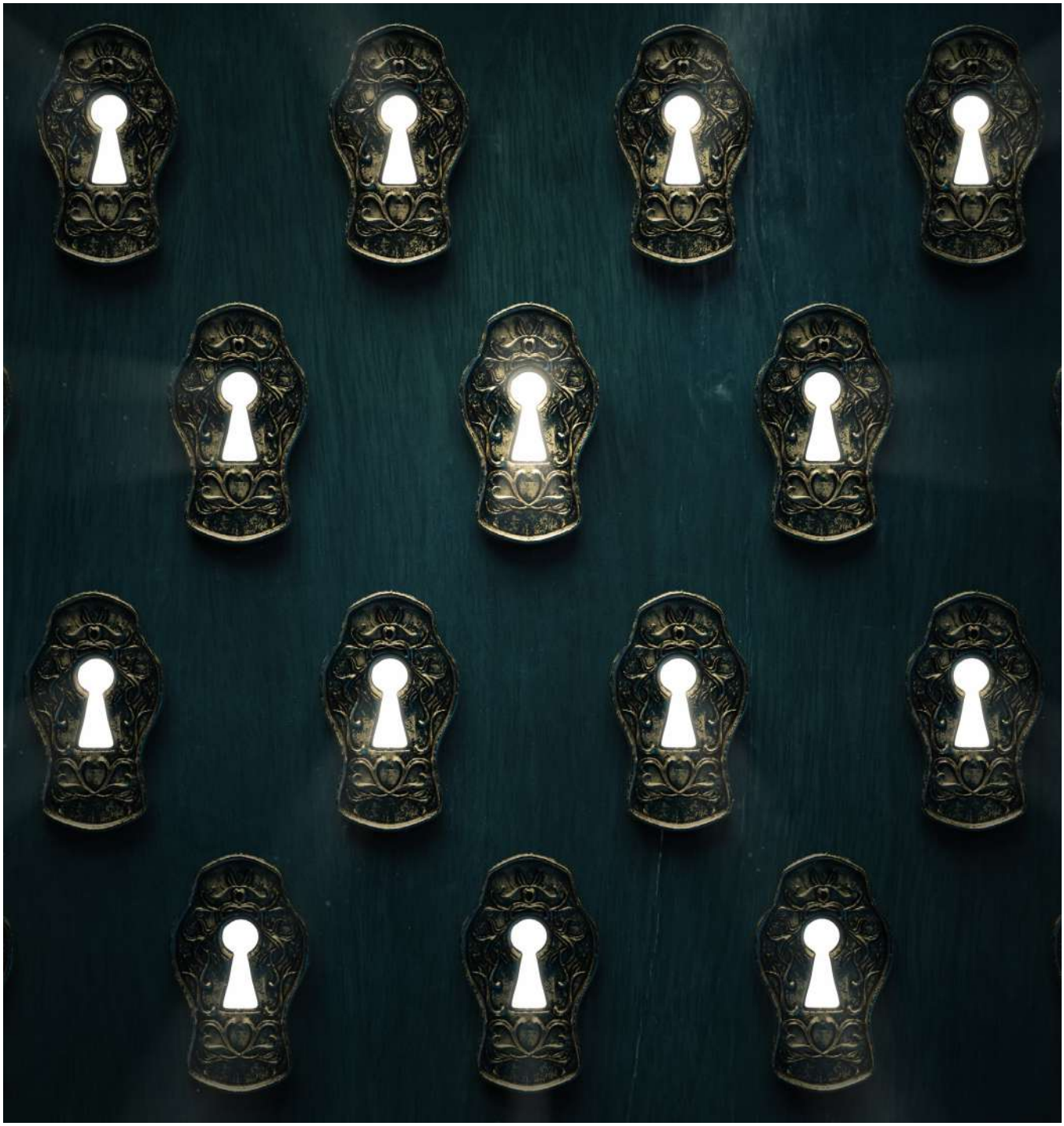
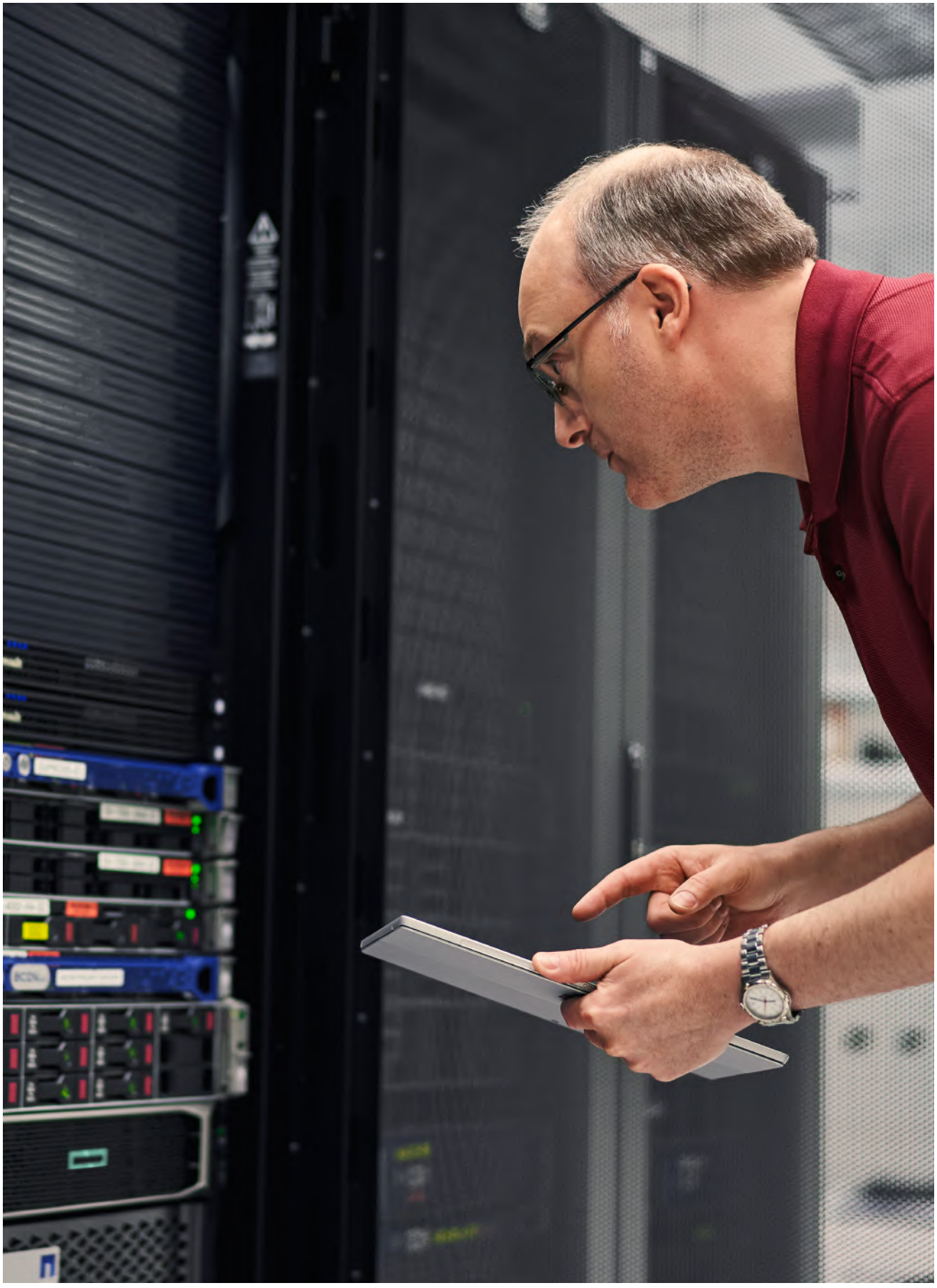
Whitepaper

