Hardening for Blue Teams

Edição 03 - Agosto/2022

Security by Design

Azure Blob Storage

Criado por: Felipe Silvany & Yves Peixoto

SUMÁRIO

CONFIDENCIALIDADE

Este documento contém informações confidenciais ou privilegiadas, sendo seu sigilo protegido por lei, não sendo autorizado o uso, cópia ou divulgação das informações ou tomar qualquer ação baseada nessas informações.
Desta forma, os destinatários destes documentos comprometem-se em:
1. Não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros.
2. Não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso.
3. Não apropriar-se de material confidencial e/ou sigiloso da tecnologia que venha a ser disponível.
4. Não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

SOBRE O AUTOR

Felipe Silvany é coordenador de Cybersecurity, com 20 anos de experiência na área de tecnologia, com sólidos conhecimentos em resposta à incidentes de segurança, SOC, hardering, análise de vulnerabilidades, pentest e grandes projetos de cybersecurity em ambientes onpremises, Cloud e mobile (AppSec).
Sólida experiência na implementação de soluções técnicas e estruturação de equipes de segurança de alta performance.
Responsável pela implementação de serviços, ferramentas e processos como: SOC/CSIRT 24x7, playbooks, Plano de Resposta à Incidentes de Segurança (RI), SIEM com base no MITRE ATT&CK, hardening e baselines de segurança, exercícios de RedTeam como Pentest, análise de vulnerabilidades DAST e SAST na infraestrutura onpremises/cloud (OpSec), mobiles Android e IOS (AppSec) e definição de arquitetura segura com conceitos de Zero Trust. Implementação de ferramentas de BlueTeam como: NGAv/EDR, NGFw, MTLS, NAC, DLP, IDS, IPS, WAF, AppControl, Anti-DDoS e outras.
Graduado em "Sistema de Informação", Pós Graduado em "Projetos e Gerência de Redes" e com MBA em "Gestão Empresarial Estratégica". Membro da ISO/ABNT/CE-021 000.027 (Comissão Especial de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade de dados), membro da ANPPD (Associação Nacional dos Profissionais de Privacidade de Dados) e certificado nos mais conceituados frameworks internacionais, como: ISO27001, ISO20000, ITIL, COBIT, Scrum, Kanban e outros. Classificado entre os TOP 5 Ethical Hackers na maior plataforma de BugBounty do Brasil e primeiro colocado em diversos programas privados.
Linkedin: https://www.linkedin.com/in/felipe-silvany-69241365/
Github: https://github.com/FelipeSilvany

Yves Peixoto é Especialista em Cybersecurity, com mais de 12 anos de experiência na área de tecnologia. Bacharel em análise de sistemas com pós-graduação em segurança da informação pela UFRJ e algumas certificações de mercado, como por exemplo: CEH, CNDA, ISO, LPI, Azure, entre outras.
Dentro da área de S.I. possui sólidos conhecimentos tanto em áreas ofensivas (Pentest, Appsec, DAST, SAST, IAST, MAST, análise de vulnerabilidades quanto em áreas defensivas (SOC, CSIRT, hardening, firewalls, WAF, IDS, IPS, EDR, infraestrutura onpremises e cloud). Possui histórico de atuação em empresas de diversos seguimentos, privados e públicos.
Linkedin: https://www.linkedin.com/in/yvespeixoto/

SOBRE ESTE DOCUMENTO

Este não é um e-book comum.
Você está prestes a obter um conhecimento privilegiado em segurança da informação e hardening.
Esta obra utiliza uma metodologia focada em *Security by Design* e implementação de boas práticas de segurança desde a concepção de projetos corporativos até sua passagem para produção.
A segurança deve ser sempre preventiva e pró ativa, nunca reativa.
Nesta segunda edição veremos boas práticas na estruturação de Storage Accounts, preparado especificamente para o Azure, mas com possibilidade de adaptação para qualquer ambiente.

