Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössische Elektrizitätskommission ElCom
Fachsekretariat

Cyber-Sicherheit 2019

Bericht der ElCom

Bern, Februar 2019

Inhaltsverzeichnis

Abbildungsverzeichnis

Zusammenfassung

Durch Eigenverbrauch und -produktion, virtuelle Speicher und Kraftwerke wird die Energieversorgung zunehmend dezentraler und die Systemführung komplexer. Um diese Komplexität zu beherrschen und die wirtschaftlichen Chancen dieser Entwicklung zu nutzen, setzen die Energieversorger zunehmend informationstechnologische Mittel ein. Dies bedeutet nicht nur Internet of Things, Big Data oder Blockchain-Applikationen, sondern auch die informationstechnologische Vernetzung von Unterwerken, Trafostationen und Messstellen. Verstärkt wird diese Entwicklung mit der im Stromversorgungsgesetz (StromVG) vorgeschriebenen Einführung von intelligenten Messsystemen (Smart Meter). Die Stromnetze werden zunehmend durch intelligente Informations- und Kommunikationstechnologien gesteuert und überwacht. Diese Systeme bieten dem Netzbetreiber mehr Steuerungsmöglichkeiten und ermöglichen einen effizienteren Systembetrieb sowie die Möglichkeit neue Dienstleistungen anzubieten.

Aufgrund der zunehmenden informationstechnologischen Vernetzung steigt aber auch das Risiko, dass zum Beispiel Hacker in das Stromnetz eindringen und die Verfügbarkeit, Integrität oder Vertraulichkeit der Daten verletzen. Betrifft ein solcher Vorfall die IT, kann dies zu einem erheblichen finanziellen Schaden und vor allem zu einem Reputationsverlust für den betroffenen Netzbetreiber führen. Ist hingegen die Operational Technology (OT), die Betriebstechnologie, von einem Cyber-Vorfall betroffen, kann dies im Extremfall zu einem grossflächigen Stromausfall mit Verletzten oder sogar Toten sowie Umweltschäden führen. Somit wird die Cyber-Sicherheit ein zentrales Thema zur Gewährleistung einer sicheren Stromversorgung.

Der ElCom obliegt gemäss Artikel 22 Absatz 3 StromVG die Überwachung der Elektrizitätsmärkte im Hinblick auf eine sichere und erschwingliche Versorgung in allen Landesteilen. In Bezug auf die Cyber-Sicherheit bedeutet dies, dass die Netzbetreiber in der Lage sein müssen, die Lieferung an Nachlieger und Endkunden sicherzustellen und dass aufgrund eines Cyber-Vorfalles die Systemstabilität der Schweiz nicht gefährdet wird.

Um sich einen Überblick über die Situation zu verschaffen, hat die ElCom entschieden, die 92 grössten Netzbetreiber zu ausgewählten organisatorischen und technischen Cyber-Sicherheitsmassnahmen zu befragen. Im Fokus der Befragung stehen einerseits organisatorische Fragen zum Risikomanagement, zur Sensibilisierung der Mitarbeitenden oder zum Umgang mit externen Dienstleistern. Andererseits werden grundlegende technische Fragen zur Netzwerkarchitektur und zur Erkennung von Cyber-Vorfällen erhoben. Bei der Erarbeitung und Auswertung der Fragebogen orientierte sich die ElCom an bestehenden Standards, Empfehlungen und Branchendokumenten.

Gestützt auf die Ergebnisse der Umfrage, ist für die ElCom die Verbesserung der organisatorischen Massnahmen zentral: insbesondere die Erarbeitung von Richtlinien in den Bereichen Detektion und Vorfallsbewältigung, Schulungs- und Sensibilisierungsprogramme in Bezug auf die OT sowie die Begleitung und Überwachung von Wartungsarbeiten an kritischen Applikationen, sowohl vor Ort als auch über einen Fernzugriff. Bei den technischen Massnahmen erwartet die ElCom, dass die OT-Infrastruktur entsprechend dem aktuellen Stand der Technik geschützt wird und im Idealfall von der IT-Infrastruktur getrennt ist. Sollten diese Infrastrukturen nicht getrennt sein, sind Verbindungen entsprechend zu schützen und die OT-Systeme regelmässig auf Sicherheitslücken zu testen. Zudem sollte zur Erkennung von Cyber-Vorfällen insbesondere der OT-Netzwerkverkehr aufgezeichnet und überwacht werden. Im Zentrum der Massnahmen sollen dabei immer die Sicherstellung der Systemstabilität und die Lieferung an die Nachlieger sowie Endkunden stehen.

Aus den genannten Gründen erwartet die ElCom eine effiziente und risikobasierte Umsetzung der Branchendokumente «ICT Continuity», «Handbuch Grundschutz für Operational Technology in der Stromversorgung» und «Richtlinien für die Datensicherheit von intelligenten Messsystemen» des Verbandes Schweizerischer Elektrizitätsunternehmen gemäss dem Leitfaden «Schutz kritischer Infrastrukturen» des Bundeamtes für Bevölkerungsschutz. Weiter begrüsst die ElCom im Sinne der Subsidiarität die Bestrebungen, ein Branchen-CERT aufzubauen.

Résumé

La consommation et la production propres, le stockage virtuel et les centrales électriques conduisent à une décentralisation croissante de l'approvisionnement en énergie et une plus grande complexité de la gestion des systèmes. Afin de gérer cette complexité et de tirer parti des opportunités économiques offertes par cette évolution, les fournisseurs d'énergie ont de plus en plus recours aux technologies de l'information. Cela englobe non seulement l'Internet des objets, les mégadonnées (« Big Data ») ou des applications de type chaîne de blocs (« Blockchain »), mais aussi l'interconnexion des sous-stations ainsi que des stations de transformation et de mesure à l'aide des technologies de l'information. Cette évolution sera renforcée par l'introduction de systèmes de mesure intelligents (« Smart Meter ») prescrits par la loi sur l'approvisionnement en électricité (LApEl). Les réseaux électriques sont de plus en plus gérés et contrôlés par des technologies de l'information et de la communication intelligentes. Ces systèmes offrent au gestionnaire de réseau davantage de possibilités d'exploitation ; ils permettent un fonctionnement plus efficace du système et de proposer de nouveaux services.

Toutefois, l'interconnexion croissante liée aux technologies de l'information accroît aussi le risque que, par exemple, des pirates informatiques infiltrent le réseau électrique et portent atteinte à la disponibilité, à l'intégrité ou à la confidentialité des données. Si un tel incident affecte les systèmes informatiques ou IT (« Information Technology »), il peut entraîner un préjudice financier considérable et surtout nuire à la réputation du gestionnaire de réseau concerné. Si, en revanche, la technologie opérationnelle (« OT – Operational Technology ») est touchée par un cyberincident, cela peut, dans des cas extrêmes, conduire à une panne de courant à grande échelle avec des blessés, voire des morts, ainsi que des dommages environnementaux. La cybersécurité est donc un facteur déterminant de la sécurité de l'approvisionnement en électricité.

En vertu de l'article 22, alinéa 3 LApEl, l'ElCom surveille l'évolution des marchés de l'électricité en vue d'assurer un approvisionnement sûr et abordable dans toutes les régions du pays. Au niveau de la cybersécurité, cela signifie que les gestionnaires de réseau doivent être en mesure d'assurer la livraison aux clients en aval et aux clients finaux et de faire en sorte que la stabilité du système électrique suisse ne soit pas compromise par un cyberincident.

Afin d'avoir une vue d'ensemble de la situation, l'ElCom a décidé d'interroger les 92 plus grands gestionnaires de réseau au sujet de certaines mesures organisationnelles et techniques de cybersécurité. L'enquête s'est concentrée d'une part sur les questions organisationnelles liées à la gestion des risques, à la sensibilisation des collaborateurs et aux relations avec les prestataires de services externes. D'autre part, des questions techniques fondamentales relatives à l'architecture du réseau et à la détection des cyberincidents ont été collectées. Pour l'élaboration et l'évaluation des questionnaires, l'ElCom s'est appuyée sur les normes, recommandations et documents existants de la branche.

Au vu des résultats de l'enquête, l'amélioration des mesures organisationnelles est pour l'ElCom absolument centrale : en particulier l'élaboration de directives dans les domaines de la détection et de la gestion des incidents, des programmes de formation et de sensibilisation en lien avec l'OT ainsi que l'encadrement et la supervision des travaux de maintenance des applications critiques, tant sur place qu'à distance. En ce qui concerne les mesures techniques, l'ElCom s'attend à ce que l'infrastructure OT soit protégée conformément à l'état actuel de la technique et, dans l'idéal, qu'elle soit séparée de l'infrastructure informatique ou IT. Si ces infrastructures ne sont pas séparées, les connexions doivent être protégées de manière adéquate et les systèmes d'OT doivent être régulièrement testés pour en détecter les failles de sécurité. En outre, pour détecter les cyberincidents, il faudrait notamment enregistrer et surveiller le trafic du réseau OT. Les mesures devraient toujours être axées sur le maintien de la stabilité du système électrique et la fourniture aux clients en aval et aux clients finaux.

C'est pourquoi l'ElCom demande une application rigoureuse et basée sur les risques des documents de la branche « ICT Continuity », « Manuel Protection de base pour les « technologies opérationnelles » (OT) dans l'approvisionnement de base » et « Directives pour la sécurité des données des systèmes de mesure intelligents » de l'Association des entreprises électriques suisses conformément

au « Guide pour la protection des infrastructures critiques » de l’Office fédéral de la protection de la population. L’ElCom salue enfin les efforts déployés pour mettre en place un CERT de la branche conformément au principe de subsidiarité.

Sintesi

Grazie al consumo e alla produzione propri, alle centrali e allo stoccaggio virtuali, l'approvvigionamento elettrico è sempre più decentralizzato e la gestione del sistema sempre più complessa. Per governare questa complessità e sfruttare le opportunità economiche offerte da tale sviluppo, le aziende di approvvigionamento energetico si avvalgono sempre più spesso delle tecnologie informatiche. Questo significa non solo internet of things, big data o blockchain, ma anche il collegamento in rete informatico di sottostazioni, stazioni di trasformazione e punti di misurazione. Questo sviluppo sarà rafforzato dall'introduzione di sistemi di misurazione intelligenti (smart meter) prescritta dalla legge sull'approvvigionamento elettrico (LAEl). Le reti elettriche sono sempre più controllate e monitorate mediante tecnologie dell'informazione e della comunicazione intelligenti. Questi sistemi offrono al gestore di rete maggiori possibilità di controllo e consentono un esercizio più efficiente del sistema e la possibilità di offrire nuovi servizi.

Tuttavia, a causa della crescente interconnessione informatica, aumenta anche il rischio che, per esempio, degli hacker penetrino nella rete elettrica e violino la disponibilità, l'integrità o la riservatezza dei dati. Se un attacco di questo genere va a colpire l'informatica (IT), il danno finanziario può essere notevole e, soprattutto, il gestore interessato può subire un'importante perdita di reputazione. Se, invece, ad essere colpita è l'operational technology (OT), la tecnologia d'esercizio, nel peggiore dei casi si può verificare un'interruzione di corrente su larga scala con feriti, o addirittura morti, e danni ambientali. La cibersicurezza è quindi un elemento chiave per garantire un approvvigionamento elettrico sicuro.

Secondo l'articolo 22 capoverso 3 LAEl, la ElCom sorveglia l'evoluzione dei mercati dell'energia elettrica in vista di assicurare un approvvigionamento sicuro ed economicamente abbordabile in tutte le regioni del Paese. Per quanto riguarda la cibersicurezza, ciò significa che i gestori di rete devono essere in grado di garantire la fornitura ai gestori di rete a valle e ai clienti finali e che la stabilità del sistema svizzero non venga compromessa da un incidente informatico.

Per ottenere un quadro generale della situazione, la ElCom ha deciso di chiedere ai 92 maggiori gestori di rete informazioni su alcune misure organizzative e tecniche di sicurezza informatica. L'inchiesta si concentra sulle questioni organizzative relative alla gestione del rischio, alla sensibilizzazione dei collaboratori e ai rapporti con i fornitori di servizi esterni. D'altro canto, vengono rilevati aspetti tecnici fondamentali relativi all'architettura di rete e al rilevamento di attacchi informatici. Nell'elaborazione e nell'analisi dei questionari, la ElCom si è orientata agli standard, alle raccomandazioni e ai documenti settoriali esistenti.

Sulla base dei risultati dell'inchiesta, la ElCom ritiene fondamentale il miglioramento delle misure organizzative: in particolare l'elaborazione di direttive nei settori del rilevamento e della gestione degli eventi, la formazione e i programmi di sensibilizzazione in ambito OT nonché il monitoraggio e la supervisione dei lavori di manutenzione sulle applicazioni critiche, sia in loco che tramite accesso remoto. Per quanto riguarda le misure tecniche, la ElCom si aspetta che l'infrastruttura OT sia protetta secondo lo stato attuale della tecnica e, nel caso ideale, separata dall'infrastruttura IT. Se queste infrastrutture non sono separate, i collegamenti devono essere protetti adeguatamente e i sistemi OT devono essere regolarmente testati per valutarne la vulnerabilità. Inoltre, in particolare, il traffico di rete OT dovrebbe essere registrato e monitorato per rilevare gli attacchi informatici. Le misure dovrebbero sempre mirare a garantire la stabilità del sistema e la fornitura ai gestori di rete a valle a valle e ai clienti finali.

Per questi motivi, la ElCom si aspetta un'attuazione efficiente e basata sui rischi dei documenti di settore «ICT Continuity», «Handbuch Grundschutz für Operational Technology in der Stromversorgung» e «Richtlinien für die Datensicherheit von intelligenten Messsystemen» dell'Associazione delle aziende elettriche svizzere conformemente alla guida «Protezione delle infrastrutture critiche» dell'Ufficio federale della protezione della popolazione. Inoltre, nell'ottica della sussidiarietà, la ElCom guarda con favore agli sforzi per istituire un Computer Emergency Response Team (CERT) di settore.

1 Einleitung

In seinem Buch «Black Out» hat Marc Elsberg die möglichen Folgen eines Black Outs aufgrund einer Cyber-Attacke beschrieben. Dabei wird klar, dass ohne kritische Infrastrukturen und insbesondere Elektrizität eine moderne Gesellschaft kaum mehr funktionieren kann. Die Beurteilung, ob dies Fiktion oder in naher Zukunft eine reale Bedrohung ist, sei jedem selbst überlassen. Fakt ist aber, dass die Digitalisierung auch in der Elektrizitätsbranche angekommen ist. Unterwerke, Trafostationen und Messstellen werden informationstechnologisch vernetzt und mit der im Stromversorgungsgesetz (StromVG) vorgeschriebenen Einführung von intelligenten Messsystemen (Smart Meter) wird diese Vernetzung noch stärker zunehmen. Die Stromnetze werden zunehmend durch «intelligente» Informations- und Kommunikationstechnologien (IKT) gesteuert und überwacht. Diese Systeme bieten dem Netzbetreiber mehr Steuerungsmöglichkeiten und ermöglichen einen effizienteren Systembetrieb sowie die Möglichkeit, neue Dienstleistungen anzubieten. Aufgrund der zunehmenden informationstechnologischen Vernetzung steigt aber auch das Risiko, dass zum Beispiel Hacker in das Stromnetz eindringen und die Verfügbarkeit[1], Integrität[2] oder Vertraulichkeit[3] der Daten verletzen oder technische Anlagen zerstören. Betrifft ein solcher Vorfall die IT, kann dies zu einem erheblichen finanziellen Schaden und vor allem zu einem Reputationsverlust für den betroffenen Netzbetreiber führen. Ist hingegen die Operational Technology[4] (OT) von einem Cyber-Vorfall betroffen, kann dies im Extremfall zu einem grossflächigen Stromausfall mit Verletzten oder sogar Toten sowie Umweltschäden führen. Somit wird die Cyber-Sicherheit ein zentrales Thema zur Gewährleistung einer sicheren Stromversorgung.

Aufgrund der neuen Geschäftsmöglichkeiten, welche durch die Digitalisierung und informationstechnologischer Vernetzung bestehender Systeme möglich sind, wurden aber die Risiken, welche damit verbunden sind, bisher nicht entsprechend berücksichtigt. Historisch war die OT, wie zum Beispiel Supervisory Control and Data Acquisition (SCADA)-Systeme, als geschlossenes System gebaut. Die möglichen Fernzugriffe zur Wartung wurden nicht auf hohe OT-Sicherheit ausgelegt, sondern auf einen zuverlässigen lokalen Betrieb. Mit der fortschreitenden Digitalisierung werden diese Systeme nun informationstechnologisch gegen aussen vernetzt. Diese Entwicklung führt zu neuen Herausforderungen bei der OT-Sicherheit. Netzbetreiber und Regierungen haben dieses Problem erkannt und entsprechende Branchendokumente (VSE Branchendokumente) respektive Strategien oder Richtlinien erlassen (zum Beispiel Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken, Directive on security of network and information systems der EU).

