WHITE PAPER

Uma Análise do Mercado de Controle de Acesso na América Latina

Um estudo realizado pela HID Global sobre usuários finais latino-americanos revelou que as corporações na região têm como imperativo urgente, atualizar seus sistemas de controle de acesso, aumentar seus níveis de proteção e complementá-los com novas funcionalidades.

SUMÁRIO EXECUTIVO

Os sistemas de controle de acesso físico não são mais simples ferramentas que autorizam ou impedem que as pessoas entrem em uma edificação. Atualmente, essas soluções integram novas tecnologias que fornecem segurança avançada e podem ser aplicadas em diversas configurações corporativas.

Apesar disso, muitas organizações ainda não têm planos para modernizar seus sistemas de controle de acesso. Essa falta de planejamento as expõe a inúmeras vulnerabilidades no ambiente atual.

Investir em um sistema moderno de controle de acesso é uma importante decisão empresarial. E como tal, é importante aproveitar ao máximo do potencial desses sistemas.

Cada um desses pontos foi levado em consideração nesta pesquisa da HID Global®, com usuários finais de uma diversidade de mercados verticais da América Latina. Como parte da pesquisa, os participantes abordaram as tecnologias de controle de acesso que eles utilizam atualmente.

Os resultados compilados neste documento, provam que muitas organizações ainda usam tecnologias legadas desatualizadas que não proporcionam a proteção que eles necessitam.

Em contraste, o mercado atual oferece muitas alternativas modernas baseadas em altos padrões de segurança e que estão ao alcance de qualquer usuário, desmistificando a ideia de que apenas organizações de grande porte podem adquirir esses tipos de soluções.

Considerando que a segurança é vital para o sucesso de uma organização, as informações neste documento estão agora disponíveis para as empresas que buscam elevar sua segurança para o próximo nível.

INTRODUÇÃO

Imagine este cenário: na década de 1970, uma marca de automóveis renomada lança um novo modelo com características excepcionais para o seu tempo. Seus níveis de conforto, desempenho e segurança se destacam no setor. Em 2018, esses automóveis continuam em circulação, cumprindo a função básica do transporte de passageiros. No entanto, eles não atendem aos padrões atuais de segurança e os clientes não estão satisfeitos com o desempenho desses veículos. Os clientes os considerariam um bom valor? Eles se sentiriam seguros dirigindo-os? Simplificando, a resposta a essas perguntas é “não”. A indústria automobilística produz continuamente veículos com novos recursos e inovações para garantir que seus produtos não apenas transportem as pessoas, mas que também ofereçam mais conforto e segurança. A inovação constante garante que uma empresa continue atendendo ativamente aos desafios, conforme as necessidades evoluem no setor. Para tentar evitar ao máximo expor os usuários finais a riscos desnecessários.

No mercado latino-americano de soluções de controle de acesso físico, algo semelhante está ocorrendo. Como muitas organizações continuam utilizando ferramentas desatualizadas, elas se situam em um (ou mais) dos três cenários a seguir:

1) Elas continuam a operar com sistemas inseguros.

2) Elas utilizam soluções obsoletas

3) Elas não utilizam os recursos avançados que as aplicações de controle de acesso oferecem.

Os resultados de uma pesquisa da HID Global com 648 funcionários da área de segurança em países da América Latina, respaldam os resultados acima. Entre os entrevistados, 29% eram consultores de segurança, 22% eram gerentes ou diretores de departamentos de segurança e 17% eram gerentes de TI, diretores ou outro pessoal relevante. Em resumo, 67% dos entrevistados se enquadram na categoria de tomadores de decisão em suas respectivas empresas, especificamente no que diz respeito aos sistemas de controle de acesso.

(Todos os participantes eram usuários finais em mercados verticais, como Construção Civil, Serviços Gerais, Tecnologia da Informação, Educação, Governo e Finanças).

A more detailed discussion of the three scenarios mentioned above follows.

