# ICS Security Umfrage

Torsten Moch, Vasgard Gmbh, Hamburg und Paderborn
Prof. Dr. Achim Schmidtmann, Fachbereich Wirtschaft und Gesundheit, Fachhochschule Bielefeld

Das Ziel dieser Umfrage war es, den aktuellen Stand der ICS Security[1] in Unternehmen aus Ostwestfalen-Lippe (und darüber hinaus) zu ermitteln und diesen IST-Zustand der Unternehmen gegen einen idealen Zustand (abgeleitet aus Anforderungen des BSI - Bundesamt für Sicherheit in der Informationstechnik -) zu spiegeln. Auf Basis der Ergebnisse der Umfrage wurden dann einerseits die Risiken verdeutlicht und andererseits geeignete Sicherheitsmaßnahmen benannt.

Durchgeführt wurde die Umfrage von der Fachhochschule Bielefeld, Professor Dr. Achim Schmidtmann, in Kooperation mit Torsten Moch von der Vasgard GmbH, Hamburg und Paderborn, im Zeitraum vom 15.03.2020 bis 30.04.2020. Sie umfasst 34 Hauptfragen, von denen einige noch in Teilfragen unterteilt sind. 34 Personen haben an der Umfrage teilgenommen, davon haben 25 Personen die Befragung vollständig abgeschlossen.

## Management Summary

Die Umfrage zur ICS Security zeigt ein heterogenes Bild. Obwohl einige Ansatzpunkte bereits in vielen Betrieben umgesetzt wurden, bleiben doch wichtige Felder nicht ausreichend beleuchtet.

Zum Vorgehen: Basierend auf dem ICS-Security-Kompendium des BSI (Bundesamt für Sicherheit in der Informationstechnik) von 2013 wurden wichtige Aspekte zusammengeführt und nach deren Umsetzungsgrad in den Unternehmen gefragt. Hintergrund dieser Vorgehensweise war einerseits der Bezug auf ein bereits seit längerem verfügbares Vorgehensmodell des BSI sowie andererseits die Reduktion der Komplexität, um die Bearbeitungszeit der Fragen in einem vertretbaren Rahmen zu halten.

Die Anzahl der eingegangenen Antworten erlaubt es nicht, den Status der ICS Security umfassend zu beurteilen. Es ergeben sich jedoch Indizien, die Rückschlüsse über zukünftige Schwerpunkte der Informations- und Umsetzungsarbeit zum Thema ICS Security in den Betrieben zulassen.

Zu den erfreulichen Ergebnissen zählt, dass wichtige Elemente der Informationssicherheit wie das Löschen von Daten bei der Entsorgung von IT-Assets, die Durchführung von Datensicherungen oder das Beschränkungen für Zugriffsberechtigungen für wichtige Assets bei der Mehrzahl der Befragten vorhanden sind. Hier zeigt sich, dass Grundlagen der IT-Sicherheit bereichsübergreifend Eingang in den betrieblichen Alltag gefunden haben.

Auf der anderen Seite fehlt es anscheinend an einigen Stellen an strukturierten Vorgehensweisen. So werden zwar Listen der IT-Systeme laufend aktualisiert (81% Zustimmung), doch wurden nur bei 5% der Teilnehmer alle IT-Komponenten in einem Netzplan verzeichnet. Gerade diese Übersicht ist jedoch für das Bewerten von Auswirkungen erkannter Schwachstellen wichtig, ebenso für das Aufstellen und Umsetzen von Notfallplänen. Insofern verwundert es nicht, dass auch letzteres nur von 19% der Antwortenden regelmäßig durchgeführt und angepasst wird.

[1] Industrial Control System (ICS) Security befasst sich mit der IT-Sicherheit in den Bereichen Fabrikautomation und Prozesssteuerung.

Weitere Hinweise für strukturelle Verbesserungspotentiale ergeben sich aus der geringen Verbreitung von Prozessen zu Change- und Patch-Management oder der Kommunikation relevanter Dokumente an die betroffenen Mitarbeiter. Diese Einschätzung deckt sich mit der geringen Verbreitung von Best-Practice-Ansätzen der IT-Sicherheit (ISO 27001, ISO 62443 oder BSI) im Kreis der Teilnehmer.

Zusammenfassend lässt sich festhalten, dass ein gewisser Grad an Bewusstsein für die Herausforderungen der ICS Security vorhanden ist. Jedoch scheint ein systematischer Ansatz zur Umsetzung nur bei einem Teil der Antwortenden eine Rolle zu spielen. Hier wäre die Anpassung vorhandener Best-Practice-Ansätze in ein stufenweises Vorgehen (Reifegradmodell) eine Möglichkeit, Unternehmen einen angepassten Einstieg in die ICS-Security zu bieten.

## Ausgewählte Ergebnisse - Tops und Flops

In dieser Rubrik werden diejenigen Ergebnisse kurz vorgestellt, die den Autoren der Untersuchung besonders positiv oder negativ aufgefallen sind, beginnend mit den positiven. Sortiert sind die Ergebnisse nach den Ergebniswerten und nicht nach der Reihenfolge in der Umfrage. Die Einordnung in die Umfrage kann den folgenden Grafiken entnommen werden.

### Positive Resultate

- Die deutliche Mehrheit der Befragten (ca. 81%) aktualisiert die Liste ihrer IT-Systeme ständig.
- 80% der Befragten führen Datensicherungen regelmäßig und in kurzen Abständen durch.
- Fast 75% der teilnehmenden Unternehmen achten bei der Entsorgung von Hardware neben den Umweltanforderungen auch darauf, dass keine vertraulichen Informationen mehr auf dieser gespeichert sind
- Über zwei Drittel (68%) der Befragten haben Virenschutzprogramme, bzw. nach einer Risikoabschätzung eine alternative Maßnahme zum Schutz der Assets, installiert.
- Fast zwei Drittel (ca. 63%) der befragten Unternehmen haben sichergestellt, dass nur berechtige Personen Zugang zu gesicherten Bereichen haben und dass dieses auch protokolliert wird.
- Die Mehrheit (ca. 63%) hat ihre Berichtslinie an das oberste Management festgelegt.
- Ebenfalls die Mehrheit der Unternehmen (ca. 61%) hat Anlagen- und Komponentenverantwortliche benannt.
- 60% der Befragten haben eine Passwortrichtlinie implementiert.
- Ebenfalls 60% der Teilnehmer vergeben Zugriffsrechte restriktiv.

## Negative Resultate

- Nur ca. 5% aller Teilnehmer haben alle ICS-Komponenten in einem Netzplan verzeichnet.
- Ca. 15% aller Teilnehmer steuern Änderungen in der ICS-Umgebung durch einen gesonderten Prozess mit (Funktions-) Rollentrennung.
- Bescheidene 17% bewerten die Kritikalität von Patches zum Beispiel anhand des Common Vulnerability Scoring System (CVSS).
- Bei ca. 19% der Befragten sind alle wesentlichen Dokumente aktuell und nur für die beteiligten Mitarbeiter verfügbar sind.
- Ebenfalls bei etwa 19% werden sicherheitsrelevante Ereignisse permanent beobachtet und bei Bedarf zeitnah Gegenmaßnahmen auf Basis eines Security Incident Response Plan eingeleitet.
- Weitere 19% testen ihre Notfall- und Wiederanlaufpläne regelmäßig und passen sie an.
- Ein Fünftel (20%) aller Befragten haben einen standardisierten Patchmanagement Prozess eingeführt.
- Bei etwa einem Viertel der Teilnehmer (24%) wird nicht benötigte Hardware deaktiviert oder entfernt. Bei 32% passiert dieses nicht und ist auch nicht geplant und 8% haben keine Angabe gemacht.
- Genauso verhält es sich mit Quarantäne-PCs zum Test von mobilen Datenträgern. Fast ein Viertel (24%) der Teilnehmer hat diese im Einsatz. Bei 32% passiert dieses nicht und ist auch nicht geplant und 8% haben keine Angabe gemacht.

## Klassifikation der Ergebnisse

Ein Ziel dieser Umfrage war der Wunsch, den Verbreitungsgrad einiger Aspekte der Informationssicherheit im Kreis der Antwortenden zu ermitteln. Diese Aspekte sind in 5 Themenbereichen mit 21 Fragen und 40 Teilfragen abgebildet. Um hierbei einen Überblick zu erhalten, wurden die prozentualen Anteile der Antwortklassen „Umgesetzt“ und „Fast umgesetzt“ addiert. Sobald die Summe bestimmte Schwellwerte überschritten hat, wurde eine Einschätzung der jeweiligen Verbreitung des Informationssicherheits-Vorgehens vorgenommen. Folgende Gruppen wurden gebildet und mit einem entsprechenden Reifegrad versehen:

- > 80 % Hoher Reifegrad
- > 60%: Mittlerer Reifegrad
- > 40%: Niedriger Reifegrad
- < 40%: Kritischer Reifegrad

| Vollständig/ fast vollständig | Farbcodierung | Anzahl | Anteil |
|---|---|---|---|
| >80% | | 7 | 17,5 % |
| >60% | | 17 | 42,5 % |
| >40% | | 9 | 22,5 % |
| <40% | | 7 | 17,5 % |
| | | 40 | 100% |

Aus der Übersicht lässt sich ablesen, dass nur wenige Ansatzpunkte bereits bei einem Großteil der Teilnehmer umgesetzt worden sind. Dies ist vor dem Hintergrund, dass das ausgewählte Modell des BSI zum Thema ICS bereits seit mehreren Jahren propagiert wird, ein nicht zufriedenstellendes Ergebnis.

