Ergebnisse der Safety & Security Umfrage 2022

Das Thema **OT-Security** wird mit der Überarbeitung der Maschinenrichtlinie auch in naher Zukunft für die Maschinensicherheit, nicht nur Kür sondern auch Pflicht.

Die Ergebnisse der Safety & Security Umfrage geben Aufschluss über das Verständnis zum Einsatz der OT-Security als Ergänzung zur Maschinensicherheit. Die Erhebung dient zudem der Vorbereitung und die inhaltliche Gestaltung für die Safety&Security Network Conference 2022.

Die Datenerhebung erfolgte mittels Onlinebefragung im April und Mai 2022. Die Stichprobengröße lag bei n = 151. Zielgruppe der Befragung waren Kunden von Pilz Österreich (Betreiber + OEMs).

Demographische Daten

Die Verteilung der Stichproben erfolgte auf 36% Betreiber und 64% OEMs.

Knapp die Hälfte der Befragten nehmen in ihren Unternehmen Führungspositionen ein (38% Abteilungs-/Gruppenleitung, +7% Vorstand und GF) und verfügen dementsprechend über eine Entscheidungsbefugnis. 13% der Umfrageteilnehmer sind Projektleiter, 4% zählen zu keiner der Positionsbezeichnungen (sonstiges).

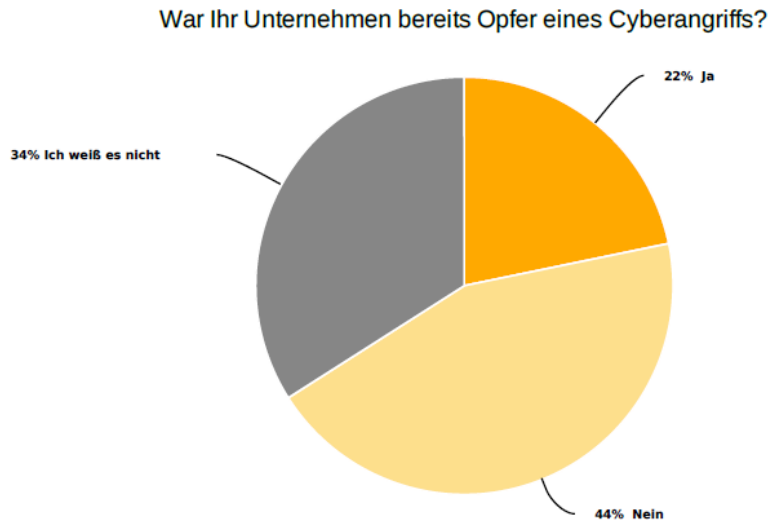
Der Teilnahme an der Umfrage erfolgte zum großen Teil durch Konstrukteure mit > 40%, sowie Entwickler (18%) und Instandhalter (13%). 25% der befragten zählt sich zu keiner der Berufsgruppen (sonstiges).

Mehr als die Hälfte der Befragten sind also bereits in sehr frühen Planungs- und/oder Entwicklungsstadien von Maschinen/Anlagen eingebunden. Die Bereitschaft zur Umfrageteilnahme in dieser Gruppe lässt damit auf das Verständnis für die Bedeutung der OT-Security schließen.

War Ihr Unternehmen bereits Opfer eines Cyberangriffs?

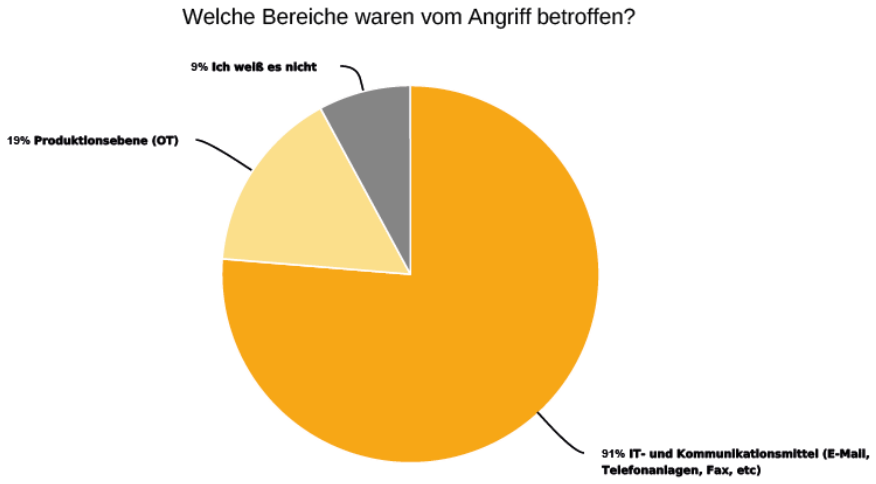
Wenn ja, welche Bereiche waren vom Angriff betroffen?

Die Frage nach einer erfolgten Cyberattacke konnten 22% bestätigen, 44% verneinten die Antwort. Rund ein Drittel der Umfrageteilnehmer (34%) konnte die Frage allerdings nicht beantworten.



Diejenigen Teilnehmer der Umfrage, die bereits Opfer einer Cyberattacke waren berichteten zum Großteil von Auswirkungen auf die IT- und Kommunikationsmittel, wogegen nur 19% der Befragten angaben, dass die Produktion betroffen war.

