3.7 Kleinere Unternehmen und deren integrierte Sicherheitspraxis

Kleine Unternehmen stehen vor der Herausforderung, dass sie nicht über die umfangreichen Ressourcen verfügen, die größeren Organisationen zur Verfügung stehen. Dennoch können auch sie effektiv integrierte Sicherheitspraktiken anwenden, indem sie speziell auf ihre Größe und Verhältnisse zugeschnittene Lösungen implementieren. Hier sind Beispiele, wie kleine Unternehmen integrierte Sicherheitskonzepte angehen können:

1. **Gemeinsame Sicherheitsschulungen:** Kleine Betriebe können Schulungen anbieten, die sowohl Arbeitssicherheit, Elektrosicherheit als auch IT-Sicherheit abdecken. Das könnte in Form von jährlichen Workshops geschehen, wo Mitarbeiter lernen, wie man sicher mit elektrischen Geräten umgeht, Erste Hilfe leistet und Passwörter sowie firmeninterne Daten schützt.
2. **Richtlinien und Prozeduren:** Auch wenn die Dokumentation nicht so umfangreich sein muss wie bei Großunternehmen, ist es wichtig, klar definierte Richtlinien und Prozeduren zu haben, die alle Sicherheitsbereiche abdecken. Diese sollten leicht verständlich und jederzeit zugänglich sein, um sicherzustellen, dass alle Mitarbeiter wissen, was im Falle eines Vorfalls zu tun ist.
3. **Integrierte Sicherheitssoftware-Lösungen:** Es gibt zahlreiche erschwingliche Software-Lösungen, die kleine Unternehmen nutzen können, um ihre Sicherheitsanforderungen zu verwalten. So können beispielsweise Arbeits- und IT-Sicherheitsprotokolle mit CRM-(Customer-Relationship-Management-) und Projektmanagement-Tools integriert werden, die Compliance-Tracking und die Meldung von Vorfällen erleichtern.
4. **Drittanbieter und Managed Services:** Kleinere Unternehmen können Drittanbieter für die Wartung und Sicherheitsüberwachung ihrer IT-Infrastruktur sowie für regelmäßige Elektrosicherheitsprüfungen nutzen. Managed Services können besonders vorteilhaft sein, um spezialisierte IT-Sicherheitskenntnisse einzubringen, die im Unternehmen selbst möglicherweise nicht vorhanden sind.
5. **Cross-Training:** In kleinen Teams ist es oft effizient, wenn Mitarbeiter mehrere Rollen übernehmen oder zumindest Grundkenntnisse in verschiedenen Bereichen haben. Ein Mitarbeiter könnte beispielsweise sowohl für die Wartung der Büro-IT als auch für die Sicherstellung der Einhaltung von Sicherheitsregeln am Arbeitsplatz zuständig sein.
6. **Nutzung von Standards und Best Practices:** Kleine Unternehmen müssen nicht alles von Grund auf neu erfinden. Sie können international anerkannte Standards und bewährte Praktiken wie ISO 27001 für Informationssicherheitsmanagement

oder OSHA-Richtlinien für Arbeitssicherheitsverfahren übernehmen und an ihre Bedürfnisse anpassen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet zudem mit dem BSI-Standard 200-3 ein Verfahren, mit dem Institutionen und kleine Unternehmen ihre Informationssicherheitsrisiken zielgerichtet steuern können.

7. **Regelmäßiges Feedback und kontinuierliche Verbesserung:** Feedback von Mitarbeitern kann genutzt werden, um Sicherheitsmaßnahmen kontinuierlich zu bewerten und zu verbessern. Dies kann in regelmäßigen Meetings oder durch anonyme Umfragen geschehen.

Durch die Anwendung dieser Praktiken können kleine Unternehmen ein robustes und integriertes Sicherheitssystem entwickeln, das die Herausforderungen und Ressourcen berücksichtigt, die für sie relevant sind.

Ein entscheidender Punkt für kleine Unternehmen ist die Flexibilität und Reaktionsfähigkeit ihrer integrierten Sicherheitspraktiken. Sie haben den Vorteil, dass weniger bürokratische Strukturen schnellere Entscheidungswege erlauben. Dies kann genutzt werden, um auf neue Sicherheitsbedrohungen effizient zu reagieren. Folgende Schritte können die Weiterentwicklung der integrierten Sicherheitspraktiken in kleinen Unternehmen unterstützen:

1. **Aktuelle Technologietrends beobachten:** Selbst in kleinen Unternehmen ist es wichtig, dass Verantwortliche für Sicherheitsaspekte über die neueste Technologie informiert sind. Beispielsweise könnte die Implementierung von Multi-Faktor-Authentifizierung (MFA) die IT-Sicherheit signifikant verbessern, ohne dass dies erhebliche Investitionen erfordert.
2. **Partnerschaften und Netzwerke:** Kleine Unternehmen können von Partnerschaften mit lokalen Behörden, Branchenverbänden und anderen Unternehmen profitieren. Durch diese Netzwerke können Wissen, Ressourcen und Best Practices effizient geteilt werden.
3. **Informations- und Ressourcenzentrale:** Eine zentrale Plattform, auf der Mitarbeiter auf Sicherheitsrichtlinien, Verfahrensanweisungen und Notfallpläne zugreifen können, ist von unschätzbarem Wert. Dies könnte eine interne Webseite, ein Intranet oder ein Cloud-System sein, abhängig von den spezifischen Ressourcen des Unternehmens.
4. **Incident Response Plan:** Jedes Unternehmen, unabhängig von seiner Größe, sollte einen klar definierten Plan für den Umgang mit Sicherheitsvorfällen haben. Dies schließt die Identifizierung von Bedrohungen, die Reaktion auf Vorfälle und die Kommunikationskette im Falle eines Ereignisses ein.