1.1 Rechtliche Grundlagen

Im StromVG bestehen für die Netzbetreiber keine expliziten Auflagen in Bezug auf die Handhabung von IKT-Risiken. Gemäss Artikel 8 Absatz 1 Buchstabe a StromVG gewährleisten die Netzbetreiber ein sicheres, leistungsfähiges und effizientes Netz. Ebenso treffen die Netzbetreiber die erforderlichen Massnahmen, damit sie den festen Endverbrauchern in ihrem Netzgebiet jederzeit die gewünschte Menge an Elektrizität mit der erforderlichen Qualität und zu angemessenen Tarifen liefern können (Art. 6 Abs. 1 StromVG). Dies beinhaltet implizit auch Massnahmen zur IKT-Sicherheit. Diese wurde mit der Energiestrategie 2050 explizit im Energiegesetz (Artikel 7 Absatz 1) festgehalten. Es werden jedoch zum Beispiel keine Aussagen über einen zu erfüllenden Mindeststandard gemacht. Bezüglich der Kosten für Sicherheitsmassnahmen sind diese gemäss bisheriger Kommunikation der ElCom anrechenbar, solange sie zur Sicherstellung der IKT-Sicherheit gemäss aktuellem Stand der Technik notwendig und effizient sind. Dabei sind der aktuelle Stand der Technik gegeben und die Angemessenheit der durchzuführenden Massnahmen vom individuellen Schutzbedarf des jeweiligen Netzbetreibers abhängig.

[1] Verfügbarkeit bedeutet, dass die zu schützenden Systeme und Daten auf Verlangen einer berechtigten Einheit zugänglich und nutzbar sind.

[2] Integrität bedeutet zum einen die Richtigkeit und Vollständigkeit der verarbeiteten Daten und zum anderen die korrekte Funktionsweise der Systeme.

[3] Unter Vertraulichkeit wird der Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse verstanden.

[4] Operational Technology (OT) meint dabei Technologien, welche direkt für die Bereitstellung oder Lieferung von Elektrizität notwendig sind (z.B. SCADA, PIA, Fernzugriff auf Installationen in Unterwerken, Rundsteuerung, Energiedatenmanagement (EDM), Smart Meter).

Dazu ist der vom Bundesamt für Bevölkerungsschutz (BABS) erarbeitete Leitfaden «Schutz kritischer Infrastrukturen» ein gutes Hilfsmittel, um entsprechend effiziente Massnahmen zu definieren. Zudem hat der Verband Schweizerischer Elektrizitätsunternehmen (VSE) die Branchenempfehlungen «ICT Continuity», «OT Grundschutz» und «Handbuch Grundschutz für die Datensicherheit von intelligenten Messsystemen» erarbeitet, in welchen Hinweise zu Sicherheitsmassnahmen und -standards sowie deren Umsetzung gemacht werden.

Der ElCom obliegt gemäss StromVG Artikel 22 Absatz 3 die Überwachung der Elektrizitätsmärkte im Hinblick auf eine sichere und erschwingliche Versorgung in allen Landesteilen. In Bezug auf die Cyber-Sicherheit bedeutet dies, dass die Netzbetreiber in der Lage sein müssen, die Lieferung an Nachlieger und Endkunden sicherzustellen und dass aufgrund eines Cyber-Vorfalles die Systemstabilität der Schweiz nicht gefährdet wird.

1.2 Ziel der Umfrage, Stichprobe und Fragebogen

Im Fokus der Befragung stehen einerseits organisatorische Fragen zum Risikomanagement, zur Sensibilisierung der Mitarbeitenden oder zum Umgang mit externen Dienstleistern. Andererseits werden grundlegende technische Fragen zur Netzwerkarchitektur und zur Erkennung von Cyber-Vorfällen erhoben. Dieser Überblick dient der ElCom als Grundlage, das weitere Vorgehen zu planen. Die Erkenntnisse aus der Auswertung der Umfrage sowie die daraus abgeleiteten Empfehlungen sollen mit den entsprechenden Akteuren des Bundes koordiniert und dadurch eine Verbesserung der Cyber-Resilienz erzielt werden.

Daher hat sich die ElCom entschieden, die 92 grössten Netzbetreiber zu ausgewählten organisatorischen und technischen Cyber-Sicherheitsmassnahmen zu befragen. Die Energieausspeisung der 92 ausgewerteten Verteilnetzbetreiber entspricht rund 89 Prozent der von allen Schweizer Verteilnetzbetreibern ausgespeisten Energie (Energieumsatz). Diese Stichprobe deckt aus Sicht der ElCom die für die Versorgungssicherheit relevanten Netzbetreiber ab.

Bei der Erarbeitung des Fragebogens orientierte sich die ElCom an bestehenden Standards, Empfehlungen und Branchendokumenten. Der Fragebogen besteht aus geschlossenen Fragen (Auswahlmenu) und einem Bemerkungsfeld. Aufgrund der regulatorischen Effizienz mussten nicht alle Verteilnetzbetreiber den vollständigen Fragebogen komplettieren: Der zweite Teil musste nur von Netzbetreibern, welche auf den Netzebenen 1 bis 4 tätig sind, ausgefüllt werden. Dieser Teil beinhaltete weitergehende Fragen bezüglich der IT-/OT-Sicherheit sowie Fragen zu Richtlinien und Zertifizierung. Daher kann es sein, dass sich die Antworten nicht immer auf die gesamte Stichprobegrösse addieren. Zudem wurden bei der Datenaufbereitung unlogische Antworten wo möglich korrigiert beziehungsweise ergänzt.

2 Auswertung

Das nachfolgende Kapitel beschreibt die die Umfrageresultate. Im ersten Abschnitt wird kurz die physische und informationstechnologische Vernetzung der befragten Netzbetreiber aufgezeigt. Der zweite Abschnitt befasst sich mit der organisatorischen Ebene und der letzte Abschnitt zeigt die Umfrageresultate der technischen Ebene.

2.1 Physische und informationstechnologische Vernetzung

Aufgrund der historischen Entwicklung der Schweizer Stromversorgung betreiben 21 Netzbetreiber gemeinsame Unterwerke mit Swissgrid und 74 Netzbetreiber haben untereinander gemeinsam genutzte Unterwerke. Die dadurch entstehenden Schnittstellen erhöhen die Herausforderungen, den physischen Zugang und Schutz der Anlagen sowie der installierten Informatik zu regeln. 18 Netzbetreiber haben keine gemeinsam genutzten Unterwerke (vgl. Abbildung 1, blaue Balken). Neben dem physischen Schutz der Anlagen ist auch die informationstechnologische Vernetzung (zum Beispiel über den Partner Informationsaustausch (PIA)) für die Cyber-Sicherheit entscheidend. Dies aufgrund der Möglichkeit, sich über ein System Zugang zu weiteren Systemen zu verschaffen. 14 Netzbetreiber sind informationstechnologisch direkt mit Swissgrid verbunden und 53 Netzbetreiber sind untereinander vernetzt. 38 Netzbetreiber sind nicht mit anderen Netzbetreibern vernetzt (vgl. Abbildung 1, orange Balken).

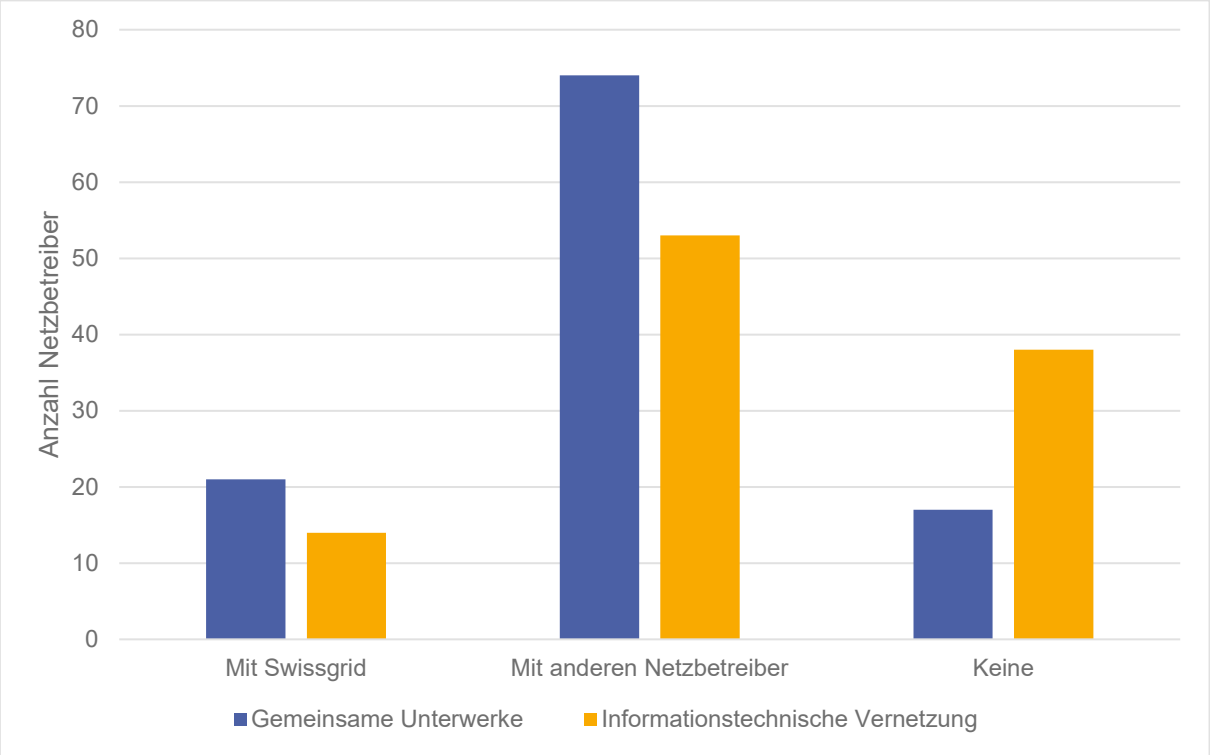

Abbildung 1: Physische und informationstechnische Vernetzung

Neben der physischen und informationstechnologischen Vernetzung unter den Netzbetreibern birgt auch die Vernetzung mit den Endkunden ein Risiko. So geben 64 Netzbetreiber an, dass sie «Smart Meter» einsetzen. In der Umfrage wurde «Smart Meter» dabei als elektronischen Elektrizitätszähler nach Artikel 8a Absatz 1 Buchstabe a der Stromversorgungsverordnung (StromVV) definiert. 23 Netzbetreiber setzten noch keine «Smart Meter» ein. Von den 64 Netzbetreiber mit «Smart Meter» setzen 22 Netzbetreiber «Smart Meter» mit Circuit-Breaker ein und von diesen ist nur gerade bei 9 Netzbetreibern diese Funktion deaktiviert (vgl. Abbildung 2).

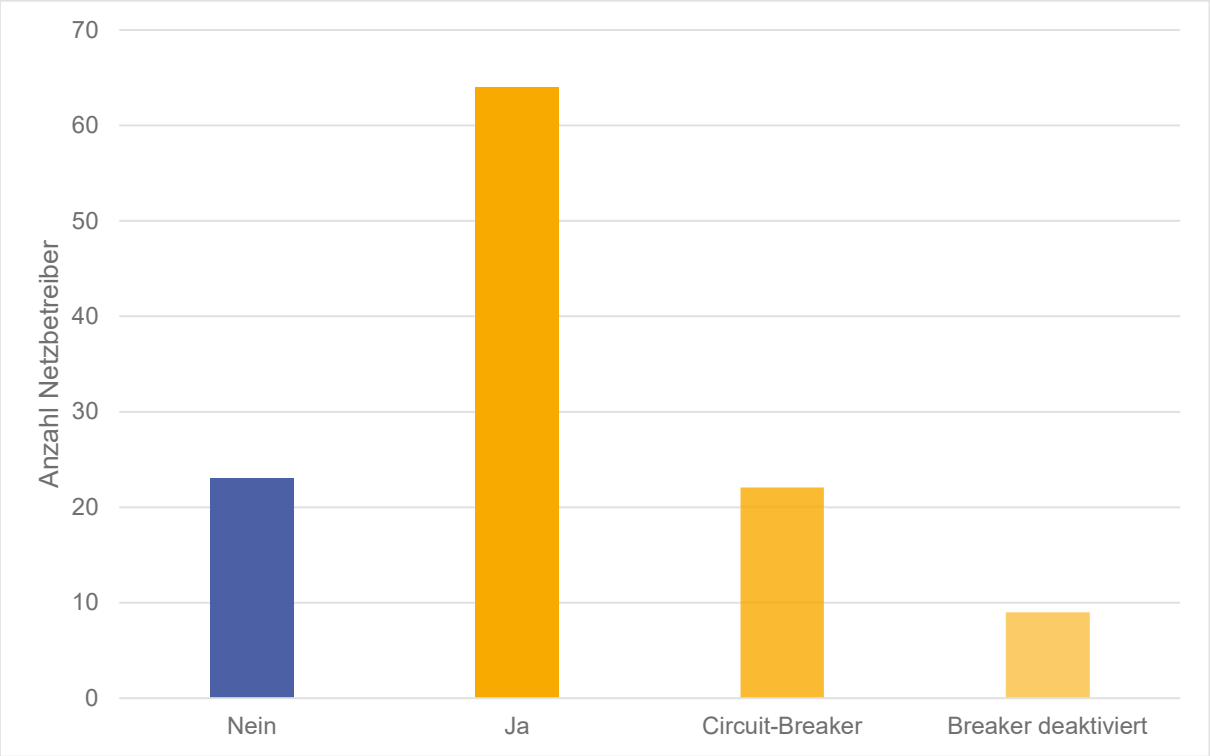

Abbildung 2: Verbreitung von Smart Meter

2.2 Organisatorische Ebene

Dieser Abschnitt soll einen Überblick über den Stand der getroffenen Schutzmassnahmen auf organisatorischer Ebene geben. Insbesondere liegt der Fokus dabei auf dem Risikomanagement und der Sensibilisierung der Mitarbeitenden sowie der Umgang mit externen Dienstleistern.

2.2.1 Risikomanagement

Effektive Cyber-Sicherheit beginnt mit dem Gefahrenbewusstsein in der Geschäftsleitung, denn Cyber-Sicherheit braucht Ressourcen. Ohne entsprechende Strukturen und Mittel lassen sich keine effizienten Cyber-Sicherheitsmassnahmen umsetzen. Dies beginnt mit einer Risikoanalyse und der Definition der aus Sicht der Geschäftsleitung tragbaren Restrisiken. Aus der Risikoanalyse folgen schlussendlich die notwendigen Massnahmen. Dabei ist wichtig, dass Cyber-Sicherheit als Prozess verstanden wird.

Abbildung 3 zeigt, von welchen Cyber-Risiken die Netzbetreiber ausgehen. Die Netzbetreiber gehen hauptsächlich von fahrlässig handelnden Mitarbeitenden aus. Gefolgt vom Verlust der Verfügbarkeit, Vertraulichkeit und Integrität der Daten. Weiter gehen die Netzbetreiber von einem APT als Bedrohung aus. Weniger wichtig scheint die Bedrohung durch Mitarbeitende, welche vorsätzlich Daten weitergeben oder Schaden anrichten.

