WHITE PAPER

Medidas avançadas de segurança para controle de acesso físico

Genetec™

genetec.com/br

Resumo

Um dos primeiros sistemas instalados para proteger uma organização é o sistema de controle de acesso, que controla entrada e saída de uma ou mais instalações.

Além de instalar leitores, implantar controladores de porta, configurar software e emitir credenciais, as organizações têm várias ferramentas potenciais à sua disposição para proteger seus funcionários e ativos. Escrito como um guia de práticas recomendadas para controle de acesso físico, este white paper primeiro oferece um resumo das ferramentas básicas de ACS e, em seguida, aprofunda as medidas avançadas de segurança física e como podem ser usadas para aumentar significativamente a segurança.

Segurança física - introdução aos sistemas de controle de acesso

O Controle de Acesso Físico trata da proteção de pessoas e ativos. O foco principal é manter uma determinada área segura, restringindo o acesso a pessoal não autorizado. Um sistema eletrônico de controle de acesso (ACS) controla a entrada e saída de salas ou instalações usando uma ampla variedade de credenciais. As credenciais podem se referir a objetos tangíveis ou intangíveis que comprovam a identidade de um indivíduo, como uma senha (algo que ele conhece), um crachá de controle de acesso (algo que ele possui) ou um recurso biométrico (algo que ele é). Com base nas credenciais apresentadas, um ACS determina quem tem permissão e onde e quando podem entrar. Basicamente, uma vez verificadas as credenciais e o ACS concede acesso ao portador do cartão autorizado, um ponto de controle de acesso – que pode ser uma porta, catraca ou outra barreira física onde o acesso é controlado eletronicamente – é desbloqueado e a movimentação é registrada pelo sistema. Além disso, o sistema também monitora as portas e envia alarmes, como quando uma porta é forçada ou mantida aberta por muito tempo após ter sido destravada.

Como implantar leitores e controladores

Usado para controlar a entrada e saída, o leitor e o controlador inteligente – chamado de 'controlador de porta' – são dois componentes básicos de qualquer ACS. Sendo um elemento integral de qualquer ponto de controle de acesso, o leitor obtém informações de credenciais e transmite esses dados ao controlador que hospeda todas as funcionalidades de segurança para tomar decisões de acesso. Um controlador é frequentemente conectado a um ou mais leitores (uma ou mais portas).

Emissão de credenciais

As credenciais são confirmações de identidade e vitais para gerenciar quem tem acesso a uma sala ou instalação. Um ACS usa credenciais para identificar quem está solicitando acesso por meio de um ponto de acesso protegido. Para que o controle de acesso seja operacional, todo portador de cartão deve possuir pelo menos uma credencial, que normalmente (mas não exclusivamente) é um cartão de controle de acesso. Algumas das formas comuns para credenciais são cartões e crachás, cartões com circuitos integrados, chaves codificadas, adesivos/tokens e chips integrados.

Definindo os direitos de acesso do portador de cartão

Na qualidade de 'quem' em qualquer sistema de controle de acesso, um portador de cartão representa uma pessoa que pode entrar e sair de áreas seguras em virtude de suas credenciais e cujas atividades podem ser rastreadas. Geralmente, é melhor implementar alguma forma de controle

de acesso baseado em função. Ao mapear áreas acessíveis e horários válidos – por exemplo, períodos de tempo durante um dia ou uma semana – uma organização pode usar seu ACS para controlar quem pode entrar onde e quando, atribuindo portadores de cartão a grupos de portador de cartão e, em seguida, concedendo privilégios de acesso a esses determinados grupos.

Além disso, um ACS eficaz e seguro deve ter

- solicitação formal e etapas de aprovação,
- capacidade de manter registros para rastrear quem está fazendo cada solicitação, para quem é a solicitação, as áreas de controle de acesso envolvidas e quem está realmente fornecendo o acesso, e
- logs de aprovação e recusa de solicitações de acesso, incluindo quem aprovou ou recusou.

Emissão de crachás impressos para identificar visualmente os portadores de cartão

Para permitir que a equipe de segurança identifique visualmente os portadores de cartão e adicione uma camada adicional de segurança, algumas organizações emitem crachás impressos que funcionam como crachás de identificação com a foto do portador do cartão impressa no crachá. Os crachás de identificação com foto impressa também permitem que o portador comum de cartão relate o uso indevido de credenciais simplesmente olhando para o crachá de identificação do portador de cartão.

Monitoramento e supervisão ACS

Por fim, um ACS básico deve supervisionar uma variedade de registros e dispositivos, incluindo portas e leitores individuais, e fornecer notificações ao pessoal de segurança sobre eventos e alarmes significativos, incluindo

- entrada bem-sucedida do portador de cartão em qualquer área,
- tentativas de entrada malsucedidas, que devem ser investigadas para determinar se algum intruso tentou obter acesso,
- uma atividade impossível, como alguém estar em dois lugares ao mesmo tempo porque é uma maneira eficaz de identificar um cartão clonado,
- a adulteração ou remoção de leitores de cartão, e
- o mau funcionamento de qualquer dispositivo no sistema.

No entanto, um ACS pode proteger efetivamente uma organização somente se o pessoal de segurança estiver monitorando continuamente o status do sistema ou for notificado em tempo real sobre quaisquer violações.