5. **Investition in Mitarbeiter:** Mitarbeiter sind oft die erste Verteidigungslinie gegen Sicherheitsbedrohungen. Investitionen in regelmäßige Schulungen sind unerlässlich, um das Bewusstsein zu schärfen und die Kompetenz im Umgang mit potenziellen Risiken zu stärken.
6. **Evaluierung der Wirksamkeit:** Integrierte Sicherheitsmaßnahmen sollten regelmäßig evaluiert werden, um ihre Effektivität sicherzustellen. Dies kann durch Simulationsübungen, Sicherheitsaudits oder Feedback-Sitzungen geschehen.
7. **Benutzerfreundliche Maßnahmen:** Sicherheitsmaßnahmen sollten praktikabel und benutzerfreundlich gestaltet sein, um von allen Mitarbeitern akzeptiert und befolgt zu werden. Komplexe Verfahren müssen vereinfacht werden, um sicherzustellen, dass sie im Alltag umsetzbar sind.

Durch die Anwendung dieser Maßnahmen können kleine Unternehmen einen kontinuierlichen Verbesserungsprozess einleiten, was langfristig nicht nur ein sicheres Arbeitsumfeld schafft, sondern auch das Vertrauen von Kunden und Geschäftspartnern in die Sicherheitsstandards des Unternehmens stärkt. Abschließend steht und fällt der Erfolg integrierter Sicherheitspraktiken mit der konsequenten Umsetzung und dem fortlaufenden Engagement auf allen Unternehmensebenen.

Die genaue Vorgehensweise wird im zweiten Teil dieses Buches beschrieben.

3.8 Inhalte und Abgrenzung von IT-Sicherheit, Elektrosicherheit und Arbeitssicherheit

Eine Übersicht soll verdeutlichen, dass keiner der drei Bereiche IT-Sicherheit, Elektrosicherheit und Arbeitssicherheit eine vollwertige Lösung des Praxisproblems der Cybersicherheit ist. Manche Punkte mögen sich überschneiden oder ähnlich auf den ersten Blick sein. Aber erst die Kombination der drei Bereiche schafft eine praxisnahe Sicherheit.

Im ersten Schritt sollen die Bereiche verglichen werden. Man erkennt in der Tabelle teilweise Überschneidungen, aber viele Einzelstellungsmerkmale, wenn am über den „IT-Suppenschüssel-Rand“ hinwegsieht:

IT-Sicherheit	Arbeitssicherheit + IT-Sicherheit	Elektrosicherheit + IT-Sicherheit	Elektrosicherheit + Arbeitssicherheit + IT-Sicherheit
Identitäts- und Zugriffs-management			
Netzwerksicherheit			
Endpunktsicherheit			
Verschlüsselung			
Sicherheitsbewusstsein	Sicherheitsbewusstsein der Mitarbeiter		Sicherheitsbewusstsein und Schulungen
Sicherheitsrichtlinien und -verfahren			
Sicherheitsüberwachung und -management			
Datenschutz	Schutz persönlicher Daten		
mobile Sicherheit	Fernarbeit und mobile Technologien		
	Kollaboration und Kommunikation		
Notfall- und Krisenmanagement	Notfall- und Krisenmanagement	Notfall- und Krisenmanagement	Notfall- und Krisenmanagement
		Vernetzung von Systemen	
		Steuerungssysteme und industrielle Kontrollsysteme	
		Schutz kritischer Infrastrukturen	Schutz kritischer Infrastrukturen
		Integration von Smart-Technologien	integrierte Systeme Automatisierung
		physischer Zugang zu Elektroanlagen	
			Arbeitssicherheit in technologisch fort-schrittlichen Umge-bungen
			Datenintegrität und -verfügbarkeit
	technologische Integration		

3.9 Was beinhaltet IT-Sicherheit?

Auch als Informationssicherheit oder IT-Sicherheit bezeichnet, ist es ein umfassendes Konzept, das darauf abzielt, Computersysteme, Netzwerke und Daten vor unautorisiertem Zugriff, Angriffen, Diebstahl, Zerstörung oder unbefugter Nutzung zu schützen. Das Hauptziel der Cybersicherheit ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen:

1. **Identitäts- und Zugriffsmanagement (IAM):** Die Kontrolle und Überwachung des Zugriffs auf Systeme und Daten durch Benutzer und Geräte.
2. **Netzwerksicherheit:** Maßnahmen zur Absicherung von Netzwerken, einschließlich Firewalls, Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS).
3. **Endpunktsicherheit:** Der Schutz von Endgeräten wie Computern, Laptops, Smartphones und anderen Geräten vor Malware, Viren und anderen Bedrohungen.
4. **Verschlüsselung:** Die Anwendung von Verschlüsselungstechnologien, um Informationen vor unbefugtem Zugriff zu schützen, insbesondere während der Übertragung.
5. **Sicherheitsbewusstsein:** Schulung und Sensibilisierung von Benutzern, um sicherzustellen, dass sie sich der potenziellen Bedrohungen bewusst sind und angemessen darauf reagieren können.
6. **Sicherheitsrichtlinien und -verfahren:** Die Entwicklung und Umsetzung von Sicherheitsrichtlinien und -verfahren, um den sicheren Umgang mit Informationen und Systemen zu gewährleisten.
7. **Incident Response und Forensik:** Die Fähigkeit, auf Sicherheitsvorfälle zu reagieren, diese zu untersuchen und Maßnahmen zu ergreifen, um zukünftige Vorfälle zu verhindern.
8. **Sicherheitsüberwachung und -management:** Die kontinuierliche Überwachung von Netzwerken und Systemen, um potenzielle Bedrohungen frühzeitig zu erkennen und darauf zu reagieren.
9. **Datenschutz:** Die Sicherstellung, dass personenbezogene Daten gemäß den Datenschutzbestimmungen geschützt werden.
10. **Mobile Sicherheit:** Maßnahmen zum Schutz von mobilen Geräten und den damit verbundenen Daten.

Die Bedeutung der IT-Sicherheit hat in den letzten Jahren aufgrund der zunehmenden Vernetzung und Digitalisierung in allen Lebensbereichen erheblich zugenommen.