Segurança Confiável para Soluções Vulneráveis

Neste estudo, 37,3% dos participantes confirmaram que a tecnologia atual utilizada por suas organizações para controle de acesso físico são cartões de baixa frequência operando na faixa de 125kHz.

Essa tecnologia de baixa frequência chegou ao mercado há mais de 25 anos e, apesar de oferecer vantagens significativas em termos de longevidade, esses cartões de identificação podem ser facilmente clonados – geralmente sem a detecção do usuário autorizado. Além disso, um cartão clonado pode abrir qualquer porta correspondente pré-configurada.

Atualmente, não existe uma forma eficiente para determinar se um sistema foi comprometido, o que gera uma falsa sensação de segurança. Como um cartão clonado é considerado como legítimo, qualquer pessoa não autorizada pode entrar na edificação de uma empresa e usar seus equipamentos ou serviços.

Segundo os pesquisadores, os códigos de barras constituem a segunda tecnologia de segurança mais implementada, com 20,4%. Essa constatação é preocupante, especialmente considerando que os códigos de barras são a tecnologia de credencial menos segura em uso no mercado atual. Apesar de ser um sistema difundido em locais como bibliotecas e supermercados, os códigos de barras não são eficazes em termos de segurança, pois seu principal elemento de proteção é diretamente visível, tornando-os extremamente vulneráveis a cópias e outros ataques. Levando em conta a simplicidade de tirar uma foto de uma identificação e criar uma cópia do original - sobretudo considerando que a maioria das pessoas no mundo possui smartphones com câmeras de alta resolução - comprometer um sistema se torna uma tarefa fácil.

A terceira tecnologia de controle de acesso mais popular é a tarja magnética, usada por 20,1% dos entrevistados da pesquisa. Mesmo o setor bancário que evolui lentamente, está eliminando essa tecnologia insegura, substituindo-a pela leitura com contato à "chip". Os cartões magnéticos armazenam e coletam informações sobre finas tiras magnéticas, que tendem a se desgastar com cada uso. Ainda mais preocupante, os analistas afirmam que não há segurança agregada a essa tecnologia, já que os dados coletados não possuem criptografia.

Em uma nota positiva, 18,5% dos entrevistados indicaram que suas organizações usam o acesso móvel como forma de identificação e controle de entradas. Mesmo que esse método de segurança ainda não seja o mais popular no mercado de segurança atual, ele está conquistando o reconhecimento por seus benefícios de uso e proteção robusta contra intrusões em potencial.

A utilização de tecnologias de PACS desatualizadas expõe a organização ao risco de duplicação fraudulenta de funcionários e uso de cartões copiados, e a submete à possibilidade de que pessoas não autorizadas entrem em suas instalações ou - pior ainda - acessem sistemas de TI e de rede, criando uma ameaça muito severa para essas organizações.

Em alguns casos, os funcionários podem copiar cartões de identificação de acesso, para entrar no sistema de uma organização e furtar informações com o nome de outro colega. Infelizmente, é muito fácil copiar e transferir informações de um cartão de proximidade para outro - existem até tutoriais em vídeo no YouTube que oferecem instruções.

Explorando Novas Opções

É evidente que o principal objetivo das soluções de controle de acesso físico é permitir que apenas pessoas autorizadas entrem em qualquer edificação. No entanto, essas ferramentas também podem oferecer benefícios adicionais que geralmente não são explorados ou utilizados pela maioria dos usuários finais.

O estudo da HID Global revelou que o recurso de sistema de autenticação mais usado pelos entrevistados (75%), é o sistema de controle de acesso físico isolado. Considerando essa estatística, é importante observar que as soluções de PACS podem ser reaplicadas para outros casos de uso - especialmente aqueles mencionados separadamente pelos participantes da pesquisa.

As aplicações adicionais para os cartões de controle de acesso, dependem do tipo de usuário. Por exemplo, em uma comunidade residencial de médio porte, a solução de segurança disponível deve manter as portas do condomínio fechadas e os portões de estacionamento inativos. No entanto, em um segmento de mercado premium, essa mesma solução também pode ser configurada para controlar a piscina, o SPA e as áreas comuns. Esses serviços integrados tornam-se viáveis quando os sistemas usam a tecnologia avançada dos cartões inteligentes, com integrações entre vários componentes de software.