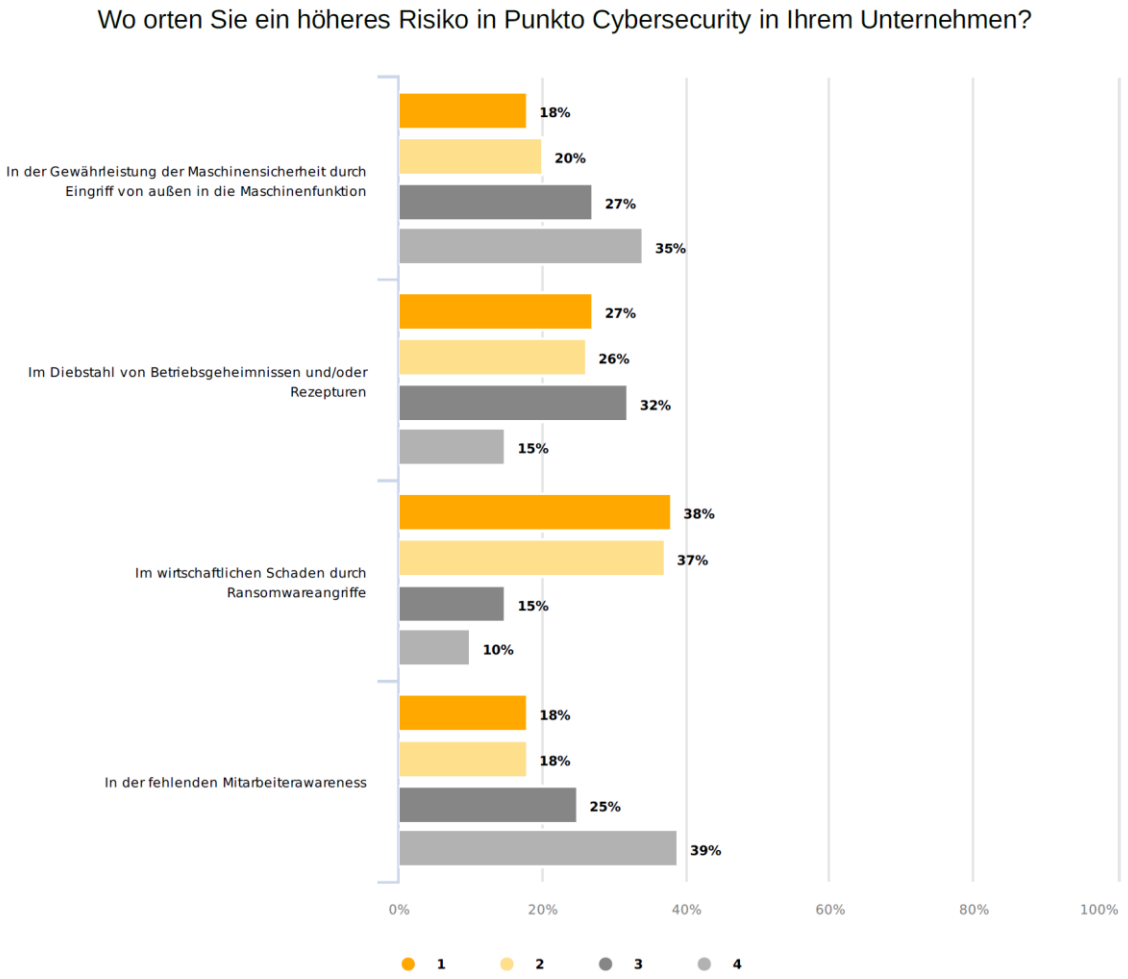
Bei dieser Frage waren Mehrfachantworten möglich.



Wo orten Sie in höheres Risiko in Punkto Cybersecurity in Ihrem Unternehmen?

Die Einschätzung des Risikos erfolgte durch Reihung von 1 (hohes Risiko) – 4 (niedriges Risiko).

Das höchstempfundene Risiko ist der wirtschaftliche Schaden des Unternehmens durch Ransomwareangriffe, gefolgt vom Diebstahl von Betriebsgeheimnissen und/oder Rezepturen. Erst an dritter Stelle wird die Gewährleistung der Maschinensicherheit durch den Eingriff in die Maschinenfunktion von außen genannt. Der fehlenden Mitarbeiterawareness wird im Verhältnis ein niedriges Risiko attestiert.



Ergebnis zur Risikoeinschätzung im Detail:

Die Umfrageteilnehmer wurden gebeten die folgenden Parameter Ihrer Einschätzung nach zu Reihen, wobei an oberster (erster) Stelle das höchste Risiko stand, an letzter (vierter) Stelle das geringste Risiko:

- Wirtschaftlicher Schaden durch Ransomwareangriffe
- Diebstahl von Betriebsgeheimnissen und/oder Rezepturen
- Gewährleistung der Maschinensicherheit durch den Eingriff von außen in die Maschinenfunktion
- In der fehlenden Mitarbeiterawareness

Grundsätzlich wird dem wirtschaftlichen Schaden durch Ransomwareangriffe das höchste Risikopotential zugeschrieben.

75% der Befragten sehen ein (eher) hohes Risiko in der wirtschaftlichen Schädigung durch Hackerangriffe, während 25% hier ein geringeres (geringes) Risiko sehen.

