WHITE PAPER

Digitalização e segurança cibernética das tecnologias de controle de acesso físico

Uma análise dos sistemas e protocolos que permitem que as empresas aproveitem todo o potencial do controle de acesso e criem um mundo mais inteligente e seguro

Agosto 2021

AXIS COMMUNICATIONS

Sumário

1 Resumo

O desenvolvimento da conectividade em nuvem está mudando o setor de segurança física, forçando os instaladores a se adaptarem para permanecerem no mercado. O controle dos sistemas de acesso parece estar migrando para o domínio das empresas globais de tecnologia, com uma expectativa de um maior valor agregado aos sistemas em si, conforme eles se tornam cada vez mais inteligentes, dimensionáveis e baseados na borda.

Essa evolução, juntamente com seu potencial de integração com outros sistemas corporativos, também significa que a segurança cibernética precisa desempenhar um papel ainda mais importante no desenvolvimento e na implantação do sistema, principalmente nos casos em que a base do sistema será a infraestrutura existente. A superação de barreiras técnicas, como a arquitetura em série, a ausência de endereços MAC e assim por diante, é uma etapa crucial na transição para sistemas de controle de acesso digitais que sejam capazes de atender às exigências atuais e futuras.

Implementar e proteger um sistema digital para controlar o acesso também significa seguir as práticas recomendadas, para garantir a melhor segurança possível. É preciso avaliar e testar todos os componentes envolvidos no sistema, sejam eles dispositivos, fornecedores ou protocolos — todos devem ser confiáveis e íntegros. Além disso, devemos estar sempre atentos ao cenário de ameaças e também às maneiras de reduzir os riscos relacionados a vulnerabilidades e falhas recém-descobertas.

Em particular, a escolha de seus fornecedores deve receber atenção especial, pois você estará permitindo que os dispositivos deles integrem a sua rede. Um fornecedor responsável deve fornecer e divulgar seus próprios processos para proteger suas ofertas — por exemplo, publicando um guia para aumento do nível de proteção, fornecendo ferramentas de gerenciamento dedicadas para simplificar o gerenciamento e a proteção dos dispositivos de rede etc. Adicionalmente, o fornecedor deve ser honesto e franco som relação à sua estratégia para gerenciar as vulnerabilidades e falhas detectadas.

2 Introdução: O futuro do controle de acesso

A conectividade em nuvem apresentou ao setor de segurança física uma nova visão de como os sistemas devem ser implantados e utilizados. Usuários finais e compradores estão exigindo soluções mais inteligentes, integradas e voltadas para os negócios, com recursos de monitoramento e controle de acesso que vão muito além daqueles oferecidos pelas antigas tecnologias tradicionais.

Muitos fornecedores criaram um modelo de negócios sólido, que gira em torno de suas experiências, serviços e conhecimentos sobre a segurança física. No entanto, a conectividade de rede e a IoT (Internet das coisas) apresentam um cenário em constante mudança, o que exige que fornecedores e instaladores tradicionais de segurança física aprendam a linguagem da TI, das plataformas abertas, da conectividade IP e da integração de software, para que se adaptem às mudanças do mercado e mantenham a relevância.

Parece que o controle está migrando rapidamente dos fornecedores de sistemas de acesso eletrônico para as empresas globais de tecnologia — que, agora, têm o poder de moldar a segurança de formas que desafiam seu modo de operação tradicional. Os edifícios e cidades inteligentes apresentam grandes oportunidades, e muitos antecipam o rápido crescimento do mercado de controle de acesso moderno, conforme a facilidade de implantação e a sofisticação das tecnologias atuais oferecem cada vez mais benefícios para os ambientes inteligentes.

Não é de surpreender o surgimento de incentivos para adotar o controle de acesso hospedado, conforme o impacto dos gigantes do setor demonstra o sucesso das tecnologias em nuvem, tão amplamente utilizadas durante a pandemia de COVID-19. Essas empresas têm o alcance, a capacidade e a imaginação necessárias para fazer mudanças radicais, e a segurança física também será transformada conforme as empresas,

percebendo o valor da nuvem, buscam soluções hospedadas para cuidar de todos os seus requisitos de segurança e negócios.

Entretanto, atualmente muitos fabricantes simplesmente não estão prontos para esse mercado dinâmico e ainda seguem modelos de negócios baseados em projetos proprietários rígidos. A transição para as soluções de segurança física inteligentes existe em contraste direto com essa abordagem tradicional, que provavelmente será fortemente contestada. Embora essa transição não aconteça da noite para o dia e as novas soluções de hospedagem em nuvem ainda não sejam predominantes, esse novo mundo promissor é o domínio dos novos técnicos que estão se juntando ao nosso setor agora.

O futuro do controle de acesso e da segurança física como um todo será, assim, baseado em expectativas de maior valor agregado. Os sistemas de controle de acesso se tornarão pontos de coleta de dados, e os controladores de portas se tornarão dispositivos de E/S inteligentes. Os códigos QR, para gerenciamento de visitantes, e o reconhecimento biométrico facial, para proporcionar um controle de acesso descomplicado, serão cada vez mais gerenciados na borda, como dados analíticos em uma câmera ou sensor. As tecnologias de controle de acesso estão passando por um momento estimulante e desafiador — para aqueles que estiverem prontos para aceitar e ajudar a moldar o futuro, uma grande oportunidade para inovar e criar um mundo mais inteligente e seguro.