Unternehmen, Regierungen und Einzelpersonen setzen verschiedene Technologien und Praktiken ein, um ihre digitalen Assets vor Cyberbedrohungen zu schützen.

Die erfolgreiche Integration von IT und OT erfordert eine enge Abstimmung zwischen den beiden Bereichen, den effektiven Einsatz von Cybersicherheitsstrategien und die Schaffung einer gemeinsamen technischen Architektur, um eine reibungslose Interoperabilität zu gewährleisten.

Die Integration von IT (Informationstechnologie) und OT (operative Technologie) findet in vielen Bereichen der Industrie und Unternehmensführung statt. Hier einige Beispiele, die diese Konvergenz veranschaulichen:

1. **Intelligente Fertigung (Smart Manufacturing):** In einem Smart Manufacturing-System können Produktionsmaschinen (OT) Daten über ihre Betriebszustände in Echtzeit an IT-Systeme übertragen. Diese Daten werden dann analysiert, um Effizienz zu steigern, Wartungsarbeiten vorherzusagen (Predictive Maintenance) und Ausfallzeiten zu minimieren. IT-Systeme können daraufhin Anpassungen an Maschineneinstellungen vornehmen oder selbstständig Serviceaufträge auslösen.
2. **Fernüberwachung und -steuerung von Energieanlagen:** Energieversorger integrieren IT- und OT-Systeme, um Stromnetze und andere Energiequellen fernzusteuern. Sensordaten von Windkraftanlagen oder Photovoltaiksolarpanels (OT) werden an zentrale IT-Netzwerke übermittelt, die Leistung und Effizienz überwachen. Bei Abweichungen können IT-Systeme automatisch Korrekturmaßnahmen einleiten, um die Energielieferung zu maximieren.
3. **Vernetztes Gesundheitswesen (Connected Healthcare):** In Krankenhäusern ermöglichen IT/OT-Integrationen, dass medizinische Geräte (OT) Patientendaten automatisch an elektronische Patientenakten (IT) senden. Das medizinische Personal erhält dadurch Echtzeitinformationen und kann auf Änderungen im Patientenzustand schneller reagieren.
4. **Intelligente Verkehrssteuerung:** Städte nutzen IT/OT-Integration, um den Verkehrsfluss zu optimieren. Verkehrssensoren und Kameras (OT) erfassen Verkehrsdichten und übermitteln diese Daten an Verkehrsleitzentralen (IT). Dort werden die Informationen analysiert und Ampelschaltungen oder Verkehrsleitsysteme dynamisch angepasst, um Staus zu vermeiden.
5. **Automatisierte Lagerverwaltung:** In modernen Lagerhäusern kommunizieren automatisierte Fördersysteme und Roboter (OT) mit Lagerverwaltungssoftware (IT). Dies ermöglicht eine effiziente Sortierung, Zusammenstellung und Lagerung von Waren. Die IT-Systeme koordinieren die Bewegungen automatisierter Geräte und sorgen dafür, dass die richtigen Produkte zur richtigen Zeit am richtigen Ort sind.

6. **Industrie 4.0 und das industrielle Internet der Dinge (IIoT):** Die vierte industrielle Revolution vereint IT und OT durch die Einrichtung vernetzter Systeme, die Echtzeitdaten austauschen. Mithilfe von IIoT-Sensoren können Betriebsdaten erfasst und über das Internet in Cloud-basierte IT-Systeme hochgeladen werden, wo sie zur Effizienzsteigerung, Qualitätskontrolle und Produktionsplanung genutzt werden.

Gehen wir einen Schritt weiter:

3.9.1 Was beinhaltet IT-Sicherheit kombiniert mit Arbeitssicherheit?

Ab in die Praxis: Die Verbindung zwischen IT-Sicherheit und Arbeitssicherheit liegt in der zunehmenden Digitalisierung von Arbeitsplätzen und Betrieben. Diese beiden Bereiche haben gemeinsame Schnittstellen und beeinflussen sich gegenseitig auf verschiedene Weisen:

1. **Technologische Integration:** Moderne Arbeitsplätze verwenden vermehrt digitale Technologien und vernetzte Systeme. IT-Sicherheit gewährleistet den Schutz dieser digitalen Infrastrukturen, während gleichzeitig Arbeitssicherheit sicherstellt, dass Mitarbeiter sicher mit diesen Technologien interagieren.
2. **Schutz persönlicher Daten:** IT-Sicherheit ist entscheidend, um personenbezogene Daten vor unbefugtem Zugriff und Missbrauch zu schützen. Dies betrifft nicht nur Kunden- oder Geschäftsdaten, sondern auch Mitarbeiterdaten. Arbeitssicherheit bezieht sich darauf sicherzustellen, dass persönliche Informationen der Mitarbeiter, insbesondere in digitalen Systemen, sicher und geschützt sind.
3. **Fernarbeit und mobile Technologien:** Die Zunahme von Fernarbeit und die Nutzung mobiler Technologien stellen neue Herausforderungen sowohl für die IT-Sicherheit als auch für die Arbeitssicherheit dar. Die Absicherung von Remote-Zugriffen und die sichere Nutzung von mobilen Geräten sind sowohl für den Schutz der Unternehmensdaten als auch für das Wohlbefinden der Mitarbeiter von Bedeutung.
4. **Sicherheitsbewusstsein der Mitarbeiter:** Schulungen und Sensibilisierung der Mitarbeiter sind sowohl in der IT-Sicherheit als auch in der Arbeitssicherheit wichtig. Mitarbeiter müssen sich der Gefahren bewusst sein, sei es in Bezug auf Phishing-Angriffe oder potenzielle Gefahren am physischen Arbeitsplatz.
5. **Kollaboration und Kommunikation:** Sichere Kommunikation und Kollaboration sind sowohl für die IT-Sicherheit als auch für die Arbeitssicherheit entscheidend. Plattformen für die Zusammenarbeit müssen sicher sein, um die Integrität

von Informationen zu gewährleisten und gleichzeitig sicherzustellen, dass die Mitarbeiter sicher und effektiv miteinander kommunizieren können.

