Technischer Bericht

Stand zur IT-Sicherheit deutscher Stromnetzbetreiber, November 2018

Bei der Erstellung dieses Berichts haben mitgewirkt:

Sebastian Pape, Goethe Universität Frankfurt
Volkmar Pipek, Universität Siegen
Kai Rannenberg, Goethe Universität Frankfurt
Christopher Schmitz, Goethe Universität Frankfurt
André Sekulla, Universität Siegen
Frank Terhaag, regio iT gesellschaft für informationstechnologie mbh

Erscheinungsjahr 2018, Universität Siegen, Siegen

Sichere Informationsnetze bei kleinen und mittleren Energieversorgern (SIDATE)

Im Fokus des Forschungsprojekts SIDATE steht die technische Unterstützung kleiner und mittelgroßer Energieversorger bei der Selbsteinschätzung und Verbesserung ihrer IT-Sicherheit. Es werden verschiedene Konzepte und Werkzeuge in Zusammenarbeit von Universität Siegen, Goethe-Universität Frankfurt am Main, TÜV Rheinland i-sec GmbH, regio iT Gesellschaft für Informationstechnologie mbh, und der Arbeitsgemeinschaft für sparsame Energie- und Wasserverwendung (ASEW) entwickelt und evaluiert.
Weitere Informationen finden sich auf der Webseite http://sidate.org/ .

Förderhinweis

Diese Forschungsarbeit wurde durch das Bundesministerium für Bildung und Forschung (BMBF) im Rahmen des Förderschwerpunktes „IT-Sicherheit für Kritische Infrastrukturen“ gefördert.

Bildnachweis

Titelbild ©TebNad / Fotolia

Inhaltsverzeichnis

Einleitung

Innerhalb des Forschungsprojektes „Sichere Informationsnetze bei kleinen und mittleren Energieversorgern“ (SIDATE) wurde eine Umfrage zum Stand der IT-Sicherheit bei deutschen Stromnetzbetreibern durchgeführt. Das Projekt selbst beschäftigt sich mit der Informations-Sicherheit bei kleinen und mittleren Energieversorgern.
Zur Durchführung der Umfrage wurden alle 890 im September 2018 bei der Bundesnetzagentur gelisteten Betreiber angeschrieben. Der Fragebogen ist eine Fortführung der im Herbst 2016 durchgeführten Umfrage zum Stand der IT-Sicherheit bei deutschen Stromnetzbetreibern[1]. In dem Umfragezeitraum vom 10. September 2018 bis zum 30. Oktober 2018 antworten 84 (9,4%) der Betreiber. Der Fragebogen fokussiert die Umsetzung der rechtlichen Anforderungen und die Implementierung eines Informationssicherheitsmanagementsystems (ISMS). Weiterhin wurden Fragen zu dem Leitsystem, Netzaufbau, Prozessen, organisatorischen Strukturen und der Büro-IT gestellt. Nachfolgend werden alle auswertbaren Ergebnisse der Umfrage präsentiert. Einige Fragen wurden nur ungenügend beantwortet, sodass auf eine Präsentation dieser Ergebnisse verzichtet worden ist.

Die Umfrage gliedert sich in folgende Teilbereiche:

A) Allgemeine Informationen zum Unternehmen
B) Organisatorisches
C) Information Security Management System (ISMS)
D) Büro IT
E) Leitsystem: Netzaufbau
F) Leitsystem: Prozess und Organisation

Es gibt zwei unterschiedliche Arten von Balkendiagrammen. Die erste besitzt farblich nur blaue Balken. Diese beziehen sich auf alle Stromnetzbetreiber, welche die entsprechende Frage beantwortet haben. Hingegen gibt es bei der zweiten Art der Balkendiagramme eine kategorische Unterscheidung zwischen den Stromnetzbetreibern. Diese liegt in der Größe, welche anhand der Anzahl der jeweils zugehörigen Zählpunkte festgemacht worden ist.

In einigen Ausnahmen wurde eine Art des Spinnennetzdiagramms verwendet. Auch in diesen Fällen wurde auf eine Kategorisierung der antwortgebenden Unternehmen verzichtet.

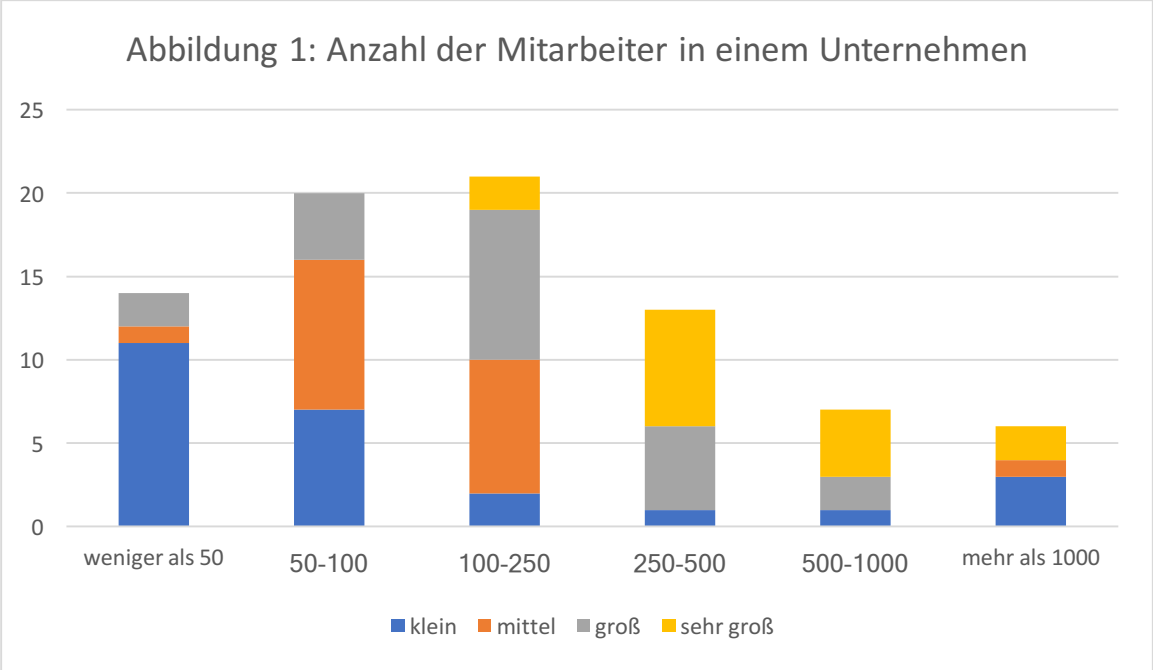
[1] Dax, Julian; Ley, Benedikt; Pape, Sebastian; Pipek, Volker; Rannenberg, Kai; Schmitz, Christopher; Sekulla, André. 2017. „Stand zur IT-Sicherheit deutscher Stromnetzbetreiber: technischer Report“, Technical Report, http://dokumentix.ub.uni-siegen.de/opus/volltexte/2017/1185, Universität Siegen.

Teil A: Allgemeine Informationen zum Unternehmen

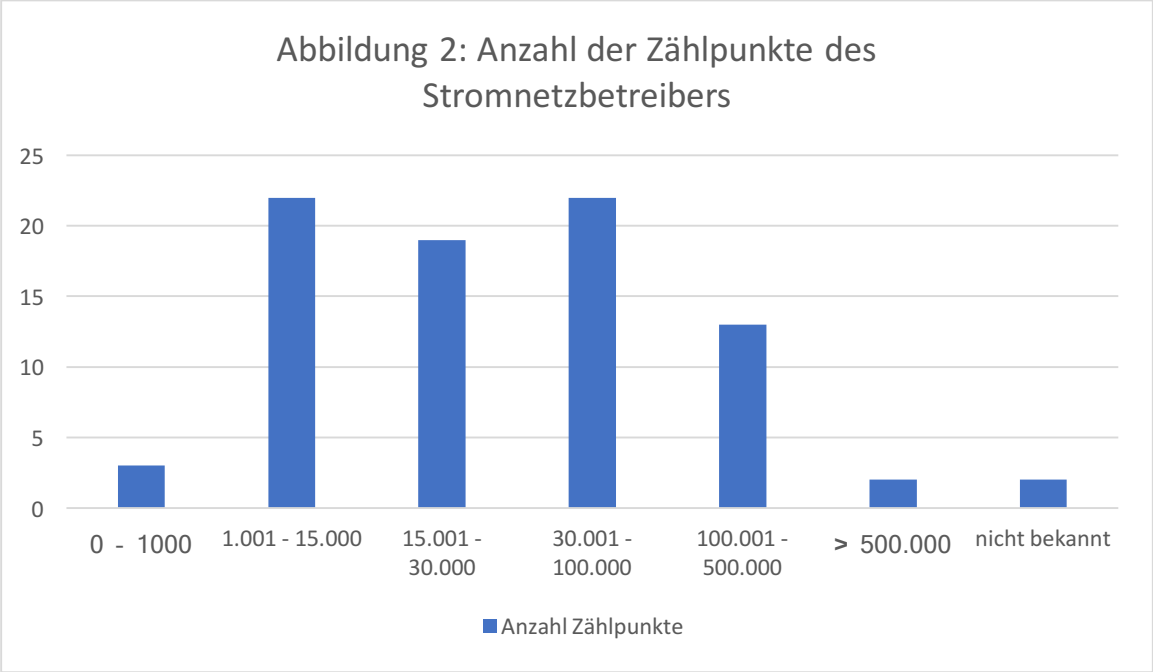
Um einen ersten Überblick zu den teilnehmenden Stromnetzbetreibern zu erhalten, wurden im ersten Abschnitt der Umfrage allgemeine Fragen gestellt. Anhand der erhaltenen Ergebnisse konnten die Stromnetzbetreiber in vier Größenkategorien unterteilt werden, um die darauffolgenden Fragen besser auszuwerten.

Die Kategorisierung der Teilnehmer ist anhand der Anzahl der Zählpunkte des Stromnetzbetreibers getätigt worden. In Abbildung 1 ist die Aufteilung der Größe gut erkennbar. Für die weiteren Ergebnisse sind die Teilnehmer in die Kategorien „klein“ (0 bis 15.000 Zählpunkte), „mittel“ (15.001 bis 30.000 Zählpunkte), „groß“ (30.001 bis 100.000 Zähpunkte) und „sehr groß“ (ab 100.001 Zählpunkte) eingeteilt.

A1 Wie viele Mitarbeiter/innen sind in Ihrem Unternehmen beschäftigt?



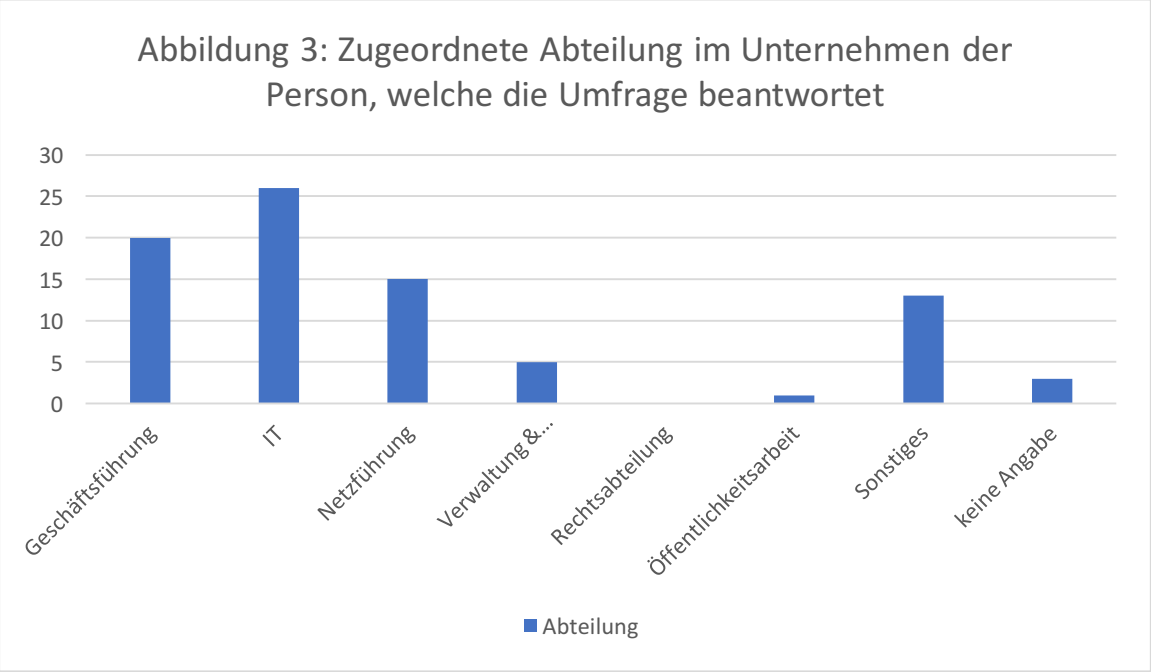
A2 Wie viele Zählpunkte werden über Ihr Stromnetz Versorgt?



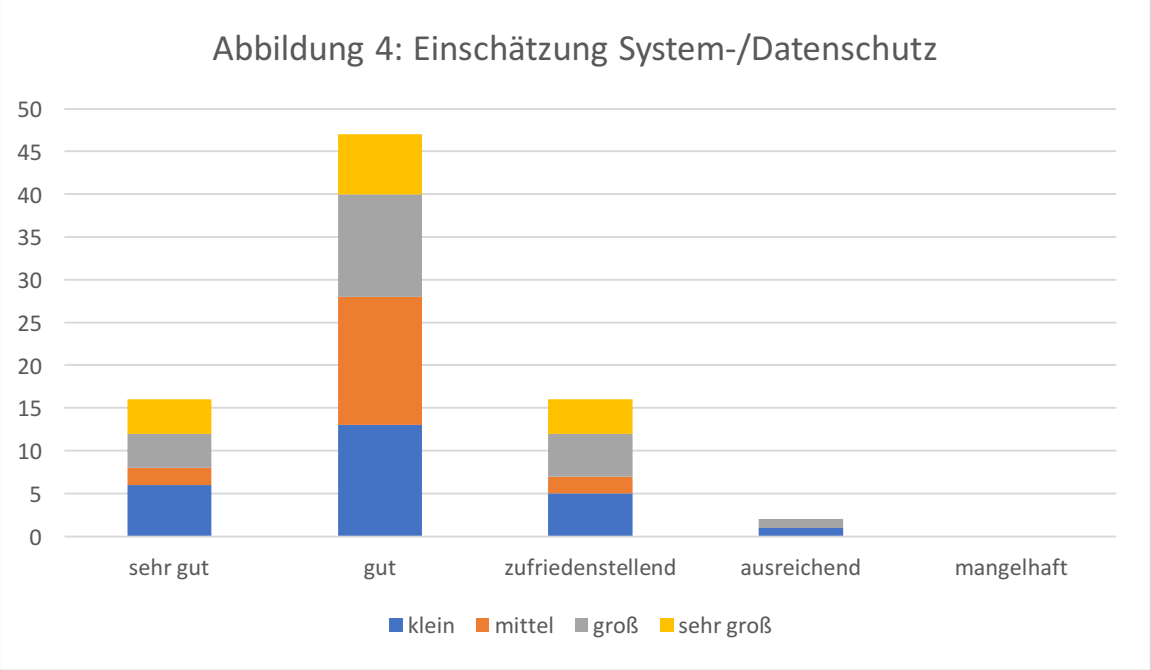
Teil B: Organisatorisches

In diesem Abschnitt der Umfrage wurden organisatorische Gegebenheiten abgeklärt. Darunter befanden sich Fragen um näheres zu der befragten Person zu erfahren. Zum Beispiel in welcher Abteilung er zugeordnet ist und welche Rolle er im Unternehmen innehat. Weiterhin wurden konkrete Fragen bezogen auf die IT-Sicherheit gestellt.