Nesta publicação, nós exploramos os aspectos que são particularmente relevantes para o controle de acesso, incluindo muitos dos recursos básicos desses sistemas. Além disso, vamos examinar as considerações relacionadas às práticas recomendadas para fornecedores, com informações e sugestões para os usuários finais, com o intuito de proporcionar a eles a confiança necessária para que questionem seus fornecedores e tomem decisões de compra mais embasadas.

3 Os desafios de um mercado de controle de acesso em evolução

Ao nos debruçarmos sobre os PACSs (Sistemas de controle de acesso físico), tendemos a abordar os fatores de risco em relação à autorização ou bloqueio da entrada física. Adotar uma abordagem equilibrada ao desenhar um sistema de controle de acesso físico é uma consideração importante, que deve ser baseada na análise das ameaças potenciais.

Atualmente, com os edifícios cada vez mais protegidos por soluções de controle de acesso eletrônico sofisticadas, esses sistemas fornecem uma maneira rápida e eficiente de gerenciar o acesso de toda uma empresa, deixando uma pegada digital que pode ser examinada e monitorada sempre que necessário, além de serem totalmente integrados a outros sistemas, como os de gestão de RH e de visitantes.

Com essa unificação de sistemas produzindo insights importantes para auxiliar na tomada de decisões de negócios e de segurança, bem como para controlar o acesso, torna-se crucial avaliar cuidadosamente a maturidade cibernética do sistema. À medida que os criminosos se tornam mais ousados e o cenário de ameaças continua a evoluir, o desafio passa a consistir em reduzir os riscos de clonagens de credenciais de acesso, ameaças internas ou ataques cibernéticos remotos.

No entanto, a própria arquitetura representa um problema. Muitos sistemas tradicionais de controle de acesso são baseados em infraestruturas ultrapassadas. Com a convergência das tecnologias de segurança que geralmente utilizam essa infraestrutura, o desafio dos fornecedores é, em parte, adaptar seu hardware para conectá-lo a essas redes corporativas e, para além disso, perceber a importância da segurança de TI e desse cenário de segurança em constante mudança, que impulsiona a necessidade de avaliar e proteger integralmente as empresas contra os diversos riscos enfrentados por elas.

A segurança cibernética deve ser um fator-chave no desenvolvimento dos novos sistemas de segurança. As tecnologias de controle de acesso são parte integrante de qualquer solução de segurança física e, portanto,

devem ser fabricadas de acordo com princípios estabelecidos de segurança cibernética, criação de relatórios de incidentes e práticas recomendadas. É importante reconhecer que a integridade de um sistema é tão forte quanto seu elo mais fraco. **Um sistema que não esteja preparado para estar em conformidade com essa premissa** constituirá um risco potencial de exposição. Se não for possível demonstrar a agilidade para aceitar, informar e implementar ações de recuperação amplamente reconhecidas, em última análise, isso afetará negativamente a capacidade do sistema de fornecer os níveis necessários de segurança física para os quais ele foi implantado.

3.1 Credenciais de segurança cibernética (maturidade cibernética)

O envolvimento crescente do setor de TI está começando a mudar a forma como as tecnologias são avaliadas, implantadas e conservadas. Uma consideração importante para as partes interessadas da área de TI é a avaliação das credenciais de segurança cibernética de uma empresa, com foco principal no conhecimento que o fornecedor tem sobre segurança cibernética. Este conhecimento também é conhecido como cibermaturidade. Ser cibermaduro sugere um bom entendimento do cenário de ameaças e da mitigação de risco. A documentação e as orientações abrangentes sobre a segurança cibernética que já foram elaboradas para as câmeras em rede também podem ser aplicadas ao controle de acesso físico, pois os desafios, avaliações e explicações sobre os riscos cibernéticos e sobre o potencial de ataques são igualmente relevantes para esses produtos.

3.2 O futuro da arquitetura dos sistemas de segurança

Os dispositivos de controle de acesso modernos são conectados por meio de cabos de rede e conectores RJ45. As redes fornecem energia aos controladores de acesso, além da comunicação entre os dispositivos e os sistemas de gerenciamento central. A força motriz do controle de acesso é a transição para sistemas baseados no protocolo TCP/IP (Protocolo de controle de transmissão/Protocolo de Internet). Desde a apresentação do primeiro controlador de porta verdadeiramente habilitado para a tecnologia IP (o AXIS A1001) em 2013, os PACSs continuaram a evoluir, agora oferecendo uma ampla variedade de recursos avançados — o que não seria possível de dependêssemos exclusivamente da tecnologia antiga.

