WHITE PAPER

Usar dados em formato de vídeo como evidência

Protegendo a integridade dos dados em formato de vídeo com o AXIS Camera Station

Julho 2021

AXIS COMMUNICATIONS

Sumário

1 Resumo

Dados em formato de vídeo de alta qualidade, confiáveis e não adulterados podem ser usados como evidência. As práticas recomendadas para usar dados em formato de vídeo como evidência usando o AXIS Camera Station:

- Crie o design, configure e valide o seu sistema adequadamente para fornecer as imagens, gravações e segurança do jeito que você deseja
- Realize manutenção regularmente
- Use evidências seguindo procedimentos predefinidos

2 Introdução

Os vídeos gerados no monitoramento já são criados praticamente prontos para uso como evidência em tribunais. Um evento "filmado", digamos, não pode ser negado. Ou pode? Bem, um juiz provavelmente só aceitaria dados em formato de vídeo de alta qualidade, confiáveis e que não tenham sido adulterados.

Mas também há casos em que o valor do vídeo como evidência é reduzido não intencionalmente. Por exemplo, gravações com falhas, nas quais pessoas ou veículos desaparecem repentinamente ou "saltam" na imagem, podem não ser consideradas confiáveis o suficiente para serem usadas como evidência. Além disso, o vídeo também pode ser questionado se seus metadados, como os carimbos de data e hora ou o endereço MAC da câmera, não fizerem sentido. Qualquer suspeita de que o vídeo possa ter sido editado, excluído ou adulterado pode reduzir a credibilidade do proprietário do vídeo.

Este white paper contém informações sobre como fazer com que vídeos possam ser usados como evidência. O material descreve, mais especificamente, a função do software de gerenciamento de vídeo (VMS) AXIS Camera Station na cadeia de evidências e o papel do proprietário do vídeo.

Figure 1. Usar videomonitoramento em locais estratégicos pode gerar evidências valiosas se tudo for configurado e gerenciado corretamente

3 Práticas recomendadas para usar dados em formato de vídeo como evidência

As empresas e organizações que usam videomonitoramento precisam ter processos e procedimentos que ditem como usar e armazenar dados em formato de vídeo. Para estar totalmente preparado para quando uma das suas câmeras capturar um incidente, é preciso se certificar de que o vídeo está protegido contra sobrescrita, adulterações ou roubo. Além disso, é preciso ter a possibilidade de exportar a gravação com segurança para um armazenamento seguro e entregá-la para as autoridades.

Mas produzir evidências em vídeo de alta qualidade é um processo que começa com um projeto de criação de sistema de vídeo bem definido. Também é de extrema importância manter o sistema atualizado e ficar atento caso surjam irregularidades. Este capítulo apresenta as etapas deste processo e como elas podem ser seguidas com a ajuda do AXIS Camera Station e sua caixa de ferramentas, a AXIS Camera Station Integrator Suite.

Se você produzir, via monitoramento, vídeos que seguem esses princípios de design e manutenção de sistema e processamento de incidentes, eles atenderão aos requisitos atuais de segurança cibernética e, muito provavelmente, serão bastante úteis como evidência, se necessário.

Figure 2. O software AXIS Camera Station facilita a configuração, a operação no dia a dia e o gerenciamento estratégico de um sistema de videomonitoramento

3.1 Projete seu sistema adequadamente...

Um sistema de videomonitoramento deve ser projetado com cuidado. É necessário selecionar o equipamento que atenda às suas necessidades e configurá-lo para que ele gere as imagens, forneça o tipo de gravação e dê a segurança que você deseja. O AXIS Site Designer oferece ajuda ostensiva para que tudo isso possa ser implantado.

3.1.1 Para fornecer imagens do jeito que você deseja

A qualidade da imagem depende da câmera e do seu posicionamento. A resolução da imagem, ou, mais especificamente, a densidade de pixels das cenas dos eventos, pode ser calculada se você souber qual é o modelo e a lente da câmera e a distância e o ângulo dela em relação à cena. Para obter imagens com uma densidade de pixels adequada do rosto de uma pessoa na cena, pode ser necessário implantar mais câmeras ou usar câmeras com resolução mais alta. É preciso investigar o campo de visão, os requisitos de iluminação e outros parâmetros específicos para as câmeras implantadas nas suas instalações. Tudo isso pode ser feito sem problemas no AXIS Site Designer.

3.1.2 Para fornecer gravações do jeito que você deseja

Para gravar vídeo, você deve usar um hardware validado de alto desempenho que tenha redundância. Para aumentar a confiabilidade do sistema, o AXIS Camera Station faz gravação em fail-over armazenando

imagens no cartão SD da câmera em rede temporariamente. Se você usar análises de VMD (detecção de movimento de vídeo), certifique-se de que as gravações sejam longas o suficiente para serem úteis na análise do incidente como um todo. Uma gravação de detecção de movimento calibrada indevidamente pode conter lacunas e mostrar imagens que não fazem sentido. Uma gravação ininterrupta muitas vezes pode ser uma escolha melhor, mas precisa de um armazenamento maior e de uma largura de banda constantemente disponível.