Weitergehende Einschätzungen hierzu wurden in den Kapiteln „Management Summary“ und „Tops und Flops“ festgehalten.

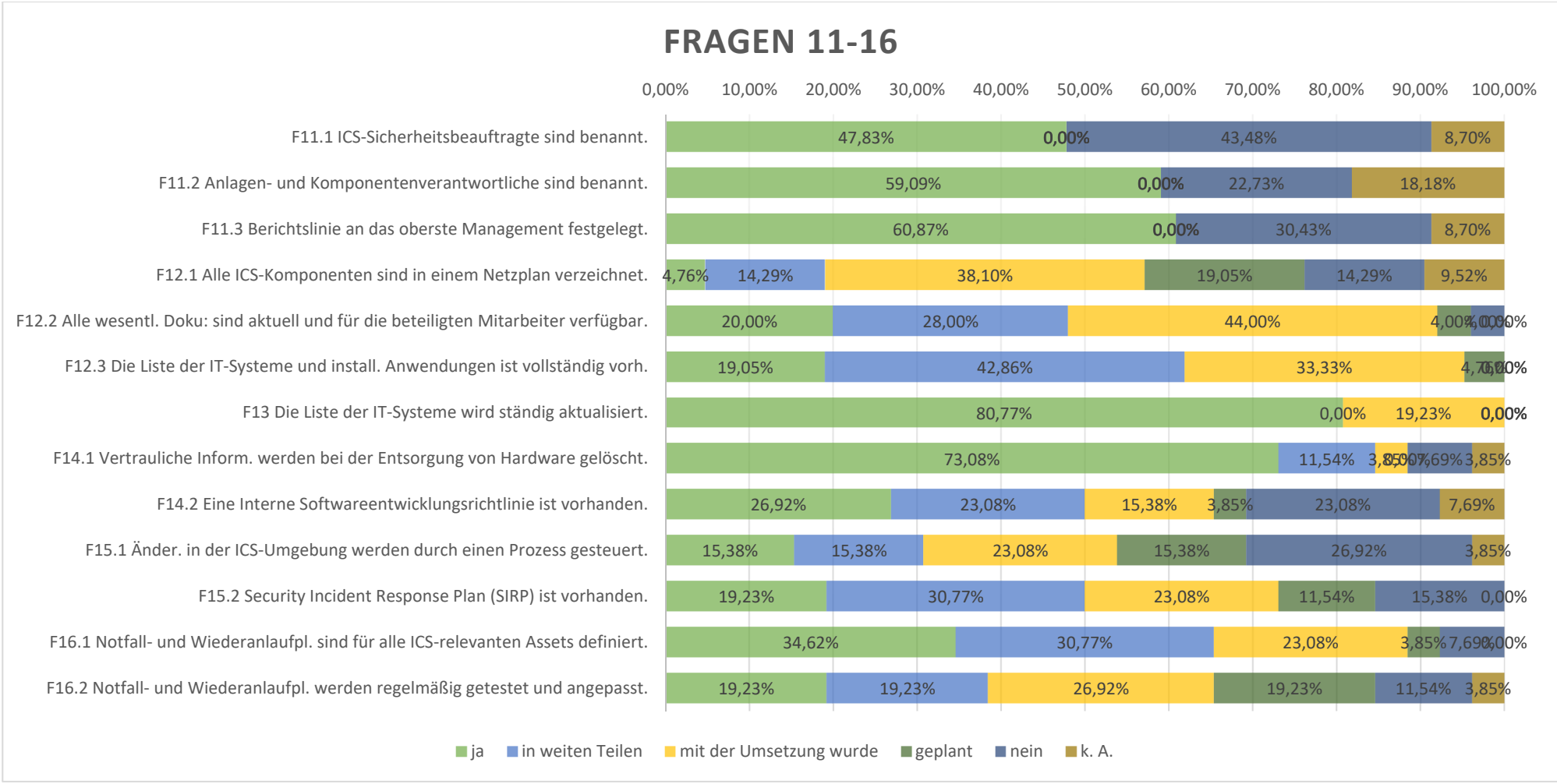
Auf den folgenden zwei Seiten finden Sie die Einordnung aller 40 Teilfragen in diese vier Reifegradkategorien. Die Farbcodierung findet im Rahmen der Darstellung der vollständigen Ergebnisse ab Seite 10 dann erneut Verwendung.

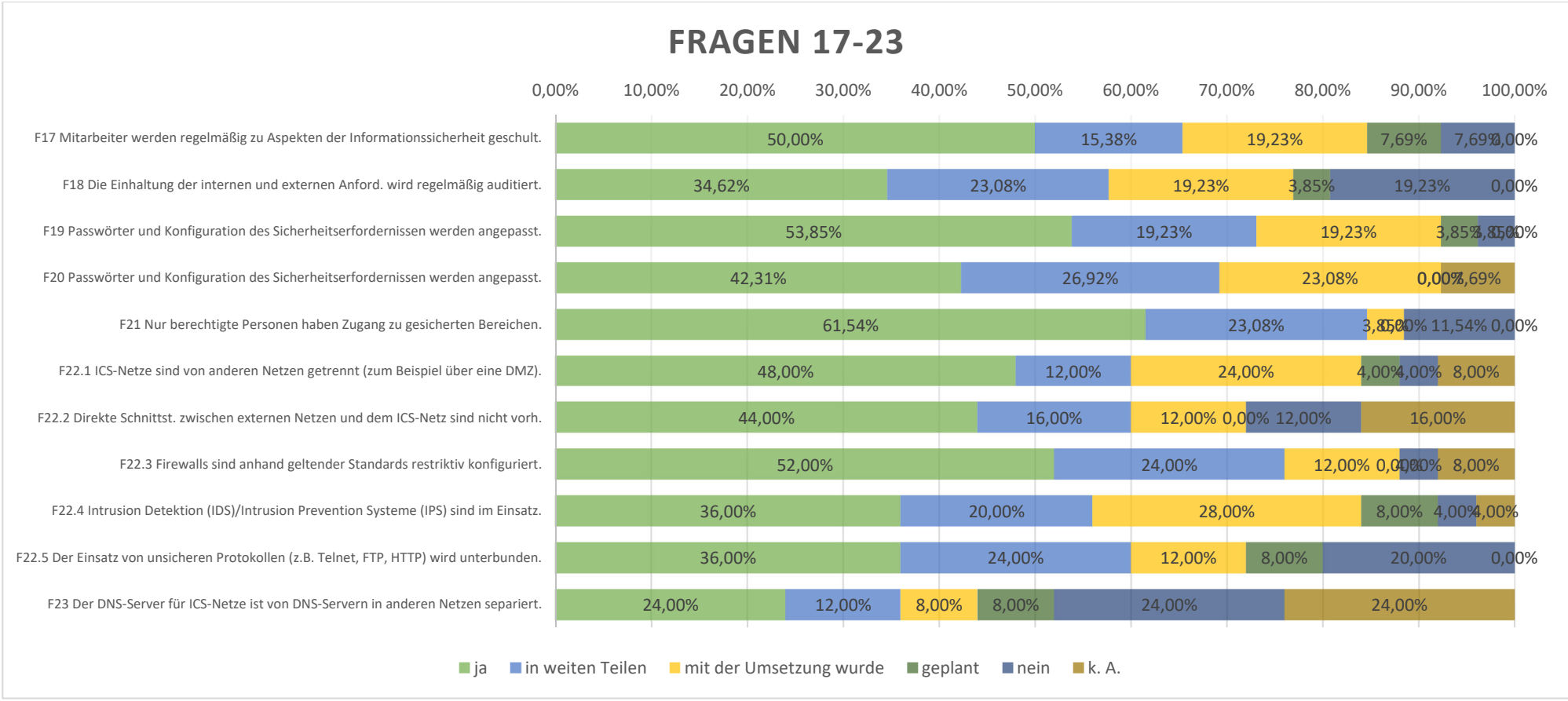
## Übersicht alle Fragen mit der Klassifikation der Ergebnisse

