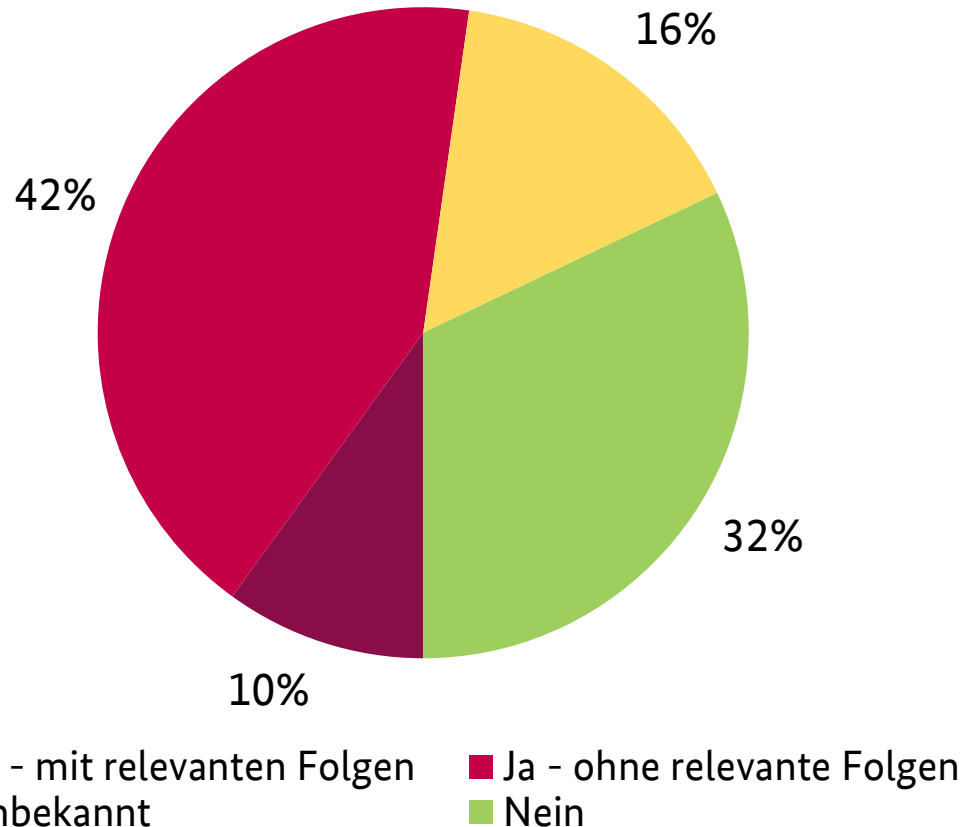


Welcher Art waren die 2014/2015 festgestellten Angriffe?

Von 248 Befragten gaben ... folgende Arten von Angriffen an



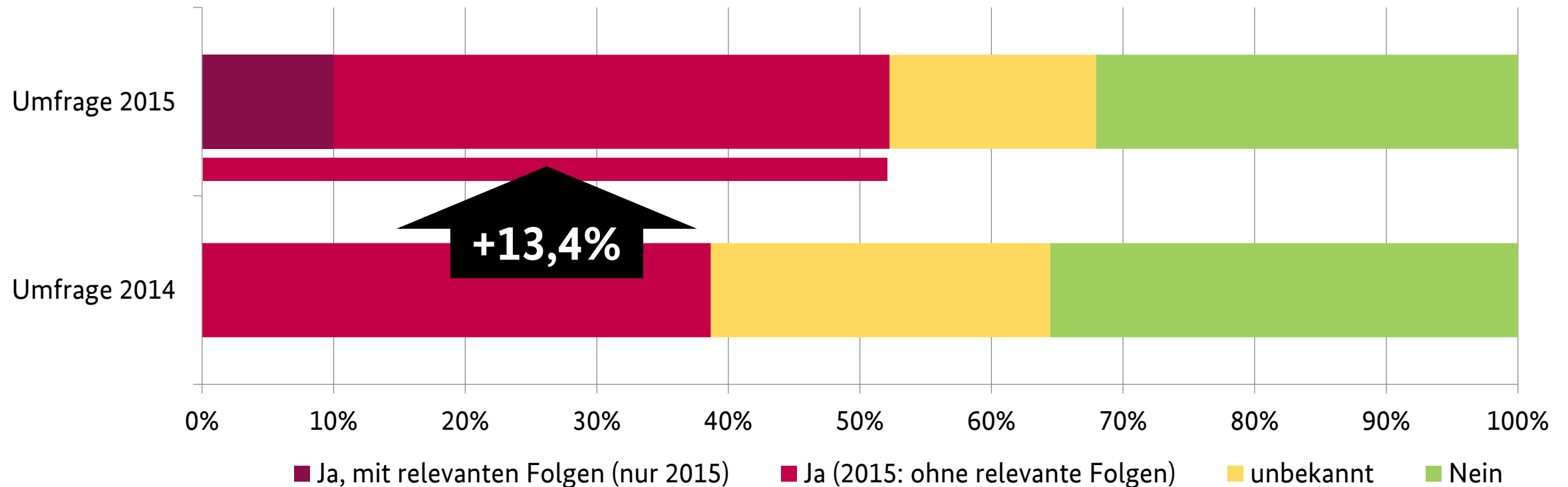
War die Institution der Befragten (überhaupt schon einmal) das Ziel eines erfolgreichen Cyber-Angriffs?