6. **Notfall- und Krisenmanagement:** Sowohl in der IT-Sicherheit als auch in der Arbeitssicherheit ist ein gut durchdachtes Notfall- und Krisenmanagement von entscheidender Bedeutung. Dies beinhaltet die Fähigkeit, auf Sicherheitsvorfälle schnell zu reagieren, Schäden zu minimieren und die Kontinuität der Geschäfts- und Arbeitsprozesse sicherzustellen.

Die Integration von IT-Sicherheit und Arbeitssicherheit ist also notwendig, um eine umfassende Sicherheitsstrategie zu entwickeln, die sowohl die digitalen als auch die physischen Aspekte der Sicherheit am Arbeitsplatz abdeckt. Unternehmen sollten sicherstellen, dass ihre Sicherheitsmaßnahmen ganzheitlich sind und sowohl die digitale als auch die physische Sicherheit ihrer Mitarbeiter und Betriebsmittel berücksichtigen.

Und jetzt den Blick in Richtung Elektro:

3.9.2 Was beinhaltet IT-Sicherheit kombiniert mit Elektrosicherheit?

IT-Sicherheit und Elektrosicherheit sind zwei verschiedene Konzepte, die sich auf unterschiedliche Aspekte der Sicherheit konzentrieren, aber es gibt Bereiche, in denen sie miteinander verbunden sind:

1. **Vernetzung von Systemen:** Mit der zunehmenden Vernetzung von Elektrosystemen und Geräten, insbesondere im Kontext des sog. „Internet der Dinge“ (IoT), entstehen neue Herausforderungen für die IT-Sicherheit. Elektrosysteme, die mit Computernetzwerken verbunden sind, können anfällig für Cyberangriffe werden. Daher ist es wichtig, sowohl die physische Sicherheit von Elektrosystemen als auch deren IT-Sicherheit zu gewährleisten.
2. **Steuerungssysteme und industrielle Kontrollsysteme (ICS):** In vielen Branchen, einschließlich Energie, Fertigung und Verkehr, werden elektrische Systeme durch industrielle Steuerungssysteme gesteuert. Diese Systeme sind oft mit Netzwerken verbunden, was sie anfällig für Cyberangriffe macht. Die Sicherheit von elektrischen Steuerungssystemen ist daher eng mit der IT-Sicherheit verknüpft.
3. **Schutz kritischer Infrastrukturen:** Elektrizitätsnetze sind ein Beispiel für kritische Infrastrukturen, die für das Funktionieren moderner Gesellschaften entscheidend sind. Eine Beeinträchtigung der IT-Sicherheit kann direkt die Betriebsfähigkeit und Sicherheit elektrischer Systeme beeinflussen, was weitreichende Auswirkungen haben kann.

4. **Integration von Smart-Technologien:** Smart Grids und intelligente Elektrogeräte sind Beispiele für Technologien, die Elektrosicherheit und IT-Sicherheit miteinander verbinden. Die Kommunikation zwischen diesen intelligenten Geräten erfolgt oft über Netzwerke, was die Notwendigkeit erhöht, sowohl die Elektrosicherheit als **auch die IT-Sicherheit zu gewährleisten**.
5. **Physischer Zugang zu Elektroanlagen:** Elektrosicherheit bezieht sich oft auf physische Aspekte wie die Vermeidung von Stromschlägen und elektrischen Bränden. In einigen Fällen kann jedoch auch der Schutz vor physischem Zugang zu elektrischen Anlagen ein Element der IT-Sicherheit sein, um zu verhindern, dass Unbefugte physischen Zugriff auf Geräte erhalten, die Teil eines vernetzten Systems sind. Obwohl das dem Arbeitsschutz schon immer ein Anliegen sein sollte.

Insgesamt verdeutlichen diese Punkte, dass die Sicherheit elektrischer Systeme heute eine integrierte Perspektive erfordert, die sowohl die traditionellen Elektrosicherheitsaspekte als auch die Herausforderungen der Cybersicherheit berücksichtigt. Eine umfassende Herangehensweise ist entscheidend, um sowohl die physische Integrität als auch die digitale Sicherheit von Elektrosystemen zu gewährleisten.

Kommen wir zur „Königsklasse“:

3.9.3 Was verbindet die IT-Sicherheit mit Elektrosicherheit und Arbeitssicherheit?

Königsklasse: Die Verbindung zwischen Cybersicherheit, Elektrosicherheit und Arbeitssicherheit liegt in der **ganzheitlichen Betrachtung der Sicherheit** in verschiedenen Dimensionen.

1. **Integrierte Systeme und Automatisierung:** Moderne Elektrosysteme sind oft hochautomatisiert und miteinander vernetzt. Die Integration von Informationstechnologie (IT) in Elektrosysteme birgt jedoch das Risiko von Cyberangriffen. Durch die Sicherstellung der Cybersicherheit wird vermieden, dass Hacker elektrische Systeme beeinträchtigen und potenziell sicherheitskritische Vorfälle verursachen.
2. **Schutz kritischer Infrastrukturen:** Elektrische Systeme gehören zu den kritischen Infrastrukturen, deren Ausfall schwerwiegende Auswirkungen haben kann. Sowohl die Cybersicherheit als auch die Elektrosicherheit sind entscheidend, um einen kontinuierlichen und zuverlässigen Betrieb sicherzustellen und gleichzeitig physische Gefahren wie Stromschläge oder Brände zu minimieren.