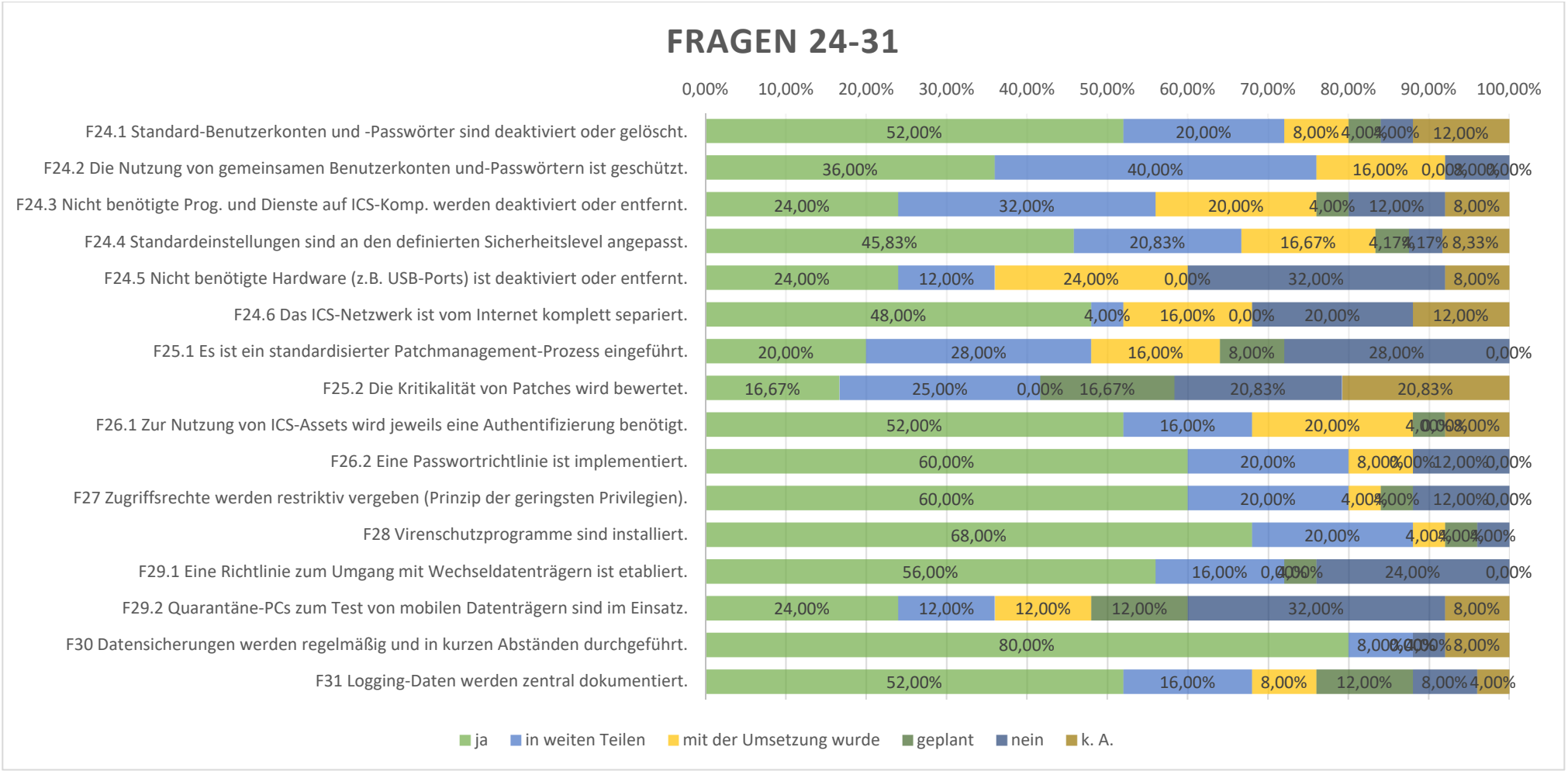
| Themenbereiche | Fragen | Teilfragen | Bewertung |
|---|---|---|---|
| Einstieg ins Security Thema | F11: Für das Thema ICS sind klare Verantwortlichkeiten geschaffen | ICS-Beauftragte benannt | |
| | | Anlagen-/Komponenten-Beauftragte benannt | |
| | | Direkte Berichtslinie an GF | |
| | F12: Abfrage grundlegender Strukturen und Dokumentationen | Netzplan | |
| | | Manuals | |
| | | Assetliste | |
| | F13: Die Liste der IT-Systeme wird ständig aktualisiert | Die Liste der IT-Systeme wird ständig aktualisiert | |
| Security-spezifische Prozesse und Richtlinien | F14: Security Management - Entsorgung von Hardware | Löschung von Daten vor der Entsorgung | |
| | | SW-Entwicklungsrichtlinie liegt vor | |
| | F15: Durchgängiges Management aller ICS-Komponenten - Security Monitoring | ChangeMgmt | |
| | | SIRP | |
| | F16: Notfallmanagement - Wiederherstellungsplan (Business Continuity Plan) für die schützenswerten Assets | Notfallpläne vorhanden | |
| | | Notfallpläne getestet | |
| | F17: Personal | Prozesse für Einstellung, Wechsel und Ausscheiden von Personal | |
| | F18: Revision & Tests - Komponentenprüfung | Revision & Tests - Komponentenprüfung | |
| Auswahl der verwendeten Systeme u. Komponenten sowie der eingesetzten Dienstleister u. Integratoren | F19: Inbetriebnahme in sicherer Konfiguration | Aktivierte Sicherheitsmechanismen und aktueller Patchstand | |
| | F20: Fernwartung durch Hersteller und Integrator - Sichere Fernwartung | Fernwartung durch Hersteller und Integrator - Sichere Fernwartung | |
| Bauliche und physische Absicherung | F21: Physische Absicherung (Zutritt) | Physische Absicherung (Zutritt) | |

| Themenbereiche | Fragen | Teilfragen | Bewertung |
|---|---|---|---|
| Technische Maßnahmen | F22: Absicherung der Netze - Nutzung von sicheren Protokollen (DMZ/Firewall/IDS) | DMZ vorhanden | |
| | | Keine Interfaces ICS und externen Netzen | |
| | | Restriktive Firewall-Regeln | |
| | | IDS/IPS im Einsatz | |
| | | FTP/HTTP unterbunden | |
| | F23: Absicherung von Diensten und Protokollen – Zeitsynchronisierung | DNS-Server separiert | |
| | F24: Härtung der IT-Systeme - Zugriff auf das Internet innerhalb des ICS-Netzwerk | Standardpassword und -konten gelöscht | |
| | | Maßnahmen bezüglich gemeinsamer Password | |
| | | Nicht benötigte Programme auf ICS gelöscht | |
| | | Standardeinstellungen an Sicherheitslevel angepasst | |
| | | Nicht benötigte HW (z.B. Ports) deaktiviert | |
| | | ICS-Netzwerk vom Intranet separiert | |
| | F25: Patchmanagement - Umgang mit End Of Support (EOS) | Standardisierter Patchmanagement-Prozess | |
| | | Bewertung der Kritikalität von Patches | |
| | F26: Authentisierung - Vermeidung von Missbrauch | Authentifizierung zur Nutzung des Assets | |
| | | Password-Richtlinien implementiert | |
| | F27: Zugriffskontrolle | Least privilege | |
| | F28: Schutz vor Schadprogrammen - Installation und Betrieb von Virenschutzprogrammen | Virenschutzprogramme o.ä. installiert | |
| | F29: Mobile Datenträger - Umgang mit Wechseldatenträgern | Richtlinie zu Wechseldatenträgern | |
| | | Quarantäne-PC vorhanden | |
| | F30: Datensicherung - Datensicherungen der Systeme | Regelmäßige Datensicherungen | |
| | F31: Protokollierung und Auswertung - Logging / Monitoring | Logging-Daten zentral dokumentiert | |

Die folgenden drei Grafiken zeigen die genaue Antwortverteilung der 40 Teilfragen.




FRAGEN 17-23
0,00% 10,00% 20,00% 30,00% 40,00% 50,00% 60,00% 70,00% 80,00% 90,00% 100,00%
F17 Mitarbeiter werden regelmäßig zu Aspekten der Informationssicherheit geschult.
50,00% 15,38% 19,23% 7,69% 7,69% 0,00%
F18 Die Einhaltung der internen und externen Anford. wird regelmäßig auditiert.
34,62% 23,08% 19,23% 3,85% 19,23% 0,00%
F19 Passwörter und Konfiguration des Sicherheitserfordernissen werden angepasst.
53,85% 19,23% 19,23% 3,85% 3,85% 0,00%
F20 Passwörter und Konfiguration des Sicherheitserfordernissen werden angepasst.
42,31% 26,92% 23,08% 0,00% 7,69%
F21 Nur berechtigte Personen haben Zugang zu gesicherten Bereichen.
61,54% 23,08% 3,85% 0,00% 11,54% 0,00%
F22.1 ICS-Netze sind von anderen Netzen getrennt (zum Beispiel über eine DMZ).
48,00% 12,00% 24,00% 4,00% 4,00% 8,00%
F22.2 Direkte Schnittst. zwischen externen Netzen und dem ICS-Netz sind nicht vorh.
44,00% 16,00% 12,00% 0,00% 12,00% 16,00%
F22.3 Firewalls sind anhand geltender Standards restriktiv konfiguriert.
52,00% 24,00% 12,00% 0,00% 4,00% 8,00%
F22.4 Intrusion Detektion (IDS)/Intrusion Prevention Systeme (IPS) sind im Einsatz.
36,00% 20,00% 28,00% 8,00% 4,00% 4,00%
F22.5 Der Einsatz von unsicheren Protokollen (z.B. Telnet, FTP, HTTP) wird unterbunden.
36,00% 24,00% 12,00% 8,00% 20,00% 0,00%
F23 Der DNS-Server für ICS-Netze ist von DNS-Servern in anderen Netzen separiert.
24,00% 12,00% 8,00% 8,00% 24,00% 24,00%
ja
in weiten Teilen
mit der Umsetzung wurde
geplant
nein
k. A.