Ein hohes Risiko wird dem Diebstahl von Betriebsgeheimnissen und/oder Rezepturen attestiert. Knapp über 50% der Befragten sehen im Diebstahl eine starke Gefährdung, für 30% der Befragten liegt das Risiko für einen Diebstahl nur mehr an 3. Stelle. Für 15% ist dieses Risiko nachgereiht.

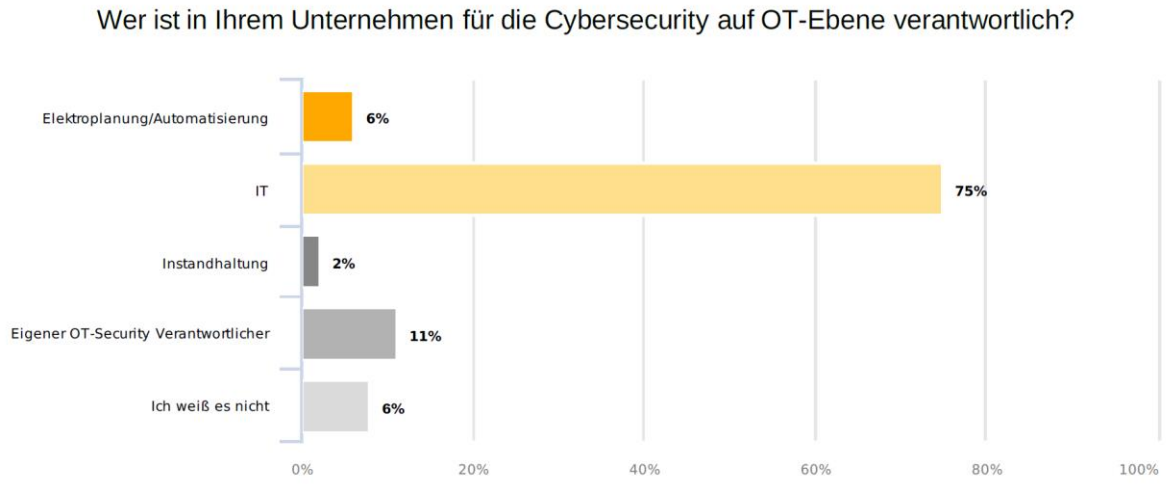
Gesamt sehen die Befragten den Eingriff in die Maschinenfunktion von außen nur an dritter Stelle. Hier geben knapp 40% von einem hohen Risiko aus. Für 35% der Befragten liegt dieses Risiko an vierter Stelle.

Erst an vierter Stelle wird die Mitarbeiterawareness als Gefahrenpotential genannt. Weit mehr als die Hälfte der Befragten (64%) sieht in der fehlenden Mitarbeiterawareness ein geringeres Risiko, nur jeweils 18% halten die mangelnde Achtsamkeit der Mitarbeiter für ein hohes/höheres Risiko.

Dies ist umso beachtenswerter, als dass zwar die wirtschaftliche Gefährdung des Unternehmens als das höchste Risiko empfunden wird. Dem Schutzpotential das aufmerksame Mitarbeiter in sich tragen, wird allerdings wenig Bedeutung beigemessen. Die aktuelle Bedrohung (Stand Juni 2022) durch die so genannte Follina Schwachstelle, eine kritische Schwachstelle in Microsoft Dokumenten, die bei unbedachter Nutzung von Office Dokumenten Malware auf den Computer spielt, zeigt dass neben technischer Maßnahmen die Schulung von Mitarbeitern eine sehr bedeutende Maßnahme bei der Abwehr von Angriffen ist. Die Wahrnehmung der Mitarbeiterverantwortung wird aber von den Befragten verhältnismäßig gering eingeschätzt.