- **9,9% der Institutionen war bereits Opfer eines Cyber-Angriffs mit relevanten Folgen**
- 42% waren bereits durch erfolgreiche Cyber-Angriffe betroffen, diese blieben aber ohne relevante Folgen
- 31,8% der Befragten verneinten die Frage
- 15,6% gaben „unbekannt“ an

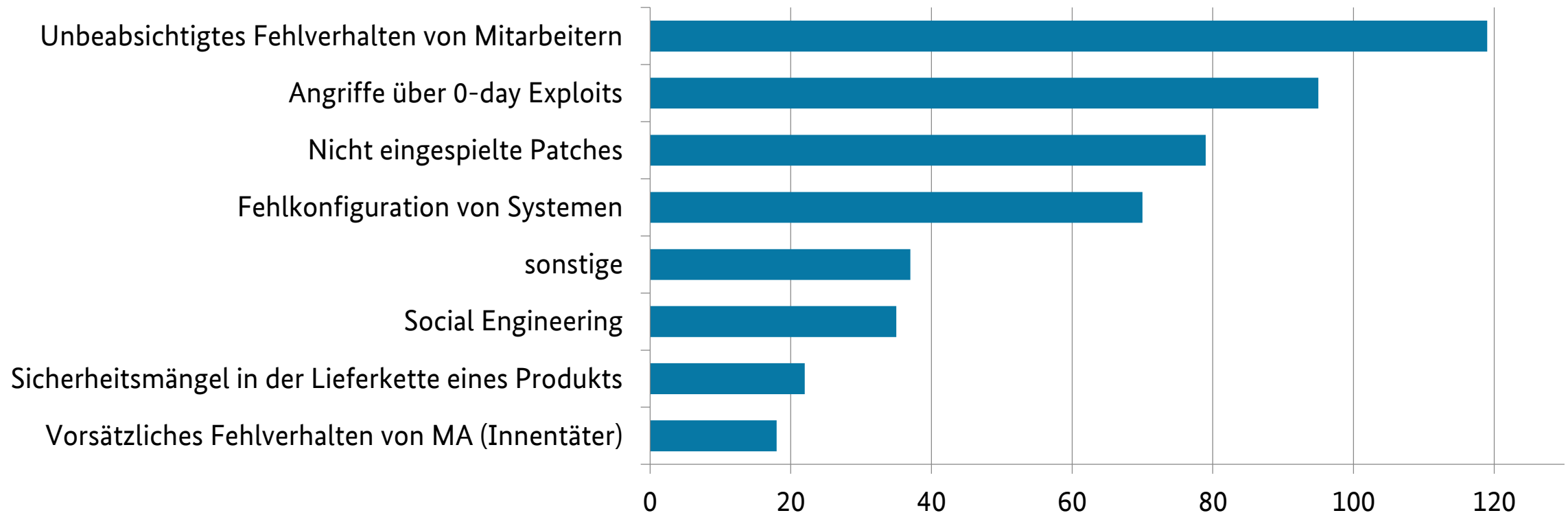
War die Institution der Befragten (überhaupt schon einmal) das Ziel eines erfolgreichen Cyber-Angriffs?

Vergleich der Werte aus den Umfragen 2015 und 2014



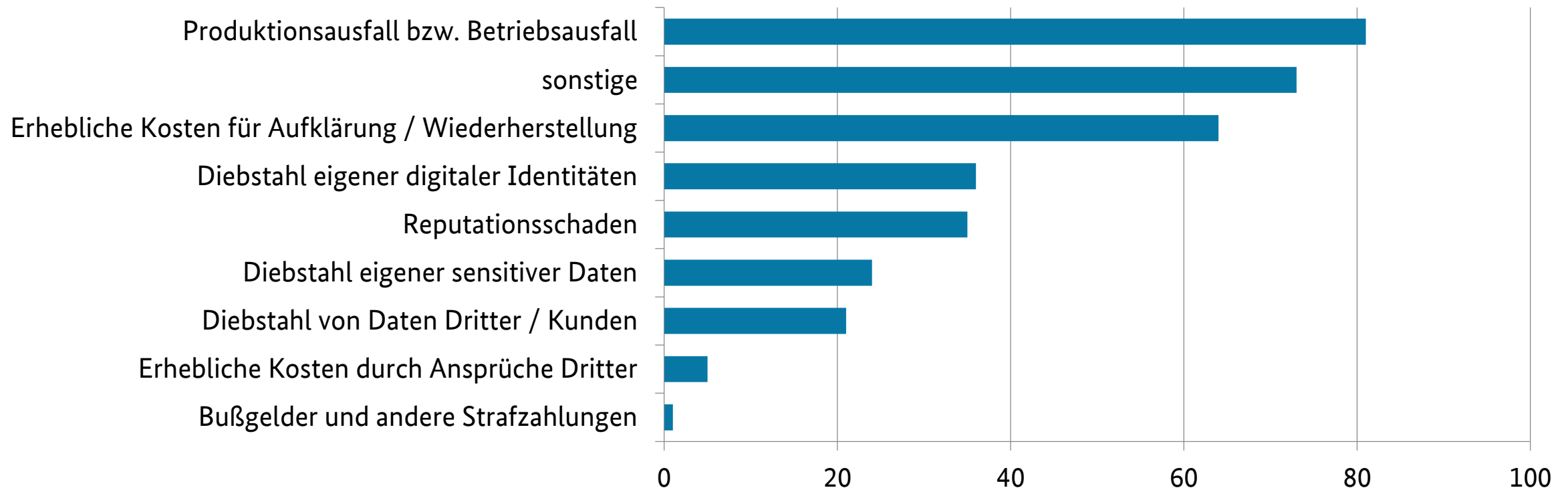
Falls eine Institution schon einmal Ziel eines erfolgreichen Cyber-Angriffs war, worauf war der Erfolg zurückzuführen?

Von 220 Befragten gaben ... folgende Ursachen für den Erfolg der Angriffe an



Falls eine Institution schon einmal Schäden durch Cyber-Angriffe erlitten hat, welcher Art waren diese?