Visitor Management para gerenciar visitantes em vez de uma ficha de entrada

Em vez de depender de fichas tradicionais de registro de visitantes ou livros de registro, um número crescente de organizações aproveita seu ACS para gerenciamento eletrônico de visitantes ou implanta um sistema de gerenciamento de visitantes de terceiros para registrar e rastrear visitantes. Com um sistema eletrônico de gerenciamento de visitantes, o visitante recebe permissão de acesso através de uma workstation e um crachá de visitante temporário que é impresso e entregue ao visitante. Os principais benefícios de usar um módulo de gerenciamento de visitantes ou um sistema dedicado incluem

- o registro preciso e consistente das informações do visitante,
- a capacidade de imprimir rapidamente um crachá de visitante personalizado que contém a foto do visitante,
- a atribuição de uma credencial a um visitante e direitos de acesso associados a uma instalação,
- a capacidade de criar rapidamente relatórios da atividade do visitante, pois todas as informações do visitante são armazenadas em um banco de dados e
- a possibilidade de pré-cadastrar os visitantes no sistema e agilizar o processo de liberação na chegada.

Medidas avançadas de controle de acesso

A seguir, as medidas de segurança mais avançadas que uma organização pode implementar para proteger ou restringir ainda mais o acesso às suas instalações. Ao implantar cada medida por conta própria, uma organização pode incrementar seu nível geral de segurança. Mas, quando várias medidas são implantadas simultaneamente, a segurança pode ser aumentada de forma exponencial.

É importante ter em mente que nem todas as soluções ACS suportam essas medidas de segurança avançadas. Consequentemente, ao tentar determinar a melhor solução ACS para uma organização, é importante determinar qual ACS oferece suporte a medidas de segurança específicas.

Botões de emergência/coação e alarmes de pânico

Botões de emergência/coação ou alarmes de pânico permitem que funcionários sob coação peçam ajuda de forma silenciosa, rápida e conveniente sem chamar a atenção para si mesmos. Como esses alarmes são silenciosos, são ideais em situações em que os funcionários acreditam que não seria seguro usar meios de comunicação mais convencionais – como um telefone – por medo de potencializar uma situação já perigosa. A maioria das organizações pode se beneficiar de botões de coação que são implantados estrategicamente em uma instalação para acionar alarmes em situações de ameaça.

Esses alarmes geralmente consistem em dois componentes, o botão de pânico e o sistema de comunicação. Instalado em locais de fácil acesso, mas escondido do observador casual, o botão é um dispositivo com ou sem fio que a pessoa ativa quando precisa de ajuda. O sistema de comunicação refere-se à maneira como a ajuda é chamada quando um botão de pânico é ativado e pode envolver o ACS se comunicando com um centro de monitoramento de alarme externo, um centro de comando de segurança, um aplicativo de celular ou com pessoal não relacionado à segurança.

Gerenciamento de portas sem leitor

As portas sem leitor fornecem supervisão adicional, permitindo que uma organização monitore portas equipadas apenas com sensores e travas. Usando essa medida de segurança, uma organização também pode automatizar quando uma porta será aberta e fechada, independentemente da presença de um leitor de controle de acesso e sem a necessidade de hardware externo, como temporizadores. Aplicações típicas para essa medida de segurança podem ser encontradas em escolas, lojas de departamento ou shopping centers com programações de desbloqueio automatizado.

Ao implantar esse tipo de configuração de porta, uma organização pode

programar horários de desbloqueio - que determinam quando uma porta deve ser desbloqueada automaticamente - e exceções para programações de desbloqueio de uma porta sem leitor. Além disso, também é possível que o ACS monitore, registre a atividade da porta e monitore os padrões de uso.

Para gerenciar uma porta sem leitor como parte de um ACS, a porta precisa estar equipada com um ou mais dos seguintes itens: uma trava, um botão ou sensor REX (solicitação para sair) e um contato de porta (detecta quando uma porta está aberta ou fechada). Em seguida, o ACS pode usar as entradas e saídas de um módulo IO (entrada/saída) padrão para monitorar e controlar o comportamento da porta, incluindo agendamentos de desbloqueio.

Antipassback—soft (suave) e hard (rígido)

O taillgating, um risco de segurança comum no ACS, ocorre quando um indivíduo simplesmente segue e entra junto com um portador de cartão autorizado – que está ciente do fato ou não – através de um ponto de acesso. Embora um ACS possa controlar qual portador de cartão tem acesso, ele não consegue, uma vez que o portador do cartão abre uma porta, controlar quantas pessoas entram pela porta atrás do portador de cartão.

Embora seja possível reduzir o uso não autorizado por meio de treinamento para conscientização de segurança do portador de cartão, o problema geralmente só pode ser resolvido de forma confiável por meio do uso de dispositivos especiais antifurto, por exemplo, catracas e portas giratórias, que permitem que apenas uma pessoa entre ou saia de uma área de cada vez. Essas medidas de segurança usam uma barreira física que permite a passagem de apenas uma pessoa por vez, ou usam sensores que detectam quando uma pessoa está tentando fazer tailgate ou quando mais de uma pessoa tenta entrar usando a mesma credencial.

A medida de segurança antipassback evita o uso indevido de um ACS estabelecendo uma sequência específica na qual as credenciais devem ser usadas
para que o sistema libere o acesso aos funcionários. Essa medida é ideal para proteger uma organização contra o uso de cartões duplicados, pois um ACS com essa medida de segurança recusará o acesso a um portador de cartão que já esteja dentro da instalação.

Comumente usado em entradas de funcionários com leitores de cartão instalados tanto
dentro como fora do ponto de acesso, esta medida de segurança exige que os funcionários passem o cartão para entrar em uma área e novamente ao sair
da mesma área. Ao garantir que cada uso de um cartão no leitor 'in' corresponda
a um uso no leitor 'out' antes que o cartão possa ser usado no leitor 'in' novamente, um ACS usa antipassback para certificar-se de que um portador de cartão só consiga
sair de uma zona de acesso em que já entrou e só pode entrar em uma zona de acesso da qual já tenha saído anteriormente. Qualquer tentativa de usar um cartão uma segunda vez para obter acesso sem antes usar o cartão para sair, acionaria uma violação antipassback.

