Technischer Bericht

Stand zur IT-Sicherheit deutscher Stromnetzbetreiber

Bei der Erstellung dieses Berichts haben mitgewirkt:

Julian Dax, Universität Siegen
Benedikt Ley, Universität Siegen
Sebastian Pape, Goethe Universität Frankfurt
Volkmar Pipek, Universität Siegen
Kai Rannenberg, Goethe Universität Frankfurt
Christopher Schmitz, Goethe Universität Frankfurt
André Sekulla, Universität Siegen

Erscheinungsjahr 2017, Universität Siegen, Siegen – Aktualisierte Version

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 881 im August 2016 bei der Bundesnetzagentur gelisteten Betreiber angeschrieben. In dem Umfragezeitraum vom 1. September 2016 bis zum 15. Oktober 2016 antworten 61 (6.9%) 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.

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.

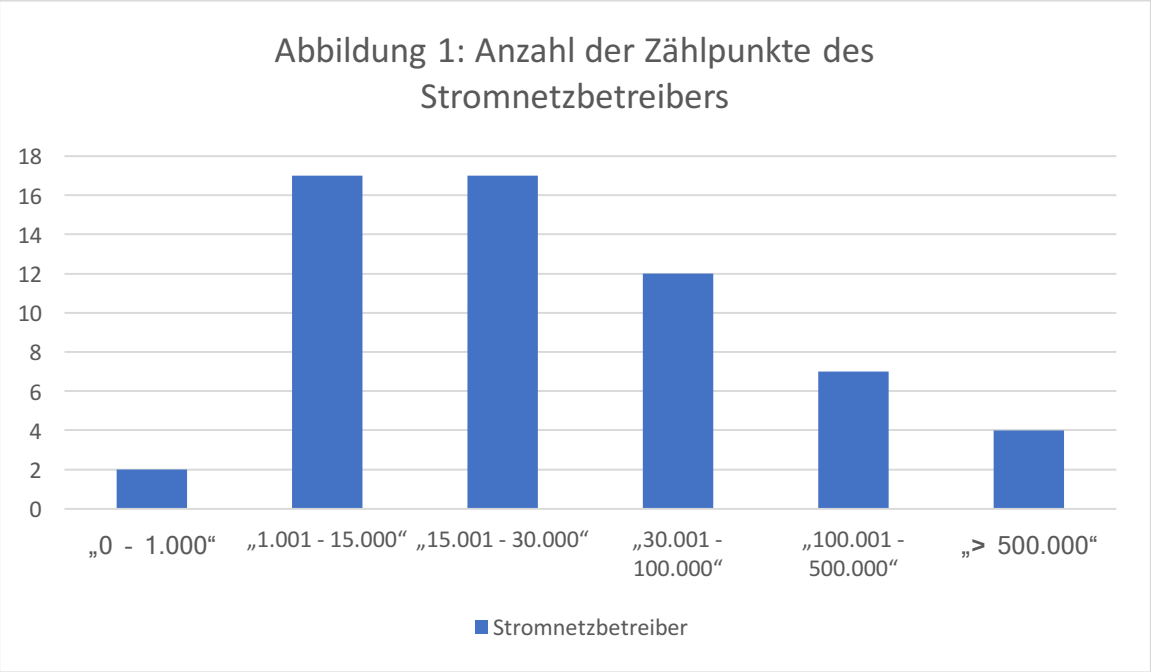


Abbildung 1: Wie viele Zählpunkte werden über Ihr Stromnetz versorgt?

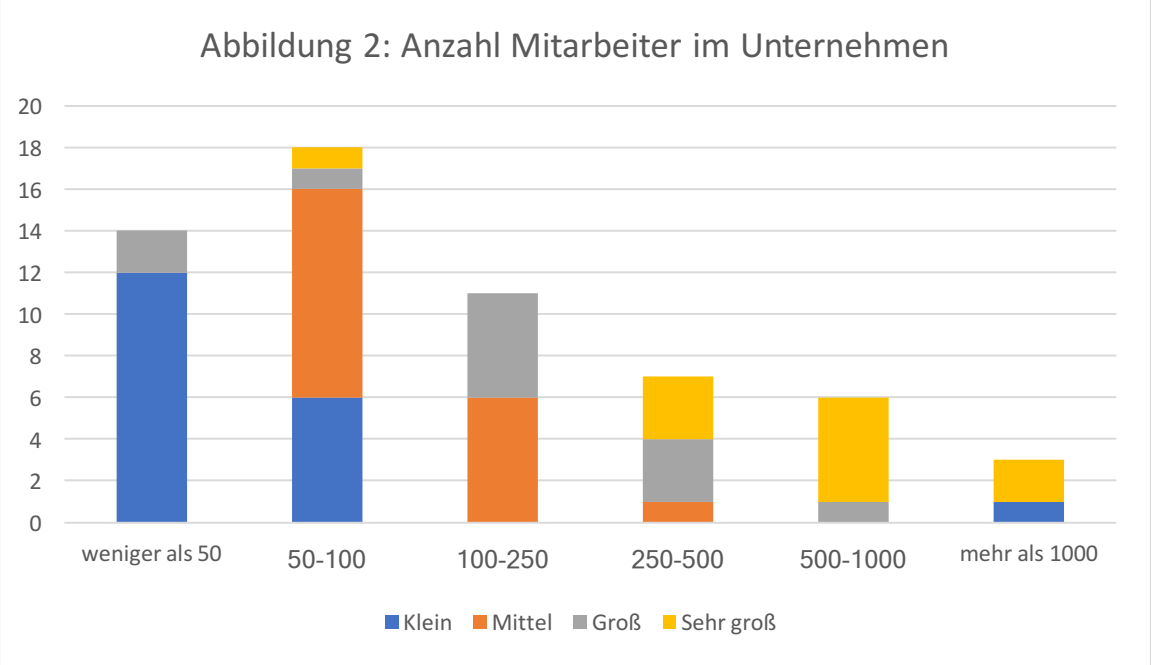


Abbildung 2: Wie viele Mitarbeiter/innen sind in Ihrem Unternehmen beschäftigt?

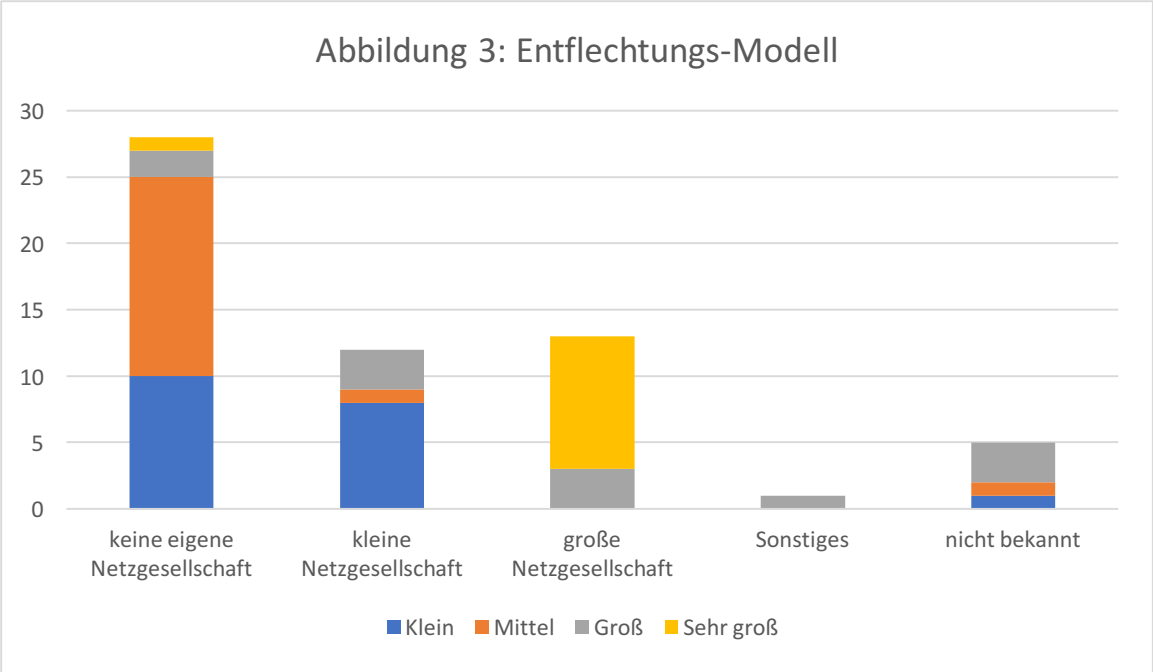


Abbildung 3: Welches Entflechtungs-Modell wurde in Ihrem Unternehmen umgesetzt?

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.

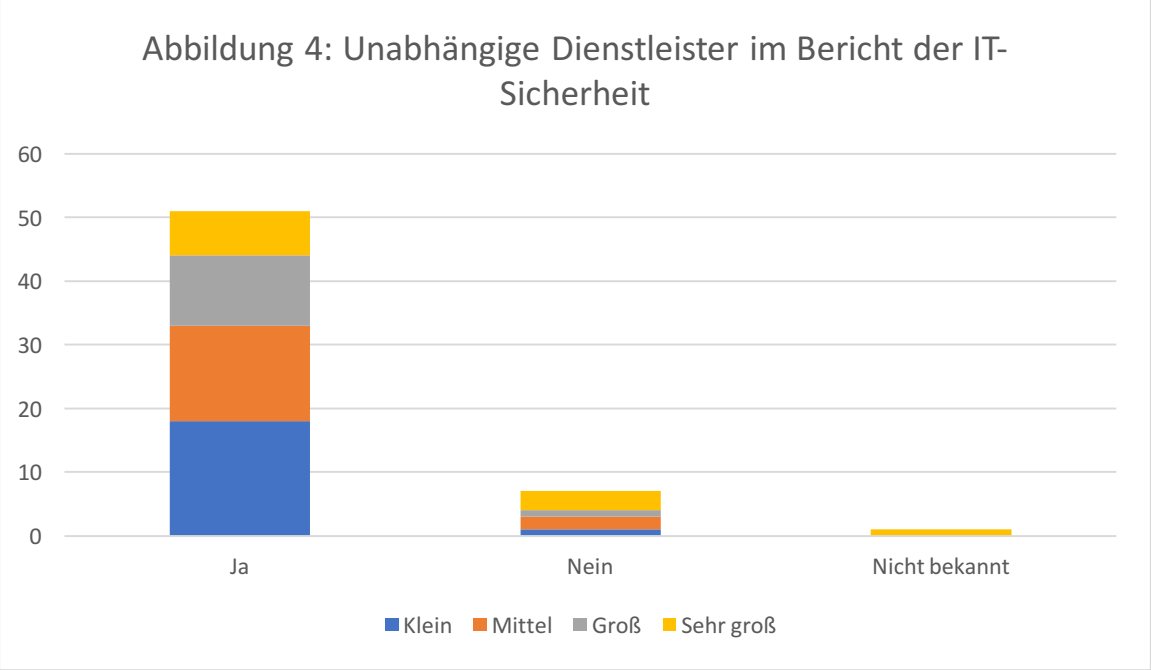


Abbildung 4: Werden in Ihrem Unternehmen, unabhängige Dienstleister im Bereich IT-Sicherheit eingesetzt?