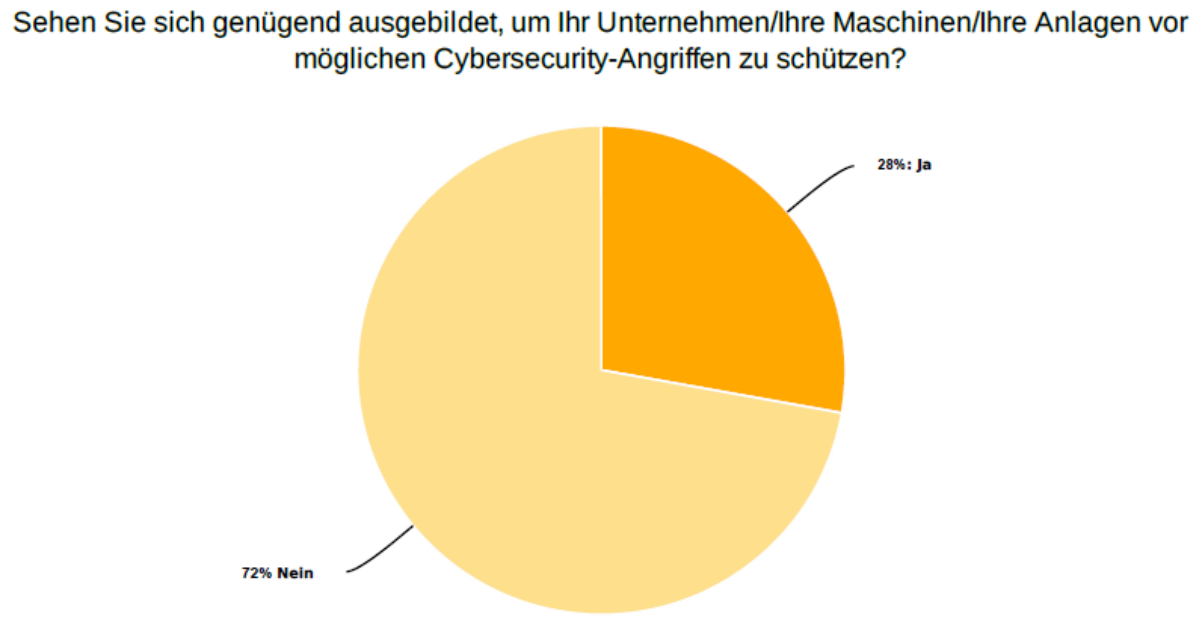
Verantwortlichkeiten

Von den Befragten 151 Unternehmen gaben 11% an, einen eigenen Verantwortlichen für den Bereich der OT-Security zu haben, in 113 der befragten Unternehmen sieht man die Verantwortlichkeit in Punkto der OT-Security in der IT- Abteilung. Die Praxis zeigt allerdings, dass die IT keine/wenig Verantwortung für die OT-Security übernimmt. Dies mag an der historischen Entwicklung liegen, dass der OT-Bereich seit jeher die Domäne der Automatisierer ist. Mit dem Fortschreiten der Digitalisierung/Vernetzung in der industriellen Kommunikation geht die Annäherung der Bereiche einher, die eine klare Kompetenzzuschreibung bedingt.



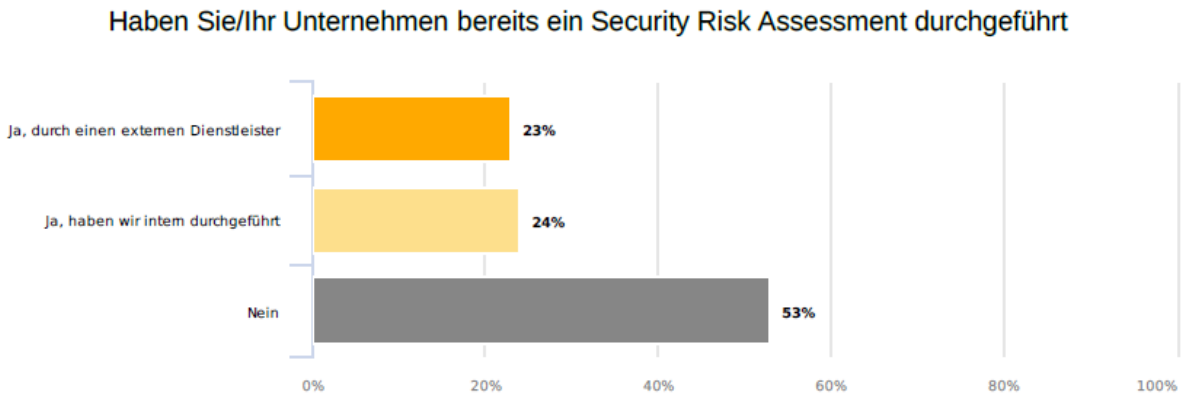
Ausbildung im OT-Security-Bereich

Knapp ¾ der Befragten sehen sich nicht genug ausgebildet, um sich vor möglichen Cyberangriffen zu schützen. Dies mag zum einen an den bisher mangelnden Ausbildungsmöglichkeiten liegen, aber auch an der Zuordnung der Verantwortung innerhalb der jeweiligen Organisation.



Security Risk Assessment

Mehr als die Hälfte der Befragten hat bisher kein Security Risk Assessment durchgeführt und nur weniger als ein ¼ der Umfrageteilnehmer haben sich durch einen externen Dienstleister beraten lassen. Obwohl es bei der Risikoeinschätzung durch Cyberattacken auf betroffene Bereiche eine klare Tendenz gibt (siehe Frage nach Risikoeinschätzung), verzichten rund 50% der befragten (Unternehmen) auf eine professionelle Einschätzung des Sicherheitsrisikos.



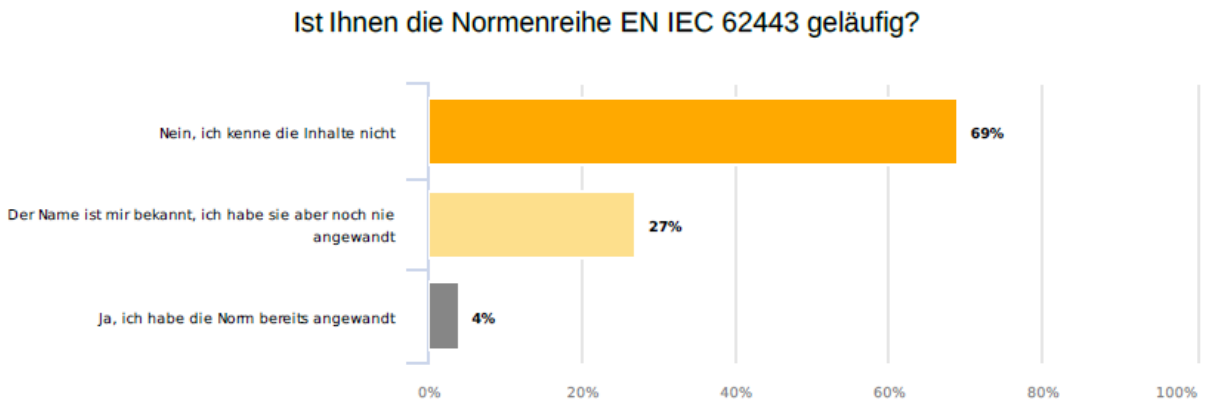
Kenntnis/Anwendung der Normenreihe EN IEC 62443

Der Stand der Technik hinsichtlich Security (EN IEC 62443) wurde nur von 4% der befragten Unternehmen bereits angewandt. Knapp 70% der befragten Unternehmen kennen die Inhalte dieser Normenreihe nicht.