Dois dos tipos mais comuns de antipassback são:

- Soft Antipassback—o ACS permite a reentrada ao portador do cartão, mas registra uma violação de antipassback quando a sequência de uso estabelecida foi violada.
- Hard Antipassback – o ACS restringe a entrada ao portador do cartão e registra uma violação antipassback quando a sequência de uso estabelecida foi violada.

Ao ativar as medidas antipassback, uma organização pode aumentar muito sua segurança eliminando o uso enganoso de cartões e gerando alarmes para cada violação antipassback. Ele também fornece a uma organização uma contagem precisa do número de pessoas em uma determinada zona de acesso.

Antipassback global

Existem dois modos de antipassback, local e global. No modo local, o ACS trabalha apenas para verificar a marcação de saída do portador de cartão em relação a uma área ou instalação local antes de permitir a reentrada;

esta área é normalmente limitada pelas portas controladas por um único controlador de porta inteligente. O antipassback global exige que o ACS verifique as marcações de saída do portador de cartão em todas as áreas e instalações de uma organização antes de permitir a reentrada; com antipassback global, diferentes controladores dentro da mesma instalação ou em várias instalações trocarão informações para que estejam todos atualizados. O antipassback global pode ser uma necessidade fundamental para implantações em vários locais ou no estilo de campus quando uma organização deseja impedir que um cartão clonado seja usado simultaneamente nos locais.

Intertravamentos e portas giratórias

O intertravamento é uma medida de segurança que impede que várias portas sejam abertas a qualquer momento para acessar uma determinada área ou sala. Geralmente visto em ambientes de maior segurança ou restritos, o intertravamento garante que apenas uma única porta seja aberta por vez.

Semelhante a um intertravamento, uma porta giratória também é usada para garantir que apenas uma única porta seja aberta para acessar uma sala. Uma porta giratória consiste em uma passagem com uma porta em cada extremidade; depois de usar suas credenciais para abrir a primeira porta, o portador do cartão entra na passagem, fecha a porta atrás dele, segue para a segunda porta e, em seguida, usa suas credenciais para entrar na sala. Ocasionalmente, portas giratórias serão equipadas com sensores – incluindo feixes eletrônicos, detectores de peso, intercomunicadors e câmeras de vídeo – que detectam o número total de pessoas presentes. Se a porta giratória detecta que há mais de uma pessoa na passagem, um alarme soa e o acesso é negado.

Embora essas medidas de segurança tenham sido tradicionalmente tratadas por meio de controladores lógicos programáveis (PLC) ou dispositivos dedicados, uma organização que implanta um ACS que oferece suporte nativo a recursos de intertravamento e armadilha

- pode aproveitar seu hardware ACS existente,
- pode configurar e monitorar todas as medidas de segurança a partir de uma única solução,
- pode evitar a implantação de equipamentos especializados, como PLCs, e
- pode eliminar a necessidade de estabelecer links entre seus ACS e dispositivos de intertravamento/porta giratória.

Controle de fluxo direcional

Com base no layout ou em preocupações específicas com segurança em uma instalação, uma organização pode querer controlar o fluxo de entrada e saída de uma determinada área ou edifício. Existem várias medidas de segurança que podem ser usadas para obter o controle de fluxo direcional:

- portões de acesso, que permitem que uma organização controle e canalize o fluxo de pessoas para dentro e para fora de uma determinada área ou edifício,
- implantar leitores somente de entrada em um conjunto de portas e leitores somente de saída em outro conjunto de portas, evitando assim que uma porta seja usada para entrada e saída,
- sensores, que detectam quando alguém está se deslocando no contrafluxo pretendido e soam um alarme.

Regras de First-Person-In para impedir a ativação de uma programação de desbloqueio

Para fornecer maiores níveis de segurança e proteção ou para proteger instalações sem vigilância, algumas organizações não querem que as pessoas tenham acesso a determinadas áreas, a menos que um supervisor ou funcionário designado tenha entrado primeiro ou esteja de fato presente no local.

Normalmente implantado em escolas e locais de varejo, a regra de First-Person-In garante que um ponto de acesso configurado para desbloquear obedecendo uma programação, permaneça bloqueado até que um supervisor designado entre na área. A partir de então, o ponto de acesso é desbloqueado de acordo com a programação definida, permitindo a entrada de outros usuários. Por exemplo, usando as regras de First-

Person-In, a entrada principal de um local de varejo que geralmente é desbloqueada durante o horário de funcionamento da loja, permaneceria bloqueada até que o gerente ou outro funcionário estivesse presente.

Regras de First-Person-In com credenciais ACS e direitos de acesso

As Regras de First-Person-In também podem ser usadas para ativar os direitos de acesso padrão do portador de cartão. Nesse caso, os funcionários podem ter acesso a determinadas áreas somente depois que uma pessoa autorizada estiver no local.

Ao habilitar a regra First-Person-In para direitos de acesso, uma organização pode garantir que um ponto de acesso permaneça restrito, impedindo que portadores de cartão autorizados obtenham acesso enquanto uma área estiver sem supervisão. Quando o supervisor está no local, os direitos de acesso padrão são ativados e os portadores de cartão podem usar suas credenciais para transitar em uma área ou instalação.

Regras de duas pessoas para acesso a áreas altamente restritas

O acesso a certas áreas altamente confidenciais que contêm ativos valiosos, incluindo salas de servidores, cofres e áreas com dados confidenciais tais como propriedade intelectual, não deveria ser permitido a um indivíduo sozinho. Para proteger esses ativos, uma organização pode aplicar regras de acesso com duas pessoas a essas áreas. Quando implementada, essa regra de segurança garante que a entrada em uma área restrita seja permitida apenas quando dois funcionários autorizados usarem suas credenciais em conjunto.