Edição 01 – Criação do Documento
Julho/2022 – Felipe Silvany e Yves Peixoto

AGRADECIMENTOS

“Ao meu filho, Thor, que me dá toda força para enfrentar todas as dificuldades e tribulações da vida com força e ânimo. À minha esposa, Fabiana, por sempre me apoiar em todos os desafios profissionais e perder várias noites de sono comigo. À minha mãe e meu pai, Maria Aparecida e Adilton, por terem me dado a maior herança que um homem por ter, o estudo. À Deus, que por intermédio do meu Senhor Jesus Cristo conduz a minha vida, me guia e me guarda.” **– Felipe Silvany**

“Primeiramente à Deus e a minha família por todo apoio em minha trajetória, principalmente nos momentos mais difíceis.” **– Yves Peixoto**

1 - INTRODUÇÃO

Acessos Públicos, anônimos, não autenticados ou outros que não sejam possíveis garantir que o acesso seja disponibilizado somente a quem é de direito e permitam auditoria de acesso futuro, devem ser evitados.
O acesso público/anônimo de leitura aos dados de um blob storage embora seja uma opção conveniente e simples para administradores configurarem o compartilhamento de dados, traz riscos de segurança.
A Microsoft recomenda que não seja permitido o acesso público a uma conta de armazenamento, salvo em último caso e que por inviabilidade técnica o cenário exija. A proibição do acesso público ajuda a evitar violações de dados causadas por acesso anônimo indesejado.

> ⚠ **Warning**
>
> When a container is configured for public access, any client can read data in that container. Public access presents a potential security risk, so if your scenario does not require it, Microsoft recommends that you disallow it for the storage account. For more information, see **Prevent anonymous public read access to containers and blobs**.

Nome (Portal do Azure)	Descrição
As contas de armazenamento devem restringir o acesso da rede	O acesso da rede às contas de armazenamento deve ser restrito. Configure as regras de rede de tal forma que somente os aplicativos das redes permitidas possam acessar a conta de armazenamento. Para permitir conexões de clientes específicos locais ou da Internet, o acesso pode ser permitido para o tráfego de redes virtuais específicas do Azure ou para intervalos de endereços IP públicos da Internet

O acesso público (anônimo) ao blob atenta contra boas práticas de segurança, como "*Princípio do Menor Privilégio*" e "*Zero Trust*".

ZERO TRUST
O principal conceito trazido pelo Zero Trust é "*nunca confie, sempre verifique*" ou para autores mais conservadores "*confiar, mas sempre verificar*", o que significa que dispositivos e serviços não devem ser confiáveis (confiados) por padrão. Redes, como WAN, LAN corporativa, VPNs são hostis e inseguras por padrão, mesmo que estejam dentro do perímetro de segurança, por isso, todo acesso deve ser validado, mesmo que já tenha sido verificado anteriormente. O Zero Trust aborda princípios chaves como: Autenticação mútua (MFA, 2FA), autenticação de máquina, autenticação de usuário, monitoramento contínuo, registro de todos os logs de acessos, entre outros. Permitir um acesso anônimo no ambiente, disponibilizado para qualquer origem (ALL) é contra todos os conceitos trazidos pelo Zero Trust.

PRINCÍPIO DO MENOR PRIVILÉGIO

O princípio do menor privilégio é aquele que preza por delegar somente os privilégios necessários para que um determinado elemento (sistema ou pessoa) possa realizar sua função.