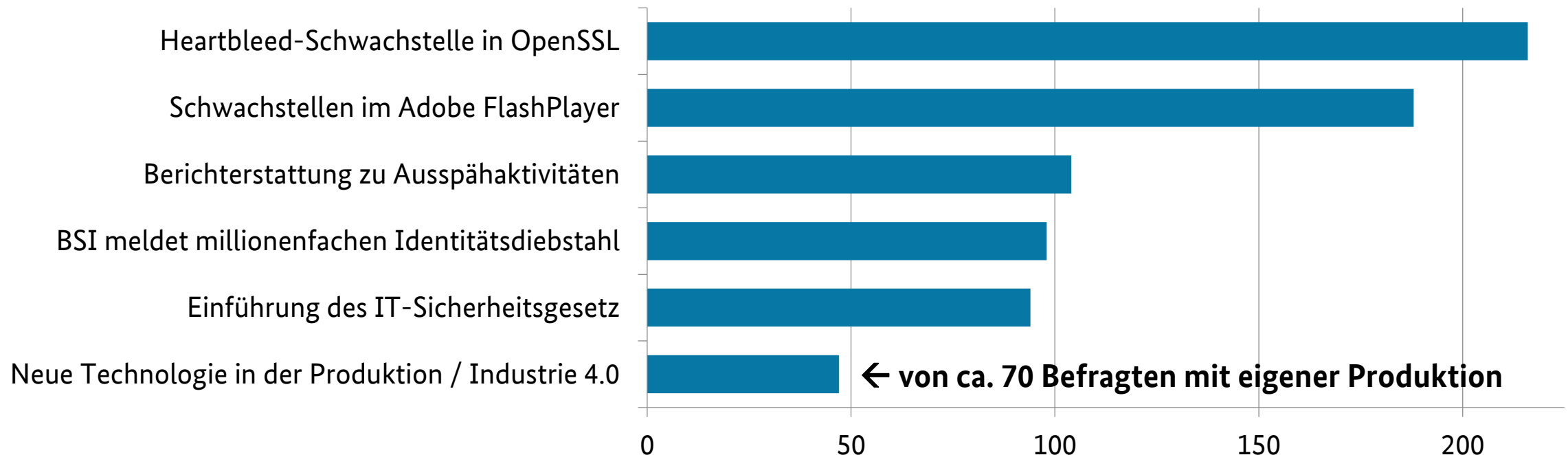
Von 220 Befragten gaben ... folgende Schäden an



Einschätzung der Cyber-Sicherheitslage

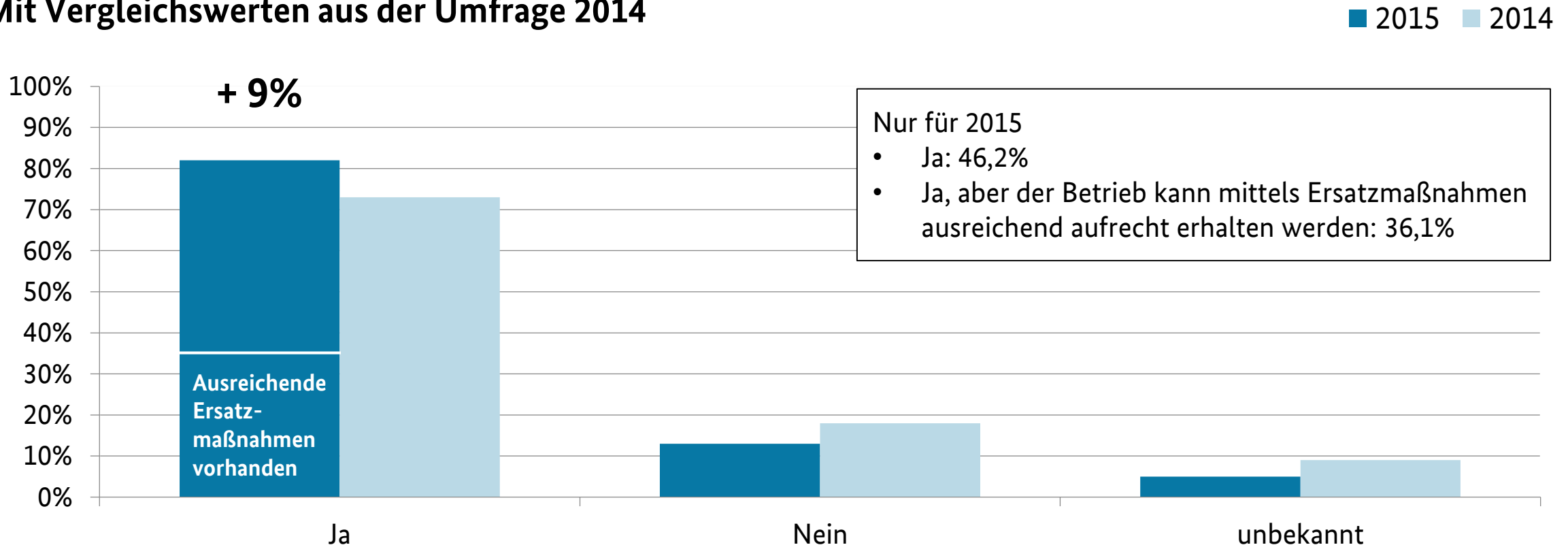
Welche der Ereignisse aus den Jahren 2014/2015 waren Auslöser für Maßnahmen zur Verbesserung der IT-Sicherheit in den Institutionen der Befragten?