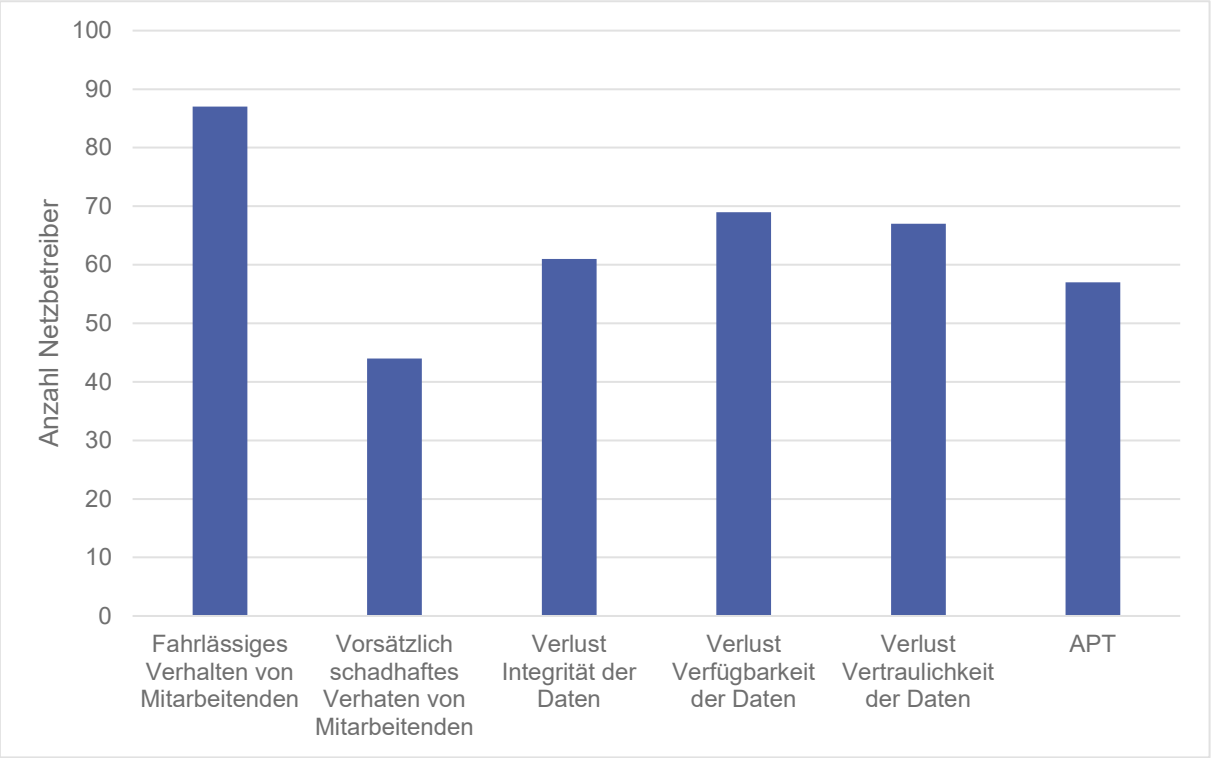

Abbildung 3: Angenommene Cyber-Risiken

Wie aus untenstehender Abbildung 4 zu sehen ist, glauben 71 Netzbetreiber, dass sie 2017/2018 von keinem Cyber-Vorfall betroffen waren. «Glauben», weil es durchaus sein kann, dass ein Netzbetreiber von einem Cyber-Vorfalle betroffen war, diesen aber nicht bemerkte (zum Beispiel Kopieren von vertraulichen Daten). 21 Netzbetreiber waren in dieser Periode von einem Cyber-Vorfall betroffen. Das Spektrum der Cyber-Vorfälle reicht von fahrlässigen Mitarbeitenden, Malware (Ransomware) bis in einem Fall zu einem Advanced Persistent Threat (APT). Dabei war nicht direkt der Netzbetrieb, sondern ein anderer Teil des Stadt- oder Verbundwerkes betroffen. Dies zeigt, dass auch schwerere Cyber-Vorfälle beim Risikomanagement nicht ausser Acht gelassen werden dürfen. Bei APT ist zu beachten, dass diese nur sehr schwer erkennbar sind.

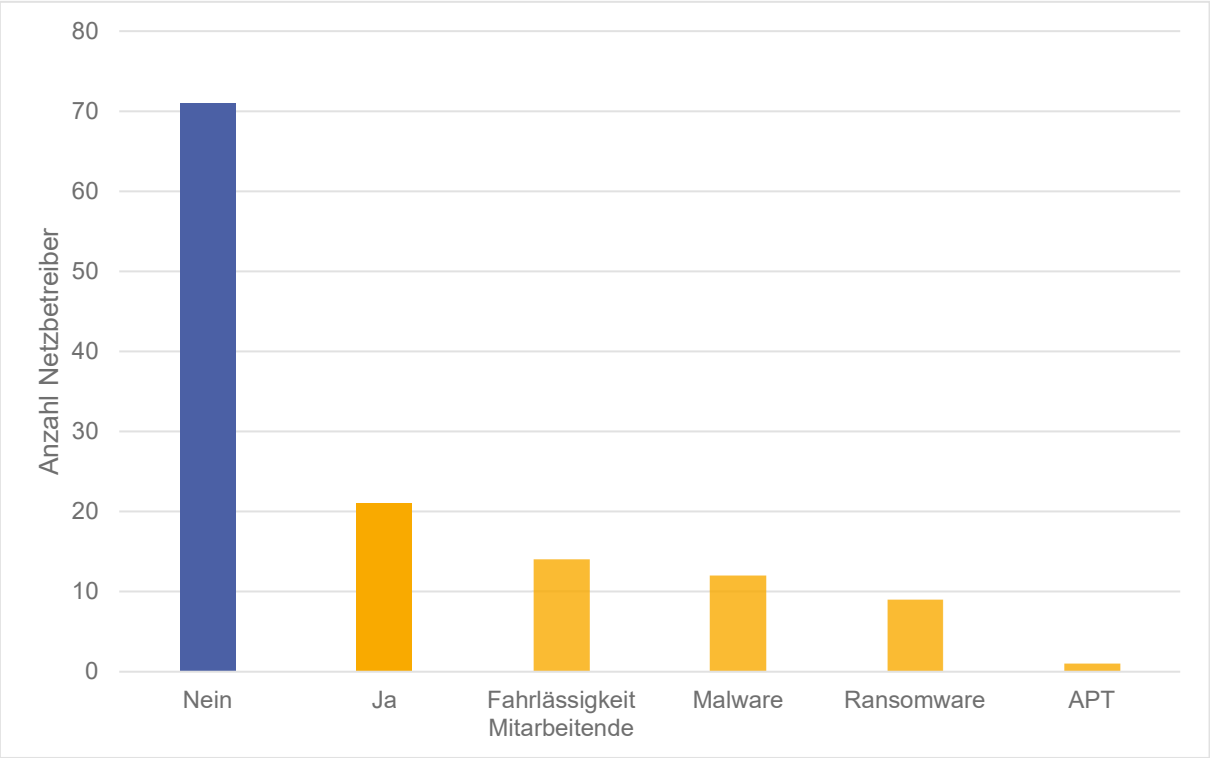

Abbildung 4: Betroffenheit und Art von Cyber-Vorfällen

Abbildung 5 zeigt, dass bei 21 Netzbetreibern Cyber-Sicherheit regelmässig, bei 38 Netzbetreibern nach Bedarf und bei 25 Netzbetreibern sowohl regelmässig als auch nach Bedarf thematisiert werden. Bei 6 Netzbetreibern werden diese Themen nach Bedarf nicht in der Geschäftsleitung, sondern innerhalb der IT-Abteilung oder durch einen spezifischen Ausschuss thematisiert. Ein Netzbetreiber hat angegeben, dass Cyber-Sicherheit momentan kein Thema sei. Häufig ist die Cyber-Sicherheit Teil des Risikomanagements der Unternehmen und wird jährlich besprochen.

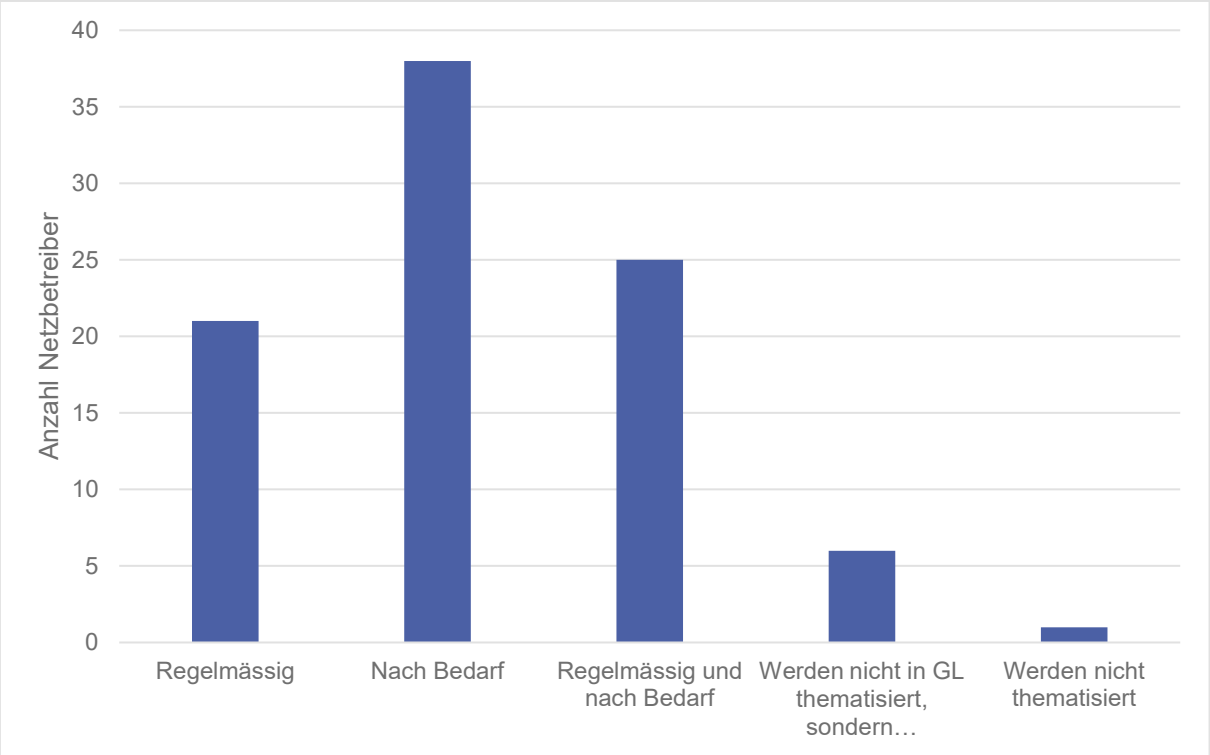

Abbildung 5: Cyber-Sicherheit in Geschäftsleitung thematisiert

Die Umsetzung von organisatorischen Cyber-Sicherheitsmassnahmen erfolgt über entsprechende Prozesse und Massnahmen. Diese sind wiederum in Richtlinien beschrieben. 70 Netzbetreiber geben an, dass sie für die von ihnen angenommen Gefahren entsprechende Prozesse, Richtlinien oder Massnahmen in den Bereichen Prävention, Detektion, Incident Reponse oder Recovery definiert haben. Am häufigsten werden dabei Richtlinien zur Recovery und Prävention genannt, gefolgt von Richtlinien bei der Detektion. Am schlechtesten dokumentiert sind die Netzbetreiber bei der Incident Response, also der Behebung des Cyber-Vorfalls (vgl. Abbildung 6). Hier ist bemerkenswert, dass 22 Netzbetreiber über keine Richtlinien und Massnahmen verfügen.

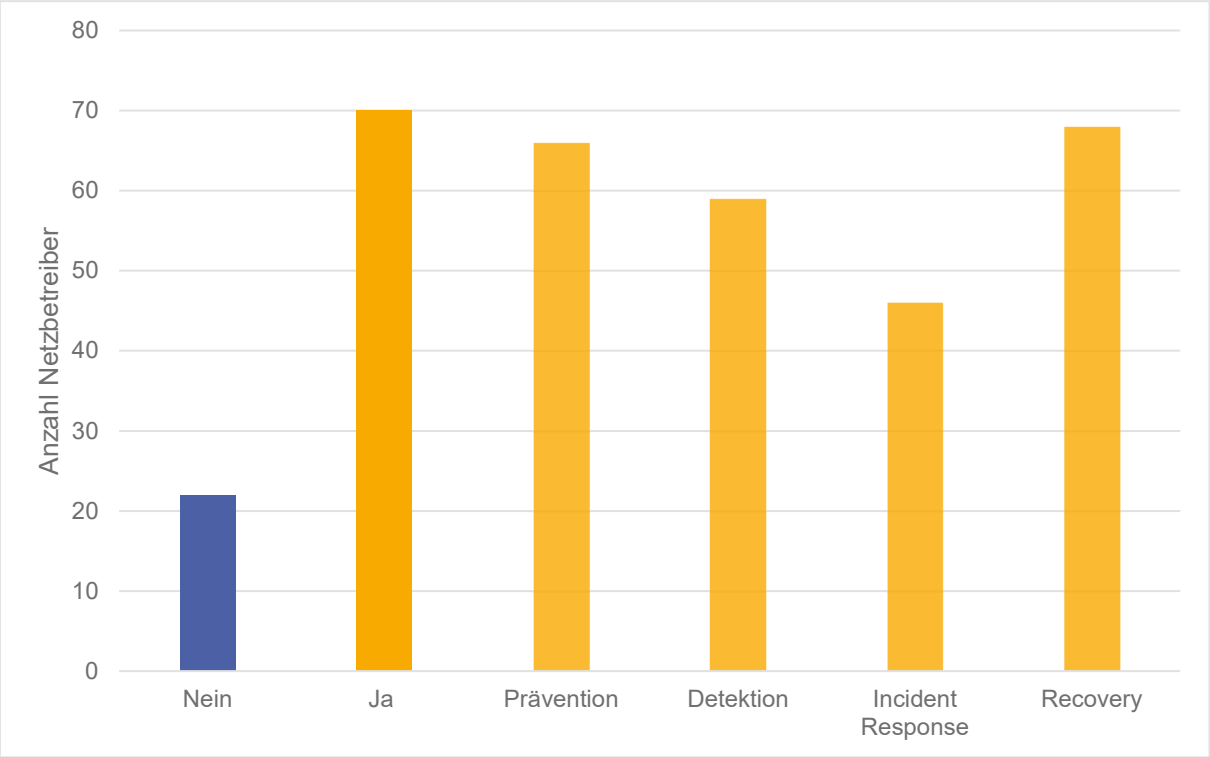

Abbildung 6: Richtlinien vorhanden

Eine vertiefte Auswertung zeigt, dass in der Regel im Bereich der IT[5] mehr sicherheitsrelevante Richtlinien und Weisungen bestehen als bei der OT[6]. Richtlinien über den physischen Zugang zu kritischen Anlagen werden gleichermassen genannt (vgl. Abbildung 7).

[5] Information Technology (IT) meint dabei Technologien zur Datenverarbeitung, welche nicht direkt mit der Bereitstellung von Elektrizität zu tun haben (z.B. Kundendatenmanagement, Personaldatenmanagement, Büroanwendungen).

[6] Operational Technology (OT) meint dabei Technologien, welche direkt für die Bereitstellung oder Lieferung von Elektrizität notwendig sind (z.B. SCADA, PIA, Fernzugriff auf Installationen in Unterwerken, Rundsteuerung, Energiedatenmanagement (EDM), Smart Meter).

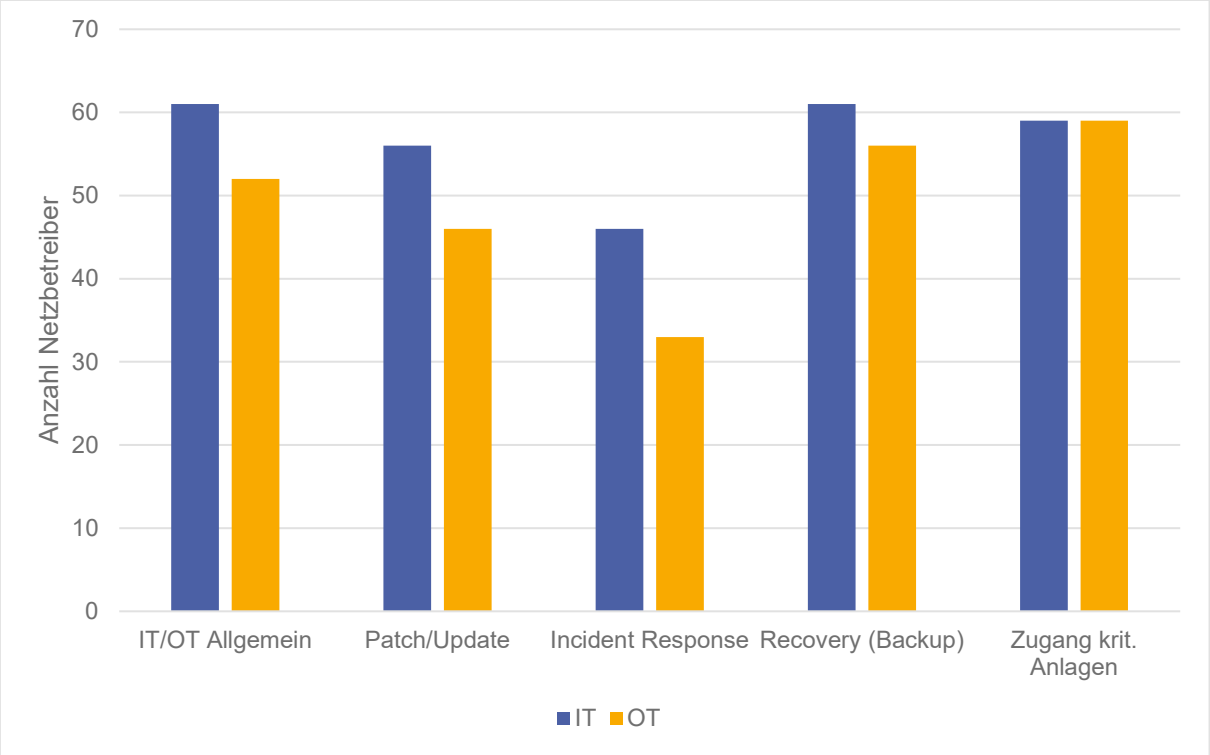

Abbildung 7: Sicherheitsrelevante Richtlinien und Weisungen

Eine Zertifizierung im Bereich der Cyber-Sicherheit soll Vertrauen in das entsprechende Unternehmen schaffen. 4 Netzbetreiber sind nach ISO 27001 / 27002 zertifiziert. Von den 63 Netzbetreibern welche angeben, dass sie nicht zertifiziert sind, streben 12 Netzbetreiber eine Zertifizierung nach ISO 2700x an (vgl. Abbildung 8).