B1 Welcher Abteilung sind Sie im Unternehmen zugordnet?



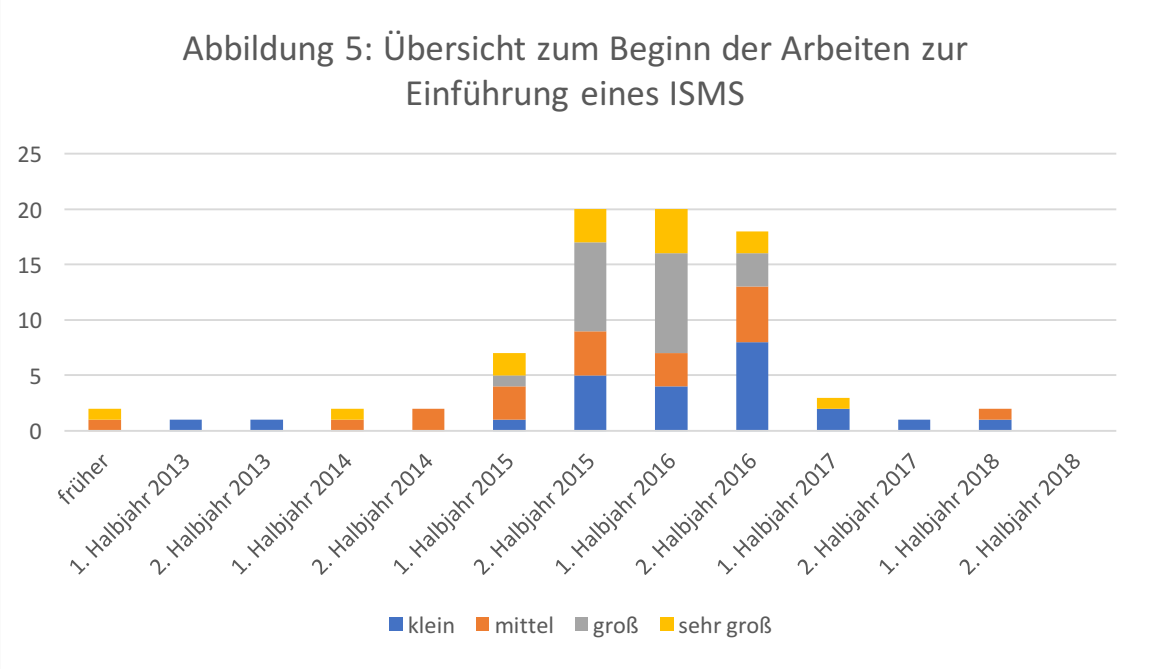
B4 Wie gut sind Ihrer Einschätzung nach die Systeme und Daten Ihres Unternehmens geschützt?



Teil C: Information Security Management System (ISMS)

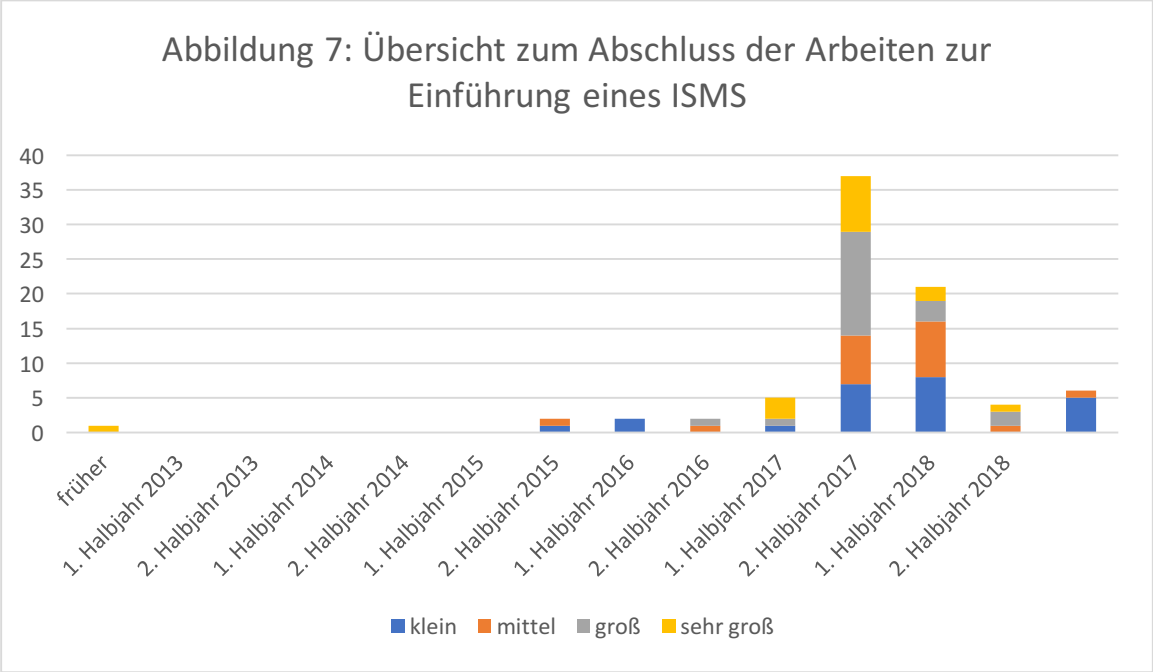
Um einen besseren Überblick zum Status der Einführung des Information Security Management Systems zu erhalten, wurden explizit Fragen dazu gestellt.

C1 Wann wurde mit den Arbeiten zur Einführung eines ISMS begonnen?

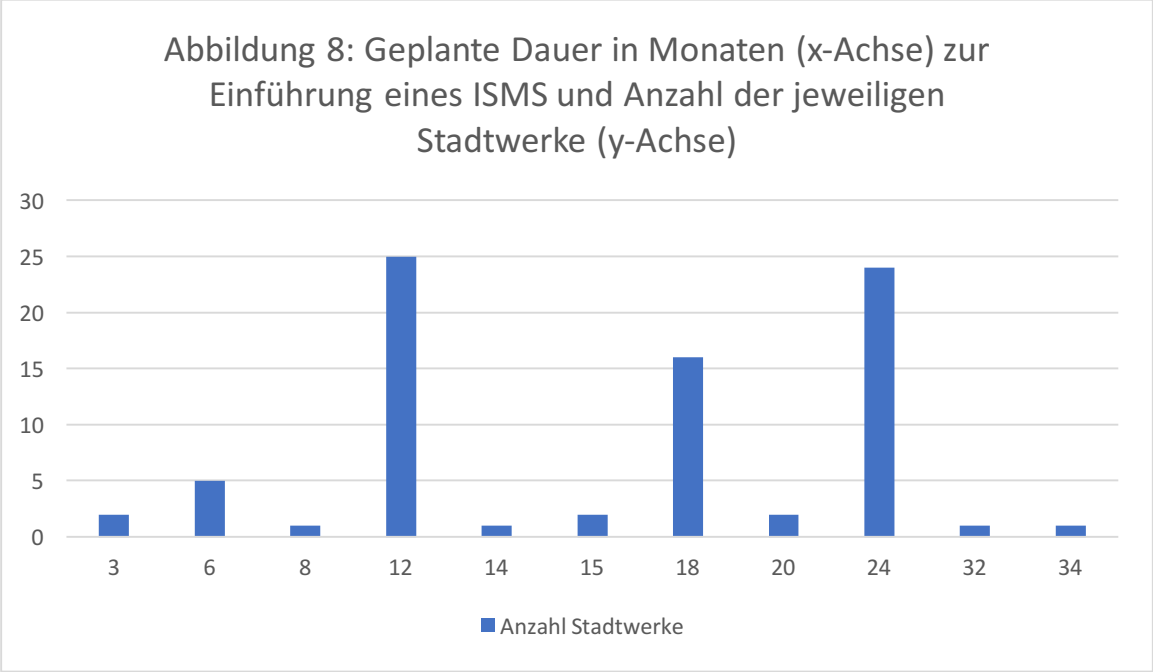


C2 Wie ist der aktuelle Stand der jeweiligen ISMS Umsetzungsphasen?

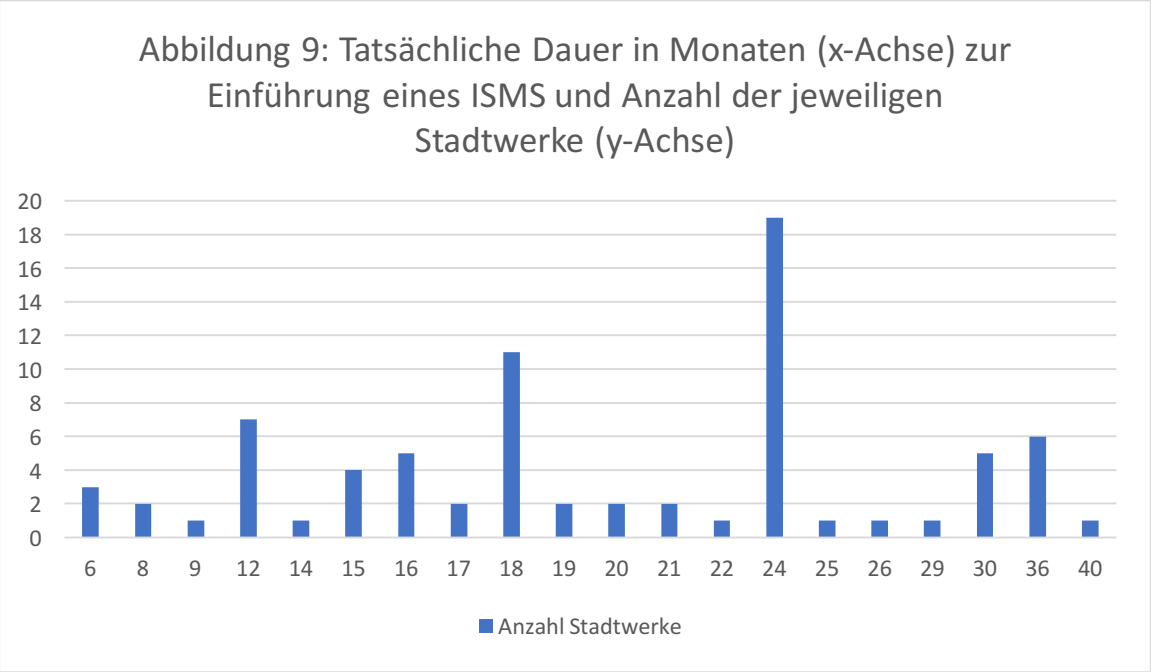
C3 Wann wurden die Arbeiten zur Einführung eines ISMS abgeschlossen?



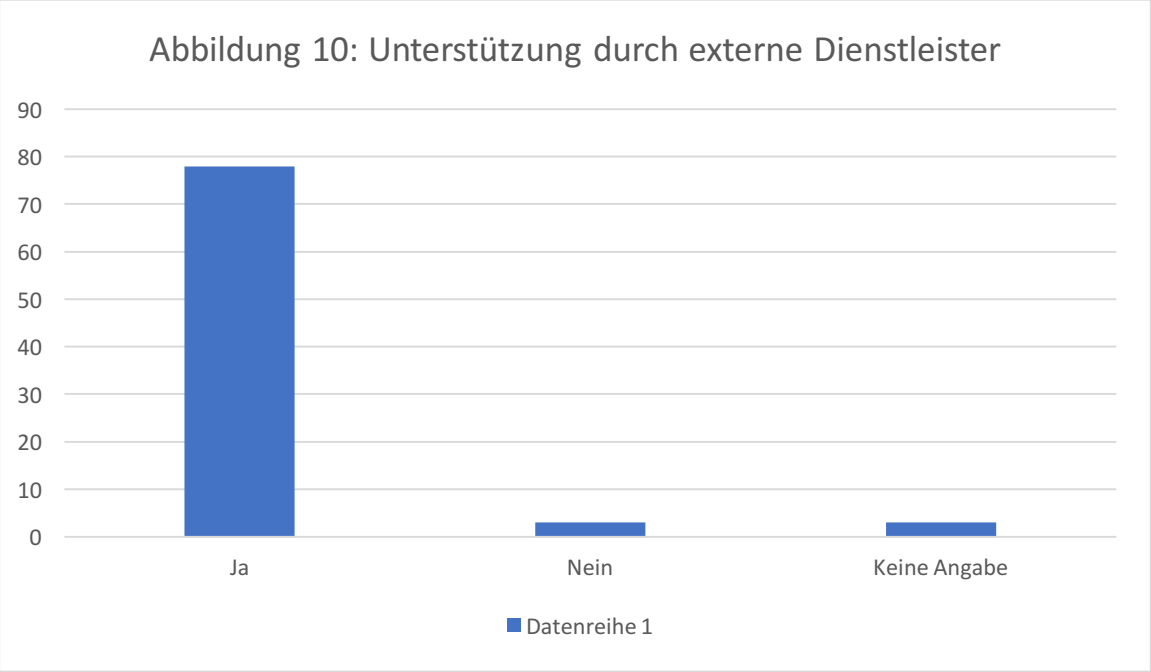
C4 Mit welcher Dauer für die Einführung eines ISMS haben Sie zu Beginn der Umsetzungsarbeiten gerechnet (in Monaten)?



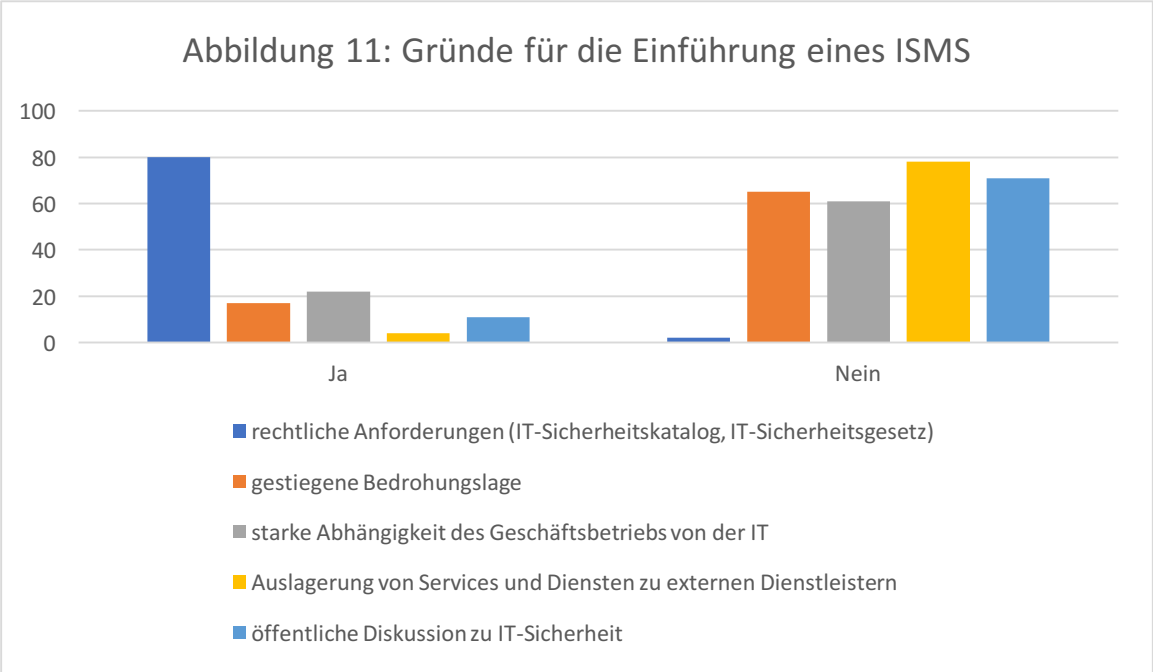
C5 Wie lange hat die Einführung Ihres ISMS tatsächlich gedauert (in Monaten)?



