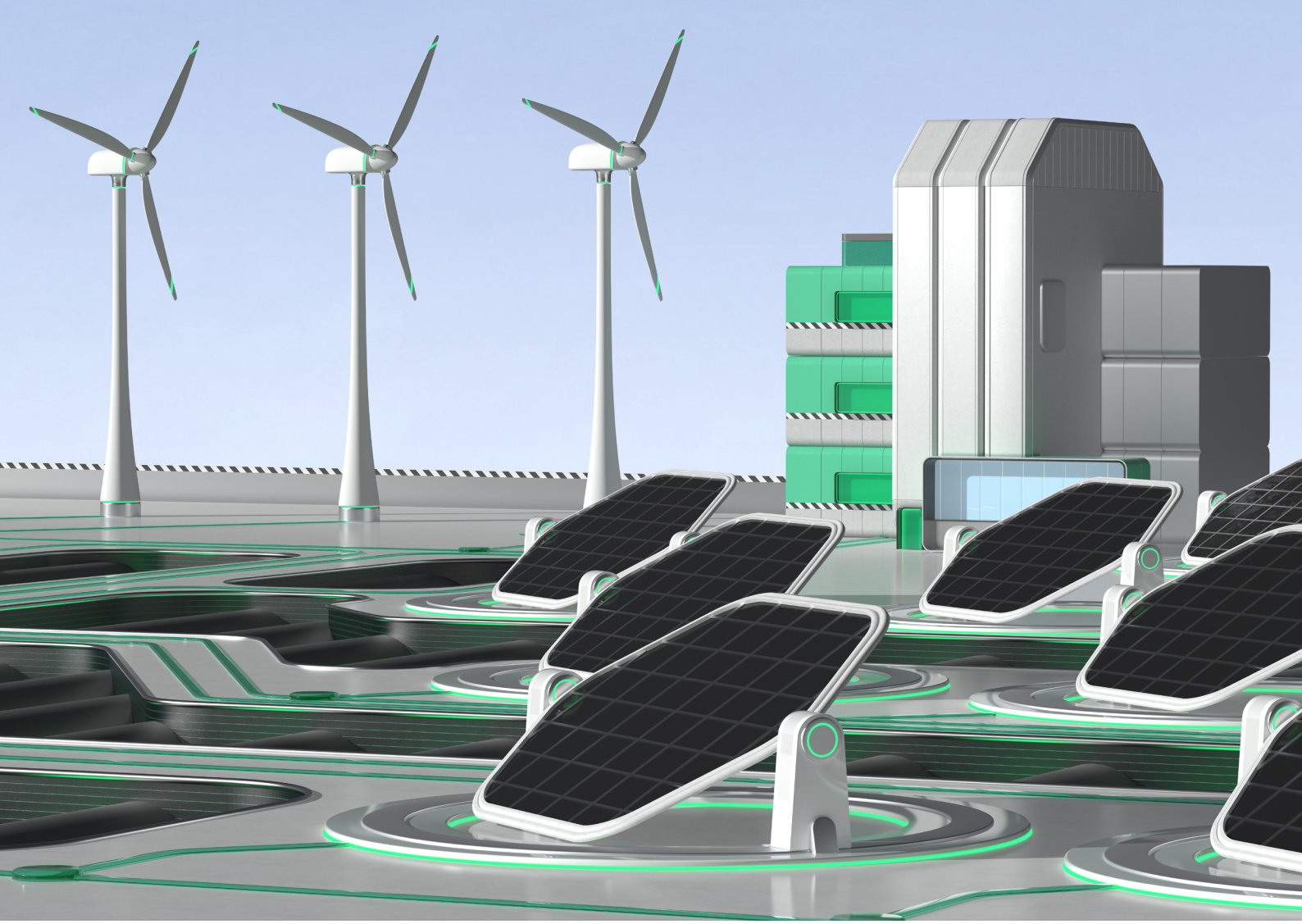

Construindo um futuro mais seguro no setor de serviços públicos

kaspersky PREPARADOS PARA O FUTURO

go.kaspersky.com/utilities_br 2022

Introdução

A produção do setor de serviços públicos – serviços de aquecimento, energia, luz, água e esgoto – corre nas veias de cada indústria do planeta como sangue sem o qual nada funcionaria. No entanto, os incidentes de segurança cibernética em 2021 demonstraram que o setor de serviços públicos é um alvo crescente de crimes cibernéticos, bem como de atos de ciberguerra.

O setor de serviços públicos está passando por uma mudança rápida que não mostra sinais de desaceleração. Além da transformação digital disruptiva, esse setor está sob uma pressão ímpar para modificar os próprios ativos que produz. Descarbonização, energias renováveis, eficiência energética e descentralização estão na ordem do dia, e apenas a tecnologia mais inteligente e inovadora pode atender a esses requisitos. Para piorar, há diversos requisitos regulatórios com os quais as concessionárias de serviços públicos devem lidar em um mercado cada vez mais global.

Neste documento, vamos abordar as principais tendências que estão transformando o setor de serviços públicos no momento e revelar os desafios e os riscos que elas trazem. A nossa visão é de um mundo onde as concessionárias de serviços públicos sejam livres para maximizar a adoção de tecnologias inteligentes impulsionadas por eficiência, sem temer a devastação que pode ser forjada por atores cibernéticos mal-intencionados.

