convergint | utilities

Guia de práticas recomendadas, **2024: Serviços públicos**

convergint® | utilities

O setor de serviços públicos está passando por **uma escalada de riscos físicos e cibernéticos em escala nacional e global** que exige a priorização do planejamento de segurança e da mitigação de procedimentos. A equipe dedicada da Convergint para o setor de utilidades fornece estratégias de proteção de alta segurança, implementação metódica de programas e soluções abrangentes com foco na condução de segurança e eficiência operacional nesse setor. Com um profundo entendimento das ameaças do setor e dos requisitos de conformidade regulatória, a Convergint implementa um projeto em camadas para garantir desempenho e funcionalidade ideais.

Incidentes e riscos de segurança em serviços públicos

Há muito tempo, os locais de operações críticas representam um risco maior para as empresas de serviços públicos devido à abundância de ativos. No entanto, até mesmo os locais de downstream provaram exigir proteção e mitigação de riscos devido aos impactos nos negócios e na comunidade e à atenção da mídia nacional que vem com um incidente de segurança.

Por fim, quando se trata de avaliações de risco para identificação de ativos, estratégia de proteção e planejamento de mitigação de riscos, **é essencial realizar avaliações por subvertical** para adaptar as soluções aos ativos, regulamentos, operações comerciais e riscos exclusivos associados a um setor específico.

Serviços públicos de energia nuclear

A energia nuclear é única por ser tão intensamente regulamentada e altamente protegida. O raciocínio é claro. Um ataque bem-sucedido, seja físico ou cibernético, poderia resultar na liberação descontrolada de radioatividade, levando a impactos ambientais e de saúde significativos, incluindo a possibilidade de fatalidades a curto e longo prazo. Por regulamentação da NRC (Comissão Reguladora Nuclear), as instalações nucleares são obrigadas a adotar uma abordagem altamente prescritiva de segurança para evitar ou atenuar o impacto de incidentes.

As usinas nucleares são estruturalmente robustas com intenção e impedem intrusões físicas por projeto. Além disso, uma abordagem rigorosa em camadas para a proteção física fornece reforço e inclui uma força de resposta humana de estilo militar. As ameaças cibernéticas também são tratadas com diligência e protocolos exaustivos que estão em vigor para gerenciar riscos, monitorar eventos constantemente e fornecer um nível de separação das redes externas. Em última análise, esse subsetor é bem protegido, mas passa por testes regulares para que os equipamentos e protocolos sejam continuamente reavaliados para garantir proteções e ameaças em evolução.

Serviços de eletricidade

As concessionárias de energia elétrica utilizam agências de resposta internas e/ou externas para interditar possíveis agentes mal-intencionados da ameaça. O aumento do risco pode levar a uma reavaliação dessa estratégia. De acordo com o Departamento de Energia, houve 95 incidentes relacionados a humanos, incluindo vandalismo e eventos cibernéticos, no primeiro semestre de 2023, o que excedeu qualquer período da história.

Os ataques físicos continuam sendo a principal preocupação desse setor. O terrorismo doméstico, especificamente, tem causado estragos nas operações de campo e nas comunidades atendidas pelas estações de transmissão elétrica. O sul dos EUA e o noroeste do Pacífico têm sido particularmente desafiados desde 2022, e a situação não parece estar melhorando. Isso exige uma defesa em várias camadas, agora cada vez mais adotada por subestações em todos os lugares.

Serviços de água

As ameaças físicas estão em alta para as concessionárias de água, o que leva a um foco na proteção dos ativos mais vulneráveis a ataques. Assim como nas instalações elétricas, uma abordagem de defesa em profundidade parece ser a mais prudente.

Lamentavelmente, as ameaças cibernéticas estão aumentando simultaneamente para as concessionárias de água. Os sistemas SCADA (Supervisory Control and Data Acquisition, Controle de Supervisão e Aquisição de Dados) são essenciais para o monitoramento operacional e o controle dos principais ativos para manter o armazenamento limpo e a distribuição de água aos consumidores. Manter o controle e a observação rigorosos desses sistemas, além de manter boas práticas de segurança cibernética nos sistemas comerciais, é fundamental para evitar ou atenuar os ataques cibernéticos. Essa necessidade é exemplificada pelo recente ataque a um prédio da autoridade de água na zona rural do condado de Allegheny, PA, aparentemente perpetrado por um agente do estado. A autoridade conseguiu se desconectar e retomar as operações manualmente sem incidentes, mas a mensagem foi recebida em alto e bom som: os esforços de segurança física precisam ser executados em paralelo com as proteções cibernéticas.

