Risco, resiliência e segurança para governos e cidades

Melhores práticas e tecnologias para manter a continuidade dos negócios

Alcatel·Lucent Enterprise

Índice

Segurança e resiliência são prioridades urgentes

Hoje, governos e cidades do mundo inteiro enfrentam uma policrise, ou seja, uma convergência de riscos cibernéticos e físicos que ameaçam cidadãos, serviços críticos e dados confidenciais.

Agora os cidadãos esperam e contam com serviços fornecidos por meio de sites seguros, e os funcionários esperam trabalhar em casa ou no escritório, com base em suas necessidades e preferências. Esses novos requisitos, juntamente com a disseminação exponencial de dispositivos da Internet das Coisas (IoT), ampliam os limites da rede em um momento em que as tensões geopolíticas e a polarização política aumentam o risco de ataques cibernéticos.

Além disso, a dark web criou um mercado lucrativo para vender anonimamente dados confidenciais do governo, tornando os sistemas governamentais alvos muito atraentes para roubo de informações. Ela também fornece um refúgio on-line para coordenar ataques a governos.

O vandalismo, o terrorismo, os tumultos e o crime também estão aumentando, criando ameaças cada vez maiores à infraestrutura cívica, de defesa e à continuidade dos negócios. Adicione a isso eventos climáticos severos e desastres naturais que tornam muito difícil, se não impossível, a prestação de serviços governamentais e a segurança dos cidadãos quando eles mais precisam. Além disso, com a inflação global pressionando os orçamentos, a necessidade de iniciativas de digitalização que aumentem a agilidade operacional, eficiência e produtividade nunca foi tão grande.

Juntamente com esses riscos, está se tornando cada vez mais difícil para governos e cidades permanecerem totalmente em conformidade com regulamentações de soberania de dados e privacidade cada vez mais rigorosas. Como resultado, existe um grande potencial para multas e ações judiciais por infrações.

Diante dessa nova realidade, governos e cidades não podem mais contar com suas estratégias anteriores de segurança e resiliência. Para mitigar esses riscos, eles devem tomar medidas ousadas e proativas para melhorar sua postura geral de segurança. É necessária uma abordagem inovadora, mais alinhada com as ameaças mais significativas do momento. Com uma segurança aprimorada, governos e cidades estarão melhor posicionados para proteger cidadãos e operações, e fortalecer sua resiliência, garantindo a continuidade dos negócios em quaisquer circunstâncias.

Os riscos são reais

Os riscos são reais e, infelizmente, é muito fácil para governos e cidades adiarem medidas de mitigação de riscos, especialmente quando incidentes notáveis estão ocorrendo apenas em locais distantes. Mas a realidade é que toda organização governamental é um alvo potencial para ataques.

Uma verificação da realidade

- Ataques cibernéticos contra governos aumentaram 95% no último semestre de 2022.[1]
- O ataque ao governo da Costa Rica foi considerado um dos mais caros do ano,[2] com o ransomware sendo o método preferido de ataques a serviços públicos.[3]
- Até 2025, estima-se que 30% das organizações de infraestrutura crítica sofrerão uma violação de segurança.[4]

À medida que as populações das cidades continuam a crescer,[5] aumentam os riscos para governos e cidadãos. A Organização das Nações Unidas (ONU) aconselha os governos a trabalharem para tornar as cidades e assentamentos humanos mais inclusivos, seguros, resilientes e sustentáveis, conforme publicado no Objetivo 11.[6]

---

[1] Ciberataques contra governos aumentaram 95% no último semestre de 2022, diz CloudSek. CSO Estados Unidos, Janeiro de 2023.

[2] Os 13 ataques cibernéticos mais caros de 2022: Retrospectiva. Inteligência de Segurança, Dezembro de 2022.

[3] Documento de política: Estratégia Cibernética Nacional 2022. Gabinete do Reino Unido, Dezembro de 2022.