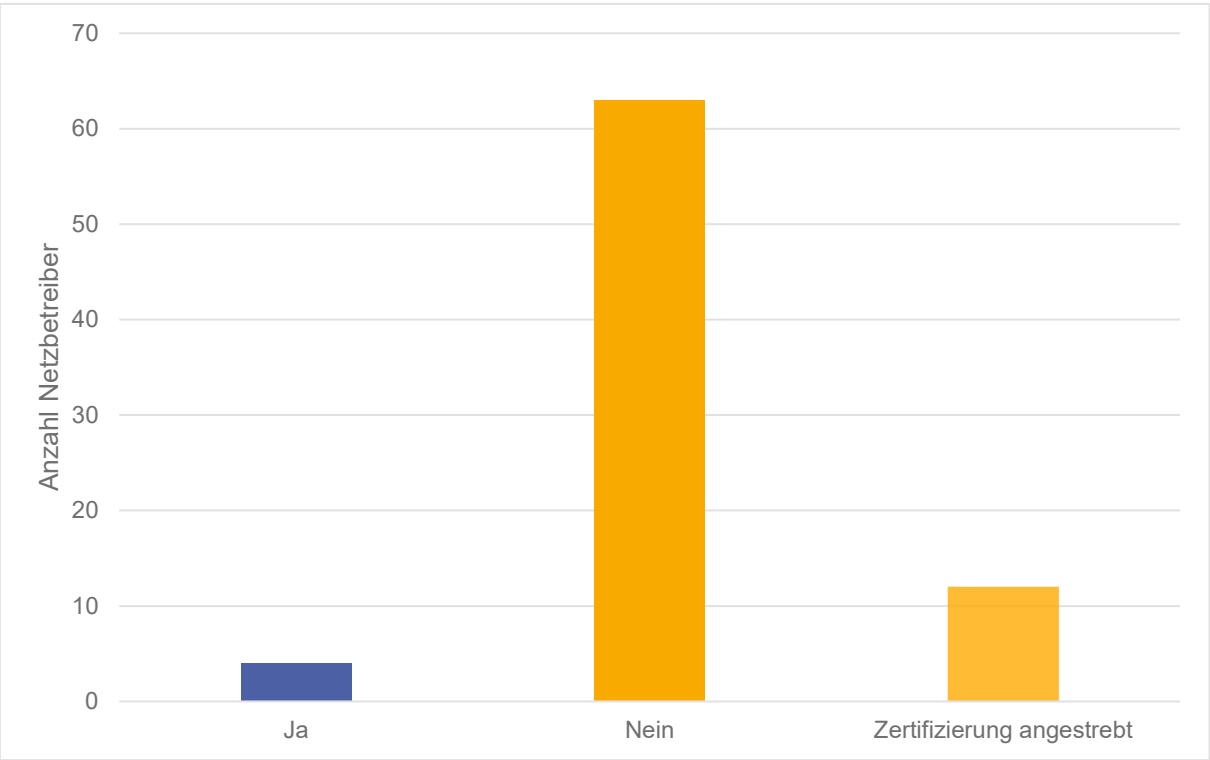

Abbildung 8: Zertifizierung Netzbetreiber

Abbildung 9 zeigt, an welchen Standards sich die Netzbetreiber bei der Erstellung ihrer Richtlinien orientieren. Dabei sind nur Standards aufgezeichnet, welche mindestens zweimal genannt wurden. Bei der Umsetzung von Cyber-Sicherheitsmassnahmen orientieren sich die Netzbetreiber auf der organisatorischen Ebene und bei Richtlinien zur IT mehrheitlich an internen Richtlinien oder am ISO 2700x sowie

dem Standard der National Institute of Standards and Technology (NIST) respektive dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Bei Richtlinien, welche die OT betreffen, orientieren sich die Netzbetreiber ebenfalls mehrheitlich an internen Richtlinien sowie ISO 2700x und dem IT-Grundschutz des BSI aber zusätzlich am VSE Branchendokument «ICT Continuity» und dem entsprechenden White Paper des Bundesverband der Energie- und Wasserwirtschaft (BDEW). Zudem fällt auf, dass im Bereich OT eine grössere Anzahl an Normen und Standards berücksichtigt werden als bei der IT.

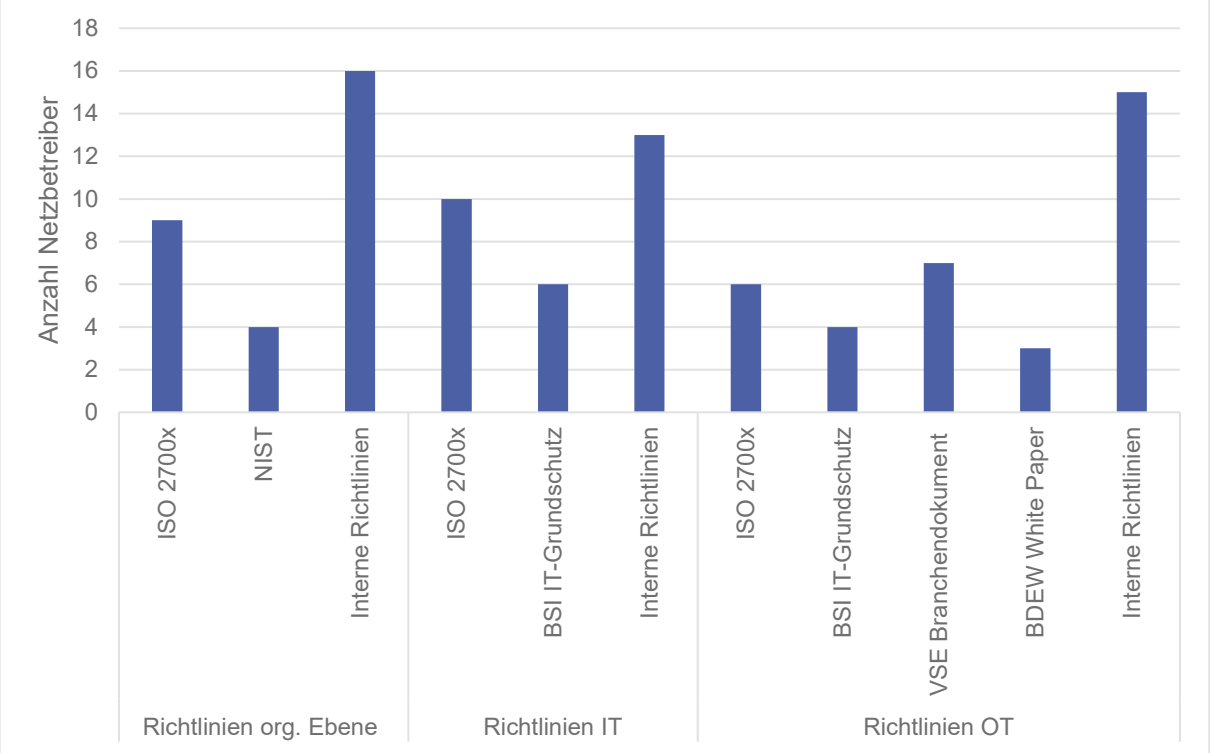

Abbildung 9: Berücksichtigte Dokumente / Standards Cyber-Sicherheit

Abbildung 10 zeigt, dass die meisten Netzbetreiber ihre Sicherheitsmassnahmen ad hoc anpassen. Nur gerade 2 Netzbetreiber reagieren nicht auf Vorfallsmeldungen oder passen ihre Massnahmen nicht regelmässig an. Bei den regelmässigen Anpassungen reicht die Zeitspanne von monatlich bis jährlich. Weiter ist festzuhalten, dass mehrere Netzbetreiber sowohl ad hoc wie auch regelmässige Anpassungen bei den Sicherheitsmassnahmen vornehmen.

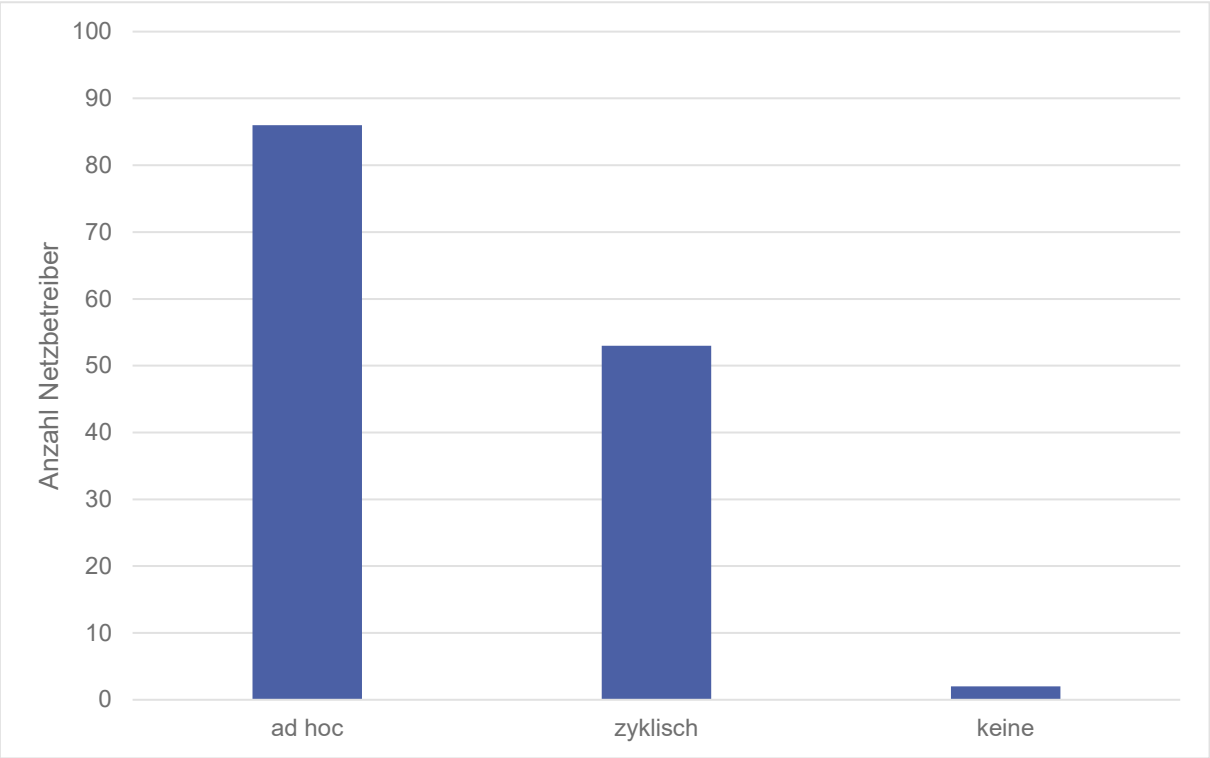

Abbildung 10: Anpassung der Sicherheitsmassnahmen

Um bei einem Cyber-Vorfall den Systembetrieb möglichst unterbruchfrei zu gewährleisten, ist eine Redundanz der Netzleitsysteme unumgänglich. Dabei geben 14 Netzbetreiber an, dass ihre Netzleitsysteme nicht redundant ausgelegt sind. Von den 76 Netzbetreibern, welche über ein redundantes System verfügen, haben 19 Netzbetreiber ihre Netzleitsysteme georedundant ausgelegt. 53 Netzbetreiber haben Redundanzen mit unterschiedlicher Technologie (vgl. Abbildung 11).

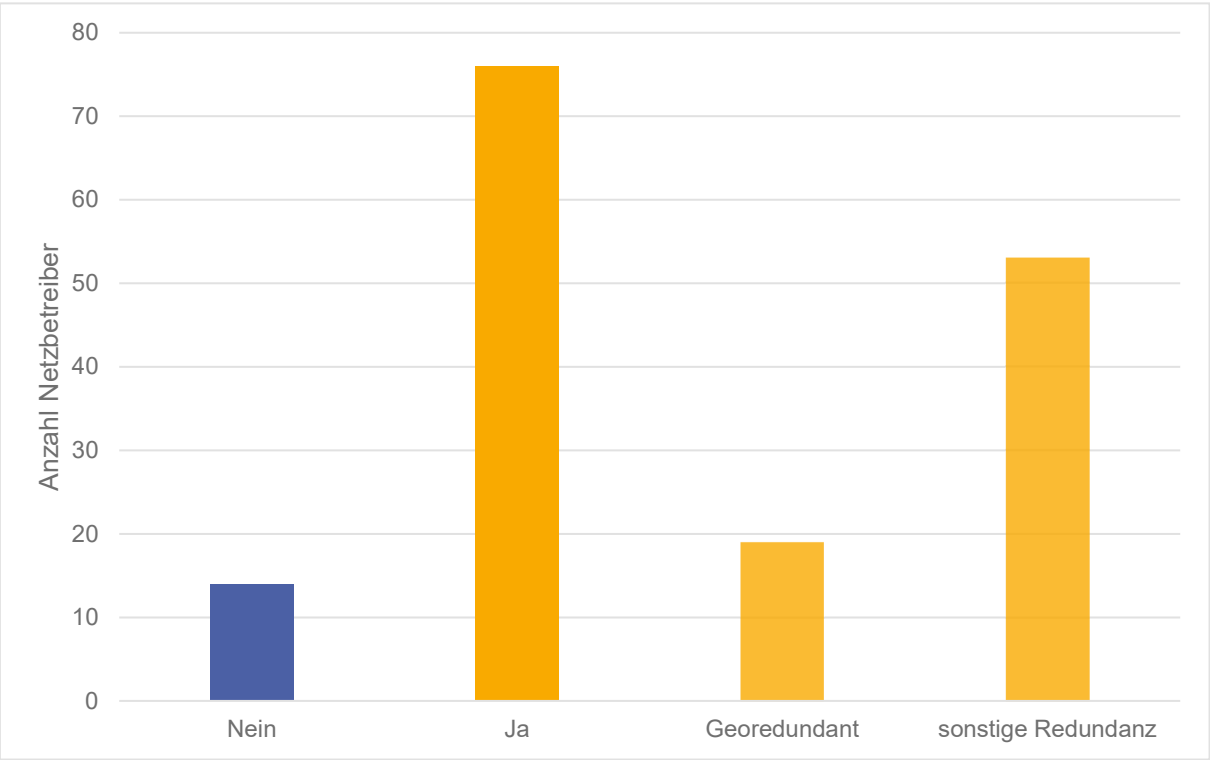

Abbildung 11: Redundante Netzleitsysteme

Das Ziel der Cyber-Sicherheitsmassnahmen ist es, dass im Ereignisfall die Lieferung an den Nachlieger oder Endkunden sichergestellt werden kann. Dies kann einerseits durch eine Redundanz der kritischen

IT-/OT-Applikationen und Systeme erfolgen oder aber durch einen manuellen Workaround. Dabei haben 49 Netzbetreiber, welche auf den Netzebenen 1 bis 4 tätig sind, ein redundantes System und einen manuellen Workaround. 11 Netzbetreiber haben nur redundante Systemen und 5 Netzbetreiber haben nur einen manuellen Workaround vorbereitet (vgl. Abbildung 12). 2 Netzbetreiber verfügen weder über ein redundantes System noch über einen manuellen Workaround.