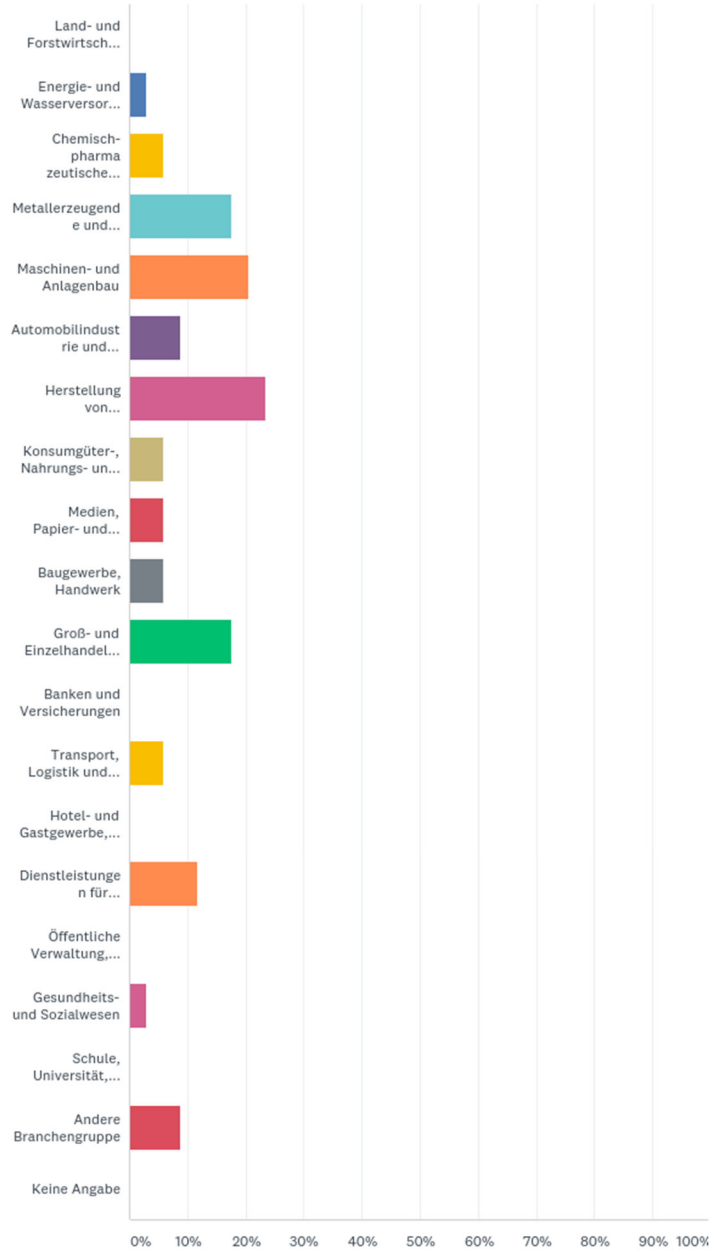

FRAGEN 24-31
0,00% 10,00% 20,00% 30,00% 40,00% 50,00% 60,00% 70,00% 80,00% 90,00% 100,00%
F24.1 Standard-Benutzerkonten und -Passwörter sind deaktiviert oder gelöscht.
F24.2 Die Nutzung von gemeinsamen Benutzerkonten und-Passwörtern ist geschützt.
F24.3 Nicht benötigte Prog. und Dienste auf ICS-Komp. werden deaktiviert oder entfernt.
F24.4 Standardeinstellungen sind an den definierten Sicherheitslevel angepasst.
F24.5 Nicht benötigte Hardware (z.B. USB-Ports) ist deaktiviert oder entfernt.
F24.6 Das ICS-Netzwerk ist vom Internet komplett separiert.
F25.1 Es ist ein standardisierter Patchmanagement-Prozess eingeführt.
F25.2 Die Kritikalität von Patches wird bewertet.
F26.1 Zur Nutzung von ICS-Assets wird jeweils eine Authentifizierung benötigt.
F26.2 Eine Passwortrichtlinie ist implementiert.
F27 Zugriffsrechte werden restriktiv vergeben (Prinzip der geringsten Privilegien).
F28 Virenschutzprogramme sind installiert.
F29.1 Eine Richtlinie zum Umgang mit Wechseldatenträgern ist etabliert.
F29.2 Quarantäne-PCs zum Test von mobilen Datenträgern sind im Einsatz.
F30 Datensicherungen werden regelmäßig und in kurzen Abständen durchgeführt.
F31 Logging-Daten werden zentral dokumentiert.
ja
in weiten Teilen
mit der Umsetzung wurde
geplant
nein
k. A.

# Vollständige Ergebnisse

Dieser Abschnitt stellt die vollständigen Ergebnisse der Umfrage entsprechend der dortigen Reihenfolge grafisch oder tabellarisch dar. Zu jeder Grafik oder Tabelle folgt ein kurzer Text, der auf die zentralen Punkte der jeweiligen Beantwortungen eingeht. Hier werden nun auch die einleitenden Fragen zu Demographie und Unternehmen, die bisher noch nicht näher betrachtet wurden, mit ihren Ergebnissen dargestellt. Aufgrund der relativ geringen Teilnehmerzahl konnten auf Basis dieser Daten aber keine Querbezüge zu den Fragen aus den Security Themenbereichen

## Demographie und Unternehmen

F1: In welchen der folgenden Branchen ist ihr Unternehmen tätig? (Mehrfachnennungen möglich)



| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| Herstellung von elektrotechnischen Gütern, IT-Industrie | 23.53% | 8 |
| Maschinen- und Anlagenbau | 20.59% | 7 |
| Metallerzeugende und -verarbeitende Industrie | 17.65% | 6 |
| Groß- und Einzelhandel (inkl. Online-Handel) | 17.65% | 6 |
| Dienstleistungen für Unternehmen | 11.76% | 4 |
| Automobilindustrie und Zulieferer | 8.82% | 3 |
| Andere Branchengruppe | 8.82% | 3 |
| Chemisch-pharmazeutische Industrie, Life-Science | 5.88% | 2 |
| Konsumgüter-, Nahrungs- und Genussmittelindustrie | 5.88% | 2 |
| Medien, Papier- und Druckgewerbe | 5.88% | 2 |
| Baugewerbe, Handwerk | 5.88% | 2 |
| Transport, Logistik und Verkehr | 5.88% | 2 |
| Energie- und Wasserversorgung | 2.94% | 1 |
| Gesundheits- und Sozialwesen | 2.94% | 1 |
| Land- und Forstwirtschaft, Fischerei, Bergbau | 0.00% | 0 |
| Banken und Versicherungen | 0.00% | 0 |
| Hotel- und Gastgewerbe, Tourismus | 0.00% | 0 |
| Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherung | 0.00% | 0 |
| Schule, Universität, Hochschule | 0.00% | 0 |
| Keine Angabe | 0.00% | 0 |
| Befragte insgesamt: 34 | | |

Fast ein Viertel der Teilnehmer (ca. 24%) hat u.a. als Branche Herstellung von elektrotechnischen Gütern, IT-Industrie angegeben. Als zweithäufigste Branche folgt der Maschinen- und Anlagenbau mit ca. 21%. Die Metallerzeugende und -verarbeitende Industrie und der Groß- und Einzelhandel (inkl. Online-Handel) kommen beide auf ca. 18%.

**F2: Befindet sich der Hauptsitz ihres Unternehmens im Bereich Ostwestfalen-Lippe?**

| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| Ja | 64.71% | 22 |
| Nein | 35.29% | 12 |
| GESAMT | | 34 |

Mehr als zwei Drittel (ca. 65%) der Unternehmen haben angegeben, dass sich ihr Hauptsitz in Ostwestfalen Lippe befindet.

**F4: Wie viele Beschäftigte sind in Ihrem Unternehmen tätig?**

| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| 1 - 50 Beschäftigte | 6.06% | 2 |
| 51 - 100 Beschäftigte | 6.06% | 2 |
| 101 - 500 Beschäftigte | 6.06% | 2 |
| 501 - 1000 Beschäftigte | 24.24% | 8 |
| 1.001 - 5000 Beschäftige | 27.27% | 9 |
| 5001 - 10000 Beschäftigte | 15.15% | 5 |
| 10.001 Beschäftigte und mehr | 15.15% | 5 |
| Keine Angabe | 0.00% | 0 |
| Befragte insgesamt: 33 | | |

Etwas über ein Viertel der Befragten *(noch 33 gesamt)* (ca. 27%) hat angegeben, zwischen 1001 und 5000 Mitarbeiter zu beschäftigen. Ein knappes weiteres Viertel (ca. 24%) gab an über 501 bis 1000 Beschäftige zu verfügen. Jeweils weitere 15% gaben an zwischen 5001 – 10000 und mehr als 10001 Mitarbeiter zu beschäftigen. Die Beschäftigenzahlen der restlichen Unternehmen teilen sich gleichmäßig auf die weiteren Optionen auf.