Entre os exemplos dessas inovações estão os leitores de código QR que facilitam o controle de acesso sem contato físico, o reconhecimento facial por meio da integração com câmeras em rede e a leitura de placas de licença, todos interagindo com os bancos de dados dos PACSs para que as decisões de autorização ou bloqueio da admissão sejam tomadas na borda. Os principais benefícios dos sistemas IP incluem os custos de instalação reduzidos, além de configurações e gerenciamento de dispositivos simplificados. A fácil integração com outros dispositivos se traduz em uma solução preparada para o futuro, que viabiliza a conectividade plug-and-play simples de novas tecnologias e aprimoramentos de segurança, à medida que forem disponibilizados.

3.3 Controle de acesso IP versus tradicional

As vantagens da tecnologia IP serão percebidas nos novos desenhos do controle de acesso moderno, principalmente em sistemas sem contato físico, que os usuários finais esperam ter por padrão. Os usuários também desejam que o controle de acesso se adapte ao uso de smartphones e tablets — e não apenas como credenciais móveis. Como o setor fornecerá sistemas de controle de acesso melhores e mais úteis, que poupem tempo/custos e que sejam capazes de acompanhar os ciclos de inovação impulsionados pelas grandes empresas de tecnologia? Esses são os desafios dos fornecedores do setor.

Até o momento, essas oportunidades não foram exploradas, possivelmente porque os sistemas de controle de acesso antigos dependem de controladores de portas instalados em arquiteturas em série e

conectados usando cabeamento RS-485 a uma unidade ou servidor central. Além disso, os sistemas são, em sua maioria, proprietários, o que significa que o controlador de porta é "bloqueado", permitindo o gerenciamento usando somente software designado pelo fornecedor. Isso limita o usuário final a um único fornecedor de hardware e software, e a complexidade de tais sistemas geralmente requer uma equipe especializada para a instalação e configuração.

Ao expandir sistemas de acesso tradicionais, o processo é complicado pela forma como os controladores centrais típicos são projetados para acomodarem somente uma determinada quantidade de portas, o que leva configurações fora do padrão a terem altos custos devido à flexibilidade limitada do sistema. Adicionar uma única porta extra, por exemplo, pode resultar em custos muito mais elevados, tornando a adição injustificadamente dispendiosa.

As redes IP permitiram a introdução de uma arquitetura de PACSs muito mais simples e fácil de instalar, com muito mais flexibilidade e capacidade de personalização. Os profissionais de TI têm acentuada preferência pelo uso de dispositivos verdadeiramente IP em sistemas de controle de acesso baseados em rede. Incluir esses profissionais no processo de desenho é fundamental, pois eles garantirão o uso desses dispositivos IP, que também são essenciais para reduzir os custos de expansões e serão um requisito nos projetos de controle de acesso do futuro.

3.4 Protocolos abertos

O futuro do controle de acesso depende da disposição dos fabricantes de compartilharem suas habilidades e capacidades em um fórum de protocolo aberto. Obviamente, essa abertura enfrenta resistência, pois muitos desenvolvedores de sistemas de acesso parecem dar preferência a um processo que vincule os usuários finais a suas soluções proprietárias, garantindo as receitas futuras. Contudo, essa abordagem não oferece nenhuma vantagem no longo prazo. Os usuários estão exigindo cada vez mais das soluções e ficam satisfeitos em compartilharem seus dados para isso.

Os designers de sistemas e os fornecedores de hardware de acesso raramente têm os recursos ou conhecimentos em TI necessários para oferecer todas as soluções de que os usuários precisam para terem um sistema de segurança física abrangente. Muitos parecem genuinamente inconscientes do fato de que suas ofertas estão sendo rapidamente ofuscadas por soluções modernas e inovadoras, que ameaçam tanto seu modelo de negócios quanto sua posição no mercado de controle de acesso. Os recursos desses novos sistemas são tão arrojados, e essas inovações surgem com tamanha velocidade, que agora estamos muito perto de não precisarmos mais dos controladores de acesso, pois as unidades de E/S inteligentes estão se tornando as substitutas óbvias.

A abertura permite que os fornecedores criem dispositivos adequados para sistemas de acesso de pequeno porte, que devem ser fundamentalmente mais simples e ter custos de aquisição e instalação competitivos. Os mesmos dispositivos podem, então, ser adaptados para operações maiores e tecnicamente mais complexas, conforme necessário. Essa flexibilidade é a marca registrada da segurança moderna e garante que os sistemas adquiridos hoje continuem a ser relevantes no futuro, conforme os negócios do usuário crescem e os requisitos mudam.

Mais informações sobre abertura e tecnologia aberta podem ser encontradas no site do ONVIF (Fórum Aberto de Interface de Vídeo em Rede), *www.onvif.org*, um órgão do setor criado para estimular o desenvolvimento de padrões abertos.

4 Barreiras técnicas à adoção

Há muito a ser considerado em relação as conexões técnicas, interfaces e dispositivos que tornam possível o controle de acesso digital. A migração dos sistemas tradicionais para os sistemas habilitados para nuvem

pode ter ramificações importantes. As próximas seções detalham os pontos que devem ser considerados para ajudar a evitar que a tecnologia existente, e os processos associados a ela, se torne uma barreira para a modernização e para a adoção de novas soluções.