Inteligência artificial

Análise de dados

Descarbonização

Recursos de energia distribuídos

Desafios regulatórios

Tendência N° 1: Inteligência artificial (IA)

A inteligência artificial está rompendo a maneira pela qual o setor atinge um fornecimento constante (e eficiente) do qual a reputação e os contratos dos fornecedores dependem. Essas tecnologias foram viabilizadas pela disponibilidade de poder computacional massivo via nuvem, pela proliferação de big data e pela sofisticação crescente da perspicácia algorítmica.

No lado da produção, as concessionárias de serviços públicos aproveitam IA para estimar cargas, otimizar produções, analisar consumo, prever demanda, evitar roubos ou interferências mal-intencionadas, e realizar manutenção profilática e tarefas de reparo. As concessionárias de serviços públicos também buscam implementar essas tecnologias disruptivas em outras funções de negócios, incluindo vendas, operações, serviços para clientes, gerenciamento de instalações, aquisições e TI.

Aplicações comuns de IA incluem análise de padrões climáticos históricos para calcular impactos futuros na rede elétrica e comportamentos de clientes e implementar equipamentos e mão de obra de forma a minimizar o tempo de inatividade futuro relacionado ao clima. Os serviços públicos estão experimentando drones não tripulados junto com IA para coletar dados e imagens de equipamentos de campo e identificar riscos de falha de forma muito mais eficiente do que por meio de inspeções manuais. As concessionárias de serviços públicos também estão apenas começando a compreender o possível papel de IA em coordenar recursos de energia distribuídos como vento, bateria e energia solar. Mas isso é apenas o começo. Os serviços públicos detêm enormes quantidades de dados de clientes inestimáveis e podem usar IA para melhorar todos os aspectos do engajamento de seus clientes, além de transformar seus modelos de negócios.

Aplicações de IA para serviços públicos:

- Remodelação da experiência dos clientes.
- Simplificação das tarefas de manutenção.
- Antecipação de cargas de energia.
- Integração de recursos de energia distribuídos (DERs).
- Otimização de geração, transmissão e distribuição.

"Uma usina de energia que funcionará a base de "inteligência artificial" está prestes a dar a largada no oeste da África. O empreendimento conjunto entre a Xcell Security House and Finance localizada na Suíça e a Beyond Limits localizada nos EUA incorporará inteligência e conscientização às operações – algo que gerará mais eficiência, melhor produtividade e maior proteção ambiental."
Forbes

IA também facilita a automação de processos robóticos (RPA). RPA é flexível, dimensionável e pode ser adaptada para os requisitos específicos de cada serviço público. Ela reduz custos e possibilita atualizações de serviços. Ela também ajuda a solucionar escassez de mão de obra, gerenciando tarefas simples para clientes como leituras automáticas de medidores e alguns aspectos de controle e conformidade regulatórios. Serviços públicos estão transferindo rapidamente processos de rotina, sistemáticos e baseados em regras para RPA.

Na maioria esmagadora dos casos, as concessionárias de serviços públicos utilizam terceiros para fornecer as tecnologias inovadoras necessárias. Esses terceiros incluem blue-chips sazonais (como a General Electric), bem como recém-chegadas (como a Open Energi). Vamos ver estes dois exemplos:

A Digital Wind Farm da General Electric usa dados constantemente coletados sobre tempo, mensagens de componentes, relatórios de serviços, e desempenho de modelos similares, para criar um modelo preditivo que permita que os clientes melhorem o desempenho e também reduzam os riscos e os custos. Nas próprias palavras da General Electric, "A Digital Wind Farm é um sistema de energia eólica end-to-end que aproveita dados, análises e aplicativos de software em parceria com as nossas soluções de hardware e serviços para melhorar a eficiência, a segurança cibernética, a confiabilidade e a lucratividade de seus ativos ao longo de suas vidas úteis."

A Open Energi "gerencia energia distribuída para reduzir radicalmente custos de eletricidade e fornecer capacidade flexível para viabilizar um sistema de energia 100% renovável." A plataforma Dynamic Demand da Open Energi explora IA para maximizar a utilização de ativos, cortar custos e otimizar desempenho. Em julho de 2021, a British Petroleum adquiriu a Open Energi e planeja expandir seu modelo de negócios globalmente.

Ameaça em destaque: IA é como energia nuclear – "tanto promissora quanto perigosa" (Bill Gates)

Os riscos de IA são universais, independente da aplicação: se o sistema computacional por trás dessas tecnologias for comprometido, os sistemas que dependem delas serão prejudicados. O problema para o setor de serviços públicos é que as apostas são muito altas. Sem eletricidade, água, esgoto, energia e luz, as nossas sociedades sucumbirão. Essa precariedade é piorada pela imaturidade dessas tecnologias disruptivas.