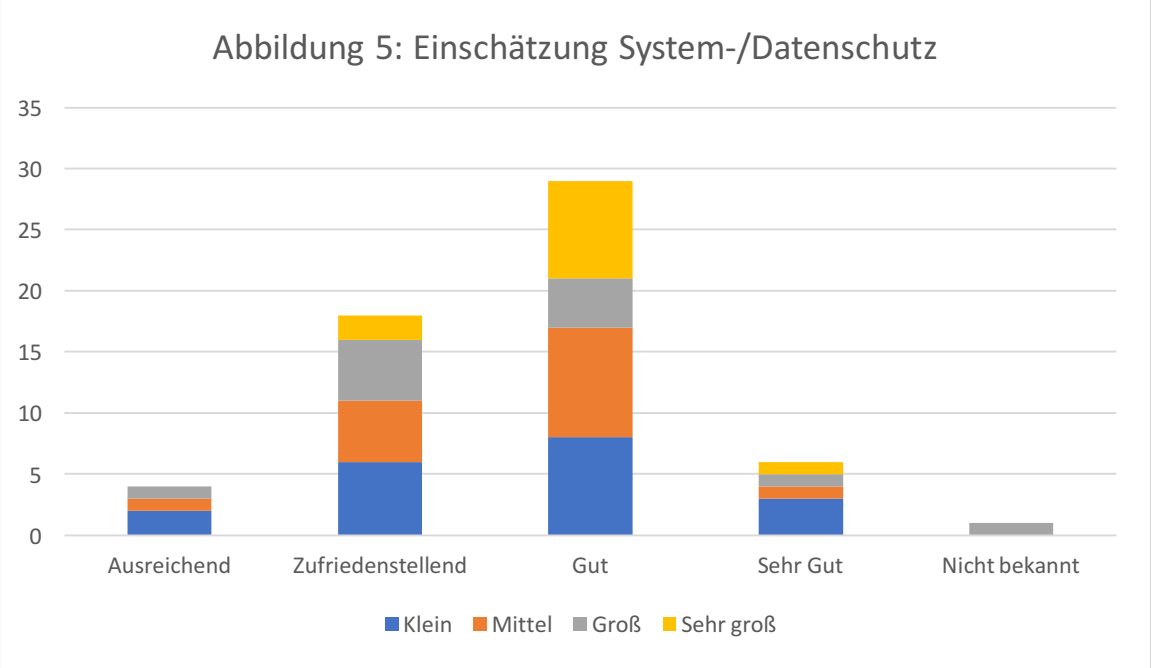
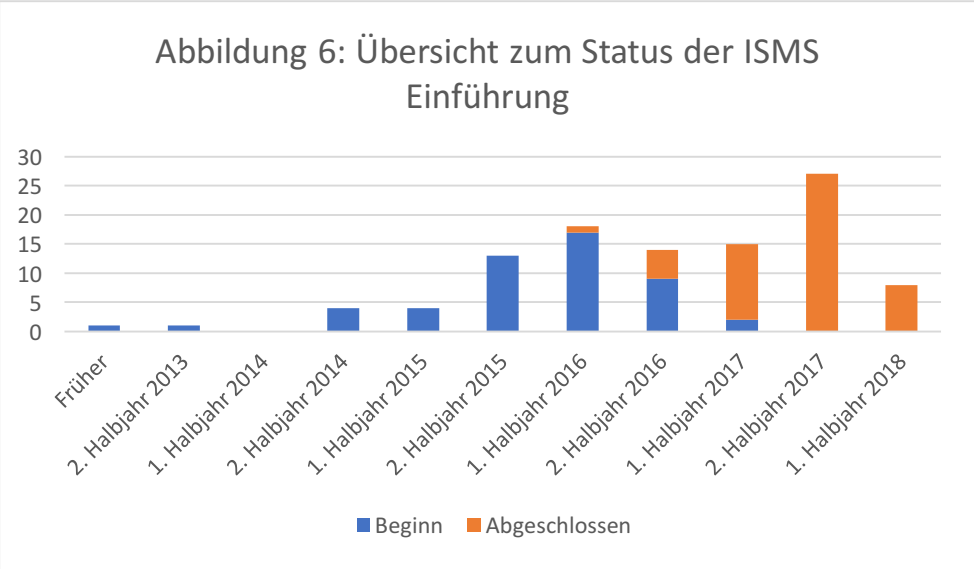


Abbildung 5: Wie gut sind Ihrer Einschätzung nach die Systeme und Daten Ihres Unternehmens geschützt?

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.



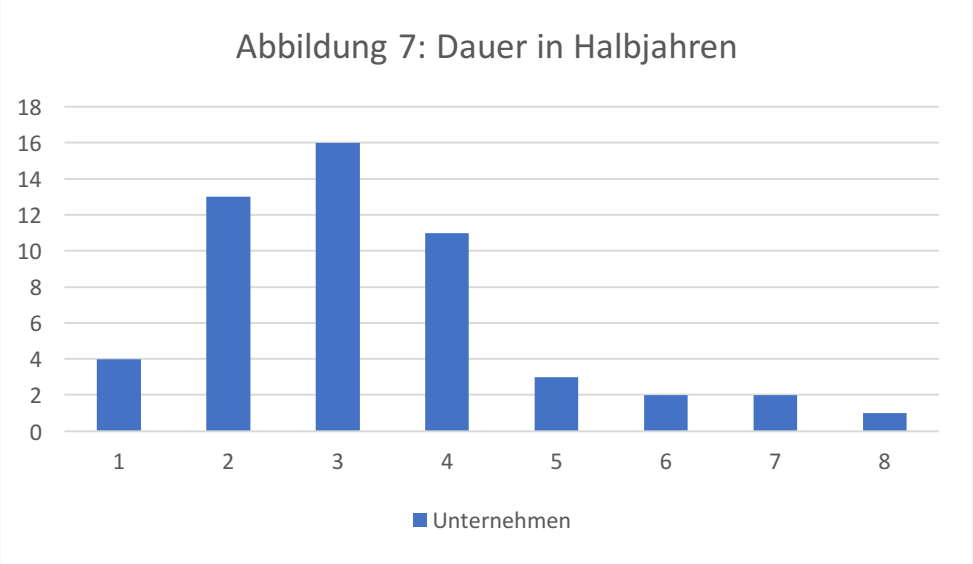


Abbildung 6 und 7 befasst sich mit folgenden Fragen:

- Die Einführung eines ISMS ...
- Wann sollen die Arbeiten zur Einführung eines ISMS beginnen?
- Wann wurde mit den Arbeiten zur Einführung eines ISMS begonnen?
- Bis wann sollen die Arbeiten zur Einführung eines ISMS abgeschlossen sein?
- Wann wurden die Arbeiten zur Einführung eines ISMS abgeschlossen?

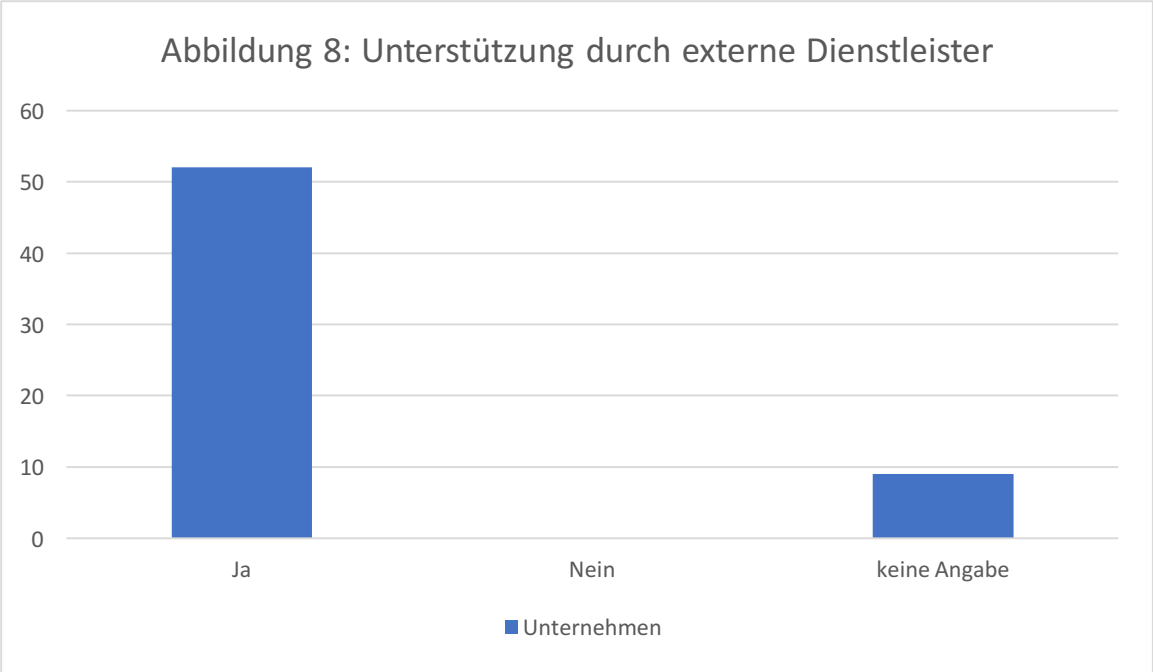


Abbildung 8: Wurden bzw. werden bei der Einführung eines ISMS externe Dienstleister (z.B. Unternehmensberater) hinzugezogen?

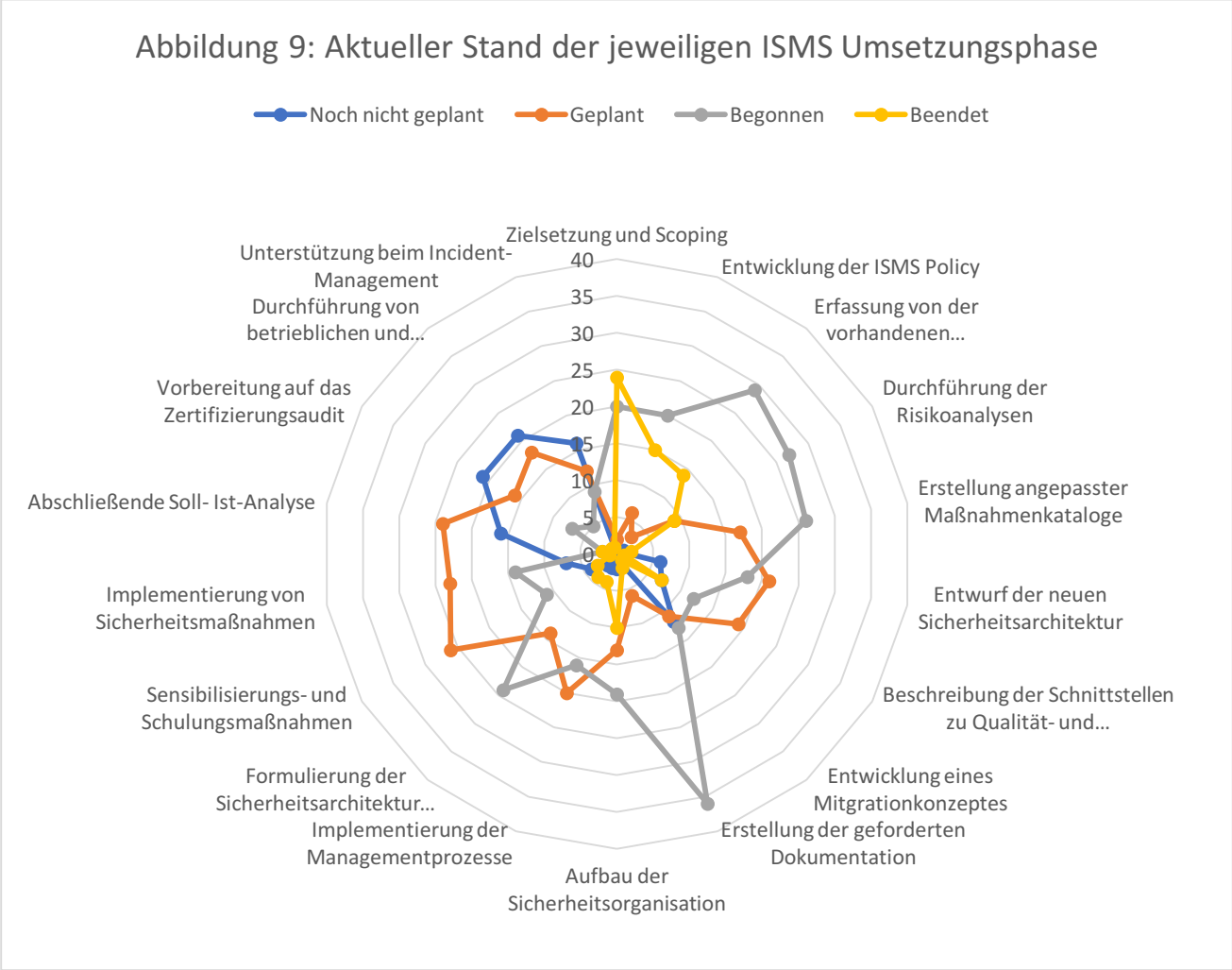


Abbildung 9: Wie ist der aktuelle Stand der jeweiligen ISMS Umsetzungsphasen?

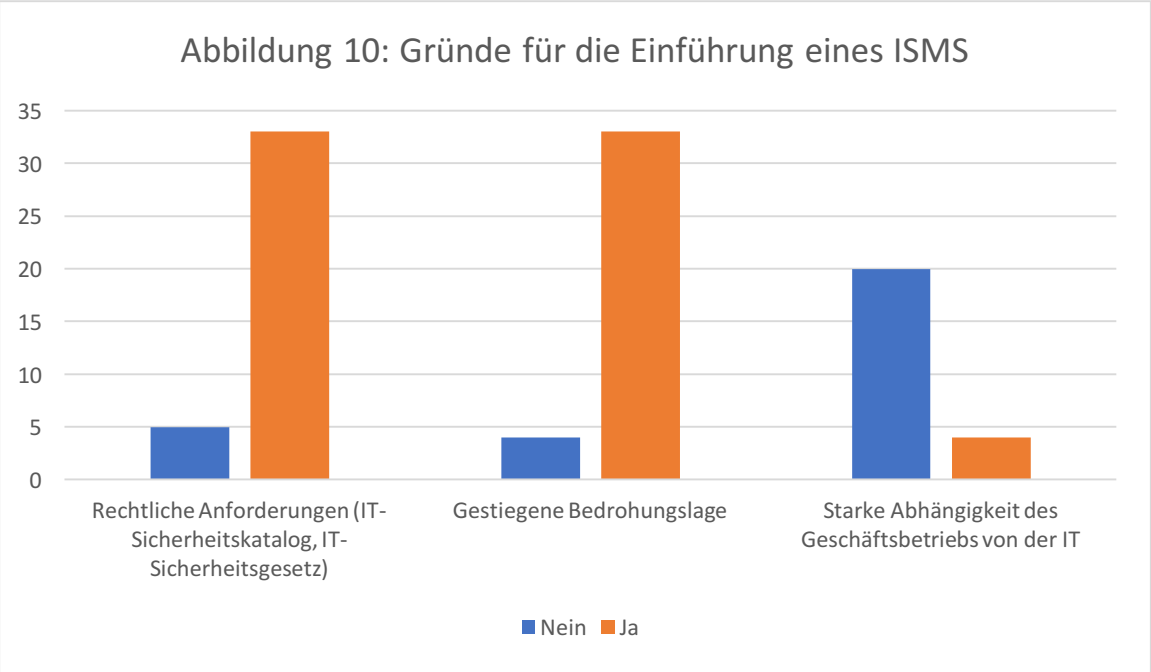


Abbildung 10: Was waren für Sie die wesentlichen Gründe für die Einführung eines ISMS (Mehrfachauswahl möglich)?