4.1 Controladores RS-485

Entre as considerações, há a implantação de controladores RS-485 e o risco potencial da instalação de dispositivos semi-inteligentes que raramente, ou nunca, têm um endereço MAC (Controle de acesso à mídia), o que dificulta sua identificação. O padrão RS-485, também conhecido como TIA-485(-A) ou EIA-485, define as características elétricas de drivers e receptores para uso em sistemas de comunicação serial. Os sinais elétricos são equilibrados e os sistemas multiponto são suportados. Mas o protocolo RS-485 especifica somente a camada física: o gerador e o receptor. Ele não comanda a camada vital de comunicação.

Observe que a ausência de um endereço MAC ou a adoção de uma arquitetura em série não representa, por si só, um problema de confiabilidade nem tem efeitos prejudiciais sobre o funcionamento de um sistema de controle de acesso, pois esses desenhos têm sido a base das tecnologias de controle de acesso há mais de 30 anos. No entanto, é difícil visualizar melhorias na área de segurança, a menos que cada dispositivo de controle em um sistema de controle de acesso seja inteligente e possa ser tratado individualmente. Partimos do princípio de que apenas sistemas totalmente inteligentes e dispositivos totalmente acessíveis poderão oferecer o valor agregado esperado no futuro. Observe que "totalmente acessíveis" não significa que os dispositivos sejam pouco seguros do ponto de vista cibernético — muito pelo contrário.

4.1.1 OSDP (Protocolo de dispositivo supervisionado aberto)

Um novo método de comunicação, que foi aceito pela IEC (Comissão Eletrotécnica Internacional) e oferece o potencial de aumentar a segurança nas comunicações de acesso, é o OSDP (Protocolo de dispositivo supervisionado aberto), um padrão de comunicação de controle de acesso desenvolvido pela SIA (Security Industry Association) dos Estados Unidos para melhorar a interoperabilidade entre os produtos de controle de acesso e de segurança. O OSDP usa criptografia de 128 bits, é compatível com instalações multiponto e supervisiona as conexões para relatar problemas com os leitores. Outro ponto a ser observado é que o OSDP é compatível com leitores de cartão, contratestas de portas, contatos de alarmes e funções de solicitação de saída usando apenas dois fios — e não várias conexões por porta, como era necessário anteriormente. O site da SIA informa que "o protocolo OSDP foi aprovado como um padrão internacional pela Comissão Eletrotécnica Internacional em maio de 2020 e foi publicado como a norma IEC 60839-11-5 em julho de 2020. O OSDP da SIA está em constante aprimoramento para manter sua posição de liderança no setor".

4.2 A importância dos dispositivos que têm um endereço MAC

O endereço MAC é o endereço global exclusivo do hardware de um adaptador de rede ou dispositivo individual. Em relação à rede de TI, o endereço MAC é tão importante quanto um endereço IP. Os endereços MAC identificam um computador na LAN (Rede de área local) de forma exclusiva e são necessários para o funcionamento dos protocolos de rede, como o TCP/IP. O endereço MAC é codificado permanentemente no dispositivo e, embora seja possível falsificá-lo por meio do sistema operacional, isso obviamente não é recomendável — o endereço deve ser protegido pela sua solução de segurança.

O protocolo TCP/IP e outras arquiteturas de rede convencionais geralmente adotam um modelo OSI (Interconexão de sistemas abertos), no qual a funcionalidade da rede é subdividida em camadas. Os endereços MAC operam na camada de link de dados (camada 2 do modelo OSI) e permitem que os computadores se identifiquem de forma exclusiva em uma rede. A filtragem de endereços MAC adiciona uma camada extra de segurança. Antes de permitir que qualquer dispositivo se conecte à rede, o roteador

verifica o endereço MAC do dispositivo em uma lista de endereços aprovados. Se o endereço do cliente estiver na lista do roteador, o acesso será concedido; caso contrário, o acesso será negado.

4.2.1 Power over Ethernet (PoE)

A tecnologia PoE oferece dois benefícios que são consistentes em todas as aplicações: economia de custos e flexibilidade de disposição dos dispositivos. O PoE transporta dados e energia no mesmo cabo, o que significa que a arquitetura de dispositivos pode ser simplificada, quando comparada aos desenhos tradicionais. É importante observar que muitos sistemas de controle de acesso são divulgados como sendo conectados por IP.

5 Os marcos das práticas recomendadas

O gerenciamento do controle de acesso é um componente importante para lidar com o fluxo de pessoas e controlar o acesso de maneira eficaz. Muito mais do que apenas trancar uma porta ou implantar uma barreira, as empresas exigem opções de controle melhores, para fornecerem um atendimento ao cliente aprimorado e altos níveis de segurança, sempre. A adoção de práticas recomendadas para um controle de acesso abrangente vai além da seleção das ferramentas certas. Ela tem a ver com a implementação da arquitetura ideal, incorporação de tecnologias de alta qualidade, procedimentos e protocolos corretos e incentivo à adoção das atitudes e comportamentos adequados pela equipe e pelas partes interessadas.