O fato de que a sobrevivência de populações inteiras (para não mencionar empresas) depende do fornecimento seguro de água, energia e gás, torna as empresas de serviços públicos alvos muito populares, não apenas para crimes cibernéticos, mas também para ciberguerra. Atores estatais sabem que paralisar a infraestrutura de serviços públicos de um país do conforto de

um computador mal-intencionado poderia destruir mais do que qualquer bomba. Um recente estudo da Forrester descobriu que 88% dos profissionais de segurança esperam que ataques orientados a IA se tornem predominantes.

Em 6 de maio de 2021, um sinal de alerta foi disparado quando o Colonial Pipeline, o maior gasoduto dos Estados Unidos, foi desligado devido a um ataque de ransomware atribuído ao DarkSide, um grupo de hacking de língua russa.

Tendência N° 2: Análise de dados

Dados são o combustível essencial que impulsiona avanços tecnológicos e digitais no setor de serviços públicos. O setor de serviços públicos está testemunhando uma revolução na coleta e na análise de dados em tempo real em um ritmo cada vez mais rápido para possibilitar planejamento proativo e tomada de decisões. A análise avançada combinada com a experiência humana permitem que os serviços públicos melhorem o engajamento de clientes, bem como gerenciem melhor as cadeias de suprimentos e os riscos da rede, além de atualizarem tarefas de manutenção preventiva e planejamento de ativos. Para facilitar a coleta de dados, os serviços públicos estão instalando e atualizando plataformas de análise projetadas para simplificar o uso e a rastreabilidade.

Medição inteligente é uma área crucial das reformas de energia. Essa tecnologia está transformando como os serviços públicos de energia, gás e água operam para atender a novos objetivos ambiciosos. A instalação global de medição inteligente está ganhando ritmo. Entre 2021 e 2025, mais de 572 milhões de medidores de eletricidade inteligentes serão implantados na China, Índia, Japão e Coreia do Sul. Medidores inteligentes são atraentes para os clientes, pois podem ser usados para reduzir contas de energia, mas a grande quantidade de dados que eles coletam também permite que os fornecedores estimulem eficiências no lado da demanda, como parte da Rede Elétrica Inteligente.

A Rede Elétrica Inteligente é uma contrapartida essencial para a revolução dos medidores inteligentes. Espera-se que o mercado de Rede Elétrica Inteligente Global atinja US$ 92+ bilhões em 2026. A tecnologia de Internet das Coisas Industrial está sendo implementada na cadeia de valores dos serviços públicos, da geração a distribuição e consumo. É previsto que o mercado de serviços públicos de IoT registre ganhos acima de 20% em 2024 segundo um relatório Global Market Insights. Sensores em equipamentos em usinas de energia, instalações hidrelétricas, turbinas eólicas e painéis solares possibilitam decisões informadas e, às vezes, automatizadas, permitindo que as concessionárias economizem custos, otimizem o abastecimento e atendam à demanda. A coleta de dados fornece insights inestimáveis sobre como melhorar a segurança e a resiliência.

O relatório da Orbis Research sobre big data global no mercado energético demonstra como big data ajudou as empresas de serviços públicos a acompanharem e preverem padrões de consumo, para alterarem o espaço e o tempo de abastecimento de forma correspondente, gerando uma utilização eficiente de ativos.

Ameaça em destaque: mais dispositivos, mais problemas ("não se engane, é uma guerra")

Adicionar dispositivos a uma rede é como adicionar janelas a um edifício. Quanto mais janelas, maior o risco de invasões (ou violações cibernéticas). Talvez também possamos acrescentar "mais dados, mais problemas"; afinal, dados representam para os criminosos cibernéticos o mesmo que dinheiro para os ladrões. Toda ferramenta de coleta de dados adicionada à rede fornece uma superfície de ataque significativa a ser explorada.

A descarbonização também está aumentando exponencialmente o número de pontos de invasão. Por exemplo, mais dispositivos, como estações de carga de veículos elétricos, estão sendo conectados o tempo todo. Esse cenário é agravado pelo fato de que as tecnologias dos dispositivos estão evoluindo e, assim, podem estar vulneráveis a ameaças cibernéticas novas e desconhecidas. Serviços públicos que protegem um grande número de endpoints com recursos limitados estão particularmente em risco. Soluções baseadas na nuvem estão possibilitando que serviços públicos engajem clientes de novas formas, mas também trazem problemas de segurança adicionais.

Os riscos são autoevidentes. Estima-se que cerca de 25% dos serviços públicos de energia dos EUA tenham sido expostos à violação massiva da SolarWinds em 2020-2021. Ataques de ransomware subiram 116% nos primeiros cinco meses de 2021 segundo a análise de segurança da Nozomi Networks.

Inteligência de ameaças específica do setor é uma parte vital do arsenal de imunidade cibernética de empresas de serviços públicos. Somente a inteligência de especialistas pode ajudar as concessionárias a permanecerem à frente de ameaças novas e desconhecidas. Os treinamentos em recuperação de desastres e resposta a incidentes também são críticos. E, com a proliferação de dispositivos e apps, a Análise Comportamental e de Anomalias deve desempenhar um papel crucial. Essas tecnologias de segurança cibernética combinam análise de dados e IA para "aprender" o comportamento de usuários e, assim, identificar e bloquear imediatamente anomalias que indiquem a presença de qualquer ameaça, até mesmo se ela ainda for desconhecida.

