Winov | Security Whitepaper

Última atualização em: 08/08/2022

O objetivo deste artigo é falar sobre as bases de segurança aplicáveis dentro da Winov. Ele oferece orientações e recomendações do nosso time de especialistas para que sua infraestrutura esteja segura e estável.

Introdução

A estrutura da Winov é totalmente projetada para ajudar você a entender e projetar as suas regras de segurança, dispondo de vários níveis de customização para se adequar a sua necessidade.

Este artigo fornece uma maneira de medir consistentemente sua carga de trabalho em relação às práticas recomendadas e identificar áreas de melhoria.

Com a intenção de descrever como aproveitar as tecnologias de nuvem da Winov para proteger dados, sistemas e ativos de uma forma que pode melhorar sua postura de segurança, este documento fornece informações detalhadas e práticas recomendadas de segurança para sua arquitetura.

Visão Geral da responsabilidade compartilhada

Segurança e conformidade são responsabilidades compartilhadas entre a Winov e o cliente. Esse modelo compartilhado pode auxiliar a reduzir os encargos operacionais do cliente à medida que a Winov opera, gerencia e controla os componentes do sistema operacional do host e a camada de virtualização, até a segurança física das instalações em que o serviço opera. O cliente assume a gestão e a responsabilidade pelo sistema operacional convidado (inclusive atualizações e patches de segurança), por outros softwares de aplicativos associados e pela configuração do

firewall do grupo de segurança fornecido pela Winov. Os clientes devem examinar cuidadosamente os serviços que escolherem, pois suas respectivas responsabilidades variam de acordo com os serviços utilizados, a integração desses serviços ao seu ambiente de TI e as leis e regulamentos aplicáveis.

A natureza dessas responsabilidades compartilhadas também oferece a flexibilidade e o controle do cliente necessários para a implantação. Como pode ser visto no gráfico abaixo, esta distinção entre responsabilidades é denominada normalmente como **segurança *"da"* nuvem** versus **segurança *"na"* nuvem**.

Responsabilidade da Winov | Segurança da nuvem

A Winov é responsável por proteger a infraestrutura que executa todos os serviços oferecidos na nuvem Winov. Essa infraestrutura é composta por hardware, software, redes e instalações que executam os Serviços de nuvem Winov.

Responsabilidade do Cliente | Segurança na nuvem

A responsabilidade do cliente será determinada pelos Serviços de nuvem da Winov contratados por ele. Isso determina a quantidade de operações de configuração que o cliente deverá executar como parte de suas responsabilidades de segurança. Por exemplo, um serviço como Servidor Virtual W2C é categorizado como IaaS (Infraestrutura como serviço) e, dessa forma, exige que o cliente execute todas as tarefas necessárias de configuração e gerenciamento da segurança.

Os clientes que implantam um servidor virtual da Winov são responsáveis pelo gerenciamento do sistema operacional convidado (o que inclui atualizações e patches de segurança), por qualquer utilitário ou software de aplicativo instalado pelo cliente nos servidores, bem como pela configuração do firewall disponibilizado pela Winov (chamado de grupo

de segurança) em cada servidor. Os clientes são responsáveis por gerenciar os dados deles (o que inclui opções de criptografia), classificando os ativos e usando as ferramentas para aplicar as permissões apropriadas.

Esse modelo de responsabilidade compartilhada entre o cliente e a Winov também se estende aos controles de TI. Assim como a responsabilidade para operar o ambiente de TI é compartilhada entre a Winov e os seus clientes, o mesmo ocorre com o gerenciamento, a operação e a verificação de controles compartilhados de TI. A Winov pode auxiliar a reduzir os encargos operacionais de controles do cliente gerenciando os controles associados à infraestrutura física implementada no ambiente da Winov que anteriormente eram gerenciados pelo cliente.

Como a Winov não tem visibilidade ou conhecimento sobre o que os clientes estão carregando em sua rede, incluindo se esses dados estão ou não sujeitos à LGPD, os clientes são essencialmente responsáveis por sua própria conformidade com a LGPD e com os regulamentos relacionados,

uma vez que a extensão do que a Winov pode regularizar conforme a Lei é a sua própria infraestrutura.