5.1 Gestão das partes interessadas e uma abordagem convergente para a segurança

Conforme observamos o cenário da tecnologia convergir para uma mesma infraestrutura a fim de fornecer as tecnologias operacionais necessárias para que essas instalações funcionem perfeitamente, também observamos a necessidade de termos processos de tomada de decisões convergentes. Há exemplos de sucesso de abordagens convergentes para a segurança ultrapassando barreiras e permitindo que diferentes equipes empresariais trabalhem em conjunto. Essa convergência nunca foi tão importante quanto é hoje, quando as ofertas tradicionais de segurança eletrônica e física existem lado a lado nas redes corporativas.

É vital que as equipes de segurança física possam contar com tecnologias que atendam a seus requisitos operacionais e que abordem os riscos associados, ao mesmo tempo apoiando as políticas de segurança de TI e garantindo que os dispositivos físicos não se tornem um backdoor para a rede corporativa. Com todas as partes interessadas trabalhando juntas, é possível criar um ambiente cibernético e físico mais seguro.

5.2 O que esperar de parceiros, vendedores e fornecedores

É importante garantir que as outras partes envolvidas entendam a importância de manter as melhores práticas de segurança à frente de tudo o que fazem e que essas partes operem para atender a necessidades específicas. Relacionamentos com outros fornecedores são essenciais para estabelecer uma cadeia de fornecimento saudável e criar vínculos de confiança sólidos.

As principais considerações ao avaliar terceiros e seu impacto sobre a cadeia de fornecimento incluem:

- Eles entendem e reconhecem os riscos associados à segurança cibernética
- Eles podem demonstrar uma abordagem de segurança cibernética madura com processos e ferramentas disponíveis
- Eles entendem o impacto dos regulamentos e da legislação em sua oferta

- Eles podem demonstrar como darão suporte aos requisitos de conformidade de um usuário
- A segurança cibernética é um processo e não apenas uma tecnologia. Eles podem demonstrar o gerenciamento do ciclo de vida da segurança cibernética para proteger a empresa de um usuário.

5.3 Gestão da segurança: governança e processos dos fornecedores

Assim como ocorre com toda segurança considerada eficaz, a segurança cibernética está relacionada ao alcance da sua defesa. Trata-se de proteger adequadamente a rede de câmeras IP em todos os níveis, dos produtos e parceiros selecionados até os requisitos definidos.

5.3.1 Normas e diretivas

A norma ISO 27001 — Gestão de Segurança da Informação ISO/IEC 27001 é um Sistema de gerenciamento da segurança que exige:

- A análise sistemática dos riscos à segurança das informações de uma organização, levando em consideração ameaças, vulnerabilidades e impactos.
- O desenho e a implementação de um conjunto coerente e abrangente de controles de segurança da informação e/ou de outros métodos de gestão de riscos (como prevenção ou transferência de riscos) para lidar aqueles considerados inaceitáveis.
- A adoção de um processo de gerenciamento geral, para garantir que os controles de segurança atendam continuamente às necessidades de segurança da informação da organização.

5.3.2 Cyber Essentials Plus

O Cyber Essentials (Fundamentos cibernéticos) é um esquema apoiado pelo governo do Reino Unido e pelo setor para ajudar as organizações a se protegerem contra ameaças on-line comuns. O Cyber Essentials é um indicador eficaz para as empresas que entendem os desafios apresentados pela segurança cibernética e consiste em uma avaliação das políticas e processos de uma empresa. O esquema analisa especificamente:

- Configurações seguras
- Controle de acesso e administração
- Proteção contra malware
- Gerenciamento de patches
- Firewall e gateways de Internet

Para os fabricantes de tecnologia, a primeira linha de defesa deve ser a atenuação dos riscos associados a seus próprios sistemas. Desde 1º de outubro de 2014, o governo do Reino Unido exige que todos os fornecedores que participam de licitações de contratos envolvendo o manuseio de determinadas informações confidenciais e pessoais sejam certificados de acordo com o esquema Cyber Essentials.

5.3.3 Secure by Design, Secure by Default

Lançada em 2019 pelo Surveillance Camera Commissioner (Comissário de Câmeras de Monitoramento) do Reino Unido, a certificação **Secure by Design, Secure by Default** (Seguro desde o projeto, seguro por padrão) define os requisitos mínimos para os fabricantes de sistemas e componentes de câmeras de monitoramento. O esquema exige que os fabricantes adotem uma abordagem holística para solucionar

os problemas de segurança em sua origem, em vez de tratar os sintomas, agindo de forma abrangente para reduzir os danos a um sistema ou a um tipo de componente.

A certificação Secure by Design, Secure by Default abrange as iniciativas técnicas de longo prazo para garantir que as características básicas de segurança adequadas sejam integradas ao software e ao hardware. Ela também abrange a tarefa igualmente exigente de garantir que essas características básicas estejam disponíveis e sejam funcionais, de forma que o mercado possa adotá-las prontamente.