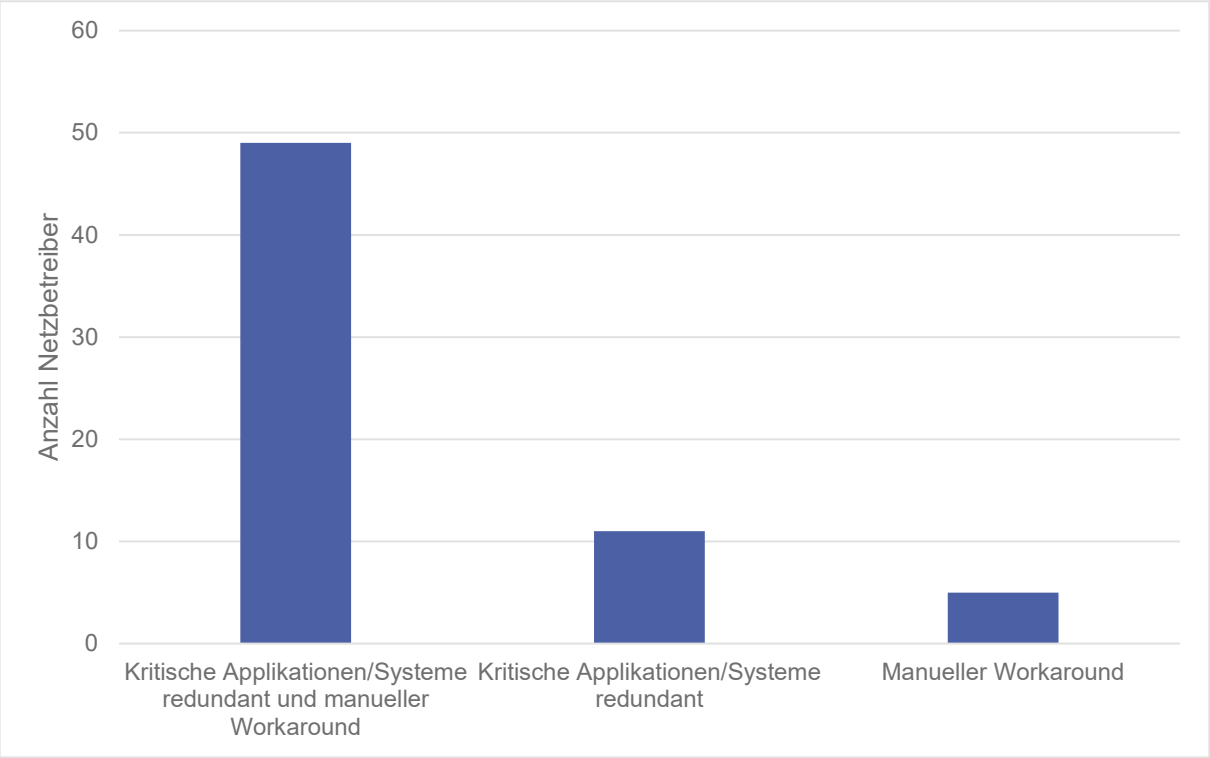

Abbildung 12: Redundanz kritischer IT-/OT-Applikationen/Systeme und manueller Workaround

Um einem Cyber-Vorfall entgegenzutreten, ist ein spezialisiertes Computer Emergency Response Team (CERT) oder Security Operations Center (SOC) neben der allgemeinen Krisenorganisation hilfreich. Dabei geben 23 Netzbetreiber, welche auf den Netzebene 1 bis 4 tätig sind, an, über ein CERT / SOC zu verfügen. Dabei betreiben 7 Netzbetreiber ein eigenes Team, 9 Netzbetreiber verfügen über ein eigenes Team mit externer Unterstützung, 2 Netzbetreiber haben sich zusammengeschlossen und 5 Netzbetreiber beziehen die CERT-Dienstleistungen von Externen (vgl. Abbildung 13).

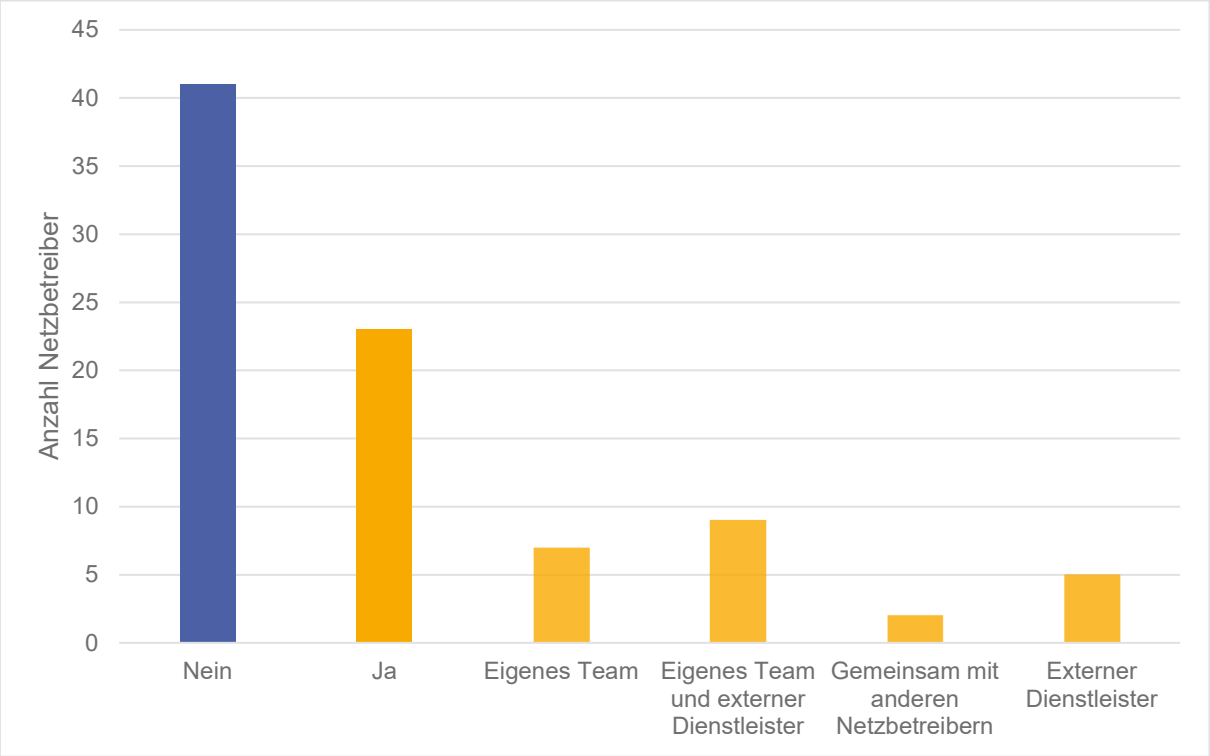

Abbildung 13: Verfügt Unternehmen über CERT/SOC?

Damit bei einem Cyber-Vorfall andere Netzbetreiber gewarnt werden können, ist es wichtig, dass die Vorfälle gemeldet werden. Dadurch ist es möglich, die Tragweite des Vorfalls und mögliche Zusammenhänge mit weiteren Vorfällen zu erkennen und andere Netzbetreiber über die Art des Cyber-Vorfalles zu informieren. Nachfolgende Abbildung 14 zeigt, dass 57 Netzbetreiber Cyber-Vorfälle freiwillig melden. 51 Netzbetreiber meldeten den Vorfall an Melde- und Analysestelle Informationssicherung (MELANI), 7 Netzbetreiber an Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) und 9 Netzbetreiber melden Cyber-Vorfälle an weitere Stellen (zum Beispiel IT-Abteilung des Kantons oder Stadt sowie externer IT-Dienstleister). Dabei kann derselbe Vorfall an mehrere Stellen gemeldet werde. 33 Netzbetreiber melden einen Cyber-Vorfall nicht. Dies hauptsächlich, weil der Netzbetreiber noch keinen Cyber-Vorfall hatte oder der Nutzen einer Meldung für den Netzbetreiber nicht ersichtlich ist. Weiter wurde angegeben, dass keine Meldepflicht besteht oder keine Ressourcen für eine Meldung vorhanden sind.

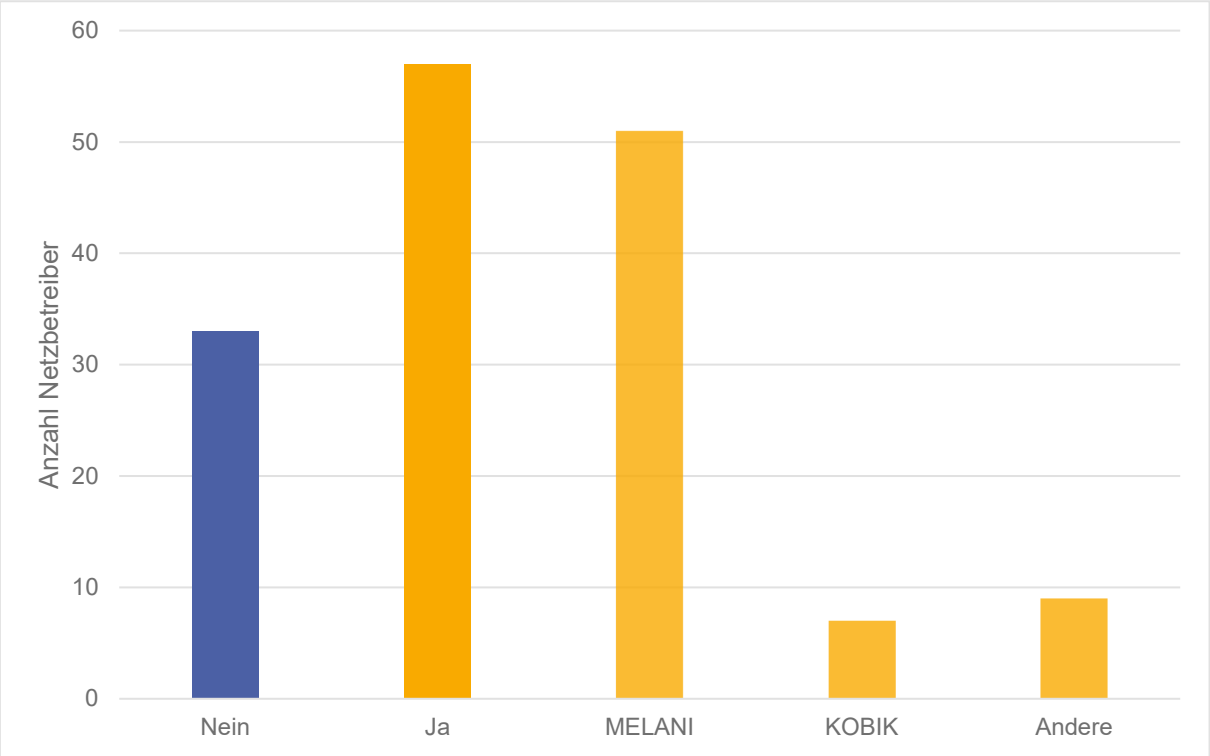

Abbildung 14: Meldung von Cyber-Vorfällen

2.2.2 Faktor Mensch

Bei der Cyber-Sicherheit spielt der Mensch eine zentrale Rolle. Sind Mitarbeitende nicht ausreichend auf die Problematik der Cyber-Sicherheit sensibilisiert, könnten sie absichtlich oder unabsichtlich einen Cyber-Vorfall auslösen.

Damit die Mitarbeitenden einen Cyber-Vorfall erkennen oder erst gar nicht entstehen lassen, ist es wichtig, die Mitarbeitenden dafür zu sensibilisieren, respektive zu schulen. 50 Netzbetreiber führen Schulungsprogramme sowohl für IT- und OT-Sicherheit durch. 18 respektive 3 Netzbetreiber führen nur Schulungsprogramme für IT- respektive OT-Sicherheit durch. 21 Netzbetreiber führen keine Schulungsprogramme durch (vgl. Abbildung 15).

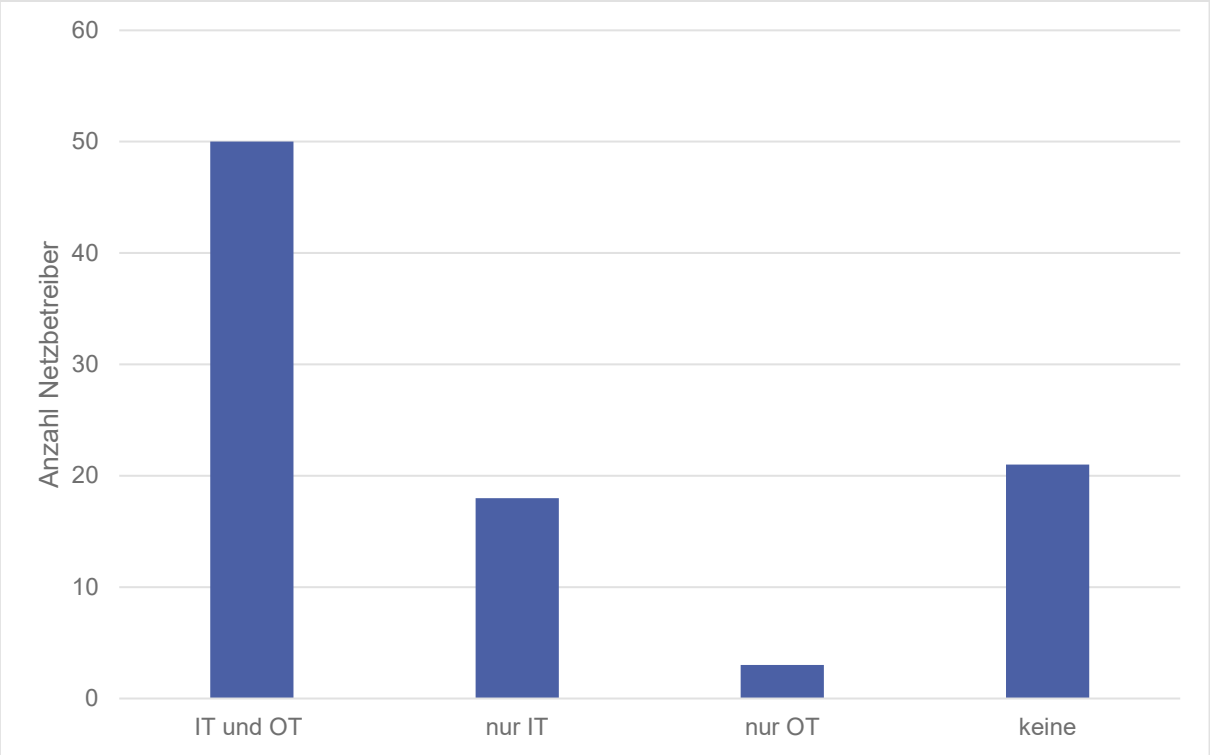

Abbildung 15: Schulung/Sensibilisierung von Mitarbeitenden

Neben der Schulung der einzelnen Mitarbeitenden in der IT-/OT-Sicherheit ist ein Austausch zwischen den IT-/OT-Sicherheitsverantwortlichen wichtig, da diese Bereiche immer stärker zusammenwachsen. 26 Netzbetreiber der Netzebene 1 bis 4 geben an, dass es sich bei den IT-/OT-Sicherheitsverantwortlichen um ein und dieselbe Person handelt. 33 Netzbetreiber führen regelmässig Schulungen durch oder tauschen sich in Sitzungen aus und 51 Netzbetreiber führen einen Austausch bei Bedarf durch. Bei 5 Netzbetreibern findet kein Austausch statt (vgl. Abbildung 16).

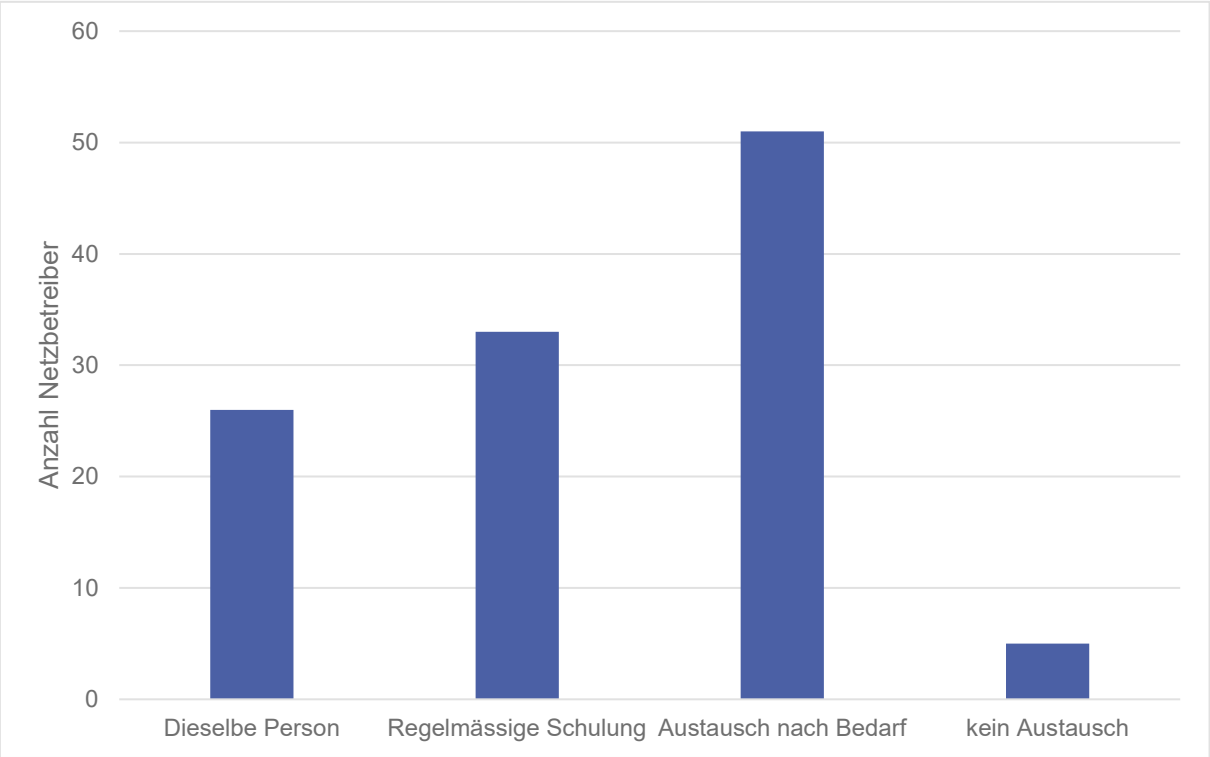

Abbildung 16: Wissensaustausch zwischen IT-/OT-Sicherheitsverantwortlichen

Durch neue technischen Möglichkeiten wurden auch Fernzugriffe auf kritische Applikationen möglich (zum Beispiel beim Piketteinsatz). 7 Netzbetreiber erlauben keinen Fernzugriff auf kritische Applikationen. Bei 85 Netzbetreibern ist der Fernzugriff erlaubt. Dabei gewähren 5 nur einen Lesezugriff während 80 Netzbetreiber einen Lese- und Schreibzugriff erlauben (vgl. Abbildung 17).