[4] Gartner prevê que 30% das organizações de infraestrutura crítica sofrerão uma violação de segurança até 2025. Gartner, Dezembro de 2021.

[5] Desenvolvimento Urbano. Banco Mundial, Abril de 2023.

[6] Objetivo11: Tornar as cidades e os assentamentos humanos inclusivos, seguros, resilientes e sustentáveis. Nações Unidas.

Com todos esses fatores em mente, fica claro que governos e cidades devem colocar foco renovado em risco, resiliência e segurança para:

- **Garantir a continuidade de serviços críticos e proteger dados confidenciais**, especialmente em tempos de crise inesperada
- **Minimizar os custos de seguros contra riscos** implementando a proteção certa para cada tipo de risco cibernético e físico que enfrentam
- **Reduzir as perdas financeiras** devido a ataques cibernéticos e físicos, ações judiciais de cidadãos e multas por violação de dados e não conformidade
- **Manter sua reputação e a confiança dos cidadãos**, que podem ser danificadas ou perdidas completamente devido a atrasos e interrupções do serviço
- **Proteger os cidadãos** fornecendo informações importantes relacionadas à saúde, segurança e proteção

A digitalização traz benefícios e riscos

No mundo digital de hoje, pessoas, objetos e processos estão conectados. Essas conexões permitem aos governos e cidades:

- Aproveitar a tecnologia IoT e as informações que ela fornece
- Automatizar os fluxos de trabalho para aumentar a eficiência e acelerar as respostas aos cidadãos
- Usar dados precisos e em tempo real para aumentar a visibilidade e tomar decisões bem embasadas
- Implementar aplicativos de construção inteligentes, que permitem operações mais sustentáveis, econômicas e resilientes

Embora essas melhorias sejam essenciais para que governos e cidades alcancem seus objetivos, as tecnologias habilitadoras também introduzem um novo conjunto de riscos cibernéticos e físicos que devem ser abordados.

Novas formas de pensar sobre vulnerabilidades

Com a digitalização, as vulnerabilidades se tornam mais visíveis, e as ameaças podem se espalhar rapidamente por sistemas, dispositivos e aplicativos interconectados:

- Uma falha em um sistema pode afetar a todos
- Os hackers podem explorar conexões entre infraestruturas para ampliar seu alcance
- Os vírus podem aproveitar as conexões para se propagar por toda a organização

A digitalização também estreita a conexão entre riscos cibernéticos e físicos. Por exemplo, agentes mal-intencionados podem hackear remotamente centros de dados governamentais ou obter acesso físico comprometendo uma fechadura eletrônica. Da mesma forma, câmeras de segurança podem ser desativadas, desconectadas ou conectadas a feeds de vídeo pré-gravados através de ataques cibernéticos ou físicos, tornando-as inúteis para fins de proteção em qualquer caso.

A convergência entre TI e tecnologias operacionais (TO) cria novas oportunidades para ataques. Agora, os hackers podem comprometer um sensor IoT para obter acesso à rede e aos sistemas de alto valor e recursos de informação conectados a ela. Por outro lado, eles podem invadir a rede diretamente, usando-a como um gateway para atacar sistemas críticos dos edifícios, como elevadores, detectores de fumaça, alarmes de incêndio e sistemas de sprinklers.

Novas tecnologias também podem ser usadas a favor e contra organizações governamentais. Tomemos a inteligência artificial (IA) como exemplo. A IA ajuda a prevenir, proteger e acelerar as respostas a ameaças cibernéticas e físicas, mas também permite que agentes mal-intencionados quebrem senhas de sistemas governamentais. No futuro, podemos esperar uma situação semelhante com a computação quântica, que ajudará os governos a resolver problemas complexos, mas também facilitará a descriptografia de informações confidenciais.

