Tornar a resiliência e a segurança uma prioridade

Soluções Alcatel-Lucent Enterprise para o setor público

Alcatel·Lucent Enterprise

e-Book

Índice

| Visão geral

| Por que a colaboração TI/TO é fundamental

| Soluções de rede resilientes e seguras

| Soluções de comunicação resilientes e seguras

| Proteja seu pessoal e ativos

| Soberania e segurança dos dados

Visão geral

Com os crescentes desafios globais e o aumento dos riscos cibernéticos e físicos, os governos devem priorizar o gerenciamento de riscos, salvaguardar a infraestrutura essencial e proteger os cidadãos. De acordo com a CloudSek, os ataques cibernéticos contra o governo aumentaram 95% em 2022.[1] A expectativa é que os negócios do governo continuem independentemente da situação, e que os cidadãos sejam mantidos em segurança. No cenário global atual, é mais importante do que nunca manter a segurança, proteger a soberania dos dados e garantir a disponibilidade do serviço.

Setor Público: por que a TIC é mais importante do que nunca

Nos últimos anos, a transformação digital no setor público avançou rapidamente, com um número cada vez maior de cidadãos acessando serviços digitais. A transformação digital também permitiu que os funcionários do governo adotassem um estilo de trabalho em qualquer lugar. Há uma pressão crescente sobre os governos para que acelerem ainda mais a transformação digital. De acordo com um artigo da Deloitte, 77% das agências governamentais afirmam que as iniciativas de transformação digital promovidas durante a pandemia já estão tendo um impacto positivo em suas organizações.[2]

A Alcatel-Lucent Enterprise trabalha com governos em todo o mundo e reconhece a importância de proteger cidadãos, operações e edifícios contra riscos cibernéticos e físicos. Nossas soluções consideram a segurança e a privacidade dos dados em todas as etapas do processo de design e são desenvolvidas com opções resilientes para atender a todos os tipos de organização. Este e-Book fornece insights sobre resiliência e segurança para suas soluções de rede, nuvem e comunicações ALE.

1 Os ciberataques contra governos aumentaram 95% no último semestre de 2022, diz o CloudSek. CSO Estados Unidos, Janeiro de 2023.
2 https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html.

Por que a colaboração TI/TO é fundamental

Antes de explorarmos como você pode melhorar a resiliência e a segurança com as soluções Alcatel-Lucent Enterprise, é importante reconhecer a mudança na relação entre Tecnologia da Informação e Tecnologia Operacional. No passado, as equipes de TI e de operações não colaboravam estreitamente, cada uma tinha suas próprias funções e responsabilidades. Esses dois mundos agora estão convergindo e precisam trabalhar como um só. Equipes de TI e de Operações que não estão cientes das atividades uma da outra, ou que não se coordenam e colaboram, colocam toda a organização em risco.

Vamos considerar, por exemplo, o grande número de dispositivos da Internet das Coisas (IoT) que estão sendo rapidamente implantados em muitas agências governamentais e cidades inteligentes. Quando a equipe de TI não está ciente de que a equipe de operações está implementando novos dispositivos IoT, ela não pode garantir que esses dispositivos estejam em conformidade com as políticas de segurança da organização. Os dispositivos de IoT vêm com níveis altamente variáveis de recursos de segurança cibernética e podem não estar equipados com os mecanismos de proteção mais recentes, ou seus recursos podem não ter sido totalmente implementados. Esses dispositivos de “shadow IT” (TI invisível) não autorizados podem executar qualquer software e estar infectados com vírus e malware. Se não forem verificados, podem facilmente introduzir novas vulnerabilidades e vetores de ataque na rede. Estamos vendo agora o surgimento da colaboração TI/TO necessária para garantir a segurança e a resiliência da rede.