3. **Arbeitssicherheit** in technologisch fortschrittlichen Umgebungen: In Bereichen, in denen fortschrittliche Technologien wie Robotik, Automatisierung und IoT eingesetzt werden, ist die Arbeitssicherheit eng mit der Elektrosicherheit verbunden. Darüber hinaus können Cyberangriffe auf diese Systeme nicht nur die Verfügbarkeit der Technologien beeinträchtigen, sondern auch direkt die Sicherheit der Arbeitsumgebung gefährden. Ein „um sich schlagender" Roboter ist wahrlich ein sehr schrecklicher Gegner jeder Arbeitssicherheitsbemühung.
4. **Datenintegrität und -verfügbarkeit:** In industriellen Umgebungen, einschließlich solcher, die mit Elektrosystemen verbunden sind, ist die Integrität und Verfügbarkeit von Daten entscheidend. Cyberangriffe können nicht nur zu Datenverlust führen, sondern auch die Genauigkeit von Messdaten und Steuerungsinformationen beeinträchtigen, was sich wiederum auf die Sicherheit der Arbeitnehmer auswirken kann.
5. **Sicherheitsbewusstsein und Schulungen:** Das Bewusstsein für Sicherheitsrisiken und Schulungen in den Bereichen Cybersicherheit, Elektrosicherheit und Arbeitssicherheit sind miteinander verbunden. Mitarbeiter müssen sich der Risiken bewusst sein und angemessene Maßnahmen ergreifen, um sich vor potenziellen Bedrohungen zu schützen.
6. **Notfall- und Krisenmanagement:** Sowohl bei Cyberangriffen als auch bei elektrischen Störungen ist ein effektives Notfall- und Krisenmanagement von entscheidender Bedeutung. Manchmal kommt auch beides zeitgleich daher. Die Integration von Plänen für den Umgang mit Cyberkrisen, elektrischen Ausfällen und Sicherheitsvorfällen am Arbeitsplatz ist wichtig, um schnell und effizient auf Notfälle reagieren zu können.

Die Verbindung zwischen diesen drei Bereichen unterstreicht die Notwendigkeit einer integrierten Sicherheitsstrategie, die verschiedene Dimensionen berücksichtigt, um ein umfassendes Sicherheitsumfeld zu schaffen. Unternehmen und Organisationen sollten sich bewusst sein, dass Schwächen in einem Bereich Auswirkungen auf die anderen haben können, und daher eine holistische Sicherheitsstrategie entwickeln. Anmerkung: Eine holistische Sicherheit basiert auf dem Systemdenken und beinhaltet die Betrachtung, wie die einzelnen Bestandteile eines Sicherheitssystems zusammenhängen und im Kontext größerer Systeme funktionieren. Also eigentlich die „praktische" Sicherheit.

4 Die VEFK und die Cybersicherheit

Die verantwortliche Elektrofachkraft (VEFK) und seine Elektrofachkräfte (EFK) spielen in erster Linie die maßgebliche Rolle im Bereich der Elektrosicherheit. Allerdings hat die zunehmende Vernetzung und Digitalisierung in vielen Branchen dazu geführt, dass auch die Cybersicherheit eine wichtige Rolle spielt. Insbesondere in industriellen Anlagen, in denen elektrische Systeme mit digitalen Steuerungssystemen verbunden sind, kann die Cybersicherheit eine kritische Komponente sein. Aber nicht nur dort! Jedes Arbeitsmittel, das im weitesten Sinn ferngesteuert, -gewartet oder auch nur ausgelesen werden kann, gehört in diesen Betrachtungsfokus.

Mit jeder Weiterentwicklung verändern sich zwangsläufig die Aufgaben einer VEFK. Wer unterstützt die VEFK seitens der Datensicherheit? Ist das seine Elektrofachkraft mit Spezialkenntnissen? Wer auch immer, dass hier ist Teamarbeit.

4.1 Verantwortlichkeiten

Die Verantwortlichkeiten für die Cybersicherheit in einem Unternehmen können je nach Größe, Struktur und Branche variieren. Es gibt jedoch bestimmte Rollen und Funktionen, die typischerweise mit der Verantwortung in größeren Unternehmen für die Cybersicherheit in Verbindung stehen:

- **Chief Information Security Officer (CISO):** Der CISO ist in vielen größeren Organisationen die Schlüsselfigur für Cybersicherheit. Diese Position ist für die Entwicklung, Umsetzung und Überwachung der gesamten Cybersicherheitsstrategie verantwortlich.
- **IT-Sicherheitsbeauftragter:** Dieser Mitarbeiter überwacht und implementiert Sicherheitsmaßnahmen im IT-Bereich. Der IT-Sicherheitsbeauftragte muss eng mit dem CISO zusammenarbeiten, um die Cybersicherheitsziele zu erreichen.
- **Netzwerkadministrator/IT-Administrator:** Administratoren spielen die wichtige Rolle bei der Sicherung von Netzwerken und Systemen, denn sie implementieren Sicherheitsrichtlinien, verwalten Zugriffsberechtigungen und überwachen das Netzwerk auf Anomalien hin.
- **Datenbanksicherheitsbeauftragter:** In Organisationen mit umfangreicher, meist personenbezogener Datenverarbeitung können Sicherheitsbeauftragte für Datenbanken sicherstellen, dass sensible Daten angemessen geschützt sind.

- **Compliance-Beauftragter:** In einigen regulierten Branchen ist ein Compliance-Beauftragter dafür verantwortlich, sicherzustellen, dass das Unternehmen die gesetzlichen Vorschriften und Branchenstandards in Bezug auf die Cybersicherheit einhält.
- **Mitarbeiter:** Alle Mitarbeiter spielen eine Rolle bei der Gewährleistung der Cybersicherheit. Hier sind Schulungen und Sensibilisierungsmaßnahmen extrem wichtig, um sicherzustellen, dass Mitarbeiter die Sicherheit am Arbeitsplatz verstehen und befolgen.

Was ist aber mit dem **OTler** und der **Fachkraft für Arbeitssicherheit**? Hierauf gehen wir später getrennt ein.

Die genaue Struktur und Benennung der Rollen können variieren. Viele Unternehmen neigen immer mehr dazu, eine klare Verantwortlichkeit für die Cybersicherheit festzulegen, um sicherzustellen, dass alle Aspekte des Sicherheitsmanagements abgedeckt sind. Das ist auch sehr empfehlenswert.

In kleineren Unternehmen kann eine Person möglicherweise mehrere dieser Rollen übernehmen. Es ist wichtig, dass die Verantwortlichen von dieser Aufgabe begeistert sind und regelmäßig geschult werden, um immer auf dem neuesten Stand und sensibel zu bleiben.