Um ponto de acesso configurado de acordo com a regra de duas pessoas funciona da seguinte forma: Dois portadores de cartão autorizados devem passar suas credenciais de acesso no leitor de cartão dentro de um tempo especificado. Uma vez que o acesso é concedido, a porta é destravada e os indivíduos são solicitados a entrar e fechar a porta.

Em alguns sistemas, após a entrada de duas pessoas autorizadas na área segura, outras pessoas também podem entrar, mas ainda assim devem validar sua entrada. Muitos sistemas de controle de acesso monitoram o número de pessoas na área segura e exibem o total de ocupação. Idealmente, as regras de duas pessoas devem ser flexíveis o suficiente para que possam ser habilitadas em pontos de entrada, pontos de saída ou ambos.

Acompanhamento a visitantes

As necessidades de uma organização em relação ao gerenciamento de visitantes variam de acordo com o nível de segurança exigido. Enquanto muitas organizações emitem credenciais de papel para identificar visualmente um visitante, outras emitem credenciais de trabalho para visitantes com acesso sem acompanhamento.

No caso de requisitos de segurança elevados, algumas organizações emitem credenciais funcionais e atribuem direitos de acesso limitados, mas ainda exigem acesso com acompanhamento a várias áreas. Se um ACS oferecer suporte ao modo Acompanhamento a Visitantes, um visitante poderá usar suas credenciais para obter acesso a uma área, mas somente quando seu acompanhante — um funcionário — obtiver acesso ao mesmo tempo. Funcionando de maneira semelhante às regras de duas pessoas, isso garante que os visitantes nunca estejam desacompanhados ao entrar em determinadas áreas e também garante que seus movimentos e os movimentos de seus acompanhantes sejam rastreados em todos os momentos.

Autorizações de segurança e gerenciamento de nível de ameaça

Para responder eficazmente a uma gama crescente de ameaças potenciais, uma equipe de segurança pode precisar bloquear uma instalação a qualquer momento, restringir o acesso a áreas afetadas, ou impedir que um intruso ganhe acesso a pessoas ou ativos críticos. Para atingir este nível de preparação, uma organização deve ter as ferramentas e recursos para alterar o status de seu sistema de segurança em tempo real e em resposta a tipos específicos de ameaças. Alguns fornecedores estão abordando essa necessidade oferecendo o que é conhecido no setor de segurança como Gerenciamento de Nível de Ameaças.

Usando o Gerenciamento de Nível de Ameaças, uma organização pode bloquear automaticamente uma sala, uma área ou um prédio simplesmente acionando um nível de ameaça específico e predefinido. A ativação do nível de ameaça correto geralmente será baseada no tipo e gravidade da ameaça identificada. Um nível de ameaça pode ser criado para restringir o acesso a todos, incluindo portadores de cartão autorizados, mas ainda permitir o acesso à equipe de segurança ou agentes da lei. Isso funciona para limitar o movimento do intruso e, ao mesmo tempo, evitar que os portadores de cartão ou visitantes fiquem em perigo. Ao atribuir antecipadamente autorizações de segurança individuais, a alteração nos direitos de acesso pode ser praticamente instantânea, desde que a funcionalidade seja suportada pelo ACS.

Outra funcionalidade importante a ser considerada é se o gerenciamento de ameaças é limitado ao ACS ou se pode ser vinculado a outros sistemas de segurança, como videomonitoramento, comunicações ou sistemas de intrusão. Sistemas mais avançados podem unificar a resposta simultânea de vários sistemas, gerando uma resposta abrangente às ameaças, em oposição a respostas fragmentadas ou sistema a sistema.

Autenticação multifator

A autenticação multifator é uma maneira altamente eficaz de garantir que a pessoa que passa seu cartão em um leitor seja a mesma pessoa para quem o cartão foi emitido inicialmente. Essa medida é ideal quando uma organização está preocupada em proteger áreas altamente confidenciais contra acesso não autorizado, inclusive quando alguém usa um cartão de acesso roubado para entrar em áreas restritas.

Essa abordagem aumenta o nível de segurança exigindo que o pessoal use uma combinação dos seguintes fatores:

- algo que eles têm, por exemplo. uma credencial,
- algo que eles sabem, por exemplo. uma senha ou um PIN do teclado,
- algo que eles são, por exemplo. um recurso biométrico como uma impressão digital.

A interação humana também pode ser usada em alguns casos para fornecer o segundo fator, como verificar a identidade do portador de cartão usando câmeras de vídeo antes de desbloquear manualmente uma porta.

Para o nível mais alto de acesso seguro, a autenticação multifator funciona melhor quando três fatores são necessários, mas implementar apenas um fator adicional em um sistema básico também pode ser eficaz. Uma senha ou PIN é um segundo fator de autenticação relativamente barato que pode ser implementado usando leitores de cartão com teclados integrados. Além de minimizar a ameaça de clonagem de cartão, os leitores com teclado integrado minimizam a probabilidade de que um cartão perdido possa ser achado por alguém e simplesmente usado para entrar em uma instalação. Avançando mais um passo, os leitores biométricos garantem que a pessoa que passa o cartão é realmente a mesma pessoa para quem o cartão foi emitido.