3.1.3 Para fornecer segurança que do jeito que você deseja

Você precisar dar ao sistema a segurança física necessária para evitar acessos não autorizados. Todos os elementos de hardware, incluindo câmeras, equipamentos em rede e cabos, servidores, armazenamento de dados, dispositivos de alimentação de energia e cabos devem ser protegidos. É necessário aplicar medidas de segurança como: deixar a sala do servidor em uma área cujo acesso é restrito, trancar o gabinete do servidor, organizar o servidor em racks no gabinete, desativar portas físicas no servidor e manter os cabos de rede protegidos.

Também é necessário se esforçar para fornecer ao sistema a segurança cibernética necessária para minimizar os riscos de uso não autorizado de dados, tentativas de adulteração de dados e ataques maliciosos. Essa proteção pode ser parcialmente fornecida por ferramentas e tecnologias de software, o que garante que o sistema vai atender aos padrões de segurança atuais. Porém, o fortalecimento também exige que o proprietário do sistema implante uma mentalidade voltada à segurança cibernética e trabalhe ativamente para propagá-la na organização. Por exemplo, todos os usuários do sistema devem estar cientes da importância de usar senhas fortes e difíceis de adivinhar e de ter cuidado para não torná-las públicas. Além disso, é necessário minimizar acessos de usuários e reduzir as permissões para usuários usando, por exemplo, a abordagem que manda conceder apenas o mínimo de privilégios. O proprietário do sistema tem a responsabilidade de ensinar ao seu pessoal as práticas recomendadas e garantir que elas sejam implementadas com sucesso. Um integrador autorizado pode até fortalecer o sistema, mas a eficácia de certas medidas de segurança cibernética depende da cooperação ativa dos usuários do sistema.

Uma forma importante de aumentar a segurança cibernética no geral é proteger os vídeos usando transporte criptografado de dados. Na transmissão de dados entre o cliente e o servidor, o AXIS Camera Station usa criptografia AES para vídeo, áudio e metadados e criptografia TLS 1.2 para outros dados. O AXIS Camera Station pode ser configurado também para criptografar, via HTTPS, os streams de dados entre as câmeras e o servidor. Outras práticas recomendadas para a proteção dos softwares: desativação de serviços não utilizados, usar filtragem de endereços IP/MAC, acomodar IEEE 802.1X, acomodar monitoramento SNMP, configurar a data e hora corretas junto com um servidor NTP confiável (para garantir a precisão dos carimbos de data e hora dos metadados do vídeo) e usar apenas o AXIS Secure Remote Access para fazer conexões remotas (em vez de usar encaminhamento de porta ou área de trabalho remota). Para conhecer medidas e recomendações detalhadas de segurança cibernética, consulte o guia para o aumento do nível de proteção da segurança cibernética da Axis.

3.1.4 Configure e valide o seu sistema

É possível configurar partes essenciais do sistema já durante a fase de design no AXIS Site Designer. Defina nomes de câmeras, resoluções e tempos de retenção específicos. Quando o seu sistema é projetado e instalado, as configurações definidas no AXIS Site Designer podem ser importadas automaticamente para o AXIS Camera Station. Nele, você pode continuar a ajustar as configurações, se desejar.

Após a conclusão da instalação em si, você pode validar o seu sistema usando o AXIS Installation Verifier, que faz parte da AXIS Camera Station Integrator Suite. O verificador de instalação testa o sistema no modo normal e no modo noturno para verificar se há largura de banda suficiente para operar com pouca luz, momento quando os níveis de ruído são mais altos e é necessário ter mais largura de banda. O AXIS Installation Verifier executa um teste de estresse que aumenta continuamente o volume de dados gerado

no sistema até que o primeiro gargalo seja encontrado. Isso revelará a capacidade de o sistema aguentar sobrecarga e indicará se é necessário fazer melhorias.

3.2 Realize manutenção regularmente

Quando seu sistema estiver instalado e funcionando, é necessário continuar monitorando e atualizando esse sistema.

Certifique-se de que o hardware, assim como o software, continua funcionando como esperado. Inspecione a qualidade do vídeo, limpe as lentes das câmeras dentro de um cronograma, verifique se não houve adulteração física e se o campo de visão e a direção das câmeras estão devidamente configurados. Estude os logs do sistema regularmente, pois eles fornecem informações sobre logins, conexões e problemas com dispositivos. O AXIS Camera Station emite notificações quando descobre irregularidades e as registra nos logs do sistema. Encaminhe os logs para o armazenamento remoto somente leitura, principalmente após um incidente importante ocorrer. A Axis também oferece monitoramento online da integridade do sistema como parte da Integrator Suite, que permite monitorar todas as suas instalações e fornece o status do sistema para facilitar o serviço e a manutenção.