Nas atividades empresariais, os cartões de acesso são a principal forma de identificação dos colaboradores, e ainda disponibilizam serviços latentes. Dependendo do software da organização, esse mesmo cartão de identificação pode ser usado para fornecer vale refeição ou gerenciar o sistema de impressão da empresa.

As possibilidades são ilimitadas quando se trata de vincular sistemas de controle de acesso a serviços adicionais, restritos apenas pela criatividade da equipe da organização. Por exemplo, é possível controlar a privacidade de documentos impressos na organização, verificar se o departamento que utiliza serviços de impressão está pagando por eles, registrar transações, gerenciar máquinas de venda automática e muito mais, com um cartão de controle de acesso.

Todas as informações necessárias já estão incluídas no cartão específico, que criptografa os dados que são reconhecidos por suas leitoras.

O Uso de Tecnologias Obsoletas Gera Insatisfação

Outro elemento abordado pela análise da HID Global refere-se ao tempo de vida útil e suporte disponíveis para as soluções de controle de acesso existentes. É vital que os usuários finais conheçam o tempo de instalação dos produtos e serviços existentes, no que se refere ao ciclo de vida completo de seus sistemas. Além disso, se uma solução tiver alguma vulnerabilidade conhecida, não for suportada ou não houver mais peças de reposição prontamente disponíveis, ela deverá ser atualizada assim que possível.

De acordo com os resultados da pesquisa, 11% dos entrevistados utilizam atualmente leitoras de cartões que foram instaladas há mais de seis anos. Este prazo também se aplica ao software (9,4%), controladoras (11,4%) e cartões (9,8%) que estão atualmente em uso.

O uso de soluções desatualizadas tem um impacto direto nos níveis de satisfação dos usuários finais: aproximadamente 46,4% dos participantes afirmaram que estavam conformados com o uso de uma ferramenta de controle de acesso, que nem sequer atendia às suas necessidades básicas ou esperadas.

A este propósito, é necessário ressaltar a importância da capacidade dos profissionais de segurança de se manterem atualizados com as tendências e tecnologias de controle de acesso. Embora seja uma dura realidade, que as empresas nem sempre disponham dos recursos financeiros necessários para atualizar suas ferramentas, é essencial que os tomadores de decisão continuem familiarizados com as novas opções do mercado.

Apesar desses fatos preocupantes, ainda existem usuários finais que não têm planos para atualizar, num futuro próximo, os componentes de seus sistemas de segurança. Especificamente, 23,6% dos entrevistados afirmaram não ter considerado a possibilidade de modernizar suas leitoras, cartões de identificação, controladoras ou softwares.

Controles de Acesso Desatualizados na América Latina

Não é segredo que a situação de segurança regional represente uma importante preocupação para governos e empresas, sem falar dos cidadãos locais. Como resultado, foi necessário identificar e adotar métodos mais avançados de proteção.

Um bom exemplo dessa necessidade surgiu em 2018 na região de Recoleta, um bairro em Buenos Aires na Argentina. Nesse caso, as autoridades trabalharam para capturar um grupo de criminosos que constantemente copiavam as chaves codificadas dos prédios residenciais locais. Essas chaves de 125 kHz eram um alvo prioritário, pois haviam sido criadas em 1990. Segundo a mídia argentina , mais de cinquenta assaltos ocorreram em aproximadamente seis meses, no final de 2018.

Essas chaves codificadas podem ser facilmente copiadas por criminosos, por meio de um dispositivo digital adquirido facilmente online. A cópia é processada em cerca de cinco segundos e custa aproximadamente US$ 1,14. Neste caso específico, a comunidade argentina optou por introduzir vários dispositivos “anti-hackers” , que impedem a abertura de uma porta do edifício quando solicitado por uma chave copiada.