Considerações e desafios exclusivos

Os riscos específicos introduzidos com a digitalização dependem das tecnologias que estão sendo implantadas. As redes modernas e as tecnologias de comunicação trazem três riscos principais:

- **Avarias**: Falhas de hardware e software podem ocorrer a qualquer momento, sem aviso prévio. Incêndios, inundações, condições meteorológicas extremas e outros fatores imprevistos também podem causar avarias, enquanto as falhas de energia podem afetar a qualidade e a estabilidade do fornecimento de energia, levando a avarias e falhas.
- **Ataques cibernéticos**: Dados confidenciais podem ser perdidos ou roubados, e redes e sistemas podem ser corrompidos, retardando ou interrompendo completamente os serviços e operações do governo. Os ataques de ransomware podem manter redes e sistemas inteiros como reféns, tornando dados e funcionalidades críticas inacessíveis.
- **Obsolescência**: Fornecedores de tecnologia podem encerrar o suporte para hardware e software, enquanto a escassez na cadeia de suprimentos pode tornar logisticamente ou economicamente impossível continuar usando as soluções. As mudanças nos requisitos de conformidade regulatória também podem tornar as soluções de tecnologia obsoletas.

Cada um desses riscos pode levar aos outros. Uma falha ou tecnologia obsoleta pode abrir a porta para ataques cibernéticos. E os ataques cibernéticos podem causar uma falha ou destacar que a tecnologia agora está obsoleta.

Juntos, esses riscos significam que governos e cidades devem melhorar sua capacidade de prevenir, proteger e reagir a ameaças. Não fazer nada não é mais uma opção. Continuar a depender de redes e tecnologias de comunicação desatualizadas e isoladas, à medida que os riscos continuam a se multiplicar, não é uma abordagem viável sob nenhuma perspectiva.

Uma abordagem holística e um processo padronizado

Cada governo e cada cidade deve desenvolver uma abordagem estratégica e tática para segurança e resiliência que seja adaptada para seu perfil de risco exclusivo, localização geográfica, mandato, orçamento e outros requisitos. Entretanto, embora os resultados de seus esforços sejam diferentes, vale a pena adotar uma abordagem padronizada e compartilhar as melhores práticas para obter melhores resultados.

Uma abordagem holística para a mitigação de riscos permite que governos e cidades aumentem a segurança e a resiliência em três áreas principais de seu mandato, que incluem:

- **Cidadãos:** Para garantir a segurança humana e proteger os dados contra todas as ameaças
- **Operações:** Para manter funções, transações e serviços seguros e confiáveis em todas as circunstâncias
- **Edifícios:** Para tornar os locais de trabalho e espaços governamentais mais inteligentes e mais seguros

Quatro etapas para aumentar a segurança e a resiliência

Com as áreas acima em mente, as etapas a seguir podem ajudar governos e cidades a determinar seu perfil de risco e escolher a rede e as soluções de comunicação corretas para sua situação específica.

1. **Avaliar**: identifique riscos cibernéticos e físicos, áreas de exposição e potenciais consequências, assim como as diferentes opções para prevenir, proteger e reagir a ataques em cada caso. Comece com uma auditoria e avalie os riscos e o potencial de perda para cada vulnerabilidade identificada. Isso ajuda a identificar as ações e soluções adequadas em cada caso.

   Embora a avaliação seja o primeiro passo, não é uma atividade única. Para combater o cenário de ameaças em rápida mudança, é importante reavaliar regularmente os riscos e monitorar continuamente os recursos cibernéticos e físicos em busca de novas vulnerabilidades.