Tanto o hardware quanto os softwares (o sistema operacional e o VMS) devem ser atualizados regularmente. Se você sempre atualizar os softwares e os firmwares para as versões mais recentes, seu sistema se beneficiará muito com os mais recentes patches de segurança e correções de bugs. O ideal seria o VMS encontrar todas as atualizações de softwares e firmwares automaticamente e solicitar a instalação ou simplesmente fazer a atualização automaticamente. Faço o download de softwares apenas de fontes confiáveis.

3.3 Use evidências seguindo procedimentos predefinidos

Se você aplicou os princípios sobre como fazer o projeto e a manutenção do seu sistema de monitoramento da forma adequada, o AXIS Camera Station conseguirá fornecer evidências confiáveis de incidentes capturados pelas câmeras do sistema. Portanto, é necessário ter em prática procedimentos que indicam como proceder.

É de suma importância seguir as instruções das autoridades. Caso tenha ocorrido um crime grave, a autoridade responsável pelo caso tem o direito de decidir como as evidências devem ser protegidas. Você precisa seguir as instruções deles.

Caso contrário, o importante é exportar as evidências com segurança. Ou seja: é necessário transmiti-las para fora do seu sistema sem que sejam adulteradas, assim preservando a credibilidade delas, como acontece dentro do sistema.

A exportação deve ser realizada por um operador designado para a tarefa, de preferência juntamente com uma testemunha. Esse operador pode ser um profissional terceirizado, contratado exclusivamente para fazer uma exportação confiável e documentá-la. Contratar um terceiro independente para fazer a exportação pode minimizar o risco de desconfiança de que o proprietário do vídeo pode estar adulterando as evidências. O operador precisa exportar um vídeo que cubra o incidente em si, mas que também forneça informações suficientes sobre eventos deram origem ao incidente e sobre suas consequências.

Os vídeos selecionados podem ser exportados para mídias somente leitura, como CD-R, DVD-R ou Blu-ray (-R), que, por sua vez, podem ser entregues às autoridades. Uma alternativa é exportar os vídeos como arquivos compactados criptografados e protegidos por senha. Os arquivos podem ser assinados digitalmente com uma assinatura com um hash baseado na senha do usuário. Para confirmar o hash e

verificar o hash atual do arquivo, a assinatura deve ser inserida no AXIS File Player. Se os hashes baterem, nenhum dado foi alterado naquele arquivo.

A Axis fornece também o AXIS Camera Station Incident Report, uma ferramenta de exportação avançada para operadores. A ferramenta deve ser configurada com antecedência por um administrador, que precisa inserir dados como tags de incidentes e o local da exportação. Depois, o Incident Report automatiza a exportação, permitindo exportar vídeos classificados por incidentes e usar tags como nomes de pastas. Um recurso local pode servir como o local da exportação. Esse recurso pode ser, por exemplo, um armazenamento conectado à rede (NAS) ou um recurso remoto, como um armazenamento na nuvem acessível via protocolo SMB. O relatório será composto por arquivos de vídeo, instantâneos em .jpg (criados manualmente no AXIS Camera Station pelo operador durante a criação do relatório), favoritos em .txt e todas as informações coletadas em um relatório em formato .pdf.

4 Recursos de segurança cibernética

A Axis aumenta o nível de proteção cibernética das fases de design, desenvolvimento e teste de dispositivos para minimizar o risco de haver falhas que podem ser exploradas em um ataque. Seguimos as práticas recomendadas de segurança cibernética do mercado. Aplicamos essas práticas, por exemplo, ao gerenciamento de vulnerabilidades de segurança, aos requisitos para transmissão e armazenamento de dados com segurança e à criptografia. Nós nos dedicamos bastante para facilitar e baratear a aplicação dos devidos controles de segurança. Além disso, nossos dispositivos contam com criptografia e gerenciamento de segurança.

Embora a Axis, como fabricante e fornecedora do sistema, faça ao máximo para oferecer o sistema ou solução mais completa e segura possível, você, como usuário final, é o grande responsável por aplicar as práticas recomendadas de segurança. A Axis oferece várias ferramentas, guias e tutoriais como ajuda para você. Consulte www.axis.com/cybersecurity, site no qual é possível encontrar, por exemplo, guias para o aumento do nível de proteção, informações sobre gerenciamento de segurança e artigos sobre segurança cibernética.

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções para melhorar a segurança e o desempenho dos negócios. Como empresa de tecnologia de rede e líder do setor, a Axis oferece soluções em vigilância por vídeo, controle de acesso, intercomunicação e áudio. Nossas soluções são aprimoradas por aplicativos de análise inteligentes e apoiados por treinamento de alta qualidade.

A Axis tem cerca de 4.000 funcionários dedicados em mais de 50 países e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e tem sede em Lund, Suécia