Tendência #3: Descarbonização

Um relatório da McKinsey faz referência à descarbonização industrial como "a próxima fronteira". É claro que, a responsabilidade por essa descarbonização não recai exclusivamente sobre os ombros do setor de serviços públicos, no entanto, há um vínculo natural, e as concessionárias de serviços públicos têm um papel fundamental a desempenhar. Para atingir a descarbonização, o relatório da McKinsey recomenda que "o vínculo entre o setor industrial e o setor de energia seja significativamente reforçado, dadas as interdependências em ambas as direções."

"As partes compartilham uma visão de longo prazo sobre a importância de compreender completamente o desenvolvimento e a transferência de tecnologia para melhorar a resiliência a mudanças climáticas e reduzir emissões de gases de efeito estufa."
Artigo 10 do Acordo de Paris

Energias renováveis e recursos de energia distribuídos (DERs) devem desempenhar um papel crítico no avanço para a descarbonização, no entanto, é a tecnologia em evolução que está tornando a mudança climática possível na escala necessária para o nosso planeta. Como parte do Acordo de Paris, assinado por 174 países e a UE, foi incluído o estabelecimento de um Technology Mechanism, gerenciado pela Convenção-Quadro das Nações Unidas sobre Mudança do Clima (UNFCCC).

"O setor de energia dos EUA está a meio caminho de emissões líquidas zero, mas ficará mais difícil agora."

Embora energias renováveis representem mais de 20% da eletricidade gerada na Europa e nos EUA, as metas são ambiciosas – 33% em 2025 e 95% de aumento líquido na capacidade de energia global até 2050. Atender ao desafio de descarbonização requer mudanças profundas em como os serviços públicos operam – englobando colaboração entre participantes, engajamento de clientes e uma grande revolução tecnológica envolvendo digitalização, sensores, dispositivos de IoT e conectividade, estendendo-se para abranger todos os aspectos de nossas vidas e automatizar iniciativas que impulsionem eficiência.

Três desenvolvimentos tecnológicos são vistos como fundamentais: a superação de motores a combustível por veículos elétricos, a redução dos custos de geração e armazenamento de energias renováveis e o corte nos custos de energias produzidas localmente eliminando a necessidade de transportar energia. Todos os itens acima representam desafios para o setor energético.

Ameaça em destaque: "hipercomplexidade + hiperconectividade + hipervolume de dados = hipervulnerabilidade" (ITU)

O Programa das Nações Unidas para os Assentamentos Humanos estima que as cidades consumam cerca de 75% da energia primária global e emitam entre 50 e 60% de todos os gases de efeito estufa do mundo, com esse número crescendo para aproximadamente 80% quando emissões indiretas geradas por habitantes urbanos são incluídas. As cidades são lugares cruciais para a implementação de novas tecnologias que as empresas de serviços públicos estão adotando de forma crescente para atender as diretrizes e os requisitos de mudanças climáticas.

Infelizmente, isso gera uma tempestade cibernética perfeita, que a ITU descreve como "hipercomplexidade + hiperconectividade + hipervolume de dados = hipervulnerabilidade." As empresas de serviços públicos estão no coração dessa tempestade, navegando por incontáveis dispositivos interconectados, acumulando e processando enormes conjuntos de dados, e enfrentando regulamentações cada vez mais rigorosas que mudam a um ritmo vertiginoso.

A ITU defende que segurança cibernética, proteção de informações e resiliência de sistemas sejam questões políticas e de governança. O relatório da ITU, "Cybersecurity, data protection and data resilience in smart cities" estressa "os possíveis efeitos de ataques mal-intencionados e desastres em sistemas e infraestrutura de ICT, incluindo privação de serviços essenciais a cidadãos, desde transportes a serviços públicos (por exemplo, redes elétricas inteligentes, gerenciamento de água)."

A revista de tecnologias emergentes Wired prevê: "Uma infraestrutura cada vez mais conectada facilitará que os hackers tomem cidades inteiras. E as cidades não estarão suficientemente preparadas..."

Um provedor de serviços de nuvem alemão identificou o setor de energia como o principal alvo de ataques cibernéticos em 2019, atraindo 16% de todos os ataques no mundo. Mais ataques cibernéticos são previstos em cadeias de abastecimento solar e baterias. Espera-se que a integração massiva de redes elétricas a recursos de energia distribuída renovável torne essas redes mais vulneráveis a ataques. Em um contexto de hiperconectividade e interdependências inevitáveis com sistemas governamentais e municipais, uma segurança de perímetro robusta é absolutamente crítica para empresas de serviços públicos.

Tendência Nº 4: Recursos de energia distribuídos (DERs)

De mãos dadas com a migração inevitável de carbono para energias renováveis, e a eventual eliminação progressiva do uso de combustíveis fósseis, está o crescimento na adoção por consumidores de recursos de energia descentralizados (DERs) que, naturalmente, incluem energias renováveis. Segundo o New Energy Outlook da Bloomberg, "as decisões de energia dos consumidores, como energia solar no telhado e baterias atrás de medidores, ajudam a moldar uma rede elétrica cada vez mais descentralizada em todo o mundo".

