

A Whitelisting de Aplicações funciona?

O Que É a Whitelisting de Aplicações?

A whitelisting de aplicações é um conceito no qual existe uma lista de programas autorizados a funcionar, e tudo o resto não tem permissão para funcionar.

As tecnologias de whitelisting de aplicações mais avançadas combinam algum tipo de lógica de origem e destino. Por exemplo, uma whitelist de aplicações pode determinar: "O Bloco de Notas do Windows tem permissão para aceder à pasta Impostos no meu ambiente de trabalho, mas o Microsoft Word não tem."

Analisaremos isto com mais detalhe, mas, de forma genérica, as estratégias defensivas de whitelisting de aplicações dependem fortemente destas duas variáveis:

1. Os atacantes concordam em seguir as regras que definiu para eles no que diz respeito à sua ferramenta de cibersegurança de whitelisting de aplicações.
2. O seu ambiente é muito pequeno, com poucas aplicações que permanecem bastante estáveis e sem explorações (exploits).

Desvantagens das Tecnologias de Whitelisting de Aplicações

Complexidade

As Redes de TI São Como Organismos Complexos

Mesmo as pequenas redes de TI são entidades em constante mudança, com uma miríade de comportamentos. As aplicações são constantemente adicionadas e removidas pelos utilizadores.

Os módulos dentro das aplicações são constantemente adicionados e removidos pelos criadores dos programas, especialmente aquando de atualizações. Por último, os comportamentos das aplicações, além das alterações no código que resultam em alterações de comportamento, são utilizados de formas diferentes por diferentes utilizadores em diferentes momentos. Agora imagine a equipa que teria de acompanhar isso constantemente, e os pedidos de suporte de TI que teriam de chegar continuamente.

Realisticamente, o único ambiente de TI estável é aquele orientado por quiosques, no qual os programas são instalados sem possibilidade de atualização, adição ou remoção, e os utilizadores estão estritamente limitados a executar apenas uma ou duas funções. Talvez um quiosque para impressão de fotografias, ou algo semelhante. Nesse caso, a whitelisting de aplicações só precisaria de ser atualizada sempre que o terminal do quiosque fosse atualizado, talvez duas vezes por ano.

Whitelists de Aplicações Mais Avançadas Significam Mais Complexidade

As whitelists de aplicações mais simples têm apenas listas de programas autorizados a existir no sistema de um utilizador.

Isto, por si só, pode ser difícil de gerir, mas conduz a uma série de melhorias potenciais.

Por exemplo, só porque o departamento de processamento de salários tem uma aplicação para interagir com o sistema de salários da empresa, não deveria existir um conjunto separado de regras para a equipa do armazém, que utiliza aplicações diferentes (não relacionadas com salários)?

Assim, as melhorias relacionadas com quais divisões ou utilizadores podem executar quais aplicações constituem uma melhoria óbvia. Uma melhoria que, agora, criou complexidade adicional, além de apenas acompanhar o número, tipo e versões dos programas existentes na sua rede.

Agora, digamos que precisamos de outro conjunto de melhorias - precisamos de decidir qual utilizador tem acesso a qual aplicação, para qual conjunto de dados.

Isso também faz todo o sentido, certo? Não quer que a sua equipa de armazém tenha acesso aos registos de Recursos Humanos, e a equipa de Recursos Humanos provavelmente não precisa de acesso aos dados operacionais da equipa de entregas do armazém.

Trata-se de um conjunto de combinações absurdamente complexo de acompanhar, agora que a localização dos dados foi acrescentada como variável.

Assim - com cada melhoria necessária para tornar as tecnologias de whitelisting de aplicações eficazes, a gestão, configuração e o suporte contínuo (poder-se-ia dizer, interminável e sempre

crescente) necessário para as manter funcionais torna a tecnologia impraticável. O resultado é, normalmente, que grandes grupos de utilizadores recebem acesso a grandes grupos de aplicações e, provavelmente, a quase todos os dados. Ou seja - uma configuração praticamente inútil da tecnologia, porque nenhuma empresa dispõe dos recursos necessários para a manter devidamente gerida.

As Aplicações Interagem Entre Si

É comum, nos sistemas operativos modernos, que as aplicações interajam com outras aplicações. Por vezes, a interação deve-se a uma integração entre duas aplicações que melhora a experiência do utilizador - como um documento do Word que abre o Microsoft Photos. Noutras ocasiões (o que é muito comum), existem chamadas entre programas que são efetuadas de uma forma tipicamente invisível para o utilizador final.

Revision #1

Created 2026-07-24 05:38:09 UTC by Dennis Underwood

Updated 2026-07-24 05:38:09 UTC by Dennis Underwood