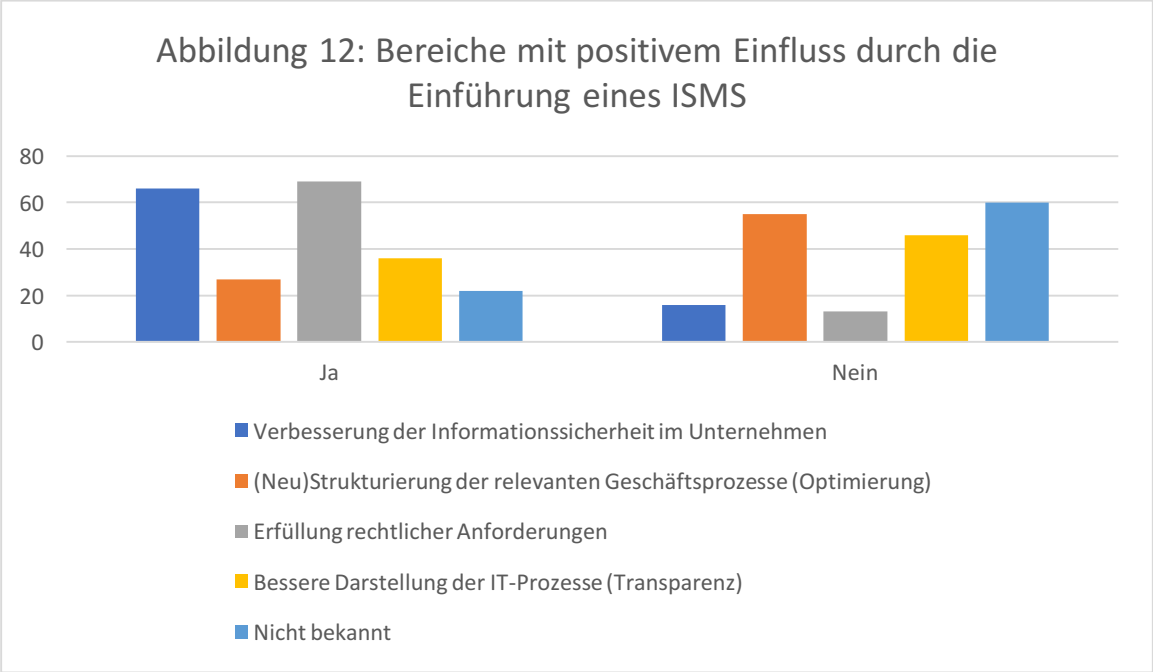
C6 Wurden bei der Einführung des ISMS externe Dienstleister (z.B. Unternehmensberater) hinzugezogen?



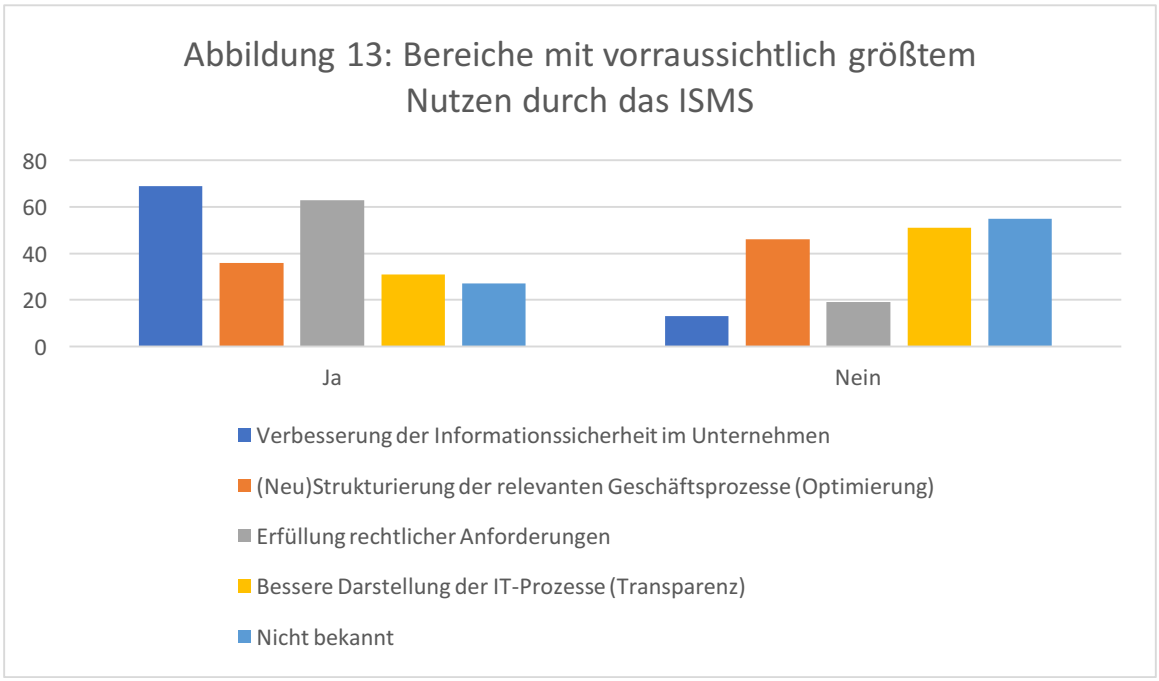
C7 Was waren für Sie die wesentlichen Gründe für die Einführung eines ISMS (Mehrfachauswahl möglich)?



C8 In welchen Bereichen konnten Sie seit der Einführung des ISMS bereits vom ISMS profitieren?



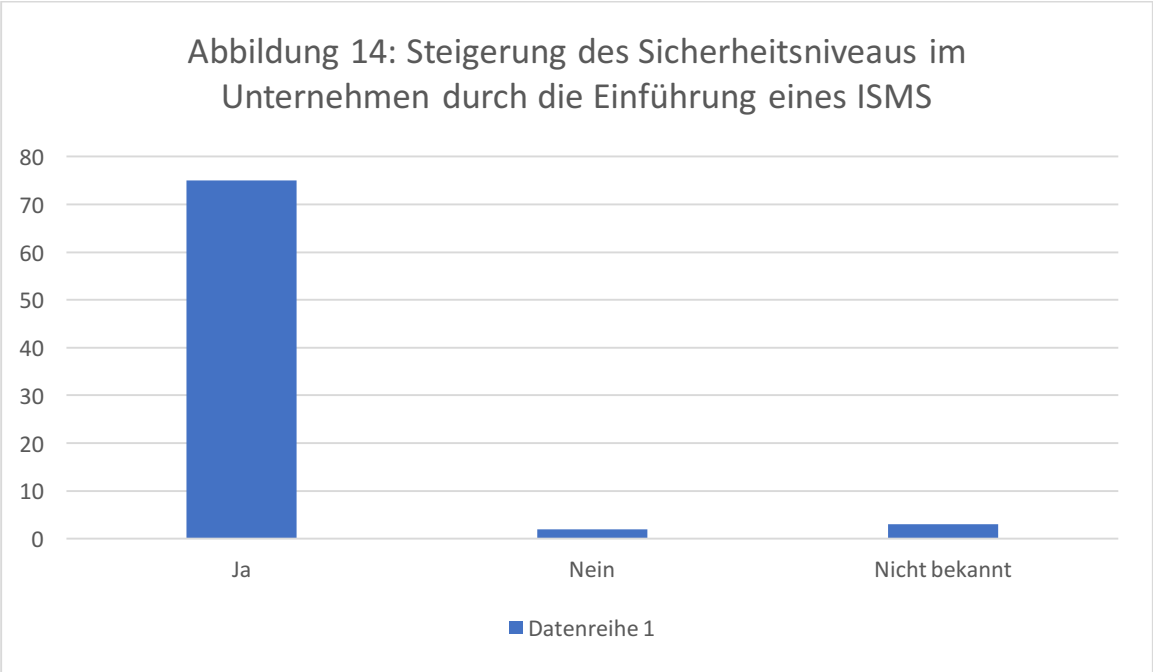
C9 In welchen Bereichen sehen Sie zukünftig den größten Nutzen des ISMS für Ihr Unternehmen?



Teil D: ISMS-Betrieb

Um einen besseren Überblick zum Betrieb eines Information Security Management Systems zu erhalten, wurden explizit Fragen dazu gestellt. Welche Bereiche konnten bereits durch das ISMS profitieren. Weiterhin konnten wir einen Einblick in die Kosten zur Einführung und dem Betrieb eines ISMS erlangen. Zusätzlich wurde die Zusammenarbeit zwischen den Netzbetreibern erfragt und die Unterstützung durch externe Dienstleistern in Bezug auf den Betrieb eines ISMS.

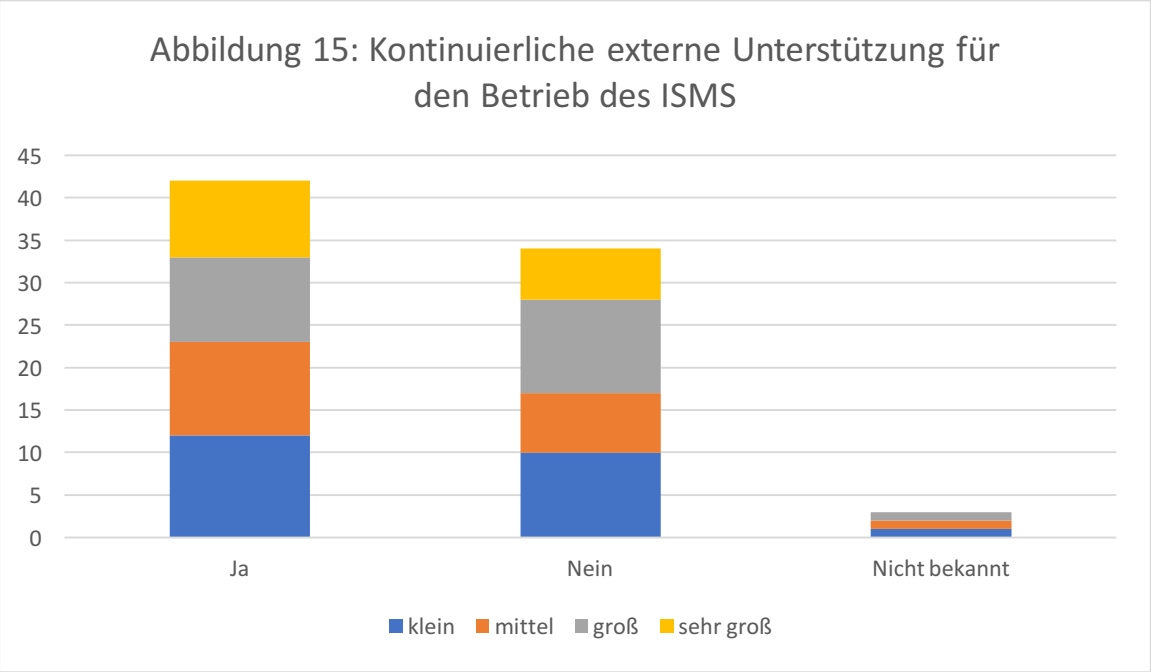
D1 Konnte nach Ihrer Meinung das Sicherheitsniveau Ihres Unternehmens durch die Einführung des ISMS verbessert werden?



D2 Wie hoch waren in Ihrem Unternehmen die initialen Kosten für die Einführung des ISMS?

	Klein		Mittel		Groß		Sehr groß	
	Intern	**Extern**	**Intern**	**Extern**	**Intern**	**Extern**	**Intern**	**Extern**
Minimum	3000	4000	10080	20000	30000	25000	30000	25000
Durchschnitt	56823	54058	180275	115891	110000	102058	323818	131333
Maximum	300000	200000	2000000	1000000	250000	220000	2000000	350000

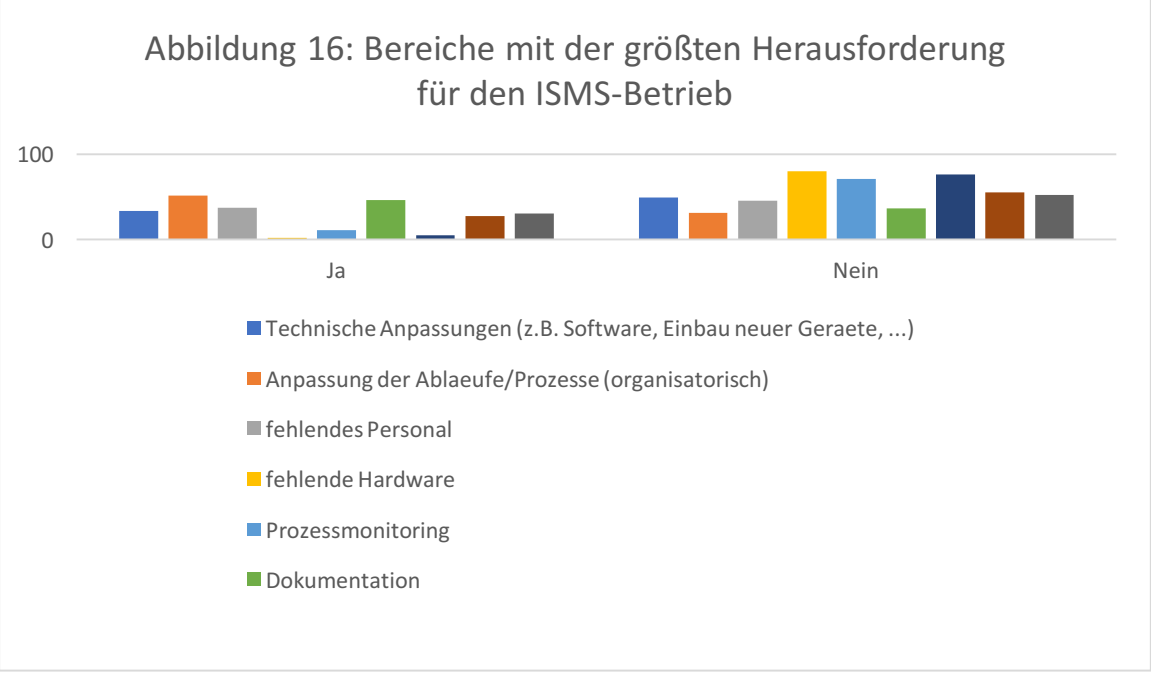
D3 Haben Sie für den Betrieb des ISMS kontinuierliche externe Unterstützung?