Die Normenreihe EN IEC 62443 schreibt die IT-Sicherheitsanforderungen an Automatisierungssysteme vor und weist dem betrachteten System Security-Level (SL) zu.

Systemintegratoren, Produktlieferanten und Dienstleister werden mit Hilfe dieser Normenreihe bewerten, in wie weit ihre Produkte und Dienstleistungen die funktionalen IT-Sicherheitsfähigkeiten erbringen können SL-T (en: target security level).

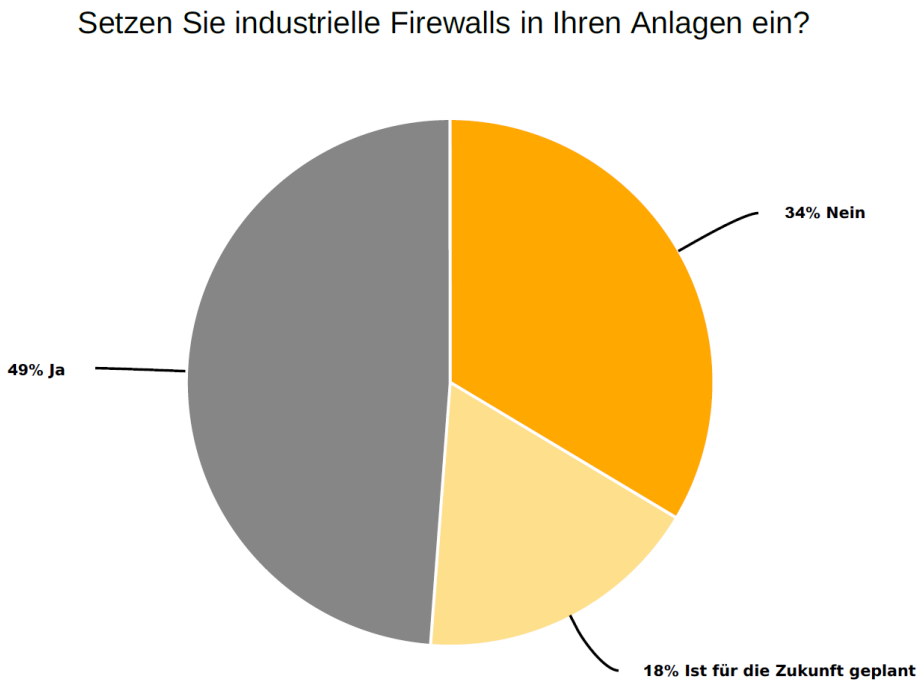
Wo diese Betrachtungen heute noch weitgehend auf „freiwilliger“ Basis beruhen, werden diese, mit der Integration des Themas „Cyber-Security“ in der zukünftigen Maschinen-Produkte Verordnung, zur Pflicht!

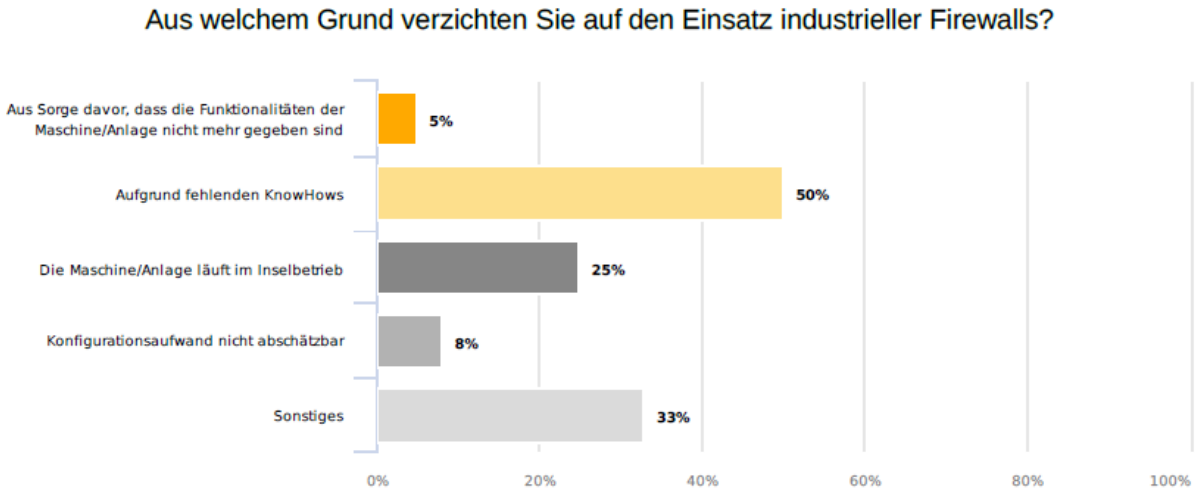


Einsatz Firewalls

Mehr als die Hälfte aller befragten Unternehmen schützen ihre Anlagen bereits mittels adäquater industrieller Firewalls. 50% der befragten Unternehmen, die keine oder noch keine Firewalls einsetzen, führten dies auf fehlendes Know How zurück und vermeintlich geglaubte Sicherheit durch Nutzung im Inselbetrieb. Lediglich 5% gaben an, aus Sorge vor Funktionseinschränkungen in der Maschine/Anlage auf den Einsatz einer Firewall zu verzichten. Die 33% der sonstigen scheinen dem dem Antwortverhalten nach auf OEMs zu entfallen, da die Verantwortung für den Einsatz einer Firewall den eigenen Kunden zugeschrieben wird.

