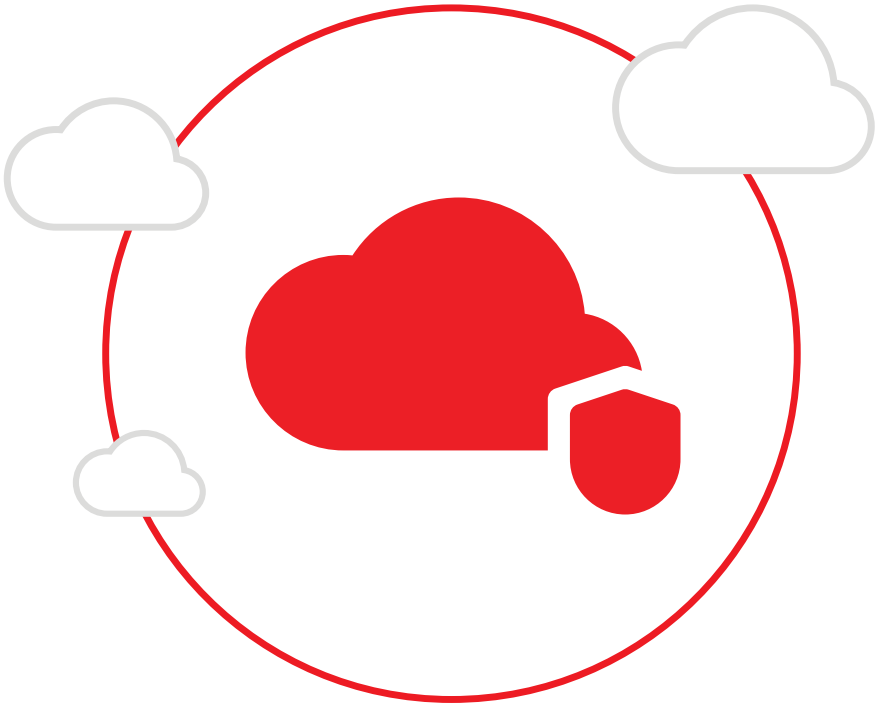
Red Hat



Aumente a segurança na nuvem híbrida

Proteja seus negócios com abordagens de segurança nativas em nuvem

Por Lucy Huh Kerner, evangelista e estrategista principal sênior de recursos técnicos globais de segurança, Red Hat

Conteúdo

Implante uma nuvem híbrida que tenha a segurança como prioridade

Hoje em dia, 94% das empresas usam algum tipo de nuvem e 58% têm uma estratégia de nuvem híbrida.[1] Nuvem híbrida é uma arquitetura de TI que incorpora alguns recursos de portabilidade de cargas de trabalho, orquestração e gerenciamento em dois ou mais ambientes conectados, porém distintos, incluindo de bare-metal, virtualizados e de nuvem privada ou pública. Com uma arquitetura de nuvem híbrida, você pode executar cargas de trabalho em qualquer um dos ambientes conectados, migrá-las de um ambiente para outro e usar recursos desses ambientes de maneira intercambiável.

As empresas adotam ambientes de nuvem híbrida para:

- Conectar infraestruturas, plataformas, aplicações e ferramentas de fornecedores diferentes.
- Aumentar a eficiência e a escalabilidade.
- Reduzir custos.
- Aumentar a agilidade.
- Otimizar a disposição dos dados.

Independentemente de onde sua empresa esteja na jornada para a nuvem híbrida, a segurança é de extrema importância. Na realidade, 81% das empresas afirmam que a segurança em nuvem é um desafio.[1] As vulnerabilidades de segurança na nuvem híbrida normalmente estão relacionadas à perda da capacidade de controlar e supervisionar recursos. Isso inclui o uso não autorizado da nuvem pública, falta de visibilidade dos recursos, controle inadequado de alterações, gerenciamento deficiente da configuração e controles de acesso ineficazes. Usuários não autorizados podem se aproveitar dessas falhas para acessar recursos internos e dados confidenciais.