Recursos de energia distribuídos (DERs) implicam em geração de energia renovável em um nível local, que contorna a infraestrutura nacional existente (ou até mesmo regional) e, portanto, depende em grande parte do grau de desregulamentação dos respectivos mercados de energia. A descentralização afeta a distribuição, bem como a geração. Ela envolve o estabelecimento de um fluxo de energia bidirecional, fornecendo a estrutura pela qual consumidores comuns com, por exemplo, painéis solares em suas casas, podem alimentar qualquer excesso de energia de volta para a rede elétrica, criando a nova função "prossumidor". Segundo a UE, isso é facilitado pela Rede Elétrica Inteligente que "permite que os consumidores produzam a sua própria energia para responder a preços e vendam o excesso para a rede."

A reunião do G7 no verão de 2021 pontuou a importância dos recursos de energia distribuídos (DERs) para solucionar desafios climáticos e de segurança. Os DERs facilitam a descarbonização possibilitando que energias renováveis sejam utilizadas – por exemplo, a substituição de combustíveis fósseis por energia solar, (as instalações de energia solar globais cresceram 138,2 GW em 2020, um aumento anual de 18%) e a substituição de gasolina por eletricidade devido aos veículos elétricos (as vendas globais de veículos elétricos cresceram 41% desde 2019 e a participação das vendas de carros elétricos atingiu um recorde de 4,6% em 2020). Ao redor do mundo, soluções de eletrificação estão proliferando com uma fonte de eletricidade renovável limpa e de rápida expansão.

A Bloomberg relata: "A Austrália e o Japão estão no caminho certo para desenvolver os dois sistemas elétricos mais descentralizados do mundo." Os EUA também estão descentralizando rapidamente. Em setembro de 2020, a Comissão Federal Reguladora de Energia Elétrica dos EUA (FERC) aprovou a Determinação 2222 abrindo as portas para um mercado atacadista de recursos de energia distribuídos (DER).

US$ 96,7 bilhões

"O mercado global de bombas de calor prevê um crescimento de US$ 60,4 bilhões em 2021 para US$ 96,7 bilhões em 2026, a uma taxa de crescimento anual composta (CAGR) de 9,9% para o período de 2021 a 2026." Pesquisa e mercados

Outra vantagem interessante dos DERs é, ao viabilizar uma série de energias eficientes, como soluções de demanda localizadas que usam energia solar e bateria, capacitar populações de países em desenvolvimento a acessar e, até mesmo, gerar (como prossumidoras), energia em nível local, contornando quaisquer deficiências da infraestrutura nacional, regional ou local. O Banco Mundial calcula que 760 milhões de pessoas no mundo não têm acesso a eletricidade em suas casas, redução de mais de um bilhão há uma década. "A eletrificação através de soluções baseadas em energias renováveis descentralizadas, em particular, ganhou força". No entanto, a distribuição pelos países também foi lamentavelmente desigual. Apenas 6,7% dos cidadãos do Sudão do Sul, 8,4% no Chade, 11,1% no Burundi, 11,2% no Malaui e 14,3% na República Centro-Africana têm acesso a eletricidade.

Os DERs, no entanto, salientam a transição das empresas de serviços públicos tradicionais que estão lutando para se adaptar do modelo do século XX, com grandes geradores centralizados, unidirecionais e conectados a redes que atendem a uma demanda estável sem praticamente oferecer flexibilidade de preços. Fluxo de energia bidirecional é um desafio que pode resultar em sobrecarga da capacidade da linha elétrica. Dispositivos de uso final representam um fardo ainda não quantificável sobre as redes. Todos os consumidores ligando bombas de calor ou carregando veículos elétricos ao mesmo tempo poderiam causar picos incontroláveis de uso de energia. A adaptação a fluxos bidirecionais está forçando os serviços públicos a investirem significativamente na atualização das redes elétricas.

Ameaça em destaque: as vulnerabilidades de redes com múltiplas estações complexas e automatizadas

A rede de energia elétrica e a infraestrutura de energia em geral não foram projetadas para fluxo bidirecional, e certamente não para um fluxo crescente entre pequenos locais de geração e distribuição. Em vez de um fluxo de energia unidirecional preciso e estritamente controlado da rede elétrica para casa (ou escritório), a descentralização gera uma teia interconectada altamente complexa de estações finais, controles avançados, sensores digitais, arquiteturas de rede e software, com suas próprias vulnerabilidades e possíveis preocupações em relação à segurança das conexões. Somando-se a isso está o fato de que essas redes complexas confiam cada vez mais em automação para funcionar – introduzindo ainda mais vulnerabilidades relacionadas ao uso de IA em hardware e software antigos.