Soluções de rede resilientes e seguras

A infraestrutura de rede é essencial para o funcionamento das organizações governamentais, bem como para o fornecimento de serviços aos cidadãos. Devido à natureza sensível das informações contidas nas redes governamentais e aos serviços essenciais que os governos executam, o tempo de inatividade ou as interrupções nos serviços de rede podem ter consequências graves, tornando a resiliência e a segurança uma prioridade. Redes confiáveis e seguras são essenciais para que os governos forneçam serviços públicos eficazes, protejam informações confidenciais e garantam operações tranquilas.

As Redes da Era Digital da ALE são resilientes e vão além do que muitos outros provedores de tecnologia oferecem. Incorporamos a segurança em nossa rede e em nossas soluções desde os primeiros estágios do projeto, sem custos adicionais de licenciamento.

6 práticas recomendadas para suas soluções de rede

1. Adote uma estratégia de segurança baseada em confiança zero. A macro e a microssegmentação de sua rede são cruciais para manter uma infraestrutura resiliente. Uma abordagem em fases para microssegmentação garante a implementação adequada e ajuda a evitar interrupções.
2. Considere adotar uma solução de Shortest Path Bridging (SPB) para redundância e segurança, pois essa abordagem redireciona dinamicamente o tráfego por vários caminhos em caso de falha, ao mesmo tempo em que cria uma rede eficiente e compartimentada. O SPB melhora a segurança com o encapsulamento MAC-in-MAC, eliminando endereços IP para evitar ataques de falsificação de IP e análise de pacotes.
3. Considere aproveitar os recursos de chassi virtual para aumentar a confiabilidade em áreas críticas, pois isso permite redundância e resiliência na rede, além de suportar atualizações de software em serviço (ISSU) e possibilitar interconexões dedicadas em malha ou anel. O chassi virtual apresenta uma solução econômica para simplificar o gerenciamento da rede e, ao mesmo tempo, garantir alta disponibilidade.
4. Considere implementar o protocolo VRRP (Virtual Router Redundancy Protocol). O VRRP aumenta a resiliência da rede fornecendo um roteador virtual de backup que pode assumir o controle imediatamente se o roteador principal falhar.
5. Implemente uma solução que garanta backups completos das configurações dos switches de rede, permitindo a restauração em caso de falha crítica ou sempre que necessário.
6. Uma medida de segurança avançada é utilizar o Secure Diversified Code, que randomiza a localização de diferentes segmentos de código nos seus switches, aumentando significativamente a segurança. Isso pode ser combinado com um processo independente de verificação e validação (IVV), conduzido por um especialista terceirizado em cibersegurança, que analisa e testa o sistema operacional para identificar e eliminar quaisquer vulnerabilidades, backdoors, malware ou exploits do sistema.

Invista em soluções de rede resilientes e seguras

Investir para garantir que sua rede seja resiliente e segura sempre faz sentido. Entretanto, entender onde investir melhor pode ser complexo e levar tempo – planejamento é fundamental. Antes de começar, aqui estão algumas áreas importantes a serem consideradas para garantir que você obtenha a segurança e a resiliência de que sua organização precisa:

- Revise e atualize o projeto da rede para garantir que os requisitos da sua organização sejam refletidos na rede, incluindo o nível adequado de resiliência para áreas sensíveis e críticas que afetam os serviços essenciais do governo. Para áreas críticas, considere adicionar servidores de backup e múltiplas conexões sempre que possível e aplicável.
- Considere a importância crescente do tempo de resposta a incidentes: por exemplo, usamos recursos de inteligência artificial (IA) e aprendizado de máquina (ML) em nosso Alcatel-Lucent OmniVista Network Advisor para identificar e resolver problemas mais rapidamente. Essa ferramenta garante que os problemas sejam resolvidos antes que afetem os usuários finais, identificando e abordando proativamente os problemas de rede ou segurança. Ele agiliza a solução de problemas e melhora a segurança da rede por meio de auditorias de configuração e administração de alertas em tempo real sobre qualquer mudança repentina no comportamento da rede.
- Considere switches reforçados para ambientes adversos. A família Alcatel-Lucent Enterprise de switches Ethernet robustos foi projetada especificamente para se destacar em ambientes desafiadores e temperaturas extremas. Esses switches são construídos com componentes resistentes e alojados em gabinetes robustos, garantindo durabilidade e confiabilidade, e têm o mesmo sistema operacional que o restante dos switches ALE. Para aumentar a segurança e proteger informações sigilosas, alguns modelos de switches são equipados com alertas de intrusão e relés de alarme que permitem a conexão de sistemas de alarme externos. Alguns modelos até são compatíveis com MACsec para comunicações de dados seguras entre as duas extremidades. Com o recurso de Chassi Virtual nos switches robustos, você pode obter redundância, resiliência e escalabilidade aprimoradas.