Segurança-da-Segurança

Segurança-da-Segurança é um conceito mais recente que é de grande interesse tanto para o departamento de segurança física quanto para o departamento de TI. Segurança-da-Segurança na verdade se refere à acessibilidade geral e segurança da própria plataforma ACS: como o acesso do administrador e do operador (usuários) é autenticado, o que os usuários estão autorizados a fazer e como os dados armazenados e transmitidos são protegidos e mantidos privados. Uma vulnerabilidade que muitas vezes passa despercebida quando se fala em segurança de uma plataforma é a criptografia em um ACS. Mesmo que alguns dados do ACS sejam criptografados, o sistema permanece vulnerável quando todo o sistema não aproveita os padrões de criptografia mais recentes. Um ACS verdadeiramente seguro é protegido em todos os níveis, usando dados criptografados e comunicações desde a credencial e leitora até o controlador de porta e software.

Enquanto as tecnologias de cartão e leitor estão se tornando cada vez mais seguras, a maior vulnerabilidade em muitas implantações de ACS é o link entre o leitor e o controlador de porta. Wiegand tem sido o padrão comum para a maioria dos leitores de cartão para controle de acesso desde o início dos anos 80. Leitores baseados em Wiegand

são em grande parte dispositivos não supervisionados, e assim podem ser comprometidos sem que o pessoal de segurança saiba. Os leitores podem ser vandalizados, apresentar defeitos ou até roubados sem notificação ao administrador do sistema. Por isso que nunca é recomendado equipar portas de perímetro com leitores Wiegand porque a organização está expondo a integridade de suas instalações com um protocolo direcional não criptografado.

Com o Open Supervisioned Device Protocol (OSDP) Secure (V2), a criptografia é um padrão, não uma opção. Usando um protocolo de comunicação bidirecional, um leitor OSDP é supervisionado, o que significa que, se o leitor for adulterado, o administrador do sistema de segurança será notificado para que uma ação possa ser tomada. Uma das formas de criptografia utilizadas no OSPD é a criptografia AES-128 bits, que criptografa e descriptografa dados em blocos de 128 bits usando chaves criptográficas evitando ataques man-in-the-middle.

Cartões inteligentes e leitores

Uma organização pode implantar cartões inteligentes e leitores que oferecem recursos de segurança adicionais e ajudam a evitar o uso indevido ou a reprodução ilegal de credenciais. Credenciais ACS tradicionais, por exemplo. os cartões de aproximação ou prox, inventados na década de 1980, ainda são amplamente utilizados, mas oferecem pouco em termos de segurança contra um número crescente de ataques. Eles usam uma faixa de frequência muito limitada, não têm os recursos de segurança adicionais das tecnologias de cartão inteligente mais avançadas e não transmitem seus dados em um formato criptografado, tornando-o mais suscetível a sniffing e clonagem de cartão.

Com um microprocessador embutido, aplicativos e recursos de segurança adicionais, um cartão inteligente é como ter um computador em miniatura em um cartão. A tecnologia de cartão inteligente sem contato ou com contato oferece a uma organização o mais alto nível de segurança e interoperabilidade por meio de mecanismos de autenticação mútua e proteção criptográfica com chaves secretas. Por exemplo, os dados de controle de acesso em um cartão sem contato podem ser protegidos usando chaves de segurança diversificadas de 64 bits com base em um

número de série exclusivo do cartão. Essa segurança pode ser customizada pelo usuário final com um programador de cartão. Além disso, os cartões inteligentes, devido à sua extensa capacidade de memória e capacidade de armazenar com segurança qualquer tipo de informação, podem servir como credenciais de vários aplicativos que também podem incluir dados biométricos e muito mais.

Formatos de cartão personalizados

Uma credencial de acesso ou cartão armazena dados e a estrutura dos dados binários armazenados no cartão é conhecida como formato de cartão. Historicamente, as organizações implantavam credenciais com formatos de cartão que eram de propriedade do fabricante do cartão ou leitor, do fornecedor do ACS ou do integrador de sistemas. Na maioria dos casos, o formato não era específico para o usuário final e provavelmente era compartilhado por muitos, e alguns formatos de cartão são tão amplamente usados que seu formato e descrição específicos estão disponíveis publicamente.

Com formatos de cartão customizados, uma organização tem a opção de definir seu próprio formato de cartão em vez de implantar formatos padrão ou conhecidos, como o formato padrão de 26 bits. Formatos de cartões customizados podem ser encontrados tanto com credenciais básicas de proximidade quanto com cartões inteligentes, com o último oferecendo muito mais flexibilidade e segurança. Cartões inteligentes com números de credenciais que utilizam algoritmos de criptografia avançados, chaves de criptografia definidas pelo usuário final e números de cartão estendidos oferecem mais segurança do que jamais antes.

Na verdade, o uso de cartões com numeração personalizada e um formato de cartão maior que o número padrão de 26 bits, como formatos de 256 bits, pode adicionar outra camada de segurança. Cartões personalizados também podem fornecer provisões adicionais para a não duplicação de números de cartão, e alguns leitores de fabricantes podem ser configurados para ignorar cartões que não estejam em total conformidade com o formato apropriado. Mas é importante que uma organização verifique se seu hardware e software de controle de acesso têm a capacidade de gerenciar formatos de cartão personalizados ou fora do padrão.

Microsoft Active Directory ou integração LDAP

Essa medida de controle de acesso avançado envolve a integração do ACS de uma organização com seu servidor Microsoft (MS) Active Directory (AD) ou com um servidor de diretório de TI.

MS Active Directory é o serviço de diretório que a Microsoft desenvolveu para redes de domínio do Windows. Incluído na maioria dos sistemas operacionais Windows Server, o MS Active Directory emprega um controlador de domínio AD para autenticar e autorizar todos os usuários e computadores em uma rede do tipo domínio Windows. Os sistemas avançados de controle de acesso podem se conectar automaticamente ao AD e habilitar sincronizações automatizadas do servidor AD. Os dados inseridos no AD podem ser usados pelo ACS, evitando a entrada duplicada de dados e garantindo que o ACS esteja sempre atualizado, o que garante que o acesso físico reflita o status atual do funcionário.