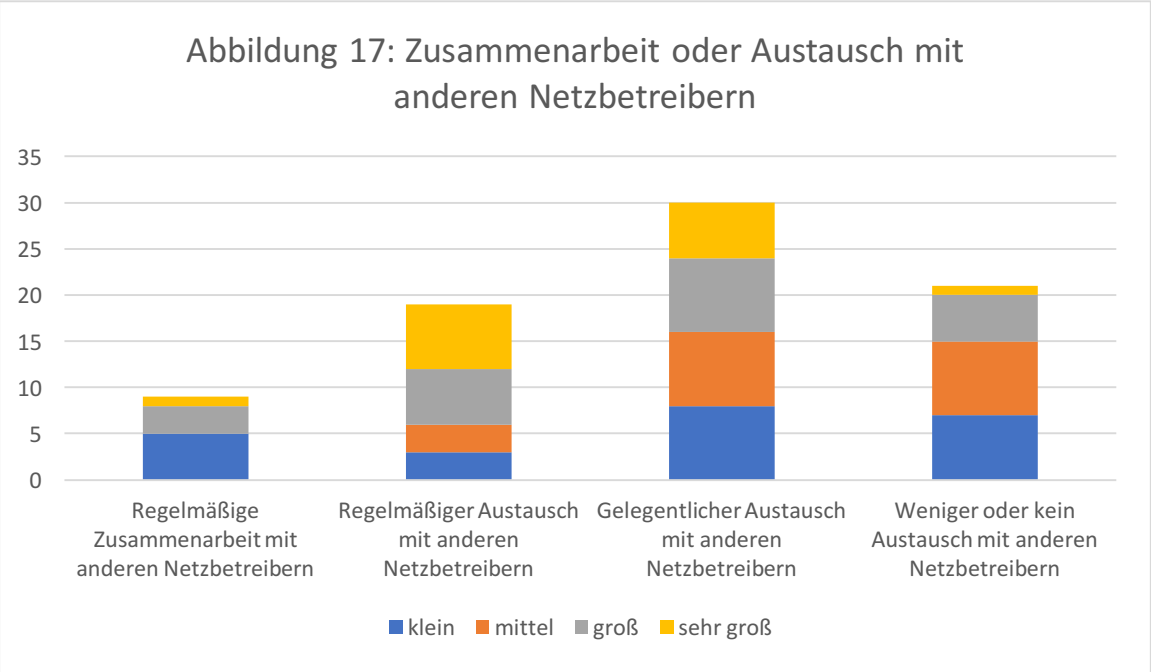
D4 Mit welchen jährlichen Kosten rechnen Sie für den Betrieb Ihres ISMS?

	Klein		Mittel		Groß		Sehr groß	
	Intern	**Extern**	**Intern**	**Extern**	**Intern**	**Extern**	**Intern**	**Extern**
Minimum	1000	1000	4320	5000	10000	5000	10000	5000
Durchschnitt	18529	10000	72621	28125	33000	21866	101538	42285
Maximum	50000	50000	800000	200000	100000	50000	500000	200000

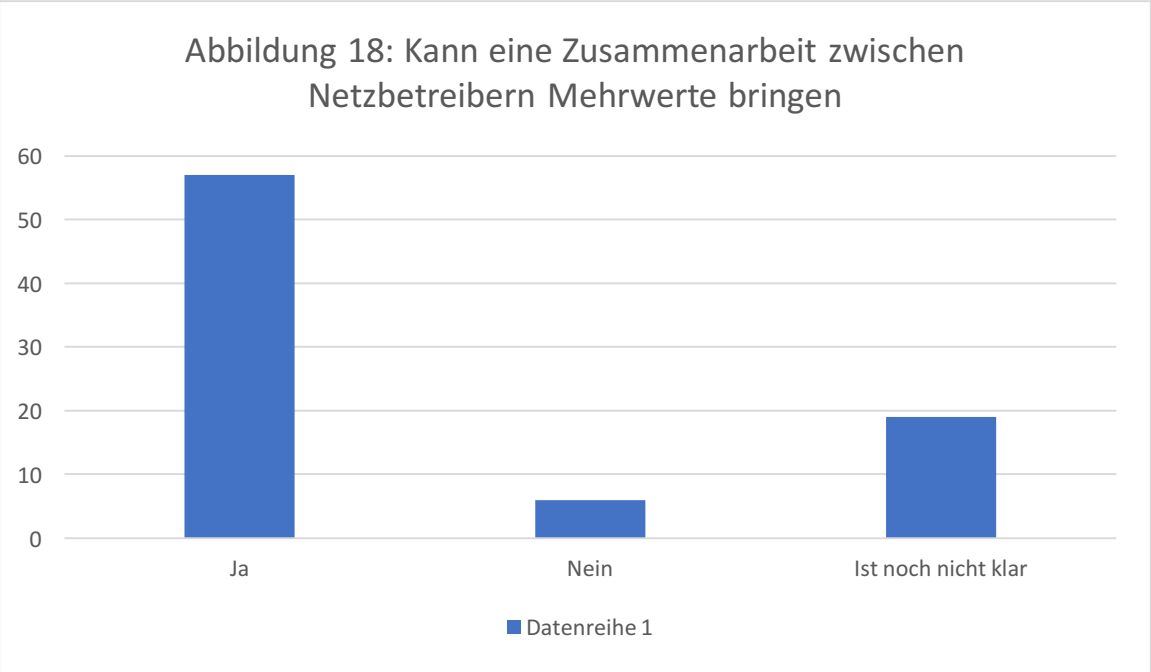
D5 In welchen Bereichen des ISMS-Betriebs liegen für Ihr Unternehmen die größten Herausforderungen?



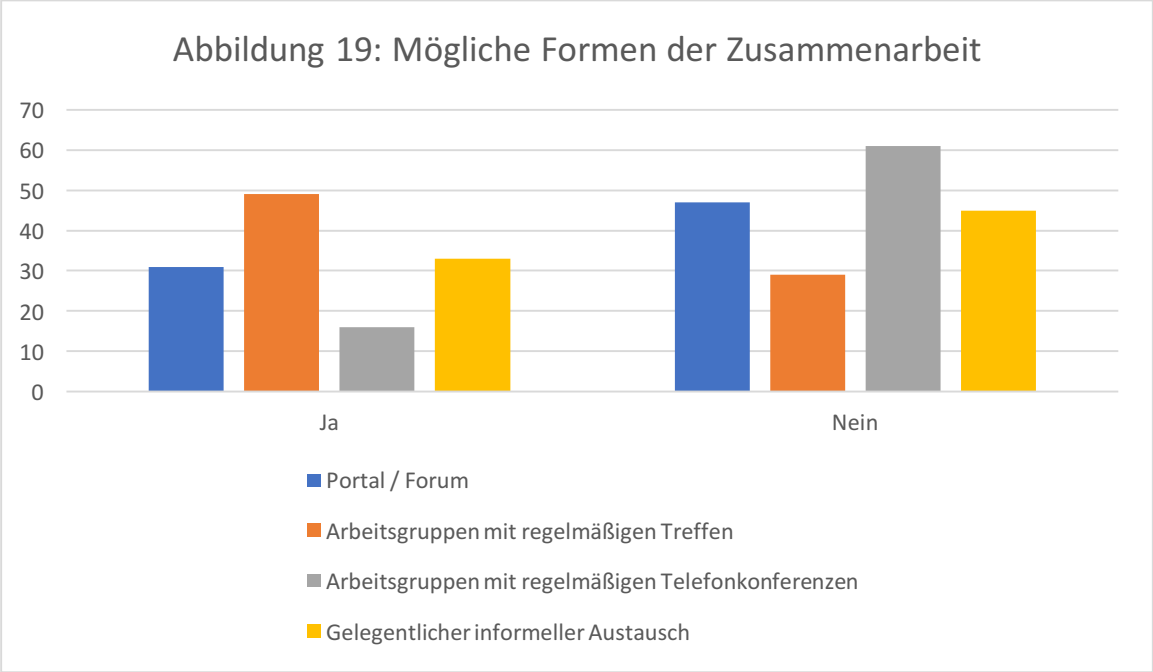
D6 Arbeiten Sie im Bereich des ISMS-Betriebs mit anderen Netzbetreibern zusammen oder tauschen Sie sich mit anderen Netzbetreibern aus?



D7 Könnte nach Ihrer Meinung die Zusammenarbeit mit anderen Netzbetreibern einen positiven Beitrag zum Betrieb Ihres ISMS bzw. für Ihr Sicherheitsniveau leisten?



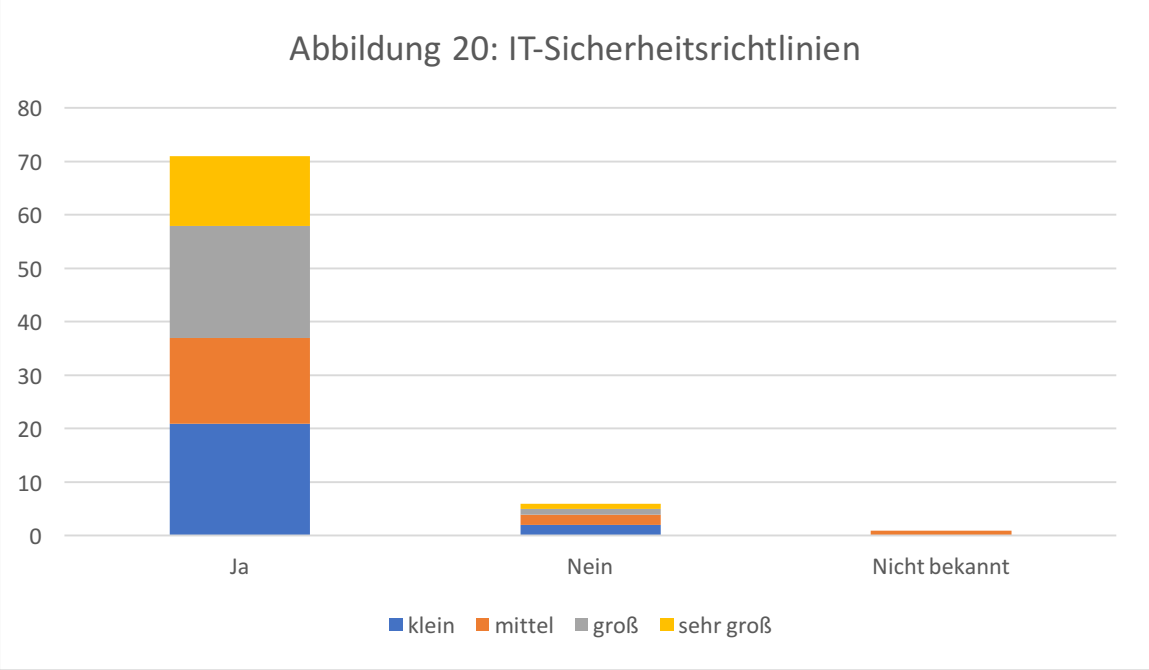
D8 Welche Formen der Zusammenarbeit könnten sie sich vorstellen?



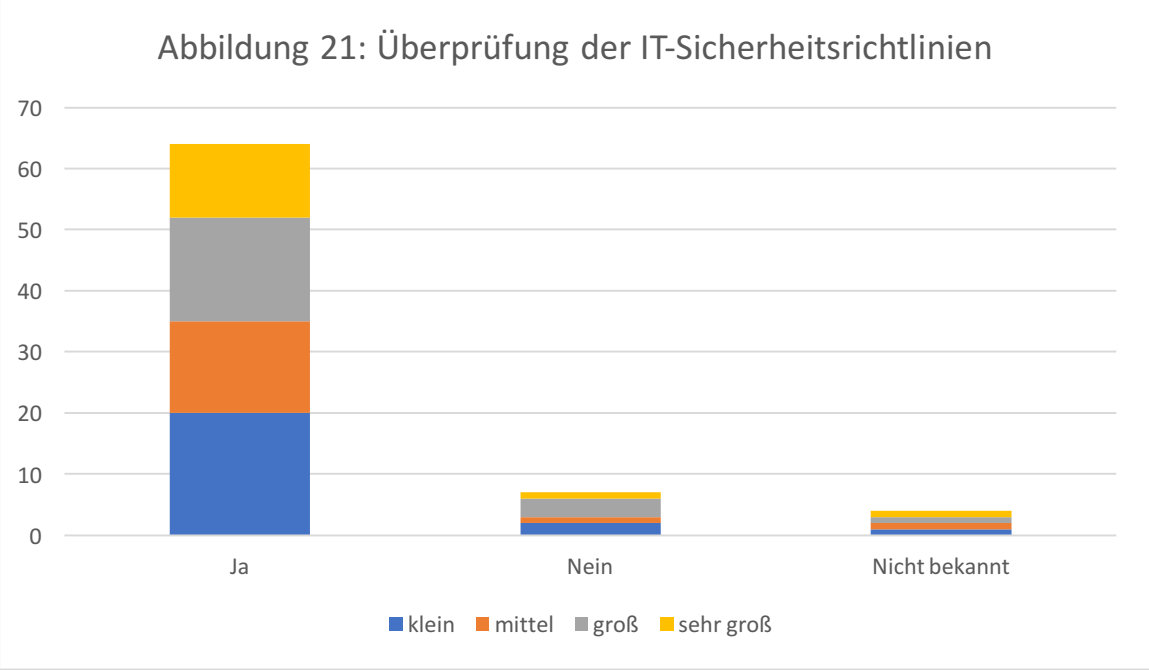
Teil E: Büro IT

In diesem Abschnitt der Umfrage wird die Büro IT im Hinblick auf die IT-Sicherheit beleuchtet. Um eine höhere Sicherheit gewährleisten zu können muss es entsprechende IT-Sicherheitsrichtlinien geben und diese müssen regelmäßig überprüft werden. Die Überprüfung ist aufgrund der ständigen Weiterentwicklung der Technik wichtig.

E1 Existieren IT-Sicherheitsrichtlinien für die Büro IT Ihres Unternehmens?