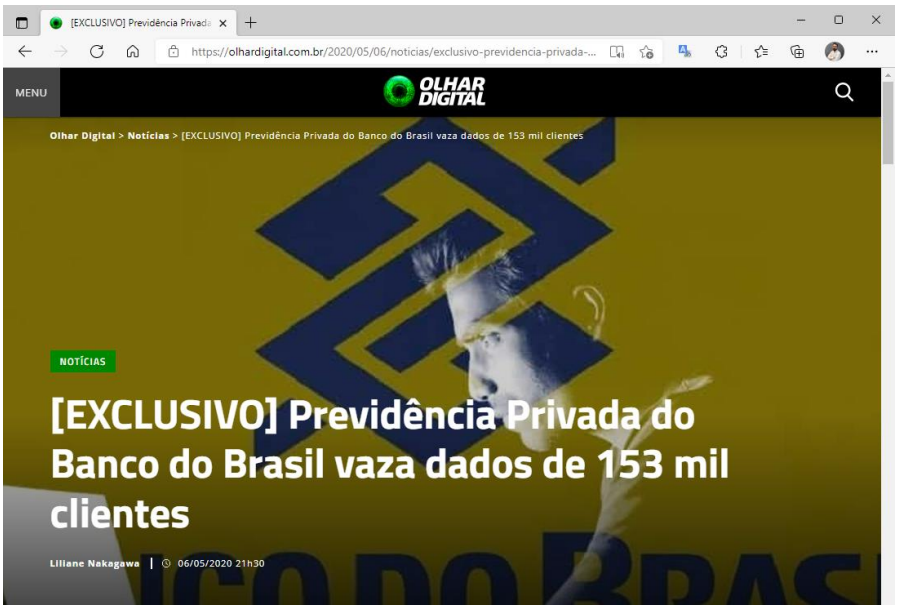
2 – GERENCIAMENTO DE IDENTIDADES

A Microsoft recomenda que não seja permitido o acesso público a uma conta de armazenamento, salvo em último caso e que por inviabilidade técnica o cenário exija. A proibição do acesso público ajuda a evitar violações de dados causadas por acesso anônimo indesejado.

Recomendação	Comentários
Use o Azure Active Directory (Azure AD) para autorizar o acesso aos dados de blob	O Azure AD oferece segurança superior e facilidade de uso em relação à chave compartilhada para autorizar solicitações de armazenamento de Blob. Para obter mais informações, consulte Autorizar o acesso aos dados no Armazenamento do Azure .
Lembre-se da entidade de menor privilégio ao atribuir permissões a uma entidade de segurança do Azure AD por meio do Azure RBAC	Ao atribuir uma função a um usuário, grupo ou aplicativo, conceda a esse objeto de segurança apenas as permissões necessárias para que execute suas tarefas. Limitar o acesso aos recursos ajuda a prevenir o uso indevido não intencional e malicioso de seus dados.
Use uma delegação de usuário SAS para conceder acesso limitado aos dados de blob aos clientes	Uma delegação de usuário SAS é protegida com credenciais do Azure Active Directory (Azure AD) e também pelas permissões especificadas para a SAS. Um SAS de delegação de usuário é análogo a um SAS de serviço em termos de escopo e função, mas oferece benefícios de segurança em relação ao SAS de serviço. Para obter mais informações, consulte Conceder acesso limitado aos recursos de armazenamento do Azure usando assinaturas de acesso compartilhado (SAS) .
Lembre-se do princípio de menor privilégio ao atribuir permissões a um SAS	Ao criar um SAS, especifique apenas as permissões exigidas pelo cliente para executar sua função. Limitar o acesso aos recursos ajuda a prevenir o uso indevido não intencional e malicioso de seus dados.
Tenha um plano de revogação em vigor para qualquer SAS que você emitir para os clientes	Se um SAS for comprometido, você desejará revogar esse SAS o mais rápido possível. Para revogar um SAS de delegação de usuário, revogue a chave de delegação de usuário para invalidar rapidamente todas as assinaturas associadas a essa chave. Para revogar um serviço SAS associado a uma política de acesso armazenada, você pode excluir a política de acesso armazenada, renomear a política ou alterar seu tempo de expiração para um tempo que já passou. Para obter mais informações, consulte Conceder acesso limitado aos recursos de armazenamento do Azure usando assinaturas de acesso compartilhado (SAS) .
Se um serviço SAS não estiver associado a uma política de acesso armazenada, defina o tempo de expiração para uma hora ou menos	Um serviço SAS que não está associado a uma política de acesso armazenada não pode ser revogado. Por esse motivo, é recomendável limitar o tempo de expiração para que o SAS seja válido por uma hora ou menos.
Desative o acesso de leitura público anônimo a contêineres e blobs	O acesso de leitura público anônimo a um contêiner e seus blobs concede a qualquer cliente acesso somente leitura a esses recursos. Evite habilitar o acesso público de leitura, a menos que seu cenário exija. Para saber como desabilitar o acesso público anônimo para uma conta de armazenamento, consulte Configurar o acesso de leitura público anônimo para contêineres e blobs .