Usinas de energia virtuais que utilizam infraestrutura de rede elétrica inteligente para conectar pequenas quantidades de ativos de energia em um único gerador possibilitam que os consumidores também sejam fornecedores (prossumidores) canalizando a energia em excesso para a rede elétrica inteligente. O modelo é atraente e o setor de energia prevê um aumento massivo de dispositivos digitais descentralizados canalizando suprimentos de energia distribuída para usinas de energia virtuais. No entanto, a dependência da infraestrutura de redes elétricas inteligentes aumenta claramente os riscos da segurança cibernética. Fontes de energia descentralizadas e disseminadas são alimentadas por endpoints vinculados à rede, o processo centralizado de usinas de energia virtuais é vulnerável a criminosos cibernéticos que podem invadir toda a rede através de um único endpoint. Por exemplo, um cibercriminoso poderia, teoricamente, parar uma quantidade significativa de baterias de armazenamento ou carregadores de carros elétricos por vingança. Não é por acaso que malware e ransomware direcionados a serviços de infraestrutura crítica estão em ascensão. O gerenciamento de riscos convencional não é mais suficiente. Os DERs claramente diminuem o controle e a supervisão que os serviços públicos anteriormente detinham sobre recursos de energia armazenados em suas redes elétricas.

Policiar essa nova rede é um desafio complicado, que piora pela imaturidade do setor descentralizado. A configuração atual fornece pouca transparência aos serviços públicos. A necessidade de padrões universais robustos e regulamentações é clara. Perguntas sobre a responsabilidade pela segurança cibernética também são grandes.

Esses riscos tornam verificações de vulnerabilidades e retentores de respostas de emergência uma necessidade absoluta para empresas de serviços públicos. Prevenção é melhor do que cura e, se o pior acontecer (talvez devido a uma vulnerabilidade em uma arquitetura separada, mas conectada), agir de forma imediata e apropriada, pode interromper o desastre em curso.

Tendência #5: Desafios regulatórios

Devido à natureza crítica dos serviços públicos, o setor está entre os mais altamente regulados do planeta, sujeito a um leque de regulamentações, em nível nacional, regional e local. Uma grande parte dessas regulamentações está relacionada ao fato de que as empresas de serviços públicos são frequentemente monopólios naturais, particularmente em países onde empresas privadas tenham vencido licitações como a única fonte de serviços públicos regionais (ou até mesmo nacional). No entanto, regulamentações de monopólio são apenas o começo da história. As operadoras de serviços públicos devem navegar por regulamentações que abrangem uma enorme série de preocupações, incluindo operações, distribuição, manutenção, interconexão, faturamento/preços, concorrência, aquisições, proteção de dados e, naturalmente, mitigação de mudanças climáticas. O não cumprimento resulta em um aumento de risco para o sistema e penalidades financeiras consideráveis.

Previsivelmente, a segurança cibernética e a resiliência no setor de serviços públicos são rigidamente controladas. Como um exemplo, a Comissão Federal Reguladora de Energia Elétrica dos EUA requer que as operadoras forneçam respostas detalhadas a perguntas sobre seus riscos de resiliência únicos, probabilidade de impacto, identificação de ameaças, planejamento de incidentes, mitigação de ameaças, análises de eventos passados, equipamentos, ativos físicos e de engenharia. Em todos os casos, os riscos cibernéticos estão listados junto com eventos naturais, como a seca, desde a Determinação de janeiro de 2018 da Comissão.

"Como as empresas de energia adaptam seus modelos de negócios para se encaixarem no atual ambiente de mercado em rápida evolução, suas funções jurídicas e de conformidade também devem se adequar. A disponibilização digital de processos de monitoramento de conformidade e regulamentações de energia pode ajudar a resolver essas questões e problemas por meio de uma solução unificada."
Deloitte

Em 2021, governos ao redor do mundo buscaram urgentemente medidas para reforçar a resiliência cibernética em empresas de serviços públicos cruciais. O ataque de 6 de maio de 2021 ao Colonial Pipeline, supostamente por um grupo de criminosos cibernéticos localizado na Rússia, interrompeu 8.851 km do gasoduto que transportava 45% do abastecimento de combustível na costa leste dos EUA. Um estado de emergência foi declarado em quatro estados americanos. Para as agências reguladoras, isso foi um alerta. Houve alguma falha de conformidade? Esse ataque podia ter sido evitado? O Departamento de Segurança Interna dos Estados Unidos estabeleceu rapidamente requisitos de segurança cibernética mais rígidos "para melhor identificar, proteger e responder a ameaças a empresas críticas no setor de gasodutos".

"Os CEOs relatam pressão regulatória em questões ambientais, sociais e de governança na pesquisa." KPMG

Atualmente, a UE está elaborando um projeto de lei (substituindo a lei de 2018) para intensificar os requisitos de segurança cibernética para fornecedores de eletricidade e energia. Adotando uma abordagem diferente, a Comissão Federal Reguladora de Energia Elétrica dos EUA (FERC) está propondo uma mudança na lei para oferecer subsídios federais (recuperação de custos diferidos) a empresas elétricas que implementem medidas de segurança cibernética acima dos padrões das regulamentações atuais.

Além disso, regulamentações introduzidas recentemente e não vinculadas à segurança cibernética causam, mesmo assim, um grande impacto nas demandas de segurança cibernética. Um exemplo disso é a Determinação 2222 da Comissão Federal Reguladora de Energia Elétrica dos EUA (FERC) que possivelmente transformará o setor de energia ao liberalizar o mercado para fornecedores de recursos de energia distribuídos (DER) atacadistas.