Para evitar situações como essa, fabricantes como a HID e sua rede de parceiros certificados recomendam a atualização da tecnologia para uma geração de dispositivos mais atual, que utilizem elementos criptográficos com prevenção contra a duplicação. Além disso, esses especialistas recomendam o uso de chaves com criptografia forte, como as oferecidas pela HID Global®, que são muito difíceis de serem clonadas .

---

[1] América Noticias (2018, September 6). América Noticias nos visita para saber sobre llaveros electrónicos.
Found at: https://www.youtube.com/watch?v=PaZc9av8gRs

[2] A24 (2018, September 6). ¿Llaveros electrónicos clonables?
Found at: https://www.youtube.com/watch?v=Mo5JFpBFxNU

[3] A24 (2018, September 2016). Entrevista en vivo con América 24 por los llaveros electrónicos.
Found at: https://www.youtube.com/watch?v=L1_pHAoRTLE

COMO VIABILIZAR A EVOLUÇÃO DESSE PANORÂMA NA AMÉRICA LATINA ?

Infelizmente, os usuários finais da América Latina continuam a utilizar tecnologias ultrapassadas com mais de 20 anos de existência, que geram grandes lacunas de segurança.

Por exemplo, alguns usuários finais acreditam que as câmeras de vídeovigilância proporcionam segurança suficiente para detectar e evitar qualquer possibilidade de risco. No entanto, esta suposição está longe da realidade. Na América Latina, é comum encontrar ambientes de segurança altamente vulneráveis e susceptíveis, como esses, originados pela falta de conhecimento dos usuários finais em relação ao controle de acesso.

Quando esses clientes são aconselhados a atualizar suas tecnologias e ferramentas, muitos respondem assim:

- "Meu sistema de identificação ainda funciona".
- "A ferramenta que estou usando tem garantia vitalícia".
- "Não tenho tempo para aprender e introduzir as melhores práticas do mercado".
- “Ter que alterar a configuração ou o protocolo no meu sistema de compras é um processo muito complexo”.
- "Os fabricantes estão apenas sugerindo isso para o seu próprio benefício".
- "Eu não tenho orçamento para isso".

Na tentativa de se proteger, as organizações do mercado latino-americano têm utilizado soluções que, embora fossem adequadas em seu tempo - ficaram aquém das atuais necessidades de segurança da região.

Os cartões de primeira geração são um excelente exemplo dessas soluções. Originários da década de 1990, eles operam em baixa frequência com 125 kHz e correm um alto risco de fraudes de duplicação.

Os cartões de segunda geração, que apareceram no mercado entre 1996 e 2002, oferecem um nível mais elevado de proteção, graças à inclusão de um chip de memória, mas ainda apresentam altos riscos de duplicação.

Os cartões de terceira geração, lançados em 2011, operam com uma frequência mais alta, em 13,56 Mhz, e incluem um SIO (Objeto de Identidade Segura) ou uma outra tecnologia geralmente equivalente. Este último utiliza um modelo de dados que permite que apenas os dados de identificação de um objeto específico sejam armazenados e transferidos. Como resultado, ele é frequentemente utilizado em dispositivos de controle de acesso, como crachás. Embora esses cartões sejam muito mais seguros, vale ressaltar que eles ainda correm o risco de replicação.

Em 2014, a última geração de tecnologia de segurança surgiu, trazendo com ela a plataforma de credenciais Seos®. Esta solução poderosa e inovadora para identificação segura, funciona extremamente bem no segmento de controle de acesso. Um dos benefícios mais significativos do Seos é que ele proporciona o acesso seguro a mais aplicações, ao mesmo tempo em que possibilita que o usuário final utilize o dispositivo de sua preferência, tudo isso propiciando total privacidade ao usuário.

Outras vantagens incluem:

- Flexibilidade na implementação de cartões de identificação físicos ou virtuais.
- Uma faixa de preço por cartão bastante inferior em comparação com o Prox.
- Segurança a longo e curto prazo.
- Funcionalidades em muitas aplicações.
- Suporte para controle de acesso móvel.