2. **Prevenir**: escolha soluções que ajudem a evitar ou conter riscos cibernéticos e físicos, como:
   - De uma perspectiva cibernética, procure soluções com recursos de segurança integrados que não precisem ser adquiridos separadamente ou renovados. As soluções devem levar em consideração a segurança durante cada etapa da definição, desenvolvimento e entrega do produto e contribuir para uma arquitetura e ambiente de tecnologia de confiança zero. Eles também devem oferecer suporte a backup e recuperação automatizados e fornecer informações para fins de auditoria.
   - Do ponto de vista físico, identifique soluções que aumentam a visibilidade e dificultam o acesso aos ativos. Soluções para vigilância por vídeo, controle de acesso, rastreamento de ativos, detecção de intrusão e alarmes, serviços baseados em localização e reconhecimento facial são bons exemplos.
3. **Proteger**: escolha soluções que ajudem a proteger contra riscos cibernéticos e físicos, por exemplo:
   - No lado cibernético, assegure-se de que as soluções sejam certificadas para atender aos padrões de segurança, incluam capacidades de criptografia nativa e mecanismos avançados de autenticação, e limitem a propagação de ataques cibernéticos e vírus.
   - Para aumentar a proteção física, vá além da vigilância por vídeo e considere o papel das comunicações, alertas e notificações, bem como soluções para proteger os trabalhadores em locais isolados.
4. **Reagir**: escolha soluções que permitam uma recuperação eficiente em caso de violação de segurança, por exemplo:
   - As soluções cibernéticas devem ser apoiadas por uma Equipe de Resposta a Incidentes de Segurança, fornecer um registro de auditoria e procedimentos de recuperação, e oferecer suporte à restauração de dados.
   - As soluções físicas devem suportar operações de comando e controle (C2) e comunicações de missão crítica.

Risco, resiliência e segurança para o setor público, governos e cidades

	1 Avaliar	2 Evitar	3 Proteger	4 Reagir
Segurança	✓	✓	✓	
Resiliência	✓	✓		✓
Cyber	• Identificação dos riscos • Avaliação • Mapeamento de ativos • Monitoramento contínuo	• Segurança desde o projeto • Avaliação/auditoria de riscos • Consultoria de pré-venda • Treinamento de usuário • Detecção de fraude • Procedimento de backup • Configuração da trilha de auditoria • Robustez para ambientes adversos. • Redundância	• Certificação de segurança • Criptografia • Autenticação	• PSIRT/CERT • Trilha de auditoria • Gerenciamento de incidentes • Procedimentos de recuperação • Restauração
Físico	• Identificação de riscos • Avaliação • Valorização • Monitoramento contínuo	• Vídeo vigilância • Controle de acesso • Rastreamento de Ativos (Asset Tracking) • Detecção e alarmes • Serviços baseados na localização • Reconhecimento facial	• Vídeo vigilância • Comunicações • Alerta e notificação • Proteção dos trabalhadores isolados	• Controle e comando • Comunicações de missão crítica

Resiliência e mecanismos de resposta ágeis são a chave para prosperar diante dos riscos

" A resiliência é mais do que apenas a capacidade de se recuperar de forma rápida. Nos negócios, resiliência significa lidar com adversidades e choques e adaptar-se continuamente para o crescimento. As organizações verdadeiramente resilientes não apenas se recuperam melhor... na verdade, elas prosperam em ambientes hostis. A agilidade permite que as organizações respondam de maneiras exclusivamente adequadas a cada crise, em vez de aplicar soluções genéricas e inflexíveis."

— McKinsey & Company

Fortalecer a segurança e a resiliência

Governos e cidades que seguem a abordagem holística e o processo recomendado na seção anterior têm novas oportunidades para aproveitar soluções de rede e comunicações para aumentar a segurança e a resiliência em relação a cidadãos, operações, edifícios e espaços.

Proteção dos cidadãos

Com soluções modernas de vigilância por vídeo, autoridades governamentais e de segurança pública têm visibilidade em tempo real de eventos e emergências à medida que acontecem, aumentando significativamente a consciência situacional. Em seguida, elas podem usar uma plataforma de gerenciamento de fluxo de trabalho e orquestração de segurança pública para compartilhar esse conhecimento e coordenar as respostas. Equipes em departamentos governamentais, agências e localidades podem facilmente compartilhar informações e percepções contextuais oportunas usando a combinação ideal de comunicações de voz, vídeo e texto para permitir uma tomada de decisão mais eficiente, efetiva e colaborativa.