4.2 Hauptaufgabe ist die Klärung der Informationsschnittstelle

Früher konnte man relativ einfach den Anlagenbetreiber, den Anlagenverantwortlichen oder den Arbeitsverantwortlichen erkennen und festlegen. Trotzdem gab es immer wieder Irritationen und Haftungsprobleme. Das wird nun aber sehr viel schwerer. Wenn in der heutigen Zeit sich der Anlagenhersteller per Datenleitung zuwählt, um eine Fehleranalyse oder ein Software-Update zu fahren, und das vielleicht sogar unangekündigt passiert, ist die Rollenverteilung zwischen Anlagenbetreiber, Anlagenverantwortlichen und Arbeitsverantwortlichen nicht mehr durchsichtig. Oder wenn ein komplexes Arbeitsmittel gehackt wird und dadurch Ausfälle oder gar Personenschäden zu beklagen sind?

Die neuen, zusätzlichen Fragen für eine VEFK sind also beispielsweise:

- Müssen komplexe Anlagen immer eine ständig eine Datenleitung zum Serviceunternehmen haben? Und wie sicher ist diese aufgestellt?
- Kann man auf beiden Seiten der Datenleitung die Einwahl stoppen?
- Gibt es ein elektronisches „Logout-Tageout"-Verfahren, um zu wissen, wer gerade steuerungsmäßig den Zugriff hat?

- Welche der firmeninternen Daten sieht der Dienstleister?
- Ist die Maschine bzw. Anlage von „außen“ elektronisch erreichbar?
- Hat der Dienstleister die Aufgabe die Sicherheit ständig zu aktualisieren?
- Kann die Maschine über ihre Schnittstelle zum Einfalltor eines Hackerangriffs auf das Firmennetzwerk werden?

Wie zu erkennen ist, wird die Cybersicherheit ein wichtiger Punkt für die nächsten Jahre im elektrotechnischen Risikomanagement jeder VEFK. Ein sehr wichtiger!

4.3 Was kommt auf die VEFK bei vernetzten Arbeitsmitteln neu hinzu?

Die verantwortliche Elektrofachkraft könnte, nein sie wird also definitiv mit der Cybersicherheit in Berührung kommen. Sie muss sicherstellen bzw. dabei unterstützen, dass elektrische Systeme gegen Cyberangriffe geschützt sind, um Störungen oder potenziell gefährliche Situationen zu verhindern. Dies erfordert die Zusammenarbeit mit Fachleuten für Informationssicherheit. Also wird der Systemadministrator Schritt für Schritt zwangsweise einer der besten Freunde der VEFK. Es gilt gemeinsam die Umsetzung von Maßnahmen zum Schutz vor Cyberbedrohungen zu definieren, immer wieder zu überprüfen und den Mitarbeitern vor Ort verständlich zu vermitteln.

Insgesamt wird die Verbindung zwischen Elektrosicherheit und Cybersicherheit relevant, wenn elektrische Systeme digitalisiert sind oder in einer Weise betrieben werden, die eine Integration von Sicherheitsmaßnahmen auf beiden Ebenen erfordert. Das wird immer mehr der Fall sein.

4.3.1 Vorgehensweise

Um die Cybersicherheit im Kontext der Elektrofachkraft zu erhöhen, können beispielhaft folgende Maßnahmen ergriffen werden. Da aber jede VEFK sich in einem anderen Umfang in der Cybersicherheit wiederfindet, muss man die jeweils infrage kommenden Punkte für sich selbst raussuchen. Hier werden alle relevanten Punkte in der bestmöglichen Reihenfolge aufgelistet:

1. **Bewusstseinsbildung:**
   - Sensibilisierung des Personals für die Bedeutung von Cybersicherheit.
   - Schulungen zur Erkennung von Phishing-Angriffen und anderen Cyberbedrohungen.

2. **Zusammenarbeit mit IT- und Arbeitssicherheitsexperten:**
   - Enge Zusammenarbeit, um sicherzustellen, dass die elektrischen Systeme und Menschen angemessen geschützt sind.
   - Integration von Richtlinien und -Standards in die allgemeinen Sicherheitsprotokolle.
3. **Regelmäßige Sicherheitsprüfungen:**
   - Durchführung regelmäßiger Sicherheitsaudits und -prüfungen, um potenzielle Schwachstellen in den elektrischen und digitalen Systemen zu identifizieren.
   - Überwachung der Netzwerkkommunikation auf Anzeichen von Anomalien oder verdächtigem Verhalten.
4. **Software- und Firmware-Updates:**
   - Aktualisierung von Software und Firmware in elektrischen Systemen, um bekannte Sicherheitslücken zu schließen.
   - Überprüfung und Aktualisierung von Passwörtern und Zugriffsberechtigungen.
5. **Netzwerktrennung:**
   - Implementierung von Sicherheitszonen und Netzwerktrennung, um das Risiko von Cyberangriffen auf kritische Systeme zu minimieren.
6. **Notfallplanung:**
   - Entwicklung eines umfassenden Notfallplans für den Fall von Cyberangriffen.
   - Schulung des Personals für den Umgang mit Cybernotfällen und die rasche Wiederherstellung des Betriebs.
7. **Verschlüsselung:**
   - Einsatz von Verschlüsselungstechnologien, um die Vertraulichkeit (wenn notwendig) von übertragenen Daten sicherzustellen.
8. **Physische Sicherheit:**
   - Sicherstellung der physischen Sicherheit von Hardwarekomponenten, um unbefugten Zugriff zu verhindern.
9. **Richtlinien und Verfahren:**
   - Entwicklung und Umsetzung von klaren Richtlinien und Verfahren für die Cybersicherheit, die von allen Mitarbeitern eingehalten werden müssen.
10. **Regelmäßige Schulungen:**
    - Kontinuierliche Schulungen für die Elektrofachkraft und alle anderen beteiligten Mitarbeiter, um sie über die neuesten Bedrohungen und bewährten Sicherheitspraktiken auf dem Laufenden zu halten.