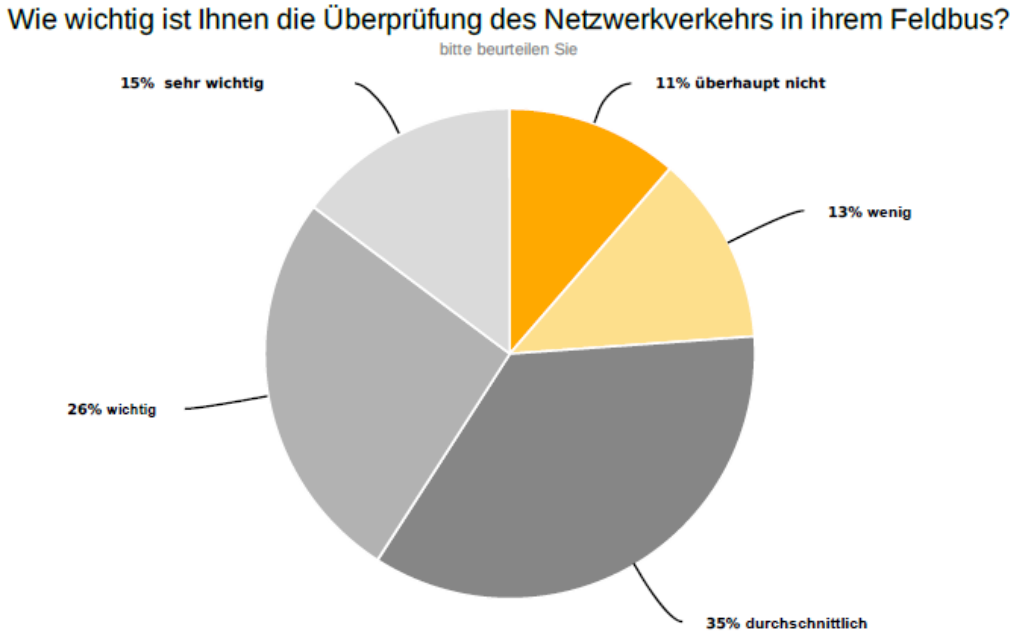
Durch den Irrglauben, dass eine Maschine nicht ans Internet angebunden wäre sieht ein Großteil der Befragten ihre Maschinen als abgesichert an. Der Aspekt, dass durch das Verbinden der Maschine über zB ein Mobiltelefon im Wartungsfall die Anlage möglicherweise mit dem Internet verbunden wird wird von vielen außer Betracht gelassen. Bei der Begründung für den Verzicht auf den Einsatz industrieller Firewalls war eine Mehrfachantwort möglich.





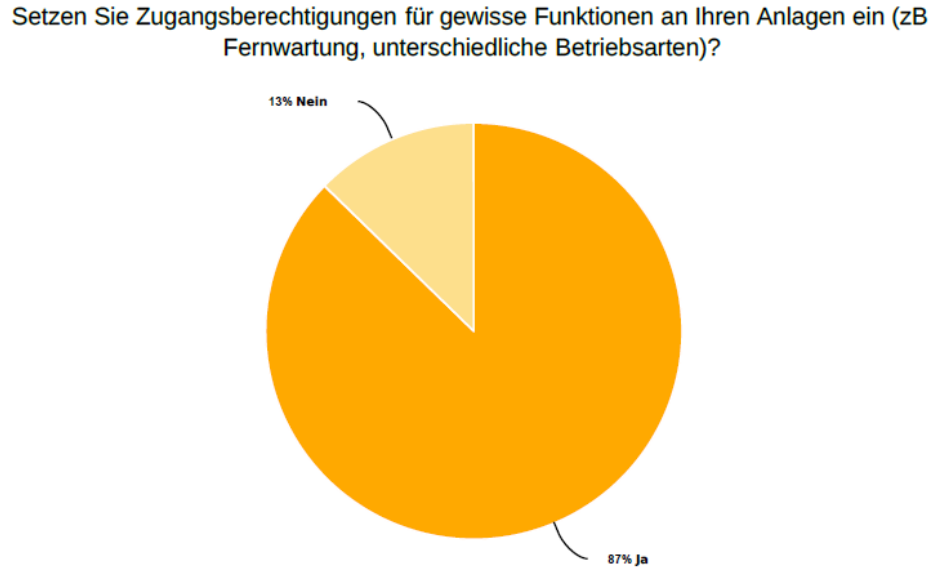
Überprüfung Netzwerkverkehr im Feldbus

Die Prüfung auf Anomalien im Datenverkehr innerhalb des Netzwerkes wird nur von 41% der Unternehmen als wichtig empfunden. Für knapp die Hälfte der befragten Unternehmen (48%), ist eine Überprüfung wenig bis gar nicht relevant. Die geringe Kenntnis über die Verbindungen innerhalb des eigenen Firmennetzwerkes stellt ein potenzielles Sicherheitsrisiko dar.



