Checklist de cybersecurity

Todos os dias, os cibercriminosos encontram novas e sofisticadas formas de capitalizar em cima de vulnerabilidades. O aumento do trabalho remoto, dos dispositivos conectados e dados amplificou os riscos de cybersecurity.

Em nosso Relatório Estado da Indústria de Segurança Física de 2024, 50% dos especialistas em TI confirmaram que as vulnerabilidades de cybersecurity eram um dos principais desafios e 61% disseram que implantaram ferramentas relacionadas à cybersecurity.

Ter uma estratégia abrangente de cybersecurity é crucial em cada etapa da sua jornada de segurança física. Abaixo estão algumas perguntas de checklist para ajudar a informar uma postura de cybersecurity mais forte antes, durante e depois da implantação de segurança física.

Genetec™

Checklist de pré-implantação

Você está implementando ou adicionando um novo sistema à sua infraestrutura de segurança física? Tenha a certeza de se preparar para obter sucesso. Este checklist ajudará você a avaliar seus fornecedores, otimizar seu plano de implantação e mitigar riscos potenciais.

Melhores Práticas

- [ ] Tenho um plano de estratégia de cybersecurity adequada?
- [ ] Avaliei a cybersecurity no escopo do meu sistema de segurança física?
- [ ] Realizei uma avaliação de vulnerabilidade para identificar lacunas que podem ser eliminadas por meio da convergência de segurança física e cybersecurity?
- [ ] Realizei uma avaliação de vulnerabilidade completa de todos os dispositivos de segurança física conectados para identificar modelos e fabricantes suspeitos?
- [ ] Estou usando apenas produtos originais e evitando produtos falsificados e não licenciados?

Gestão de riscos

- [ ] Tenho uma estratégia abrangente de gestão de risco?
- [ ] Criei novos protocolos de linha de base para orientar as operações de segurança e o gerenciamento de incidentes?
- [ ] Minhas equipes de TI e segurança física estão alinhadas com um programa de segurança abrangente?
- [ ] Identifiquei todos os usuários que podem acessar dispositivos e sistemas físicos de segurança?
- [ ] Uso dispositivos de borda de fabricantes confiáveis?
- [ ] Tenho uma política e procedimento para gerenciamento de violação?
- [ ] Preciso de seguro cibernético?
- [ ] Tenho um plano para fazer backup de meus dados importantes e protegê-los contra desastres?
- [ ] Como faço para garantir que meu sistema esteja disponível quando eu precisar dele?

Certificações e regulamentações

- [ ] Quais normas, diretrizes ou estruturas de proteção de dados se aplicam à minha situação específica?
- [ ] Avaliei o que precisamos fazer para estar em compliance com o GDPR, NIS2, PIPEDA ou outras normas e diretrizes de proteção de dados aplicáveis?
- [ ] As soluções consideradas incluem alguma certificação internacional ou relevante?
- [ ] A arquitetura da solução está alinhada com os padrões de compliance específicos da indústria e também oferece suporte aos padrões de compliance da autoridade reguladora relevante (ISO 27001)?
- [ ] As soluções escolhidas vêm com ferramentas e recursos que podem ajudar atender ao compliance regulamentar e manter as melhores práticas de cybersecurity?
- [ ] Há evidências que possam ser fornecidas de que foi feito um mapeamento de due diligence de normas e padrões para controles/arquitetura/processos?

Avaliação do fornecedor

- [ ] O fornecedor tem notificações que avisam sobre a hora da manutenção ou outros eventos que exigem que um sistema seja colocado off-line ou reinicializado?
- [ ] O fornecedor tem notificações para quando o sistema deve ser colocado offline?
- [ ] Quão transparentes são os fornecedores sobre vulnerabilidades cibernéticas?
- [ ] O fornecedor tem e está disposto a compartilhar um plano documentado de resposta a incidentes de segurança?
- [ ] O fornecedor possui uma estratégia abrangente para eliminar falhas e vulnerabilidades de segurança?
- [ ] O fornecedor prioriza cybersecurity no desenvolvimento de seus produtos?
- [ ] Quem é responsável se o seu equipamento for usado para acessar informações privadas?
- [ ] Quem são os responsáveis pela empresa que fabrica seu software e hardware?
- [ ] O fornecedor contrata auditores terceirizados e realiza testes de penetração para identificar e solucionar falhas de segurança?
- [ ] O fornecedor possui certificações de órgãos reguladores e associações internacionais e adere aos padrões de segurança da informação?
- [ ] Eles avaliam e selecionam cuidadosamente os parceiros para garantir os mais altos níveis de cybersecurity e compliance?
- [ ] Quão estável e estabelecido é o fornecedor? Há evidências de que podemos confiar nesse fornecedor e de que ele continuará a oferecer suporte e desenvolver a solução no futuro?