Para apoiar nossas tecnologias, a Axis alinhou as exigências da certificação Secure by Design, Secure by Default ao código de conduta do plano de Estratégia Nacional de Segurança Cibernética:

- Solicitação de senha
- Indicador de nível de segurança da senha
- Criptografia HTTPS (Protocolo de transferência de hipertexto seguro)
- 802.1x
- Acesso remoto DESATIVADO (NAT traversal)

6 Guias e ferramentas (processos do fornecedor)

Quando se trata de proteger uma rede, as organizações geralmente implantam vários controles técnicos para criar uma abordagem de "defesa em camadas", o que ajuda a limitar os pontos únicos de falha e exposição. Entretanto, um processo importante, que muitas vezes é negligenciado, é o "aumento do nível de proteção do sistema", que inclui fazer alterações nas configurações padrão para que o sistema fique mais protegido contra ameaças à segurança da informação. Além disso, esse processo ajuda a reduzir a quantidade de vulnerabilidades inerentes que existem em todos os sistemas.

6.1 Guia para aumento do nível de proteção na fabricação

Um processo para o aumento do nível de proteção do sistema deve ser implementado para todos os dispositivos conectados a uma rede. Isso inclui estações de trabalho, servidores e outros dispositivos de rede. Como cada fabricante conhece sua própria instalação e configuração do sistema melhor do que ninguém, sua responsabilidade é fornecer aos parceiros e usuários as informações necessárias para proteger a integridade dos dispositivos e da instalação do usuário final. Um guia para aumento do nível de proteção deve fornecer orientações técnicas a todos os envolvidos na implantação de soluções de videomonitoramento. Ele deve definir uma configuração básica, bem como fornecer informações abrangentes sobre como lidar com o cenário de ameaças em evolução.

Todos os fornecedores devem se esforçar para implementar as práticas recomendadas de segurança cibernética ao desenho, ao desenvolvimento e aos teste dos dispositivos, a fim de minimizar o risco de falhas que possam ser exploradas em um ataque. No entanto, proteger uma rede, os dispositivos conectados a ela e os serviços que a apoiam requer a participação ativa de toda a cadeia de fornecimento do fornecedor e também da organização do usuário final. Um ambiente seguro depende de seus usuários, processos e tecnologia. Um bom guia para aumento do nível de proteção deve seguir os usos básicos, como o CIS Controls (Controles do Center for Internet Security) — Versão 6.1. Esses controles eram anteriormente conhecidos como SANS Top 20 Critical Security Controls (20 principais controles críticos de segurança da System Administration, Networking and Security).

6.2 Gerenciamento de dispositivos

Um gerenciador de dispositivos é uma ferramenta local que fornece uma maneira simples, econômica e segura de gerenciar os dispositivos conectados. Ele oferece a instaladores e administradores de sistemas uma ferramenta altamente eficaz para gerenciar todas as principais tarefas de instalação, segurança e manutenção.

Inventário de dispositivos/sistema de gerenciamento de ativos:

- Política de contas e senhas
- Instalação eficiente de atualizações de firmware e aplicativos
- Aplicação de controles de segurança cibernética — gerencie os certificados HTTPS e carregue os certificados IEEE 802.1x; gerencie de contas e senhas
- Garantia de gerenciamento do ciclo de vida — gerencie todas as principais tarefas de instalação, segurança e operacionais
- Configuração rápida e fácil de novos dispositivos — faça backup e restaure configurações
- Indicado para instalações de todos os portes — instalações em uma única unidade ou em várias unidades

6.3 Os desafios associados aos OEMs/ODMs

Os OEMs (Fabricantes de equipamento original) são fabricantes que revendem produtos de outra empresa usando seu próprio nome e marca. Um ODM (Fabricante de projeto original) é uma empresa que projeta e fabrica um produto que é especificado e vendido sob a marca de outra empresa. Essas empresas permitem que uma marca se envolva na fabricação sem precisar montar ou administrar uma fábrica.

Para um fabricante, há muitas vantagens em ser um OEM ou ODM de um produto de outro fornecedor. A primeira é que isso elimina os risco e custos da fabricação, permitindo que a organização se concentre nos processos de vendas e marketing. Este é um dos principais motivos que leva muitos fabricantes de câmeras do setor de segurança a terem produtos de marca de OEMs ou ODMs.

Essa questão apresenta vários desafios — um dos mais óbvios é a segurança cibernética. Se um fabricante oferecer produtos que apresentem alguma vulnerabilidade, isso poderá afetar todos os outros revendedores e parceiros por toda a cadeia de fornecimento, o que também pode dificultar a visibilidade total da cadeia. Com o grande número de OEMs e ODMs em operação, um usuário final que tenha praticado a devida diligência e se recuse a usar tecnologias de um determinado fabricante pode acabar usando essas tecnologias inadvertidamente através de produtos de outras marcas.

6.4 Chip microprocessador de CPU

Parece que os chips genéricos de processamento de CPU instalados em alguns dispositivos estão sendo alvos de hackers, com muitas vulnerabilidades sendo identificadas. Um dos principais motivos é a escalabilidade gerada a partir de uma única vulnerabilidade identificada. Exemplos recentes incluem as falhas "Meltdown" e "Spectre", dois ataques relacionados de canal lateral contra microprocessadores de CPU modernos, que têm a capacidade de acessar dados de forma ilícita usando códigos sem privilégios.