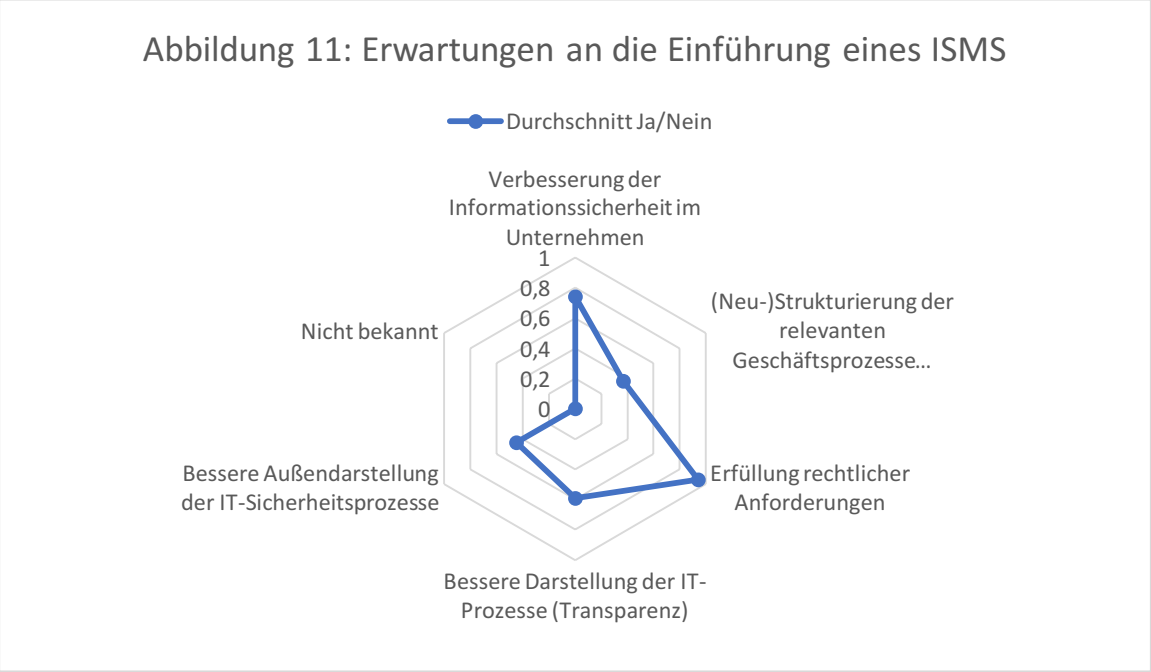


Abbildung 11: Was erhoffen Sie sich bzw. erwarten Sie von der Einführung eines ISMS (Mehrfachauswahl möglich)?

Teil D: 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.

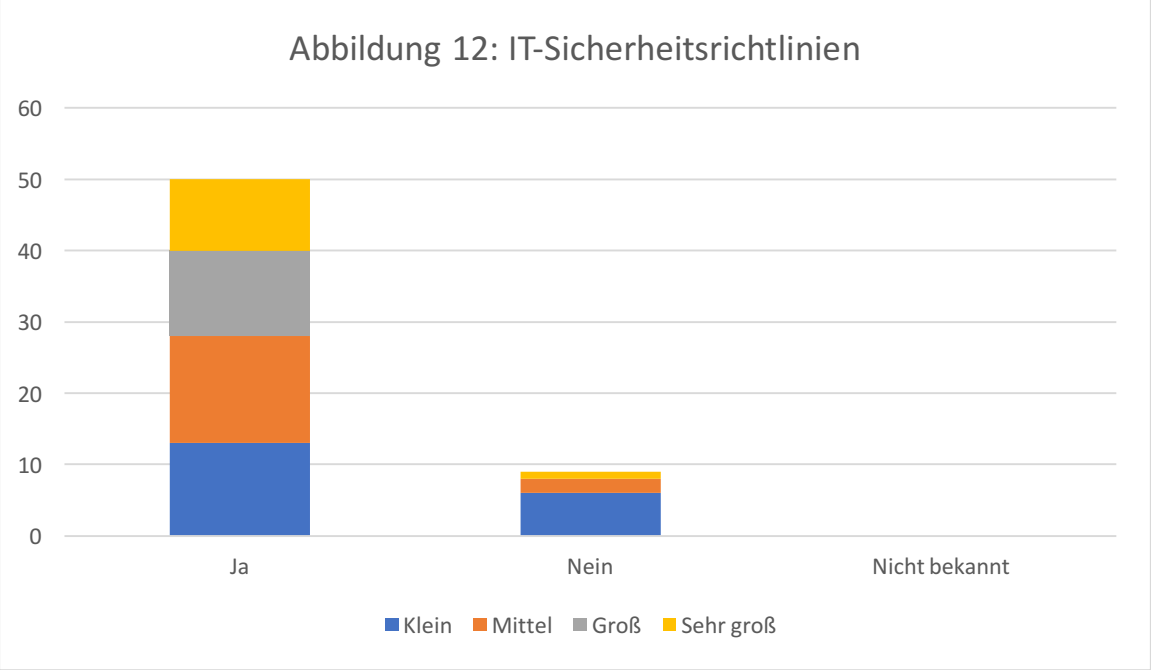


Abbildung 12: Existieren IT-Sicherheitsrichtlinien für die Büro IT Ihres Unternehmens?

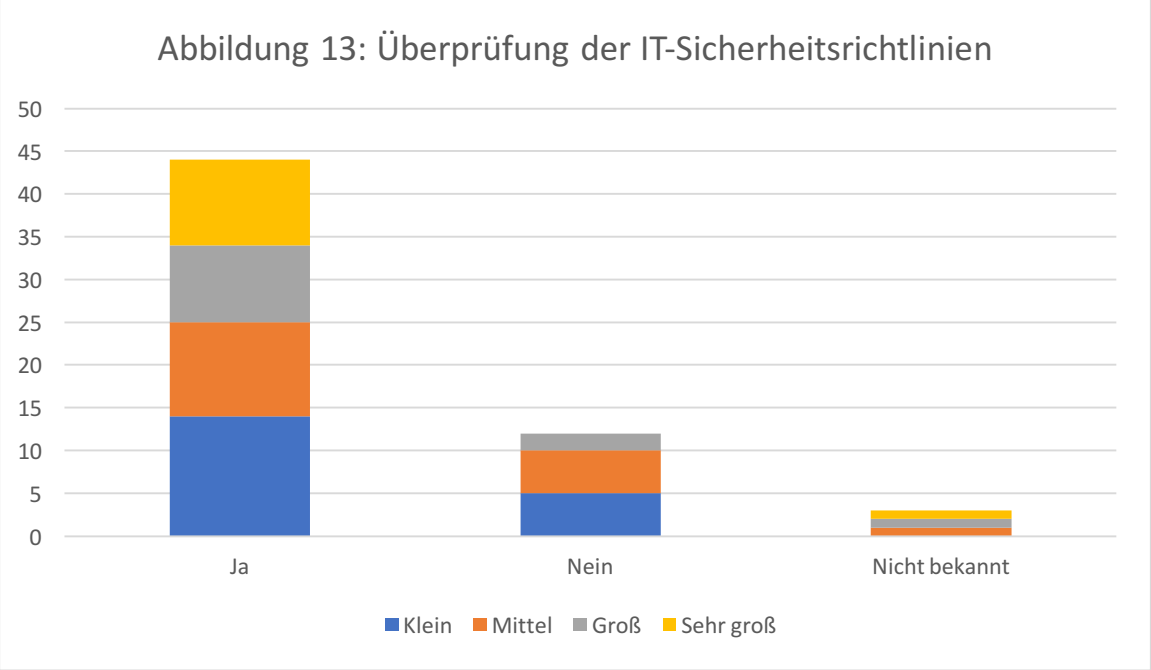


Abbildung 13: Werden die IT-Sicherheitsrichtlinien in regelmäßigen Zeitabständen überprüft und ggf. angepasst?

Teil E: 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.

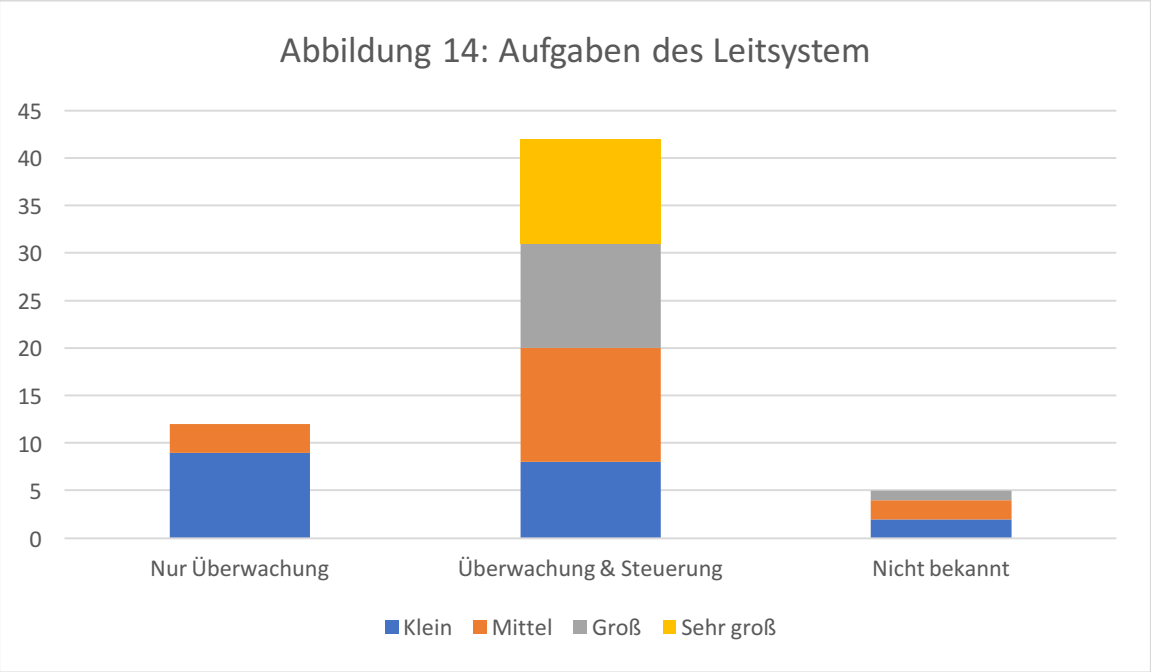


Abbildung 14: Dient Ihr Leitsystem nur der Netzüberwachung oder können hierüber auch Schaltvorgänge durchgeführt werden?

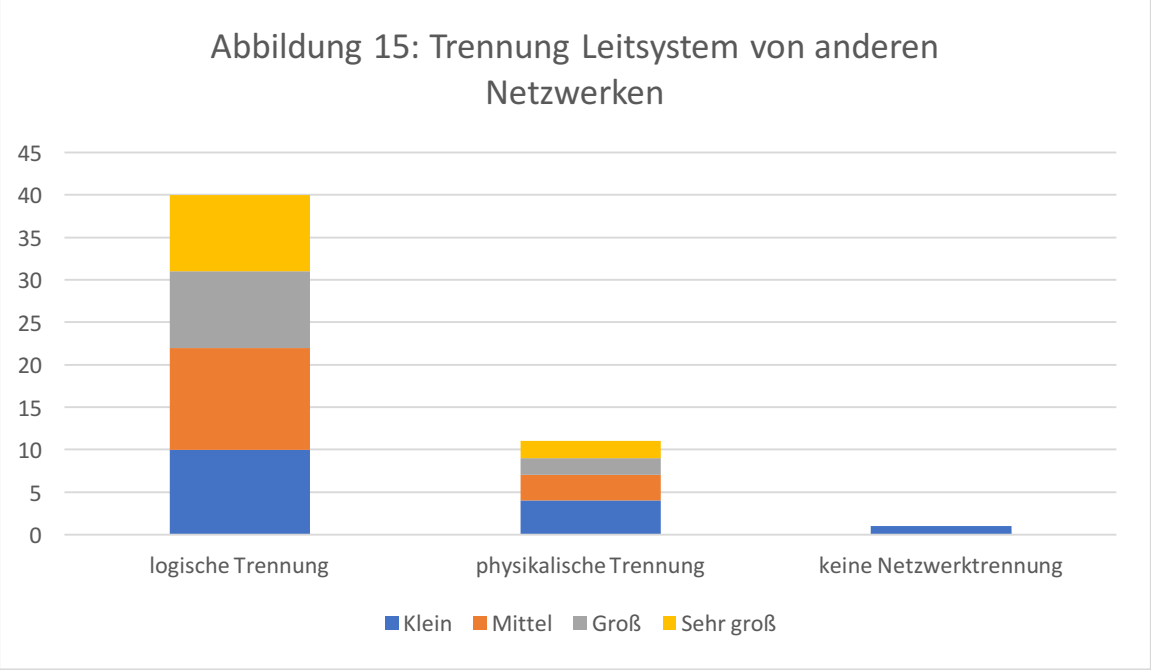


Abbildung 15: Wie ist das IT-Netzwerk Ihres Leitsystems von anderen Netzwerken (z. B. Büro IT, Internet, Wartungsfirmen) getrennt?