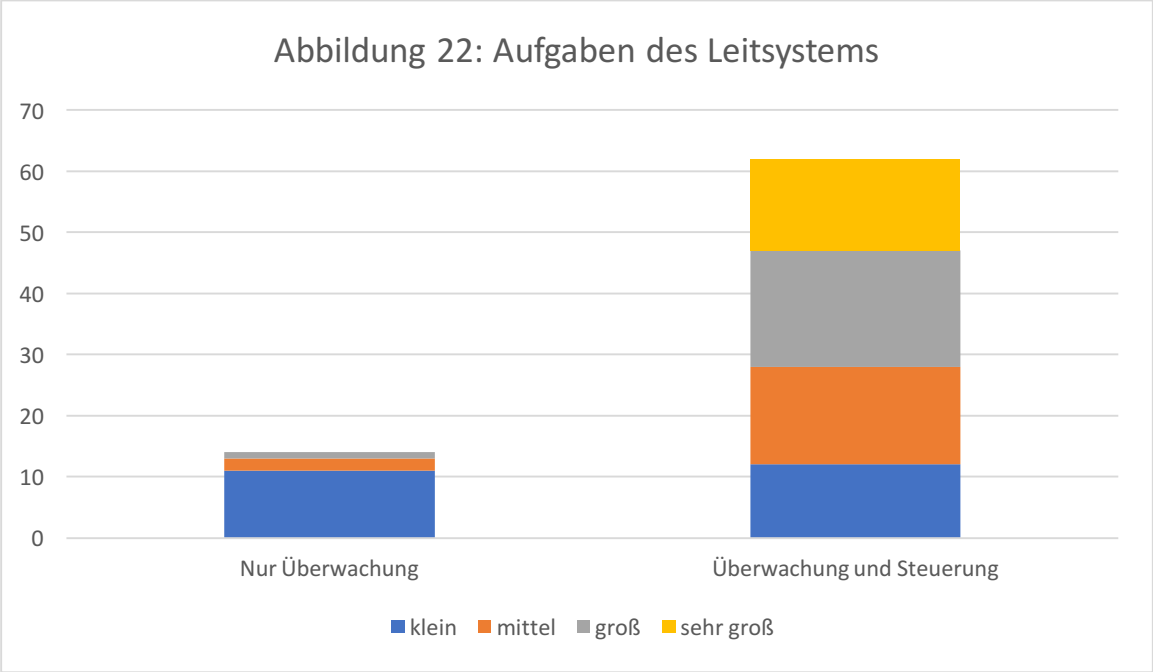
E2 Werden die IT-Sicherheitsrichtlinien in regelmäßigen Zeitabständen überprüft und ggf. angepasst?



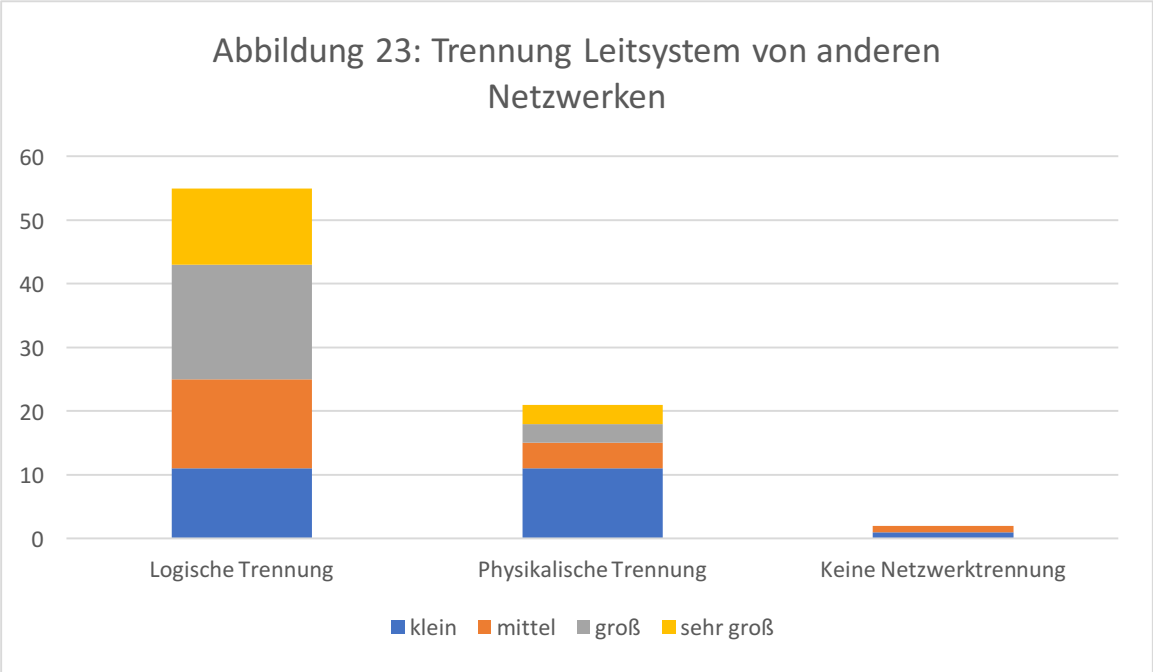
Teil F: Leitsystem: Netzaufbau

Das Leitsystem stellt den Kern des Stromnetzbetreibers dar. Um mehr Informationen über den generellen Aufbau des Leitsystems zu erhalten, sind spezifische Fragen zu dem Netzaufbau gestellt worden.
Zwei Hauptaufgaben des Leitsystems sind die Netzüberwachung und –steuerung bzw. die Durchführung von Schaltvorgängen.
Ein weiterer wichtiger Aspekt des Netzaufbaus ist die Trennung zwischen dem Leitsystem und den anderen Netzwerken (z. B. Büro IT; Internet; Wartungsfirmen). Liegen keine Trennungen vor, könnte dies eine Gefahrenstelle bzw. ein möglicher Angriffspunkt sein, welcher geschützt werden muss.

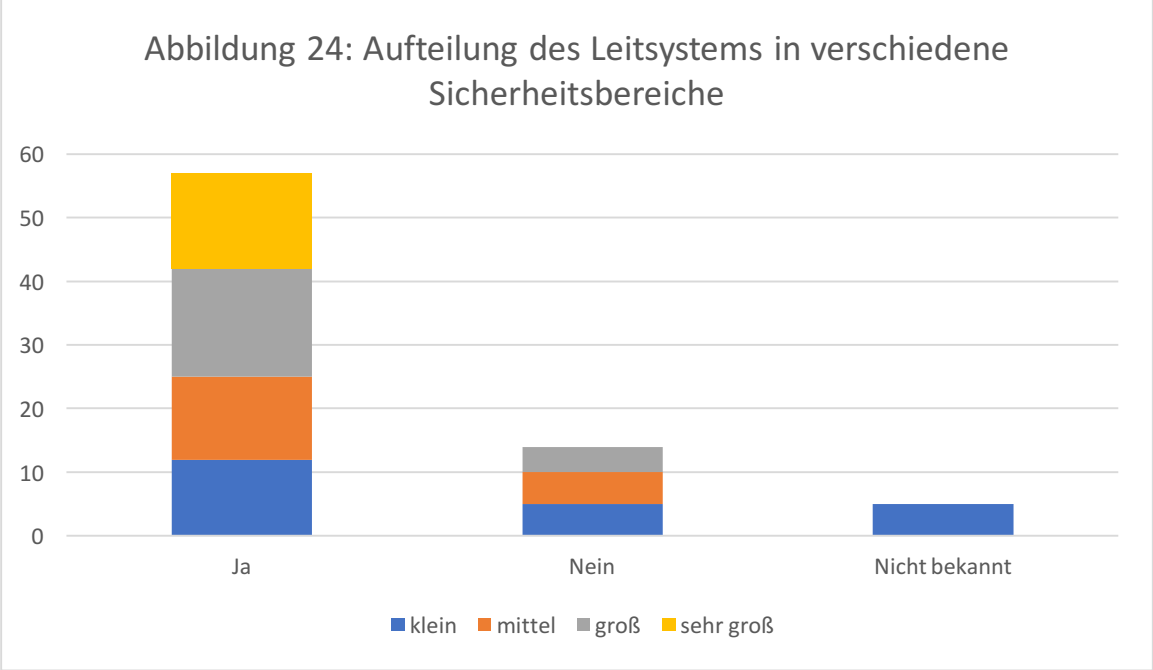
F1 Dient Ihr Leitsystem nur der Netzüberwachung oder können hierüber auch Schaltvorgänge durchgeführt werden?



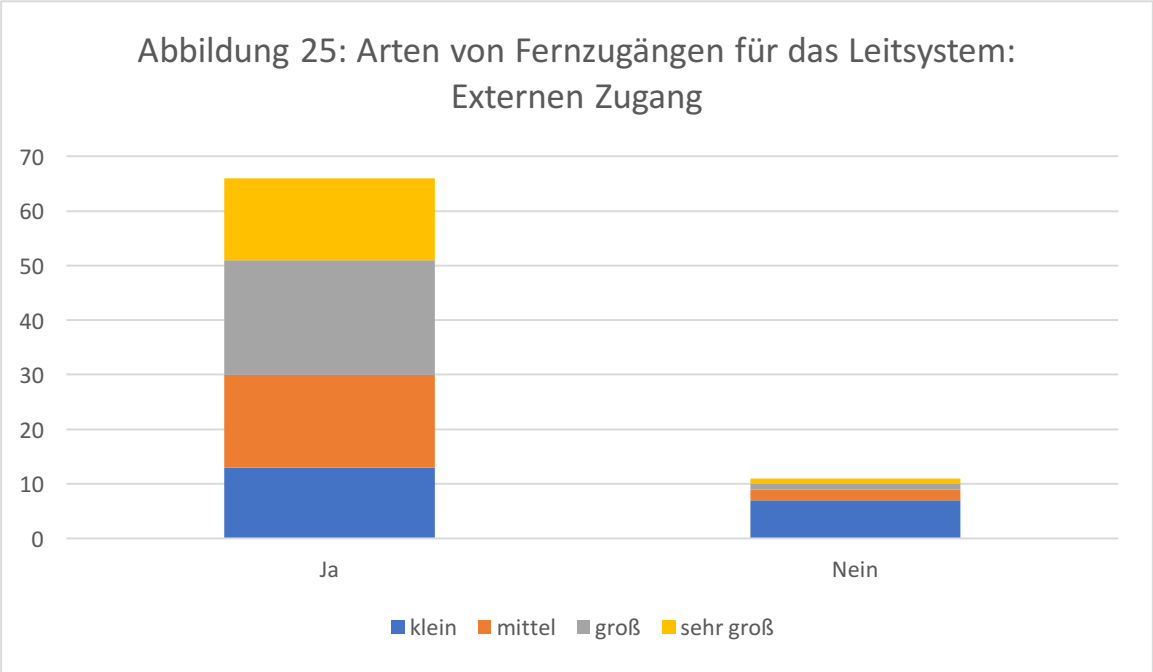
F2 Wie ist das IT-Netzwerk Ihres Leitsystems von anderen Netzwerken (z.B. Büro IT, Internet, Wartungsfirmen) getrennt?



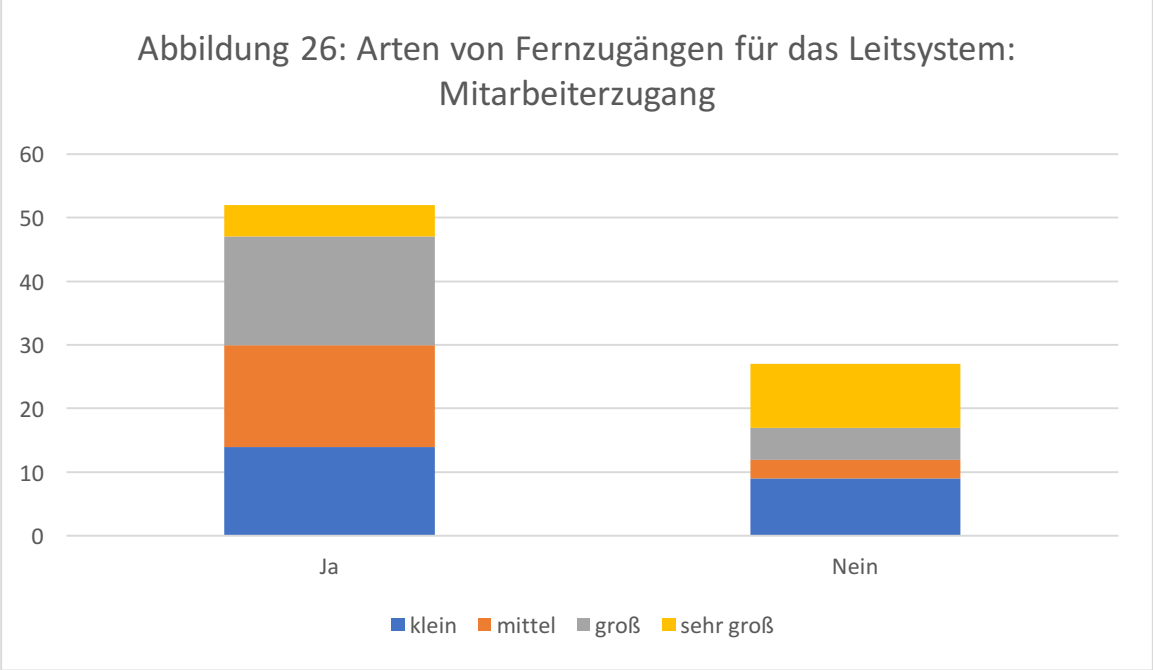
F3 Ist das Netzwerk Ihres Leitsystems in verschiedene Sicherheitsbereiche unterteilt (z.B. durch verschiedene VLANs)?



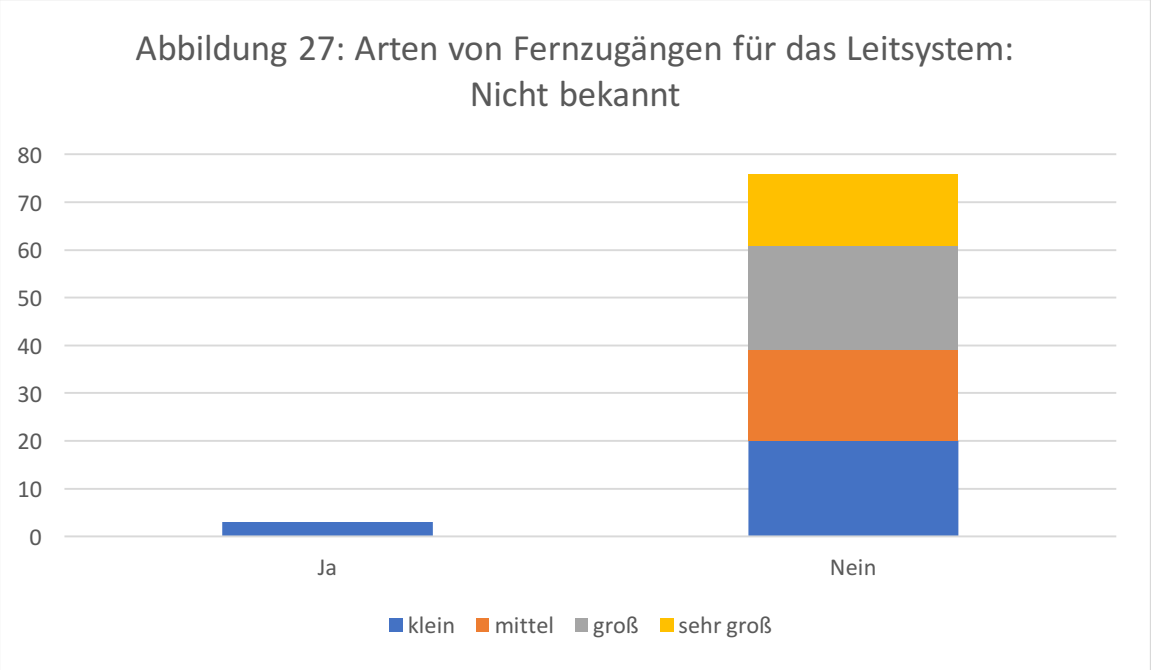
F4 Welche Arten von Fernzugängen sind für Ihr Leitsystem eingerichtet: Externer Zugang für die Wartung und Konfiguration des Leitsystems?