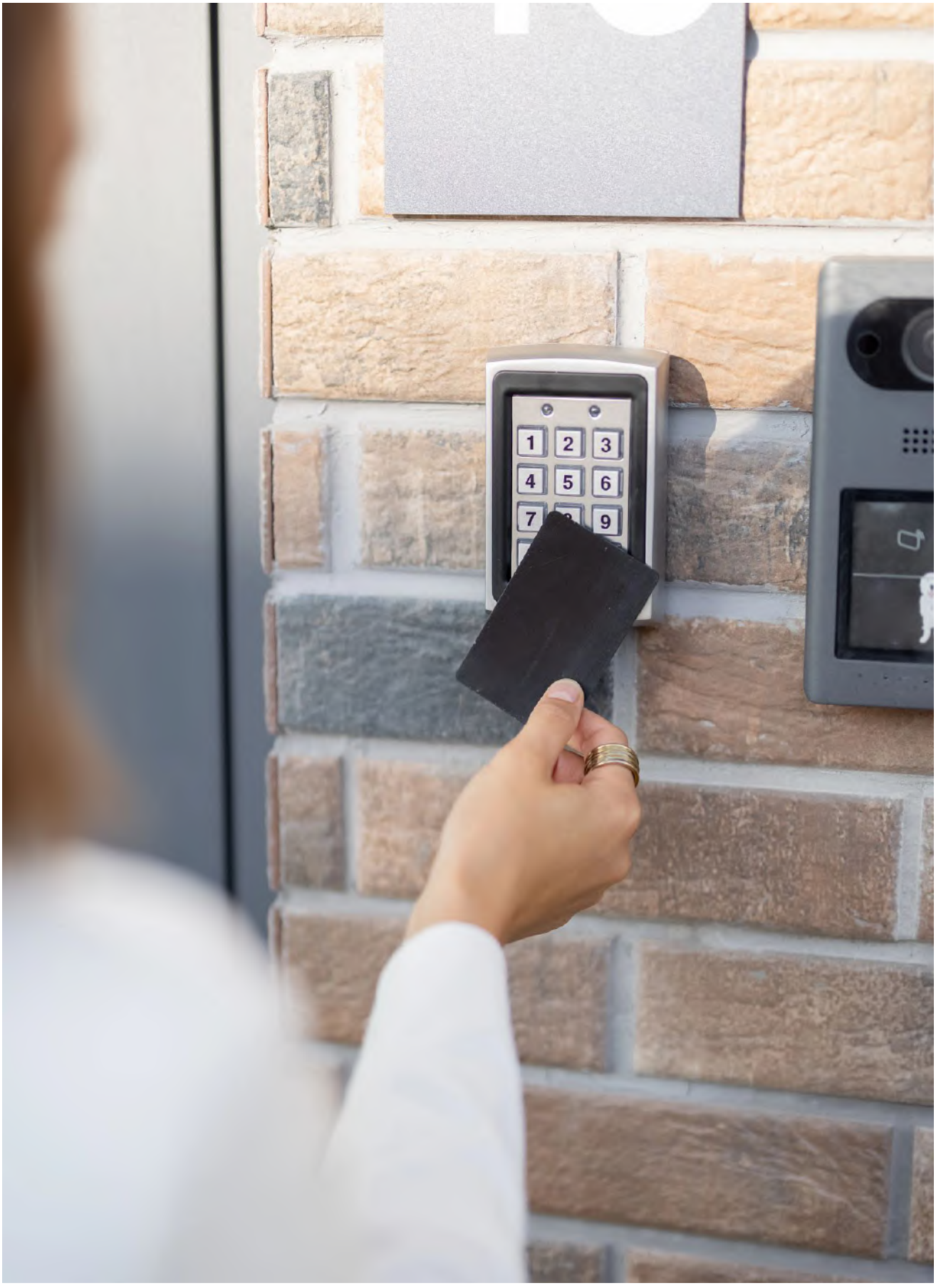
Riscos em sistemas de controle de acesso legados