A integração do AD permite que uma organização vincule grupos de segurança do Windows a grupos de portadores de cartão ACS, levando a um gerenciamento de controle de acesso mais eficiente. Não apenas as contas são criadas ou desativadas automaticamente com base nas sincronizações do servidor AD, mas os portadores de cartão podem receber automaticamente seus direitos de acesso físico a toda a instalação. Como resultado, qualquer alteração em um grupo de segurança do Windows leva a alterações automáticas nos grupos de portadores de cartão e seus direitos de acesso. Isso garante que o ACS seja atualizado em tempo real e de forma precisa.

A integração do ACS com o Active Directory facilita a propagação imediata de quaisquer alterações, economizando tempo e reduzindo ocorrências de erro humano, pois a equipe de TI e segurança não precisa criar ou excluir manualmente o portador de cartão em diferentes sistemas. Outro benefício é a eliminação das lacunas de tempo antes que o acesso físico seja revogado após uma mudança no AD.

Notificação do operador e revisão remota

Notificação do operador

Um ACS pode proteger efetivamente uma organização somente se o pessoal de segurança for notificado sobre adulterações e eventos críticos de maneira eficiente e a tempo. Portanto, além de implantar medidas físicas para evitar violações de segurança, também é importante que uma organização considere como as equipes de segurança e os operadores são notificados quando ocorrem exceções às regras de controle de acesso estabelecidas ou quando surgem ameaças.

As equipes de segurança e os operadores devem ser notificados instantaneamente em caso de eventos críticos e emergências que justifiquem uma resposta. Embora não seja uma lista totalmente abrangente, alguns dos eventos mais críticos que requerem resposta imediata incluem o seguinte:

- Alarmes de alta prioridade
- Nível de ameaça acionado
- Abertura Forçada de Porta
- Acesso Negado
- Violação de antipassback
- Porta aberta por tempo excessivo
- Tamper de hardware (leitor ou controlador)
- Unidade, controlador ou leitor offline
- Estação manual ativada

As notificações podem assumir muitas formas. Alguns exemplos de notificações
automáticas incluem:

- Alarme sonoro e/ou visual na aplicação de monitoramento
- Mudança de cor na tela do operador
- Mensagem de texto ou pop-up na aplicação de monitoramento
- Mensagem de texto SMS enviada para um telefone celular
- Envio de notificação por push para um aplicativo em um smartphone ou tablet
- E-mail com anexos

Acessibilidade remota para revisão

Um ACS que oferece suporte a acesso remoto permite que os operadores monitorem e gerenciem o ACS de qualquer lugar, independentemente de sua localização. Eles não apenas podem receber alarmes ou ver a mudança de estado do sistema de segurança, mas também podem agir e responder a ameaças. Dois recursos importantes que devem fazer parte de qualquer ACS para gerenciamento remoto são o suporte a um Cliente Web e o acesso a uma variedade de Aplicativos para Smartphone.

Além do controle de acesso – como unificação com sistemas de terceiros podem aumentar a segurança física

Ao implementar um ACS baseado em protocolo de Internet (IP), uma organização pode operar, expandir e customizar mais facilmente sua infraestrutura de controle de acesso físico. Além de poder incorporar as medidas de segurança avançadas mencionadas acima, uma organização também pode aproveitar a tecnologia IP para

- padronizar sua infraestrutura de controle de acesso,
- reduzir o número de pontos de falha e simplificar o monitoramento e o gerenciamento do sistema, mudando a inteligência (de decisão) para a porta e
- obter economias significativas no Custo Total de Propriedade (TCO) por meio da simplificação da futura expansão e modificação da infraestrutura.

Um IP ACS de arquitetura aberta também deve ser unificado com vários sistemas de segurança de terceiros, incluindo videomonitoramento, comunicações e intrusão, para fornecer maior consciência situacional e níveis mais elevados de segurança.

Unificação com vídeo

A unificação do ACS com um sistema de gerenciamento de vídeo (VMS) forneceria aos operadores de segurança mais informações – informações visuais na forma de vídeo correlacionado – para avaliar situações presentes e passadas. A unificação com vídeo forneceria monitoramento ao vivo do acesso e possibilitaria aos operadores validar a imagem do portador de cartão em relação ao vídeo ao vivo ou gravado.

A notificação do operador e a revisão remota em um ACS também se tornam mais eficazes por meio da unificação com vídeo. Como resultado, um operador terá instantaneamente mais informações sobre um evento crítico, incluindo abertura forçada de uma porta ou adulteração, e poderá tomar decisões mais informadas. Por exemplo, após receber uma notificação, um operador pode monitorar imediatamente as câmeras de vídeo no sistema e visualizar a cena. Isso pode ser um fator chave para ajudar os operadores de segurança a identificar falsos positivos e responder em tempo hábil.

Unificação com comunicações

A unificação de um ACS baseado em IP com um sistema avançado de comunicação de terceiros aumenta a segurança e a eficiência ao simplificar a forma como uma organização responde às solicitações diárias de ACS, incluindo chamadas de emergência e cartões perdidos, como gerencia ameaças e como responde a violações de segurança. Por exemplo, a unificação do ACS e das comunicações permitiria que uma organização incluísse outra camada de segurança às suas operações, adicionando comunicações de intercomunicação dentro de um ambiente de alta

segurança, permitindo assim que os operadores de segurança concedam ou neguem acesso a salas ou áreas altamente seguras, validando áudio e as informações de controle acesso ao mesmo tempo.