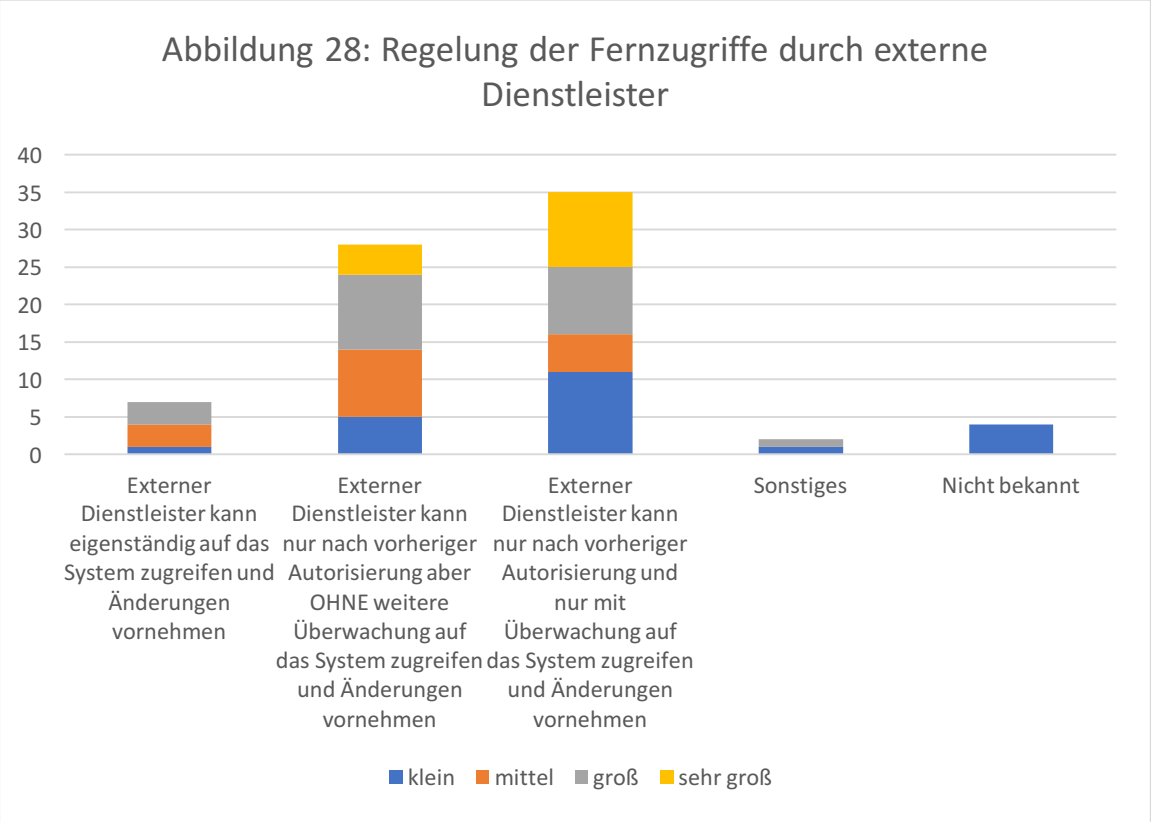
F4 Welche Arten von Fernzugängen sind für Ihr Leitsystem eingerichtet: Mitarbeiterzugänge z.B. für Bereitschafts- oder Entstörungsdienst?



F5 Welche Arten von Fernzugängen sind für Ihr Leitsystem eingerichtet: Nicht bekannt



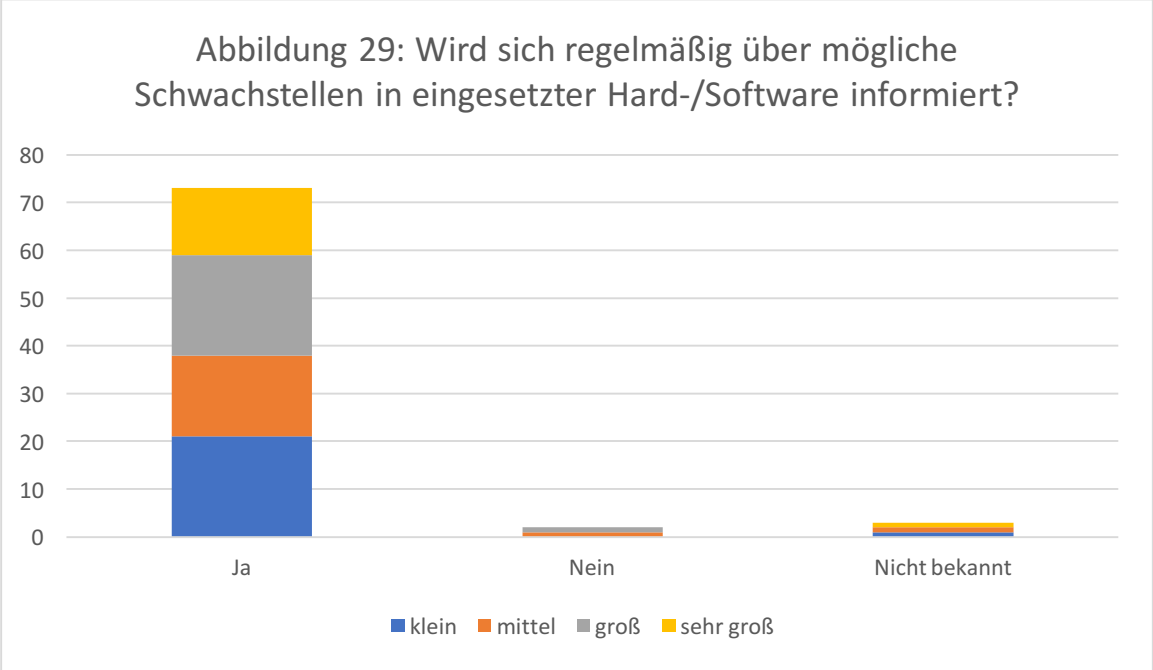
F5 Wie sind Fernzugriffe durch externe Dienstleister geregelt?



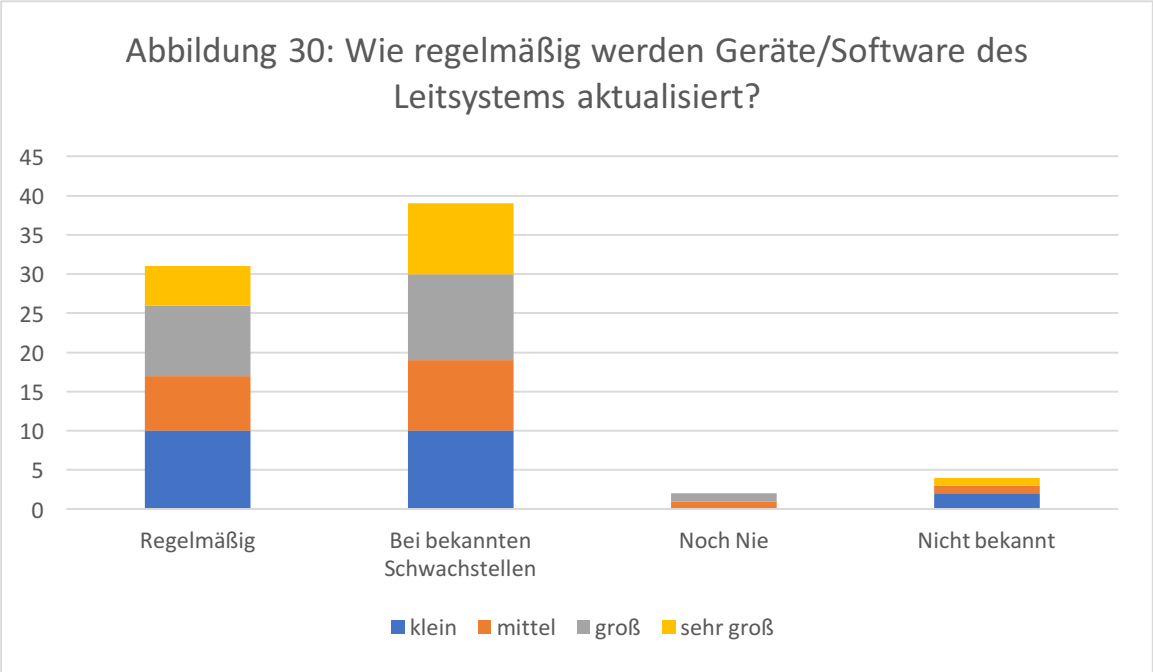
Teil G: Leitsystem: Prozesse und Organisation

Neben den technischen Daten des Leitsystems, ist das Prozess und die organisatorischen Strukturen dahinter mindestens genauso wichtig. IT-Sicherheit muss stetig überwacht und verbessert werden, da sich die Mittel und Techniken der potentiellen Angreifer ständig weiterentwickelt. Genauso müssen aufgedeckte Schwachstellen behandelt werden und es sollte eine regelmäßige Überwachung und Informationsweitergabe innerhalb des Unternehmens gegeben sein, um eine Prävention gegen Hackerangriffe bieten zu können.

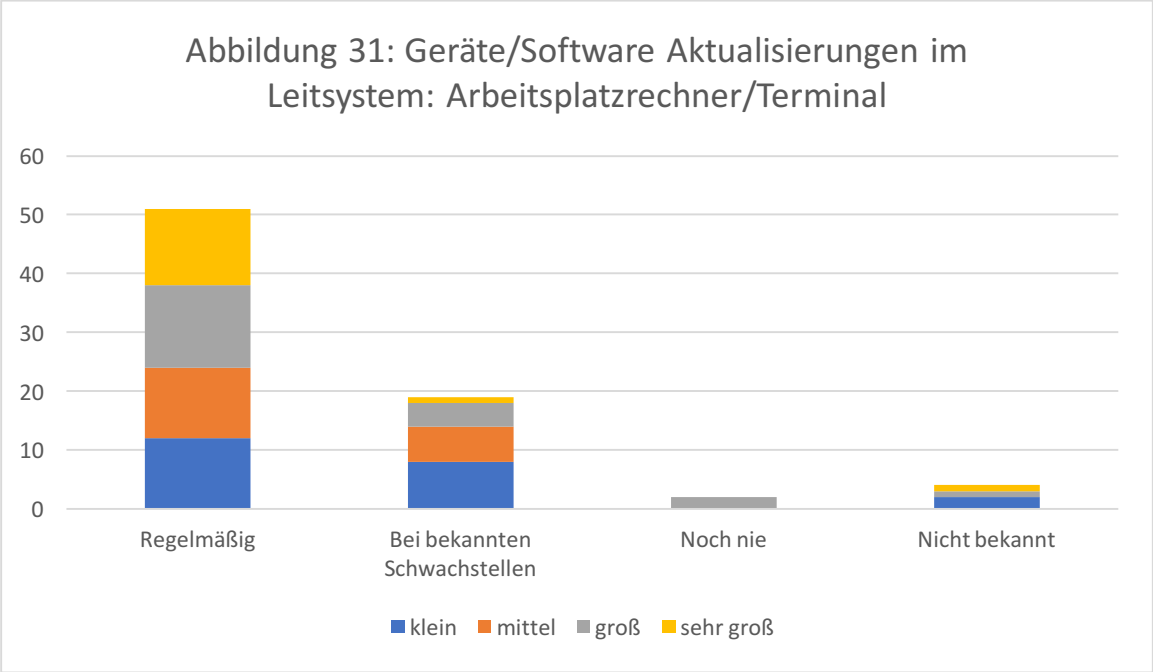
G1 Informieren Sie sich, bzw. die verantwortlichen Mitarbeiter Ihres Unternehmens, regelmäßig über mögliche Schwachstellen eingesetzter Hard- und Software?



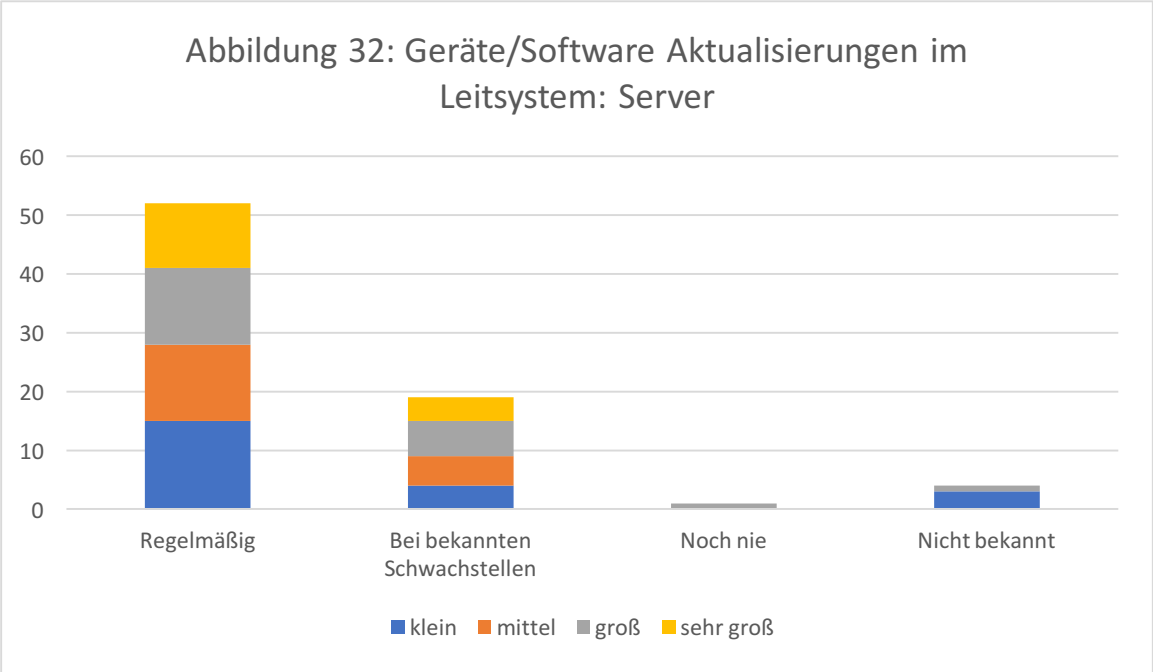
G2 Wie regelmäßig werden Geräte und Software innerhalb Ihres Leitsystems aktualisiert bzw. erneuert: Netzwerk-Equipment (z.B. Router, Switches)?