Genetec™



Conteúdo


1 2 3
4 5 6
7 9

Sumário Executivo

Muitas organizações estão mantendo sistemas de controle de acesso que estão com 15 anos ou mais. Os sistemas de controle de acesso mais antigos podem parecer funcionar o suficiente para que os colaboradores entrem e saiam, mas esse tipo de tecnologia herdada pode ser vulnerável a ameaças cibernéticas.

As novas e mais seguras soluções de controle de acesso cibernético apresentam criptografia de ponta a ponta e autenticação avançada, além de outros recursos para se defender contra ataques cibernéticos e malware. Uma abordagem moderna e unificada de controle de acesso pode tornar sua organização mais resiliente a ameaças cibernéticas, ao mesmo tempo em que agrega muito mais valor do que simplesmente bloquear e desbloquear portas.

1

Introdução

Em todo o mundo, criminosos cibernéticos experientes estão procurando brechas de segurança para obter acesso a instalações, sistemas de vigilância e dados confidenciais que podem vender no mercado negro ou usar para extorquir uma organização. Os afetados pagam um alto preço; o custo médio de uma violação de dados subiu de US$ 3,86 milhões em 2020 para US$ 4,24 milhões em 2021[1] , mas o custo para algumas empresas foi de dezenas de milhões. Em 2021, uma empresa foi solicitada a pagar US$ 70 milhões de resgate[2] o mais alto já exigido em um ataque cibernético.

Computadores e servidores não são os únicos dispositivos vulneráveis a ameaças cibernéticas. Qualquer dispositivo conectado à Internet ou à sua rede local pode ser um ponto fraco quando se trata de cybersecurity.

Vulnerabilidades em sistemas de controle de acesso legados podem introduzir pontos fracos de cybersecurity que colocam sua organização em risco. As ameaças cibernéticas emergentes podem ter como alvo essas vulnerabilidades em todos os níveis: a credencial, o controlador e o servidor ou workstations.

Se um cibercriminoso violar sua rede para obter acesso a dados confidenciais, como informações proprietárias ou informações privadas de clientes, o impacto de uma violação de cybersecurity em seu sistema de controle de acesso pode causar danos muito além dos domínios de sua empresa. Isso pode afetar não apenas seus resultados, mas também a sua reputação e de seus colaboradores, a privacidade de seus clientes e muito mais.