Von 424 Befragten gaben jeweils ... an

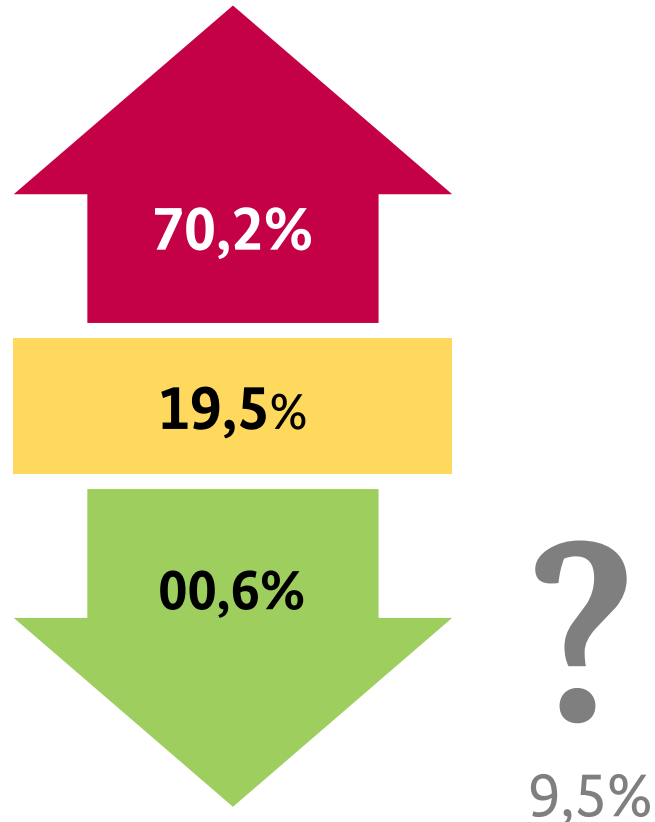


Stellen Cyber-Angriffe eine relevante Gefährdung für die Betriebsfähigkeit der Institutionen dar?

Mit Vergleichswerten aus der Umfrage 2014



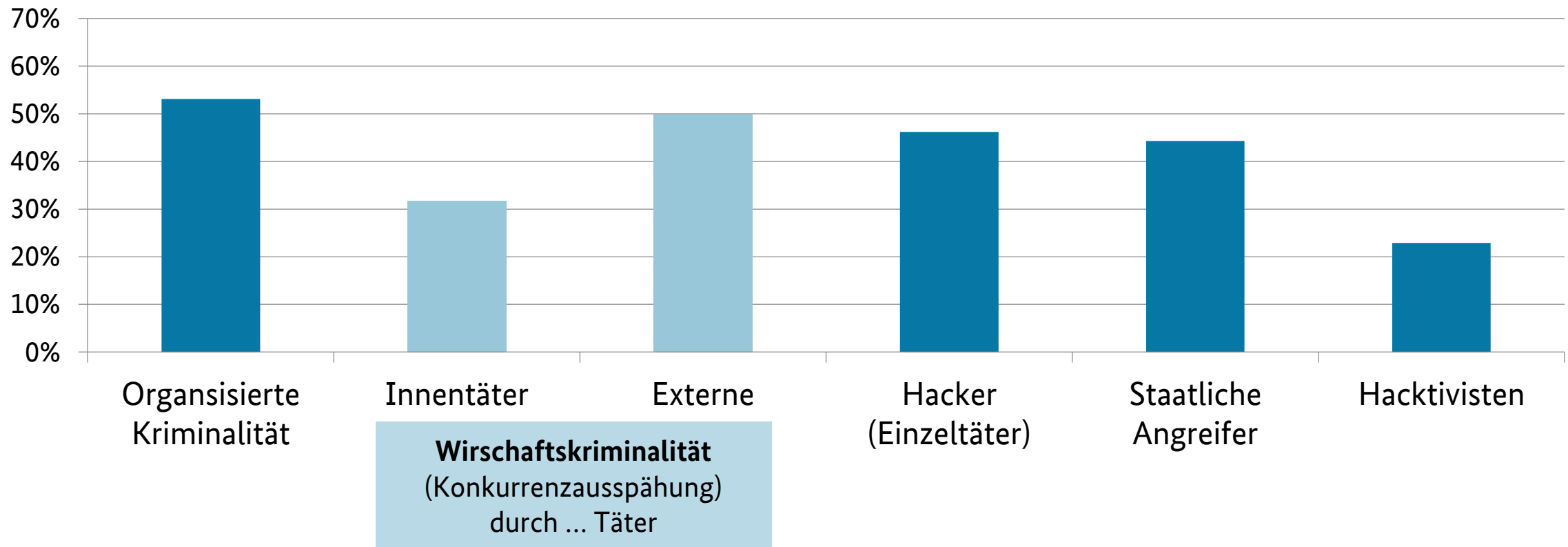
Falls Cyber-Angriffe eine relevante Bedrohung für die Betriebsfähigkeit der Institution darstellen, wie hat sich die Risikobewertung in den letzten 2 Jahren verändert?



- **70,2% bewerten Cyber-Risiken als zunehmend**
- 19,5% sehen keine Veränderung
- 0,6% der Befragten erkennen ein sinkendes Risiko
- 9,5% gaben „unbekannt“ an
- Alle genannten Werte entsprechen in etwa den Werten aus der Umfrage 2014