Dispositivos e serviços na nuvem

- [ ] Como estou me certificando de que meus dispositivos de segurança estão configurados de forma segura?
- [ ] Tenho um antivírus e um antimalware especializados protegendo meus dispositivos de borda e dispositivos de segurança?
- [ ] A solução de nuvem foi criada e testada tendo em mente a privacidade e proteção de dados?
- [ ] Vem com defesas integradas de cybersecurity e proteção de privacidade padrão para me ajudar a melhorar a mitigação de riscos e compliance regulamentar?
- [ ] Meu provedor de nuvem está garantindo a segurança e governança dos meus dados?
- [ ] O provedor de serviços na nuvem tem a capacidade de restringir o armazenamento de nossos dados a países ou localizações geográficas específicas?
- [ ] Os dados trocados e armazenados na nuvem estão totalmente protegidos?
- [ ] A infraestrutura de hospedagem passou por uma auditoria SOC 2 Tipo 2?
- [ ] O provedor de serviços na nuvem garante que os patches de segurança mais recentes sejam aplicados aos sistemas operacionais/ativos/aplicações em tempo hábil?
- [ ] O provedor de serviços na nuvem consegue isolar nosso ambiente/dados dos ambientes/dados de outros clientes?
- [ ] O fornecedor de nuvem tem um plano para devolver ou destruir os dados no encerramento da relação comercial?
- [ ] Qual é o histórico da solução na nuvem em termos de confiabilidade e tempo de atividade, e quais medidas estão em vigor para backup e recuperação de desastres?

Checklist de implantação

Pronto para implantar seu novo sistema de segurança física? Siga este checklist para monitorar seu upgrade ou instalação, mitigar riscos e garantir uma implantação tranquila.

Melhores Práticas

- [ ] Treinei meus colaboradores adequadamente sobre as melhores práticas de cybersecurity?
- [ ] Eu monitoro e compartilho informações sobre ameaças cibernéticas atuais e tendências no setor e incentivo a colaboração em ações e respostas preventivas?
- [ ] Tenho um inventário atualizado de todos os ativos de segurança física e IoT?

Proteção de dados

- [ ] Os dados multimídia armazenados em meu sistema são protegidos?
- [ ] Os dados multimídia são protegidos quando transferidos no meu sistema?
- [ ] Os dados de comando e controle são protegidos?
- [ ] Implementei criptografia de ponta a ponta?
- [ ] Como minhas chaves de criptografia são gerenciadas?
- [ ] Estou aproveitando todos os mecanismos internos disponíveis para garantir a integridade dos dados e evitar modificações ou adulterações não autorizadas?

Segurança do dispositivo

- [ ] Meu vídeo, controle de acesso, hardware de reconhecimento de placas de veículos e outros dispositivos de segurança física estão protegidos?
- [ ] Mantenho informações detalhadas sobre cada dispositivo de segurança física, por exemplo, fabricante e versão de firmware?
- [ ] Tenho um inventário atualizado de todos os dispositivos conectados à rede?
- [ ] Tenho um plano para substituir dispositivos não protegidos?
- [ ] Eu sei como identificar e usar os vários recursos de criptografia e cybersecurity compatíveis com cada dispositivo ou versão de firmware?
- [ ] Meu software de controle de acesso e vídeo está atualizado, juntamente com os dispositivos e servidores usados para armazenar dados e hospedar consoles de monitoramento?
- [ ] Qual é a minha estratégia para corrigir o firmware do meu dispositivo imediatamente?