Zugangsberechtigungen

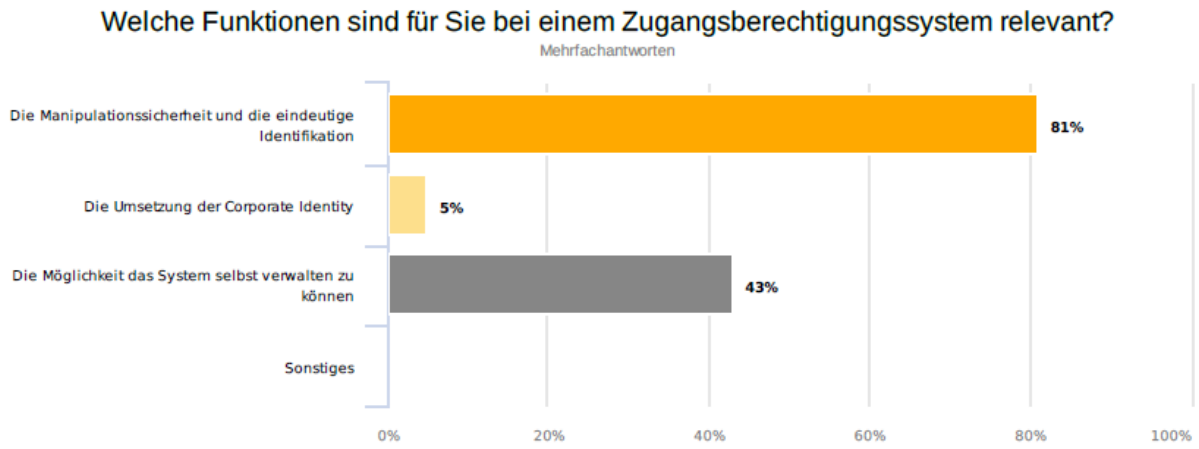
Zugangsberechtigungen für unterschiedliche Betriebsarten sind zwar in 87% implementiert allerdings lässt die Beantwortung der Fragen den Schluss zu, dass nicht alle Gefahren, die zB durch das Thema der Fernwartung entstehen, den Befragten bewusst sind.



Relevante Funktionen bei Zugangsberechtigungssystem?

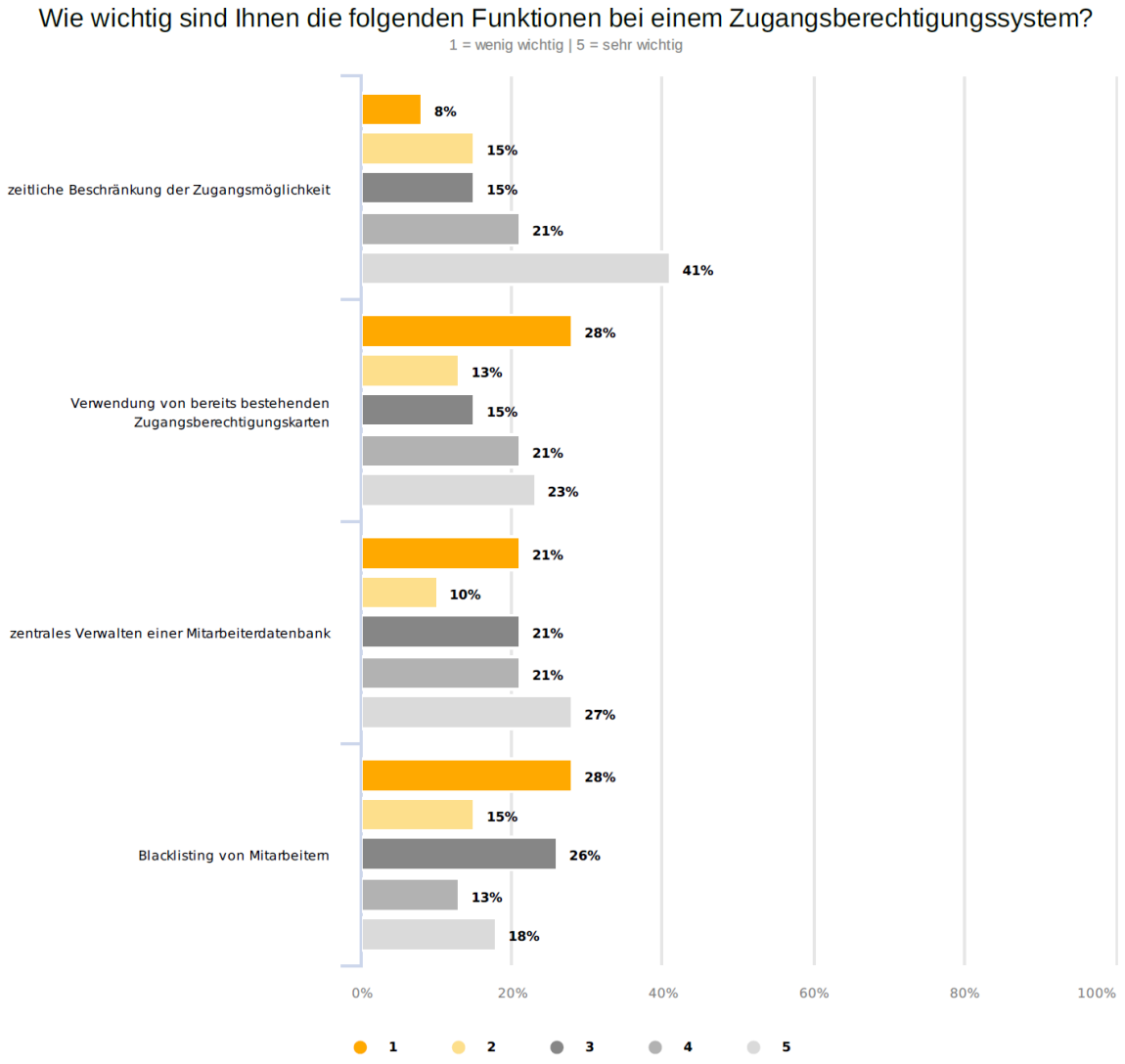
Die Frage nach der Relevanz von Funktionen bei Zugangsberechtigungen wurde nur OEMs ausgespielt, bzw. mur von dieser Gruppe beantwortet.

