CONFIRA!

ATAQUES À CADEIA DE SUPRIMENTOS:

Por que agora e o que fazer?

AS CADEIAS DE SUPRIMENTOS ESTÃO MAIS VULNERÁVEIS DO QUE NUNCA

O QUE FAZER PARA PROTEGÊ-LAS?

Um terço das empresas monitora **menos de 75%** de sua superfície de ataque, e **quase 20%** acreditam que mais da metade de sua superfície é desconhecida. Com a dependência de fornecedores e terceiros, as empresas aumentaram, em alguns casos a perder vista, o tamanho da superfície digital e, por consequência, da complexidade em protegê-la.

Todos os serviços que precisam da internet para funcionar, são construídos em um ecossistema hierárquico de serviços e infraestruturas de terceiros. Mas, imagine que cada terceiro tem terceiros próprios, que têm terceiros próprios, e assim por diante. Isso significa que as vulnerabilidades de seus fornecedores e dos fornecedores de seus fornecedores muitas vezes se tornam as suas vulnerabilidades.

Essa é a realidade das cadeias de suprimento, ou Supply Chain, hoje. Existem várias razões pelas quais elas estão vulneráveis neste momento, e nós explicaremos melhor neste e-book. Mas, o que você precisa entender agora é que os atores de ameaças sabem que é mais fácil explorar profundamente uma vulnerabilidade dentro de uma cadeia de suprimentos do que atacar uma empresa pela porta da frente.

Assim, as cadeias de suprimentos são agora a superfície de ataque que mais cresce para a maioria das empresas.

Estima-se que, hoje de 50% a 60% de todos os ataques cibernéticos sejam perpetrados por terceiros.

Ataques recentes, como o da Solar Winds, demonstraram o que os hackers já entenderam há anos: que uma brecha em qualquer lugar da cadeia de suprimentos pode facilitar um comprometimento de serviços, usuários, clientes e arruinar a reputação de sua marca.

Por isso, preparamos esse material. Para ajudar você a adotar uma abordagem proativa na resolução das vulnerabilidades em toda a sua superfície de ataque externo — incluindo terceiros e além.

ATAQUES A CADEIA DE SUPRIMENTOS AMEAÇAM A CONTINUIDADE DE NEGÓCIOS PARA TODAS AS EMPRESAS

Violações cibernéticas não são estáticas; suas táticas e capacidades estão sempre evoluindo. **A cadeia de suprimentos está sob ataque como nunca. Listada entre as sete principais preocupações de segurança para 2022 pelo Gartner, a segurança de Supply Chain agora está no topo da mente para equipes de cibersegurança, CISOs e todo o C-Level.** Pela primeira vez, esses ataques estão ameaçando a continuidade de negócios para empresas de grande porte.

Os hackers frequentemente procuram portas e sistemas inseguros em sistemas industriais conectados à Internet. As cadeias de fornecimento de TI/OT/ICS em integração contínua são particularmente vulneráveis, pois oferecem aos atacantes muitos pontos de entrada. E os sistemas OT legados não foram projetados para proteger contra ataques cibernéticos.

Proteger sistemas críticos contra ameaças à segurança cibernética é, naturalmente, um esforço desafiador. Todos eles têm estruturas operacionais únicas, com pontos de acesso e uma variedade de sistemas legados e tecnologias emergentes. A explosão de dispositivos conectados também está tornando tudo mais complexo. Isso, combinado com um aumento nos sensores em rede, está criando oportunidades de ataque para hackers em todas as infraestruturas digitais.

Para mitigar ameaças e lidar com vulnerabilidades no contexto das cadeias de suprimentos, é preciso aplicar uma estrutura de risco abrangente que inclua segurança por design, defesa aprofundada e confiança zero.

DUAS DAS RAZÕES PELAS QUAIS AS CADEIAS DE SUPRIMENTOS DIGITAIS ESTÃO ESPECIALMENTE VULNERÁVEIS AGORA:

1. **Ataques da cadeia de suprimentos digitais** valem o investimento para hackers. A natureza da cadeia de suprimentos digital permite replicar uma única exploração, o que amplia uma rede de ataque. Isso aumenta exponencialmente a recompensa potencial do ataque e o ROI do desenvolvimento de exploração.

2. **A segurança do serviço em nuvem** muitas vezes cai em uma terra digital de ninguém. Os serviços de nuvem gerenciados pela SaaS ou PaaS operam em um modelo de responsabilidade compartilhada. Isso cria uma área cinza entre os fornecedores, dificultando a identificação de soluções tradicionais de segurança cibernética se um componente de terceiros foi adulterado.

CONFIRA:

4 AÇÕES PARA SEREM TOMADAS AGORA

1. REALIZAR DUE DILIGENCE EM FORNECEDORES

Ao contratar novos fornecedores, é importante realizar a devida diligência para garantir que eles atendam aos seus requisitos de proteção. Isso inclui revisar seus protocolos de segurança e garantir que eles estejam atualizados com os patches de correção mais recentes.