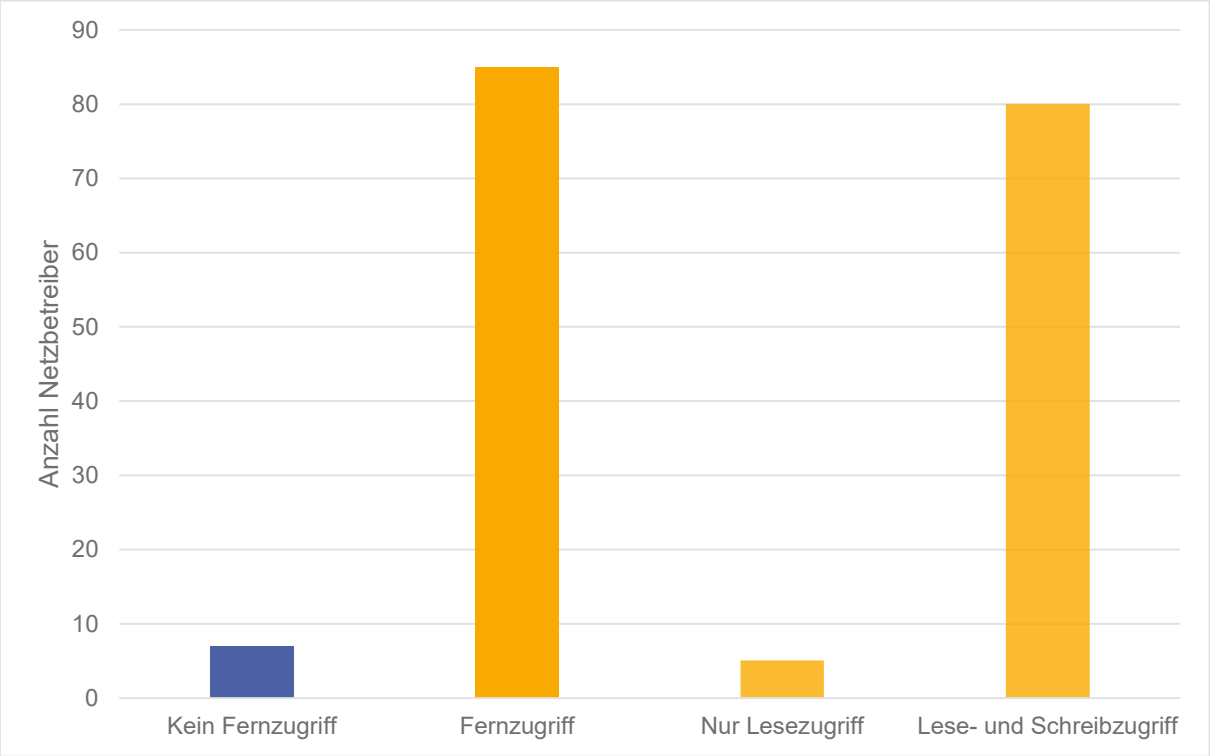

Abbildung 17: Fernzugriff auf kritische Applikationen und Zugriffsrechte

Weiter kann die Cyber-Sicherheit bei Fernzugriffen gesteigert werden, wenn bei den Zugriffsberechtigten eine Hintergrundprüfung durchgeführt wird. Diese wird bei 13 Netzbetreibern durchgeführt. Weiter zeichnen 56 Netzbetreiber der Netzebene 1 bis 4 Fernzugriffe auf (vgl. Abbildung 18).

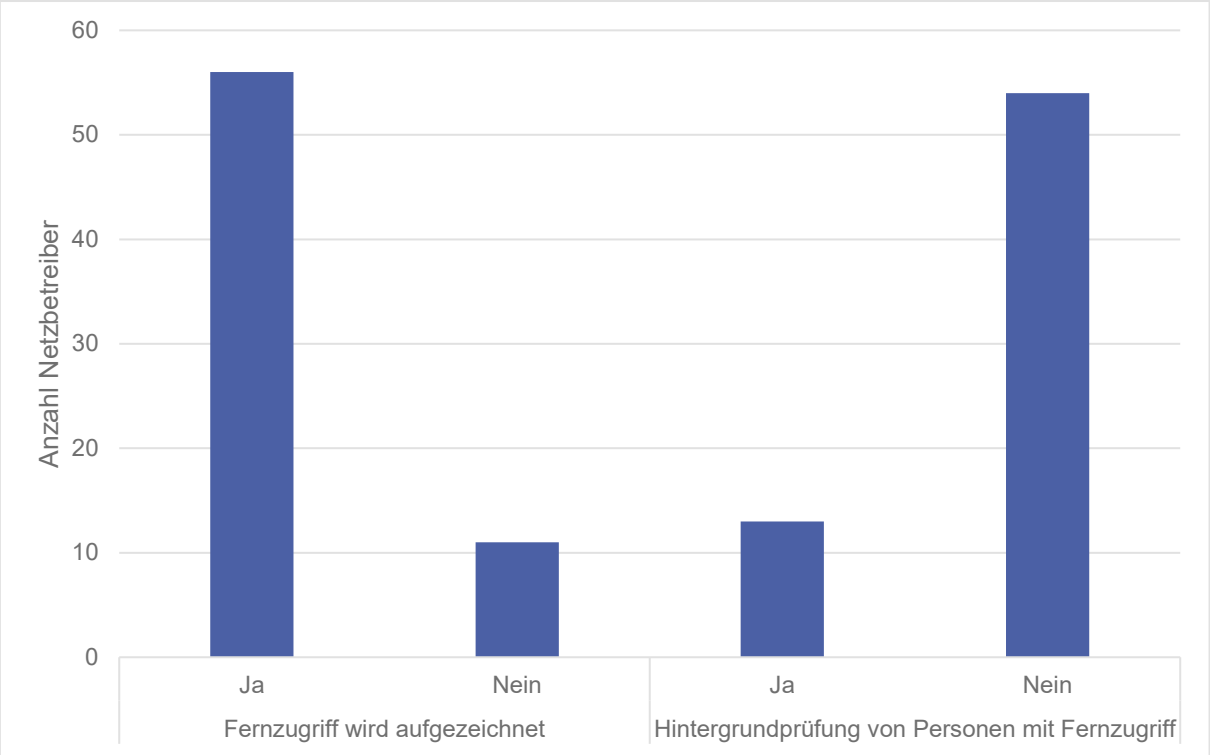

Abbildung 18: Aufzeichnung und Hintergrundprüfung bei Fernzugriff auf kritischen Applikationen

2.2.3 Externe Dienstleister

Neben den eigenen Mitarbeitenden ist auch der Umgang mit externen Dienstleistern bei der Cyber-Sicherheit zu berücksichtigen. Einerseits geht es darum, ob die IT-Dienstleistungen ausgelagert wurden und anderseits, wie kritische IT- und OT-Systeme durch externe Dienstleister gewartet werden. Abbildung 19 zeigt, dass 37 Netzbetreiber ihre IT ausgelagert haben und 28 davon auch einen Fernzugriff erlauben. Die Zugriffsberechtigung erfolgt in den meisten Fällen durch eine 2 Faktor-Authentifizierung oder über einen Antrag bei der IT-Abteilung. Dabei sind 21 Netzbetreiber selbst für die IT-Sicherheit zuständig und bei 15 Netzbetreibern ist der Outsourcingpartner für die IT-Sicherheit zuständig. Die Verantwortung bleibt beim Netzbetreiber.

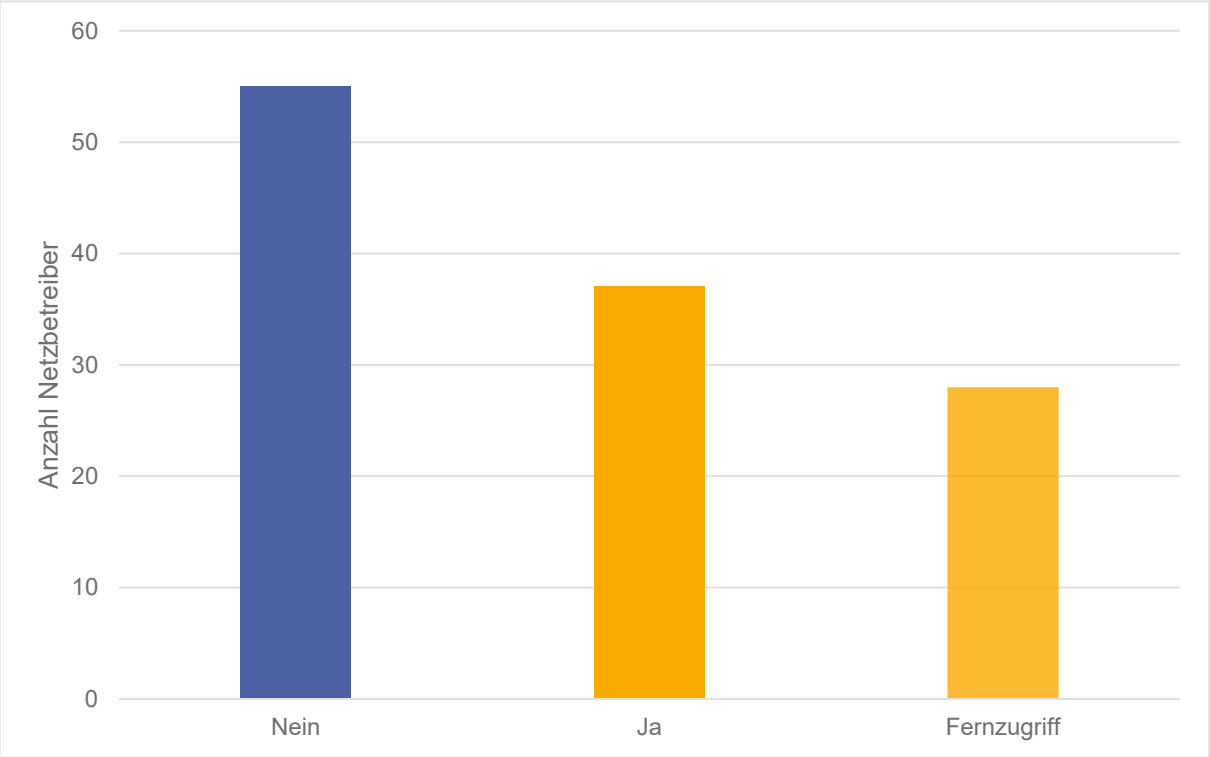

Abbildung 19: Auslagerung IT und Fernzugriff Outsourcingpartner

Bei 42 Netzbetreibern der Netzebene 1 bis 4 werden externe Dienstleister bei der Wartung von kritischen IT-Systemen vor Ort durch einen Mitarbeitenden des Netzbetreibers physisch begleitet. Dies ist für kritische OT-Systeme bei 52 Netzbetreibern der Fall. 3 respektive 1 Netzbetreiber lassen zu, dass der externe Dienstleister kritische IT- respektive OT-Systeme vor Ort alleine wartet. Dabei erlauben 45 respektive 46 Netzbetreiber einen Fernzugriff zur Wartung der kritischen IT- respektive OT-Systeme (vgl. Abbildung 20). Dieser Zugang wird meistens über eine 2 Faktoren Authentifizierung freigegeben. Weiter wird der Zugang zum Teil zeitlich begrenzt, ereignisbezogen freigegeben und in seltenen Fällen überwacht.

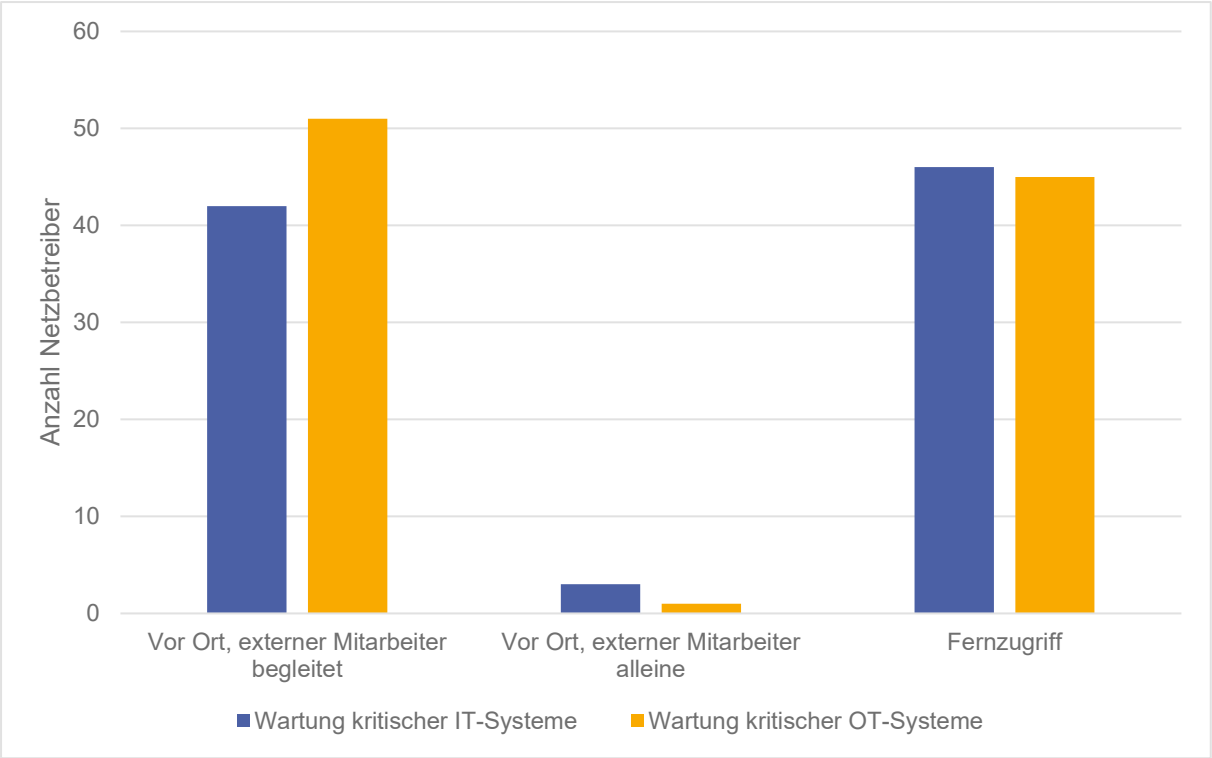

Abbildung 20: Wartung kritischer IT-/OT-Systeme

2.3 Technische Ebene

Dieser Abschnitt soll einen Überblick über den Stand der getroffenen Schutzmassnahmen auf technischer Ebene geben. Insbesondere liegt der Fokus dabei auf der Netzwerkarchitektur und des Sicherheitsmonitorings.

2.3.1 Netzwerkarchitektur

Abbildung 21 zeigt, dass 44 Netzbetreiber IT- und OT-Infrastruktur voneinander physisch getrennt haben. Von den 48 Netzbetreibern, welche die Systeme nicht physisch getrennt haben, schützen 47 Netzbetreiber den Übergang mit einer Firewall und 12 durch Verschlüsselung. Nur 1 Netzbetreiber hat weder getrennte Systeme noch eine Firewall oder Verschlüsselung zum Schutz der Übergänge eingesetzt.