As empresas podem pagar um preço caro pelas violações de segurança. Em média, o prejuízo resultante de uma violação de segurança gira em torno de US$ 3,92 milhões, sendo que 36,2% desse custo está associado à perda de negócios.[2] E as ameaças estão aumentando a cada dia que passa. A probabilidade de uma empresa sofrer uma violação de segurança nos próximos dois anos é de 29,6%.[2] Tanto o número de registros de dados quanto o tempo de identificação e contenção de tais violações, em média, aumentaram em 2019.[2]

Mesmo em face desses desafios, é possível implantar uma **nuvem híbrida que tenha a segurança como prioridade**. E uma das soluções para fazer isso é adaptar seus métodos para que as diferenças entre a arquitetura on-premise e de nuvem sejam levadas em consideração. Neste e-book, você descobrirá novas abordagens e ficará a par de algumas considerações sobre como proteger seus negócios na nuvem híbrida.

Impactos de uma segurança ineficaz

As violações de segurança custam caro e as ameaças estão aumentando a cada dia.

US$ 3,92 milhões
foi prejuízo médio causado por cada violação de dados em 2019.[2]

279 dias
foi o tempo em média que se levou para identificar e conter cada violação de dados em 2019.[2]

US$ 1,22 milhão
seria a economia de custos caso uma violação fosse identificada e contida em

200 dias
ou menos.[2]

29,6%
é a probabilidade de uma empresa sofrer uma violação dentro de dois anos.[2]

1 *Flexera, "RightScale 2019 State of the Cloud Report from Flexera", fevereiro de 2019.* info.flexerasoftware.com/SLO-WP-State-of-the-Cloud-2019.

2 *IBM Security, "2019 Cost of a Data Breach Report", 2019.* ibm.com/security/data-breach.

A segurança é um processo, não um produto

Para ter certeza da eficácia das medidas de segurança, é necessário adotar uma abordagem holística que incorpore pessoas, processos e tecnologias. Apenas implantar soluções e ferramentas dedicadas à segurança não é suficiente para proteger sua infraestrutura, nuvem ou empresa. É essencial implementar também processos e estratégias de segurança. Assim, você usa os recursos de suas soluções e reduz efetivamente os riscos de segurança. Além disso, é preciso continuar adaptando tais processos e estratégias com o passar do tempo, à medida que as tecnologias, ameaças e necessidades evoluem.

Os ambientes de nuvem híbrida exigem uma mudança em como as empresas abordam a segurança. Como tais ambientes não são delimitados por um perímetro físico, as abordagens de segurança tradicionais não são eficazes. Centralizar o gerenciamento de identidades e o controle de acesso é um fator fundamental nas abordagens de segurança voltadas para a nuvem. Para realizar essas tarefas de maneira centralizada e eficaz, é necessário usar o princípio do privilégio mínimo para conceder aos usuários apenas o acesso de que eles realmente precisam. Essa abordagem requer uma auditoria dos atuais direitos de acesso de cada usuário e, em seguida, uma reavaliação das necessidades de cada um para determinar o nível de acesso ideal.

Além disso, para que a nuvem híbrida fique de fato protegida, é preciso elaborar uma estratégia de segurança estratificada e detalhada que use os recursos de cada camada do ambiente, incluindo sistemas operacionais, plataformas de containers, ferramentas de automação, soluções de software como serviço (SaaS) e serviços em nuvem.

Sistema operacional

Busque ferramentas incorporadas que ajudarão você a assegurar a conformidade com as políticas de segurança, implementar medidas físicas de proteção, melhorar a segurança da rede, controlar o acesso de usuários, isolar processos e aumentar a segurança dos dados. Como exemplo, podemos citar OpenSCAP, USBGuard, firewalls, Security-Enhanced Linux® (SELinux), gerenciamento de identidades e criptografia de disco vinculada à rede (NBDE).

Plataforma de containers

Use recursos integrados à sua plataforma e o Kubernetes para aumentar a segurança de containers. Alguns exemplos são políticas de segurança de pods, controles de tráfego de rede, controles de entrada e saída de clusters, controles de acesso baseado em função (RBACs), gerenciamento integrado de certificados e microssegmentação de rede.