E, unificando ainda mais o ACS e as comunicações avançadas com vídeo, uma organização possibilitaria que os operadores atendessem chamadas de emergência recebidas, assistissem vídeos ao vivo ao mesmo tempo em que respondem e tomam as ações corretas para lidar com situações, como ativar ou não os níveis de ameaça — à medida que analisam as informações visuais à mão. Isso também agilizaria a forma como os operadores respondem às solicitações referentes a cartões perdidos pelos funcionários. Como as estações de chamada de intercomunicação seriam vinculadas a portas e câmeras de vídeo com controle de acesso, os operadores poderiam aceitar chamadas recebidas, confirmar a identidade de quem está chamando por meio de vídeo ao vivo e o perfil do portador de cartão e conceder acesso rapidamente a partir de uma única aplicação de segurança unificada.

Unificação com monitoramento de invasão

Outra forma de proteger recursos e ativos é por meio da unificação do ACS com um sistema de monitoramento de intrusão. Devido às valiosas informações encaminhadas pelo sistema de intrusão, os operadores de segurança podem tomar decisões com base em uma compreensão mais abrangente da situação que se apresenta. Essa unificação também permitiria o monitoramento em tempo real do status dos painéis de alarme (se armado, desarmado ou em alarme) e opções de armamento mais avançadas, como configurar ações automatizadas para armar com base no tempo ou nos eventos do sistema.

Visão geral do Synergis e das medidas de segurança que oferece

O Sistema de Controle de Acesso IP Synergis™ da Genetec™ é a solução ACS ideal para qualquer organização que queira aumentar a segurança e proteção de seu pessoal e instalações.

O sistema Synergis é uma solução completa com design de crachá integrado, gerenciamento de portadores de cartão e visitantes, assim como relatórios avançados que permitem que uma organização atenda de forma eficaz e eficiente às suas necessidades diárias de segurança. E o Synergis também oferece as medidas de segurança avançadas necessárias para proteger pessoas e ativos durante situações críticas, incluindo

- Gerenciamento de nível de ameaça
  - › Escolher rapidamente a resposta certa para ameaças percebidas e restringir o acesso por meio de níveis de ameaça pré-criados com base nas políticas de segurança da organização.
- Criptografia de ponta a ponta
  - › Garanta que as comunicações sejam protegidas entre aplicativos cliente, aplicativos de servidor e controladores de porta com criptografia habilitada por meio do Synergis.
- Integração do Microsoft Active Directory
  - › Simplifique o gerenciamento de usuários e portadores de cartão com sincronizações automatizadas entre o diretório de TI e o Synergis e garanta que os direitos de acesso de usuários e portadores de cartão ao Synergis ACS estejam atualizados.
- Gestão Global de Portador de Cartão
  - › Implante sistemas Synergis independentes que sincronizam os portadores de cartão e credenciais automaticamente entre locais, um recurso que permite que organizações maiores emitam um cartão para todos os sites e usem antipassback global para proteger ainda mais seus sites.
- Recursos adicionais incluem suporte para cartões inteligentes e leitores, formatos de cartão customizados, regras de duas pessoas e First-Person-In e muito mais.

Juntamente com o sistema Synergis, uma organização também pode implantar a plataforma unificada Genetec Security Center para consolidar e executar todas as suas atividades de segurança, incluindo controle de acesso, vídeo, intercomunicador e sistemas de intrusão, a partir de um único aplicativo. Ao unificar o Synergis com sistemas de videomonitoramento, intercomunicador, gerenciamento de ativos e sistemas de intrusão, uma organização pode tomar decisões de segurança mais claras e oportunas com base em mais informações quando comparado aos sistemas tradicionais de controle de acesso autônomos.

Tabela com lista de medidas de segurança, quando usá-las, prós e contras

A tabela abaixo resume as medidas de segurança apresentadas neste white paper e fornece orientação sobre quando cada medida é melhor usada, juntamente com algumas vantagens e possíveis desvantagens da medida de segurança.

Medida de segurança	Visão geral	Quando usar	Prós	Contras
Botões de Emergência/ Coação e Alarmes de Pânico	Capacida os funcionários a pedir ajuda de forma silenciosa e rápida	Quando os funcionários acreditam que não seria seguro usar meios mais convencionais de comunicação	Peça ajuda sem potencializar uma situação já perigosa	Esses dispositivos não funcionam proativamente para evitar emergências ou situações perigosas
Gerenciamento de portas sem leitor	Permite o monitoramento de portas equipadas apenas com sensores e fechaduras	Instalações com horários de desbloqueio automatizados, como escolas ou lojas de varejo	Automatize quando uma porta será aberta e fechada sem a necessidade de hardware externo ou leitor de controle de acesso	Liberar portas em resposta a eventos não programados pode ser difícil se não for apoiado pelo ACS
Antipassback soft	Os eventos antipassback são registrados, mas o acesso é concedido	Necessidade de identificação quando os portadores de cartão não estão usando suas credenciais para acessar uma instalação de acordo com a política da empresa	Identifique instantaneamente o uso indevido de credenciais Não intrusivo, pois os portadores de cartão não são impedidos de obter acesso	Difícil para alterar comportamento porque não impede o acesso