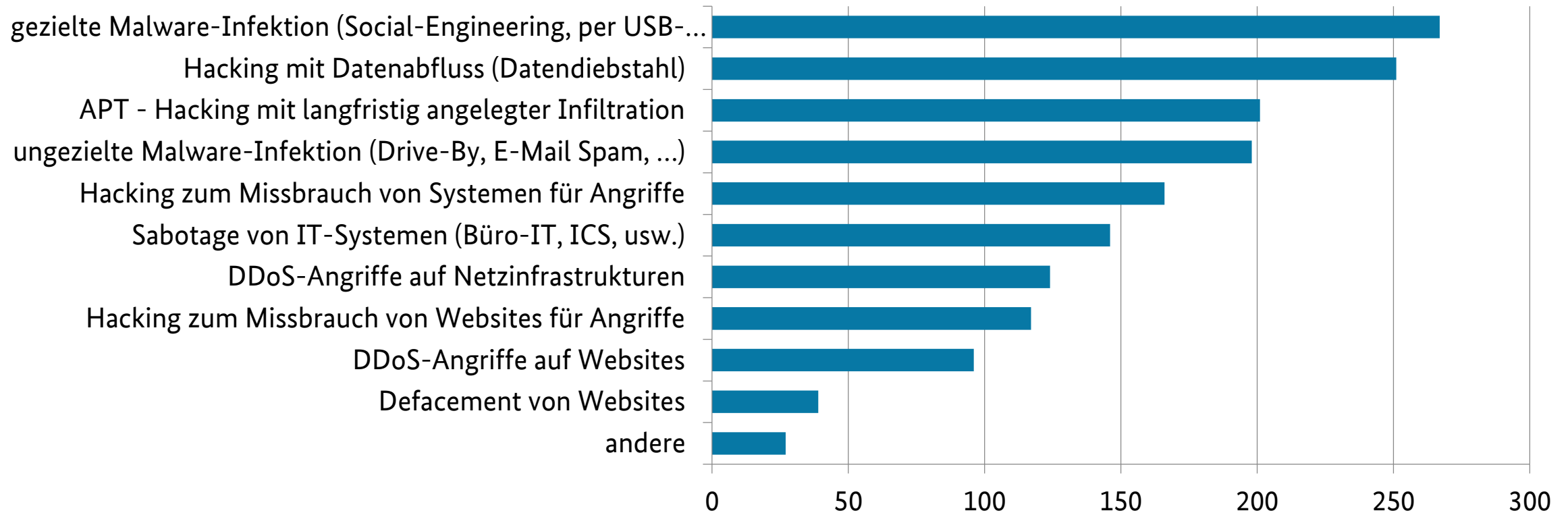
Welcher Gruppe von Cyber-Angreifern messen die Befragten für die kommenden 2 Jahre das größte Bedrohungspotenzial bei?

Von 424 Befragten gaben jeweils ... % an



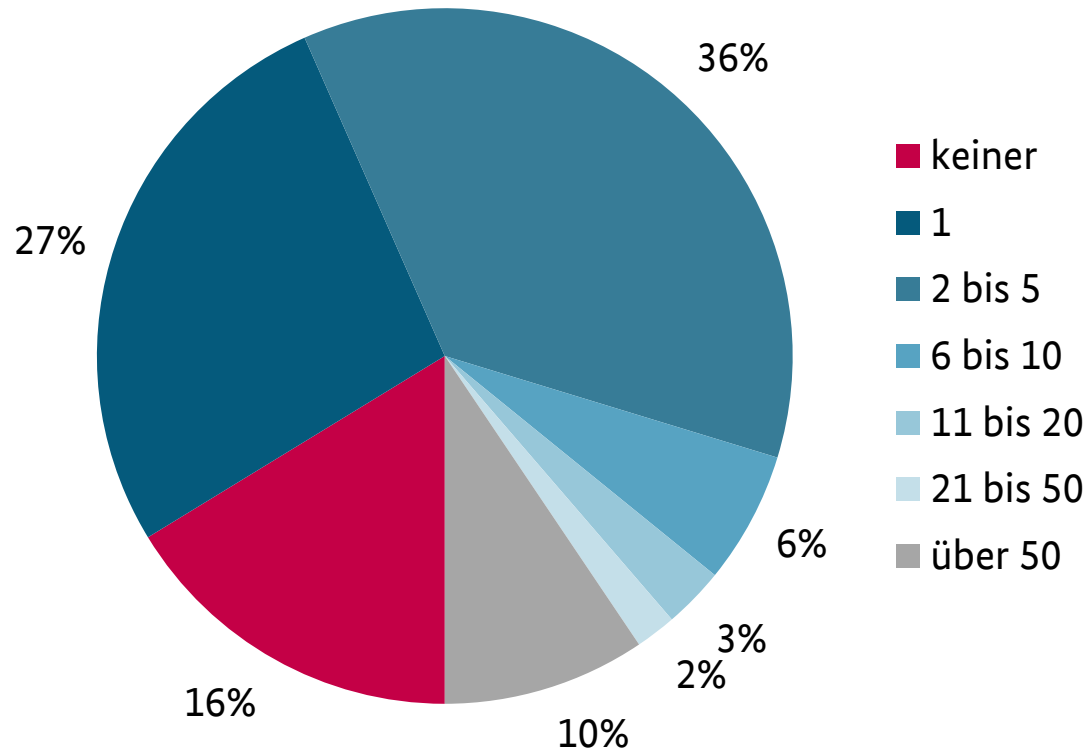
Welchen Arten von Cyber-Angriffen messen die Befragten für die kommenden 2 Jahre das größte Bedrohungspotential bei?

Von 424 Befragten gaben jeweils ... an



Maßnahmen zum Schutz vor Cyber-Angriffen

Wie viele Mitarbeiter sind in der jeweiligen Institution überwiegend (> 50% Zeitanatz) mit Aufgaben der eigenen IT-Sicherheit beschäftigt

