convergint | utilities

Leitfaden für bewährte Praktiken, 2024: Versorgungsunternehmen

convergint® | utilities

Der Versorgungssektor erlebt **eine Eskalation der physischen und Cyber-Risiken auf nationaler und globaler Ebene**, die eine Priorisierung der Sicherheitsplanung und Verfahrensminderung erfordert. Das engagierte Versorgungsteam von Convergint bietet hochsichere Schutzstrategien, methodische Programmimplementierung und umfassende Lösungen, die sowohl die Sicherheit als auch die betriebliche Effizienz in diesem Sektor verbessern. Convergint kennt die Bedrohungen der Branche und die Anforderungen an die Einhaltung von Vorschriften genau und setzt ein mehrstufiges Design ein, um optimale Leistung und Funktionalität zu gewährleisten.

Sicherheitsvorfälle und Risiken bei Versorgungsunternehmen

Kritische Betriebsstandorte stellen seit langem ein höheres Risiko für Versorgungsunternehmen dar, da sie über eine große Anzahl von Anlagen verfügen. Es hat sich jedoch gezeigt, dass auch nachgelagerte Standorte aufgrund der Auswirkungen auf das Geschäft und die Gemeinschaft sowie der nationalen Medienaufmerksamkeit, die ein Sicherheitsvorfall mit sich bringt, Schutz und Risikominderung erfordern.

Wenn es um Risikobewertungen für die Identifizierung von Vermögenswerten, Schutzstrategien und die Planung von Risikominderungsmaßnahmen geht, **ist es unerlässlich, Bewertungen nach Teilbereichen vorzunehmen**, um Lösungen auf die einzigartigen Vermögenswerte, Vorschriften, Geschäftsabläufe und Risiken einer bestimmten Branche zuzuschneiden.

Kernenergieversorger

Die Kernenergie ist einzigartig, weil sie so stark reguliert und streng bewacht wird. Die Gründe dafür liegen auf der Hand. Ein erfolgreicher Angriff, ob physisch oder im Internet, könnte zu einer unkontrollierten Freisetzung von Radioaktivität führen, was erhebliche Auswirkungen auf die Umwelt und die Gesundheit hätte, einschließlich der Möglichkeit von kurz- und langfristigen Todesfällen. Durch die Regulierung der NRC (Nuclear Regulatory Commission) sind kerntechnische Anlagen gezwungen, ein sehr präskriptives Sicherheitskonzept zu verfolgen, um die Auswirkungen von Zwischenfällen zu verhindern oder abzumildern.

Kernkraftwerke sind strukturell robust und schrecken von vornherein vor physischen Eingriffen ab. Darüber hinaus sorgt ein strenger, mehrschichtiger Ansatz für den physischen Schutz für Verstärkung und umfasst eine militärisch anmutende menschliche Eingreiftruppe. Cyber-Bedrohungen wird ebenfalls mit Sorgfalt und umfassenden Protokollen begegnet, die für das Risikomanagement, die ständige Überwachung von Ereignissen und die Abtrennung von externen Netzwerken eingesetzt werden. Letztlich ist dieser Teilbereich gut geschützt, wird aber regelmäßig getestet, so dass die Ausrüstung und die Protokolle ständig neu bewertet werden, um den Schutz und die Entwicklung von Bedrohungen zu gewährleisten.

Stromversorgungsunternehmen

Elektrizitätsversorgungsunternehmen setzen entweder vor Ort und/oder externe Agenturen ein, um potenziell gefährliche Akteure zu stoppen. Eine Eskalation des Risikos könnte eine Neubewertung dieser Strategie erforderlich machen. Nach Angaben des Energieministeriums gab es in der ersten Hälfte des Jahres 2023 95 von Menschen verursachte Vorfälle, einschließlich Vandalismus und Cyber-Ereignisse, und damit mehr als in jedem anderen Zeitraum der Geschichte.