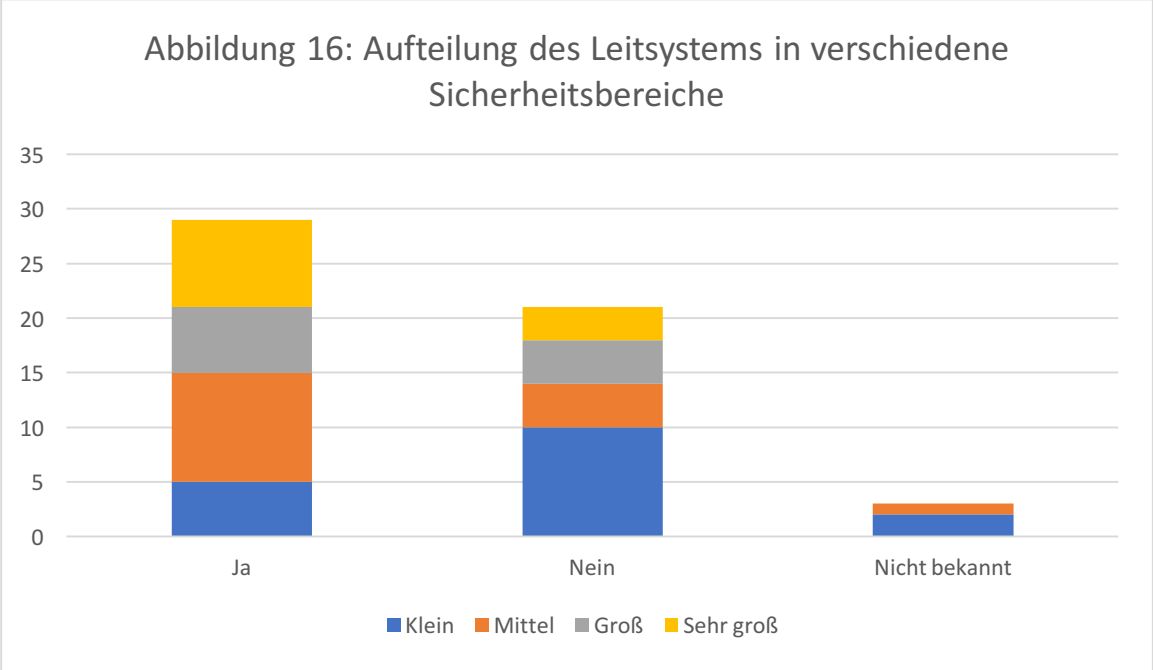


Abbildung 16: Ist das Netzwerk Ihres Leitsystems in verschiedene Sicherheitsbereiche unterteilt (z. B. durch verschiedene VLANs)?

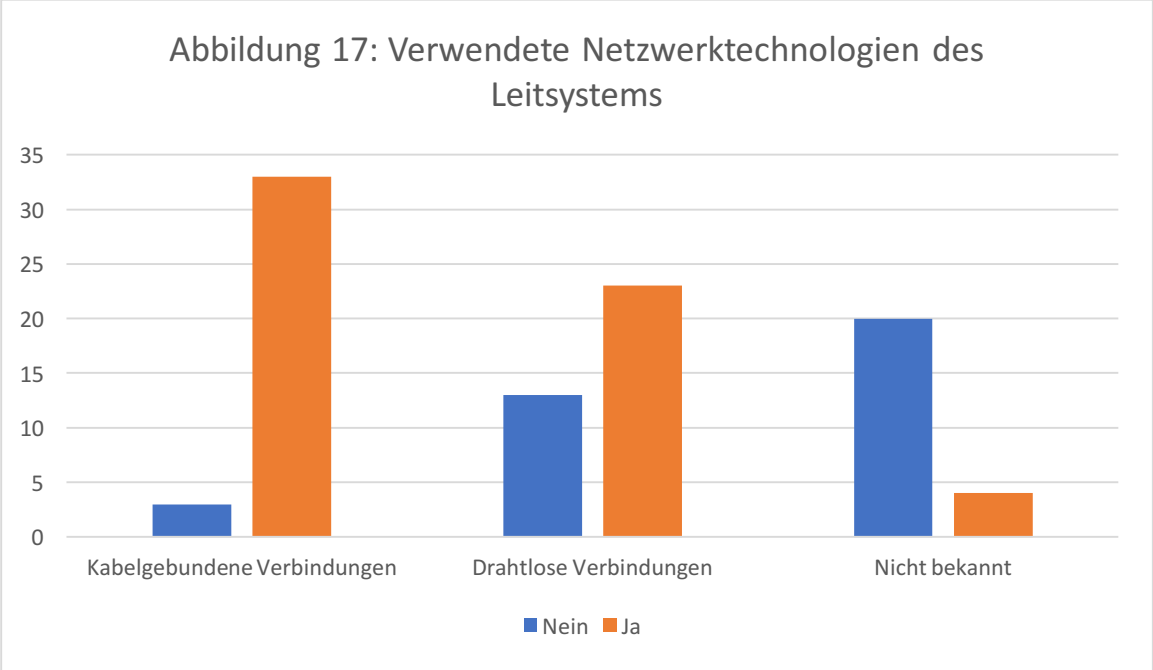


Abbildung 17: Welche Netzwerktechnologien werden im Netzwerk Ihres Leitsystems eingesetzt (Mehrfachnennungen sind möglich)?

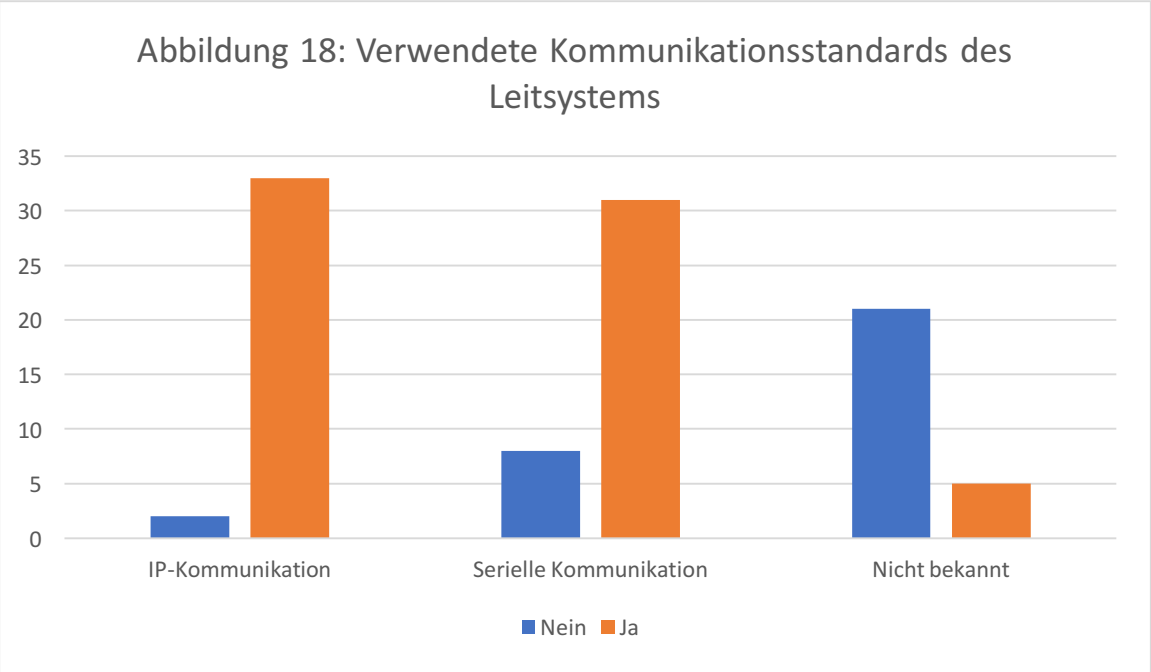


Abbildung 18: Welche Kommunikationsstandards werden im Netzwerk Ihres Leitsystems verwendet (Mehrfachnennungen sind möglich)?

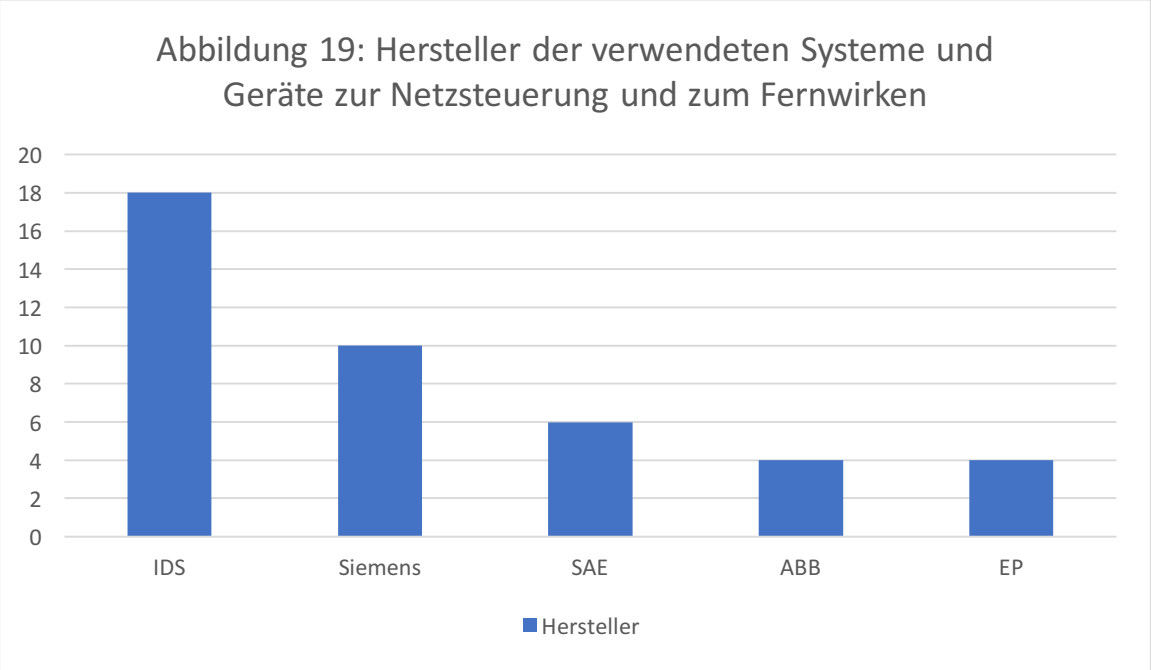


Abbildung 19: Von welchen Herstellern setzen Sie Systeme und Geräte zur Netzsteuerung und zum Fernwirken ein? (ab mind. vier Nennungen in der Abbildung aufgenommen)

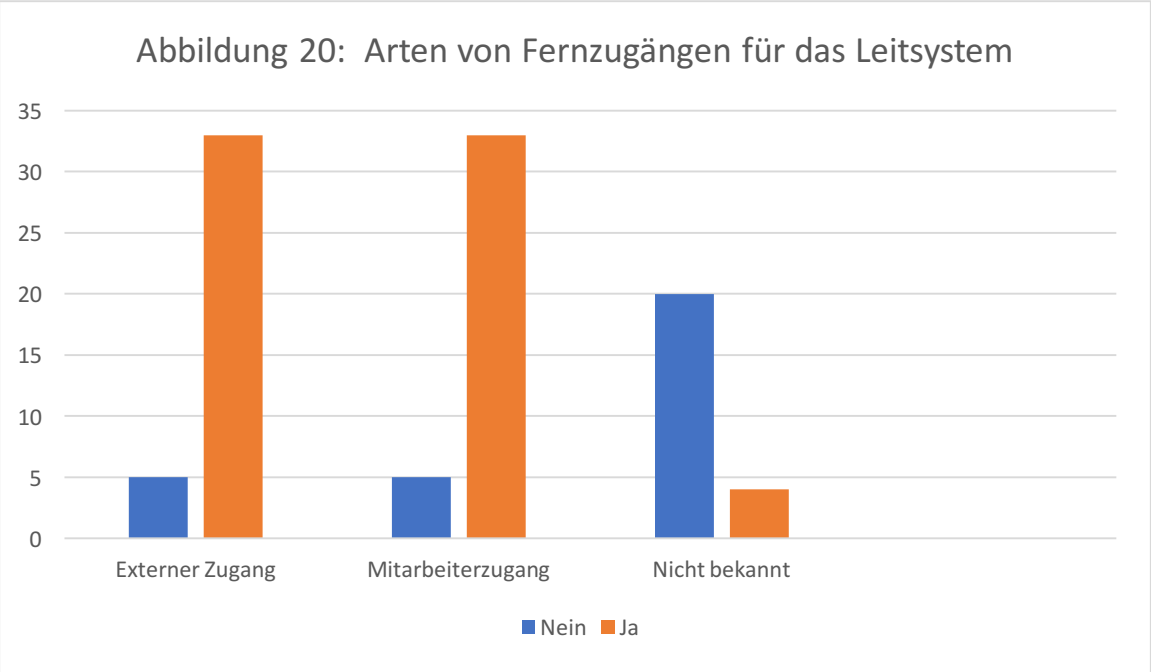


Abbildung 20: Welche Arten von Fernzugängen sind für Ihr Leitsystem eingerichtet (Mehrfachnennungen möglich)?