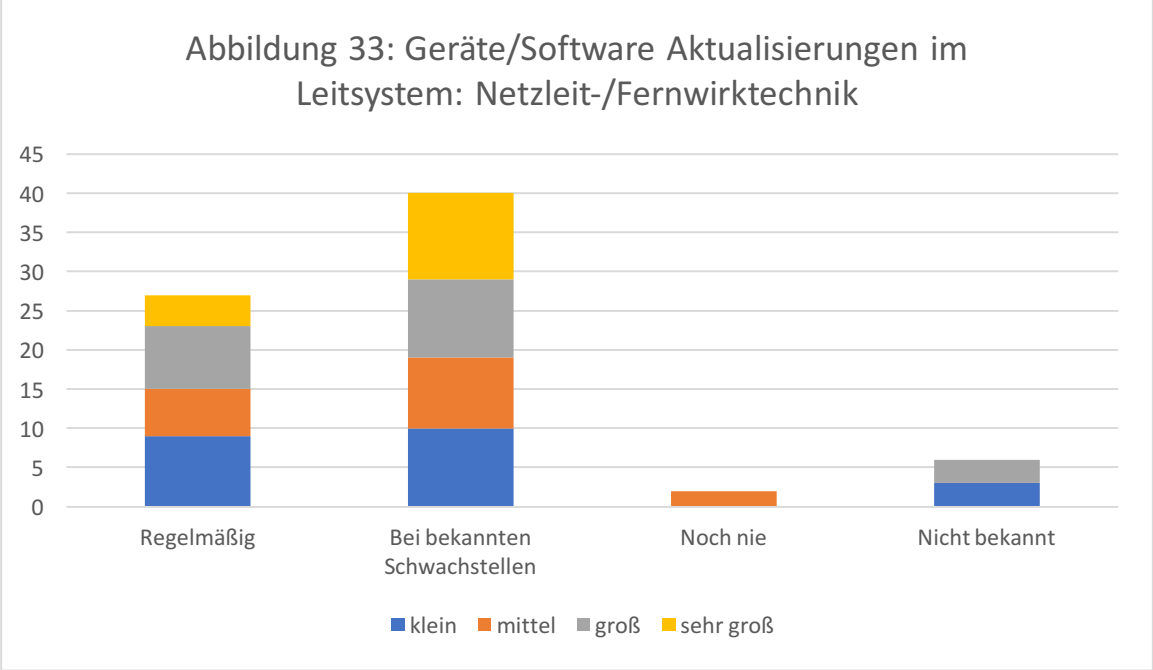
G2 Wie regelmäßig werden Geräte und Software innerhalb Ihres Leitsystems aktualisiert bzw. erneuert: Arbeitsplatzrechner/Terminal?



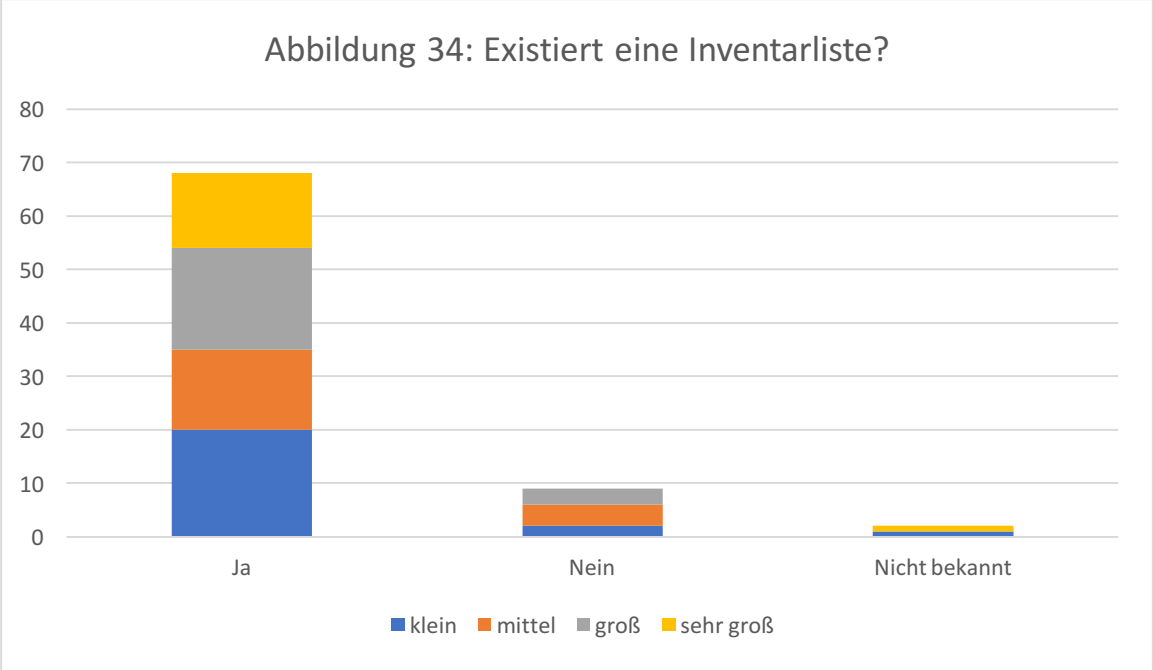
G2 Wie regelmäßig werden Geräte und Software innerhalb Ihres Leitsystems aktualisiert bzw. erneuert: Server?



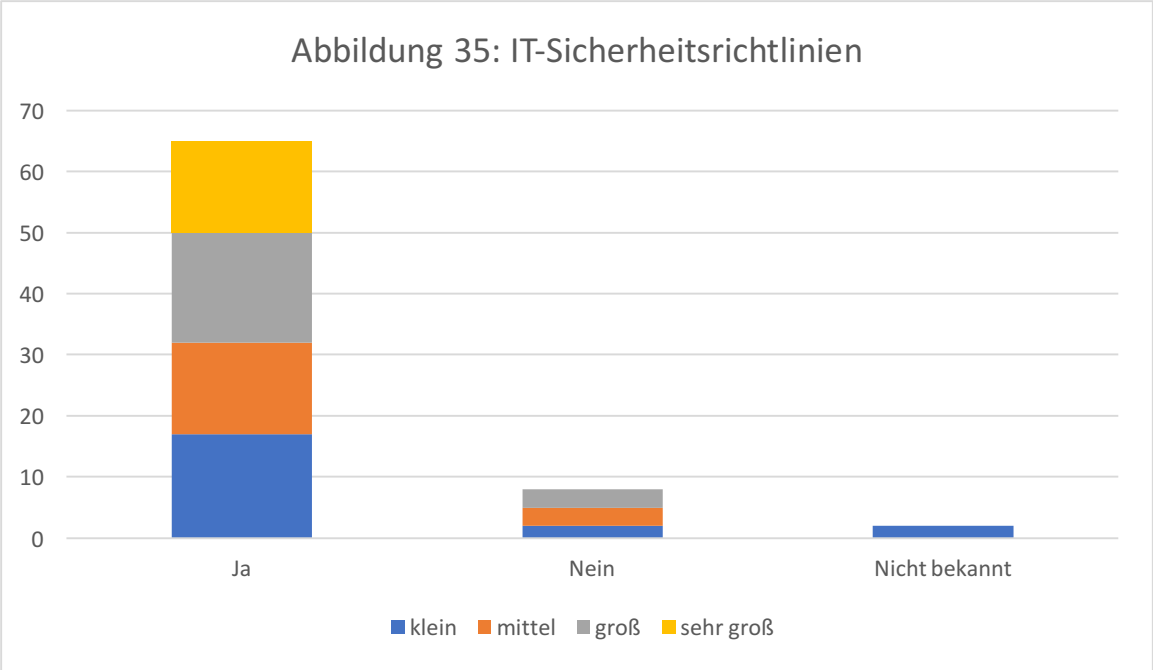
G2 Wie regelmäßig werden Geräte und Software innerhalb Ihres Leitsystems aktualisiert bzw. erneuert: Netzleit-/Fernwirktechnik?



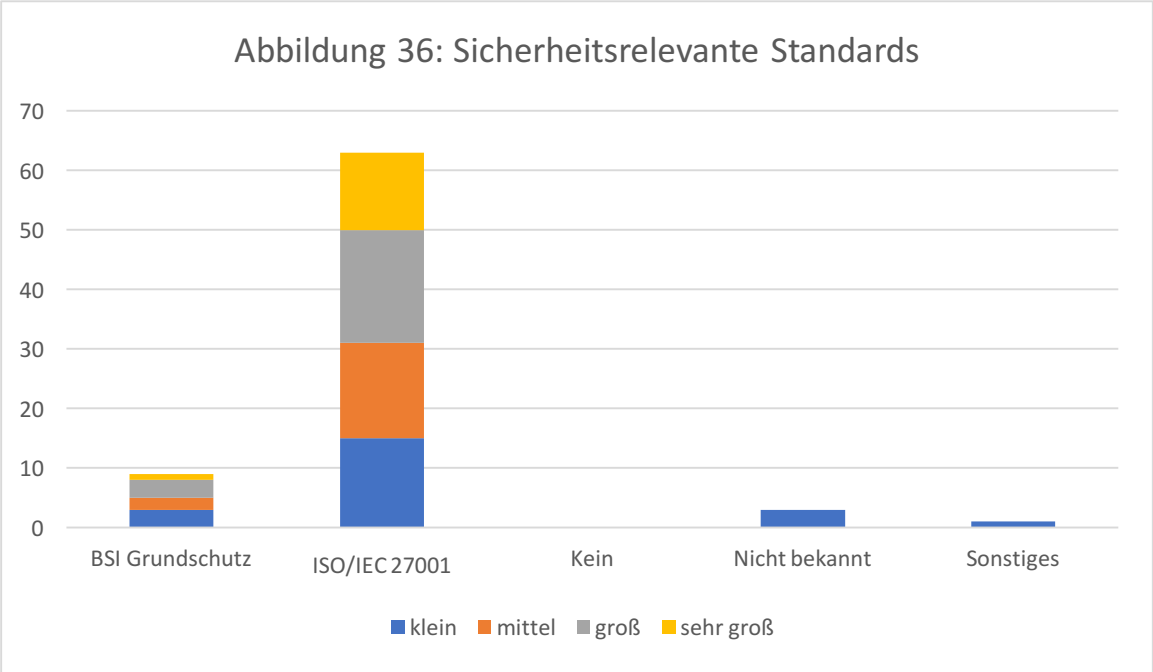
G3 Existiert eine aktuelle Inventarliste, in der alle Softwarestände dokumentiert sind (z.B. mit Versionsnummern, zugeordneten Accounts und IP-Adressen)?



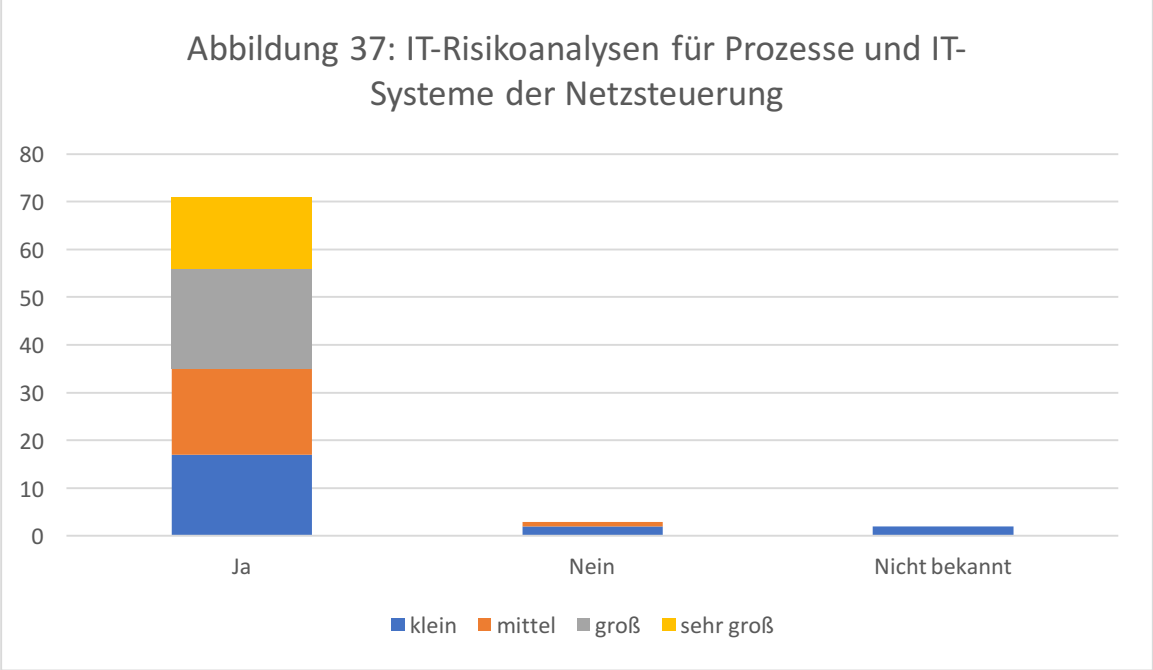
G4 Gibt es in Ihrem Unternehmen niedergeschriebene IT-Sicherheitsleitlinien für den Bereich des Leitsystems?



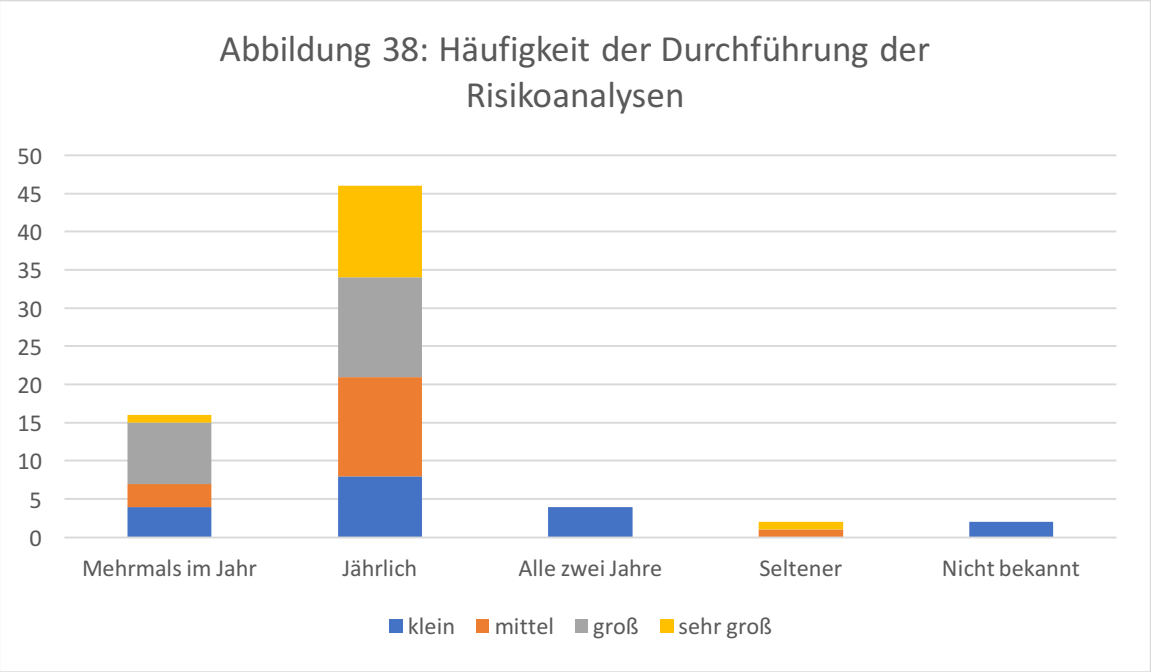
G5 Anhand welcher sicherheitsrelevanten Standards sind Ihre IT-Systeme und Prozesse zur Netzsteuerung ausgelegt?