Um detalhe de extrema importância é que você é responsável pela gerência e alteração de suas senhas em nosso ambiente. Após a entrega da VM por parte da WINOV, a senha de acesso, que foi gerada randomicamente, não é salva, ficando a seu encargo administrá-la e alterá-la, caso ocorra uma perda dessa senha, a instância terá que ser recriada.

Regras disponíveis para aplicação

A Winov dispõe de diversos filtros e configurações aplicáveis para seu ambiente, cada um com sua característica e aplicabilidade.
Todos os filtros podem ser configurados e fica a seu encargo optar ou não pela utilização deles.

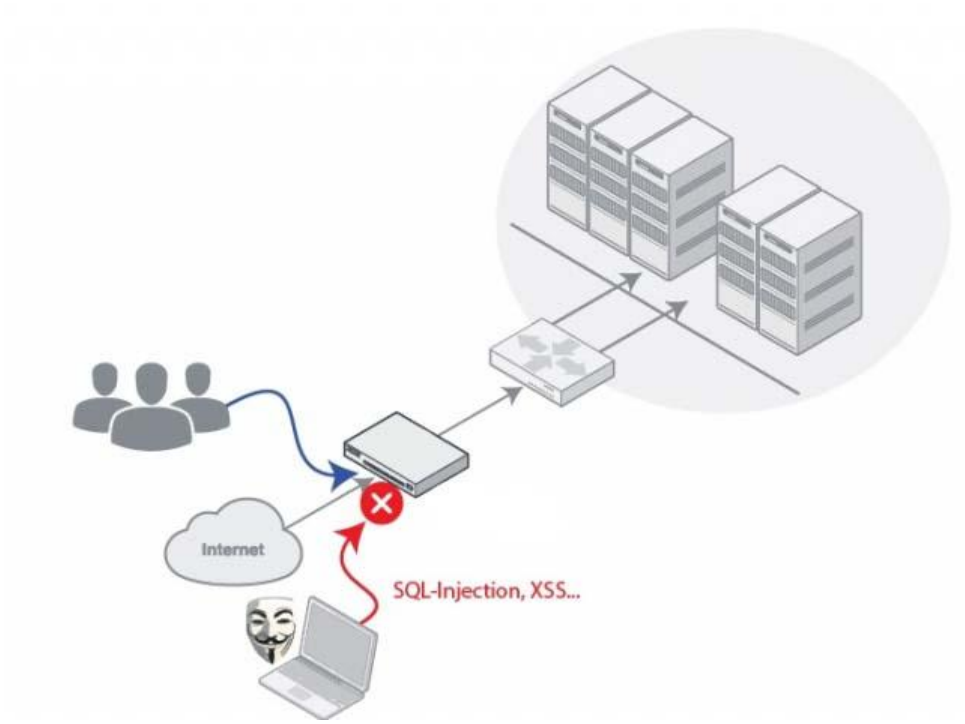
- WAF
- IPS
- AV de Borda
- Anti DoS
- Inspeção de Certificado (SSL)
- DNS Filter
- Botnet e categorias maliciosas
- GeoIP e Service Databases

WAF (Web Application Firewall)

São recursos avançados que defendem seus aplicativos da Web contra ameaças conhecidas e de dia zero.

Ele previne e bloqueia os ataques às aplicações web em tempo real, preservando as operações e minimizando o risco de vazamento de informações. Ele é capaz de identificar técnicas de invasão direcionadas

ao código da aplicação, como por exemplo, SQL Injection, XSS, entre outros.