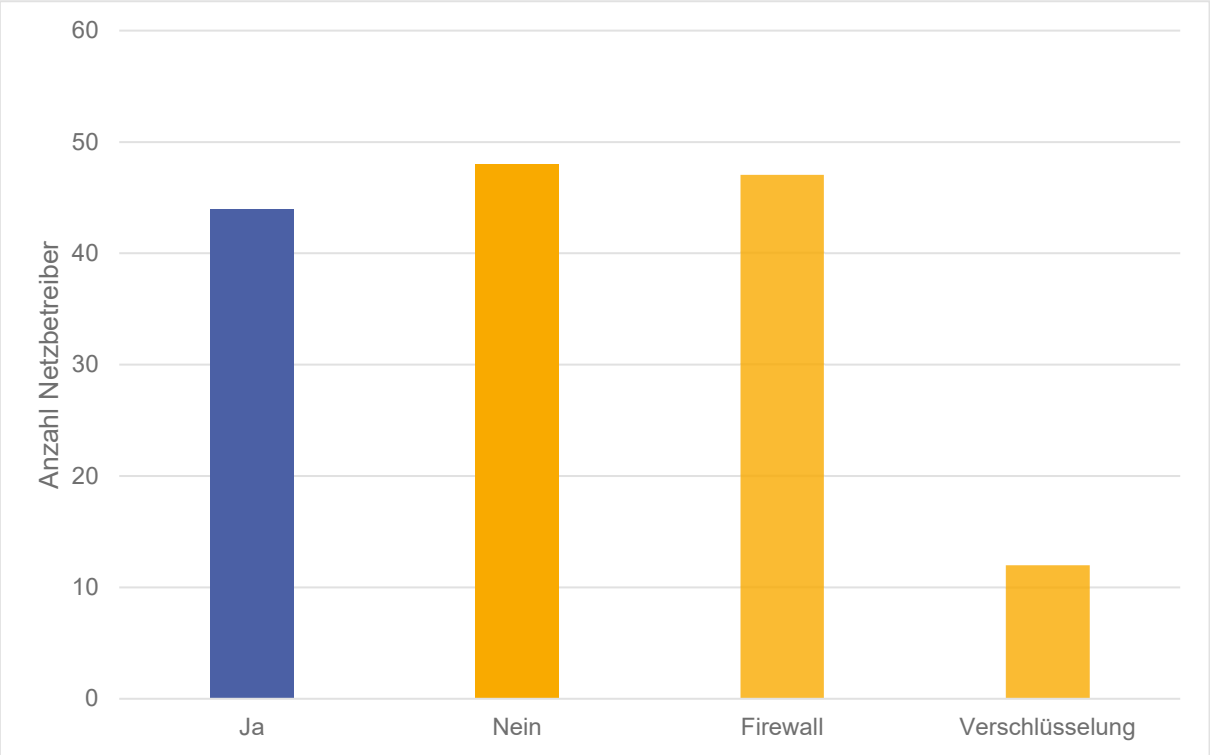

Abbildung 21: IT-/OT-Infrastruktur getrennt und Schutzmassnahmen

Durch die Segmentierung der Netzwerkarchitektur in verschiedene Zonen lässt sich die Cyber-Sicherheit erhöhen. Durch die im Idealfall geschützten Übergänge könnte bei einem Cyber-Vorfall Zeit gewonnen werden, bis der Angreifer auf kritische Systeme zugreifen kann (Defense-in-Depth Konzept). Von den Netzbetreibern der Netzebene 1 bis 4 verwenden 59 ein Zonenkonzept. 7 Netzbetreiber verwenden kein Zonenkonzept. 32 Netzbetreiber verwenden dabei ein Zonenkonzept, welches alle 4 Zonen (offen, vertraulich, geschäftskritisch und betriebskritisch) des VSE Branchendokuments «ICT Continuitiy» berücksichtigt. Die offene Zone besitzt eine niedrige Schutzstufe während die betriebskritische Zone eine hohe Schutzstufe hat. In der offenen Zone sind beispielsweise Netzwerke Dritter oder das Internet. In der vertraulichen Zone kann die allgemeine Büro IKT liegen, während die Büro-IKT zur Bearbeitung der Finanzen oder von Personaldaten in der geschäftskritischen Zone liegen. In der betriebskritischen Zone liegt die Prozess IKT, also die OT[7]. Hauptsächlich wird zwischen einer offenen Zone, einer vertraulichen Zone und einer betriebskritischen Zone unterschieden (vgl. Abbildung 22).

[7] VSE Branchenempfehlung «ICT Continuity», 2011

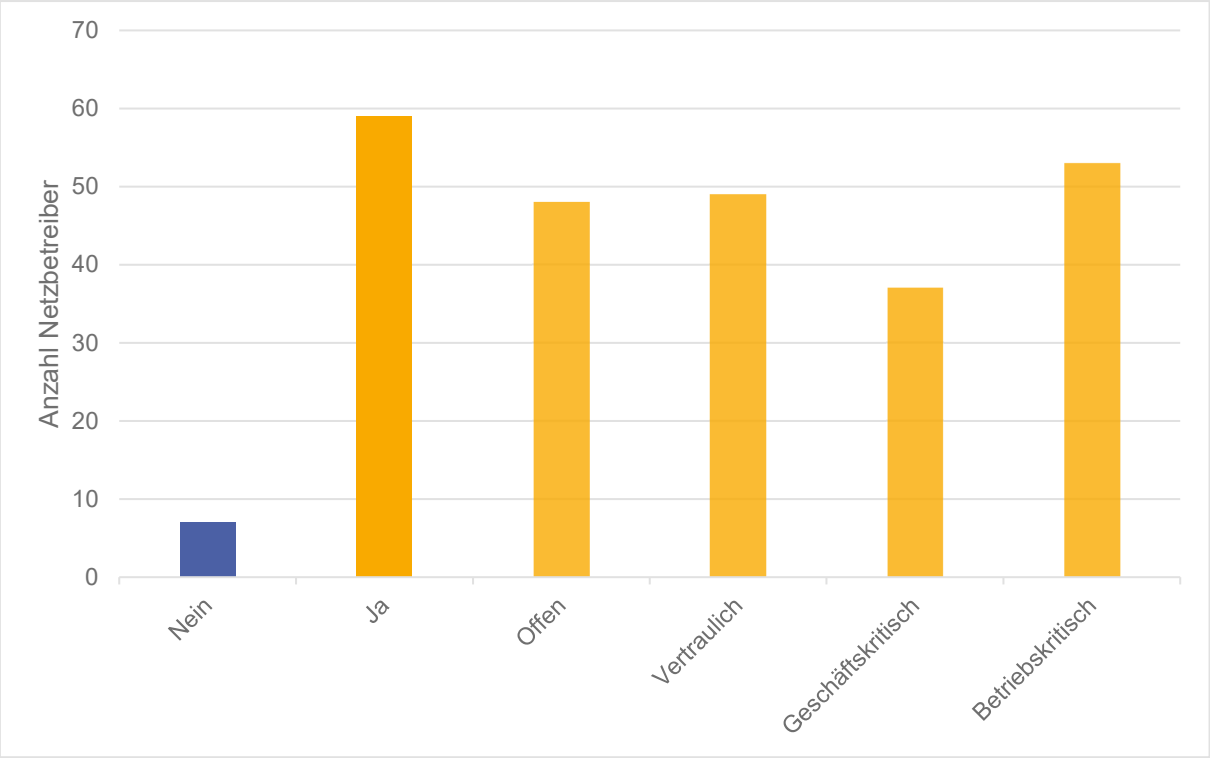

Abbildung 22: Verwendung Zonenkonzept

2.3.2 Sicherheitsmonitoring

Um Cyber-Vorfälle zu erkennen, ist es entscheidend, den eigenen Netzwerkverkehr zu überwachen. Dies kann über Intrusion Detection Systeme, über eine Aufzeichnung des Netzwerkverkehrs und/oder über die Auswertung von Log-Files geschehen.

Bei der IT setzen 40 Netzbetreiber der Netzebene 1 bis 4 Intrusion Detection Systeme ein. Bei der OT sind es 26 Netzbetreiber. Bei 4 Netzbetreibern stehen solche Systeme vor der Einführung (vgl. Abbildung 23).

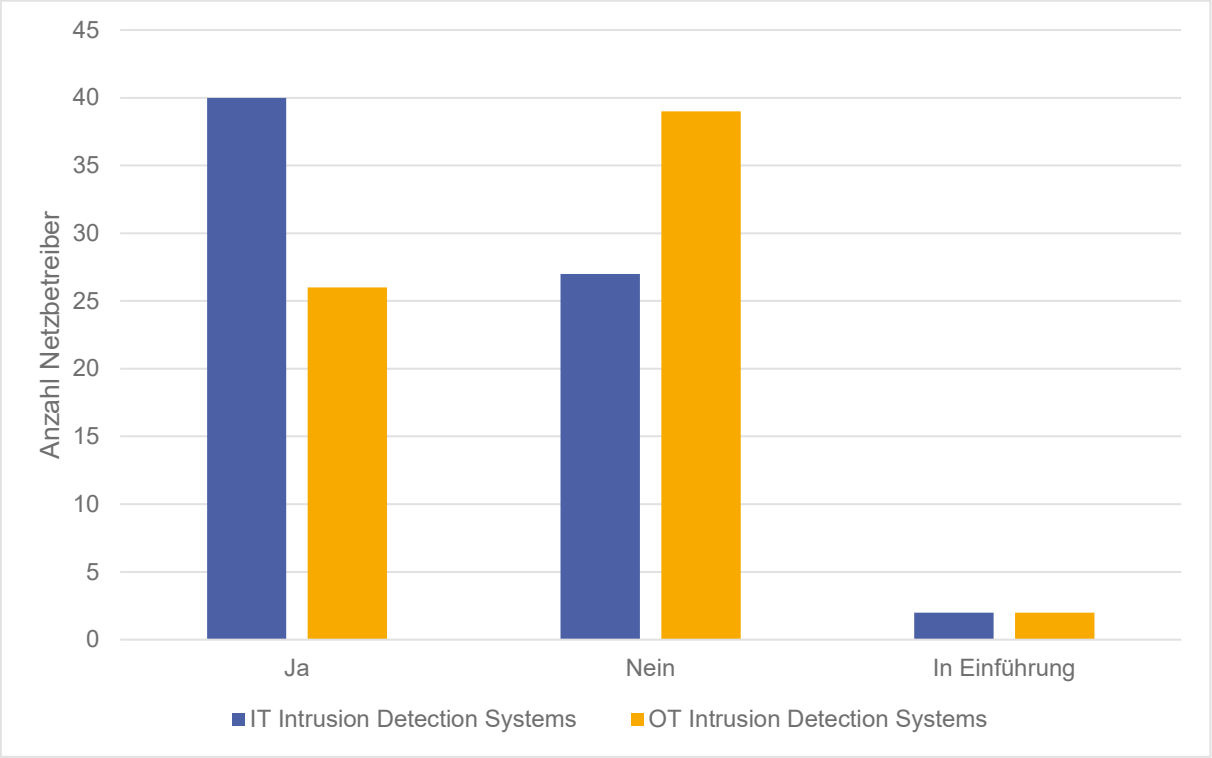

Abbildung 23: Intrusion Detection Systems

Ein weiteres Element des Sicherheitsmonitorings ist die Aufzeichnung und Überwachung des Netzwerkverkehrs auf Anomalien im Datenfluss. Für die Gewährleistung der Versorgungssicherheit steht hier insbesondere der OT-Netzwerkverkehr im Vordergrund. 35 Netzbetreiber haben keine Überwachung oder Aufzeichnung des OT-Netzwerkverkehrs. Bei 11 Netzbetreibern wird der OT-Netzwerkverkehr nur aufgezeichnet, bei 10 Netzbetreibern nur überwacht und bei 11 Netzbetreibern wird der OT-Netzwerkverkehr sowohl aufgezeichnet wie überwacht (vgl. Abbildung 24).

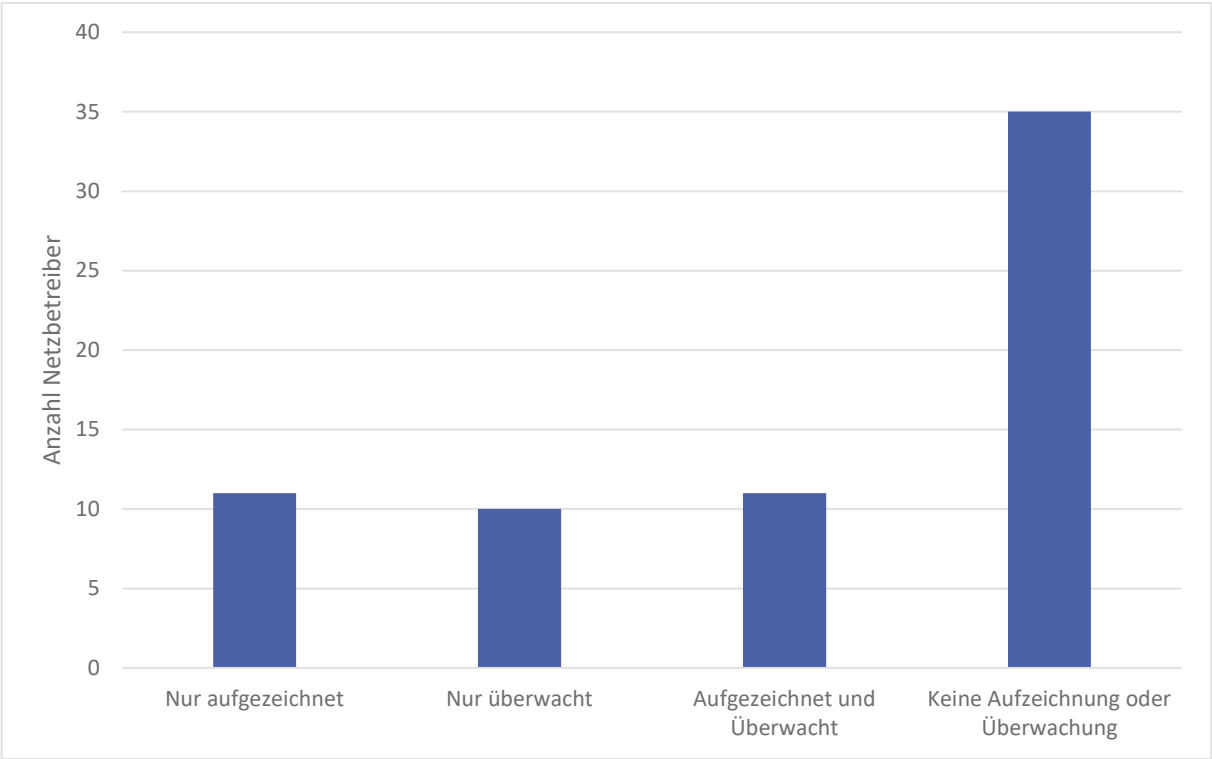

Abbildung 24: Aufzeichnung / Überwachung OT-Netzwerkverkehr

Neben der Beobachtung eines spezifischen Aspekts des Netzwerkverkehrs, kann auch die Analyse von Log-Files Aufschluss über Systemanomalien und somit Hinweise auf einen möglichen Cyber-Vorfall geben. Dazu werten 26 Netzbetreiber der Netzebene 1 bis 4 ihre Log-Files aus (vgl. Abbildung 25).

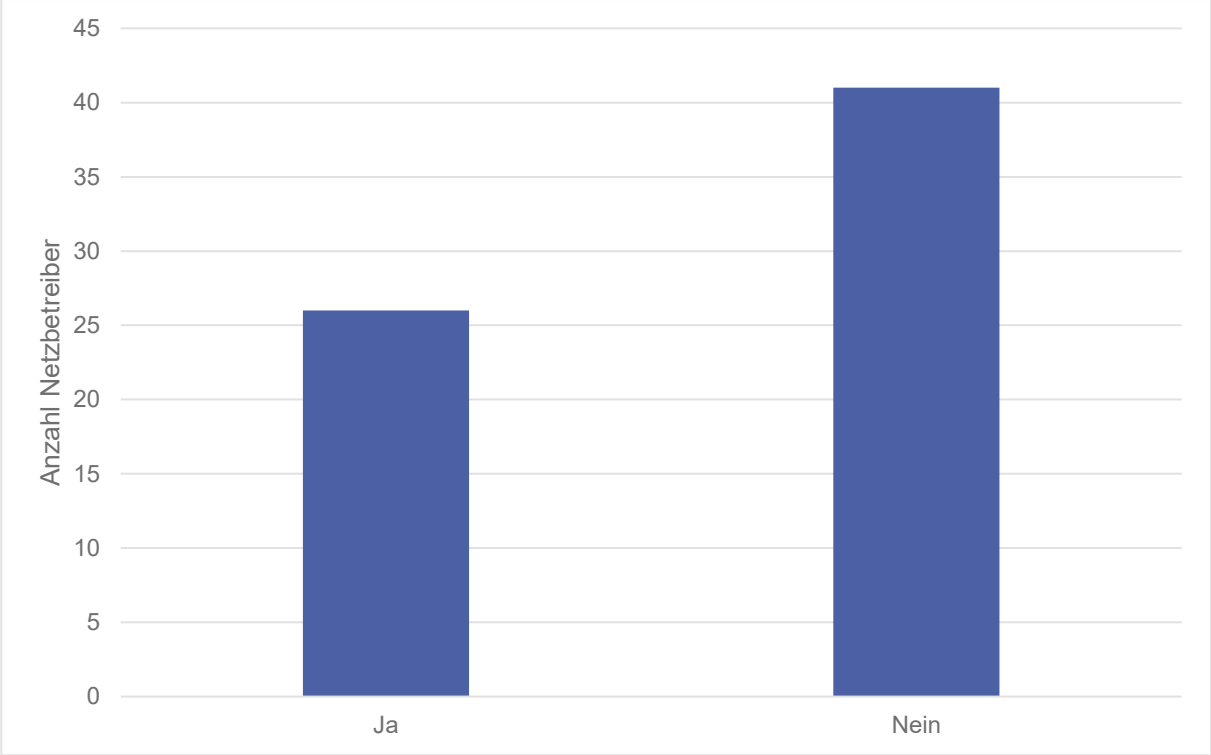

Abbildung 25: Zentrale Log-Auswertung

Neben der kontinuierlichen Überwachung des Netzwerkverhaltens sind punktuelle Überprüfungen des Cyber-Sicherheitsmassnahmen durch ein Audit oder Tests einzelner Systemkomponenten durch einen Penetration-Test für die Sicherstellung der Cyber-Sicherheit unumgänglich.