Soluções de comunicação resilientes e seguras

As comunicações são essenciais para que os governos interajam com os cidadãos, as partes interessadas e outros órgãos governamentais, assim como para a divulgação de informações importantes. Os sistemas de comunicação devem estar disponíveis em tempos de crise, quando os cidadãos mais precisam da assistência do governo. A resiliência e a segurança estão evoluindo, e revisões regulares ajudarão a manter sua solução de comunicações Alcatel-Lucent Enterprise sempre segura e disponível.

As soluções de comunicação da ALE são seguras desde o conceito. Isso significa que consideramos a segurança em cada etapa da definição, do desenvolvimento e da entrega do produto. Todos os sistemas operacionais e de hardware são reforçados, e a proteção contra negação de serviço (DoS) é integrada. Estamos em conformidade com certificações e credenciais reconhecidas para padrões globais de segurança e privacidade (ISO 27001, ISO 27017 e ISO 27018). Além disso, aderimos a padrões de segurança e privacidade específicos do setor, como o Health Insurance Portability and Accountability Act (HIPAA) nos EUA e o Hébergeurs de Données de Santé (HDS) para hospedagem de dados de saúde na França, bem como a padrões regionais de segurança e privacidade, como o General Data Protection Regulation (GDPR) na União Europeia.

6 práticas recomendadas para suas soluções de comunicação

A seguir apresentamos 6 práticas recomendadas para ajudar a garantir que você otimize totalmente a resiliência e a segurança incorporadas às suas soluções de comunicação ALE.

1. Certifique-se de ter a versão mais recente do software ou os patches corretos para ter as mais recentes melhorias de segurança, garantindo mais proteção.
2. Considere uma solução que inclua monitoramento de alarmes e lembre-se de realizar atualizações regulares com os limites corretos. Verifique se as notificações sobre falhas no sistema de comunicação ou alertas de qualidade são enviadas às pessoas apropriadas.
3. Revise e aplique uma política de senhas fortes, de preferência usando autenticação externa com um servidor RADIUS. Implemente lembretes aos usuários para ajudar a prevenir fraude nas chamadas telefônicas, que ainda são uma ameaça em muitos países.
4. Ofereça aos funcionários um treinamento de conscientização sobre segurança e garanta que eles estejam cientes dos riscos e das medidas de prevenção.
5. Assegure-se de ter o backup automatizado do sistema remoto para evitar a perda dos dados de configuração.
6. Considere uma VLAN específica para voz. Separar o tráfego de voz de outros tipos de tráfego reduz a chance de contaminação, o que pode potencialmente interromper as operações e até mesmo os serviços públicos.

Invista em soluções de comunicação resilientes e seguras

Nos últimos anos, o ambiente global tem destacado a importância das comunicações entre o governo e os cidadãos. A seguir, algumas áreas importantes a serem consideradas pelos órgãos governamentais que planejam investir em soluções de comunicação para aumentar a resiliência e a segurança.

- Arquitetura redundante e resiliente. Sua arquitetura deve ser totalmente redundante e resiliente. A duplicação de servidores de chamadas em áreas críticas, a implementação de redundância em locais remotos e a duplicação de servidores de aplicativos críticos podem oferecer proteção adicional.
- Crie um fluxo de trabalho usando o Rainbow e/ou o Visual Notification Assistant (VNA) da Alcatel-Lucent, com acionadores automáticos (acionador humano, IoT ou sistema) para notificar as pessoas-chave sobre os problemas do sistema, para que ajam rapidamente e acelerem o processo de recuperação.
- Implemente uma criptografia forte A criptografia é baseada em padrões da indústria integrados na solução, sem nenhum impacto sobre a qualidade e o desempenho da voz.