**F5: Wie viele Mitarbeiter arbeiten in Ihrer IT (incl. ICS-IT)?**

| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| 1 - 10 | 18.18% | 6 |
| 11 – 50 IT-Mitarbeiter | 42.42% | 14 |
| 51 - 100 IT-Mitarbeiter | 9.09% | 3 |
| 101 – 500 IT-Mitarbeiter | 18.18% | 6 |
| 501 IT-Mitarbeiter und mehr | 9.09% | 3 |
| Keine Angabe | 3.03% | 1 |
| Befragte insgesamt: 33 | | |

Die häufigste Angabe (mit ca. 42% bei 33 Antworten) war eine Mitarbeiterzahl in der IT von 11 bis 50 Personen. Am zweithäufigsten gaben die Befragten mit jeweils 18% eine Anzahl von 1 bis 10 und 101 bis 500 IT-Mitarbeitern an. Ein Unternehmen hat hierzu keine Angabe gegeben. Die restlichen Antworten teilen sich gleichmäßig auf.

**F6: Arbeiten Sie selbst in der IT (incl. ICS-IT) Ihres Unternehmens?**

| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| Ja | 87.88% | 29 |
| Nein | 12.12% | 4 |
| Befragte insgesamt: 33 | | |

Ein Großteil (ca. 88%) hat angegeben selbst in der IT ihres Unternehmens zu arbeiten.

**F7: Welche dieser Hierarchiepositionen trifft am ehesten auf Ihre Rolle zu?**

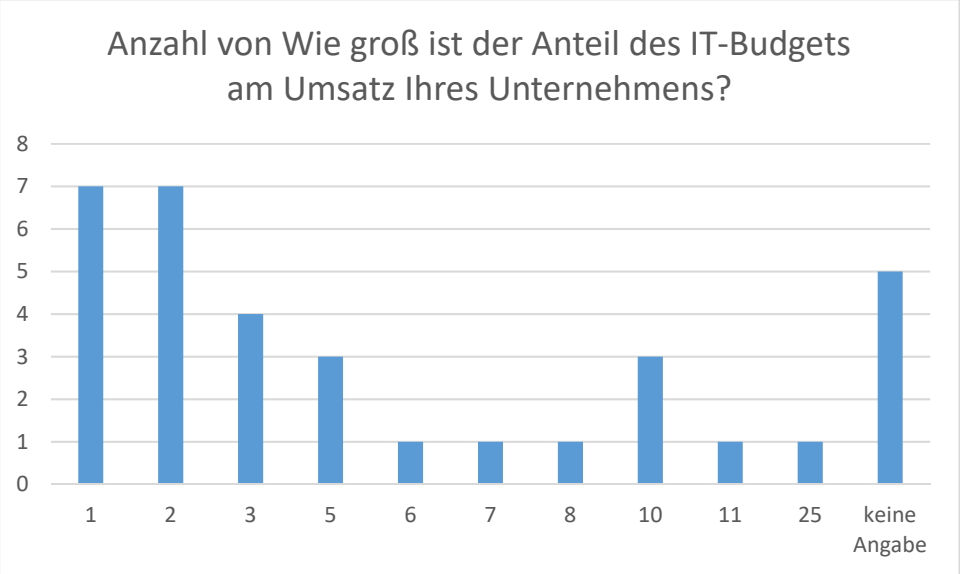
| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| Top Level Management | 26.47% | 9 |
| Mittleres Management | 44.12% | 15 |
| 1. Führungsebene | 17.65% | 6 |
| Operative Ebene | 20.59% | 7 |
| Befragte insgesamt: 34 | | |

Beinahe die Hälfte (ca. 44% bei insgesamt 34 Antworten) der Unternehmen hat angegeben, sich selbst am ehesten dem mittleren Management zuzuordnen. Am zweithäufigsten wurde mit ca. 26% das Top Level Management angegeben. Auf weitere ca. 21% trifft am ehesten die operative Ebene zu. Die restlichen Befragten (6) gaben die 1. Führungsebene an.

Mehrfachantworten waren möglich – zweimal 1. Führungsebene und Operative Ebene und einmal Top Level und Mittleres Management gleichzeitig

**F8: Wie groß ist der Anteil des IT-Budgets am Umsatz Ihres Unternehmens?**

| ANTWORTOPTIONEN | DURCHSCHNITTLICHE ANZAHL | GESAMTANZAHL | BEANTWORTUNGEN |
|---|---|---|---|
| | 5 | 135 | 29 |
| Befragte insgesamt: 29 | | | |



**F9: Welche Zertifizierungen im Bereich der IT-Sicherheit und benachbarter Bereiche besitzt Ihre Organisation bzw. strebt sie an?**

| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| ISO/IEC 9001 | 25.00% | 4 |
| ISO/IEC 20000 | 6.25% | 1 |
| ISO/IEC 27001 | 50.00% | 8 |
| IT-Grundschutz BSI | 18.75% | 3 |
| ISO/IEC 62443 | 0.00% | 0 |
| ITQ-13 | 0.00% | 0 |
| VdS-Richtlinie 3473 | 0.00% | 0 |
| BS 7799 | 0.00% | 0 |
| ISIS12 | 0.00% | 0 |
| Sonstiges (bitte angeben) | 0.00% | 0 |
| GESAMT | | 16 |

**F10: Welche Zertifizierungen im Bereich IT-Sicherheit und benachbarter Bereiche besitzt Ihre Organisation bzw. strebt sie an?**

| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| ISO/IEC 9001 | 30.00% | 6 |
| ISO/IEC 20000 | 10.00% | 2 |
| ISO/IEC 27001 | 30.00% | 6 |
| IT-Grundschutz BSI | 40.00% | 8 |
| ISO/IEC 62443 | 10.00% | 2 |
| ITQ-13 | 0.00% | 0 |
| VdS-Richtlinie 3473 | 0.00% | 0 |
| BS 7799 | 0.00% | 0 |
| ISIS12 | 0.00% | 0 |
| Befragte insgesamt: 20 | | |

Betrachtet man die Antworten der Fragen 9 und 10 im Zusammenhang, wird ein eindeutiger Trend erkennbar. Die ISO/IEC 27001 ist am weitesten verbreitet, dicht gefolgt von ISO/IEC 9001 und dem IT-Grundschutz BSI. Insbesondere die branchenspezifische Norm IEC 62443 findet dagegen im Kreis der Antwortenden kaum Anwendung.

Nach diesen Fragen aus dem Bereich Demographie und Unternehmen beginnen nun die Fragen zur ICS Security, dem Kernbereich dieser Umfrage. Er umfasst die Themenbereiche:

- Einstieg ins Security Thema,
- Security-spezifische Prozesse und Richtlinien,
- Auswahl der verwendeten Systeme u. Komponenten sowie der eingesetzten Dienstleister u. Integratoren,
- Bauliche und physische Absicherung und
- Technische Maßnahmen

Die Darstellung der Antworten erfolgt in tabellarischer Form, auf die eine Farbcodierung entsprechend der Klassifikation in verschieden Reifegrade von Seite 4 mit einem kurzen Erklärungstext folgt.

## Einstieg ins Security Thema

**F11: Für das Thema ICS sind klare Verantwortlichkeiten geschaffen:**

| | JA | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|
| ICS-Sicherheitsbeauftragte benannt | 45.83% 11 | 45.83% 11 | 8.33% 2 | 24 | 1.50 |
| Anlagen- und Komponentenverantwortliche benannt | 60.87% 14 | 21.74% 5 | 17.39% 4 | 23 | 1.26 |
| Berichtslinie an das oberste Management festgelegt | 62.50% 15 | 29.17% 7 | 8.33% 2 | 24 | 1.32 |

| | |
|---|---|
| | Die Gewichtung zwischen den Befragten, die **ICS-Sicherheitsbeauftrage benannt** haben, sowie es nicht getan haben, ist mit jeweils ca. 46% gleich. Ca. 8% haben hierzu keine Angabe gemacht (bei 24 Antworten insgesamt). |

| | |
|---|---|
| | Die Mehrheit der Unternehmen (ca. 61%) hat **Anlagen- und Komponentenverantwortliche benannt**. Ca. 22% haben dieses nicht gemacht und ca. 17% haben hierzu keine Angabe gemacht (bei 23 Antworten insgesamt). |

| | |
|---|---|
| | Ebenfalls die Mehrheit (ca. 63%) **hat ihre Berichtslinie an das oberste Management festgelegt**. Ca. 29% haben keine Berichtslinie an das oberste Management festgelegt und ca. 8% haben hierzu keine Angabe gemacht (bei 24 Antworten insgesamt). |

## F12: Abfrage grundlegender Strukturen und Dokumentationen:

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Alle ICS-Komponenten sind in einem Netzplan verzeichnet. | 4.55% 1 | 13.64% 3 | 36.36% 8 | 18.18% 4 | 13.64% 3 | 13.64% 3 | 22 | 3.26 |
| Alle wesentlichen Dokumente (Anweisungen, Handbücher, Notfallanweisungen...) sind aktuell und für die beteiligten Mitarbeiter verfügbar. | 19.23% 5 | 26.92% 7 | 42.31% 11 | 3.85% 1 | 3.85% 1 | 3.85% 1 | 26 | 2.44 |
| Die Liste der IT-Systeme und installierten Anwendungen ist vollständig vorhanden. | 22.73% 5 | 40.91% 9 | 31.82% 7 | 4.55% 1 | 0.00% 0 | 0.00% 0 | 22 | 2.18 |

Nur ca. 5% aller Teilnehmer gaben an, dass bei ihnen **alle ICS-Komponenten in einem Netzplan verzeichnet** sind. Die Hälfte (50%) hat mit der Umsetzung dazu begonnen oder sie schon in weiten Teilen abgeschlossen. Bei weiteren ca. 18% ist sie geplant. Fast 14% verneinen dies.