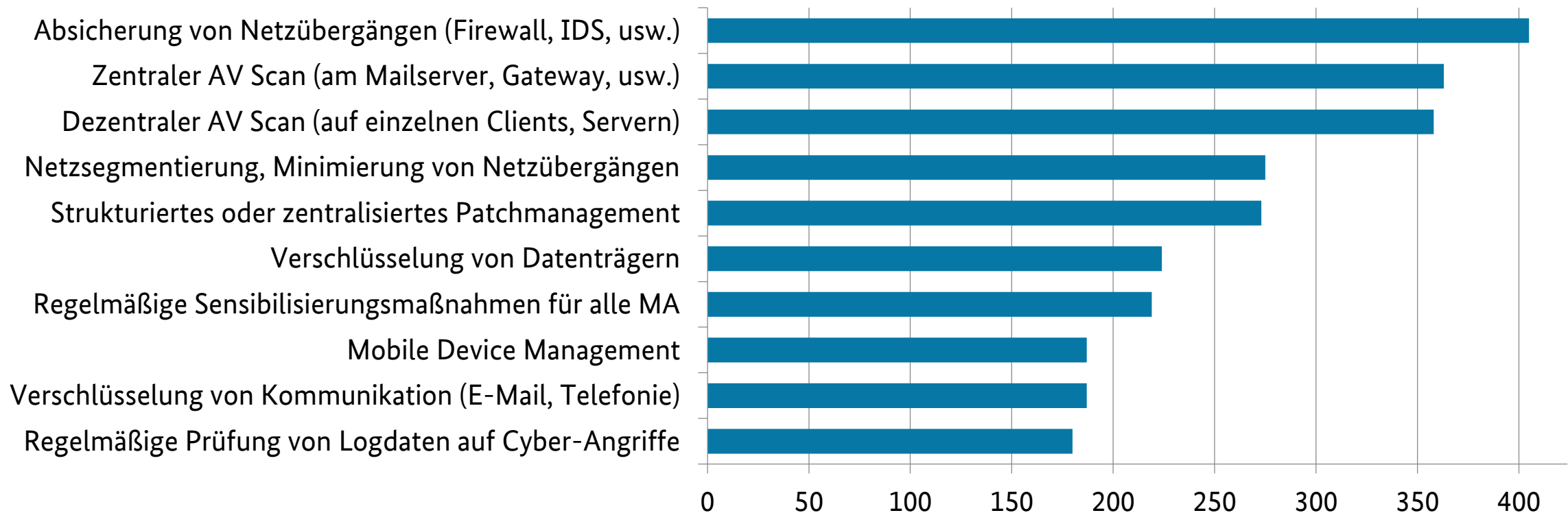


- **16,3% antworteten: keiner**
davon hatten 60% der Institutionen < 250 und 85% der Institutionen < 1.000 Mitarbeiter
- **27,1% antworteten: 1**
davon 45% < 50; 80% < 1.000 MA
- **36,3% antworteten: 2 bis 5**
davon 50% < 250; 72% < 1.000; 94% < 10.000 MA

Anmerkung zum Fall „über 50“: In der Detailauswertung zeigt sich, dass ein kleiner Teil der Antworten entsprechend Gesamt-Mitarbeiterzahl und Branche noch plausibel sein könnte. Der Überwiegende Teil dürfte aber auf Missverständnisse zurückzuführen sein z.B. Anzahl der insgesamt vorhandenen Experten bei IT-Sicherheitsdienstleistern, usw.

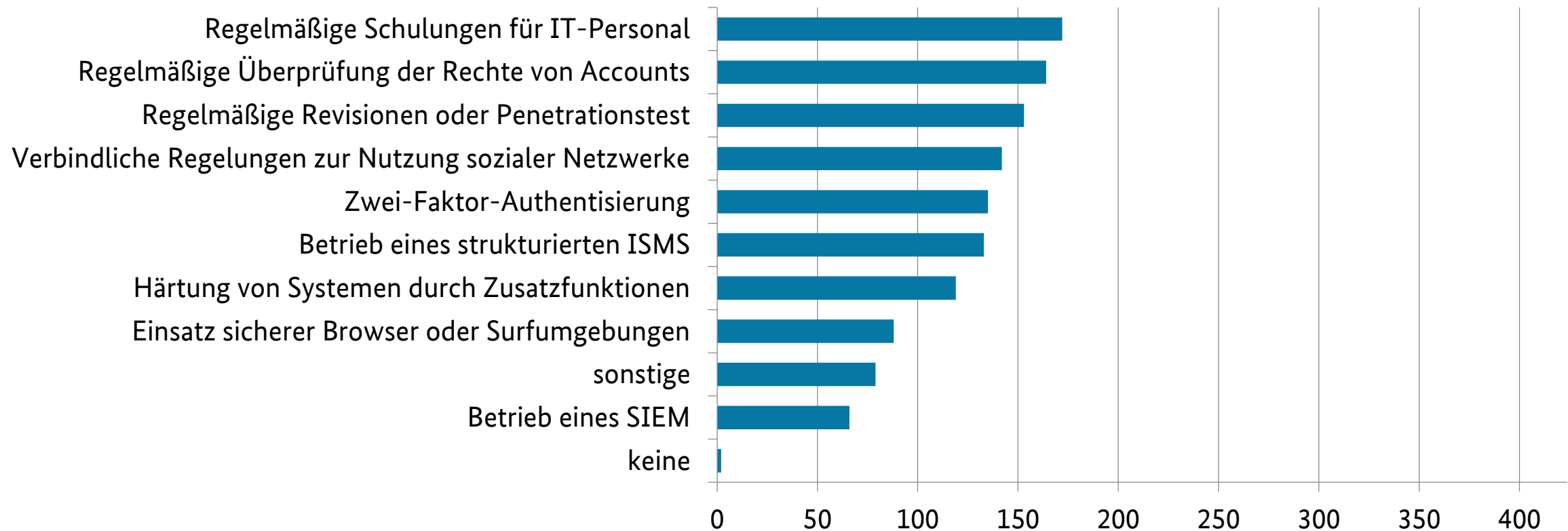
Welche Maßnahmen werden in den Institutionen zum Schutz vor Cyber-Angriffen umgesetzt? (Seite 1 von 2)