A maioria dos dispositivos, de smartphones a hardware em data centers, pode estar vulnerável em algum nível. Os principais fornecedores de sistemas operacionais criaram patches que atenuam os problemas, embora algumas partes dessas correções precisem ser instaladas pelo OEM, pois contêm elementos

específicos da plataforma. O NCSC (National Cybersecurity Centre) do Reino Unido recomenda a aplicação de patches nos dispositivos o mais rápido possível.

6.5 Estratégia de firmware

O firmware assinado é importante para os usuários finais e atenua alguns riscos potenciais de violação dos dispositivos ao longo do processo de logística e/ou distribuição. A assinatura, por vezes denominada hash, é anexada ao firmware na distribuição. Um processador calcula seu próprio hash e só carregará uma imagem de firmware que tenha um hash correspondente assinado por um certificado em que ele confie.

6.6 Gerenciamento de vulnerabilidades

O avanço contínuo dos crimes cibernéticos e dos riscos associados a eles estão forçando muitas organizações a se concentrarem mais na segurança da informação. O processo de gerenciamento de vulnerabilidades deve fazer parte das iniciativas de uma organização para controlar os riscos à segurança da informação. Esse processo fornecerá uma visão geral contínua das vulnerabilidades no ambiente de TI e dos riscos associados a elas. Somente identificando e atenuando as vulnerabilidades no ambiente de TI será possível impedir que os invasores penetrem nas redes e roubem informações.

É essencial que os fornecedores garantam que o gerenciamento de vulnerabilidades seja abordado em suas operações, incluindo processos para detectar e corrigir vulnerabilidades em todos os sistemas e para evitar que novas vulnerabilidades sejam introduzidas durante os processos de alteração e implantação de novos sistemas. Todas as questões relacionadas ao risco que o fornecedor aceita devem ser comunicadas e acordadas com o usuário final. Se esse princípio não for implementado, os invasores podem explorar vulnerabilidades nos sistemas para realizar ataques cibernéticos contra uma empresa e seus fornecedores.

Os patches de segurança de TI e as atualizações relacionadas a vulnerabilidades de segurança devem ser instalados por meio de processos aprovados e em tempo hábil, para evitar violações de segurança. Os sistemas do fornecedor que, por algum motivo, não possam ser atualizados devem implementar medidas para proteger o sistema vulnerável. Todas as alterações devem ser realizadas de acordo com o processo de gerenciamento de alterações do fornecedor.

6.7 Notificações de alertas de segurança

Os alertas de segurança ajudam a reduzir os riscos relacionados a vulnerabilidades conhecidas. O alerta de segurança pode se referir ao banco de dados CVE (Vulnerabilidades e exposições comuns) oficial ou a outros relatórios sobre vulnerabilidades e inclui descrição da vulnerabilidade, avaliação de risco, recomendações e informações sobre quando uma versão do serviço estará disponível. A maioria dos fornecedores implementa um modelo de vendas indiretas e tem um programa de parceria em vigor.

As Notificações de alertas de segurança permitem que os clientes que não estejam registrados em um programa de parceiro do fabricante obtenham notificações de segurança cibernética relevantes de maneira oportuna assim que elas forem comunicadas ao canal. Essa é uma ferramenta vital para usuários finais que tenham equipamentos instalados, mas que não tenham um contrato com a empresa que realizou a instalação originalmente.

6.8 BSIMM (Building Security in Maturity Model)

O BSIMM (Modelo de maturidade para construção segura) é um esquema de cálculo de segurança de software definido para ajudar as organizações a compararem sua segurança de software com outras

iniciativas e a descobrirem como está seu desempenho. O BSIMM ajuda a avaliar processos, atividades, funções e responsabilidades nos seguintes quesitos:

- Análises do desenho e da arquitetura
- Análises de códigos
- Testes de vulnerabilidades conhecidas
- Execução de uma ferramenta padrão de verificação de vulnerabilidades que possa identificar vulnerabilidades CVE em pacotes de código aberto

6.9 LTS (Suporte de longo prazo)

O LTS é uma política de gerenciamento do ciclo de vida de um produto em que uma versão estável do software é mantida por um período de tempo mais longo do que a edição padrão. O firmware de Suporte de longo prazo deve incluir apenas patches de estabilidade, desempenho e segurança. Os fornecedores oferecem LTS para firmware por até 10 anos a partir do lançamento de um dispositivo no mercado.

Espera-se que o LTS exista paralelamente, porém de forma independente, ao suporte de software ativo existente. Um dos principais benefícios do LTS é que, quando comparado à versão original do firmware, ele manterá a integração com outros fornecedores.