Physische Angriffe sind nach wie vor das Hauptproblem in diesem Sektor. Vor allem der inländische Terrorismus hat den Betrieb vor Ort und die von den Stromübertragungsstationen versorgten Gemeinden in Mitleidenschaft gezogen. Der Süden der USA und der pazifische Nordwesten sind seit 2022 besonders stark betroffen, und die Situation scheint sich nicht zu verbessern. Dies erfordert eine mehrschichtige Verteidigung, die nun zunehmend von allen Umspannwerken übernommen wird.

Wasserversorgung

Die physischen Bedrohungen für Wasserversorgungsunternehmen nehmen zu, was dazu führt, dass man sich auf den Schutz der am stärksten gefährdeten Anlagen konzentriert. Wie bei den elektrischen Anlagen scheint ein "Defense in depth"-Ansatz am sinnvollsten zu sein.

Bedauerlicherweise nehmen gleichzeitig die Cyber-Bedrohungen für Wasserversorgungsunternehmen zu. SCADA-Systeme (Supervisory Control and Data Acquisition) sind von entscheidender Bedeutung für die betriebliche Überwachung und Steuerung der wichtigsten Anlagen zur Aufrechterhaltung der sauberen Speicherung und Verteilung von Wasser an die Verbraucher. Die Aufrechterhaltung einer strengen Kontrolle und Beobachtung dieser Systeme ist neben der Aufrechterhaltung guter Cybersicherheitspraktiken für Geschäftssysteme der Schlüssel zur Verhinderung oder Eindämmung von Cyberangriffen. Ein Beispiel für diese Notwendigkeit ist der jüngste Angriff auf ein Gebäude der Wasserbehörde im ländlichen Allegheny County, PA, der offenbar von einem nationalen Akteur verübt wurde. Der Behörde gelang es, die Verbindung zu unterbrechen und den Betrieb manuell wieder aufzunehmen, ohne dass es zu Zwischenfällen kam, aber die Botschaft war klar und deutlich: Die Bemühungen um physische Sicherheit müssen parallel zum Cyberschutz laufen.

Erneuerbare Energien: Solar-, Wind- und Bio-Energie

Obwohl die erneuerbaren Energien in der Landschaft der Versorgungsunternehmen weniger stark vertreten sind, haben sie eine wachsende nationale Präsenz, was eine Zunahme potenzieller Ziele und Risiken bedeutet. Die erneuerbaren Energien verfügen über Anlagen, die ebenfalls anfällig sind, und haben sich veranlasst gesehen, sowohl physische als auch Cyber-Abwehrmaßnahmen zu ergreifen. Ein Brand, der 2023 in einer Solaranlage in Las Vegas als "politisches

Statement" gelegt wurde, ist nur ein Hinweis darauf, was passieren kann, wenn dieses Teilsegment nicht mit einer angemessenen Reaktion auf neue Bedrohungen vorbereitet ist.

Die Industrie als Ganzes

Die physische Sicherheit scheint für alle Versorgungsunternehmen das Hauptanliegen zu sein, und das zu Recht. Die Kosten von Einbrüchen sind landesweit in den Schlagzeilen zu sehen. Allerdings **rücken Cyber-Bedrohungen immer mehr in den Vordergrund, da veraltete Systeme** und offene Netzwerke eine klare Zugangsmöglichkeit bieten. Auch staatliche Akteure werden zu einer immer größeren Bedrohung, so dass das Risiko über einfaches Hacken hinausgeht.

Es ist von entscheidender Bedeutung, dass die Branche eine harte Haltung gegenüber der Cyberkriminalität einnimmt und angemessen investiert, um Bedrohungen abzuschrecken und zu entschärfen, während gleichzeitig umfassende physische Sicherheitsstrategien umgesetzt werden.