Sistemas de notificação em massa podem alertar rapidamente as pessoas e os processos sobre emergências, permitindo que tomem as medidas apropriadas mais rapidamente. As chamadas dos funcionários em campo têm prioridade nas rotas para os centros de atendimento governamentais, e as capacidades de preservação das chamadas mantêm os funcionários e os cidadãos conectados ao pessoal do centro de atendimento em todas as circunstâncias. Soluções de comunicação para trabalhadores isolados, situações de man-down e rastreamento de contatos aceleram ainda mais as respostas e aumentam a conscientização sobre situações potencialmente perigosas.

Para ajudar a prevenir emergências e acelerar as respostas, soluções de IA conectadas a múltiplas fontes de dados podem ser usadas para identificar riscos e eventos problemáticos potenciais, bem como para automatizar fluxos de trabalho.

Aumento da confiabilidade nas operações

Uma rede empresarial segura e resiliente suporta comunicações de missão-crítica, bem como tecnologias de segurança física e cibernética essenciais para operações confiáveis.

As soluções de rede ideais incluem recursos que são fundamentais para proteger o acesso à rede e às informações que ela contém, incluindo:

- **Software e código-fonte robusto dos switches de rede**: o código-fonte é deliberadamente variado para dificultar que possíveis invasores explorem as vulnerabilidades. Além disso, o código e o software são verificados e validados independentemente para garantir sua integridade e segurança.
- **Macro e microssegmentação**: No contexto de confiança zero, a segmentação recebe atenção especial em ambos os níveis, macro e micro. A macrossegmentação divide a rede em zonas distintas com base em fatores como função, aplicação ou grupo de usuários, isolando ativos e recursos críticos do restante da rede. A microssegmentação adota uma abordagem mais detalhada, segmentando a rede no nível do usuário ou dispositivo para possibilitar um controle mais preciso sobre o acesso à rede e a aplicação de políticas de segurança.
- **Operações autônomas**: Automatizar o posicionamento de ativos e recursos em macrossegmentos e aplicar políticas no nível do usuário e do dispositivo ajuda a reduzir o risco de erros humanos, uma causa comum de violações de segurança cibernética.

- **Equipamento robusto**: Os equipamentos de rede podem resistir a condições adversas, como temperaturas extremas e vibrações severas. O equipamento suporta redundância de energia a partir de duas fontes para garantir operações contínuas durante quedas de energia. O tempo médio entre falhas (MTBF) pode garantir confiabilidade, minimizando paralisações inesperadas e interrupções causadas por quebras e falhas.

Governos e cidades também obtêm flexibilidade para implantar soluções de rede e comunicações em suas instalações, bem como em ambientes de nuvem pública e privada. Essas opções de implantação permitem estratégias de redundância geográfica e espacial que são fundamentais para manter a continuidade dos negócios durante falhas e emergências, mesmo em locais remotos.

Aumento da segurança em edifícios e espaços

Uma rede multisserviços segura é necessária para suportar as aplicações e processos necessários para proteger contra riscos e manter a disponibilidade do serviço o tempo todo. Além disso, para suportar o crescente número de dispositivos sem fio conectados à rede Wi-Fi, governos e cidades precisarão de uma rede sem fio robusta e confiável, que opere sem problemas, sem congestionamento que possa reduzir sua eficiência.

As mesmas soluções avançadas de vigilância por vídeo que ajudam a proteger os cidadãos também ajudam a manter os prédios e espaços governamentais seguros. Essas soluções são complementadas com rastreamento de ativos, que torna mais rápido e fácil encontrar pessoas e ativos críticos durante eventos e emergências inesperadas.