Von 424 Befragten gaben jeweils ... folgende Maßnahmen an



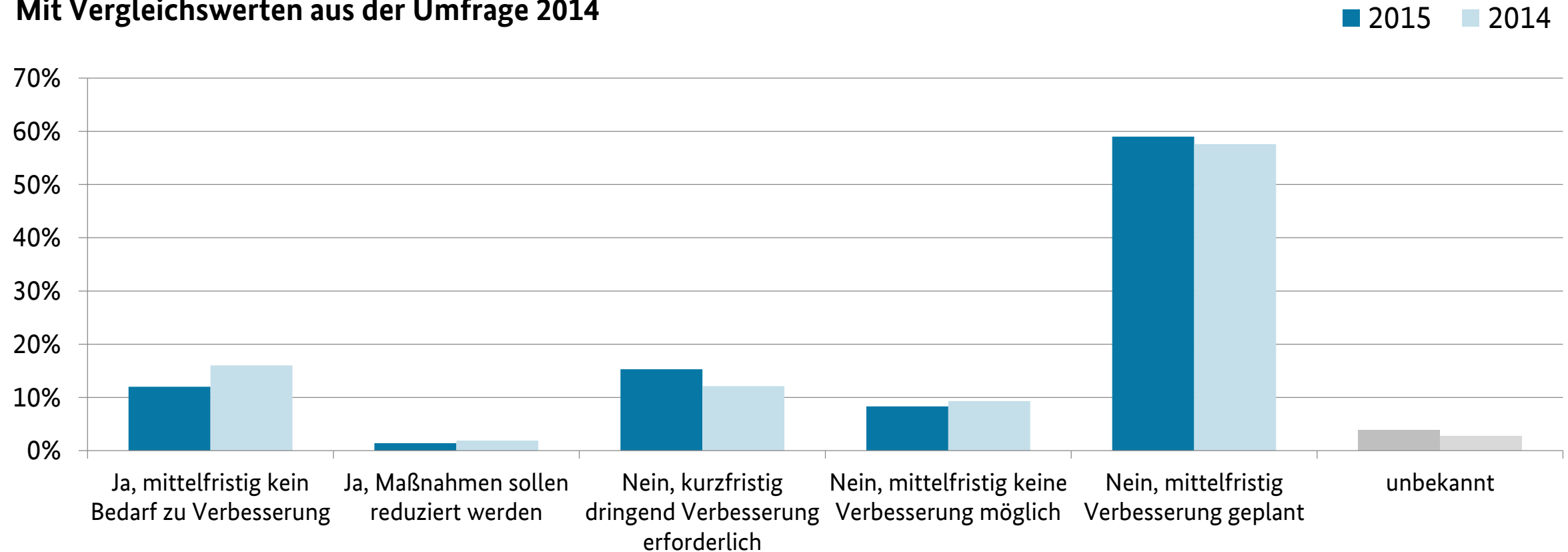
Welche Maßnahmen werden in den Institutionen zum Schutz vor Cyber-Angriffen umgesetzt? (Seite 2 von 2)

Von 424 Befragten gaben jeweils ... folgende Maßnahmen an



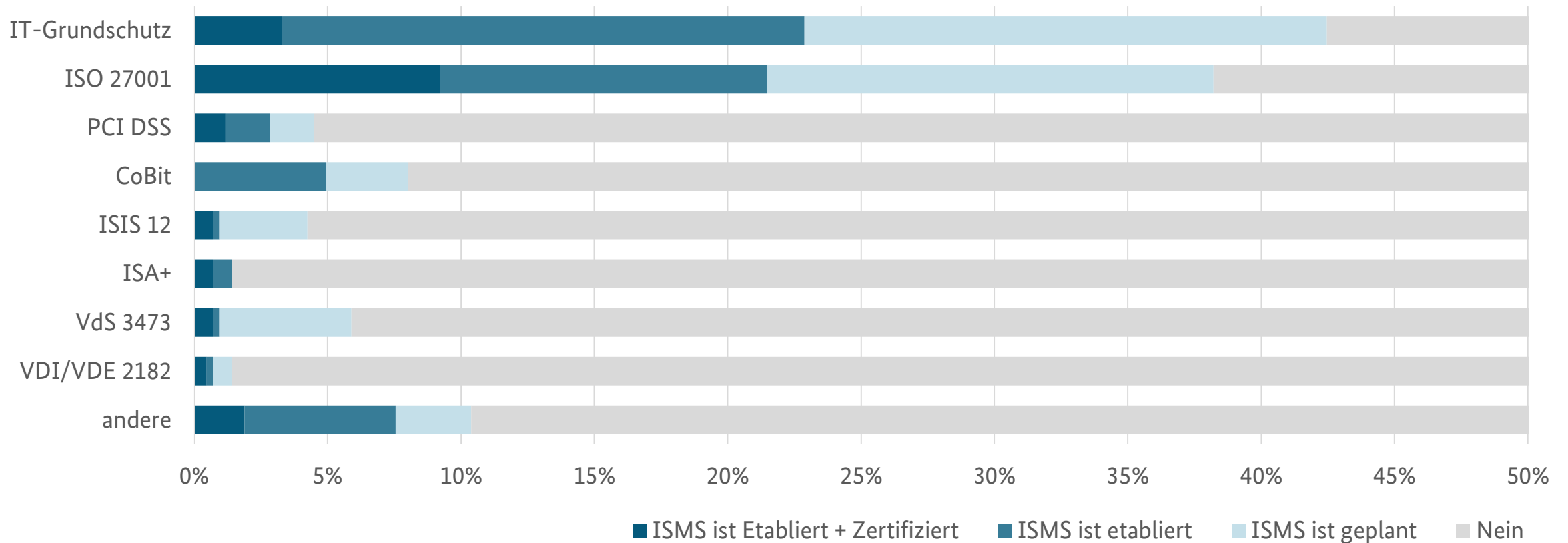
Sind die in der jeweiligen Institution getroffenen Maßnahmen zum Schutz gegen Cyber-Angriffe ausreichend?