Renováveis: Solar, eólica e bioenergia

Embora menos proeminentes no cenário de serviços públicos, as energias renováveis têm uma pegada nacional crescente, o que significa um aumento de alvos e riscos potenciais. As energias renováveis têm ativos que são igualmente vulneráveis e foram levadas a preparar defesas físicas e cibernéticas. Um incêndio ocorrido em 2023 em uma instalação de painéis solares em Las Vegas como uma "declaração política" é apenas uma indicação do que pode acontecer se esse

subsegmento não estiver preparado com uma resposta adequada às ameaças emergentes.

O setor como um todo

A segurança física parece ser a principal preocupação de todas as empresas de serviços públicos, e com razão. O custo das invasões é evidente nas manchetes dos jornais do país. Dito isso, **as ameaças cibernéticas estão se tornando mais proeminentes à medida que sistemas obsoletos** e redes abertas criam uma clara oportunidade de acesso. Além disso, os agentes do estado-nação estão se tornando uma ameaça mais proeminente, aumentando o risco além da simples invasão.

É essencial que o setor adote uma postura firme em relação ao crime cibernético e invista adequadamente para impedir e atenuar as ameaças e, ao mesmo tempo, implemente estratégias abrangentes de segurança física.

O custo de ataques físicos ou cibernéticos

Há quatro categorias principais de perdas resultantes de uma intrusão física ou cibernética para as empresas de serviços públicos:

1. **Reputação/confiança:** Embora as concessionárias de serviços públicos possam não convidar incidentes, a percepção de falta de preparação pode minar a confiança do cliente e prejudicar sua reputação na comunidade. Em muitos casos, mudar para um concorrente não será uma opção, mas um impacto na percepção da marca ainda é significativo para uma empresa de serviços públicos.
2. **Perda de negócios**: Os desligamentos de serviços públicos forçados por ataques físicos ou cibernéticos geram uma perda comercial tangível e um declínio mensurável nos fluxos de receita.
3. **Multas:** As multas por não conformidade física para as concessionárias de energia elétrica podem exceder US$ 1 milhão por dia e por local e, dada a visibilidade das concessionárias de serviços públicos, as regulamentações são fortemente aplicadas. Posteriormente, foram documentados casos de mais de US$ 50 milhões em multas em um único local. Outros subverticais têm uma estrutura de multas semelhante. As penalidades cibernéticas não são tão codificadas, mas a não conformidade ainda é um empreendimento caro devido às sanções.
4. **Vida humana**: Obviamente, o resultado mais preocupante após um ataque físico é a perda de vidas humanas. As ramificações a jusante são claramente exemplificadas por um incidente na Carolina do Norte, onde um ativo de nível inferior foi atacado fisicamente com impactos significativos em uma comunidade de mais de 50 mil habitantes. Pessoas perderam a vida devido à incapacidade de ligar o ar condicionado durante uma onda de calor sufocante.

Riscos futuros mais ameaçadores

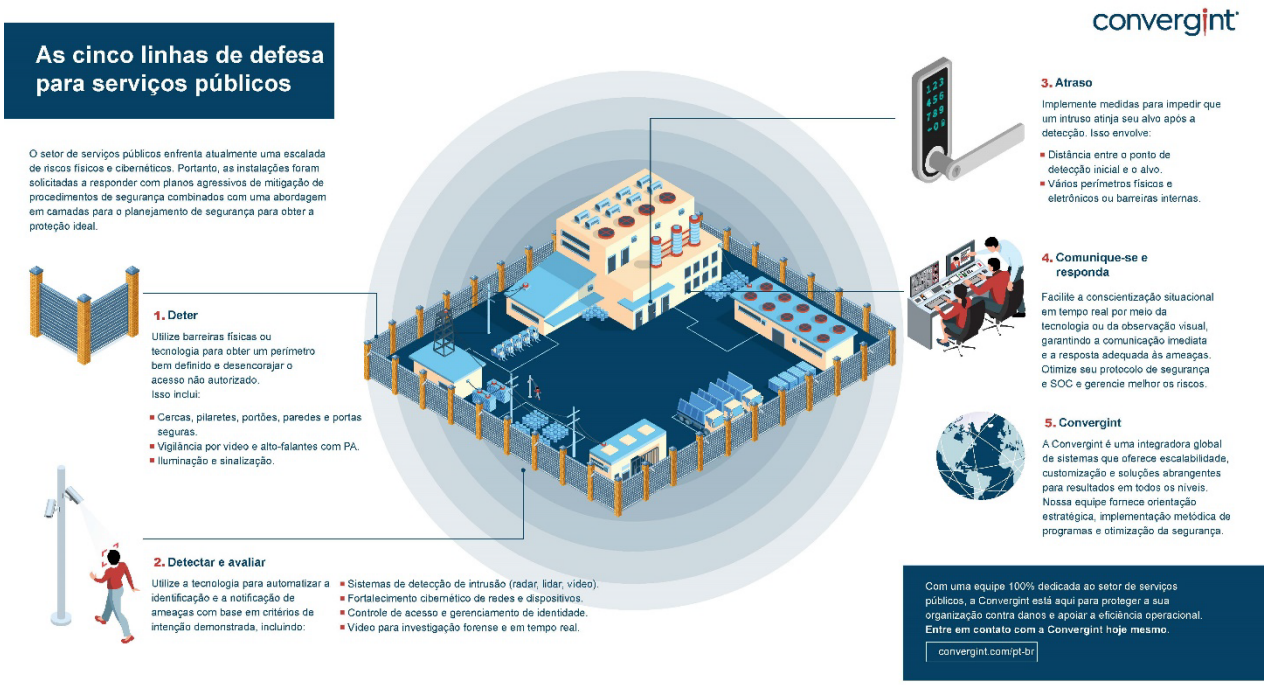
As ameaças físicas já mostraram ramificações tangíveis, e uma resposta cada vez maior das concessionárias e da supervisão governamental é um testemunho da seriedade desse problema em evolução. E à medida que as ameaças cibernéticas se tornam cada vez mais proeminentes, provavelmente veremos mais orientações, mais restrições e mais requisitos de proteção. A rápida escalada da ameaça cibernética exigirá que a resposta acompanhe esse ritmo. Dito isso, a natureza fluida da ameaça cibernética se traduz em uma resposta tecnológica menos prescritiva e mais proativa.