Você precisa proteger aquilo que está protegendo você. É por isso que as organizações empresariais, governamentais, educacionais e de segurança pública estão se afastando de soluções proprietárias em prol de soluções de controle de acesso seguro. Eles estão procurando uma plataforma de segurança física unificada criada com cybersecurity em mente.

[1] https://www.ibm.com/security/data-breach
[2] https://www.welives`ecurity.com/2021/09/30/eset-threat-report-t22021/

Se um cibercriminoso violar sua rede para obter acesso a dados confidenciais, como informações proprietárias ou informações privadas de clientes, o impacto de uma violação de cybersecurity em seu sistema de controle de acesso pode causar danos muito além dos domínios de sua empresa.

2

Pontos fracos em sistemas de controle de acesso legados

A maioria dos sistemas de controle de acesso hoje são baseados em Protocolo de Internet (IP), conectados a uma rede local através da Internet. Os sistemas baseados em IP são poderosos, mas os sistemas legados carecem de recursos vitais de cybersecurity que são necessários para se defender de ameaças cibernéticas em constante evolução.

Seu sistema de controle de acesso é tão forte quanto seu elo mais fraco. Os cibercriminosos podem explorar pontos fracos nas credenciais do sistema de controle de acesso, controladores, servidores ou workstations conectadas à rede. Uma vez que alguém tenha violado sua rede, eles podem obter o controle de outros sistemas dos edifícios, visualizar ou roubar informações confidenciais de registros internos ou lançar ataques projetados para deixar os principais sistemas offline.

Algumas ameaças comuns de cybersecurity envolvendo sistemas de controle de acesso incluem:

- **Ataques man-in-the-middle** — Quando um cibercriminoso obtém acesso a uma rede para coletar informações trocadas entre dispositivos, como códigos de abertura de portas ou logins e senhas de dispositivos
- **Skimming e ataque de retransmissão** — Quando um criminoso usa seu leitor para acessar e clonar informações do cartão da vítima sem consentimento
- **Ataques ao controlador** — Quando um criminoso substitui o firmware do controlador, tornando o dispositivo inutilizável

Uma vez que alguém tenha violado sua rede, eles podem obter o controle de outros sistemas dos edifícios, visualizar ou roubar informações confidenciais de registros internos ou lançar ataques projetados para deixar os principais sistemas offline.

3

Vulnerabilidades no âmbito da credencial

Os sistemas de controle de acesso dependem das credenciais do usuário para determinar quem tem e quem não tem permissão para acessar áreas específicas. Existem muitos tipos de credenciais usadas por esses sistemas, incluindo códigos PIN, aplicativos de smartphone, impressões digitais e chaveiros ou cartões.

Os cibercriminosos podem roubar credenciais de usuários em ataques de skimming. É quando eles usam seu próprio leitor não autorizado para acessar informações sem o conhecimento do usuário. Como alternativa, se eles puderem obter acesso à sua rede, poderão interceptar dados de credenciais enviados pela rede e armazená-los para uso posterior. Eles podem usar esses dados para 'falsificar' ou clonar alguns tipos de cartões-chave ou chaveiros mais antigos que ainda são comumente usados. Muitas credenciais mais antigas, como cartões de aproximação, podem ser copiadas com muita facilidade usando um dispositivo barato que pode ser comprado online.

Algumas credenciais comuns usadas em sistemas de controle de acesso legados com tarja magnética e cartões de aproximação de 125kHz também têm vulnerabilidades conhecidas. Muitos se comunicam através do protocolo Weigand, que se tornou o padrão da indústria desde sua invenção em 1974. Infelizmente, os hackers aprenderam a adulterar os leitores de cartão comumente usados com esse tipo de sistema para recuperar informações sensíveis.

A comunicação Wiegand é unidirecional, portanto, se o leitor for adulterado, o controlador não será notificado, a menos que esteja conectado a um interruptor de adulteração. Os dados enviados por meio de um sistema estilo Wiegand também não são criptografados, portanto, mesmo ao usar credenciais seguras, informações confidenciais podem ser extraídas.

A vulnerabilidade mais comum no âmbito da credencial, no entanto, é o erro humano. Compartilhar códigos PIN ou chaveiros, perder cartões-chave, segurar ou prender portas abertas.

Para mitigar o risco de ataques man-in-the-middle, procure um sistema que tenha um protocolo bidirecional seguro entre o leitor e o controlador, como o OSDP2. Isso garantirá que, se alguém tentar roubar credenciais adulterando o leitor ou substituindo-o por um leitor fraudulento, não poderá extrair informações confidenciais. O protocolo bidirecional também notificará o operador de que houve uma tentativa de adulteração do sistema, para que sua equipe de segurança possa responder rapidamente e neutralizar a ameaça.