Mit Vergleichswerten aus der Umfrage 2014

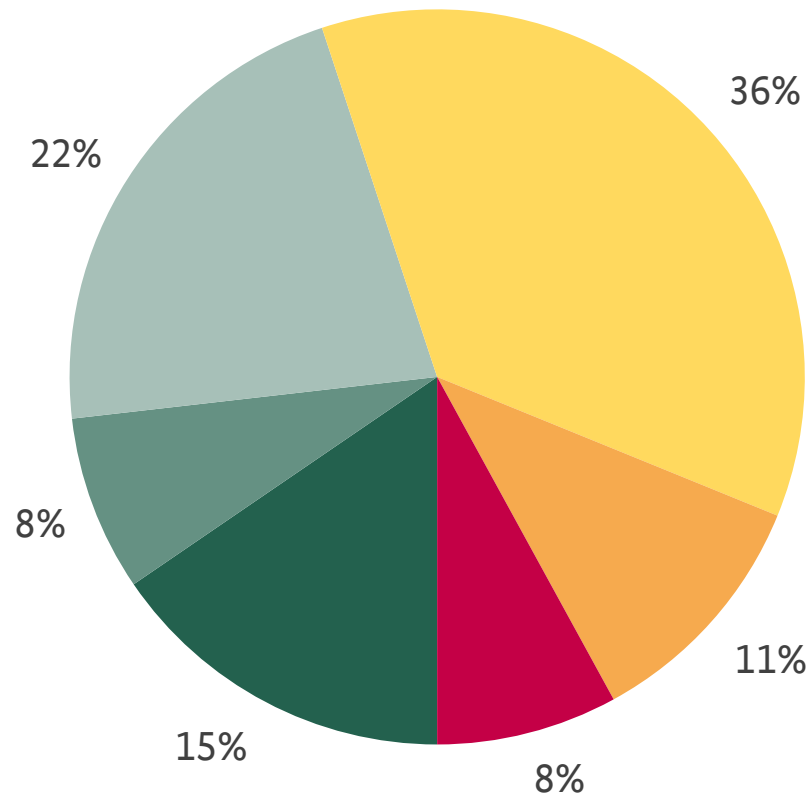


Wird in der jeweiligen Institution ein Managementsystem für Informationssicherheit (ISMS) betrieben?

Von 424 Befragten betreiben/planen ... % ein ISMS auf Basis des Rahmenwerks ...



Wird in der jeweiligen Institution der Status von Maßnahmen zur IT-Sicherheit regelmäßig und strukturiert mit Revisionen und/oder Penetrationstest überprüft?

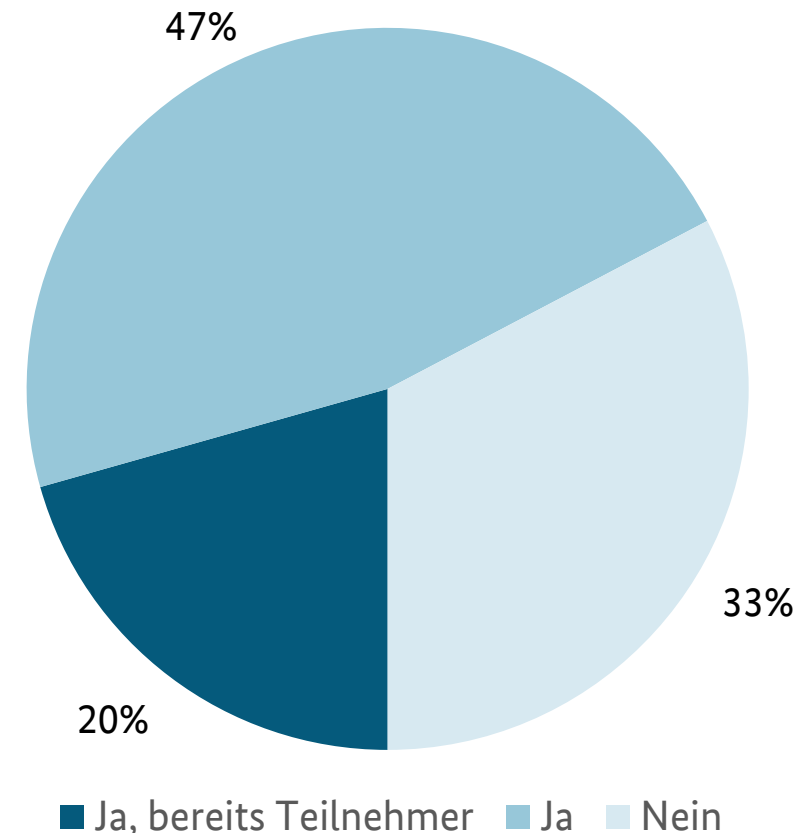


- Ja, regelmäßig durch externe Prüfer
- Ja, regelmäßig durch externe Prüfer im Rahmen einer Zertifizierung
- Ja, regelmäßig durch interne Prüfer
- Nein, nur unregelmäßig und/oder unstrukturiert
- Nein, als Reaktion auf Sicherheitsvorfälle
- Nein, überhaupt nicht

Allianz für Cyber-Sicherheit

War den Befragten die Allianz für Cyber-Sicherheit (ACS) bereits vor der Umfrage bekannt?

- 20,5% sind bereits Teilnehmer der ACS
- 46,5% der Befragten war die ACS bereits ein Begriff, sind aber keine Teilnehmer
- 32,5% kannten die ACS nicht



Wie bewerten die Befragten die Angebote der Allianz für Cyber-Sicherheit in Schulnoten?

Teilnehmer der Allianz für Cyber-Sicherheit gaben unseren Angeboten die die Gesamtnote 2,2

- Allgemeines Informationsangebot und: **2,2**
- BSI-Veröffentlichungen zur Cyber-Sicherheit: **2,1**
- Informationsangebot zur Cyber-Sicherheitslage: **2,2**
- Angebote von Partnern & BSI zu Schulungen / Seminaren: **2,3**
- Cyber-Sicherheits-Tage / Veranstaltungen: **2,2**



Vielen Dank für Ihr Interesse



Kontakt

Geschäftsstelle der Allianz für Cyber-Sicherheit
c/o Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185 – 189
53175 Bonn

info@cyber-allianz.de

Tel. +49 (0) 228 99 9582 5977
Fax +49 (0) 228 99 109582 6050
www.allianz-fuer-cybersicherheit.de