E-BOOK

CIBERSEGURANÇA

A chave para a sobrevivência do **agronegócio**

SUMÁRIO

SUMÁRIO

A crescente ameaça dos grupos de ransomware durante os períodos de colheita e plantio fez com que a segurança cibernética se tornasse uma preocupação crítica no mundo do agronegócio. **Mais de 320 incidentes foram registrados no setor só em 2023**, segundo um levantamento feito pela ISH e SafeLabs, ressaltando essa urgência.

Os dados coletados ao longo dos anos pela agência de segurança nacional dos EUA indicam um notável aumento nos ataques de sequestro virtual direcionados a essas áreas específicas durante essas janelas temporais críticas.

Neste e-book, vamos abordar de forma abrangente as razões pelas quais a cibersegurança se tornou uma prioridade no setor agrícola.

Vamos falar sobre as ameaças em constante evolução que enfrentam as empresas agrícolas, fazendas e organizações relacionadas, bem como as melhores práticas e estratégias para proteger suas atividades, dados e infraestrutura contra esses ataques.

Para quem atua no setor, é fundamental entender o cenário atual da cibersegurança no agronegócio e tomar medidas proativas para garantir a continuidade e a segurança das operações nesse setor essencial.

1. SEGURANÇA NO PERÍODO DA COLHEITA

A agricultura, em sua essência, é uma atividade delicada e altamente dependente de fatores externos, como condições climáticas e prazos estritos para o plantio e colheita.

Por isso, é importante entender sobre a **segurança cibernética durante o período da colheita no contexto do agronegócio**, onde o fator tempo se torna crítico. Veja, a seguir, algumas informações relevantes.

1.1. AGRICULTURA E PERECIBILIDADE DE PRODUTOS

O agronegócio é intrinsecamente ligado a produtos perecíveis. Sejam eles frutas, vegetais, grãos ou carne, a qualidade e prazo de entrega desempenham um papel fundamental no sucesso dessa indústria.

Qualquer atraso na colheita ou na distribuição dos produtos pode resultar em perdas substanciais.

Os ataques cibernéticos direcionados a sistemas agrícolas podem impactar diretamente a **eficiência operacional e o cumprimento de prazos.**

Além disso, a interrupção dos sistemas de monitoramento e controle automatizados pode levar a **perdas de safra**, afetando a economia e a segurança alimentar.

1.2. TEMPO COMO UM FATOR CRÍTICO

O tempo é um **recurso não renovável, principalmente na agricultura**. Existem janelas específicas durante o ano em que a semeadura, a fertilização e a colheita são mais apropriadas.

Qualquer atraso durante essas fases essenciais pode prejudicar a produtividade e a qualidade dos produtos.

Os cibercriminosos estão cientes dessa vulnerabilidade temporal. Sendo assim, os ataques cibernéticos podem interromper a programação de operações agrícolas, causando atrasos, perdas e, em casos extremos, **a inviabilização de todo um ciclo produtivo**.

1.3. MECANIZAÇÃO E DIGITALIZAÇÃO

A modernização da agricultura trouxe avanços significativos, incluindo a mecanização e a digitalização de processos. Máquinas autônomas, sistemas de irrigação automatizados, sensores de monitoramento e softwares de gerenciamento são componentes importantes da agricultura contemporânea.

No entanto, essa digitalização também abre portas para ameaças cibernéticas. Se esses sistemas forem comprometidos, as implicações podem ser devastadoras.

Uma colheitadeira autônoma hackeada, por exemplo, pode colher no **momento errado ou danificar colheitas**. A cibersegurança no período da colheita no agronegócio é mais do que uma preocupação teórica; **é uma necessidade iminente.**

2. CIBERSEGURANÇA E MAQUINÁRIO AGRÍCOLA

A modernização da agricultura trouxe uma revolução tecnológica que viu a integração de máquinas agrícolas avançadas com redes de comunicação de alta velocidade, incluindo a tecnologia 5G.

Essa convergência oferece uma série de benefícios notáveis para o setor, **como a agricultura de precisão**, onde o sensoriamento e monitoramento inteligente de plantações se tornam realidade. Veja mais informações:

2.1. A AGRICULTURA DE PRECISÃO E O POTENCIAL DO 5G

O uso do 5G em máquinas agrícolas potencializa a agricultura de precisão de maneiras sem precedentes. Essa tecnologia oferece velocidades de comunicação ultrarrápidas e latência mínima, permitindo a coleta de dados em tempo real e a tomada de decisões instantâneas.

Sensores avançados instalados em máquinas agrícolas podem coletar informações, como detalhamento sobre o solo, condições climáticas, saúde das plantas e muito mais. Esses dados são então transmitidos para sistemas de análise que ajudam os agricultores a otimizar o uso de recursos, como água, fertilizantes e pesticidas.