Ca. 19% der Befragten gaben an, dass **alle ihre wesentlichen Dokumente aktuell und nur für die beteiligten Mitarbeiter verfügbar** sind. Weitere ca. 27% sehen den Prozess dahin als in weiten Teilen abgeschlossen an und ca. 42% haben mit der Umsetzung dazu begonnen.

Fast ein Viertel der Unternehmen (23%) gab an, dass die **Liste der IT-Systeme und installierten Anwendungen vollständig vorhanden** ist. Über 70% haben mit der Umsetzung dazu begonnen oder sie schon in weiten Teilen abgeschlossen.

## F13: Die Liste der IT-Systeme wird ständig aktualisiert.

| ANTWORTOPTIONEN | BEANTWORTUNGEN | |
|---|---|---|
| ja | 81.48% | 22 |
| nicht regelmäßig | 18.52% | 5 |
| nein | 0.00% | 0 |
| keine Ahnung | 0.00% | 0 |
| GESAMT | | 27 |

Die deutliche Mehrheit der Befragten (ca. 81%) hat angegeben, die Liste der IT-Systeme ständig zu aktualisieren. Ca. 19% gab an, dies immerhin nicht regelmäßig zu tun.

## Security-spezifische Prozesse und Richtlinien

### F14: Security Management - Entsorgung von Hardware

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTET MITTELWER |
|---|---|---|---|---|---|---|---|---|
| Bei der Entsorgung von Hardware achten wir neben den Umweltanforderungen auch darauf, dass keine vertraulichen Informationen mehr auf ihnen gespeichert sind | 74.07% 20 | 11.11% 3 | 3.70% 1 | 0.00% 0 | 7.41% 2 | 3.70% 1 | 27 | 1. |
| Eine Interne Softwareentwicklungsrichtlinie zur sicheren Erstellung und Integration von Eigenentwicklungen ist vorhanden. | 29.63% 8 | 22.22% 6 | 14.81% 4 | 3.70% 1 | 22.22% 6 | 7.41% 2 | 27 | 2. |

Fast drei Viertel der Teilnehmer (ca. 74%) haben angegeben, bei der **Entsorgung von Hardware** neben den Umweltanforderungen auch darauf zu achten, dass keine vertraulichen Informationen mehr auf ihnen gespeichert sind. Ca. 11% haben dies in weiten Teilen abgeschlossen und ca. 7% achten nicht darauf.

Eine **interne Softwareentwicklungsrichtlinie** zur sicheren Erstellung und Integration von Eigenentwicklung ist bei ca. 30% der Unternehmen vorhanden. Insgesamt etwas über ein Drittel (37%) hat mit der Umsetzung dazu bereits begonnen oder sie schon in weiten Teilen abgeschlossen.

### F15: Durchgängiges Management aller ICS-Komponenten - Security Monitoring

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Änderungen in der ICS-Umgebung werden durch einen gesonderten Prozess (Changemanagement-Prozess) mit (Funktions-)Rollentrennung gesteuert. | 14.81% 4 | 14.81% 4 | 22.22% 6 | 14.81% 4 | 25.93% 7 | 7.41% 2 | 27 | 3.24 |
| Sicherheitsrelevante Ereignisse werden permanent beobachtet und bei Bedarf werden zeitnah Gegenmaßnahmen auf Basis eines Security Incident Response Plan (SIRP) eingeleitet. | 18.52% 5 | 29.63% 8 | 22.22% 6 | 11.11% 3 | 14.81% 4 | 3.70% 1 | 27 | 2.73 |

Ca. 15% aller Teilnehmer gaben an, dass in ihrem Unternehmen **Änderungen in der ICS-Umgebung durch einen gesonderten Prozess mit (Funktions-) Rollentrennung gesteuert** werden. Fast 50% haben die Umsetzung entweder in Planung, sie bereits begonnen oder schon in weiten Teilen abgeschlossen. Ca. 26% haben dies verneint und ca. 7% keine Angabe gemacht.

Etwa 19% haben angegeben, dass **sicherheitsrelevante Ereignisse permanent beobachtet** und bei Bedarf zeitnah Gegenmaßnahmen auf Basis eines Security Incident Response Plan eingeleitet werden. Ca. 30% gaben an, dass sie die Umsetzung bereits in weiten Teilen abgeschlossen haben. Bei ca. einem Drittel ist die Umsetzung in Planung oder hat schon begonnen

## F16: Notfallmanagement - Wiederherstellungsplan (Business Continuity Plan) für die schützenswerten Assets

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Notfall- und Wiederanlaufpläne sind für alle ICS-relevanten Assets definiert. | 33.33% 9 | 29.63% 8 | 22.22% 6 | 3.70% 1 | 7.41% 2 | 3.70% 1 | 27 | 2.19 |
| Notfall- und Wiederanlaufpläne werden regelmäßig getestet und angepasst. | 18.52% 5 | 18.52% 5 | 25.93% 7 | 18.52% 5 | 11.11% 3 | 7.41% 2 | 27 | 2.84 |

Ein Drittel (33%) aller Teilnehmer hat angegeben, in ihrem Unternehmen **Notfall- und Wiederanlaufpläne für alle ICS-relevanten Assets** definiert zu haben. Weitere ca. 30% haben die Umsetzung dorthin bereits in weiten Teilen abgeschlossen. Ca. 7% haben es verneint.

Davon haben jeweils 19% angegeben, dass ihre **Notfall- und Wiederanlaufpläne regelmäßig getestet und angepasst** werden oder dass die Umsetzung bereits in weiten Teilen abgeschlossen ist. Etwas über ein Viertel (26%) hat immerhin mit der Umsetzung begonnen und weitere ca. 19% haben sie geplant. Ca. 11% haben es verneint.

## F17: Personal - Prozesse für Einstellung, Wechsel und Ausscheiden von Personal

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Mitarbeiter werden regelmäßig zu Aspekten der Informationssicherheit geschult. | 51.85% 14 | 14.81% 4 | 18.52% 5 | 7.41% 2 | 7.41% 2 | 0.00% 0 | 27 | 2.04 |

Etwas mehr als die Hälfte (ca. 52%) der Teilnehmer hat angegeben, dass ihre Mitarbeiter regelmäßig zu Aspekten der Informationssicherheit geschult werden. Weitere 15% gaben an, den Prozess dazu in weiten Teilen abgeschlossen zu haben. Immerhin ca. 19% haben bereits mit der Umsetzung dazu begonnen.

**F18: Revision & Tests - Komponentenprüfung**

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|
| Die Einhaltung der internen und externen Anforderungen wird regelmäßig auditiert. | 37.04% 10 | 22.22% 6 | 18.52% 5 | 3.70% 1 | 18.52% 5 | 27 | 2.44 |

Etwas mehr als ein Drittel (ca. 37%) der Befragten gab an, die Einhaltung der internen und externen Anforderungen regelmäßig zu auditieren. Weiterhin hat etwas weniger als ein Viertel (ca. 22%) angegeben, dies in weiten Teilen abgeschlossen zu haben. Jeweils ca. 19% haben angegeben, mit der Umsetzung dazu bereits begonnen zu haben oder aber die Anforderungen überhaupt nicht auditieren zu lassen.

## Auswahl der verwendeten Systeme u. Komponenten sowie der eingesetzten Dienstleister u. Integratoren

**F19: Inbetriebnahme in sicherer Konfiguration - Aktivierte Sicherheitsmechanismen und aktueller Patchstand**

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Bei Inbetriebnahme von Komponenten werden Passwörter und Konfiguration des Sicherheitserfordernissen angepasst. | 55.56% 15 | 18.52% 5 | 18.52% 5 | 3.70% 1 | 3.70% 1 | 0.00% 0 | 27 | 1.81 |

Über die Hälfte der Teilnehmer (ca. 56%) gab an, dass bei der Inbetriebnahme von Komponenten, Passwörter und Konfiguration den Sicherheitserfordernissen angepasst werden. Jeweils ca. 19% haben diesen Sicherheitsmechanismus bereits in weiten Teilen abgeschlossen oder mit der Umsetzung dazu begonnen.