Die Umsetzung dieser Maßnahmen erfordert eine proaktive Haltung gegenüber Cybersicherheit und eine kontinuierliche Anpassung an neue Bedrohungen und Technologien. Durch die Integration von Cybersicherheitspraktiken in die täglichen Abläufe können Elektrofachkräfte dazu beitragen, die Integrität, Verfügbarkeit und Vertraulichkeit ihrer elektrischen Systeme zu gewährleisten.

5 Wer kann in der Praxis die Cybersicherheit unterstützen?

Reden wir über Verantwortlichkeiten. Vorweg sei erwähnt, dass der erste Adressant immer der Unternehmer, der jeweilige Vorgesetzte, der Behördenleiter oder ähnliche Personen mit Führungsaufgaben sind. Diese suchen sich wiederum zuverlässige und fachkompetente Personen, der Jurist spricht hier von „Verrichtungsgehilfen" und die tatsächliche Arbeit sachgerecht durchführen zu lassen. Sprich, hier kommen der Arbeitsschützer, der Informatiker und die Elektrofachkraft wieder zum Zuge. Warum? Weil nur sie es eben tatsächlich können.

Aber was können oder dürfen sie überhaupt?

5.1 Was kann eine Elektrofachkraft unternehmen, damit in seinem Bereich keine Cyberangriffe stattfinden könnten?

Als Elektrofachkraft ist es zwar nicht unbedingt die Hauptverantwortung, Cyberangriffe zu verhindern, da dies in den Bereich der IT-Sicherheit fällt, aber sie muss in ihrem Arbeitsbereich dennoch wichtige präventive Maßnahmen ergreifen, um das Risiko von Cyberangriffen zu reduzieren. Hier sind einige Strategien, die die Elektrofachkraft in dieser Reihenfolge verwenden könnte, um zur Cybersicherheit beizutragen:

1. **Bewusstsein schaffen:** Informieren über die Grundlagen der Cybersicherheit und die gängigen Arten von Cyberangriffen bei z. B. Arbeitsmitteln mit Schnittstellen (z. B. Phishing, Malware, Ransomware) um erkennen zu können, wie solche Angriffe aussehen. Das ist der erste Schritt zur Prävention.
2. **Sichere Passwörter nutzen:** Verwenden von starken, einzigartigen Passwörtern für alle Systeme und Geräte und regelmäßig ändern. Nicht nur beim PC!
3. **Aktualisierungen durchführen:** Sicherstellen, dass alle Systeme und Geräte mit der neusten Software und den aktuellen Sicherheitsupdates ausgestattet sind.
4. **Zugangskontrollen implementieren:** Beschränken des Zuganges zu sensiblen Systemen auf Befugte und entsprechende Authentifizierungsmechanismen.
5. **Sicherheitsrichtlinien folgen:** Unternehmensinterne IT- und OT-Sicherheitsvorschriften einhalten. Unterstützung der Mitarbeiter in diesem Arbeitsbereich.

6. **Regelmäßige Sicherheitsprüfungen:** Regelmäßige Prüfungen der elektrischen/elektronischen Systeme auf Sicherheitslücken oder solche Prüfungen anregen, wenn man es nicht selbst machen kann.
7. **Netzwerksicherheit:** Wenn Sie Zugang zu Netzwerkeinrichtungen haben, achten Sie darauf, dass angemessene Firewall- und Verschlüsselungstechnologien zum Einsatz kommen. Das gilt auch für die Verknüpfungen der Maschinen und Anlagen.
8. **Physische Sicherheit:** Sorgen, dass Räume mit sensiblen Geräten, Maschinen oder Netzwerken physisch gesichert sind bzw. der Zutritt kontrolliert wird.
9. **Schulung und Training:** Schulungen zum Thema Cybersicherheit besuchen und auf dem neuesten Stand bezüglich Sicherheits-Best-Practices sein.
10. **Notfallplanung:** Entwicklung und Kenntnisnahme von Notfallplänen für den Fall einer Sicherheitsverletzung.
11. **Kommunikation:** Informieren des Vorgesetzten oder die IT-Sicherheitsabteilung, wenn eine Sicherheitslücke oder verdächtige Aktivitäten bemerkt werden.

Die Elektrofachkraft kann nicht alle Aspekte der Cybersicherheit abdecken, aber durch proaktive Maßnahmen und das Bewusstsein für potenzielle Sicherheitsrisiken können die EFKs einen wertvollen Beitrag zur Sicherheit in ihrem Bereich leisten.

5.1.1 Beispiel Aufzug

Ein Aufzug, welcher eine IP-Serviceverbindung mit dem Hersteller hat, wird von außen gehackt. Welche Probleme können für den Aufzug und die Menschen im Aufzug entstehen?

Darüber denken die wenigsten nach! Ein Aufzug mit einer IP-Serviceverbindung, der von außen gehackt wird, kann eine Vielzahl von Problemen verursachen. Fahrgäste könnten durch eine übernommene Kontrolle der Steuerung Verletzungen oder Schäden erleiden, da der Hacker den Aufzug abrupt anhalten, starten oder die Geschwindigkeit ändern könnte. Dies könnte auch zur Folge haben, dass der Aufzug ausfällt und Menschen im Innenraum gefangen sind. Zusätzlich besteht die Gefahr von Datenschutzverletzungen, falls der Hacker Zugriff auf gesammelte Daten des Aufzugs erhält. Die Integrität der Betriebsdaten könnte durch Manipulation beeinträchtigt werden und zu fehlerhaften Wartungsentscheidungen führen, was langfristige Sicherheitsrisiken birgt.