2.2. AMEAÇAS À SEGURANÇA CIBERNÉTICA

Embora a integração de tecnologia 5G e máquinas agrícolas traga inúmeros benefícios, ela também apresenta riscos significativos de segurança cibernética. As ameaças vão desde ataques direcionados a máquinas agrícolas e sistemas de gerenciamento até a interceptação de dados críticos.

Hackers podem acessar e controlar máquinas remotamente, causando danos físicos, interrompendo operações e até mesmo ameaçando a segurança dos trabalhadores no campo.

2.3. PROTEGENDO O MAQUINÁRIO AGRÍCOLA

As medidas de proteção do maquinário agrícola podem incluir:

implementação de firewalls;

aplicação de sistemas de detecção de intrusões em máquinas;

a criptografia de dados transmitidos;

a autenticação rigorosa de usuários autorizados.

Além disso, a conscientização e a capacitação dos operadores das máquinas são relevantes para prevenir ações que possam comprometer a segurança.

Em resumo, podemos dizer que a integração da tecnologia 5G em máquinas agrícolas está transformando a forma como a agricultura é conduzida, impulsionando a eficiência e a produtividade. No entanto, essa revolução tecnológica traz consigo o desafio crítico da segurança cibernética. Proteger o maquinário agrícola é fundamental para garantir a continuidade das operações e a segurança dos dados.

3. INFRAESTRUTURA DE TI NAS FAZENDAS: COMO INVESTIR?

No cenário atual do agronegócio, a incorporação de tecnologias de ponta e infraestrutura de TI nas fazendas é essencial para otimizar a produção e a eficiência.

A agricultura moderna se beneficia da Inteligência Artificial (IA), que permite a agricultura de precisão, melhorando o monitoramento e a gestão de plantações, animais, inventário e relacionamento com clientes. No entanto, essa integração de alta tecnologia também introduz desafios significativos em termos de segurança cibernética e proteção de dados.

3.1. AMEAÇAS CIBERNÉTICAS E PROTEÇÃO DE DADOS

O agronegócio lida com volumes substanciais de dados, desde informações sobre colheitas e gado até detalhes de clientes e estoque. Esse cenário de dados valiosos torna o setor um alvo atraente para ameaças cibernéticas.

Proteger essas informações críticas é essencial, não apenas para a continuidade das operações, mas também para o cumprimento das regulamentações específicas do setor agrícola.

3.2. PARCERIAS E REGULAMENTAÇÕES NO AGRONEGÓCIO

Uma abordagem proativa para a segurança cibernética no agronegócio envolve a criação de parcerias com especialistas em segurança e o cumprimento das regulamentações relevantes.

Os agricultores e fazendeiros devem atuar com empresas especializadas em segurança cibernética para avaliar e fortalecer sua infraestrutura de TI.

3.3. SOLUÇÕES PARA SEGURANÇA CIBERNÉTICA

A infraestrutura de TI nas fazendas está cada vez mais conectada a sistemas de controle automatizados, drones, sensores e dispositivos IoT.

Nesse contexto, a aplicação da **Tríade de Visibilidade do Vision** pode ser uma estratégia eficaz para mitigar ameaças cibernéticas. Tal metodologia se divide em:

Gerenciamento de Detecção e Resposta (SIEM/MDR): envolve a criação de uma visão de longo alcance do ambiente digital, com monitoramento contínuo e detecção avançada de ameaças. Ele detecta ataques antes que causem danos, investiga incidentes e aplica políticas personalizadas para fortalecer a segurança;

Detecção e Resposta em Endpoints (EDR): fornece alta visibilidade em todos os endpoints do parque tecnológico, detectando ameaças potenciais por meio de machine learning e análise comportamental, oferecendo respostas a incidentes;

Detecção e Resposta em Redes (NDR): realiza a detecção no tráfego de rede com base na análise de protocolos e conteúdo transferido, extraindo arquivos de seções monitoradas.

Além dessas ferramentas, é importante integrar uma solução eficaz de OT (Tecnologia Operacional), como o Vision OT. Ele oferece funcionalidades projetadas para melhorar a segurança cibernética em infraestruturas críticas e ambientes industriais, como:

Visibilidade de Ativos e Rede: permite a descoberta automática e o gerenciamento de inventário de ativos de OT, IoT e TI, fornecendo visibilidade completa da rede e dos dispositivos conectados, o que é essencial para entender o ambiente operacional e identificar possíveis vulnerabilidades;

Detecção de Ameaças e Resposta: utiliza tecnologias avançadas, incluindo inteligência artificial, para detectar ameaças e anomalias em tempo real, proporcionando uma resposta rápida a incidentes cibernéticos e ajudando a mitigar riscos antes que possam causar danos significativos;

Gestão de Vulnerabilidades e Riscos: ajuda na identificação e priorização de vulnerabilidades nos ativos de OT e IoT, facilitando a gestão de riscos e a implementação de medidas de segurança adequadas para a proteção contra ataques cibernéticos;

Monitoramento Contínuo da Rede: fornece monitoramento contínuo da rede para detecção comportamentos suspeitos e violações de segurança, permitindo uma vigilância constante sobre o ambiente;

Conformidade e Padrões de Segurança: auxilia na manutenção da conformidade com padrões e regulamentações de segurança relevantes, como ISA/IEC 62443, NERC CIP, NIS2 Directive, SEC Cybersecurity Rules e TSA Security Directives, garantindo que as práticas de segurança estejam alinhadas com as exigências do setor.

