Infraestruturas críticas no Brasil: requisitos de segurança e oportunidades para o gerenciamento de vídeo

requisitos de segurança e oportunidades para o gerenciamento de vídeo

Infraestruturas críticas no Brasil

MEDELLÍN, MEDELLIN, COLOMBIA, May 11, 2022 /EINPresswire.com/ -- As infraestruturas críticas são classificadas como instalações, serviços e bens públicos ou privados, considerados essenciais e que podem provocar sérios impactos social, econômico, político, internacional ou à segurança nacional, caso tiverem suas atividades interrompidas ou sua integridade afetada. Por essas razões os governos têm aumentado sua preocupação com as ameaças que devem ser superadas para a proteção dessas instalações, das quais depende o bem-estar dos cidadãos.

No Brasil as questões de segurança relacionadas com essa categoria de sites têm recebido uma grande atenção por parte do governo federal nestas últimas décadas. Desde 2007, a CREDEN (Câmara de Relações Exteriores e Defesa Nacional) vinculada ao GSI (Gabinete de Segurança Institucional) da Presidência da República, instituiu um GTSI (Grupo Técnico de Segurança de Infraestruturas Críticas), para propor medidas e ações de segurança específicas para os setores da água, energia, transportes, telecomunicações e finanças. Em 2018, os setores da biossegurança e bioproteção foram integrados nessa categoria de sites e por meio de um decreto presidencial foi estabelecida a PNSIC (Política Nacional de Segurança de Infraestruturas Críticas), que em 2020 evoluiu com a criação da ENSIC (Estratégia Nacional de Segurança de Infraestruturas Críticas).

A expansão desse arcabouço regulamentar e dos setores implicados nesta categoria de instalações denota a importância da abordagem de sua segurança no Brasil e em outras regiões

do mundo, como por exemplo na União Europeia, que desde 2006 instituiu o PEPIC (Programa Europeu para Proteção de Infraestruturas Críticas), e também nos Estados Unidos que dispõe de um órgão governamental específico para essa finalidade, a CISA (Agência de Segurança para as Infraestruturas e Cibersegurança).

Entre as principais ameaças à integridade dessas instalações, destacam-se três categorias principais: aquelas de ordem técnica provenientes de falhas nas maquinas e sistemas, as que são provenientes de ameaças humanas, de roubos até os ataques terroristas, e finalmente os incidentes de origem natural, como incêndios, inundações e etc. Os fatores de risco seguem aumentando em todas essas categorias de ameaças, mas cabe destacar o agravamento das questões climáticas com o aquecimento global e o aumento das catástrofes naturais, que podem impactar as infraestruturas críticas, justificando assim o monitoramento constante de sua integridade e segurança.

No âmbito da água e energia, nos últimos anos o Brasil tem enfrentado crescentes impactos e segundo a ANEEL (Agência Nacional de Energia Elétrica), em 2021 o país sofreu a maior escassez hídrica em 91 anos, com repercussão direta nas estruturas das centrais de produção, principalmente nas grandes usinas hidrelétricas (UHE). Em contrapartida, houve uma significativa ampliação da geração de energia eólica e também da PCHs (Pequenas Centrais Hidrelétricas) com mais de 1000 em construção atualmente, e mais de 1500 já em operação no país. Todo esse parque instalado e em construção, requer medidas e sistemas evoluídos, de acordo com a importância que representam para a economia e bem-estar da nação, com significativas oportunidades surgidas para os profissionais e empresas atuando na área da segurança.

Por todas essas razões os investimentos para proteção das infraestruturas críticas estão evoluindo proporcionalmente ao aumento dos riscos e a assimilação de sua importância pelos governos, empresas e organizações internacionais. De acordo com um estudo publicado em 2020 pela Report Linker, plataforma de inteligência de mercado, os investimentos para a proteção dessas instalações seguirão crescendo em média, mais de 7% ao ano neste período, atingindo a cifra de US$ 108,57 bilhões em 2025.

O papel do gerenciamento de vídeo na proteção da infraestrutura crítica

Vale ressaltar que para essa proteção, as estratégias de segurança são obviamente consideradas sob as duas vertentes, física e lógica; e que ambas têm evoluído em convergência, com a gestão da segurança física patrimonial cada vez mais próxima e integrada com a gestão dos sistemas de informação, da TI e suas redes de conexão.