Die Kosten von physischen oder Cyber-Angriffen

Es gibt vier Hauptkategorien von Verlusten, die sich aus einem physischen oder Cyber-Eingriff für Versorgungsunternehmen ergeben:

1. **Reputation/Vertrauen:** Auch wenn Versorgungsunternehmen Vorfälle nicht heraufbeschwören, kann ein wahrgenommener Mangel an Vorbereitung das Vertrauen der Kunden untergraben und ihren Ruf in der Gemeinschaft schädigen. In vielen Fällen ist ein Wechsel zu einem Konkurrenten keine Option, aber eine Beeinträchtigung der Markenwahrnehmung ist für ein Versorgungsunternehmen dennoch von Bedeutung.
2. **Verlust von Geschäftsmöglichkeiten**: Die durch physische oder Cyberangriffe erzwungene Abschaltung von Versorgungseinrichtungen bedeutet einen spürbaren Geschäftsverlust und einen messbaren Rückgang der Einnahmen.
3. **Geldstrafen:** Die Bußgelder für die Nichteinhaltung von Vorschriften für Stromversorgungsunternehmen können bis zu 1 Mio. USD pro Tag und Standort betragen, und angesichts der Sichtbarkeit von öffentlichen Versorgungsunternehmen werden die Vorschriften streng durchgesetzt. In der Folge gab es dokumentierte Fälle von Bußgeldern in Höhe von 50 Mio. $ und mehr allein für einen Standort. Andere Teilbereiche haben eine ähnliche Bußgeldstruktur. Cyber-Strafen sind nicht ganz so kodifiziert, aber die Nichteinhaltung ist angesichts der Sanktionen immer noch ein kostspieliges Unterfangen.
4. **Menschenleben**: Die schlimmste Folge eines physischen Angriffs ist natürlich der Verlust von Menschenleben. Die nachgelagerten Auswirkungen werden durch einen Vorfall in North Carolina deutlich, bei dem eine untergeordnete Anlage physisch angegriffen wurde, was erhebliche Auswirkungen auf eine Gemeinde mit über 50.000 Einwohnern hatte. Die Menschen verloren ihr Leben, weil die Klimaanlage während einer brütenden Hitzewelle nicht betrieben werden konnte.

Bedrohlichste zukünftige Risiken

Physische Bedrohungen haben bereits greifbare Auswirkungen gezeigt, und die zunehmende Reaktion der Versorgungsunternehmen und der staatlichen Aufsichtsbehörden zeugt von der Ernsthaftigkeit dieses sich entwickelnden Problems. Und da Cyber-Bedrohungen immer stärker in den Vordergrund rücken, werden wir wahrscheinlich mehr Richtlinien, mehr Beschränkungen und mehr Anforderungen an den Schutz sehen. Die rasche Eskalation der Cyber-Bedrohungen wird es erforderlich machen, dass die Reaktionen darauf Schritt halten. Da sich die Cyber-Bedrohung jedoch ständig weiterentwickelt, ist eine weniger präskriptive, proaktivere technologische Reaktion erforderlich.