Agora, governos e cidades também possuem as capacidades de automação necessárias para implementar e gerenciar eficientemente soluções IoT para aplicações de segurança, como controle de acesso e rastreamento de ativos. Eles podem incorporar um grande número de novos dispositivos IoT automaticamente e com segurança, com impressão digital, classificação e contenção de dispositivos, sem o risco de que o pessoal de TI introduza inadvertidamente alguma vulnerabilidade.

Um parceiro para apoiar suas estratégias

À medida que os riscos para governos e cidades continuam a crescer, a necessidade de um parceiro tecnológico especializado também aumenta.

A Alcatel-Lucent Enterprise, uma inovadora tecnológica há mais de 100 anos, desenvolveu um quadro de Risco, Resiliência e Segurança (RRS) que se alinha com os requisitos de governos e cidades. A estrutura de RRS inclui os processos, melhores práticas e soluções necessárias para governos e cidades preverem, monitorarem e evitarem a exposição a riscos físicos e cibernéticos.

A equipe da ALE, composta por especialistas altamente conhecedores do setor governamental, trabalha em parceria com líderes governamentais e municipais para ajudá-los a:

- Identificar seu conjunto único de riscos e escolher soluções para abordar esses riscos.
- Preencher as lacunas entre segurança cibernética, segurança física e resiliência.
- Justificar a aprovação do orçamento.

Soluções flexíveis e totalmente compatíveis

A ALE incorpora segurança em suas soluções de rede e comunicações desde os estágios iniciais do projeto. Para garantir a máxima segurança e resiliência, as soluções:

- São construídas com medidas de segurança confiáveis por governos e organizações de defesa em todo o mundo
- São testadas usando técnicas especializadas específicas de segurança, como testes de penetração
- Estão em conformidade com padrões de segurança e privacidade de dados globais, regionais ou específicos da indústria, incluindo padrões importantes do setor de segurança, como o Common Criteria EAL2+

- Podem ser implantadas em qualquer combinação de modelos locais e em nuvem para atender aos requisitos mais complexos
- Suportam padrões abertos para reduzir complexidades de integração e incompatibilidades entre soluções e fornecedores

Além dos modelos tradicionais de compra, a ALE oferece planos de assinatura para que os clientes possam acessar as tecnologias mais recentes e os avanços em segurança, ao mesmo tempo em que atendem a restrições orçamentárias. Um conjunto completo de serviços para apoiar governos e cidades em cada estágio de sua jornada também está disponível.

Experiência + Especialização

Os especialistas e as soluções da ALE têm a confiança de organizações governamentais e municipais no mundo inteiro. Veja a seguir apenas alguns exemplos:

- A Metz Eurometropolis na França, onde a ALE ajudou a área metropolitana a garantir a continuidade de serviços críticos e comunicações, a disponibilizar rapidamente serviços de emergência e conectar de forma segura usuários e objetos conectados em edifícios.
- O governo escocês, onde as soluções da ALE fornecem uma infraestrutura consistente, segura e confiável, além do controle de acesso à rede e segurança aprimorada de dados, para mais de 40 agências governamentais.
- O Departamento de Defesa dos EUA, onde soluções robustas e modernas oferecem suporte confiável a comunicações e aplicativos de missão crítica, atendendo a todos os requisitos ambientais e de choque, assim como à Lei de Acordos Comerciais (TAA) e aos requisitos de certificação de defesa.
- Escolas públicas do Condado de Gwinnett nos Estados Unidos, onde as soluções da ALE oferecem suporte à segurança física, monitoramento de vídeo, E-911, computação segura e muito mais, em um grande distrito escolar onde a segurança é primordial.

Saiba mais

Para saber como a Alcatel-Lucent Enterprise pode ajudar sua organização a mitigar os riscos para aumentar a segurança e a resiliência, visite nosso site ou entre em contato conosco hoje.

Alcatel·Lucent Enterprise