Eine weitere Gefahr ist die mögliche Beschädigung der Aufzugshardware, was teure Reparaturen nach sich ziehen können. Sollten Kameras oder Mikrofone installiert sein, könnten diese zum Abhören oder Überwachen der Fahrgäste missbraucht werden,

was gravierende Eingriffe in die Privatsphäre darstellt. Ein solcher Vorfall schädigt das Vertrauen in den Hersteller und Betreiber des Aufzugs und kann zu rechtlichen Konsequenzen und Haftungsfragen führen. Des Weiteren könnte die Rufschädigung tiefgreifend sein und das Image des Unternehmens erheblich beeinträchtigen.

Es ist daher unerlässlich, dass Aufzugsbetreiber in effektive Sicherheitsmechanismen investieren, zu denen regelmäßige Software-Updates, die Verwendung von starker Verschlüsselung, das Monitoring des Netzwerktraffics und die gezielte Cybersicherheit-Schulung des Personals gehören, um solche Angriffe zu verhindern und die Sicherheit für Nutzer und Daten zu gewährleisten.

So, wer fährt nun noch sorgenfrei mit dem Aufzug? Okay, Aufmerksamkeit erreicht? Aber was kann man hier machen, wie kann man hier gegensteuern?

1. **Regelmäßige Wartung und Inspektionen:** Physische Wartungen sollten in regelmäßigen Abständen gemäß den Empfehlungen der Hersteller und den örtlichen Vorschriften durchgeführt werden. Dabei wird sichergestellt, dass mechanische Komponenten wie Seile, Rollen, Bremsen und Türen korrekt funktionieren und keine sichtbaren Anzeichen von Verschleiß oder Schäden aufweisen. Das ist keine neue Erkenntnis, dies sollte jeder Betreiber auf seiner Liste stehen haben!
2. **Upgrade von Hard- und Software:** Die Software der Steuerungssysteme muss regelmäßig aktualisiert werden, um Software-Schwachstellen zu beseitigen. Auch die Hardware sollte gegebenenfalls modernisiert werden, um sicherzustellen, dass sie aktuellen Sicherheitsstandards entspricht. Auch nicht so richtig Neues!
3. **Zugangsbeschränkungen für Steuerungssysteme:** Der Zugang zu den Aufzugssteuerungssystemen sollte strikt begrenzt und überwacht werden. Nur autorisierte Servicetechniker sollten physischen oder Remote-Zugang haben, wobei jede Zugangsanfrage dokumentiert werden muss.
4. **Implementierung von Netzwerksicherheit:** Für IP-basierte Fernwartungszugänge sind Netzwerksicherheitsmechanismen wie Firewalls, Intrusion Detection Systems und starke Authentifizierungsmethoden unerlässlich. Verschlüsselten Verbindungen, z. B. über VPNs, dienen dem Schutz vor unerlaubtem Zugriff.
5. **Ausbildung und Training:** Die Schulung von Betriebspersonal über Risiken, Sicherheitsprotokolle und Notfallverfahren ist entscheidend. Das Personal sollte lernen, wie mit Sicherheitsvorfällen umzugehen ist und wie verdächtige Aktivitäten zu erkennen und zu melden sind.
6. **Notfallpläne und Reaktionsstrategien:** Im Falle eines Sicherheitsvorfalls sollte ein klar definierter Plan vorhanden sein, der die Schritte für eine schnelle und effektive Reaktion vorgibt. Dies beinhaltet die Evakuierung von Passagieren, die Wiederherstellung des Betriebs und die Mitteilung an die betroffenen Parteien.

7. **Physische Sicherheitskontrollen:** Zugangskontrollsysteme und Überwachungskameras in und um den Aufzug unterstützen dabei, unberechtigten Zugang zu verhindern und bieten eine Möglichkeit zur Überprüfung im Falle von Vorfällen.
8. **Datenschutz und -integrität:** Daten, die von Aufzugssystemen gesammelt werden, sollten geschützt und regelmäßig auf Integrität geprüft werden. Richtlinien zum Datenschutz sollten implementiert und beachtet werden, um die Privatsphäre der Nutzer zu wahren.
9. **Partnerschaft mit Sicherheitsexperten:** Die Zusammenarbeit mit Cybersecurity-Experten und Spezialisten für physische Sicherheitseinrichtungen kann helfen, Risiken zu identifizieren und präventive Maßnahmen zu implementieren, die den neuesten Best Practices entsprechen.

Fazit: Vergessen wir unsere Aufzüge nicht!

Indem Aufzugsbetreiber diese bewährten Sicherheitspraktiken umfassend implementieren, können sie das Risiko von Unfällen und Sicherheitsverletzungen minimieren und sowohl für die Nutzerinnen und Nutzer des Aufzugs als auch für das Betreiberunternehmen ein hohes Maß an Sicherheit gewährleisten.

5.1.2 Aber wie macht das ein Hacker?

Ransomware-Attacken könnten z. B. die Kontrollsysteme von Aufzügen infizieren, um dann für die Freigabe der gesperrten Systeme ein Lösegeld zu fordern. Denial-of-Service-Angriffe wären ebenfalls eine Bedrohung, die Netzwerkkomponenten durch Überlastung zum Erliegen bringen könnten. Bei Man-in-the-Middle-Angriffen werden Informationen zwischen dem Aufzug und Kontrollsystemen abgefangen und manipuliert, was potenziell falsche Signale zur Folge hätte.

Die Kontrollpanels der Aufzüge könnten durch Hacking manipuliert werden, was eine ungeregelte Bewegung ermöglichen würde. Spoofing-Angriffe könnten durch Imitation von Wartungsdiensten unberechtigten Zugriff verschaffen, und eingeschleuste Schadsoftware könnte enormen Schaden anrichten. Spionage und Datendiebstahl sind reale Bedrohungen, die darauf abzielen, sensible Daten der Nutzer und des Betriebs zu sammeln.

Darüber hinaus sind viele Aufzugssteuerungen Teil des Internet of Things und können speziell auf IoT-Geräte ausgerichteten Angriffen ausgesetzt sein, die auf Schwachstellen in der Software abzielen. Supply-Chain-Angriffe stellen ein weiteres Risiko dar, indem bereits in der Produktionskette Schadsoftware oder Hintertüren in das Aufzugssystem eingebracht werden können.