Empresas especializadas em cibersegurança podem facilitar a implementação, otimização e gerenciamento da solução de segurança, garantindo que se possam maximizar o valor e a eficácia de estratégias de segurança cibernética em OT e IoT.

Investir em segurança cibernética e infraestrutura de TI nas fazendas é uma parte crítica da modernização do agronegócio. Medidas como essas não apenas protegem os ativos e dados, mas também asseguram que a agricultura moderna seja capaz de operar eficazmente em um ambiente cada vez mais digital.

4. CONSCIENTIZAÇÃO E TREINAMENTO: O PAPEL DAS PESSOAS NA CIBERSEGURANÇA

Embora a tecnologia desempenhe um papel importante na cibersegurança do agronegócio, o elemento humano é igualmente fundamental para manter a proteção eficaz contra ameaças cibernéticas.

A conscientização e o treinamento das pessoas envolvidas no setor agrícola desempenham um papel central na prevenção de violações de segurança e na mitigação de riscos. Acompanhe algumas informações relevantes:

4.1. CONSCIENTIZAÇÃO CIBERNÉTICA

A conscientização cibernética é o primeiro passo para construir uma cultura de segurança nas fazendas e empresas agrícolas.

Os funcionários, dos operadores de máquinas agrícolas aos gerentes de TI, devem estar cientes das ameaças cibernéticas que enfrentam. Eles devem ser capazes de reconhecer sinais de possíveis ataques, como phishing, e entender como relatar incidentes de segurança.

4.2. TREINAMENTO E EDUCAÇÃO

O treinamento em segurança cibernética é fundamental para capacitar os profissionais do agronegócio a adotar práticas seguras. Isso inclui treinamentos sobre o uso adequado de sistemas de TI, senhas fortes, procedimentos de segurança de dados e comportamentos seguros online.

Além disso, as equipes de TI devem ser treinadas para lidar com detecção, resposta e recuperação de incidentes.

4.3. CULTURA DE SEGURANÇA

Uma cultura de segurança deve ser cultivada em todos os níveis da organização.

Os líderes e gerentes desempenham um papel fundamental ao estabelecer um exemplo de segurança cibernética, demonstrando a importância da proteção de dados e incentivando a comunicação aberta sobre possíveis ameaças.

4.4. TREINAMENTO CONTÍNUO

A cibersegurança é uma disciplina em constante evolução, com novas ameaças emergindo regularmente.

Portanto, o treinamento em segurança cibernética deve ser **contínuo**. As equipes de TI e os funcionários devem se manter atualizados sobre as últimas ameaças e melhores práticas em cibersegurança.

4.5. PROMOÇÃO DE UMA MENTALIDADE DE SEGURANÇA

É imprescindível que as pessoas no agronegócio entendam que a segurança cibernética é responsabilidade de todos. A proteção de dados e sistemas não é apenas um problema para a equipe de TI; é uma preocupação que **afeta toda a organização**.

A cibersegurança no agronegócio é uma **colaboração entre tecnologia e pessoas**. A conscientização e o treinamento desempenham um papel central na manutenção da segurança cibernética em fazendas e empresas agrícolas. Ao educar e capacitar os profissionais envolvidos, é possível reduzir o risco de ameaças cibernéticas e manter a integridade das operações no setor agrícola.

O agronegócio moderno é uma abordagem abrangente, que não apenas protege ativos digitais, mas também contribui para a sustentabilidade e o sucesso a longo prazo do agronegócio na era digital.

CONSTRUINDO UM AGRONEGÓCIO MAIS SEGURO E RESILIENTE

A agricultura moderna, impulsionada pela tecnologia, está sujeita a ameaças cibernéticas cada vez mais sofisticadas. Nesse sentido, a dependência de infraestrutura digital, maquinário agrícola conectado e sistemas de IA torna essencial a proteção eficaz dos dados e operações.

Desde o período crítico de colheita até a integração de maquinário agrícola de última geração e sistemas 5G, a segurança cibernética se tornou uma preocupação incontornável.

Além disso, a conscientização e o treinamento das pessoas são fundamentais para estabelecer uma cultura de segurança sólida nas fazendas e empresas agrícolas.

A ISH PODE AJUDAR A IMPLEMENTAR A MELHOR ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA PARA A SUA EMPRESA.

Entre em contato com nosso time de especialistas e conheça as melhores soluções de cibersegurança do mercado.