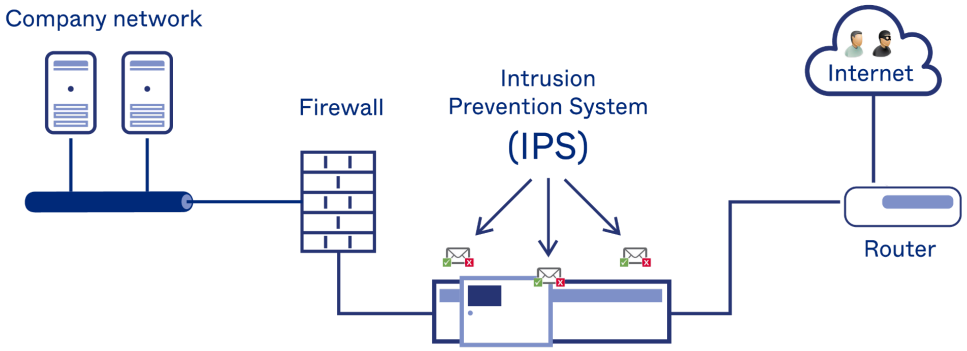
IPS (Intrusion Prevent System)

O IPS atua monitorando os pacotes que trafegam na rede, em busca de atividades suspeitas. Sua detecção é baseada em assinaturas e anomalias, que são atualizadas constantemente.

- Detecção baseada em anomalias
    - Leva em consideração amostras de tráfego de rede e realiza a comparação com um nível de desempenho pré-calculado. Quando as amostras estão fora do padrão, uma ação é tomada de acordo com os parâmetros informados.

- Detecção baseada em assinaturas
    - São assinaturas com visibilidade de vulnerabilidades no sistema direcionado. Essas assinaturas permitem uma proteção avançada contra as mais conhecidas ameaças, ataques

direcionados avançados de dia zero, ransomware, malware polimórfico, ataques distribuídos de negação de serviço, entre outros.



Antivírus de Borda

O AV Sandbox oferece uma poderosa combinação de detecção avançada, mitigação automatizada, percepção acionável e implantação flexível para interromper ataques direcionados e subsequente perda de dados

Anti DoS

O Anti DoS leva em consideração amostras de tráfego de rede e realiza a comparação com um nível de desempenho pré-calculado. Quando as amostras estão fora do padrão, uma ação é tomada de acordo com os parâmetros informados.

Inspeção de Certificado (SSL)

A inspeção SSL / TLS ou interceptação HTTPS é o processo de interceptar a comunicação criptografada SSL / TLS da Internet entre o cliente/servidor.

Junto com suas informações legítimas, o conteúdo malicioso também pode ser escondido no tráfego criptografado. E porque é criptografado, ele

passa despercebido pelos mecanismos de segurança comuns, o que significa que pode causar os danos que foi criado para causar.

DNS Filter

Você pode aplicar a filtragem de categoria DNS para controlar o acesso aos recursos da web.

A filtragem de DNS tem os seguintes recursos:

- Filtra a solicitação de DNS com base na classificação do domínio.
- Bloqueia a solicitação de DNS para os domínios de botnet conhecidos.
- Filtragem de domínio de categoria dinâmica externa

Botnet e categorias maliciosas

Você pode aplicar filtragens para que suas instâncias não sejam acessíveis para IPs contidos em listagens maliciosas.

Existem diversas categorias pré-mapeadas por nossos especialistas de segurança, que evitam acessos oriundos de IPs maliciosos já conhecidos pela internet, como por exemplo: tráfego vindos da rede Tor, Phishing, Shodan, entre outros.

GeoIP e Service Databases

É possível também a configuração para proteger uma instância contra ataques de países com os quais o usuário não tem relações comerciais.
Estudos feitos por nossos especialistas geraram algumas listagens de países que são os maiores vetores de ataques. Na maioria dos casos, você pode não ter relação comercial com eles, podendo assim, ampliar ainda mais seu nível de segurança

Existe a possibilidade de limitação de bloqueio/liberação por origens específicas, de acordo com a sua necessidade.

Conclusão

A segurança é um esforço contínuo. Quando ocorrem incidentes, eles devem ser tratados como oportunidades para melhorar a segurança da arquitetura.

A Winov se esforça para ajudar você a criar e operar os recursos de segurança que protegem informações, sistemas, ativos e assim entregar valor ao seu negócio.

Caso alguma dessas configurações faça sentido e você queira aplicá-las em sua estrutura, fale com um de nossos especialistas através das nossas plataformas de comunicação