Ferramentas de automação

Escolha uma linguagem de automação que todos os interessados na empresa, incluindo as equipes de desenvolvimento, operações, segurança e conformidade, possam aprender e usar com facilidade. Busque recursos de controle de acesso, geração de registros e auditoria. Consulte a **página 4** para mais informações sobre automação.

Por fim, revise as ferramentas e os processos de segurança atualmente em uso na sua empresa. Você deve ter certeza de que estão sendo usados todas as funcionalidades disponíveis. Determine se é possível reconfigurar ou modificar as configurações para aumentar a proteção ou se você precisa de novos processos e ferramentas.

1. Crie um inventário dos ativos e ferramentas de TI da sua empresa em uso no momento.
2. Documente as arquiteturas de segurança e rede, as políticas de segurança cibernética e os processos de trabalho existentes, bem como as habilidades e os talentos que precisam ser adquiridos.
3. Estabeleça um modelo de ameaça e determine a tolerância aos riscos e as estratégias de mitigação em caso de violação da segurança cibernética.
4. Avalie suas arquiteturas, políticas e processos para identificar as áreas que necessitam de mudanças.
5. Avalie as ferramentas e os ativos que sua empresa usa atualmente para determinar se são compatíveis com os novos processos e estratégias. Documente e planeje como as brechas de segurança serão solucionadas.

Nas seções a seguir, apresentamos considerações essenciais sobre a segurança na nuvem híbrida e dicas de como você pode aumentar a proteção.

CONSIDERAÇÕES SOBRE A SEGURANÇA

Colaboração

Por que ela é importante?

Abordagens compartimentalizadas geralmente resultam em brechas de segurança e esforços duplicados, pois nesses casos a segurança acaba ocupando um lugar secundário no desenvolvimento de aplicações e na implantação da infraestrutura. Conforme o desenvolvimento é acelerado e a implantação se torna mais flexível, aumenta a importância de pensar sobre a segurança no começo do processo. Tentar aplicar uma segurança que seja eficaz somente no fim dos ciclos de desenvolvimento consome um tempo substancialmente maior, o que pode resultar em atrasos na entrega e incentivar as equipes a poupar na segurança.

Recomendações e práticas recomendadas

Unifique a segurança em toda a empresa usando uma abordagem de DevSecOps. Trata-se de um framework colaborativo no qual a segurança é uma responsabilidade compartilhada, que é integrada do início ao fim. A segurança se torna uma preocupação de todas as equipes, em vez de ficar nas mãos de uma única equipe desconexa que é responsável por definir as políticas dessa área. Os membros das equipes de operações, desenvolvimento e segurança trabalham juntos, têm visibilidade dos mesmos recursos e compartilham feedbacks, lições aprendidas e insights. Nesse tipo de abordagem, a segurança é incorporada desde o início do desenvolvimento da aplicação e da implantação da infraestrutura, aumentando a proteção.

Os programas de treinamento formais ajudam todos a entender a importância da segurança e qual o papel deles na proteção da empresa. Esses programas devem incluir tópicos como os seguintes:

- Como manter aplicações e recursos em conformidade com as políticas e normas de segurança.
- Como estabelecer abordagens de segurança diferentes para ambientes tradicionais, em containers e de nuvem híbrida.
- Como criar uma estratégia de aplicação de patches que ajude a acompanhar vulnerabilidades atuais e novas.

O aval do corpo executivo também é importante. Diretores e gestores devem incentivar a colaboração e estar abertos para o recebimento de feedback das diversas equipes envolvidas.

Etapas táticas

Tente adotar as medidas abaixo para aumentar a colaboração na sua empresa.

Comece do básico e expanda.

Escolha primeiro um projeto simples. Incentive a experimentação e melhorias contínuas e iterativas para ajustar e otimizar o processo. Comemore os sucessos e exiba o valor comprovado para os outros na empresa.

Defina metas e cronogramas claros com que todos estejam de acordo.

A transparência é crucial para DevSecOps. Certifique-se de que todos os envolvidos entendam e concordem com as metas e os cronogramas do projeto.