Em suma, a vulnerabilidade cibernética de ativos de energia digitais integrados digitalmente ainda precisa ser completamente testada. **Uma pesquisa da KPMG descobriu que 48% dos CEOs de serviços públicos acreditam que se tornar vítima de um ataque cibernético é uma questão de "quando" e não "se".**

Ameaça em destaque: falha em cumprir regulamentações leva a consequências fatais

O não cumprimento de regulamentações pode causar dois resultados fatais. Primeiro, onde as regulamentações fornecem uma estrutura de padrões de segurança cibernética, o não cumprimento pode levar a uma violação devastadora. Segundo, no lado da governança, o não cumprimento pode causar perda de licença. Ambos os resultados podem deixar a operadora de serviços públicos de joelhos.

A lista de ataques cibernéticos a serviços públicos pelo mundo em 2021 mostra a escala do problema. Para destacar apenas dois: em agosto de 2021, uma violação na T-Mobile possibilitou acesso não autorizado a informações pessoais de mais de 50 milhões de pessoas. Em maio de 2021, a Volue, empresa de tecnologia de energia da Noruega, foi atingida por um ataque de ransomware que a forçou a desligar importantes instalações de água e tratamento de água. A consequência de violações como as acima é que as agências reguladoras serão obrigadas a continuar endurecendo suas regras.

As multas também estão ficando mais pesadas. Em 2019, a Duke Energy recebeu uma multa recorde de US$ 10 milhões das autoridades federais após a exposição de falhas de segurança cibernética extensas que, supostamente, "representaram um grave risco" à segurança e confiabilidade da rede elétrica. A recém-assinada Lei de Segurança de Dados da China (setembro de 2021) contém provisões detalhadas que regulam a coleta, o uso e a proteção de dados, bem como medidas rigorosas em caso de não cumprimento de provisões, incluindo possível suspensão da empresa.

O não cumprimento não é o único desafio relacionado a regulamentações. A vertiginosa matriz de regulamentações que afetam as operadoras de serviços públicos ao redor do mundo, no contexto de consequências drásticas por não conformidade, é exaustiva, particularmente para empresas que operam em vários mercados. Isso se torna ainda mais complicado com o constante surgimento de novas tecnologias e incertezas sobre as regulamentações que aparecerão para regê-las.

Para empresas de serviços públicos, preparar-se para regulamentações também significa adotar segurança cibernética apropriada para o setor.

Resumo

As cinco tendências descritas acima realçam grandes oportunidades e desafios que esperam as empresas de serviços públicos. Não é apenas imprescindível abraçar novas tecnologias, elas também devem ser protegidas. Criar uma cultura de imunidade cibernética possibilitará que as empresas de serviços públicos realmente colham os benefícios dos altos níveis de conectividade e automação, minimizem quaisquer impactos negativos e maximizem o retorno sobre o investimento. No ambiente volátil e de rápida evolução de hoje, a Kaspersky projetou e ajustou perfeitamente soluções e serviços – com base na inteligência de segurança líder mundial – para proteger, ininterruptamente, os dados e a continuidade dos negócios contra ameaças avançadas e ataques direcionados – mitigando riscos, detectando ataques precocemente, neutralizando ataques em tempo real e fortalecendo a proteção futura.

A Kaspersky oferece uma **abordagem de cibersegurança por estágios** projetada para esclarecer qual nível de segurança, bem como quais soluções específicas são mais adequadas à sua organização. Os estágios fornecem um conjunto facilmente gerenciável de medidas de proteção que se coordenam perfeitamente umas com as outras para atender às necessidades de cada organização individual e oferecem um roteiro de segurança cibernética que garante uma transição suave de um nível de maturidade em segurança de TI para outro quando chegar a hora.

Abordagem por estágios de cibersegurança da Kaspersky

1

Kaspersky Security Foundations – núcleo essencial de proteção automatizada cloud-based para todos os dispositivos, VDI e infraestruturas de servidor híbrido, antes que as organizações avancem continuamente para...

2

Kaspersky Optimum Security - para organizações que exigem mais segurança especializada contra ameaças novas e evasivas, antes de implementar sem esforço...

3

Kaspersky Expert Security – para organizações com equipes de segurança de TI maduras e estabelecidas, combatendo os ataques direcionados mais complexos.

Cibersegurança nível de maturidade	Solução
TI Organizações menores sem um especialista de segurança de TI	**O quê?** Kaspersky Security Foundations **Como?** Implemente segurança fundamental para organizações de qualquer tamanho e complexidade de infraestrutura, oferecendo prevenção automática cloud-managed de ameaças virtuais comuns em qualquer dispositivo, VDI e infraestruturas de servidor híbrido. ▸ **Endpoints:** Proteja todos os endpoints em sua organização com o Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security ▸ **Cloud:** Beneficie-se da segurança sem fronteiras com o Kaspersky Hybrid Cloud Security ▸ **Network:** Proteja seu perímetro com o Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway ▸ **Dados:** proteja dados valiosos e confidenciais com o Kaspersky Security for Storage ▸ **Gerenciamento de segurança:** experimente a excelência com o Kaspersky Premium Support; Kaspersky Professional Services
Segurança de TI Organizações que precisam de defesas avançadas, mas com recursos especializados em segurança de TI limitados	**O quê?** Kaspersky Optimum Security **Como?** Combate ameaças evasivas com detecção e resposta de endpoint eficazes e monitoramento de segurança contínuo – mas sem custos ou complexidade proibitivos ▸ **Detecção avançada:** análise de comportamento Boost ML, sandboxing, inteligência de ameaças e busca automática de ameaças* com o Kaspersky Sandbox, Kaspersky Threat Intelligence Portal e Kaspersky Managed Detection and Response Optimum ▸ **Análise e investigação:** aumente a visibilidade da ameaça e simplifique o processo de investigação com a Kaspersky Endpoint Detection and Response Optimum ▸ **Respostas rápidas:** implemente opções de resposta automatizadas no produto, bem como cenários de resposta guiada e gerenciada* com o Kaspersky Endpoint Detection and Response Optimum e Kaspersky Managed Detection and Response Optimum ▸ **Conscientização de segurança:** equipe os funcionários com ferramentas automatizadas em todos os níveis e desenvolva as principais habilidades de cibersegurança com o Kaspersky Security Awareness Training *Suportado por experts da Kaspersky