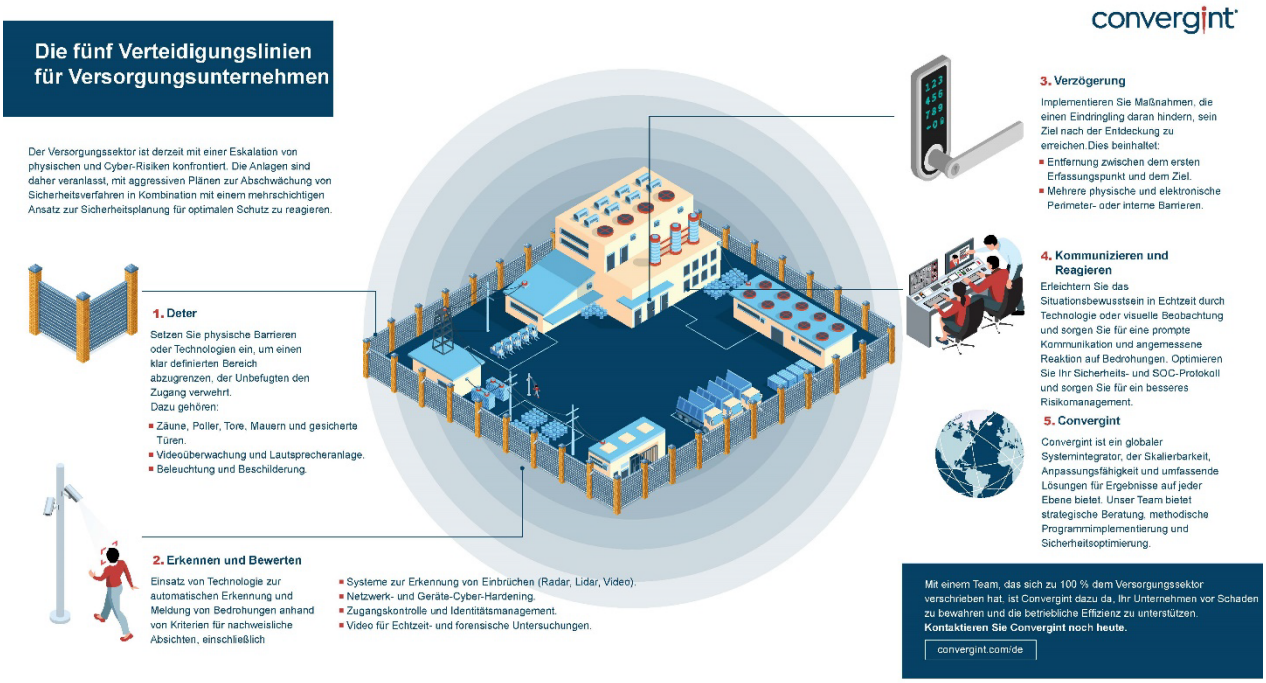
Insgesamt werden die Sicherheitsvorschriften und die Empfehlungen zur Risikominderung für Versorgungsunternehmen ständig angepasst, um angesichts der zunehmenden Zahl von Angriffen und der zunehmenden Raffinesse eine angemessene Orientierung zu bieten. Dies wird auch die Anlagen betreffen, die bisher als weniger risikoreich galten. Letztendlich werden Mindestsicherheitsmaßnahmen festgelegt, die nicht verhandelbar sein werden.

Sicherheitstechnische Gegenmaßnahmen

Convergint empfiehlt **Versorgungsunternehmen, aufkommenden physischen und Cyber-Bedrohungen mit einem Defense-in-Depth-Ansatz für die Sicherheit zu begegnen**. Jedes Sicherheitssystem kann in Frage gestellt werden, wenn genügend Zeit und Geld zur Verfügung steht; daher hängt die Bereitschaft von der Komplexität und einer umfassenden Strategie ab. Aktuelle Ereignisse veranlassen Versorgungsunternehmen dazu, mit aggressiven Plänen zur Verfahrensminderung und mehrschichtigen Sicherheitslösungen zu reagieren:

- **Abschrecken:** Durch den Einsatz von physischen Barrieren oder Technologien für einen klar definierten Bereich, um unbefugten Zugriff zu verhindern.
- **Erkennen und Bewerten**: Durch den Einsatz von Technologie zur automatischen Erkennung und Benachrichtigung von Bedrohungen mit definierten Kriterien für nachweisbare Absichten.
- **Verzögerung.** Durch die Umsetzung von Maßnahmen, die einen Eindringling davon abhalten, die Zielobjekte zu erreichen, kann die Abschreckung überwunden werden.
- **Kommunizieren und Reagieren:** Durch die Nutzung von Echtzeit-Bewusstsein über Technologie und visuelle Beobachtung, um eine schnelle Kommunikation und angemessene Reaktion auf Bedrohungen zu gewährleisten.

convergint | utilities



Letztlich **stoppen** die **Maßnahmen zur Tiefenverteidigung die Angreifer in ihrer Spur oder liefern Warnungen und Benachrichtigungen, um eine Reaktion zu koordinieren**. Physikalische oder Cyber-Infiltrationen, die eine Ebene überwinden, werden durch die nächste Ebene verlangsamt oder blockiert, so dass mehr Zeit zur Verfügung steht, um die negativen Folgen für eine Anlage oder einen Betrieb abzumildern oder zu verhindern.