Treine seu pessoal de maneira multidisciplinar.

Estabeleça caminhos de aprendizado sobre segurança, infraestrutura e desenvolvimento que sejam atualizados regularmente e disponibilizados de imediato para os membros de todas as equipes.

Crie um grupo de trabalho dedicado à segurança.

Crie uma equipe integrada e multidisciplinar para definir os casos de uso e as estratégias de segurança.

Aprenda com os outros.

Aproveite as descobertas de outras entidades, como o Departamento de Receita Federal (IRS) e o Departamento de Segurança Interna (DHS) dos Estados Unidos.

CONSIDERAÇÕES SOBRE A SEGURANÇA

Automação

Por que ela é importante?

Configurações incorretas e o controle inadequado das alterações são as principais ameaças à segurança.[3] Essas configurações podem deixar os sistemas vulneráveis a ataques. Já o controle de alterações é crítico para entender quem modificou as configurações, quando isso foi feito e o que foi alterado durante os ciclos de vida dos sistemas. Com a automação, é possível otimizar as operações diárias, bem como integrar a segurança a processos, aplicações e infraestrutura desde o início. Na verdade, implantar uma automação total dos processos e tarefas de segurança pode reduzir o custo médio de uma violação em 95%, mas apenas 16% das empresas fizeram isso.[4]

Recomendações e práticas recomendadas

Implementar uma estratégia de automação unificada para reduzir o risco de configurações incorretas e erros manuais por toda a empresa. A automação otimiza e aumenta a consistência no gerenciamento da infraestrutura, no desenvolvimento de aplicações e nas operações de segurança para aprimorar a proteção, a conformidade e o controle de alterações.

- Configure recursos de modo consistente e de acordo com políticas pré-aprovadas. Além disso, faça a manutenção proativa de tais recursos de maneira repetível durante todo o ciclo de vida.
- Identifique rapidamente os sistemas que precisam de patches ou de reconfiguração.
- Facilite a aplicação de patches ou a alteração das configurações do sistema de acordo com linhas de base definidas, de forma consistente em um grande número de sistemas.
- Simplifique a auditoria e a solução de problemas com logs de ação registrados automaticamente.

Ao implementar gerenciamento de identidades e controles de acesso para seus processos e plataforma de automação, você tem certeza de que apenas o pessoal autorizado será capaz de executar tarefas de automação.

Escolha uma plataforma de automação que todos os envolvidos possam usar. Com uma plataforma que ajude a implementar uma linguagem de automação comum e fácil de aprender, é possível melhorar os seguintes pontos:

- **Visibilidade.** Todos podem entender o que cada tarefa automatizada faz.
- **Repetitividade.** Com uma plataforma e uma linguagem acessíveis, todos os funcionários aprovados podem usar a automação com eficácia e eficiência.
- **Colaboração.** As tarefas de automação podem ser compartilhadas por vários setores na empresa, permitindo que outras equipes aproveitem o trabalho que já foi realizado, assim, evitando esforços duplicados.
- **Auditoria.** Vários funcionários podem verificar as tarefas de automação e visualizar os logs para fins de auditoria.

Etapas táticas

Tente adotar as medidas para começar agora mesmo a implementar a automação na segurança.

Comece com apenas um projeto.

Não tente automatizar tudo de uma vez. De início, escolha um projeto ou um conjunto limitado de tarefas.

Escolha tarefas repetitivas.

Automatize as tarefas que têm processos repetitivos, incluindo gerenciamento de configuração, gestão de pacotes e patches de software, identificação e correção de vulnerabilidades de segurança e aplicação de políticas.

Avalie, adapte e repita.

Trabalhe de forma iterativa para implantar a automação, avaliar os resultados e adaptar de acordo com o necessário.

Planeje a ampliação.

Tenha certeza de que todas as automações sejam verificáveis e compartilháveis para que outras pessoas da sua empresa possam aproveitar os benefícios.

3 *Cloud Security Alliance, "Top Threats to Cloud Computing: The Egregious 11", agosto de 2019.* **cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven**.

4 *IBM Security, "2019 Cost of a Data Breach Report", 2019.* **ibm.com/security/data-breach**.