Die eindeutige Identifikation, wer wann an der Maschine arbeitet (81%) und die Möglichkeit dieses Zugangssystem selbst verwalten zu können (43%) wird als besonders wichtig angesehen. Hier sehen die Befragten die Priorität darin bereits bestehende Zugangskarten verwenden zu können, diese selbst verwalten zu können, um bestimmte Mitarbeiter von bestimmten Funktionen ausschließen zu können.



Gewichtung Funktionen bei Zugangsberechtigungssystem

Im Falle der Betreiber wurde die Bedeutung der einzelnen Funktionen bei Zugangsberechtigungen erhoben.



Die Umfrageteilnehmer wurden gebeten den folgenden Parametern einen Stellenwert zuzuordnen, wobei 1 wenig wichtig und 5 sehr wichtig bedeutet:

- Zeitliche Beschränkung der Zugangsmöglichkeit
- Verwendung von bereits bestehenden Zugangsberechtigungskarten
- Zentrales Verwalten einer Mitarbeiterdatenbank
- Blacklisting von Mitarbeitern

Generell ist die zeitliche Beschränkung der Zugangsmöglichkeit für die Betreiber von hoher Bedeutung. 62% der befragten Betreiber bewerten diese Funktion als sehr wichtig bzw. wichtig. 30% schreiben dieser Funktion eine durchschnittliche bzw. untergeordnete Rolle zu. Für 8% der Betreiber hat die zeitliche Beschränkung keine Relevanz.

An zweiter Stelle in der Reihung der Funktionalitäten steht die zentrale Verwaltung einer Mitarbeiterdatenbank, die für knapp die Hälfte der Betreiber wichtig bzw. sehr wichtig ist (49%). An

dritter Stelle wird die Verwendung von bereits bestehenden Zugangsberechtigungskarten genannt (31%) und erst an vierter und letzter Stelle rangiert das Blacklisting von Mitarbeitern, das nur für 21% der Betreiber eine wesentliche Funktion darstellt.

Resümee:

Mit einem Einfluss von 19% der Cyberattacken auf den OT Bereich, erkennt man eine steigende Bedeutung der Wichtigkeit zum Schutze dieses, für den wirtschaftlichen Fortbestand eines Unternehmens, wichtigen Bereichs. Der wirtschaftliche Schaden stellt die größte Sorge dar, gefolgt vom Diebstahl von Daten und/oder Rezepturen, oder aber böswilliger Veränderung von Rezepturen, was wiederum Einfluss auf Qualität, Reputation und damit wirtschaltfliche Probleme durch den Ausfall kompletter Chargen bzw. Rückrufen mit sich führt. Die Gewährleistung der Maschinensicherheit kommt erst an dritter Stelle. Die immer noch fehlende Mitarbeiter-Awareness hinsichtlich Security wird immer noch als sehr großes Risiko empfunden.

In Punkto der Zuständigkeiten gerade für den Bereich der OT-Security lassen die Antworten der Befragten auf nicht geklärte Verantwortlichkeiten schließen. Ebenso sehen sich noch viele unserer Befragten nicht entsprechend ausgebildet, um das Thema Security auf der OT-Ebene adäquat zu implementieren. Das zeigt auch die fehlende Kenntnis der Norm IN IEC 62443 und dass mehr als 50% der befragten noch nie ein Security Risk Assessment durchgeführt haben. Rund 40% der Befragten setzen keine industrielle Firewall ein, wobei die Hälfte als Begründung fehlendes Know-how angibt. Ebenso gering wird die Notwendigkeit zur Prüfung von Anomalien im Datenverkehr eingeschätzt.

Zusammenfassend kann festgehalten werden, dass die Auswirkungen der Maschinen-Produkte-Verordnung, die eben das Thema Cyber-Security“ von der Kür zur Pflicht macht, in den Unternehmen erst flächendeckend ausgerollt werden muss. Sowohl der aktuelle Kenntnisstand als auch das mangelnde Verständnis und fehlende Verantwortlichkeiten werden die Umsetzung der neuen Verordnung IN IEC 62443 erschweren.