Verbesserung der Effektivität des Sicherheitspersonals/ Kostenreduzierung

Versorgungsunternehmen stehen vor besonderen betrieblichen Herausforderungen. Viele haben sowohl mit einer alternden Infrastruktur als auch mit einer alternden Belegschaft zu kämpfen. Daher ist es wichtig, dass sie die Effektivität des Sicherheitspersonals durch den Einsatz von physischer und elektronischer Sicherheitstechnologie verbessern.

Sich entwickelnde Bedrohungen machen eine Neubewertung von Richtlinien, Verfahren, Implementierungsstrategien, der Charakterisierung von Vermögenswerten und der Klassifizierung der einzelnen Auswirkungen auf das Geschäft erforderlich. Darüber hinaus müssen Unternehmen die Ausgaben mehrerer Abteilungen für jeden Standort übergreifend nutzen und die Sicherheitsmaßnahmen für optimale Sicherheit und bessere Geschäftsergebnisse zusammenführen. Die Einbeziehung und Beteiligung aller Geschäftsbereiche an einer organisatorischen Sicherheitsstrategie sorgt für ein größeres Sicherheitsbewusstsein, mehr Eigenverantwortung und mehr Verantwortlichkeit, was **zu einem robusteren Geschäftsprogramm führt**.

Verwaltung des Sicherheitsbudgets

Die Budgets müssen die Umweltbedingungen, die Risiken und die Rangfolge der Vermögenswerte berücksichtigen. Außerdem empfehlen wir:

1) **Kurzfristig:** Die Versorgungsunternehmen konzentrieren sich nicht mehr ausschließlich auf die Senkung der Kosten des Sicherheitsbudgets, sondern versuchen stattdessen, mehr aus den Ausgaben zu machen. Ein Umdenken im Bereich der Sicherheit in Bezug auf betriebliche Vorteile und Effizienzsteigerungen ist von größerem Wert. - Grafik "Operative Effizienz" hinzufügen
2) **Langfristig:** Die Versorgungsunternehmen sollten sich überlegen, wie sie die "Stadt", die sie bedienen, nutzen können - Behörden, Gesundheitswesen, Schulen usw. Erkundigen Sie sich, was die Kunden/Nachbarn in puncto Sicherheit tun und wie die Integration alle Beteiligten effizienter machen kann. Prüfen Sie, ob es eine Dualität zwischen Sicherheit und Betrieb und möglicherweise sogar Sicherheit gibt, die Sie durch die Bündelung Ihrer Bemühungen fördern könnten. Denken Sie über die proaktive Fähigkeit der Nutzung von Sicherheitstechnologien in allen vertikalen Bereichen nach, insbesondere angesichts der Geschwindigkeit des Fortschritts. Bidirektionale Daten und Integration würden es den Versorgungsunternehmen ermöglichen, einen isolierten Ansatz für die Sicherheit zu überwinden und die Effektivität auf sehr effiziente Weise zu verbessern. Durch die gemeinsame Nutzung von SOCs könnte die Sicherheit weniger zu einer Kostenstelle und mehr zu einem Profitcenter werden. Dies mag im Moment noch schwer vorstellbar sein. Mit der Bewältigung von Cyber-Bedrohungen ist der Übergang zu einer Cloud-basierten Umgebung jedoch unvermeidlich, was die Integration erleichtern wird.

Einsatz von Sicherheitstechnologie zur Verbesserung der Wettbewerbsfähigkeit von Unternehmen oder Marken

Letztendlich verbessert der Einsatz modernster Sicherheitstechnologie zur Erhöhung der Sicherheit und zur Unterstützung der betrieblichen Effizienz die Gesamtleistung des Unternehmens und sorgt für ein optimales Kundenerlebnis. Und ganz nebenbei führt dies zu mehr Sicherheit und Zufriedenheit der Mitarbeiter.