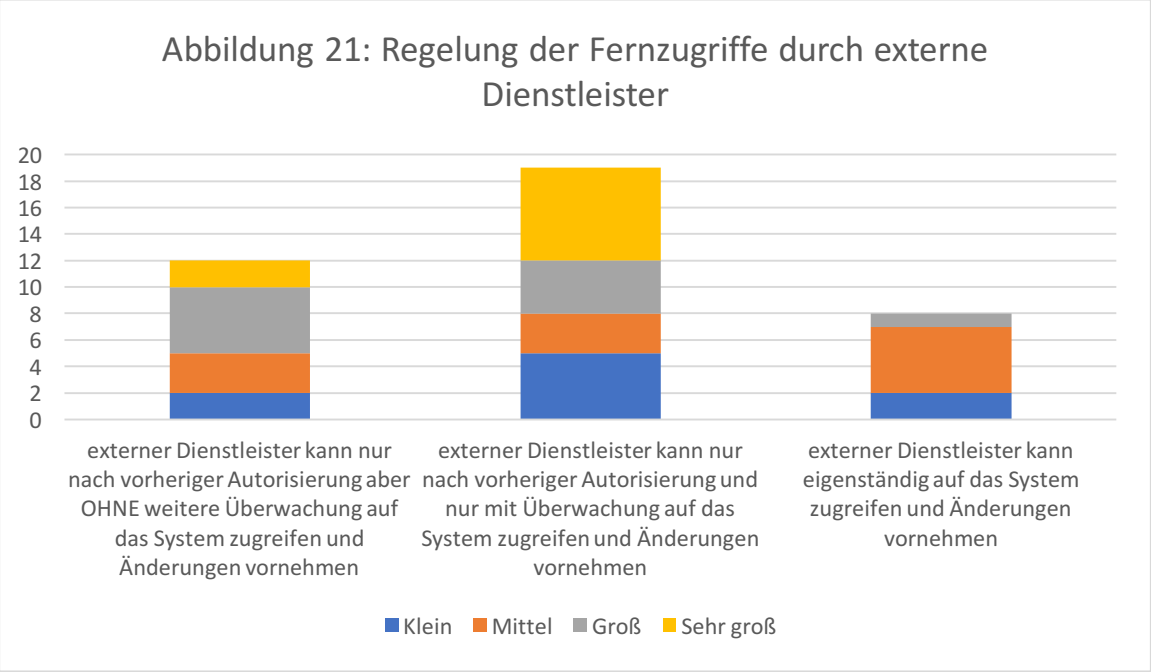


Abbildung 21: Wie sind Fernzugriffe durch externe Dienstleister geregelt?

Teil F: Leitsystem: Prozess 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.

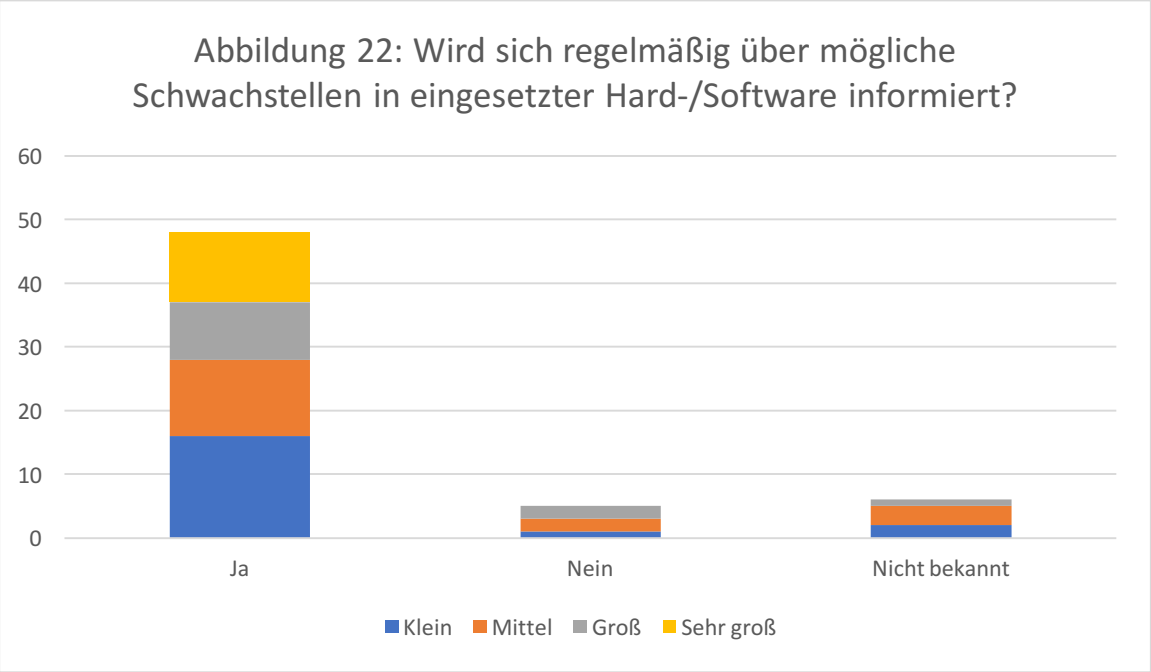


Abbildung 22: Informieren Sie sich, bzw. die verantwortlichen Mitarbeiter Ihres Unternehmens, regelmäßig über mögliche Schwachstellen eingesetzter Hard- und Software?

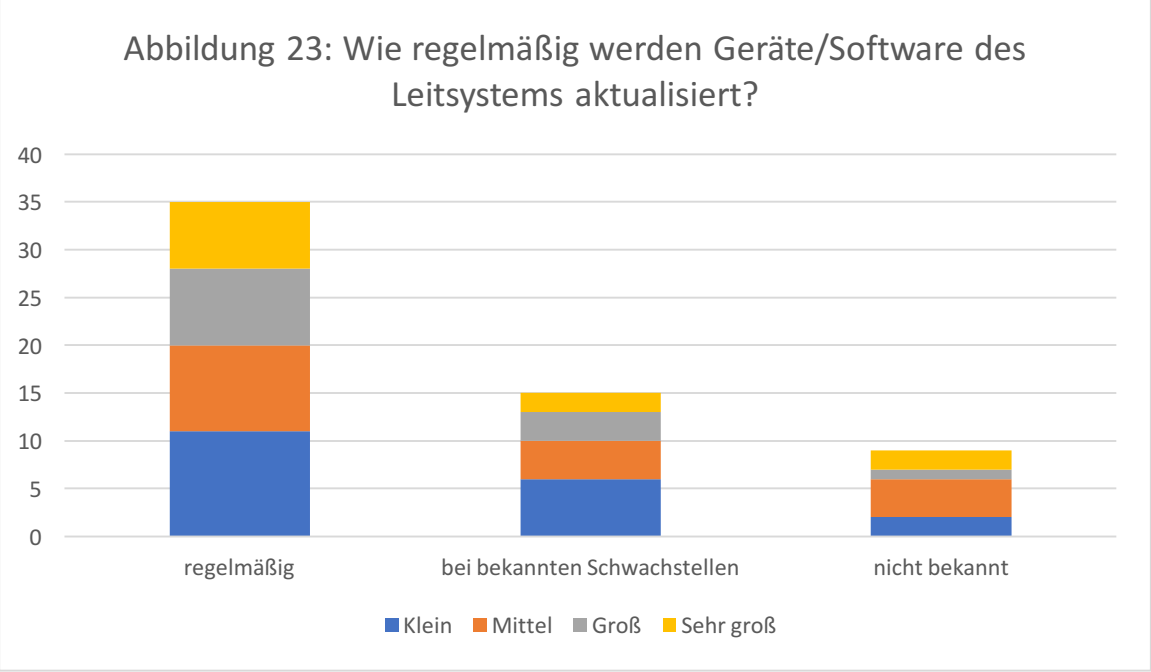


Abbildung 23: Wie regelmäßig werden Geräte und Software innerhalb Ihres Leitsystems aktualisiert bzw. erneuert?

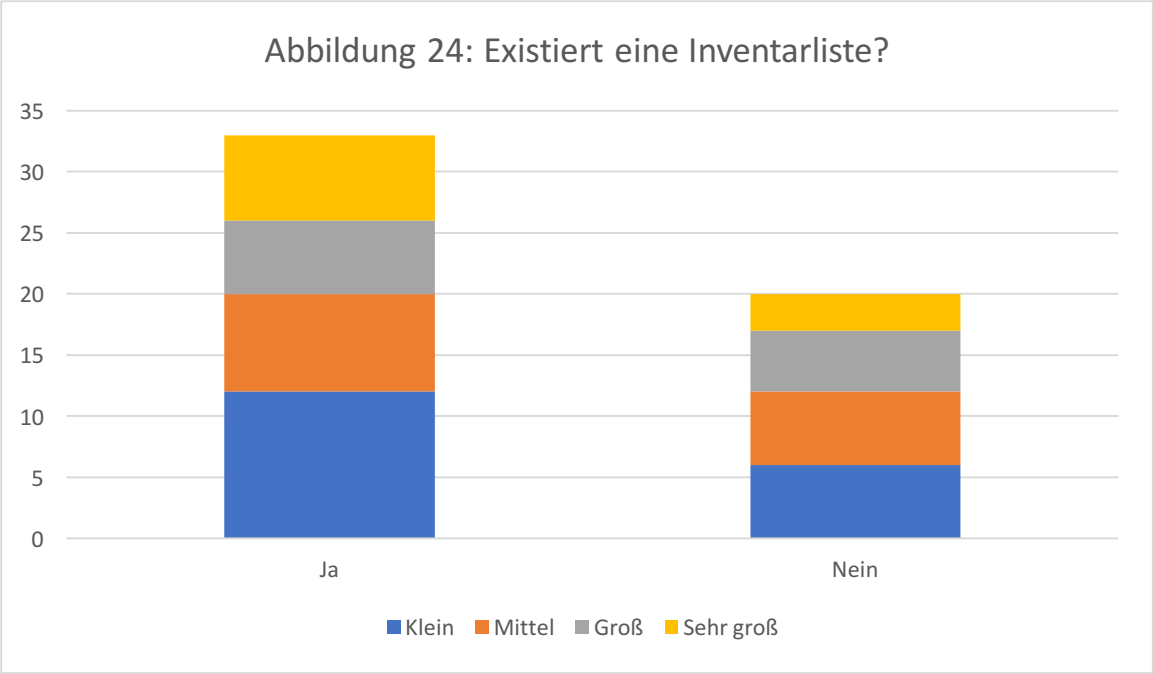


Abbildung 24: Existiert eine aktuelle Inventarliste, in der alle Softwarestände dokumentiert sind (z. B. mit Versionsnummern, zugeordneten Accounts und IP-Adressen)?

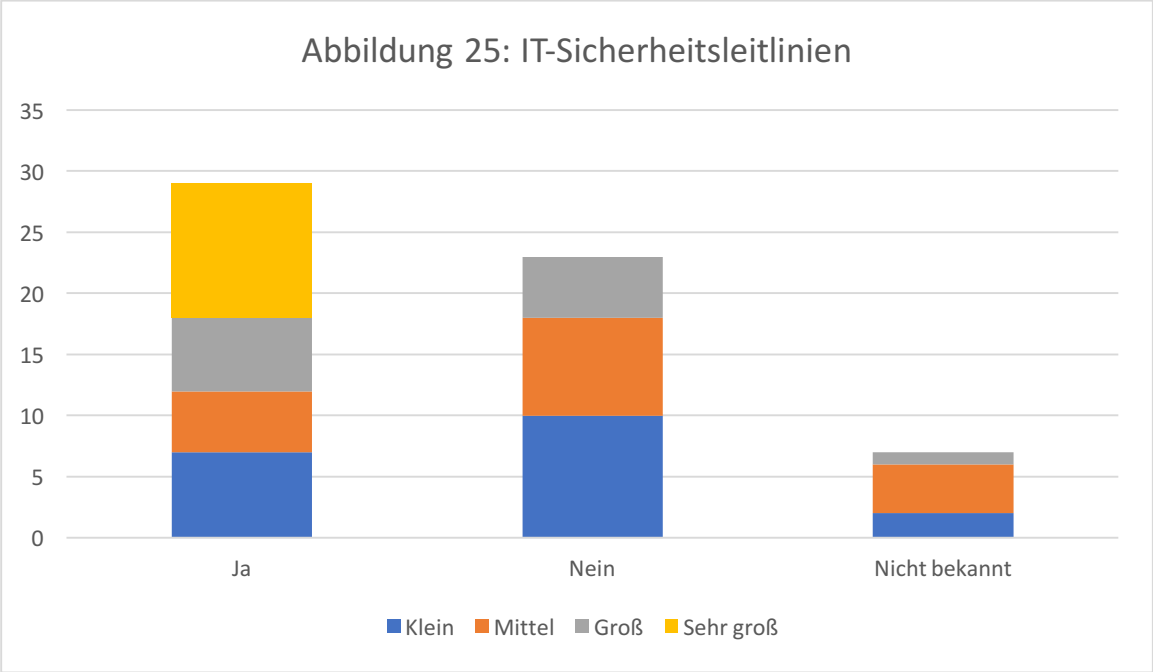


Abbildung 25: Gibt es in Ihrem Unternehmen niedergeschriebene IT-Sicherheitsleitlinien für den Bereich des Leitsystems?