Neste sentido, as plataformas de VMS (Sistemas de Gerenciamento de Vídeo), se apresentam como uma excelente resposta para prover a base da segurança nas instalações das infraestruturas críticas. Essas plataformas integram uma diversidade de soluções para o monitoramento inteligente em contínuo das instalações por meio de câmeras, controle de

acesso para pessoas e veículos, alarmes contra intrusão e perimetral, detecção contra incêndios, rondas programadas, sistemas de monitoramento comportamental e de incidentes, entre outros. Todavia, apesar da oferta de soluções de VMS ser relativamente abundante no mercado, poucas são aquelas de alto desempenho com recursos avançados, de nível corporativo, requeridos para atender às especificações de instalações distribuídas e/ou de médio à grande porte.

Tomando por base as infraestruturas para geração e distribuição de eletricidade, ou ainda as de telecomunicações, que tem em comum o aspecto “multi-site”, onde as instalações estão distantes geograficamente umas das outras e geralmente dispõem de uma central de comando e controle, onde é realizada a gestão operacional e de segurança. Para este tipo de aplicação a plataforma de gerenciamento de segurança deverá dispor de recursos adaptados, implicando uma boa escalabilidade e evolutividade, capacidades avançadas para configuração de dispositivos em rede, alta disponibilidade como o gerenciamento de “Failover” no servidor para atender aos planos de contingência, versões de atualização regulares agregando novos firmwares e opções de segurança, entre outros atributos.

O aspecto da flexibilidade para opções de dispositivos, por meio de uma ampla e evolutiva gama de integrações, em plataforma aberta (multimarcas e multiprotocolos), pode ser um bom balizador para a definição da plataforma à adotar. Algumas das plataformas líderes neste mercado já oferecem atualmente opções de mais de 11.000 dispositivos integrados, incluindo câmeras IP, módulos inteligentes para diferentes funções, além da integração com sistemas de alarme e controle de acesso de terceiros, tudo isso para compor uma solução completa e multifuncional.

Um outro aspecto balizador para que a plataforma multifuncional de gerenciamento de vídeo atenda aos requisitos estabelecidos pelas equipes de TI responsáveis por instalações de infraestruturas críticas, é a conformidade com os controladores de domínio e seus diretórios ativos, como o Active Directory (AD) da Microsoft, habilitando a configuração dos usuários no sistema de forma evoluída e centralizada. Em complemento como requisito para a gestão de usuários, um outro recurso avançado cuja conformidade poderá ser evocada é o suporte para logon único (single signo on, SSO), amplamente utilizado em ambientes corporativos.

A virtualização de hardware também é amplamente adotada nos sistemas de TI mais avançados, possibilitando potencializar os recursos em servidores com estrutura de processamento e memória de alta capacidade, com a instalação de múltiplas máquinas virtuais, economizando na utilização de espaço e consumo de energia nos centros de dados.

No entanto, com o crescente aumento dos ataques cibernéticos, a segurança dos sistemas de informação assumiu uma função ainda mais preponderante sobretudo no tocante à questão da criptografia de dados. Portanto, os sistemas mais robustos e avançados devem integrar recursos de criptografia e dispor de conformidade com algum referencial de segurança, como a certificação FIPS 140-2, um padrão governamental dos EUA que define os requisitos mínimos de

segurança para módulos criptográficos em produtos de tecnologia da informação.

A conformidade com esses padrões e funcionalidades, como a virtualização, o anuário AD, logon único (SSO), Failover, FIPS 140-2, entre outros abordados aqui acima, geralmente encontra-se disponível apenas nas plataformas de VMS mais completas e robustas.

Vislumbrando este conjunto resumido com a enorme diversidade de oportunidades que se apresenta no segmento das infraestruturas críticas, assim como de alguns dos requisitos para responder às especificações técnicas necessárias para sua segurança, é possível constatar que as aplicações multifuncionais baseadas nas plataformas de VMS, mais avançadas e completas, dispõem dos atributos para proporcionar uma resposta versátil, evolutiva e perene; e para tanto basta identificar o fornecedor com capacidade de oferecer o produto adequado para essa finalidade. Com certeza a escolha do bom produto e do bom parceiro fornecedor de VMS será decisiva para seu sucesso na abordagem e implementação dos projetos de segurança para essas instalações.

Victor Galvis
Siganalis Group
email us here