Autenticação e autorização

- [ ] Estou gerenciando as senhas corretamente?
- [ ] Estabeleci uma política e um processo para gerenciamento do ciclo de vida de credenciais?
- [ ] Troquei todos os nomes de usuário e senhas padrão?
- [ ] Estou usando senhas fortes para acessar meu sistema de segurança e todos os dispositivos conectados?
- [ ] Implementei várias formas de autenticação para impedir o acesso não autorizado?
- [ ] Implementei uma estratégia de várias camadas que inclui autenticação multifatorial e autorizações de usuário definidas para reforçar a segurança do acesso dos usuários aos sistemas?
- [ ] Centralizo ao máximo o gerenciamento de identidades para todos os meus sistemas de segurança?
- [ ] Tenho alguma proteção contra ataques de força bruta para descobrir senhas?
- [ ] Configurei meus grupos de usuários corretamente e atribuí permissões às pessoas certas?
- [ ] Estamos usando ferramentas que suportam o gerenciamento de acesso baseado em funções?
- [ ] Tenho alguma proteção para restringir o acesso do usuário após inatividade prolongada?
- [ ] Os usuários autorizados têm acesso somente ao que de fato precisam?
- [ ] Estamos aplicando o princípio de privilégio mínimo na concessão de acesso?

Pós-implantação

Depois que sua implantação estiver concluída, o trabalho não termina aí. Esta lista de verificação irá ajudá-lo a monitorar a integridade do seu sistema, checar sua postura de cybersecurity e planejar ações preventivas para manter seu sistema funcionando livre de problemas.

Manutenção e atualizações

- [ ] Tenho ferramentas para manter meus dispositivos e software de segurança física atualizados?
- [ ] Estou atento às atualizações críticas de segurança para meus sistemas in loco?
- [ ] Confirmei a origem e a legitimidade de cada atualização de software e firmware antes da instalação?
- [ ] Verifiquei o inventário do dispositivo em relação às informações publicadas sobre fabricantes e modelos que identificaram riscos de segurança?
- [ ] Tenho um plano para melhorar o design da rede conforme necessário para segmentar dispositivos mais antigos e reduzir possíveis ataques cruzados?
- [ ] Estou aplicando patches e hotfixes de software adequados?
- [ ] Mantenho adequadamente meu ecossistema do Windows?
- [ ] Tenho as ferramentas adequadas para manter tudo atualizado e ciberneticamente seguro?
- [ ] Como posso manter minha lista de usuários atualizada?
- [ ] Tenho ferramentas para automatizar minha manutenção?
- [ ] Como mantenho o sistema operacional dos meus dispositivos de segurança atualizados?
- [ ] Tenho ferramentas para analisar quais usuários têm acesso aos nossos sistemas, aplicações e dados e atualizar os privilégios dos usuários?

Monitoramento de integridade e gerenciamento de riscos

- [ ] Tenho as ferramentas adequadas para monitorar o status dos meus sistemas e dispositivos?
- [ ] Consigo monitorar de forma centralizada o status e integridade de várias implantações?
- [ ] Os alertas automáticos estão configurados para eventos e limites críticos?
- [ ] Estou mantendo uma cadeia de custódia?
- [ ] Estou realizando análises de registros de trilha de auditoria ou automatizando relatórios sobre ações do usuário, eventos do sistema e tentativas de acesso?
- [ ] Estou sempre atento a novas ameaças e vulnerabilidades?
- [ ] Tenho técnicas de análise de logs para investigar em caso de um incidente cibernético?

Monitore a integridade do seu sistema Genetec com confiança

A equipe de Serviços Profissionais da Genetec pode ajudá-lo a verificar sua postura de cybersecurity e compartilhar medidas preventivas para manter seu sistema funcionando com eficiência.

Descubra como nossos especialistas em segurança podem ajudar

A Genetec Inc. é uma empresa de tecnologia que oferece soluções in loco e hospedadas na nuvem que abrangem 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 e serviços hospedados na nuvem, projetados para melhorar a segurança nas comunidades em que vivemos.

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

ATUALIZADO: 18-09-2024