Desde 2017, as empresas começaram a realizar atualizações, principalmente porque tiveram mais recursos para efetuá-las. Infelizmente, o mesmo não se aplica a muitas pequenas e médias empresas, que não tiveram o mesmo nível de capital para realizar esses investimentos.

Embora mais usuários finais identifiquem o risco inerente à sua situação, o investimento em tais atualizações tem sido relativamente baixo. Então, para que esses projetos produzam um impacto global e afetem vários países da região, a designação de um orçamento significativo será fundamental. Isto é, além de definir a segurança como uma prioridade para os negócios.

SOLUÇÕES MODERNAS: ALTERNATIVAS QUE PODEM TRANSFORMAR A REALIDADE PRESENTE

É impossível abordar as modernas soluções de controle de acesso sem mencionar a tecnologia que torna possível cada uma dessas inovadoras ferramentas: o Seos. Disponível para credenciais físicas e digitais, o Seos é desenvolvido para ser altamente portátil.

Essa portabilidade significa que o Seos pode estar embarcado em um cartão físico ou em um dispositivo móvel, bem como em outros dispositivos, como smartwatches. O Seos é uma plataforma que permite maior segurança, proporcionando a conveniência de uma solução de controle de acesso em constante evolução.

Considerando a taxa diária de furto de celulares na América Latina, no entanto, fica claro que as condições de segurança em toda a região representam um desafio crucial para os sistemas de controle de acesso móvel. Apesar dos benefícios substanciais que o Seos proporciona, dúvidas inevitavelmente surgem quando se considera os efeitos de um telefone perdido ou furtado. Como se desconecta o sistema do próprio dispositivo para que outro indivíduo não possa usar as credenciais anexadas?

Fazendo face a essa preocupação, os especialistas asseguram que, assim como os crachás físicos, os crachás virtuais só funcionam se seus sistemas correspondentes os autorizarem a acessar uma área restrita. Assim, com o HID Mobile Access, um administrador do sistema pode remover imediatamente quaisquer autorizações associadas concedidas a um funcionário caso ele perca seu telefone ou se desligue da organização.

É evidente que essas tecnologias modernas são positivas para muitas empresas, não apenas devido à maior segurança que elas oferecem, mas também porque não são onerosas, nem complicadas de serem implementadas. As leitoras de cartões Seos, por exemplo, podem ser facilmente ajustadas para aceitar credenciais específicas, assim o usuário final estará preparado e pronto para utilizá-la quase instantaneamente.

Atualizações Tecnológicas Acessíveis a Todos

Pequenas e médias empresas podem muito bem presumir que essa gama de tecnologias modernas e específicas é destinada e acessível apenas para organizações de grande porte. Que opções têm uma empresa com uma pequena operação e equipe limitada, especialmente se a solução atual de controle de acesso não for segura, e se eles quiserem adotar algo mais confiável, eficiente e seguro? Considerando esses pontos, a solução deverá ser difícil de duplicar e disponível por uma faixa de preço razoável.

As respostas para essas preocupações podem ser encontradas nas modernas soluções de controle de acesso, algumas das quais não requerem um investimento elevado e não são complementadas por recursos de demais soluções conhecidas por sua qualidade máxima. Essas duas características, por si só, superam as mais convencionais ferramentas de segurança.

Uma preocupação conexa é o Retorno sobre o Investimento (ROI) e os benefícios potenciais obtidos com a implementação de tal atualização (ou novo sistema geral). Os especialistas da HID indicam que é difícil obter com precisão um cálculo de ROI, para soluções focadas exclusivamente em credenciais, devido às variações do projeto. Embora algumas atualizações de solução possam incluir simples adequações dos cartões, outras podem exigir complementos distintos, com custos adicionais. Nesse caso, o preço é semelhante e não implica necessariamente uma grande alteração, já que uma simples análise dos detalhes de cada aplicação será suficiente para detectar quaisquer diferenças em questão. Assim, a partir de uma perspectiva de ROI, a variação potencial origina-se nas diferenças de custo entre as aplicações.