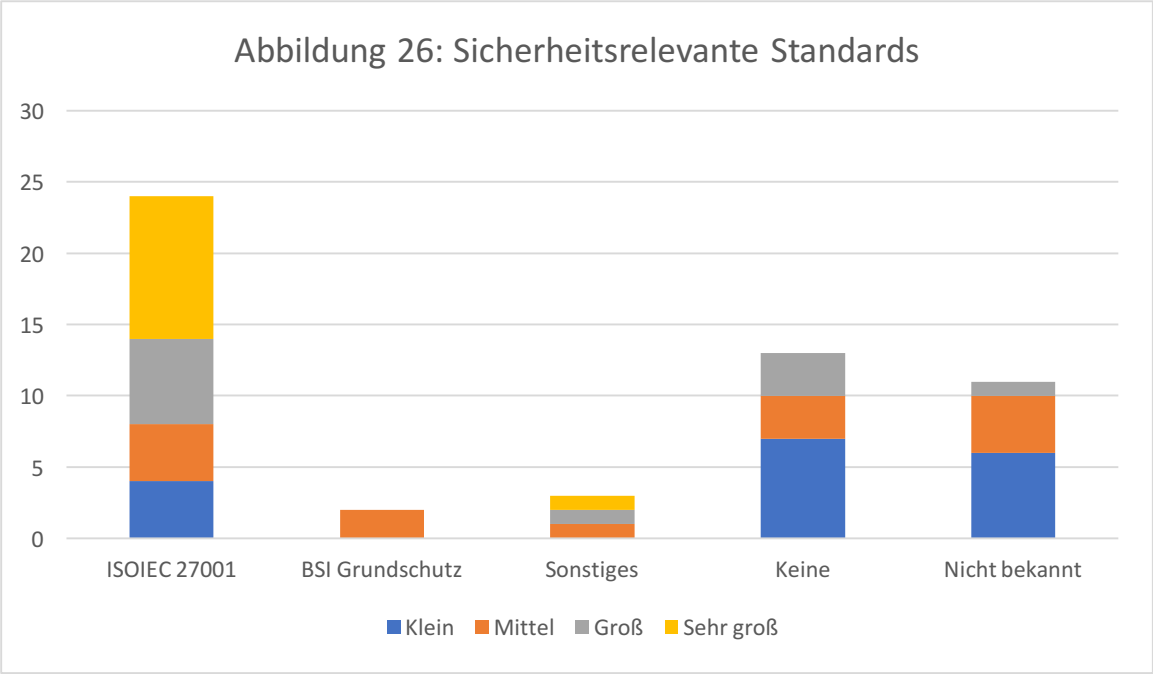


Abbildung 26: Anhand welcher sicherheitsrelevanter Standards sind Ihre IT-Systeme und Prozesse zu Netzsteuerung ausgelegt?

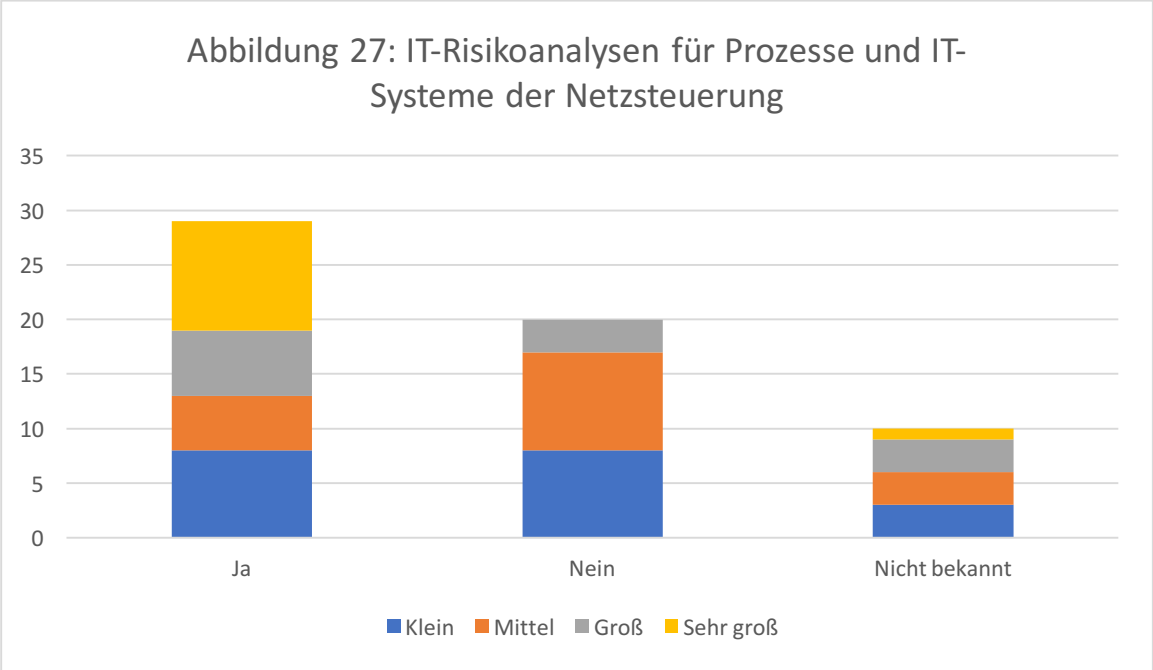


Abbildung 27: Führen Sie IT-Risikoanalysen für die Prozesse und IT-Systeme zur Netzsteuerung durch?

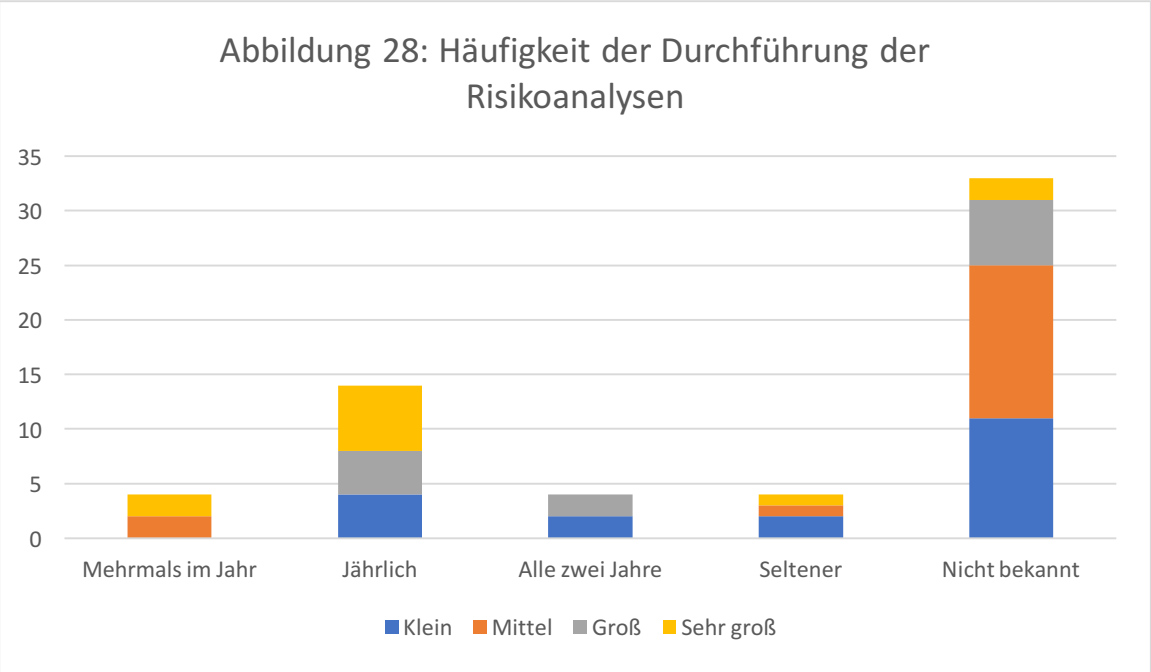


Abbildung 28: Wie regelmäßig führen Sie solche Risikoanalysen durch?

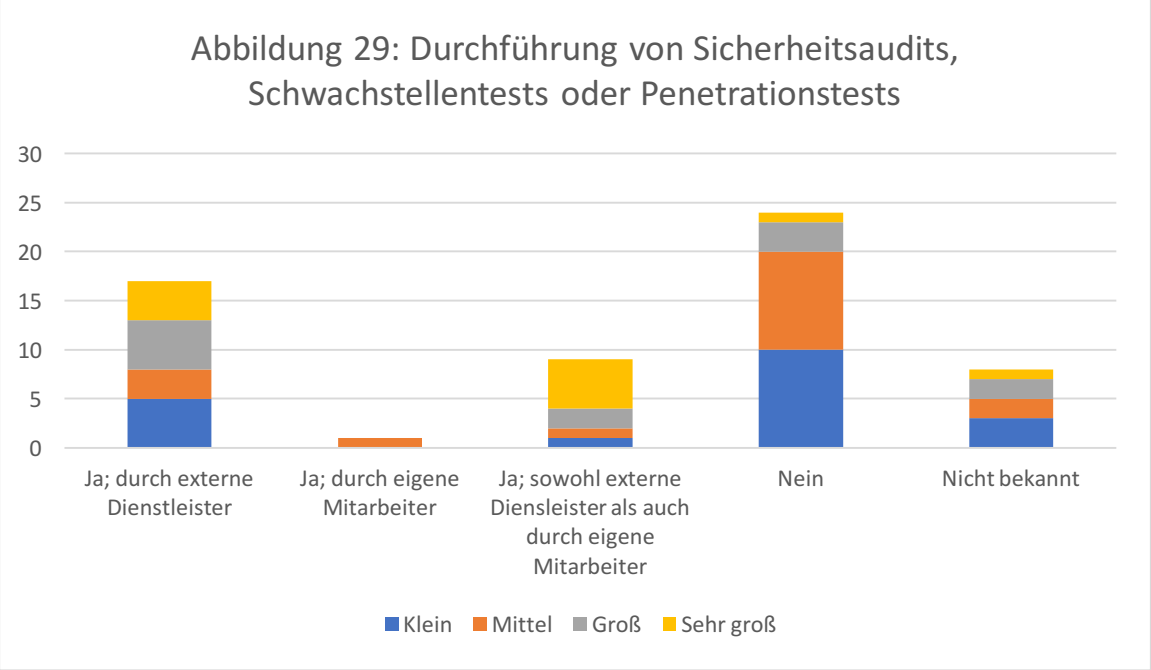


Abbildung 29: Führen Sie Sicherheitsaudits, Schwachstellenscans oder Penetrationstests für die Systeme zur Steuerung der Netzleittechnik durch?

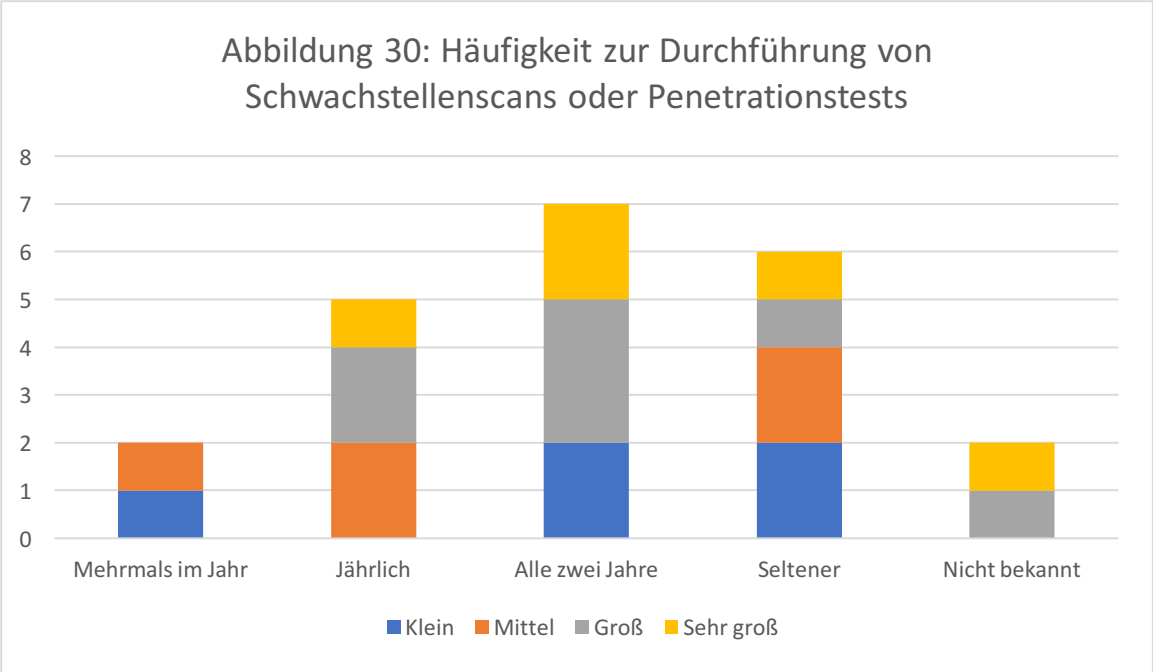


Abbildung 30: Wie häufig führen Sie solche Schwachstellenscans oder Penetrationstests durch?