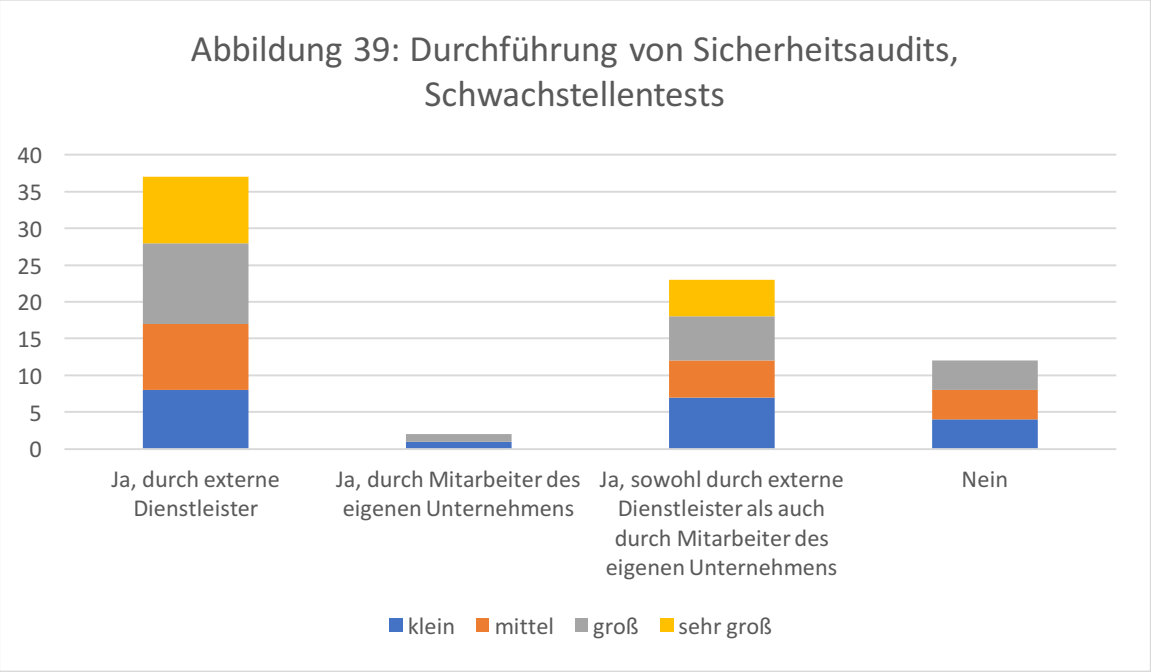
G6 Führen Sie IT-Risikoanalysen für die Prozesse und IT-Systeme zur Netzsteuerung durch?



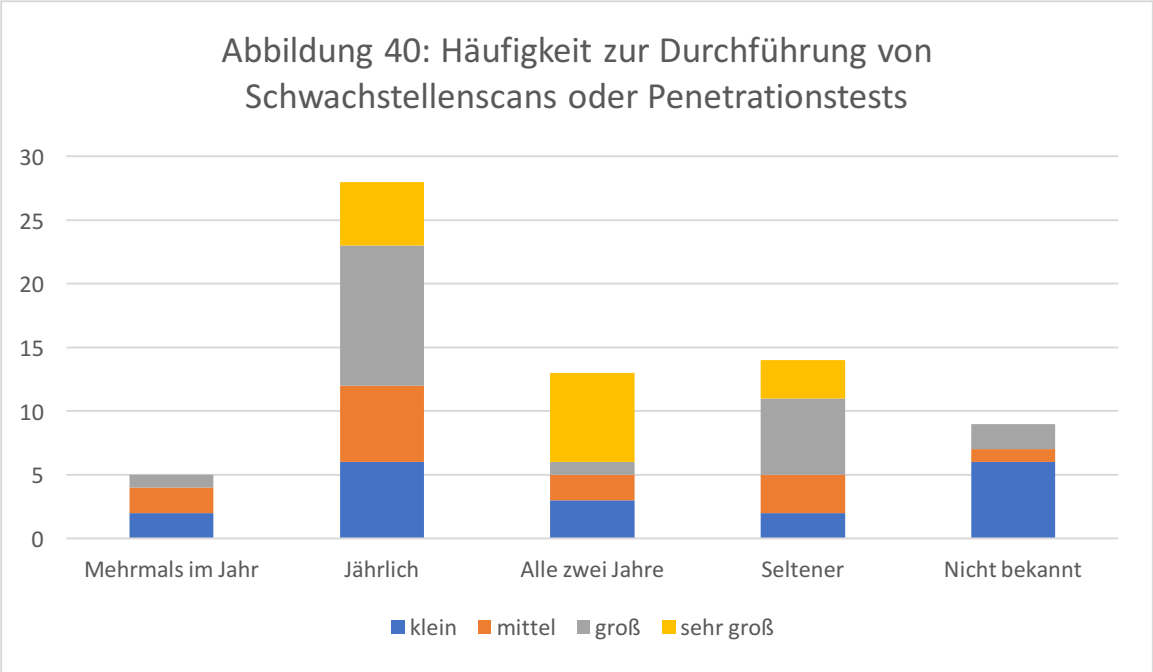
G7 Wie regelmäßig führen Sie solche Risikoanalysen durch?



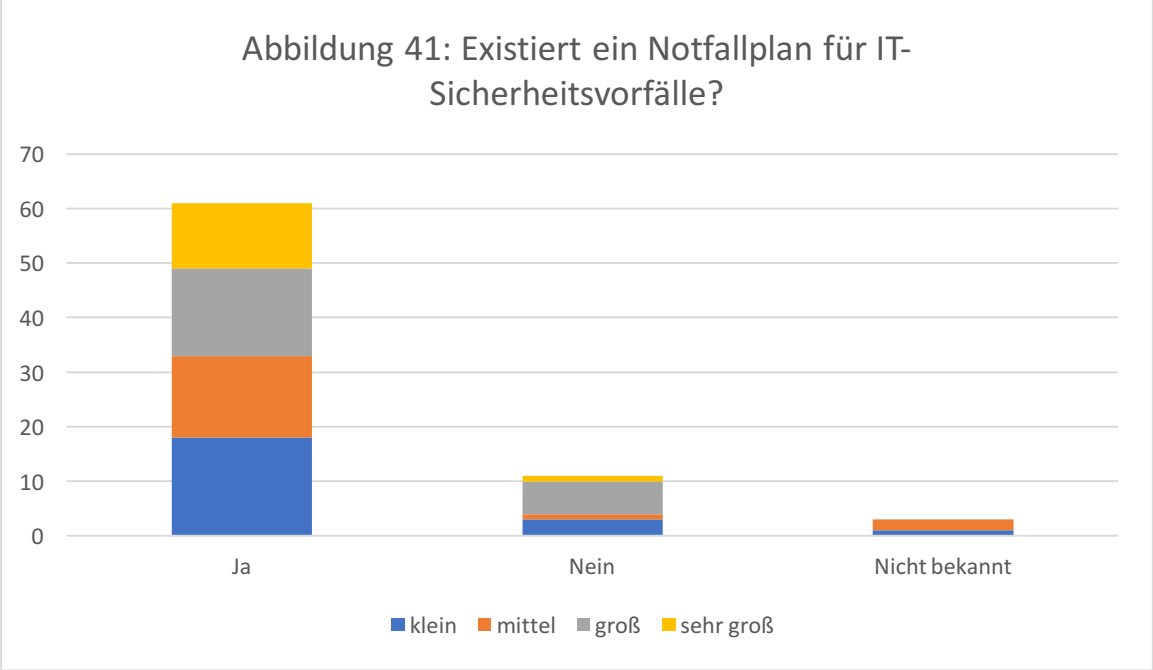
G8 Führen Sie Sicherheitsaudits, Schwachstellenscans oder Penetrationstests für die Systeme zur Steuerung der Netzleittechnik durch?



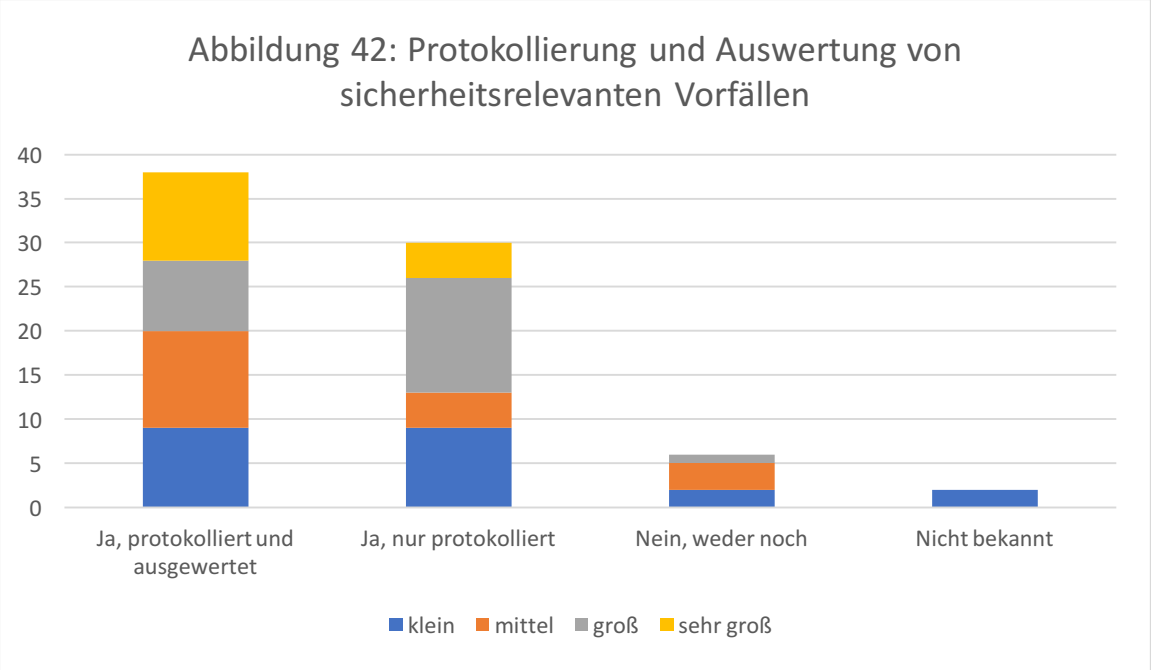
G9 Wie häufig führen Sie solche Schwachstellenscans oder Penetrationstests durch?



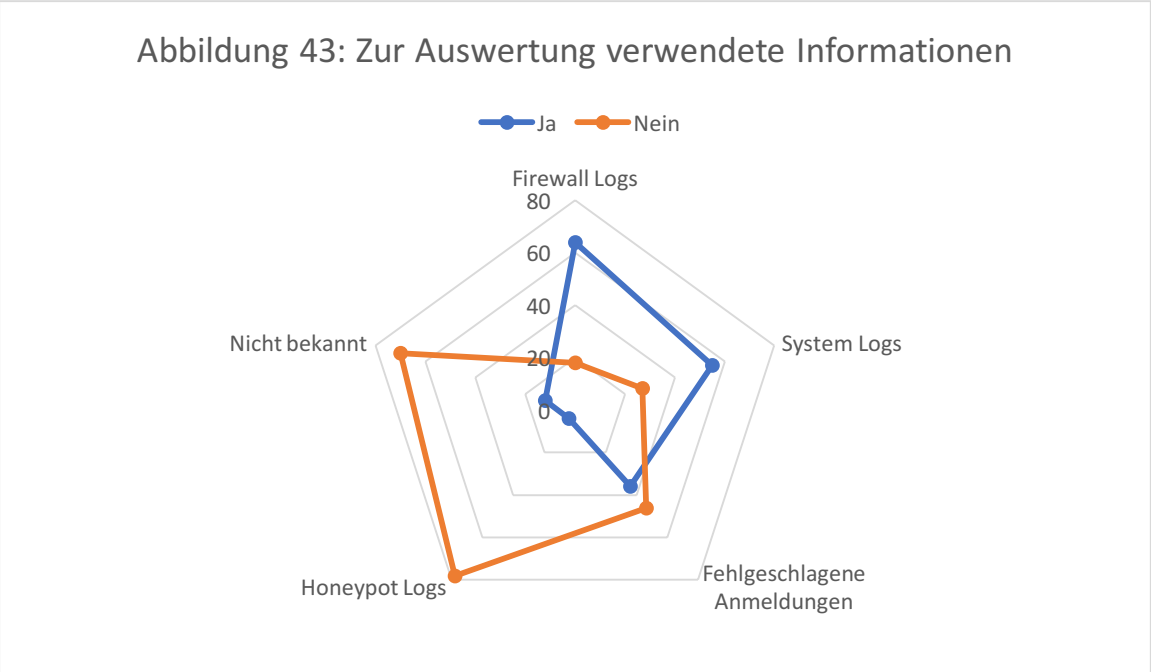
G10 Haben Sie einen Notfallplan für IT-Sicherheitsvorfälle, die die Netzsteuerung betreffen?



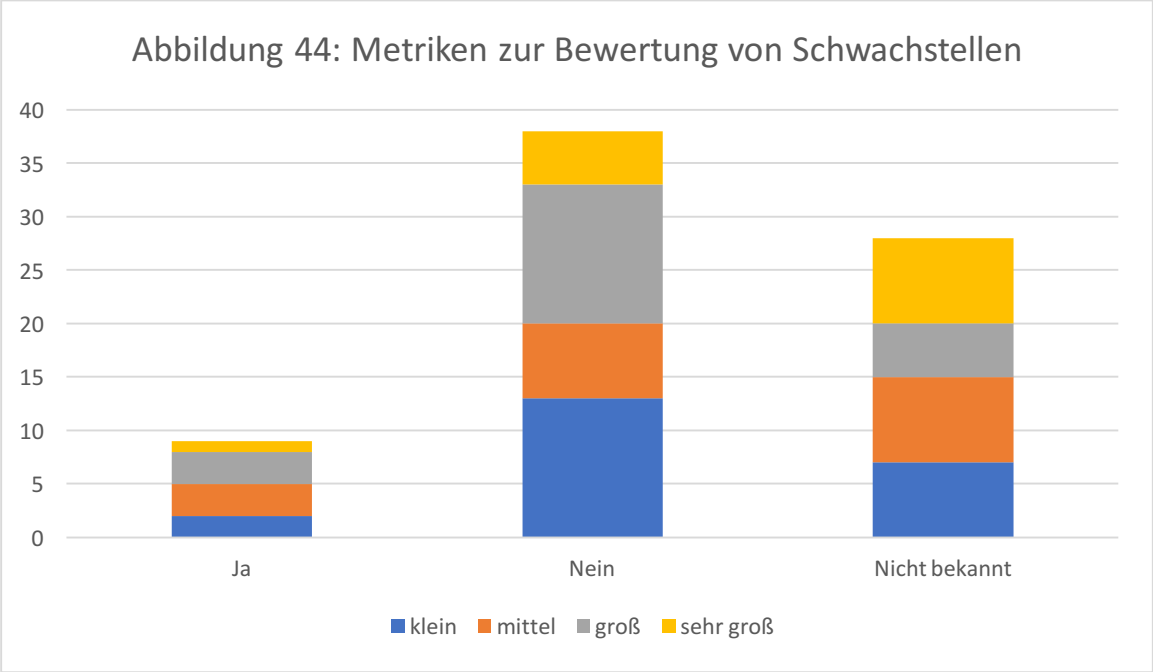
G11 Werden sicherheitsrelevante Vorfälle (z.B. Portscans, fehlgeschlagene Anmeldeversuche, nicht autorisierte Vorgänge) protokolliert und ausgewertet?



G12 Welche Informationen werten Sie zur Identifikation von Angriffen auf die IT-Systeme zur Netzsteuerung aus?



G13 Setzen Sie Metriken zur Bewertung von Schwachstellen ein (z.B. CVSS)?



G14 Ist IT-Sicherhit als eine Anforderung beim Kauf neuer Hard- und Software definiert?