- Implemente o Rainbow™ da Alcatel-Lucent Enterprise, a ferramenta colaborativa ideal para complementar as soluções de comunicação da ALE. O Rainbow oferece um conjunto abrangente de recursos, incluindo voz, vídeo e mensagens instantâneas, possibilitando comunicações contínuas e colaboração eficiente. Com o Rainbow, você pode trocar imagens, vídeos e feeds de vigilância por vídeo, aprimorando a percepção contextual e permitindo uma melhor tomada de decisão. O Rainbow também oferece comunicações híbridas com conectividade segura entre o local e a nuvem. Garante comunicações resilientes, mantendo você conectado a colegas e clientes que usam o Rainbow, fornecendo conectividade ininterrupta mesmo em situações desafiadoras. As comunicações híbridas também têm a vantagem de as operações na nuvem e no local serem executadas em locais diferentes, para garantir a máxima resiliência e manter as comunicações abertas.
- Para agências com requisitos de segurança mais rigorosos, o Rainbow Edge oferece uma alternativa no local, com uma nuvem privada. Pode ser hospedada em qualquer data center, fornecendo controle total sobre servidores, armazenamento e redes, permitindo que as agências personalizem e configurem a infraestrutura de acordo com suas necessidades. Políticas personalizadas de segurança podem ser implementadas, e os recursos podem ser gerenciados de forma autônoma. Esse nível de controle oferece total visibilidade e autoridade sobre a infraestrutura, permitindo que as agências tomem decisões bem embasadas e otimizem o desempenho de acordo com seus objetivos.
- Defina uma estratégia de comunicação segura para a força de trabalho distribuída. A ALE oferece várias opções de comunicação e colaboração para funcionários distribuídos, móveis ou que trabalham em casa, incluindo:
  - Rainbow
  - IP Desktop Softphone
  - Softphone ALE
  - Deskphone com VPN incorporada, que pode ser implementado em massa com segurança incorporada (VPN)

Proteja seu pessoal e seus ativos

A ALE oferece sistemas de comunicação e notificação em tempo real flexíveis, seguros e altamente disponíveis. Essas soluções podem ser integradas às operações dos centros de controle de segurança pública ou de cidades inteligentes, simplificando o envio e a priorização de chamadas, facilitando a troca de informações contextuais com dados de IoT e aprimorando os esforços de colaboração entre os socorristas e várias partes interessadas, o que permite melhorar a tomada de decisões e a coordenação.

A capacidade de interconectar dispositivos de IoT em edifícios, locais e cidades, combinada com análise e IA, está transformando fundamentalmente o cenário das comunicações. Por meio da integração de sensores, vigilância por vídeo, fluxo de trabalho Rainbow e IA, é possível mudar de uma abordagem reativa para proativa, aumentando a eficiência do processo em termos de tempo e custo. Essa integração facilita uma compreensão abrangente do contexto, apoia os processos de tomada de decisão e, consequentemente, reduz os tempos de resposta a emergências. Funcionalidades como rastreamento de ativos, controle de fechaduras e luzes inteligentes simplificam as operações. Além disso, a capacidade de gravar comunicações e registrar ações simplifica a análise pós-evento, aprimorando os processos de segurança e reduzindo possíveis responsabilidades. Para alcançar esse nível de evolução, é fundamental um ambiente conectado com acesso Wi-Fi onipresente e fácil integração de IoT.

Para plataformas de comunicação em tempo real sensíveis ao tempo, seguras e altamente disponíveis, uma infraestrutura robusta é vital para garantir operações contínuas. Sua infraestrutura de tecnologia deve abranger o software adequado, protocolos de rede de alta disponibilidade e a flexibilidade para incorporar switches de rede robustos que possam se integrar perfeitamente ao seu ecossistema e suportar condições ambientais adversas incluindo fluxo de ar limitado, choques e temperaturas climáticas extremas. Optar por equipamentos robustos garante a longevidade em locais muito desafiadores, onde os equipamentos não robustos seriam menos duráveis.

