**Nicolas Gustavo Magrini Pereira**

**Segurança de Endpoint**

Como, cada vez mais, a necessidade de proteção de dispositivos aumenta, indo além de apenas computadores e laptops para uma ampla gama de dispositivos como smartphones e dispositivos IoT. É preciso que uma política mais rígida de proteção a estes endpoints entre em vigor para garantir que os ativos e dados corporativos permaneçam protegidos mesmo quando há o acesso remoto a eles.

Abaixo serão listadas e explicadas algumas práticas recomendadas de segurança de endpoint.

**Descoberta de ativos**

É o processo de identificar e catalogar todos os dispositivos que se conectam à rede, tanto os autorizados quanto os não. É um processo essencial para manter os endpoints visíveis e sob controle, assim como para avaliar os riscos e vulnerabilidades de cada um.

Para que estes ativos sejam descobertos, as empresas podem usar ferramentas automatizadas que escaneiam a rede de tempos em tempos, gerando relatórios que contenham informações, tais como nome, tipo, sistema operacional que estejam instalados nos dispositivos analisados. Estas ferramentas também podem alertar sobre mudanças repentinas nos endpoints, como dispositivos novos, perdidos ou até infectados.

**Criação de perfis de dispositivos**

Classifica e agrupa os dispositivos de acordo com suas funções. É um processo importante para aplicar as políticas de segurança adequadas à cada endpoint.

Para que estes perfis sejam criados, a empresa pode usar critérios como categoria, propriedade, localização, função, acesso etc.

**Segurança do dispositivo do usuário final**

É o conjunto de medidas que visam proteger os dispositivos contra ameaças externas e internas. São elas: uso de métodos de autenticação de multifatores; criptografia de dados; uso de VPNs; manter atualizados todos os sistemas e softwares; instalação de antivírus.

**Princípio do acesso de privilégio mínimo usando Zero Trust**

O princípio do acesso de privilégio mínimo é uma abordagem de segurança que consiste em conceder aos usuários e dispositivos apenas os direitos e permissões necessários para realizar suas tarefas, evitando o acesso excessivo ou indevido a recursos sensíveis. Esse princípio está relacionado ao conceito de Zero Trust, que é uma filosofia de segurança que não confia em nenhum usuário ou dispositivo por padrão, e exige a verificação contínua de sua identidade e comportamento.

Para a implementação desta prática, a empresa pode usar ferramentas como: gerenciamento de identidade e acesso; gerenciamento de configuração; gerenciamento de vulnerabilidades.

**Segurança do dispositivo IoT**

A segurança do dispositivo IoT é o conjunto de medidas que visam proteger os dispositivos conectados à internet das coisas, como os sensores, as câmeras, os termostatos ou as geladeiras. Esses dispositivos são cada vez mais usados nas empresas para coletar e transmitir dados, mas também são cada vez mais alvos de ataques cibernéticos, pois muitas vezes não possuem mecanismos de segurança adequados.

Algumas recomendações de uso devem ser seguidas, são elas: protocolos de comunicação seguros; uso de senhas fortes e únicas; uso de firewalls e redes separadas.

**Referências**

BERNARD**. As 5 Melhores Práticas de Segurança de Endpoints Para Manter os Dados Corporativos Seguros**. Disponível em: https://microhard.com.br/as-5-melhores-praticas-de-seguranca-de-endpoints-para-manter-os-dados-corporativos-seguros/. Acesso em: 30 set. 2023.