ATAQUES RECENTES DIVULGADOS NA MÍDIA

Em Maio/2020 diversos dados de clientes do Banco do Brasil foram expostos após serem divulgados de forma equivocada (erro humano) em um storage público. A equipe técnica do Banco em uma atualização do sistema apontou os dados dos clientes que anteriormente estavam em um storage privado para um storage público e não perceberam o erro a tempo do vazamento.



3 – RISCOS DE SEGURANÇA

MODIFICAÇÃO OU EXCLUSÃO DE DADOS

Mesmo que os dados estejam definidos como somente leitura, não existindo o risco de exclusão, inserção ou modificação de dados, se algum administrador inadvertidamente em um processo de change modificar o permissionamento deste storage um atacante terá permissão para deletar todo conteúdo do blob, modificar as imagens e banners por imagens políticas (semelhante ao caso iFood), conteúdo erótico ou outros que atentem contra a reputação da empresa, ou ainda, poderá inserir malwares no storage e utilizar o mesmo como repositório de arquivos maliciosos até mesmo para atacar outras empresas.

DIVULGAÇÃO DE DADOS SIGILOSOS

Mesmo que os dados armazenados não sejam "sigilosos" e estejam definidos somente como leitura, não existindo o risco de exclusão, inserção ou modificação de dado, se algum administrador inadvertidamente em um processo de change apontar um storage público para despejo de informações confidenciais (semelhante ao caso do Banco do Brasil), ou ainda, definir um storage privado como público todos terão acesso às informações ali armazenadas

FALHA HUMANA

Sabemos que a gestão das configurações e de ambientes são feitas por pessoas, desta forma todos nós temos grandes chances de falhar. Os dois tópicos acima ilustram bem o que pesquisas e estudos demonstram: Erros humanos lideram a causa raíz das violações de dados e cyberataques.

ENUMERAÇÃO DE DNS

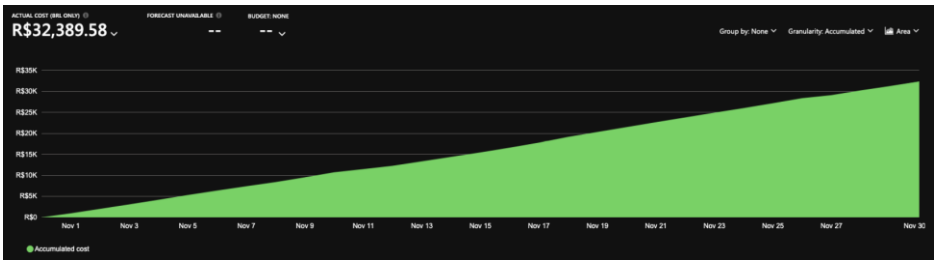
A partir do momento que uma URL é conhecida, é possível a realização de enumeração sobre informações do host, como contas de serviços públicas, CNAME's, MX e outros.

ATAQUE DE NEGAÇÃO DE SERVIÇO

Em um ataque de DoS (negação de serviço) ou DDoS (negação de serviço distribuída), um invasor sobrecarrega seu alvo com tráfego. A partir do momento em que temos um recurso acessível publicamente, pode-se configurar uma botNet enviando dezenas, centenas ou milhares de requisições por segundo para o serviço até atingir o throughput. Em conversa com a Microsoft, relatam que trabalham para mitigar ataques e manter a disponibilidade dos ambientes. Entretanto, negações de serviço não estão descartadas caso não exista a configuração do Azure DDoS ativada e devidamente configurada.