A vulnerabilidade mais comum no âmbito da credencial, no entanto, é o erro humano. Compartilhar códigos PIN ou chaveiros, perder cartões-chave e segurar ou prender portas abertas são pequenas decisões comuns que podem ter um grande impacto na segurança do seu prédio.

Escolher credenciais seguras avançadas ou biometria é a melhor abordagem para reduzir vulnerabilidades no âmbito da credencial. Melhorar a higiene cibernética também pode ajudar a reduzir os riscos relacionados ao erro humano. Certifique-se que todos os colaboradores recebam treinamento, avisos e lembretes para criar uma cultura de trabalho que incentive e reforce a boa higiene cibernética. Esse requisito deve se estender aos parceiros com quem você trabalha, pois uma violação deles também pode afetar sua segurança. Peça a todos os parceiros de software que descrevam as ações que realizam para garantir que sua equipe siga as melhores práticas de higiene cibernética – e inclua cybersecurity como um componente dos requisitos de solicitação de proposta – ao buscar novos parceiros de software ou fornecedores de hardware conectado à rede.

O gerenciamento de direitos de acesso é outro processo propenso a erros quando as informações são gerenciadas e rastreadas manualmente. Escolha parceiros de segurança que também possam fornecer uma solução unificada para gerenciar direitos de acesso com base em funções e status do usuário, não em indivíduos. Isso permite que você faça upgrade, downgrade, adicione ou cancele automaticamente direitos de acesso para grupos de pessoas conforme as necessidades mudam. Por exemplo, quando uma colaboradora sai de licença maternidade, muda de função ou deixa a empresa. Quando o status do colaborador muda no banco de dados vinculado, seus direitos de acesso também mudam, para que você possa eliminar o risco de alguém usar um cartão-chave antigo para entrar em áreas nas quais não trabalham mais. Esse sistema também permite que você revogue o acesso rapidamente se o cartão-chave de alguém ou outra credencial for perdido ou roubado.

4

Vulnerabilidades no âmbito do controlador

Os controladores interpretam as credenciais do leitor e comparam com uma whitelist sincronizada do servidor de controle de acesso. Se as credenciais forem iguais, ele envia um sinal para a trava da porta para abrir ou negar o acesso.

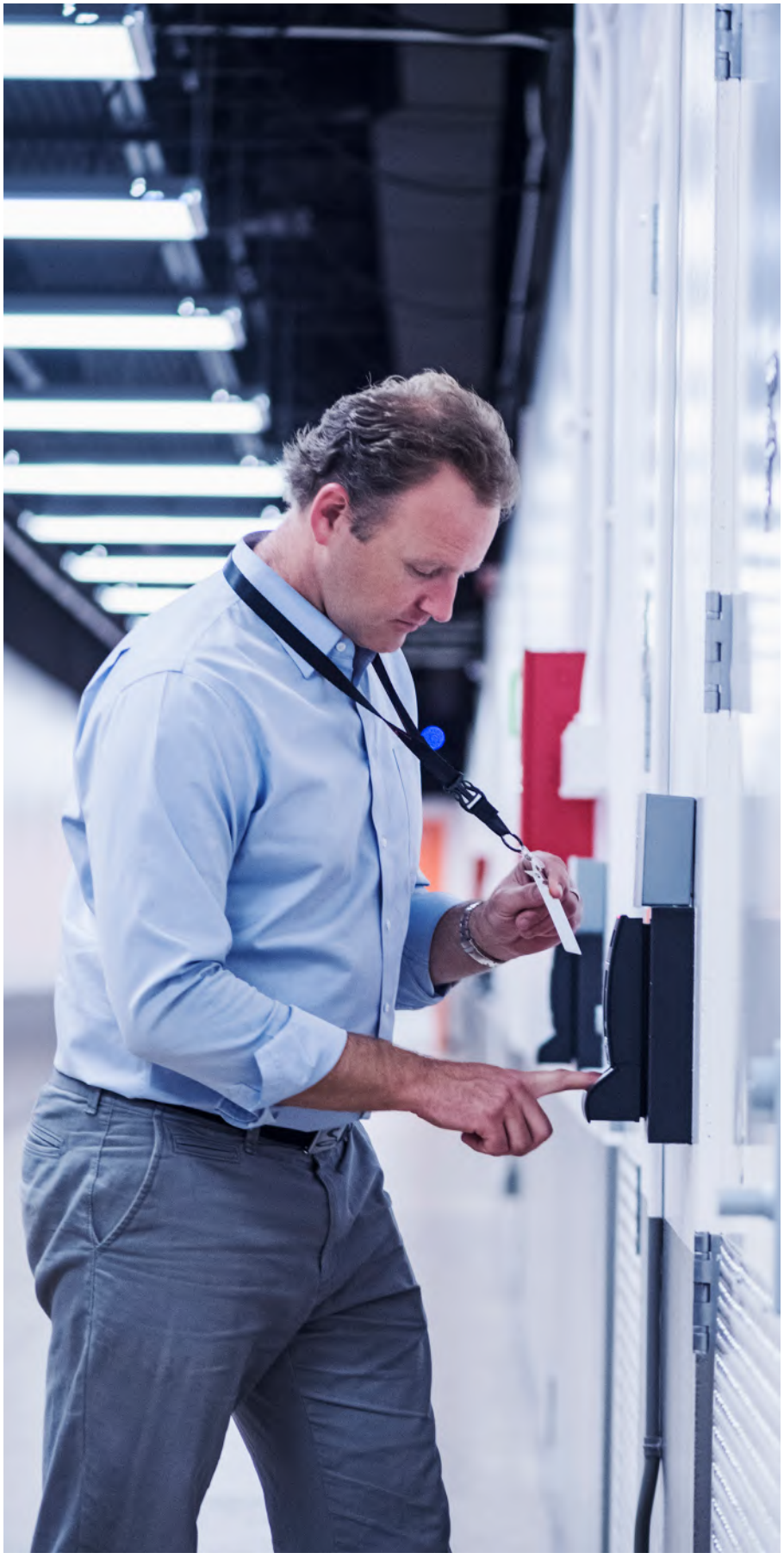
Uma criptografia ou senha fraca pode permitir que cibercriminosos obtenham acesso aos seus controladores e assim se apossando das chaves de suas instalações.