**F20: Fernwartung durch Hersteller und Integrator - Sichere Fernwartung**

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Bei Inbetriebnahme von Komponenten werden Passwörter und Konfiguration den Sicherheitserfordernissen angepasst. | 44.44% 12 | 25.93% 7 | 22.22% 6 | 0.00% 0 | 0.00% 0 | 7.41% 2 | 27 | 1.76 |

Fast die Hälfte der Befragten (44%) gab an, auch bei der Fernwartung durch Hersteller und Integrator, bei der Inbetriebnahme von Komponenten, Passwörter und Konfiguration den Sicherheitserfordernissen anzupassen. Ein Viertel der Teilnehmer (ca. 26%) haben den Prozess zu diesem Mechanismus in weiten Teilen abgeschlossen und ca. 22% haben mit der Umsetzung dazu begonnen.

## Bauliche und physische Absicherung

### F21: Physische Absicherung

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Es ist sichergestellt, dass nur berechtigte Personen Zugang zu gesicherten Bereichen haben und dieses wird protokolliert. | 62.96% 17 | 22.22% 6 | 3.70% 1 | 0.00% 0 | 11.11% 3 | 0.00% 0 | 27 | 1.74 |

Fast zwei Drittel (ca. 63%) der befragten Unternehmen gaben an, dass sichergestellt ist, dass nur berechtige Personen Zugang zu gesicherten Bereichen haben und dieses auch protokolliert wird. Fast ein Viertel (ca. 22%) haben diese Absicherung in weiten Teilen abgeschlossen und ca. 11% verneinen diese Absicherung.

## Technische Maßnahmen

### F22: Absicherung der Netze - Nutzung von sicheren Protokollen

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| ICS-Netze sind von anderen Netzen getrennt (zum Beispiel über eine DMZ). | 48.00% 12 | 12.00% 3 | 24.00% 6 | 4.00% 1 | 4.00% 1 | 8.00% 2 | 25 | 1.96 |
| Direkte Schnittstellen zwischen externen Netzen und dem ICS-Netz sind nicht vorhanden. | 44.00% 11 | 16.00% 4 | 12.00% 3 | 0.00% 0 | 12.00% 3 | 16.00% 4 | 25 | 2.05 |
| Firewalls sind anhand geltender Standards restriktiv konfiguriert (zum Beispiel Filterung jeglichen eingehenden und ausgehenden Datenverkehrs). | 52.00% 13 | 24.00% 6 | 12.00% 3 | 0.00% 0 | 4.00% 1 | 8.00% 2 | 25 | 1.70 |
| Intrusion Detektion (IDS)/Intrusion Prevention Systeme (IPS) sind im Einsatz. | 36.00% 9 | 20.00% 5 | 28.00% 7 | 8.00% 2 | 4.00% 1 | 4.00% 1 | 25 | 2.21 |
| Der Einsatz von unsicheren Protokollen (z.B. Telnet, FTP, HTTP) wird unterbunden. | 36.00% 9 | 24.00% 6 | 12.00% 3 | 8.00% 2 | 20.00% 5 | 0.00% 0 | 25 | 2.52 |

| | |
|---|---|
| | Beinahe die Hälfte aller Befragten (48%) hat angegeben, dass ihre **ICS-Netze von anderen Netzen getrennt** sind. Weitere 40% sehen den Prozess dorthin als geplant, bereits in Umsetzung oder diese als schon in weiten Teilen abgeschlossen an. |

| | |
|---|---|
| | 44% der Unternehmen gaben an, dass **keine direkten Schnittstellen zwischen externen Netzen und dem ICS-Netz** vorhanden sind. Weitere insgesamt 28% haben die Umsetzung dorthin begonnen oder sie schon in weiten Teilen abgeschlossen. 12% haben es verneint. |

| | |
|---|---|
| | Fast die Hälfte der Befragten (44%) gab an, auch bei der Fernwartung durch Hersteller und Integrator, bei der Inbetriebnahme von Komponenten, Passwörter und Konfiguration den Über die Hälfte der Teilnehmer (52%) hat angegeben, dass **Firewalls anhand geltender Standards restriktiv konfiguriert** sind. Insgesamt 36% weitere Unternehmen sehen dies als in Umsetzung oder diese bereits als in weiten Teilen abgeschlossen an. |

| | |
|---|---|
| | Etwas über ein Drittel aller Unternehmen (36%) gab an, **dass Intrusion Detektion (IDS)/Intrusion Prevention Systeme (IPS) im Einsatz** sind. 56% der übrigen Unternehmen gaben an, dass die Umsetzung zu dem Einsatz dieser in Planung ist, bereits vorgenommen wird oder schon zu weiten Teilen abgeschlossen ist. |
| | Über ein Drittel (36%) hat angegeben, dass der **Einsatz von unsicheren Protokollen unterbunden** wird. 24% haben die Umsetzung dorthin bereits in weiten Teilen abgeschlossen. Insgesamt 20% haben die Umsetzung in Planung oder immerhin schon begonnen. Weitere 20% haben es verneint. |

### F23: Absicherung von Diensten und Protokollen – Zeitsynchronisierung

| | JA | IN WEITEN TEILEN UMGESETZT | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Der DNS-Server für ICS-Netze ist von DNS-Servern in anderen Netzen separiert. | 24.00% 6 | 12.00% 3 | 8.00% 2 | 8.00% 2 | 24.00% 6 | 24.00% 6 | 25 | 2.95 |

| | |
|---|---|
| | Fast ein Viertel (24%) der Teilnehmer gab an, dass in ihrem Unternehmen der DNS-Server für ICS-Netze von DNS-Servern in anderen Netzen separiert ist. Immerhin 12% haben dies in weiten Teilen umgesetzt und 8% mit der Umsetzung begonnen. Fast ein weiteres Viertel (24%) separiert hier nicht. |

## F24: Härtung der IT-Systeme - Zugriff auf das Internet innerhalb des ICS-Netzwerk

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Standard-Benutzerkonten und -Passwörter sind deaktiviert oder gelöscht. | 52.00% 13 | 20.00% 5 | 8.00% 2 | 4.00% 1 | 4.00% 1 | 12.00% 3 | 25 | 1.73 |
| Für die Nutzung von gemeinsamen Benutzerkonten und-Passwörtern sind Maßnahmen ergriffen worden, die einen Missbrauch verhindern. | 36.00% 9 | 40.00% 10 | 16.00% 4 | 0.00% 0 | 8.00% 2 | 0.00% 0 | 25 | 2.04 |
| Nicht benötigte Programme und Dienste auf ICS-Komponenten werden deaktiviert oder entfernt. | 24.00% 6 | 32.00% 8 | 20.00% 5 | 4.00% 1 | 12.00% 3 | 8.00% 2 | 25 | 2.43 |
| Standardeinstellungen sind an den definierten Sicherheitslevel angepasst. | 45.83% 11 | 20.83% 5 | 16.67% 4 | 4.17% 1 | 4.17% 1 | 8.33% 2 | 24 | 1.91 |
| Nicht benötigte Hardware (zum Beispiel lokale Schnittstellen wie USB-Ports) Ist deaktiviert oder entfernt. | 24.00% 6 | 12.00% 3 | 24.00% 6 | 0.00% 0 | 32.00% 8 | 8.00% 2 | 25 | 3.04 |
| Das ICS-Netzwerk ist vom Internet komplett separiert. | 48.00% 12 | 4.00% 1 | 16.00% 4 | 0.00% 0 | 20.00% 5 | 12.00% 3 | 25 | 2.32 |

Über die Hälfte (52%) der Unternehmen hat angegeben, dass **Standard-Benutzerkonten und -Passwörter** deaktiviert oder gelöscht sind. 32% haben angegeben, dass die Umsetzung dorthin in Planung ist, sie bereits damit begonnen haben oder sie schon in weiten Teilen abgeschlossen ist. 12% haben keine Angabe gemacht.

Über ein Drittel der Befragten (36%) gab an, dass für die **Nutzung von gemeinsamen Benutzerkonten und -Passwörtern** Maßnahmen ergriffen worden sind, die einen Missbrauch verhindern. Insgesamt 56% haben die Umsetzung dafür bereits begonnen oder sie schon in weiten Teilen abgeschlossen. 8% haben keine Angabe gemacht

Etwa ein Viertel (25%) hat **nicht benötigte Programme und Dienste** auf ICS-Komponenten als deaktiviert oder entfernt angegeben. 32% haben die Umsetzung dafür als bereits in weiten Teilen abgeschlossen angegeben. Weitere 20% haben sie wenigstens begonnen. 12% haben dies verneint.

Ca. 46% haben angegeben, dass **Standardeinstellungen** an den definierten Sicherheitslevel angepasst sind. Etwas über 40% haben die Umsetzung dafür in Planung, sie bereits begonnen oder schon in weiten Teilen abgeschlossen. 4% haben es verneint.