Equipe de segurança de TI experiente e totalmente formada e/ou SOC dedicado

- Têm um ambiente de TI complexo e distribuído
- São um alvo altamente provável para ataques complexos e do tipo APT
- Têm um apetite de baixo risco devido aos altos custos de incidentes de segurança e violações de dados
- Estão preocupados com a conformidade regulatória

O quê?
Kaspersky Expert Security

Como?
Domínio completo sobre os ataques virtuais mais complexos e direcionados

- **Equipados:** equipe seus especialistas internos para resolver incidentes complexos de cibersegurança. Beneficie-se de uma solução unificada de cibersegurança. A Kaspersky Anti Targeted Attack Platform com o Kaspersky EDR em seu núcleo capacita a sua equipe com recursos de XDR.
- **Informado:** enriqueça seu conjunto de conhecimentos com a inteligência de ameaças e qualifique seus especialistas para lidarem com incidentes complexos:
  - Integre a inteligência de ameaças imediata prática ao seu programa de segurança. O Kaspersky Threat Intelligence oferece acesso instantâneo a inteligência de ameaças técnica, tática, operacional e estratégica.
  - Desenvolva as habilidades práticas da sua equipe interna, incluindo trabalho com evidências digitais, análise e detecção de software mal-intencionado e adoção de melhores práticas para resposta a incidentes, com o Kaspersky Cybersecurity Training.
- **Reforçado:** chame especialistas externos para avaliação, suporte imediato e backup:
  - Aproveite o suporte imediato da equipe da Kaspersky Incident Response, com analistas e investigadores altamente experientes para resolver completamente seu incidente cibernético com rapidez e eficácia.
  - Obtenha uma segunda opinião e a experiência em busca gerenciada de ameaças de um parceiro confiável com o Kaspersky Managed Detection and Response, de modo que seus especialistas internos em segurança de TI tenham mais tempo para reagir a resultados críticos que exijam atenção.
  - Entenda o quão eficazes suas defesas seriam realmente contra ameaças virtuais em potencial e se você já é o alvo involuntário de um ataque furtivo de longo prazo, por meio do Kaspersky Security Assessment.

Soluções direcionadas

O quê?	Como?
 **Kaspersky Fraud Prevention**	A Automação Avançada permite autenticação contínua e sem atrito, reduzindo os custos de processos de segundo fator para usuários legítimos, enquanto mantém altas taxas de detecção de fraude em tempo real. A Análise de Fraudes Automatizada analisa exaustivamente os eventos que ocorrem durante toda a sessão, transformando-os em dados valiosos. Protege o perímetro externo de qualquer organização, garantindo segurança e proteção aos cidadãos/clientes.
 **Kaspersky Industrial Cybersecurity**	O KICS oferece uma abordagem holística à cibersegurança industrial, agregando valor a qualquer estágio do processo de segurança de OT do cliente – desde avaliações e treinamento em segurança cibernética a resposta a incidentes e tecnologias avançadas. Um ecossistema de produtos e serviços integrados permite proteger camadas de tecnologia operacional e elementos de sua organização – incluindo servidores SCADA, HMIs, estações de trabalho de engenharia, PLCs, conexões de rede e, até mesmo, engenheiros – sem afetar a continuidade operacional e a consistência do processo industrial.
 **Avaliação da segurança do Kaspersky ICS**	Para organizações preocupadas com o possível impacto operacional da segurança de TI/TO, a Kaspersky fornece uma avaliação de segurança cibernética com pré-instalação minimamente invasiva. Como uma primeira etapa crucial em estabelecer requisitos de segurança no contexto de necessidades operacionais, ela também pode fornecer insights significativos sobre níveis de segurança cibernética sem qualquer implantação de tecnologias de proteção.

Notícias sobre ameaças virtuais: www.securelist.lat

Notícias sobre segurança de TI: www.kaspersky.com.br/blog

Portal de inteligência de ameaças: opentip.kaspersky.com

Tecnologias em resumo: www.kaspersky.com/TechnoWiki

Prêmios e reconhecimentos: media.kaspersky.com/en/awards

Ferramenta de portfolio interativa: kaspersky.com/int_portfolio/br

kaspersky PREPARADOS PARA O FUTURO