CUSTOS DO AZURE BLOB STORAGE

Associado aos ataques de (D)DoS, estão os custos elevados de cobrança do Azure. Os storage accounts são cobrados por transações, onde a cada 10.000 transações são cobrados aproximadamente R$ 0,112. Inserções, leituras, downloads entre outros tipos de acesso aos conteúdos ali postados são considerados transações. Imagine uma botNet configurada para tentativa de ataque DDoS, onde serão realizadas milhares de leituras dos arquivos ali hospedados. Além da possível degradação ou indisponibilização do serviço, um custo elevado de transações seria cobrado pela Microsoft. Em conversa com a Microsoft, recomendaram limitar o acesso aos storages. Além de uma boa prática de segurança é também uma boa prática de governança na gestão de dados, custos e/ou evitar surpresas nas cobranças.



WATERING HOLE ATTACK

É uma estratégia de ataque onde um invasor infecta os conteúdos legítimos com malwares ou utiliza o repositório para hospedar malwares e atacar outros clientes. A partir do momento que consegue acesso ao storage account público, poderá utilizar esta estratégia de ataque.

Nem sempre o alvo do ataque poderá estar diretamente focado na empresa detentora do storage. O atacante pode utilizar a infraestrutura da empresa alvo para esconder a real origem do ataque.

STORAGE TAMPER ATTACK

O ataque de adulteração de armazenamento é extremamente eficaz e perigoso, onde a partir do momento que um hacker consegue acesso à chave do storage account, seja por técnicas de exfiltração, enumeração, interceptação ou outras, poderá listar o Blobs usando a CLI do Azure. Realizar upload de scripts maliciosos, arquivos PDF adulterados e muito mais. Veja abaixo um exemplo para listar Blobs usando CLI do Azure.

```
az storage blob list -c MyContainer --prefix foo
```

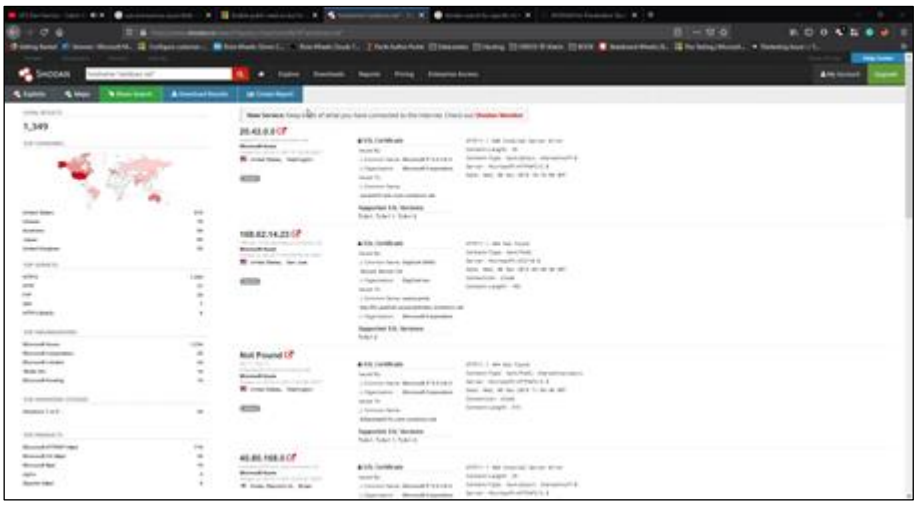
ATAQUES DE PHISHING

Um atacante em posse de imagens reais/originais, pode criar ataques de phishing usando as imagens do Blob Storage. Clientes “menos atentos”, não perceberão, pois são as

mesmas imagens que eles já viram no App e/ou site da respectiva empresa. Clientes “mais atentos” verificarão que a URL da imagem aponta para um domínio legítimo da Microsoft, utilizado pela Empresa e mesmo assim cairão no golpe.