No campo dos sistemas de segurança física, os riscos são altos. Cada minuto e cada pedaço de vídeo pode ser crucial para as autoridades identificarem irregularidades, identificarem a origem de um incidente ou entenderem a causa de um desastre. Uma infraestrutura robusta de vigilância por vídeo é essencial. A infraestrutura de rede deve não apenas fornecer largura de banda suficiente e Power over Ethernet (PoE) para as câmeras de vigilância, mas também integrar-se perfeitamente aos sistemas de gerenciamento de vigilância por vídeo. Essa integração garante uma rede de vigilância eficiente e confiável com operação tranquila e fácil solução de problemas. A equipe de operações deve ser capaz de resolver prontamente qualquer problema de vídeo, especialmente em ambientes onde cada quadro do vídeo é essencial. As integrações da solução Alcatel-Lucent OmniSwitch®, realizadas por meio de plugins com os principais sistemas de gerenciamento de vídeo, permitem que você atinja esse objetivo vital.

Além disso, há situações em que o rastreamento de ativos ou a localização de indivíduos ou equipamentos em sua organização se torna necessário. Uma solução eficaz de rastreamento de ativos depende de sua capacidade de localizar pessoas e ativos de forma fácil e precisa. Esse sistema também aumenta a segurança e a proteção, permitindo o envio rápido de assistência quando a localização dos indivíduos é conhecida. Com a solução Alcatel-Lucent OmniAccess® Asset Tracking, equipes e equipamentos podem ser localizados rapidamente e mostrados em um mapa de planta baixa. O rastreamento de ativos também fornece informações sobre os padrões de uso. Saber se os ativos estão sendo utilizados em excesso ou subutilizados pode fornecer informações valiosas.

Soberania e segurança dos dados

A Alcatel-Lucent Enterprise supera outros provedores de tecnologia na implementação das melhores práticas necessárias para a cibersegurança de ponta a ponta. Na ALE, nós:

- Seguimos as melhores práticas e recomendações do National Institute of Science and Technology (Instituto Nacional de Ciência e Tecnologia, NIST) ao realizar avaliações de risco em novos recursos e ao implementar em nossas soluções recursos de segurança cibernética, como criptografia nativa.
- Temos a certificação Common Criteria EAL2+ (Avaliação de Garantia de Nível 2 ou superior).
- Aplicamos as normas ISO 27001 a todas as nossas soluções baseadas em nuvem
- Apoiamos a ZTNA, segmentação de rede granular e políticas de segurança altamente específicas para reduzir o risco de atividades não autorizadas
- Executamos em nossos produtos testes específicos de segurança altamente especializados, como testes de penetração
- Garantimos que nossos produtos obtenham as principais certificações do setor, como HDS, HIPAA e Lei de Privacidade e Direitos Educacionais da Família (FERPA)
- A ALE International cumpre a Diretiva de Segurança de Redes e Informações da União Europeia (NIS 2).

Como especialistas reconhecidos em segurança cibernética, contribuímos para as propostas da União Europeia em relação às diretrizes de cibersegurança. Também aproveitamos nossa expertise em cibersegurança para ajudar os clientes a escolher e implementar a combinação certa de soluções seguras de comunicações unificadas e colaboração para atender às suas necessidades, além de treinar seus funcionários nas melhores práticas de cibersegurança.

©2025 ALE International, ALE USA Inc. Todos os direitos reservados em todos os países. O nome e o logotipo da Alcatel-Lucent são marcas comerciais da Nokia usadas sob licença pela ALE. Para ver uma lista de marcas registradas proprietárias da ALE, acesse: www.al-enterprise.com/en/legal/trademarks-copyright. DID23070401PT-BR (Abril de 2025)

Alcatel·Lucent Enterprise