As auditorias de fornecedores podem ajudar a verificar se eles estão aderindo aos seus padrões de segurança e oferecem uma oportunidade valiosa para identificar possíveis pontos falhos em suas operações.

Além disso, a comunicação regular com os fornecedores sobre suas expectativas de segurança pode ajudar a garantir que eles permaneçam proativos em seus esforços para proteger seus dados.

Ao tomar essas medidas, você pode ajudar a garantir que seus relacionamentos com fornecedores sejam construídos em uma base de confiança e respeito mútuo.

2. IMPLEMENTAR A AUTENTICAÇÃO MULTIFATOR (MFA) PARA TODAS AS CONTAS, INCLUINDO AQUELAS USADAS PELOS FORNECEDORES

A autenticação multifator (MFA) é uma importante medida de segurança que deve ser implementada para todas as contas de uma empresa, incluindo aquelas usadas pelos fornecedores.

A MFA adiciona uma camada extra de proteção, exigindo que os usuários forneçam duas ou mais evidências para verificar sua identidade. Isso pode incluir algo que eles sabem (como uma senha), algo que eles têm (como um código gerado por um aplicativo de segurança) ou que eles são (como sua impressão digital).

Ao exigir várias formas de autenticação, com a MFA torna significativamente mais difícil para os cibercriminosos obterem acesso às contas. Como resultado, a implementação da MFA pode ajudar a proteger sua organização contra violações de dados e outras ameaças à segurança cibernética.

3. CRIPTOGRAFAR TODOS OS DADOS, TANTO EM REPOUSO QUANTO EM TRÂNSITO

Uma das maneiras mais eficazes de proteger informações em uma cadeia de suprimentos é criptografar todos os dados, tanto em repouso quanto em trânsito.

Quando os dados são criptografados, eles são transformados em um código que só pode ser descriptografado por usuários autorizados. Isso significa que, mesmo que os dados sejam roubados, eles não serão úteis para os cibercriminosos, a menos que eles tenham a chave para descriptografá-los.

Isso torna muito mais difícil para os hackers acessarem e usarem quaisquer informações roubadas. Além disso, os dados criptografados são muito mais difíceis de falsificar, o que ajuda a evitar atividades fraudulentas.

Como resultado, criptografar todos os dados é uma etapa essencial para proteger empresas e consumidores.

4. IMPLEMENTE AUDITORIAS DE SEGURANÇA REGULARES E TESTES DE PENETRAÇÃO

Para manter um alto nível de segurança, é importante auditar regularmente seus sistemas e testar vulnerabilidades.

Internamente, isso significa ter uma equipe de especialistas em segurança que monitoram constantemente sua rede em busca de sinais de intrusão e testam seus sistemas a procura de pontos fracos.

Externamente, você também deve contratar os serviços de uma empresa de segurança para realizar testes periódicos de penetração. Isso ajudará a identificar possíveis vulnerabilidades em seu sistema antes que eles possam ser explorados por invasores.

Ao tomar essas precauções, você pode ajudar a garantir que seu sistema permaneça seguro contra o cenário de ameaças em constante evolução.

AÇÃO EXTRA:

AUTOMATIZE A DESCOBERTA DE ATIVOS:

Você não pode proteger o que não vê, então descubra proativamente o que está por aí em todas as camadas da Internet. Encontre e mapeie ativos externos, e leve em consideração os ativos não controlados que formam sua cadeia de suprimentos, não importa quão distantes estejam. Existem tecnologias para isso hoje.

Saiba mais aqui

CONTE COM UMA **PARCERIA ESPECIALIZADA** PARA PROTEGER A SUA EMPRESA

Como vimos, há várias maneiras para as empresas mitigarem o risco desses ataques cibernéticos caros e prejudiciais, como adoção de políticas seguras e eficazes.

Isso inclui a implementação de protocolos de segurança, a realização de due diligence ao buscar novos fornecedores, a criptografia de dados e a realização de auditorias de segurança regulares.

Além disso, também é importante atentar-se para a construção de relacionamentos sólidos com fornecedores e criar estratégias cada vez mais aprimoradas para que todo o processo de gerenciamento da cadeia de suprimentos seja feito de forma segura e protegida.

Ao tomar essas medidas, é fundamental que as corporações contem com a parceria de empresas especialistas em segurança cibernética para ajudar não só na proteção de dados, mas também de seus clientes e de sua cadeia de suprimentos contra os ataques maliciosos.

CONHEÇA A **ISH**

Nós cuidamos da segurança digital da sua empresa
para que você foque no crescimento do seu negócio!

Entre em contato com um de nossos especialistas
e saiba como usar inteligência em tempo real
para identificar e corrigir vulnerabilidades.

ACESSE

ISH.COM.BR/BLOG/