Como um todo, as normas de segurança e as recomendações de mitigação para empresas de serviços públicos serão continuamente ajustadas para fornecer orientação adequada diante do aumento do número de ataques e dos níveis de sofisticação. Isso afetará até mesmo os ativos anteriormente considerados de nível inferior em termos de risco. Em última análise, haverá medidas mínimas de segurança estabelecidas, e elas não serão negociáveis.

Contramedidas de tecnologia de segurança

A Convergint recomenda que **as empresas de serviços públicos combatam as ameaças físicas e cibernéticas emergentes com uma abordagem de defesa em profundidade para a segurança**. Qualquer sistema de segurança pode ser desafiado com tempo e dinheiro suficientes; portanto, a prontidão depende da complexidade e de uma estratégia abrangente. Os eventos atuais levam as concessionárias a responder com planos agressivos de mitigação de procedimentos e soluções de segurança em várias camadas para:

- **Dissuadir:** Utilizando barreiras físicas ou tecnologia para um perímetro bem definido para desencorajar o acesso não autorizado.
- **Detectar e avaliar**: Utilizando a tecnologia para automatizar a identificação e a notificação de ameaças com critérios definidos para intenção demonstrada.
- **Atraso.** Ao implementar medidas para impedir que um invasor atinja os ativos visados, eles devem superar a dissuasão.
- **Comunicar e responder:** Aproveitando a conscientização em tempo real por meio da tecnologia e da observação visual para garantir a comunicação imediata e a resposta adequada às ameaças.



Em última análise, **as medidas de defesa em profundidade impedem que os perpetradores fiquem em seu caminho ou fornecem alertas e notificações para coordenar uma resposta**. As infiltrações físicas ou cibernéticas que conseguem passar por uma camada são retardadas ou bloqueadas pela camada seguinte, dando ainda mais tempo para atenuar ou evitar um resultado negativo para um ativo ou operações.

Melhoria da eficácia da força de trabalho de segurança/ Redução de custos

Os serviços públicos são únicos em seu conjunto de desafios operacionais. Muitos estão gerenciando uma infraestrutura e uma força de trabalho envelhecidas. Portanto, é essencial que elas melhorem a eficácia da força de trabalho de segurança por meio do aumento da tecnologia de segurança física e eletrônica.

A evolução das ameaças gera a necessidade de reavaliar o processo de políticas, os procedimentos, as estratégias de implementação, a caracterização dos ativos e a classificação de cada impacto nos negócios. Além disso, as entidades precisam alavancar os gastos de vários departamentos em todos os locais, unindo as operações de segurança para obter a segurança ideal e resultados comerciais mais impactantes. A inclusão e a participação de todas as unidades de negócios em um utilitário para uma estratégia de segurança organizacional proporcionam maior conscientização, propriedade e responsabilidade pela segurança, **resultando em um programa de negócios mais robusto**.