Zusammenfassung der Empfehlungen, 2024

Da der physische und digitale Fußabdruck des Versorgungssektors immer größer wird und sich weiterentwickelt, um die ständig wachsende Nachfrage der Verbraucher zu befriedigen, müssen auch die Schutzmaßnahmen für bestehende und neue Anlagen angepasst werden. Die Branche wird ständig bedroht, und der ständige Kampf der Versorgungsunternehmen mit ihren Sicherheitspartnern und böswilligen Akteuren erfordert einen kontinuierlichen Prüfungs- und Bewertungsprozess über den gesamten Lebenszyklus. Dies bedeutet eine ständige Neubewertung von Richtlinien, Prozessen, Verfahren und Technologien, um sicherzustellen, dass das Versorgungsunternehmen ein hohes Maß an Bedrohungsbewusstsein und ein robustes Sicherheitsprogramm aufrechterhält, das auf Auswirkungen reagieren oder Risiken für den Geschäftsbetrieb und das Personal mindern kann. Ergänzt wird dies durch eine wiederkehrende Charakterisierung der Anlagen, Schwachstellenbewertungen und Bedrohungsevaluierungen, bei denen Abhilfestrategien, einschließlich technologischer Verbesserungen und Änderungen, gründlich getestet werden müssen.

Die finanzielle Belastung durch die Entwicklung einer robusteren und mehrschichtigen Schutzstrategie muss nicht allein durch die Budgets der typischen Sicherheitsabteilungen

gedeckt werden. Die Ausgaben mehrerer Abteilungen können durch den Einsatz von Mehrzwecktechnologien genutzt werden, die die betriebliche Effizienz steigern und die Sicherheit verbessern. Video- und Zugangskontrollsysteme auf Unternehmensebene können als integrierte Plattform dienen, um alle Arten von Informationen für die betriebliche Nutzung bereitzustellen. Systeme wie Anlagenüberwachung, Umweltsensoren, Luftqualität, Lebensschutzsysteme und andere Sicherheitssysteme können über eine einzige Plattform an verschiedene Interessengruppen und Abteilungen übermittelt werden. Anschließende schnelle Echtzeit-Benachrichtigungen können den Bedarf an Vor-Ort-Ressourcen für die Instandhaltung verringern und Prüfpfade erleichtern.

Letztlich ist Kommunikation der Schlüssel, und kein Problem muss in einem Vakuum gelöst werden. Die ständige Zusammenarbeit mit anderen Branchen oder Unternehmen, die mit ähnlichen Bedrohungen konfrontiert sind, kann dabei helfen zu ermitteln, welche Lösungen realistisch sind, um den Geschäftsanforderungen gerecht zu werden und diese zu sichern. Betriebliche Einblicke durch Benchmarking und Benutzerforen können relevante Anwendungsfälle und bewährte Praktiken enthalten, die wiederum für Finanzierungsanträge und die Entwicklung von Strategien zur Einführung von Innovationen genutzt werden können. Die Kommunikation mit den zuständigen Behörden wie den örtlichen Strafverfolgungsbehörden oder den Regulierungsbehörden der Branche kann dazu beitragen, dass ein Unternehmen über lokale oder branchenspezifische Bedrohungen auf dem Laufenden bleibt.

Eine Sicherheitsstrategie sollte vielschichtig sein und unter sorgfältiger Berücksichtigung der spezifischen geschäftlichen und betrieblichen Anforderungen entwickelt werden, wobei alle verfügbaren Ressourcen und relevanten Erfahrungen genutzt werden sollten. Convergint ist der perfekte Ratgeber, um Versorgungsunternehmen auf diesem Weg zu begleiten. Wir **nutzen Branchen-Benchmarking, Technologiepartner und engagierte Sicherheitsexperten** für alle Teilbereiche der Versorgungswirtschaft, um eine optimierte und maßgeschneiderte Lösung zu entwickeln, die diese Anforderungen erfüllt.