CONSIDERAÇÕES SOBRE A SEGURANÇA

Atualizações e patches

Por que ela é importante?

Sistemas desatualizados e que não receberam os devidos patches podem ser uma fonte de problemas de conformidade e vulnerabilidades de segurança. De fato, a maioria das vulnerabilidades exploradas quando uma violação ocorre são aquelas que já são conhecidas pelas equipes de TI e segurança.

Recomendações e práticas recomendadas

Aplique os patches frequentemente. Teste-os para ter certeza de que foram aplicados corretamente. Verifique os sistemas diariamente em busca de vulnerabilidades de segurança e problemas de conformidade que precisam ser corrigidos com patches. Priorize as ações voltadas à correção dos itens encontrados de acordo com seu modelo de ameaça, além de dar atenção a considerações sobre risco, desempenho e tempo. Aplique patches regularmente em todos os devidos sistemas para mantê-los atualizados com a correção de problemas importantes. Aplique patches para corrigir problemas críticos e vulnerabilidades conhecidas assim que possível. Teste a funcionalidade dos sistemas que receberam patches antes de recolocá-los na produção.

Além disso, você deve atualizar a estratégia de aplicação de patches para que seja compatível com os recursos de nuvem e containers, que são implantados a partir de imagens base. Certifique-se de que essas imagens base estejam em conformidade com as linhas de base de segurança da sua empresa. Assim como é feito com sistemas físicos e virtualizados, verifique e aplique patches nas imagens base regularmente. Ao fazer isso, crie e implante novamente todos os recursos de nuvem e containers baseados nas imagens.

Por fim, implemente a automação para otimizar as operações de aplicação de patch. Crie um fluxo de trabalho de automação para a aplicação de patches a fim de acelerar as operações, reduzir o risco de erros e aumentar a consistência em todos os sistemas. Por exemplo, você pode usar um pipeline de integração/implantação contínuas (CI/CD) baseado em Jenkins tanto para as aplicações quanto para a infraestrutura, a fim de automatizar processos de ciclo de vida, como a aplicação de patches.

Etapas táticas

Siga estas etapas para criar uma estratégia mais sólida de atualização e aplicação de patches.

1. Identifique os sistemas que precisam de patches.
2. Priorize as ações com base no seu modelo de ameaça, nos riscos previstos, nos impactos no desempenho e nas janelas de aplicação de patch disponíveis.
3. Automatize a aplicação de patches para melhorar a consistência e a repetitividade para infraestruturas tradicionais e de nuvem híbrida.
4. Periodicamente, reavalie e adapte sua estratégia de aplicação de patches para acompanhar a evolução de recursos, tecnologias e ameaças.

CONSIDERAÇÕES SOBRE A SEGURANÇA

Tecnologias open source

Por que ela é importante?

As **tecnologias open source** são fatores essenciais para as operações de nuvem e em containers. No entanto, elas também poderão ser uma fonte de vulnerabilidades de segurança se sua empresa usar softwares sem assinatura ou implantar essas tecnologias de maneira não segura. Usar softwares open source não aprovados recebidos direto das comunidades upstream pode deixar sua empresa desprotegida contra vulnerabilidades de segurança e ataques à cadeia de fornecedores, que exploram fraquezas em serviços e softwares de terceiros para comprometer um alvo final. Esses ataques ocorrem de diversa formas, incluindo por meio do sequestro de atualizações de software e da injeção de código mal-intencionado em um software legítimo. Os ataques à cadeia de fornecedores aumentaram em 78% em 2018.[5]

Recomendações e práticas recomendadas

Tenha certeza de que entende quem distribui as tecnologias open source que a sua empresa usa. Além disso, você deve implantar essas tecnologias de maneira segura. Primeiro, faça um inventário das tecnologias open source em uso atualmente na sua empresa. Pare de usar qualquer uma que não foi obtida de fontes conhecidas e confiáveis. Defina processos e políticas para que as equipes de TI e de segurança assumam novamente o controle das tecnologias restantes.