ENUMERAÇÕES (HUNTING)

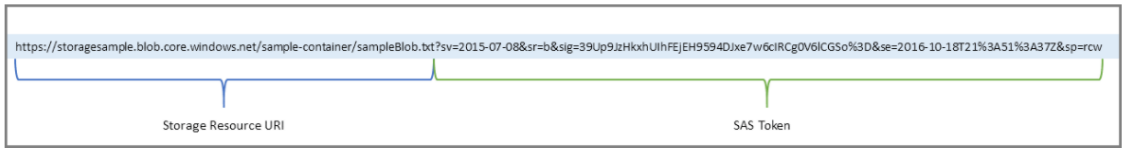
Através de técnicas de OSSINT (Open Source Social Network Intelligence) como Google Hacking ou Shodan.io é possível enumerar storages configurados na internet através da string “*host:Windows.net*” ou filtrar por organizações ou empresas com a string “*org:Nome_da_empresa*”. (imagem ilustrativa)

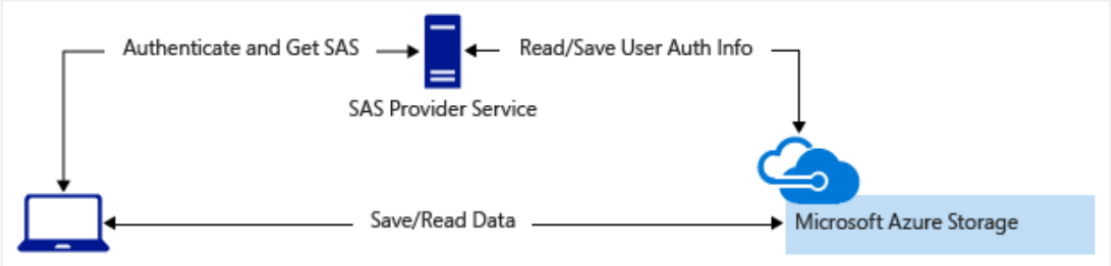


4 – CONTRAMEDIDAS E RECOMENDAÇÕES DE SEGURANÇA

Recomenda-se que não sejam permitidos acessos anônimos ou públicos no ambiente corporativo, de forma que todo acessos seja autenticado, validado e logado. Seja utilizando credenciais, tokens de acesso, MTLS ou qualquer método de autenticação que possua compatibilidade com a arquitetura existente. A Microsoft possui algumas opções de tokens para acesso compartilhado, como Shared Access Signatures (SAS), arquiteturas propostas como o SAS Provider Service, o Front End proxy Service ou o Azure Private Endpoint.

Shared Access Signatures (SAS): O Token de assinatura de acesso compartilhado é um URI assinado que aponta para um ou mais recursos de armazenamento. O URI inclui um token que contém um conjunto especial de parâmetros de consulta. O token indica como os recursos podem ser acessados pelo cliente. Um dos parâmetros de consulta, a assinatura, é construído a partir dos parâmetros SAS e assinado com a chave que foi usada para criar o SAS. Essa assinatura é usada pelo Armazenamento do Azure para autorizar o acesso ao recurso de armazenamento.
O token SAS é uma string que você gera no lado do cliente, por exemplo, usando uma das bibliotecas de cliente do Armazenamento do Azure.





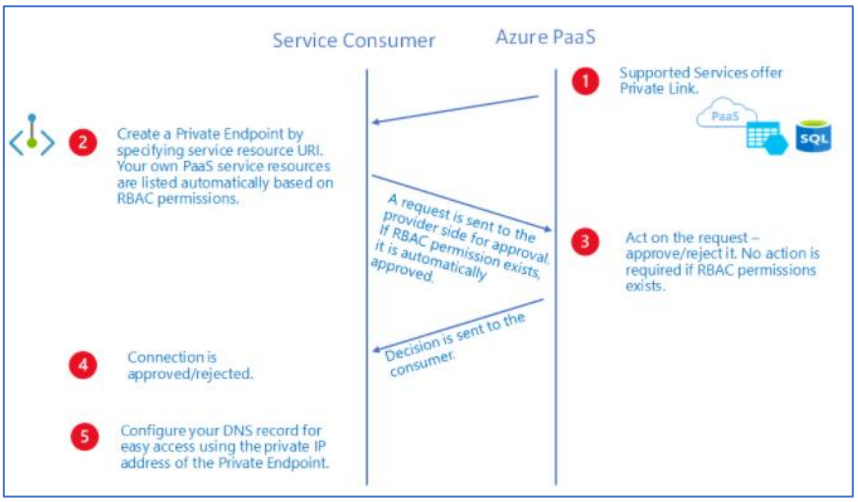
Link adicional: https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

SAS Provider Service: Serviço leve que autentica o cliente conforme necessário e, em seguida, gera um SAS. Depois que o aplicativo cliente recebe o SAS, ele pode acessar os recursos da conta de armazenamento diretamente. As permissões de acesso são definidas pelo SAS e para o intervalo permitido pelo SAS. O SAS atenua a necessidade de roteamento de todos os dados por meio do serviço de proxy front-end.