Gerenciando o orçamento de segurança

Os orçamentos devem considerar as condições ambientais, os riscos e a classificação dos ativos. Além disso, recomendamos:

1) **Curto prazo:** As empresas de serviços públicos deixam de se concentrar exclusivamente na redução do custo do orçamento de segurança e, em vez disso, buscam obter mais dos gastos. Há mais valor a ser obtido ao repensar a segurança em termos de benefícios operacionais e maior eficiência. - Adicionar gráfico de eficiência operacional
2) **Longo prazo:** Os serviços públicos consideram a possibilidade de aproveitar "a cidade" atendida - governo, saúde, escolas etc. Pergunte o que os clientes/adjuntos estão fazendo em termos de segurança e como a integração pode tornar todos mais eficientes. Avalie se há dualidade entre segurança e operações e, potencialmente, até mesmo segurança no futuro, o que poderia ser facilitado por meio de camadas de esforços. Pense na capacidade proativa de alavancar a tecnologia de segurança em todos os setores verticais existentes, especialmente considerando o ritmo do avanço. A integração e os dados bidirecionais permitiriam que as concessionárias de serviços públicos fossem além de uma abordagem isolada da segurança, melhorando a eficácia de uma maneira muito eficiente. A segurança poderia se tornar menos um centro de custos e mais um centro de lucros com coisas como o compartilhamento de SOCs. Isso pode ser difícil de visualizar no momento. Dito isso, como as ameaças cibernéticas são gerenciadas, a mudança para um ambiente baseado em nuvem é inevitável, o que facilitará a integração.

Utilização da tecnologia de segurança para melhorar a competitividade da empresa ou da marca

Em última análise, aproveitar a tecnologia de segurança de ponta para aumentar a segurança e apoiar a eficiência operacional melhora o desempenho geral dos negócios e garante uma experiência ideal para o cliente. E isso leva à segurança e à satisfação dos funcionários ao longo do caminho.

Resumo das recomendações, 2024

Como a pegada física e digital do setor de serviços públicos continua a se expandir e evoluir para atender a uma demanda cada vez maior dos consumidores, o mesmo deve ocorrer com as proteções para os ativos existentes e novos. As ameaças ao setor são contínuas, e a batalha constante entre o setor de serviços públicos e seus parceiros em segurança e agentes mal-intencionados significa que deve haver um processo contínuo de auditoria e avaliação do ciclo de vida. Isso se traduz em uma reavaliação constante de políticas, processos, procedimentos e tecnologias para garantir que a empresa de serviços públicos mantenha um alto nível de conscientização sobre as ameaças e um programa de segurança robusto que possa responder aos impactos ou atenuar os riscos às operações comerciais e ao pessoal. Isso é complementado pela caracterização recorrente de ativos, avaliações de vulnerabilidade e avaliações de ameaças, que devem testar exaustivamente as estratégias de atenuação, inclusive aprimoramentos e modificações tecnológicas.

O ônus financeiro do desenvolvimento de uma estratégia de proteção mais robusta e em camadas não precisa ser coberto apenas pelos orçamentos típicos do departamento de

segurança. Os gastos de vários departamentos podem ser aproveitados com o emprego de tecnologias multiuso que geram eficiência operacional e aumentam a segurança. Os sistemas de controle de acesso e vídeo de nível empresarial podem servir como uma plataforma integrada para trazer todos os tipos de informações para uso operacional. Os sistemas que incluem monitoramento de ativos, sensores ambientais, qualidade do ar, sistemas de segurança de vida e outros sistemas de segurança podem aproveitar uma única plataforma para transmitir informações a várias partes interessadas e departamentos. As notificações subsequentes, rápidas e em tempo real, podem reduzir a demanda de recursos de campo para manutenção e facilitar as trilhas de auditoria.

Em última análise, a comunicação é fundamental, e nenhum problema precisa ser resolvido em um vácuo. A colaboração constante com outros setores ou empresas que enfrentam ameaças semelhantes pode ajudar a determinar quais soluções são realistas para implementação a fim de atender e proteger as necessidades dos negócios. Os insights operacionais por meio de benchmarking e fóruns de usuários podem incluir casos de uso relevantes e práticas recomendadas que, por sua vez, podem ser aproveitados para solicitações de financiamento e desenvolvimento de estratégias de implementação de inovação. A comunicação com as agências de resposta, como as autoridades policiais locais ou os órgãos reguladores do setor, pode ajudar a manter a empresa atualizada sobre as ameaças locais ou específicas do setor.

Uma estratégia de segurança deve ter várias camadas e ser projetada com uma consideração cuidadosa das necessidades específicas do negócio e das operações, utilizando todos os recursos disponíveis e a experiência relevante. A Convergint é o guia perfeito para conduzir as empresas de serviços públicos nessa jornada. Aproveitamos **o benchmarking do setor, os parceiros de tecnologia e os especialistas em segurança dedicados** a todos os subverticais de serviços públicos para apoiar o desenvolvimento de uma solução otimizada e personalizada para atender a essas necessidades.