Dito isto, seria muito difícil estimar o custo de um indivíduo não autorizado, que obtivesse acesso e copiasse as informações das credenciais corporativas. Neste caso, o indivíduo poderia entrar onde e quando quisesse. Imagine se isso ocorresse em uma empresa que gerencie informações altamente confidenciais ou inventários. Quanto essa violação poderia custar à organização? Qual seria o preço para garantir que ninguém entrasse em uma edificação para ameaçar ou causar danos para sua equipe? Felizmente, cada uma dessas situações pode ser evitada com o uso de soluções de segurança, como as credenciais móveis.

Por outro lado, o gerenciamento e o processamento de cartões de identificação físicos também geram outros custos, como os resultantes da impressão e distribuição. Algumas empresas acabam alocando quantias significativas, para remeter cartões aos funcionários remotos. Ao comparar esses custos com as possíveis economias obtidas com o uso de novas tecnologias, é fácil concluir que essas modernas ferramentas de controle de acesso são muito mais eficientes financeiramente. Uma combinação de métodos de identificação física e digital também é uma opção viável, graças a esses novos sistemas.

Expandindo Além dos Métodos de Segurança Física

Em contraste com as opiniões de muitos usuários finais, o controle de acesso não protege apenas as instalações físicas. Esse equívoco se deve à falta de consideração sobre as possíveis vulnerabilidades de uma organização que não possui a segurança necessária. Além disso, não leva em conta ainda que a própria experiência do usuário mudou.

As soluções móveis mudaram significativamente esse cenário, pois revelaram as vulnerabilidades e deficiências de segurança das ferramentas anteriores. Eles simplificam para os diretores de TI a enorme responsabilidade de gerenciar não apenas computadores desktop, mas também servidores e aplicações baseados em nuvem. Agora, a TI deve garantir acesso, monitorar vídeo e assegurar a segurança física, além de proteger contra possíveis intrusões. Como resultado, o cenário da segurança evoluiu - portanto, o controle de acesso também deverá evoluir.

Nesta perspectiva, é importante que os profissionais de segurança considerem todas as possíveis fragilidades e inseguranças, sejam elas relacionadas a TI ou as ameaças físicas.

CONCLUSÃO

Antes da Internet, era possível depender de tecnologias relativamente seguras, pois a maioria das pessoas não sabia como invadir os sistemas de segurança. Como não existia nenhum método de transferência de informações tão eficiente quanto a Internet, aquele período foi uma era de "segurança por ocultação".

Atualmente, com tantas diferentes formas para acessar informações pela Internet, indivíduos maliciosos podem facilmente infringir a segurança física e lógica de uma empresa. Adicione a isso a disponibilidade de recursos de clonagem relativamente acessíveis, e a gravidade da situação se torna mais do que clara.

Então, por que correr o risco? A informação e a tecnologia necessárias para aumentar a segurança organizacional não estão apenas disponíveis, mas ao alcance de todos. Os riscos são uma realidade e a fraude de identidades é regularmente realizada graças a grandes lojas virtuais e pontos de venda. Quanto maior o perigo, maiores as consequências sofridas pelo usuário final.

Por essa razão, a proteção não deve ser limitada apenas à configuração física, mas também deve se estender por todo o espectro tecnológico da edificação. A falha de uma empresa em realizá-la seria o equivalente a operar um negócio com o Windows 3.0, a popular versão do sistema operacional Windows lançada em 1990.

Segurança e privacidade são extremamente importantes para os usuários finais. Como resultado, organizações de todos os tamanhos devem permanecer atentas e atualizadas sobre as notícias e tendências relacionadas aos acessos físico e lógico. As soluções de acesso móvel da HID estão disponíveis para empresas de qualquer porte, incluindo as que estimam não poderem investir em um novo sistema de controle de acesso, ou que não estejam planejando modernizar sua solução existente.

2019-04-29-hid-pacs-lam-acc-crtl-ind-lam-wp-en

PLT-04897