Medida de segurança	Visão geral	Quando usar	Prós	Contras
Antipassback hard	Os eventos antipassback são registrados e o acesso é negado	Necessidade de identificação quando os portadores de cartão não estão usando suas credenciais para acessar uma instalação de acordo com a política da empresa	Identifique instantaneamente o uso indevido de credenciais Ajuda a alterar o comportamento do portador de cartão	Pode ser um transtorno para os portadores de cartão de cartão porque impede o acesso
Antipassback global	Os controladores em várias instalações trocam informações para verificar os registros de saída do portador de cartão antes de permitir a reentrada.	Necessidade de identificação interligada em vários sites, como em um campus universitário, quando os portadores de cartão não estão usando suas credenciais para acessar uma instalação de acordo com a política da empresa	Identifique instantaneamente o uso indevido de credenciais em vários sites	Pode ser um transtorno para os portadores de cartão de cartão porque impede o acesso
Intertravamentos e portas giratórias	Impede o tailgating - quando um intruso entra junto ou atrás de uma pessoa autorizada através de um ponto de acesso	Em áreas de grande fluxo, onde a segurança pode ser comprometida por tailgating Quando o acesso a uma área precisa seguir políticas rígidas	Maior segurança controlando o fluxo de pessoas nos pontos de acesso	Pode causar congestionamento ao diminuir o fluxo de indivíduos ao passar por um ponto de acesso
Controle de Fluxo Direcional	Permite o controle do fluxo de entrada e saída de uma determinada área	Para controlar ou canalizar o fluxo de entrada e saída de uma determinada área Para evitar que um mesmo ponto de acesso seja usado como entrada e saída	Maior segurança controlando o fluxo de pessoas nos pontos de acesso	Pode causar transtornos aos portadores de cartão que precisam se deslocar no contrafluxo

Medida de segurança	Visão geral	Quando usar	Prós	Contras
Regras de First-Person-In	Concede acesso a indivíduos ou portadores de cartão apenas quando um supervisor ou funcionário designado entrar primeiro ou estiver presente no local.	Instalações desprotegidas ou sem vigilância com portas com horários programados de liberação, como escolas ou lojas de varejo	Maior nível de segurança, pois o ponto de acesso permanece bloqueado até que o supervisor ou funcionário autorizado esteja no local	Se algo inesperado acontecer com o supervisor ou funcionário autorizado, o ponto de acesso permanece bloqueado, o que pode interferir nas operações comerciais normais
Regras de duas pessoas	Concede acesso a uma área restrita apenas através de credenciais combinadas de duas pessoas autorizadas dentro de um tempo especificado	Ideal para áreas altamente sensíveis que contêm ativos valiosos, incluindo salas de servidores e cofres	Maior nível de segurança, pois dois funcionários autorizados devem usar suas credenciais combinadas antes que o acesso seja liberado	Pode retardar as operações comerciais
Acompanhante de Visitantes	O visitante recebe credenciais funcionais, mas requer acesso acompanhado a várias áreas	Ideal para instalações com áreas altamente sensíveis que contêm ativos valiosos	O visitante nunca entra sozinho em determinadas áreas Garante que os movimentos de visitantes e acompanhantes possam ser rastreados o tempo todo	Pode atrapalhar para que tanto o visitante quanto o acompanhante se desloquem juntos, principalmente quando há mais de um visitante por acompanhante
Security Clearance and Threat Level Management	Capacidade de bloquear automaticamente uma sala, área ou edifício acionando um nível de ameaça predefinido	Para organizações que enfrentam uma gama crescente de ameaças potenciais aos funcionários e às instalações	Maior nível de segurança e proteção, sendo capaz de responder de forma rápida e eficaz a potenciais ameaças	Pode causar inconvenientes ao restringir o acesso de funcionários a áreas específicas assim que um nível de ameaça for acionado

Medida de segurança	Visão geral	Quando usar	Prós	Contras
Autenticação Multifator	Garante que a pessoa que apresenta suas credenciais é a mesma para a qual essas credenciais foram emitidas	Para qualquer organização interessada em aumentar a segurança em suas instalações	Eficaz e muitas vezes uma maneira barata de aumentar a segurança	Pode obstruir o fluxo de pessoas
Cartões inteligentes e leitores	Evita o uso indevido ou reprodução ilegal de credenciais, aproveita a criptografia	Para organizações preocupadas com o uso indevido de credenciais por funcionários ou possíveis invasores	Oferecem maior nível de segurança e interoperabilidade Oferece maior segurança aproveitando algoritmos de criptografia avançados e chaves de criptografia definidas pelo usuário final	Alguns tipos são suscetíveis à clonagem e a ser danificados
Formatos de cartão customizados	Permite que uma organização defina seu próprio formato de cartão, dificultando a duplicação fraudulenta	Para organizações interessadas na opção que permite definir seus próprios formatos de cartão	Oferece maior segurança aproveitando os números de cartão customizados e estendidos	Pode obstruir o fluxo de pessoas
Integração com Microsoft Active Directory ou LDAP	Vincula grupos de segurança do Windows a grupos de portadores de cartão e administradores ACS, fornecendo controle de gerenciamento de acesso mais eficiente	Para qualquer organização interessada em economizar tempo e reduzir instâncias de erro humano associadas a determinar e alterar direitos de acesso físico para portadores de cartão	As contas são criadas ou desativadas automaticamente com base nas sincronizações do servidor Active Directory Os portadores de cartão podem receber automaticamente seus direitos de acesso físico para a instalação toda	Alguns tipos são suscetíveis à clonagem e a ser danificados

A Genetec™ desenvolve software de plataforma aberta, hardware e serviços baseados na nuvem para o setor de segurança física e segurança pública. Seu principal produto, o Security Center, unifica o videomonitoramento baseado em IP, controle de acesso e reconhecimento automático de placas de veículos (ALPR) em uma única plataforma. Um inovadora global desde 1997, a Genetec™ está sediada em Montreal, Canadá, e atende organizações empresariais e governamentais por meio de uma rede integrada de revendedores, integradores e consultores em mais de 80 países. A Genetec™ foi fundada com base no princípio da inovação e permanece na vanguarda das tecnologias emergentes que unificam os sistemas de segurança física. Para mais informações sobre a Genetec™, visite: genetec. com/br