Os sistemas modernos de controle de acesso usam uma ferramenta inteligente de gerenciamento de certificados para autenticar o controlador e garantir comunicações seguras entre o servidor de controle de acesso e o controlador. A autenticação confirmará que um controlador autorizado está conectado a um servidor legítimo do qual recebe instruções. Para proteger as comunicações entre os dois componentes, é recomendável criptografar as comunicações usando o protocolo TLS (Transport Layer Security) versões 1.2 e superiores.

Os controladores exigem atualizações regulares de firmware para garantir que a segurança esteja atualizada. É importante garantir que sua equipe de segurança verifique as atualizações regularmente ou delegue isso a terceiros ou fornecedores confiáveis para que sejam imediatamente instaladas.

Por fim, uma ação simples, mas importante, a ser tomada para proteger seus controladores é garantir que as senhas padrão sejam alteradas para algo exclusivo que não possa ser facilmente adivinhado. Outra prática recomendada é ter um sistema de gerenciamento de senhas que altere automaticamente e regularmente as senhas usadas entre os dispositivos.

Os controladores exigem atualizações regulares de firmware para garantir que a segurança esteja atualizada. É importante garantir que sua equipe de segurança verifique as atualizações regularmente para que sejam instaladas de imediato.



5

Vulnerabilidades no âmbito do servidor ou da workstation

Os servidores armazenam e gerenciam a lista de credenciais aprovadas fornecidas aos indivíduos e se comunicam com os controladores para autenticar os dados das credenciais. Esta informação deve ser transmitida através de uma rede. Se os dados não estiverem criptografados, os cibercriminosos que obtiverem acesso à rede poderão roubar informações de credenciais e outros dados confidenciais.

Os dados de credenciais capturados de leitores e armazenados em servidores devem ser protegidos por métodos fortes de criptografia, autenticação e autorização. A maioria das vulnerabilidades no âmbito do servidor envolve:

- Usuários não autorizados explorando métodos fracos de autenticação
- Permissões de usuário excessivamente generosas, que permitem que as pessoas acessem dados que devem ser restritos ou façam alterações não autorizadas no sistema
- Quão bem o servidor gerencia a autenticação do usuário para garantir que apenas pessoas aprovadas possam visualizar informações confidenciais

Os dados de credenciais capturados de leitores e armazenados em servidores devem ser protegidos por métodos fortes de criptografia, autenticação e autorização.

6

Melhores práticas de cybersecurity para sistemas de controle de acesso

A tecnologia de controle de acesso passou por uma grande transformação nos últimos anos. Este mercado tradicionalmente proprietário mudou agora para um esquema mais aberto. Os clientes nem sempre estão presos a um fornecedor e, como resultado, as empresas estão desenvolvendo produtos e serviços mais inovadores. Essas soluções novas e ciberneticamente mais seguras apresentam criptografia de ponta a ponta e autenticação avançada, além de outros recursos para se defender contra ataques cibernéticos e malware.