Bei den auf den Netzebenen 1 bis 4 tätigen Netzbetreibern haben 49 in den letzten 5 Jahren mindestens ein Sicherheitsaudit bei der IT durchgeführt. Dabei haben 15 Netzbetreiber 3 oder mehr Audits intern und 17 Netzbetreiber 3 oder mehr Audits durch einen externen Dienstleister durchgeführt (vgl. Abbildung 26, blaue Balken). Bei der OT haben 40 Netzbetreiber in den letzten 5 Jahren ein Audit durchgeführt. Im Gegensatz zur IT wurde hier häufig nur ein Audit durch einen externen Dienstleister durchgeführt (vgl. Abbildung 26, orange Balken).

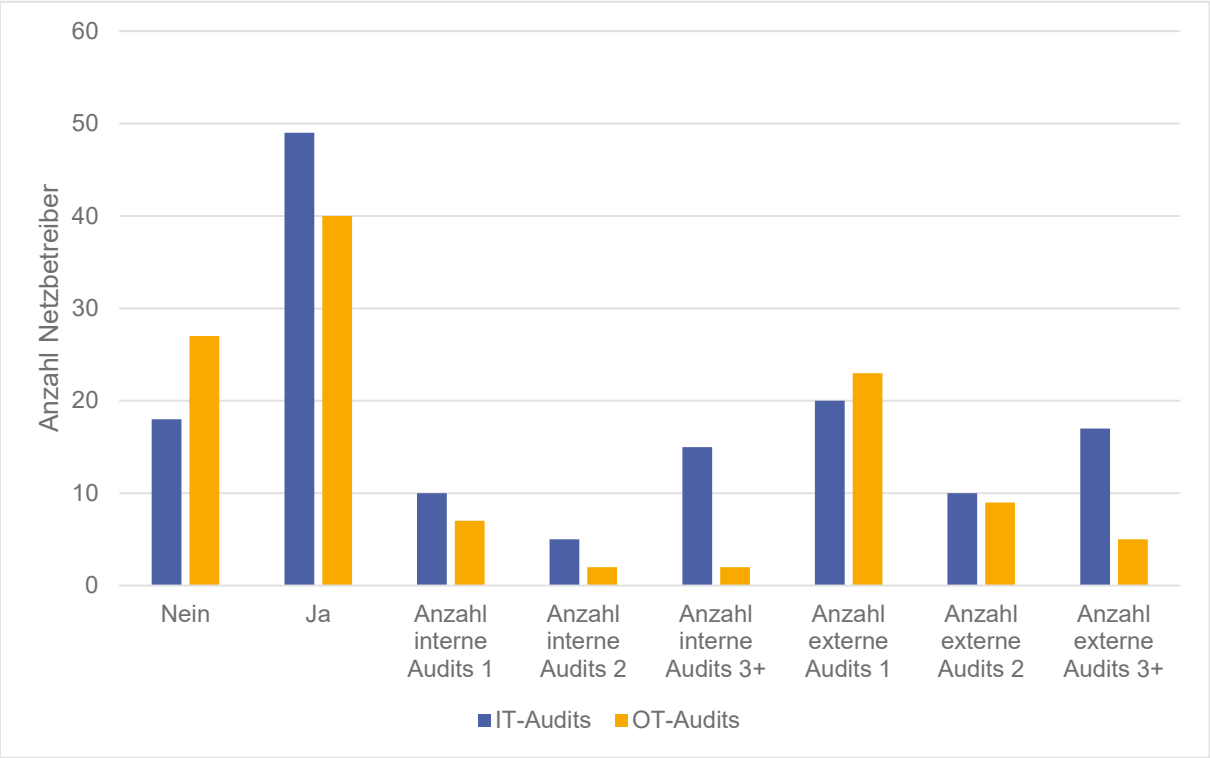

Abbildung 26: Durchführung IT-/OT-Audits

Neben der Überprüfung des Gesamtsystems ist auch der Test einzelner Systemkomponenten für die Cyber-Sicherheit entscheidend. So führen 43 der auf den Netzebenen 1 bis 4 tätigen Netzbetreiber IT-Penetration-Tests durch. Dabei finden die Penetration-Tests in der Regel alle Jahre oder nach Bedarf statt (vgl. Abbildung 27, blaue Balken). Bei der OT führen 27 Netzbetreiber Penetration-Tests durch. Im Gegensatz zur IT finden diese in der Regel alle 3 Jahre oder nach Bedarf statt (vgl. Abbildung 27, orange Balken).

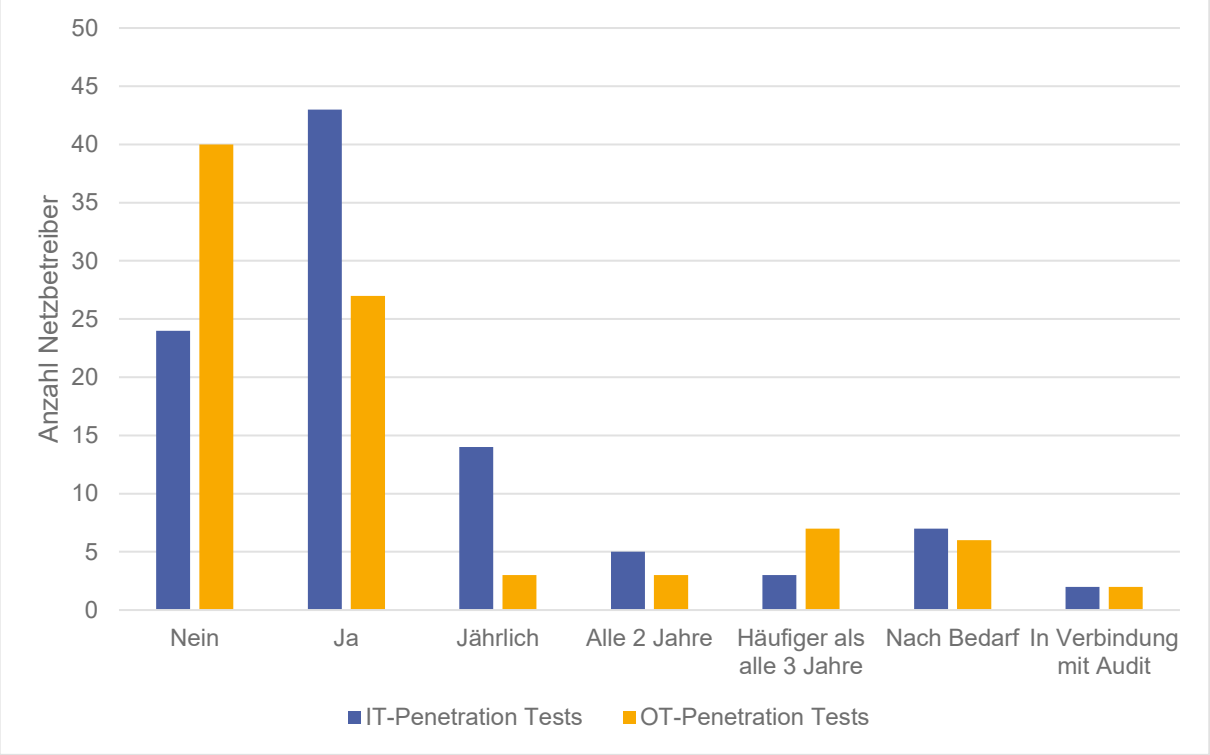

Abbildung 27: IT-/OT-Penetration Tests

Neben dem Monitoring der eigenen Informatiksysteme ist auch das Monitoring der allgemeinen Cyber-Bedrohungslage wichtig, damit zum Beispiel auf spezifische Ereignisse reagiert werden kann. Dazu erstellen 51 Netzbetreiber eine eigene Bedrohungsanalyse und 45 Unternehmen kaufen die Bedrohungsanalyse extern ein oder ergänzen dadurch ihre selbst erstellte Analyse.

3 Fazit

Wie eingangs erwähnt, müssen die Netzbetreiber ein sicheres (Strom-)Netz gewährleisten. Dies betrifft auch den Schutz des (Strom-)Netzes vor Cyber-Risiken. Dieses Risiko nimmt zu, je stärker ein Netzbetreiber informationstechnologisch vernetzt ist. Aufgrund der zunehmenden Digitalisierung und dem geplanten Smart Meter Rollout wird die bereits starke informationstechnologische Vernetzung der Netzbetreiber (vgl. Kapitel 2.1) in Zukunft weiter zunehmen. Dadurch wird auch die Angriffsfläche für Cyber-Vorfälle grösser. Als Folge davon steigt die Bedeutung der Cyber-Sicherheit mit steigender Digitalisierung und informationstechnologischer Vernetzung an.

Die ElCom beleuchtet in diesem Bericht nicht den Zustand der gesamten Cyber-Sicherheitsmassnahmen der Netzbetreiber, sondern nur ausgewählte Elemente. Eine gesamte Analyse würde zu weit führen. Die hier gemachten Aussagen und Empfehlungen beziehen sich daher nur die betrachteten Themengebiete. Dabei orientiert sich die ElCom an bestehenden Standards, Empfehlungen und Branchendokumenten.

3.1 Organisatorische Massnahmen

Bei den organisatorischen Massnahmen lassen sich zusammenfassend folgende Punkte festhalten:

- Der Cyber-Sicherheit wird die nötige Aufmerksamkeit geschenkt, da diese entweder in der Geschäftsleitung oder zumindest in einem speziellen Gefäss thematisiert wird. So werden auch die Sicherheitsmassnahmen situativ und grösstenteils sogar zyklisch angepasst. Dies ist insbesondere bei der historisch gewachsenen starken Vernetzung der Netzbetreiber zentral.
- Bezüglich der Erarbeitung von sicherheitsrelevanten Richtlinien und Massnahmen bei der OT sieht die ElCom Handlungsbedarf. Hier verfügen nicht alle Netzbetreiber über entsprechende Richtlinien, insbesondere in den Bereichen der Detektion und Vorfallsbewältigung (Incident Response).
- Aufgrund der Resultate sind nur wenige Netzbetreiber bereits zertifiziert oder streben eine Zertifizierung an. Dies ist aus Sicht der ElCom unproblematisch, da eine effektive Cyber-Sicherheit auch ohne Zertifikat möglich ist und ein Zertifikat im Gegenzug nicht immer eine effektive Cyber-Sicherheit bedeutet.
- Damit die Lieferung auch bei einem Cyber-Vorfall gesichert ist, müssen die Systeme redundant ausgelegt oder ein manueller Workaround vorbereitet sein. Es gibt Netzbetreiber, welche keine redundanten Systeme oder manuelle Workarounds haben. Hier besteht aus Sicht der ElCom Nachholbedarf, damit im Ereignisfall die Stromlieferung sichergestellt werden kann.
- Weiter betreiben wenige Netzbetreiber ein eigenes CERT oder SOC. Häufiger wird diese Dienstleistung durch einen externen Dienstleister ergänzt oder ganz übernommen. Sehr selten ist eine Kooperation unter Netzbetreibern. Hier ist festzuhalten, dass es aus ökonomischen Überlegungen nicht effizient ist, dass jeder Verteilnetzbetreiber ein eigenes CERT betreibt.
- Ein Grossteil der Netzbetreiber meldet vorgefallene Cyber-Vorfälle, insbesondere an MELANI. Dies ermöglicht es, das Lagebild der Cyber-Vorfälle im Elektrizitätsbereich bei MELANI aktuell zu halten.
- Ebenso führt rund die Hälfte der befragten Netzbetreiber Schulungs- und Sensibilisierungsprogramme sowohl für IT wie auch für OT durch. 21 Netzbetreiber führen jedoch keine Schulungsprogramme durch. Vor dem Hintergrund, dass die meisten Cyber-Vorfälle durch ein menschliches Fehlverhalten ausgelöst werden ist es aus Sicht der ElCom nicht vertretbar, keine Schulungs- oder Sensibilisierungsprogramme durchzuführen. Zudem sollten regelmässige Schulungen oder Sitzung zwischen IT- und OT-Sicherheitsverantwortlichen stattfinden.
- Die meisten Netzbetreiber erlauben den eigenen Mitarbeitenden einen Fernzugriff auf kritische Applikationen. Dieser Zugriff wird bei den meisten Netzbetreibern auch aufgezeichnet. Nur bei wenigen wird bei Mitarbeitenden mit einem Fernzugriff eine Hintergrundprüfung durchgeführt.
- Weit verbreitet ist auch die Auslagerung der IT Dienstleistungen. Dies häufig in Verbindung mit einem Fernzugriff der externen Dienstleister. Dieser Zugriff wird in den meisten Fällen mindestens mit einer

2 Faktoren Authentifizierung geschützt. Aus Sicht der ElCom könnte die Cyber-Sicherheit weiter erhöht werden, wenn der Fernzugriff zum Beispiel zeitlich beschränkt freigegen und zusätzlich überwacht wird.

- Bei der Wartung von kritischen IT- oder OT-Systemen durch externe Dienstleister ist meistens ein interner Mitarbeiter vor Ort anwesend. Leider ist auch festzuhalten, dass Netzbetreiber externe Dienstleister unbeaufsichtigt Wartungs- oder Installationsarbeiten durchführen lassen. Dieses Verhalten ist sehr fahrlässig in Bezug auf die Cyber-Sicherheit und dürfte nicht sein. Die Begleitung eines externen Dienstleisters ist kein Misstrauensbeweis, sondern eine Absicherung. Auch dem externen Dienstleister können fahrlässige Fehler unterlaufen, welche durch ein 4-Augen-Prinzip erkannt werden können. Zudem ist dem Unternehmen so auch bekannt, welche Arbeiten ausgeführt wurden. Auch hier sind Fernzugriffe weit verbreitet.

3.2 Technische Massnahmen

Im Bereich der technischen Massnahmen ist Handlungsbedarf bei der Erkennung von Cyber-Vorfällen feststellbar. Ziel sollte es sein, Cyber-Vorfälle zu erkennen, damit deren Auswirkungen frühzeitig eingedämmt werden können. Dazu sollte aus Sicht der ElCom insbesondere der OT-Netzwerkverkehr aufgezeichnet und überwacht werden. Die OT stellt das Kerngeschäft der Netzbetreiber dar. Daher erwartet die ElCom, dass die OT-Infrastruktur entsprechend dem aktuellen Stand der Technik geschützt wird. Im Idealfall ist die OT- und IT-Infrastruktur getrennt. Sind diese Infrastrukturen nicht getrennt, sind die Verbindungen zu schützen. In diesem Fall ist die regelmässige externe Überprüfung der OT aus Sicht der ElCom zwingend. In diesem Zusammenhang ist die Wirkung interner Audits und Penetration Tests aufgrund der Befangenheit der Auditoren zu hinterfragen. Nichtsdestotrotz können bei entsprechender Durchführung auch interne Audits und Penetration Test Schwachstellen aufzeigen. Abschliessend ist festzuhalten, dass bei einem Netzbetreiber die IT nicht von der OT getrennt ist und auch der Übergang zum Teil nicht geschützt ist. Eine solche Netzwerkarchitektur ist aus sicherheitstechnischer Sicht äusserst fahrlässig.

3.3 Empfehlung

Die Cyber-Sicherheit nimmt aufgrund der zunehmenden Vernetzung weiter an Bedeutung zu. Die effiziente und risikobasierte Umsetzung der VSE Branchendokumente «ICT Continuity», «Handbuch Grundschutz für Operational Technology in der Stromversorgung» und «Richtlinie für die Datensicherheit von intelligenten Messsystemen» gemäss dem Leitfaden «Schutz kritischer Infrastrukturen» des BABS wird von der ElCom nicht nur begrüsst, sondern auch erwartet. Im Zentrum der Massnahmen sollen dabei immer die Sicherstellung der Systemstabilität und die Lieferung an die Nachlieger und Endkunden stehen. Die Bestrebungen, ein Branchen-CERT aufzubauen, ist im Sinne der Subsidiarität zu begrüssen.

4 Anhang

4.1 Glossar

Abkürzung	Bedeutung
APT	Advanced Persistent Threat
CERT	Computer Emergency Response Team
KOBIK	Koordinationsstelle zur Bekämpfung der Internetkriminalität
MELANI	Melde- und Analysestelle Informationssicherung
OT	Operational Technology
PIA	Partner Informationsaustausch
SOC	Security Operations Center