Front End Proxy Service: Clientes carregam e baixam dados de forma segura por meio de um serviço de proxy front-end, que executa a autenticação. Este serviço de proxy front-end permite a validação de regras de negócios. Mas, para grandes quantidades de dados ou transações de alto volume é importante criar um serviço que possa ser escalonado para atender à demanda pode ser caro ou difícil.

Azure Private Endpoint: Adaptador de rede que usa um endereço IP privado de sua rede virtual. Esse adaptador de rede conecta você de forma privada e segura a um serviço da plataforma do Link Privado do Azure. Ao habilitar um ponto de extremidade privado, você está trazendo o serviço para sua rede virtual.

Desta forma, o app "falaria" com o storage para carregamento das imagens e banners através de uma rede privada e não mais pela internet.



SDK para blob storage: A Microsoft disponibiliza SDK's (software development kit) para diversas linguagens. Com este SDK a equipe de desenvolvimento consegue gerenciar os Blobs de maneira muito mais segura. Trazendo inúmeras possibilidades...Por exemplo:

Cenário 1: É possível criar, deletar, fazer upload de arquivos usando métodos disponíveis. Para alguns cenários, não seria necessário existência de um blob storage permanente. Ele poderia ser criado em tempo de execução ou até que uma determinada tarefa/chamada exista. Com isto o storage criado não ficaria disponível a todo tempo (diminuindo exposição e custos), poderá ter seu nome modificado sempre que criado (dificultando a enumeração) e após isto pode ser removido por meio dos métodos disponíveis.

Link de SDK para Java: GitHub - Azure-Samples/azure-sdk-for-java-storage-blob-upload-download: How to upload and download blobs from Azure Blob Storage with Java

Cenário 2: Além de implementar as chamadas de criação de blobs, conforme cenário anterior, adicionar chamadas por API Rest para criação de tokens SAS, trazendo uma camada de segurança para o determinado blob storage ? Desta forma as chamadas seriam protegidas pelo recurso Shared Access Signatures (SAS) e também poderiam permitir o rotacionamento destes tokens.

https://docs.microsoft.com/en-us/azure/cognitive-services/translator/document-translation/create-sas-tokens?tabs=Containers

Cenário 3: Imagine a possibilidade de juntar o cenário 1 + cenário 2 e guardar os tokens gerados pelo SAS em local seguro?
A Microsoft disponibiliza também SDK para o Key Vault (serviço de proteção de chaves da Microsoft), que por métodos podem ser chamados para guarda ou obtenção da chave.

Link de exemplo de SDK para Key Vault usando Java: https://github.com/Azure-Samples/key-vault-java-authentication

5 – CONCLUSÃO

A Microsoft recomenda que não seja permitido o acesso público a uma conta de armazenamento, salvo em último caso e que por inviabilidade técnica o cenário exija. A proibição do acesso público ajuda a evitar violações de dados causadas por acesso anônimo indesejado.
O acesso da rede às contas de armazenamento também deve sofrer restrições. Configure as regras de rede de forma que somente os aplicativos que necessitam acesso, consigam acessar a conta de armazenamento.

6 – LEITURA COMPLEMENTAR

- https://azure.microsoft.com/pt-br/updates/choose-to-allow-or-disallow-blob-public-access-on-azure-storage-accounts/
- https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations
- https://docs.microsoft.com/en-us/azure/storage/common/storage-plan-manage-costs
- https://docs.microsoft.com/pt-br/azure/private-link/private-endpoint-overview
- https://ninocrudele.com/the-three-most-effective-and-dangerous-cyberattacks-to-azure-and-countermeasures-part-2-attack-the-azure-storage-service
- https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html