Para melhorar a cybersecurity da sua rede

- Atualize seu sistema: sistemas mais antigos não foram criados para lidar com as ameaças atuais
- Use credenciais seguras, inteligentes e/ou móveis e os protocolos de comunicação mais recentes para proteger os dados enviados pela Internet
- Forneça treinamento aos colaboradores para educá-los sobre as melhores práticas de cybersecurity e garantir que eles sejam frequentemente solicitados a atualizar as senhas
- Use um sistema de gerenciamento de identidade para garantir que os usuários só possam acessar áreas e dados relacionados à sua função e status atual do colaborador
- Crie redes locais separadas para dispositivos que armazenam ou compartilham informações altamente confidenciais, para que não possam ser acessadas de sua rede usual

Muitas organizações preferem uma abordagem híbrida, para que possam aproveitar a flexibilidade e a escalabilidade do software na nuvem e das opções de armazenamento de dados, ao mesmo tempo em que mantêm alguns servidores gerenciados in loco.

- Escolha um provedor de segurança que comprove compliance com estruturas de controle de segurança estabelecidas
- Garanta que seu sistema de controle de acesso use métodos comprovados de criptografia de dados, bem como autenticação em várias etapas
- Trabalhe com um parceiro que tenha uma equipe dedicada para monitorar ameaças cibernéticas e garantir que o software seja atualizado com frequência e corrigido conforme necessário

Você não precisa escolher entre uma solução hospedada na nuvem ou in loco. Muitas organizações preferem uma abordagem híbrida, para que possam aproveitar a flexibilidade e a escalabilidade do software na nuvem e opções de armazenamento de dados, além de manter alguns servidores gerenciados localmente.

7

Os modernos sistemas de controle de acesso são mais do que apenas ciberseguros

Um sistema de controle de acesso unificado que usa os mais recentes padrões de cybersecurity para proteger a comunicação, os servidores e os dados. A solução de controle de acesso Genetec Synergis™ pode proteger melhor os ativos e as pessoas de uma organização, mas também ajudar a melhorar as operações de negócios e a tomada de decisões. Ao escolher um sistema de controle de acesso IP de arquitetura aberta, as organizações têm o poder de fazer upgrade para a mais recente tecnologia suportada a qualquer momento, evoluir em seu próprio ritmo e trabalhar dentro do orçamento disponível.

O sistema de controle de acesso Synergis™ usa os mais recentes padrões de cybersecurity para proteger a comunicação, os servidores e os dados em todos os níveis de sua arquitetura. Com proteção avançada de cartões de acesso a software, você pode gerenciar o acesso às suas instalações com confiança, sabendo que olhares invasivos serão mantidos longe.

O Genetec Security Center™ é uma plataforma de arquitetura aberta que unifica videomonitoramento IP, controle de acesso, reconhecimento automático de placas de veículos (ALPR), comunicações e analíticos. A Genetec também desenvolve soluções hospedadas na nuvem e serviços projetados para melhorar a segurança e contribuir com novos níveis de inteligência operacional para governos, empresas, transporte e as comunidades em que vivemos.

O Security Center é uma plataforma de arquitetura aberta que unifica videomonitoramento IP, controle de acesso, reconhecimento automático de placas de veículos (ALPR), comunicações e analíticos.

8

Os modernos sistemas de controle de acesso oferecem benefícios além de bloquear e desbloquear portas

Sistemas de controle de acesso mais novos e ciberseguros, como o Synergis, podem fazer muito mais do que apenas trancar e destrancar portas de acordo com um cronograma específico. Eles podem fazer uso da riqueza de dados coletados pelos sistemas de controle de acesso e combiná-los com dados de outras fontes para revelar novos e poderosos insights que podem ajudá-lo a melhorar as operações diárias, bem como a segurança. Como resultado, o retorno do investimento nesses sistemas é muito mais impressionante.

O Synergis vai além dos limites para liberar novos insights que ajudam você a tomar melhores decisões e melhorar as operações diárias. Na qualidade de um sistema verdadeiramente aberto, ele se conecta a uma grande e crescente lista de dispositivos de controle de acesso de terceiros. Ele agrega e exibe dados em um formato dinâmico para capacitá-lo a tomar melhores decisões.

Por exemplo, durante a pandemia de COVID, os clientes do Synergis puderam instalar de forma rápida e fácil novos leitores biométricos que reduziram a necessidade de contato físico[3], para que pudessem limitar a propagação de germes. Também foram capazes de usar os dados do sistema de controle de acesso para dar suporte ao rastreamento de contatos[4] se um funcionário testou positivo para o vírus, bem como para gerenciar os níveis de ocupação e os requisitos de distanciamento físico[5] exigido pelas autoridades de saúde pública.

Do gerenciamento de ocupação em tempo real ao monitoramento de infraestrutura remota, o Synergis™ pode ajudar a proteger suas operações – não apenas suas portas.