Além disso, crie uma estratégia para o uso de tecnologias open source de forma a priorizar a segurança. Essa estratégia deve incluir medidas para assegurar que suas tecnologias open source sejam fornecidas por fontes confiáveis, recebam patches continuamente de maneira automatizada e sejam configuradas com a segurança em mente. Por fim, incentive o uso de ofertas open source corporativas que incluam suporte corporativo durante todo o ciclo de vida.

78% a mais de ataques à cadeia de fornecedores ocorreram em 2018 do que no ano anterior.[5]

Etapas táticas

Experimente estas medidas para melhorar a segurança das tecnologias open source que a sua empresa usa.

Mude para versões disponíveis comercialmente.

Migre os softwares open source que sua empresa usa diretamente dos projetos upstream para **versões disponíveis comercialmente** e confiáveis. Essas versões são testadas e validadas para reduzir o risco da ocorrência de bugs e vulnerabilidades de segurança. Elas também podem incluir um suporte corporativo que acelere o fornecimento de patches de segurança e dê orientações sobre como configurar o software de forma a preservar a segurança.

Leia mais sobre a proteção de tecnologias open source **neste artigo**.

Implante software open source com base em modelos.

Verifique se suas ferramentas de gerenciamento e plataforma oferecem provisionamento por autosserviço com base em templates predefinidos e aprovados. Você pode usar templates para assegurar que apenas tecnologias open source confiáveis e atualizadas sejam implantadas. A implantação automatizada e rápida também é um incentivo para que os usuários empreguem recursos de TI autorizados, em vez de implantar aqueles que estão fora do controle das equipes de TI e de segurança.

5 *Symantec, "Internet Security Threat Report, Volume 24", fevereiro de 2019.*

Vamos começar?

A segurança na nuvem híbrida é uma preocupação importante para todas as empresas. Independentemente de onde sua empresa esteja na jornada para a nuvem híbrida, a Red Hat pode ajudar você a implantar uma solução que priorize a segurança. Com recursos de segurança incorporados e integrados, o portfólio de software open source voltados à produção da Red Hat oferece as ferramentas e plataformas de que você precisa para superar os desafios de segurança e conformidade atuais e futuros. A Red Hat também fornece suporte de classe corporativa, treinamentos hands-on e serviços especializados para ajudar você a criar e operar seu ambiente de nuvem híbrida de maneira eficiente e segura.

Leia os recursos a seguir para saber mais sobre a abordagem de segurança e conformidade da Red Hat.

- **Visão geral da segurança na nuvem híbrida**
- **Por que escolher a Red Hat para a segurança contínua da TI?**
- **Por que automatizar a segurança e a conformidade**
- **Red Hat® Services: automatize a segurança e a conformidade de sistemas**

Agende uma discovery session gratuita:
https://red.ht/consultoria

Sobre Lucy Huh Kerner, evangelista e estrategista técnica principal sênior global de segurança, Red Hat

Lucy Huh Kerner ajudou a desenvolver uma liderança inovadora em segurança e chefia a estratégia técnica e de mercado de segurança globalmente para todo o portfólio da Red Hat. Ela também ajuda a criar e fornecer conteúdo técnico sobre segurança para profissionais, clientes, parceiros, analistas e imprensa, além de ter palestrado em inúmeros eventos. Antes de sua função atual, ela ocupava o cargo de arquiteta sênior de soluções de nuvem na equipe dedicada a empresas do setor público na América do Norte da Red Hat. Devido a seus domínio e especialização em tecnologias de nuvem, ela colaborou com os esforços de vendas de nuvem da Red Hat, elaborando e apresentando soluções para uma ampla gama de clientes no setor público na América do Norte. Lucy tem mais de 15 anos de experiência profissional como engenheira de desenvolvimento de software e hardware e arquiteta de soluções pré-venda, especializando-se em diversos aspectos da segurança cibernética.

Copyright © 2020 Red Hat, Inc. Red Hat e o logotipo da Red Hat são marcas comerciais ou registradas da Red Hat, Inc. e suas subsidiárias nos Estados Unidos e em outros países.

F18867_0220_KVM

Red Hat