Checklist de cybersecurity

Todos os dias, os cibercriminosos encontram novas e sofisticadas formas de capitalizar em cima de vulnerabilidades. O aumento do trabalho remoto, dispositivos conectados e dados, amplificaram os riscos de cybersecurity. Em nosso Relatório sobre o Estado da Indústria de Segurança Física de 2021, 52% dos entrevistados afirmaram que a vulnerabilidade de cybersecurity foi o principal desafio enfrentado por sua organização.

É por isso que uma estratégia abrangente de cybersecurity é crucial em cada etapa do seu processo de implantação de segurança física. Aqui estão três checklists para ajudar a fortalecer sua postura de cybersecurity antes, durante e após a implantação.

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

- [ ] Eu tenho um plano para uma estratégia de cybersecurity adequada?
- [ ] Avaliei a cybersecurity no escopo do meu sistema de segurança?
- [ ] Realizei uma avaliação de vulnerabilidade para identificar lacunas que podem ser fechadas 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 genuínos e evitando falsificações e produtos não licenciados?
- [ ] Além do aspecto técnico, existem outras coisas a considerar para ajudar a mitigar os riscos?

Gestão de riscos

- [ ] Tenho uma estratégia abrangente de gestão de risco estabelecida?
- [ ] Criei uma nova linha de base para orientar as operações de segurança e gestão 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?
- [ ] Estou usando 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 posso garantir que meu sistema esteja disponível quando eu precisar?

Certificações e regulamentações

- [ ] As soluções consideradas incluem as certificações necessárias?
- [ ] Qual regulamentação ou estrutura de proteção de dados se aplica à minha situação específica?
- [ ] Avaliei o que fazer para estar em compliance com o GDPR?
- [ ] Avaliei o que fazer para estar em compliance com o PIPEDA?

Avaliação do fornecedor

- [ ] O fornecedor possui documentação e ferramentas para ajudar na implementação de cybersecurity?
- [ ] O fornecedor tem notificações para quando o sistema deve ser colocado offline?
- [ ] Quão transparentes são os fornecedores sobre vulnerabilidades cibernéticas?
- [ ] 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 é o dono da empresa que constrói seu software e hardware?

Dispositivos e serviços na nuvem

- [ ] Como posso ter certeza de que meus dispositivos de segurança estão configurados com segurança?
- [ ] Tenho um antivírus especializado protegendo meu sistema de segurança?
- [ ] Estou escolhendo soluções de nuvem seguras?
- [ ] Meu provedor de nuvem está garantindo a segurança e hospedagem dos meus dados?
- [ ] Os dados trocados e armazenados na nuvem estão totalmente protegidos?

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

- [ ] Já treinei adequadamente meus colaboradores sobre as melhores práticas de TI?
- [ ] Eu monitoro e compartilho informações sobre ameaças cibernéticas atuais e tendências no setor e incentivo a colaboração em ações e respostas preventivas?
- [ ] Mantenho um inventário de todos os bens?
- [ ] 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?

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?
- [ ] Preciso de algo mais robusto do que um único fator para impedir o acesso não autorizado?
- [ ] Implementei uma estratégia multicamada que inclui autenticação de acesso multifator e autorizações de usuário definidas para fortalecer 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?
- [ ] Tenho alguma proteção para restringir o acesso do usuário após inatividade prolongada?
- [ ] Os usuários autorizados têm acesso somente ao que de fato precisam?

Segurança do dispositivo

- [ ] Minhas câmeras são protegidas?
- [ ] Mantenho informações detalhadas sobre cada dispositivo de segurança física, por exemplo, fabricante e versão de firmware?
- [ ] Tenho um inventário atualizado de todas as câmeras e sistemas de controle conectados à rede?
- [ ] Tenho um plano para a substituição de dispositivos não protegidos?
- [ ] Tenho um plano que permite identificar os tipos de criptografia e recursos de cybersecurity suportados em cada dispositivo ou versão de firmware e posso usá-lo?
- [ ] Meu hardware de controle de acesso está protegido?
- [ ] Confirmei que meu software VMS e ACS está atualizado junto com os dispositivos e servidores usados para armazenar dados e hospedar consoles de monitoramento?
- [ ] Meus dispositivos de reconhecimento de placas de veículos são protegidos?
- [ ] Qual é a minha estratégia para corrigir o firmware do meu dispositivo imediatamente?

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 atualizados?
- [ ] Estou sempre atento a atualizações críticas de segurança?
- [ ] Verifiquei a origem e legitimidade de cada atualização de software 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 os patches e hotfixes de software adequados?
- [ ] Estou mantendo adequadamente meu ecossistema do Windows?
- [ ] Tenho as ferramentas adequadas para manter tudo atualizado e ciberneticamente seguro?
- [ ] Como mantenho minha lista de usuários atualizada?
- [ ] Tenho ferramentas para automatizar minhas atividades de manutenção?
- [ ] Como mantenho o sistema operacional dos meus dispositivos de segurança atualizados?
- [ ] Tenho ferramentas para revisar e atualizar todos os privilégios de usuário?

Monitoramento de integridade e gerenciamento de riscos

- [ ] Tenho as ferramentas adequadas para monitorar o status dos meus sistemas e dispositivos?
- [ ] Tenho a capacidade de monitorar o status e a integridade de várias implantações?
- [ ] Estou mantendo uma cadeia de custódia?
- [ ] Estou sempre atento a novas ameaças e vulnerabilidades?
- [ ] Tenho técnicas de análise de log 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 checar 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/locations
info@genetec.com
@genetec

ATUALIZADO: 23-09-2022