Os sistemas de controle de acesso coletam muitos dados, mas os sistemas mais antigos dificultam a coleta e a compreensão desses dados. O Synergis™ possui painéis que fornecem uma visão unificada de todos os seus sistemas de segurança e dados de sensores, para que você possa identificar tendências e ser proativo em vez de reativo com as decisões operacionais.

Do gerenciamento de ocupação em tempo real ao monitoramento de infraestrutura remota, o Synergis™ pode ajudar a proteger suas operações – não apenas suas portas. Você pode atender às necessidades de mudança ajustando facilmente as configurações do software ou adicionando/fazendo upgrade do hardware, sem precisar alterar todo o sistema. Você pode usar os dados de controle de acesso para habilitar a automação predial, desligar as luzes, por exemplo, ou ajustar o aquecimento e o resfriamento quando as pessoas não estiverem presentes. Você também pode entender melhor quais áreas dos edifícios são mais usadas, para entender se precisa de tanto espaço.

[3] https://www.genetec.com/podcasts/engage/episode-10-stepping-up-cybersecurity-biometrics-and-multifactor-authentication
[4] https://www.genetec.com/press-center/press-releases/2021/02/genetec-helps-westminster-property-ventures-ensure-safe-return-to-work-for-its-commercial-tenants
[5] https://resources.genetec.com/en-industry-focuses/genetec-occupancy-management-package

9

Conclusão

Um sistema de controle de acesso unificado que usa os mais recentes padrões de cybersecurity para proteger comunicações, servidores e dados, como o Security Center Synergis™ pode não apenas proteger melhor os ativos e as pessoas de uma organização, mas também ajudá-los a melhorar suas operações de negócios e a tomada de decisões que vão além de trancar e destrancar portas. Ao escolher um sistema de controle de acesso IP de arquitetura aberta, as organizações têm o poder de fazer upgrade para a mais recente tecnologia suportada a qualquer momento, evoluir em seu próprio ritmo e trabalhar dentro do orçamento disponível.

Pronto para mais?

Faça download do nosso checklist para ficar por dentro das 7 principais coisas que você precisa considerar ao migrar para um sistema de controle de acesso IP.

Obtenha o checklist

A Genetec Inc. é uma inovadora empresa de tecnologia com um amplo portfólio de soluções que abrange segurança, inteligência e operações. O produto carro-chefe da empresa, o Genetec Security Center™ é uma plataforma de segurança física que unifica videomonitoramento IP, controle de acesso, reconhecimento automático de placas de veículos (ALPR), comunicações e analíticos. A Genetec também desenvolve soluções hospedadas na nuvem e serviços projetados para melhorar a segurança e contribuir com novos níveis de inteligência operacional para governos, empresas, transporte e as comunidades em que vivemos. Fundada em 1997 e sediada em Montreal, Canadá, a Genetec atende seus clientes globais por meio de uma extensa rede de revendedores, integradores, parceiros de canal certificados e consultores em mais de 159 países.

Videomonitoramento: Obtenha uma maior consciência situacional e aumente a segurança em sua cidade com a capacidade de compartilhar câmeras entre agências e organizações, fornecendo uma imagem operacional em comum e melhorando o tempo de resposta a incidentes.

Controle de acesso: Aumente a segurança da sua organização de forma eficaz, responda às ameaças e tome decisões mais claras e oportunas usando uma plataforma unificada e pronta para IP, seja para implantação de um novo sistema de controle de acesso ou para atualizar uma instalação existente.

Reconhecimento automático de placas de veículos: Automatize a detecção de veículos de interesse, aumente a eficiência da fiscalização em estacionamentos e acelere as investigações de segurança pública por meio da capacidade de compartilhar informações de placas de veículos com agências selecionadas e organizações parceiras, sem violar propriedade e privacidade.

Suporte à decisão operacional: Gere mais eficiência no tratamento de incidentes e tomada de decisões através de fluxos de trabalho avançados que guiam os operadores durante alertas de situação por meio de procedimentos baseados em políticas para exportação de compilação detalhada de casos.

Gerenciamento de caso investigativo: Simplifique o gerenciamento de casos e acelere as investigações com uma plataforma que permite centralizar evidências digitais e colaborar de forma segura com investigadores, agências externas e o público.

Serviços na nuvem: Estenda os recursos do seu sistema de segurança on-premises e reduza os custos de TI com serviços na nuvem altamente escalável, on-demand que capacitam sua cidade a lidar facilmente com os requisitos de segurança em rápida mudança e operar com maior eficiência.

Genetec Inc.
genetec.com/br/fale-conosco
info@genetec.com
@genetec

UDPT: 01-06-2023