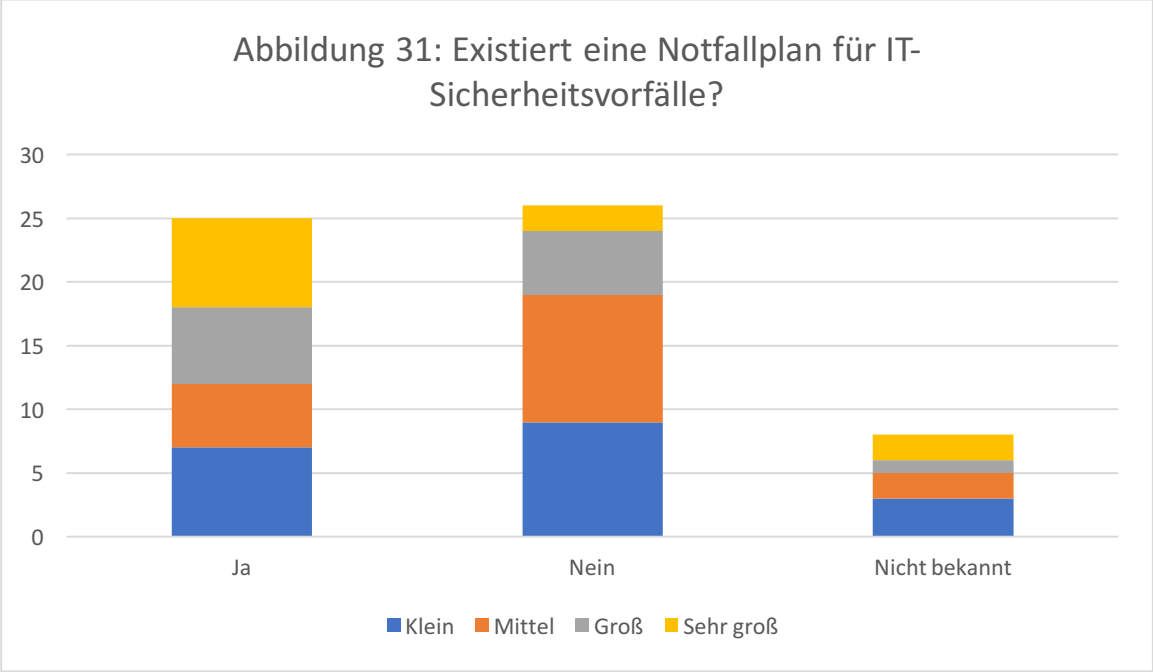


Abbildung 31: Haben Sie einen Notfallplan für IT-Sicherheitsvorfälle die die Netzsteuerung betreffen?

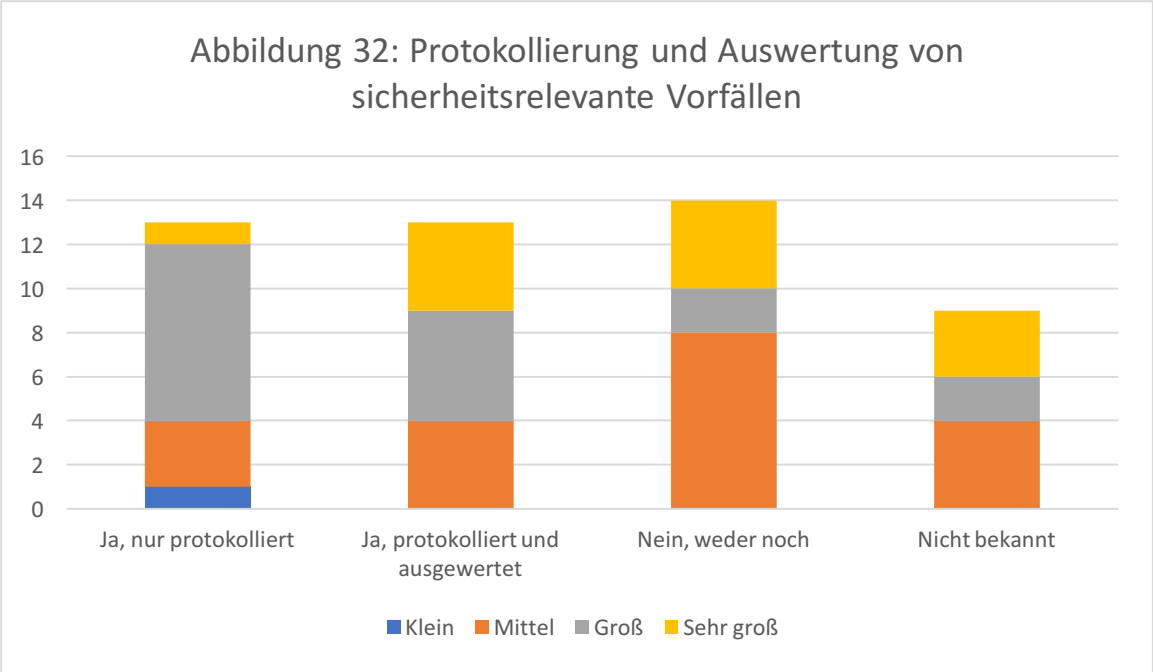


Abbildung 32: Werden sicherheitsrelevante Vorfälle (z. B. Portscans, fehlgeschlagene Anmeldeversuche, nicht autorisierte Vorgänge) protokolliert und ausgewertet?

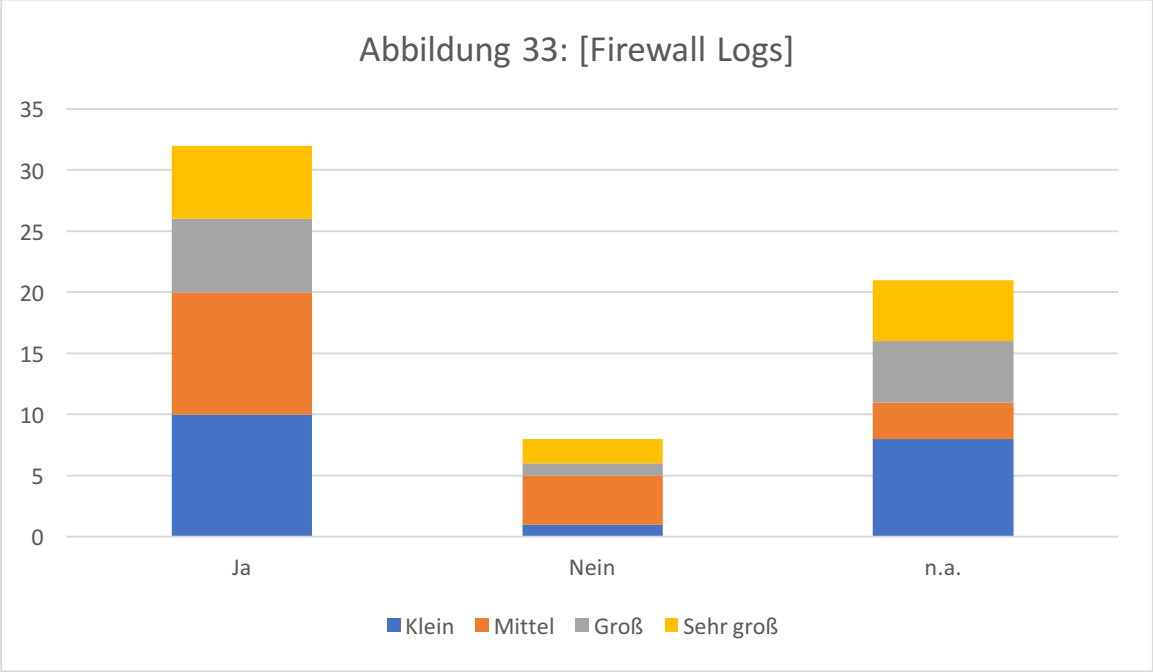


Abbildung 34: [System Logs]

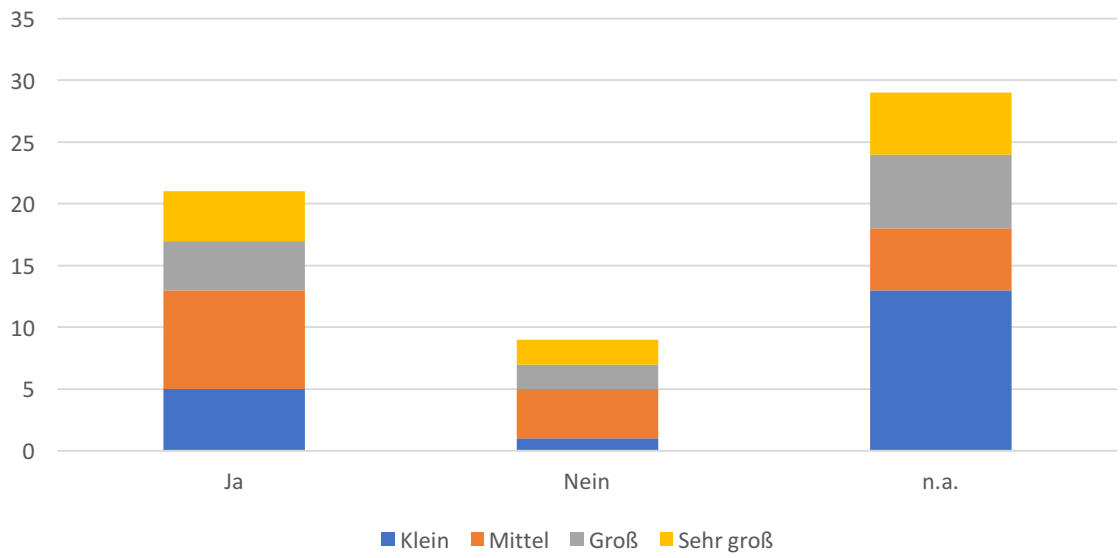
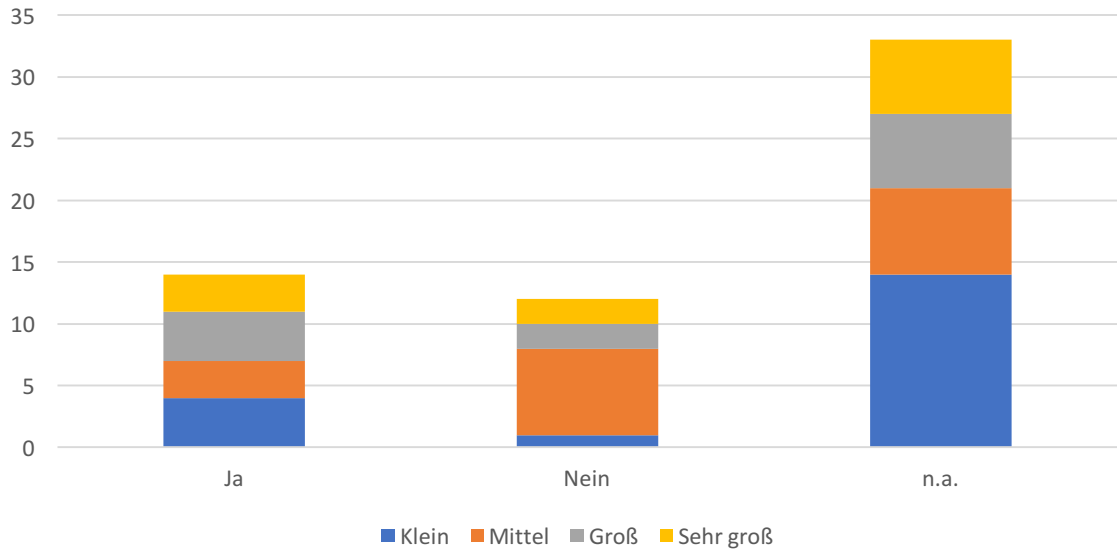


Abbildung 35: [fehlgeschlagene Anmeldungen]