6.10 Aprendizagem e colaboração

Entre as principais áreas a serem consideradas ao selecionar um fornecedor de tecnologia estão o treinamento e o suporte oferecidos por ele. À medida que os desafios enfrentados pelo canal e pelo setor evoluem, especialmente no que diz respeito à segurança cibernética, os fabricantes devem buscar abordar proativamente esses pontos e fornecer garantias e conteúdo para o mercado. Os exemplos potenciais incluem:

- Cursos presenciais gratuitos sobre segurança cibernética
- Treinamento on-line em segurança cibernética
- Teste rápido on-line da segurança cibernética
- Guia para aumento do nível de proteção
- Políticas relativas a vulnerabilidades
- Melhores práticas de segurança cibernética
- Conceitos e terminologia relacionados à segurança cibernética

7 Como criar um perfil de higiene cibernética: próximos passos e considerações

Uma boa higiene cibernética envolve identificar, priorizar e responder aos riscos a que estão sujeitos os principais serviços e produtos da organização. A implementação das melhores práticas de segurança cibernética ajuda a evitar violações de dados e configurações incorretas dos sistemas, além de minimizar os riscos associados aos negócios. Também é importante definir junto às partes interessadas quais são as

principais áreas de ameaças, para que o foco seja voltado para os principais objetivos de gerenciamento de riscos.

Embora esta não seja uma lista completa, as considerações a seguir ajudarão a melhorar a eficiência no tratamento das ameaças cibernéticas.

7.1 Fornecedores

Verifique os registros e certificações

Analise os registros e certificações adequados: por exemplo, solicite evidências do registro ISO 9000 e de outras certificações de qualidade. Determine se os produtos do fornecedor foram projetados para uso em redes corporativas.

Busque evidências da aplicação de práticas recomendadas

Certifique-se de que o fornecedor selecionado possa demonstrar a implementação das práticas recomendadas de segurança cibernética. Ele deve oferecer um guia para aumentar o nível de proteção cibernética, que deve descrever as medidas de segurança física e cibernética e as práticas recomendadas para ajudar a proteger a rede.

Audite o seu fornecedor

Conduza uma auditoria minuciosa antes de se comprometer com a aquisição. Verifique os termos do negócio para garantir que sejam claros e que haja transparência. Do ponto de vista financeiro, é importante averiguar o que aconteceria com o produto e o suporte caso a empresa enfrente problemas.

Determine os recursos para um suporte contínuo

Garanta que seu fornecedor tenha os recursos necessários para continuar a criar as soluções que você prevê que precisará no futuro. Um fornecedor deve ter as dimensões, o alcance e a capacidade para apoiar os requisitos da sua empresa no futuro.

Defina as necessidades futuras da empresa

Concentre-se nas suas necessidades para o futuro. Dispositivos e soluções inteligentes devem ter os recursos necessários para aprimorar e preparar uma empresa para o futuro, portanto, você deve ter a confiança de que o seu fornecedor suprirá ou superará suas expectativas, com contratos de manutenção e suporte contínuo.

Procure verificar as práticas empresariais éticas

Verifique se há evidências de práticas éticas e sustentáveis. Uma parceria construída sobre confiança e objetivos comuns é uma base poderosa para a longevidade. O fornecedor tem sistemas de gestão ambiental, um programa de CSR (Responsabilidade social corporativa) ou uma política de fornecimento ético?

7.2 Produtos e sistemas

Pratique a devida diligência

Realize a devida diligência técnica no sistema e em seus principais elementos, para garantir que ele agregue valor e que não haja fatores subjacentes que possam afetar a operação em andamento. Certifique-se de que as informações sobre avaliações e atenuação de riscos sejam claras e estejam disponíveis.

Verifique o contrato de manutenção

Verifique o que está incluído no contrato de serviço e manutenção, como atualizações de software e firmware do fabricante.

Proteja os dispositivos conectados

Garanta que seu sistema de segurança física conectado à rede seja seguro. Os sistemas de segurança devem ser implantados levando em consideração a segurança cibernética: altere nomes de usuário e senhas padrão, instale o firmware mais recente, utilize criptografia (idealmente HTTPS) e desabilite o acesso remoto.

Solicite uma declaração de segurança do design

O seu fornecedor deve ser capaz de fornecer uma declaração de segurança do design como prova do status da segurança cibernética de todos os dispositivos conectados à rede.

Avalie a inteligência do sistema

Dispositivos conectados totalmente inteligentes são aqueles que estão em rede com um endereço MAC e que fazem parte da arquitetura do sistema intrinsecamente. Dispositivos sem endereço MAC não são inteligentes e não podem ser identificados, gerenciados ou protegidos individualmente.

Avalie a conformidade com a LGPD/Lei de Proteção de Dados

A LGPD (Lei Geral de Proteção de Dados) entrou em vigor em 2018, juntamente com a atualização da Lei de Proteção de Dados de 1998. Certifique-se de que os produtos e sistemas estejam em conformidade com a Lei de Proteção de Dados de 2018 e com a LGPD.

T10168631/PT/M3.2/2108

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções de rede capazes de fornecer percepções para melhorar a segurança e novas maneiras de fazer negócios. Como líder do setor em vídeo em rede, a Axis oferece produtos e serviços de para sistemas de vigilância e análise de vídeo, controle de acesso, intercomunicação e áudio. A Axis conta com mais de 3.800 funcionários dedicados em mais de 50 países e colabora com parceiros em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e sua sede é em Lund, Suécia.

Para obter mais informações sobre a Axis, visite nosso site *axis.com*.