Etwa ein Viertel der Teilnehmer (24%) hat geantwortet, dass **nicht benötigte Hardware z.B. Ports** deaktiviert oder entfernt wird. Weitere 36% haben die Umsetzung dafür begonnen oder schon in weiten Teilen abgeschlossen. 32% haben es verneint und 8% keine Angabe gemacht.

Fast die Hälfte der Befragten (48%) hat angegeben, dass ihr **ICS-Netzwerk** vom Internet komplett separiert ist. Insgesamt 20% die Umsetzung begonnen oder schon zu weiten Teilen abgeschlossen. 20% haben dies verneint und 12% keine Angabe gemacht.

## F25: Patchmanagement - Umgang mit End Of Support (EOS)

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Es ist ein standardisierter Patchmanagement-Prozess eingeführt. | 20.00% 5 | 28.00% 7 | 16.00% 4 | 8.00% 2 | 28.00% 7 | 0.00% 0 | 25 | 2.96 |
| Die Kritikalität von Patches wird bewertet, zum Beispiel anhand des Common Vulnerability Scoring System (CVSS). | 16.67% 4 | 25.00% 6 | 0.00% 0 | 16.67% 4 | 20.83% 5 | 20.83% 5 | 24 | 3.00 |

Ein Fünftel (20%) aller Befragten gab an, einen **standardisierten Patchmanagement Prozess** eingeführt zu haben. Über die Hälfte (52% insgesamt) gab an diesen geplant zu haben oder mit der Umsetzung dazu begonnen bzw. sie schon in weiten Teilen abgeschlossen zu haben. 28% verneinen die Einführung.

Ca. 17% haben angegeben, dass bei ihnen die **Kritikalität von Patches zum Beispiel anhand des Common Vulnerability Scoring System (CVSS) bewertet** wird. Bei weiteren 25% ist dieses in weiten Teilen abgeschlossen. 17% der Befragten haben es geplant aber 42% verneinen dieses Vorgehen oder haben keine Angabe gemacht.

## F26: Authentisierung - Vermeidung von Missbrauch

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Zur Nutzung von ICS-Assets wird jeweils eine Authentifizierung benötigt. | 52.00% 13 | 16.00% 4 | 20.00% 5 | 4.00% 1 | 0.00% 0 | 8.00% 2 | 25 | 1.74 |
| Eine Passwortrichtlinie ist implementiert. | 60.00% 15 | 20.00% 5 | 8.00% 2 | 0.00% 0 | 12.00% 3 | 0.00% 0 | 25 | 1.84 |

Etwas über die Hälfte (52%) der befragten Unternehmen gab an, dass bei ihnen **zur Nutzung von ICS-Assets jeweils eine Authentifizierung** benötigt wird. Insgesamt 36% haben mit der Umsetzung dazu bereit begonnen oder sie schon in weiten Teilen abgeschlossen. 4% haben angegeben, sie in Planung zu haben.

60% der Befragten haben angegeben, eine **Passwortrichtlinie implementiert** zu haben. Bei weiteren 28% hat die Umsetzung dazu bereits begonnen oder ist schon in weiten Teilen abgeschlossen. 12% haben es verneint.

## F27: Zugriffskontrolle

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Zugriffsrechte werden restriktiv vergeben (Prinzip der geringsten Privilegien). | 60.00% 15 | 20.00% 5 | 4.00% 1 | 4.00% 1 | 12.00% 3 | 0.00% 0 | 25 | 1.88 |

Insgesamt 80% der Teilnehmer gaben an, dass bei ihnen **Zugriffsrechte restriktiv vergeben** werden oder die Umsetzung dazu in weiten Teilen abgeschlossen ist. Weitere 8% haben dies geplant oder zumindest mit der Umsetzung begonnen. 12% gaben an, ihre Zugriffsrechte nicht restriktiv zu vergeben.

## F28: Schutz vor Schadprogrammen - Installation und Betrieb von Virenschutzprogrammen

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Virenschutzprogramme sind installiert, bzw. es sind nach einer Risikoabschätzung alternative Maßnahmen zum Schutz der Assets installiert. | 68.00% 17 | 20.00% 5 | 4.00% 1 | 4.00% 1 | 4.00% 1 | 0.00% 0 | 25 | 1.56 |

Über zwei Drittel (68%) der Befragten gaben an, Virenschutzprogramme, bzw. nach einer Risikoabschätzung eine alternative Maßnahme zum Schutz der Assets, installiert zu haben. Insgesamt 8% haben diese Schutzmaßnahme geplant oder mit der Umsetzung dazu begonnen und 20% haben sie bereits in weiten Teilen abgeschlossen.

## F29 Mobile Datenträger - Umgang mit Wechseldatenträgern

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Eine Richtlinie zum Umgang mit Wechseldatenträgern (zum Beispiel USB-Sticks) ist etabliert. | 56.00% 14 | 16.00% 4 | 0.00% 0 | 4.00% 1 | 24.00% 6 | 0.00% 0 | 25 | 2.24 |
| Quarantäne-PCs zum Test von mobilen Datenträgern sind im Einsatz. | 24.00% 6 | 12.00% 3 | 12.00% 3 | 12.00% 3 | 32.00% 8 | 8.00% 2 | 25 | 3.17 |

Über die Hälfte (56%) der Teilnehmer gab an, dass in ihrem Unternehmen eine **Richtlinie zum Umgang mit Wechseldatenträgern etabliert** ist. Weitere insgesamt 20% haben dies geplant oder die Umsetzung schon in weiten Teilen abgeschlossen. Fast ein Viertel (24%) ha keine entsprechende Richtlinie etabliert.

Fast ein Viertel (24%) der Teilnehmer hat außerdem angegeben, **Quarantäne-PCs zum Test von mobilen Datenträgern im Einsatz zu haben**. Über ein Drittel (insgesamt 36%) hat dies geplant, mit der Umsetzung dazu begonnen oder sie schon in weiten Teilen abgeschlossen. 32% verneinen den Einsatz.

## F30: Datensicherung - Datensicherungen der Systeme

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Datensicherungen werden regelmäßig und in kurzen Abständen durchgeführt. | 80.00% 20 | 8.00% 2 | 0.00% 0 | 0.00% 0 | 4.00% 1 | 8.00% 2 | 25 | 1.26 |

| | |
|---|---|
| | 80% der Befragten gaben an, dass Datensicherungen regelmäßig in kurzen Abständen durchgeführt werden. Bei weiteren 8% ist dieser Prozess zumindest in weiten Teilen abgeschlossen. |

## F31: Protokollierung und Auswertung - Logging / Monitoring

| | JA | IN WEITEN TEILEN ABGESCHLOSSEN | MIT DER UMSETZUNG BEGONNEN | GEPLANT | NEIN | K. A. | INSGESAMT | GEWICHTETER MITTELWERT |
|---|---|---|---|---|---|---|---|---|
| Logging-Daten werden zentral dokumentiert. | 52.00% 13 | 16.00% 4 | 8.00% 2 | 12.00% 3 | 8.00% 2 | 4.00% 1 | 25 | 2.04 |

| | |
|---|---|
| | Etwa die Hälfte (52%) hat angegeben, dass die Logging-Daten zentral dokumentiert werden. Insgesamt 36% haben die Umsetzung davon geplant, mit ihr begonnen oder diese schon in weiten Teilen abgeschlossen. 8% tun dies nicht. |

## Fazit

Schließen möchten wir mit folgenden vier Forderungen an einen guten Einstieg in die ICS-Security:

- Beginnen Sie mit einer ehrlichen IST-Aufnahme.
- Wählen Sie zur Umsetzung einen systematischen Ansatz auf Basis der vorhandenen Best-Practice-Ansätze.
- Nutzen Sie dabei ein stufenweises Vorgehen (Reifegradmodell).
- Vergleichen Sie Ihre Vorgehensweisen, um von anderen zu lernen.

Wir würden uns freuen, wenn diese Auswertung den Ausgangspunkt für weitere Diskussionen bildet.

Abschließend gilt es allen Beteiligten an der Umfrage noch einmal herzlich für Ihre Aufwände und Unterstützung zu danken. Auch wenn es an verschiedenen Stellen noch Verbesserungspotential gibt, so geben die Ergebnisse bereits einen guten Einblick in die aktuelle Situation von ICS-Security in OWL und bieten gleichzeitig auch viele Hinweise auf Optimierungsmöglichkeiten.

Paderborn/Bielefeld im August 2020

Wenn Sie Fragen oder Anmerkungen zu Ihrer Auswertung haben, so wenden Sie sich bitte an:


| | |
|---|---|
| Achim Knust-Bock<br>Senior Project Manager<br>Vasgard GmbH<br>Bahnhofsstraße 31b<br>33102 Paderborn<br>Mobil: +49-171-2930629<br>Telefon: +49-5251-5449456<br>achim.knust-bock@vasgard.com<br>www.vasgard.com | Professor Dr. Achim Schmidtmann<br>Fachhochschule Bielefeld<br>Fachbereich Wirtschaft und Gesundheit<br>Interaktion 1<br>33619 Bielefeld<br>Telefon: +49.521.106-5065<br>Telefax: +49.521.106-5086<br>achim.schmidtmann@fh-bielefeld.de<br>www.fh-bielefeld.de |