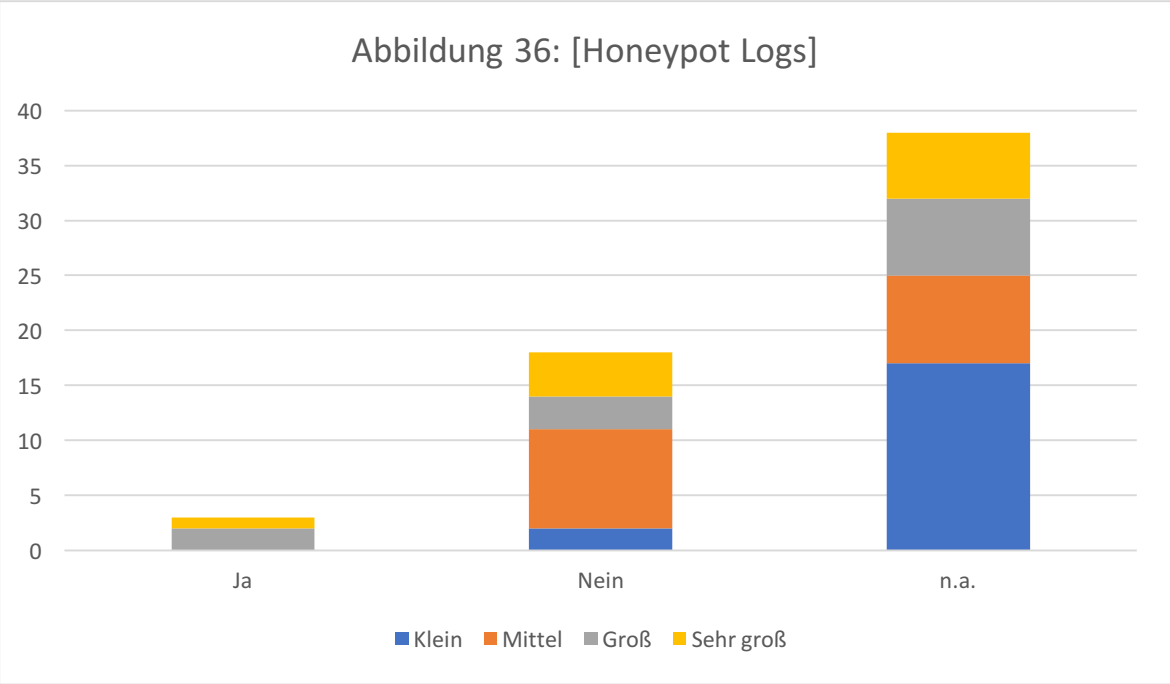


Abbildung 36: [Honeypot Logs]
40
35
30
25
20
15
10
5
0
Ja
Nein
n.a.
Klein
Mittel
Groß
Sehr groß

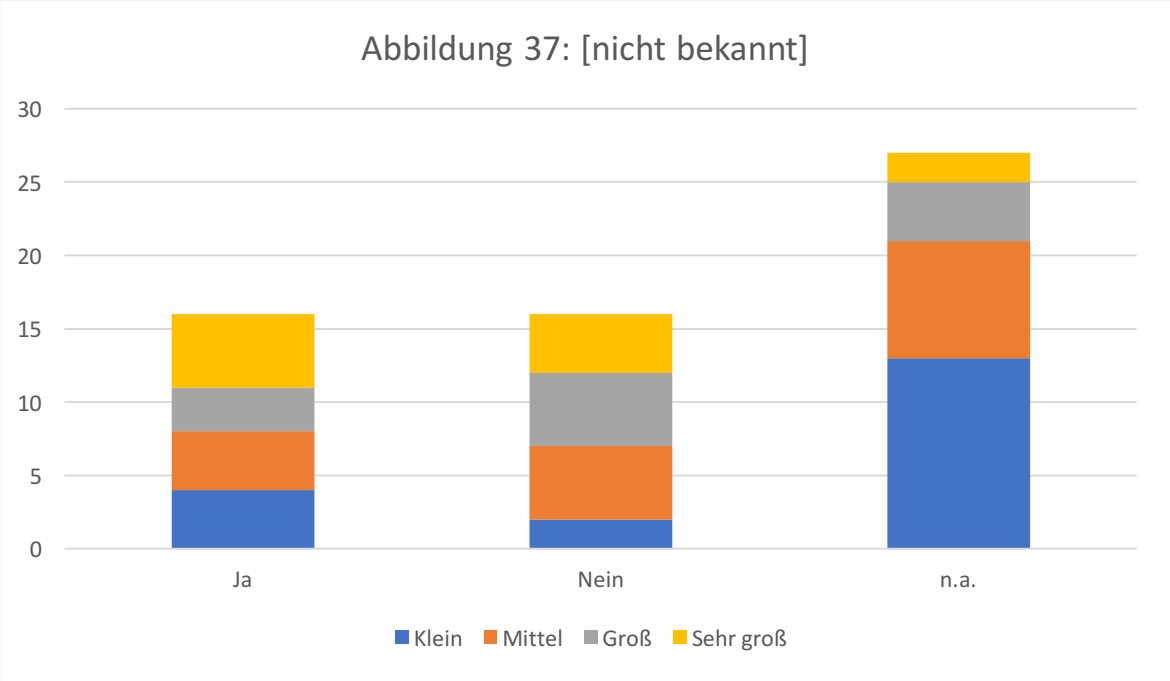


Abbildung 37: [nicht bekannt]
30
25
20
15
10
5
0
Ja
Nein
n.a.
Klein
Mittel
Groß
Sehr groß

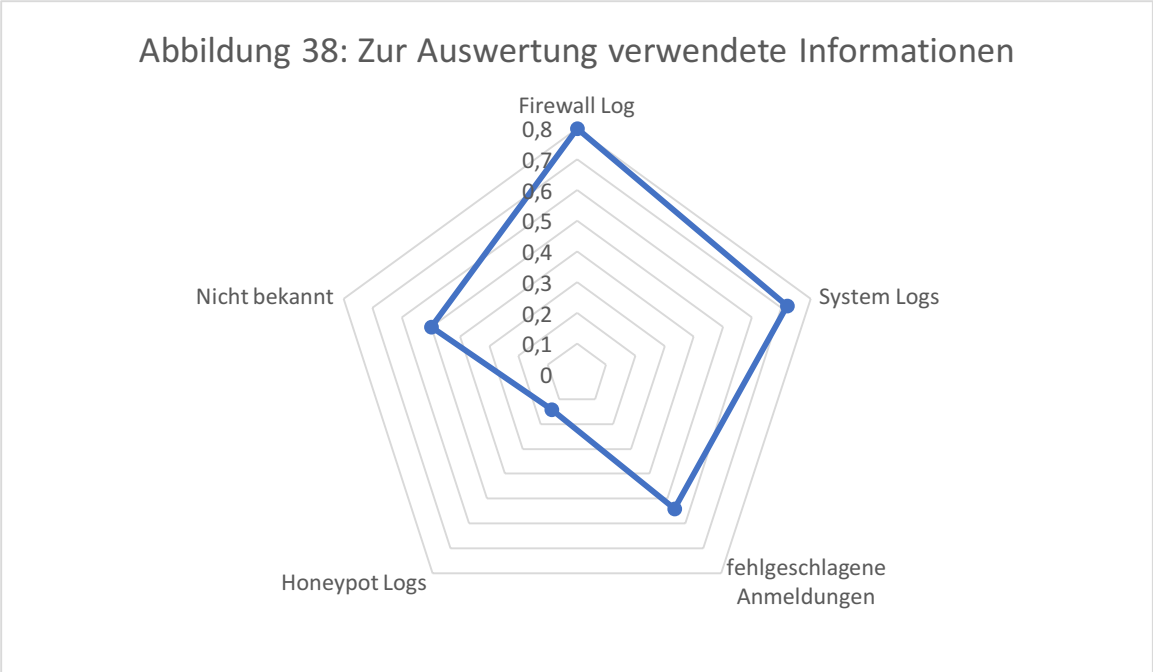


Abbildung 33 bis 38: Welche Informationen werten Sie zur Identifikation von Angriffen auf die IT-Systeme zur Netzsteuerung aus (Mehrfachauswahl möglich)?

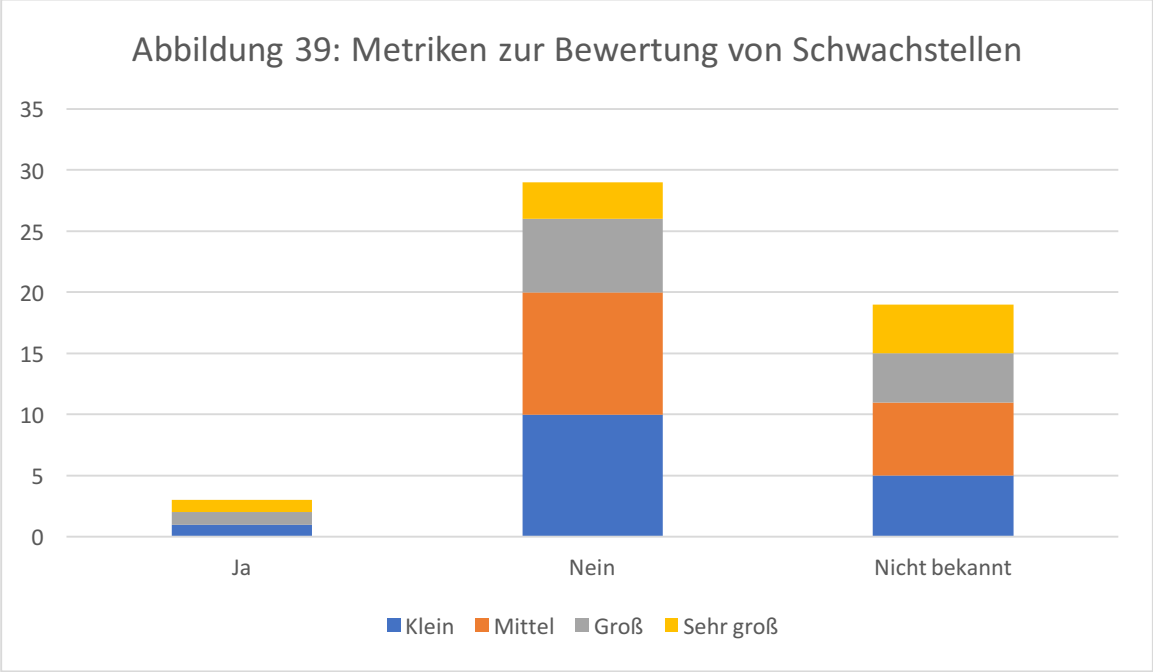


Abbildung 39: Setzen Sie Metriken zur Bewertung von Schwachstellen ein (z. B. CVSS)?

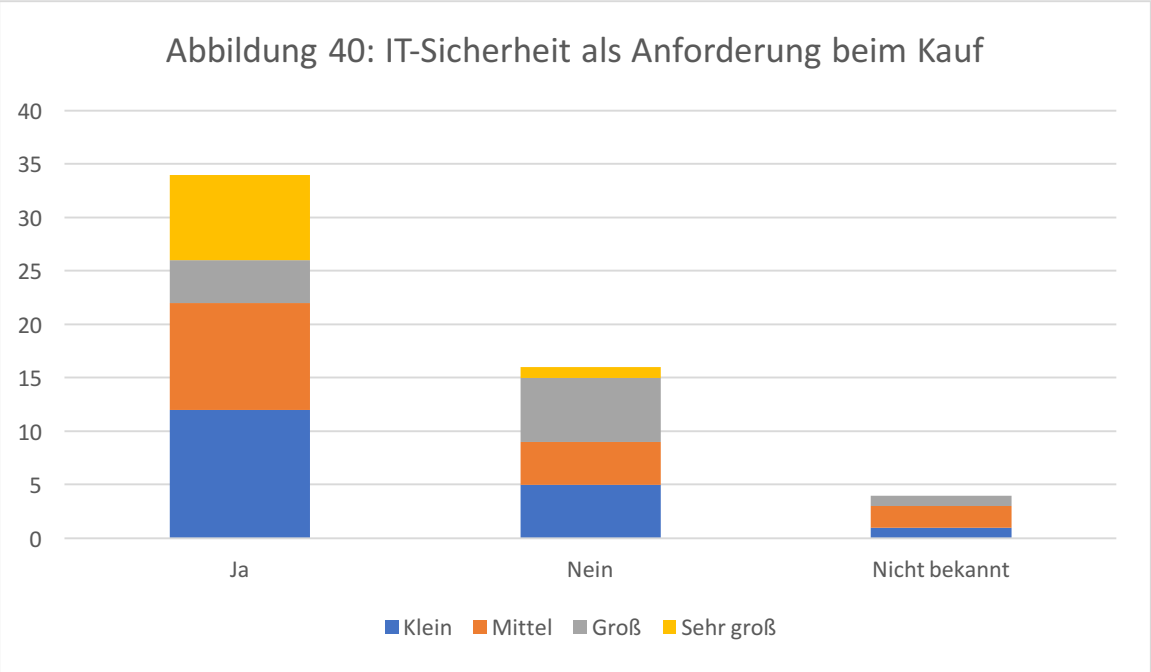


Abbildung 40: Ist IT-Sicherheit als eine Anforderung beim Kauf neuer Hard- und Software definiert?