Hardening for Blue Teams

Edição 02 - Maio/2022

Security by Design

Azure Database (DBs)

Criado por: Felipe Silvany

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

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

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 um servidor de Bando de Dados, preparado especificamente para o Azure, mas com possibilidade de adaptação para qualquer ambiente.

Edição 01 – Criação do Documento
Maio/2022 – Felipe Silvany

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.

1 - INTRODUÇÃO

Coletar e analisar informações com inteligência passou a ser um dos principais objetivos das empresas. Um dos motivos é a possibilidade de identificar tendências e oportunidades de negócio fundamentais para o sucesso. Em virtude disso, é possível afirmar que dados são o novo petróleo (Data is the new oil). Em virtude disso, databases passaram a ser alvo das principais fontes de ataques e a exposição ou comercialização destas informações se tornou cada vez mais comum na deep e darkweb.

É extremamente importante que o armazenamento e tratamento dos dados sejam realizados de forma segura e com o nível de hardening apropriado.

2 – CONCEITOS BÁSICOS

ACESSO À REDE PÚBLICA DEVE SER DESATIVADO

Certifique-se que o banco de dados nunca esteja exposto diretamente para internet, ou com IP público associado. A desabilitação da propriedade de acesso à rede pública aprimora a segurança garantindo que o Banco de Dados seja acessado somente de pontos de extremidade privados. Essa configuração nega todos os logons que correspondem às regras de firewall de IP ou baseadas em rede virtual.

A exposição de Base de Dados para internet expõe à riscos eminentes as informações ali armazenadas, ainda que existam regras de firewall bem definidas para mitigar o risco.

PRIVATE ENDPOINT CONNECTIONS

As conexões de ponto final privados reforçam a comunicação segura, permitindo conectividade privada ao Banco de Dados.

Use os pontos finais do serviço Azure Virtual Network para fornecer acesso seguro ao database através de uma rota otimizada da rede backbone do Azure sem cruzar a internet.

O acesso privado é uma medida adicional de defesa à autenticação e segurança de tráfego oferecida pelos serviços do Azure.

Para conectar duas ou mais redes virtuais no Azure, use o peering de rede virtual. O tráfego entre redes virtuais é privado e mantido na rede backbone do Azure.

SERVIÇO DE NOME DE DOMÍNIO SEGURO (DNS)

Siga as melhores práticas de segurança do DNS para mitigar ataques comuns como DNS Amplifications Attacks, DNS Poisoning and Spoofing , DoS, DDoS e outros.

Quando o Azure DNS for usado como seu serviço de DNS autoritário, certifique-se de que as zonas e registros de DNS estejam protegidos contra modificações acidentais ou maliciosas usando o Azure RBAC e bloqueios de recursos.

JUMPSERVER OU AZURE BASTION

Jumpservers ou Jumpbox são servidores seguros e isolados, extremamente importantes para a segurança de funções administrativas ou sensíveis.

Utilize o Azure Bastion, jumpservers ou jumpbox para garantir que o acesso aos bancos de dados só seja possível a partir deste ponto de extremidade seguro e altamente hardenizado.

LIBERE APENAS A ADMINISTRAÇÃO SUFICIENTE (PRINCÍPIO DO MENOR PRIVILÉGIO)

O Azure está integrado ao controle de acesso baseado em papéis do Azure (Azure RBAC) para gerenciar seus recursos. O Azure RBAC permite que você gerencie o acesso de recursos do Azure através de atribuições de papéis. Você pode atribuir essas funções aos usuários, serviços, grupos e às identidades gerenciadas. Existem funções incorporadas pré-definidas para determinados recursos, e essas funções podem ser inventariadas ou consultadas através de ferramentas como Azure CLI, Azure PowerShell ou o portal Azure. Os privilégios que você atribui aos recursos através do Azure RBAC devem ser sempre limitados ao que é exigido pelas funções. Isso complementa a abordagem just-in-time (JIT) do Azure AD, Privileged Identity Management (PIM) e deve ser revisto periodicamente.

Use funções incorporadas para alocar permissões e só crie funções personalizadas quando necessário.

PADRONIZE O AZURE AD COMO PADRÃO DE IDENTIDADE E AUTENTICAÇÃO

Defina o Azure Active Directory (Azure AD) como o serviço padrão de gerenciamento de identidade e acesso. Você deve padronizar o Azure AD para gestão de identidade e o gerenciamento de acesso da sua organização.

Proteger o Azure AD deve ser uma prioridade na prática de segurança na nuvem da sua organização. O Azure AD fornece uma pontuação de segurança de identidade para ajudá-lo a avaliar a postura de segurança de identidade em relação às práticas recomendadas da Microsoft. Use a pontuação para medir o quão de perto sua configuração corresponde às recomendações de práticas recomendadas e para fazer melhorias em sua postura de segurança.

> Nota: O Azure AD suporta identidades externas que permitem que usuários sem uma conta Microsoft entrem em seus aplicativos e recursos com sua identidade externa.

A autenticação do Azure AD permite o gerenciamento simplificado de permissões e o gerenciamento centralizado de identidades de usuários de bancos de dados e outros serviços Microsoft.

IMPLEMENTE O CREDENTIAL SCANNER

Projeta-se contra exposição de credenciais. O Azure SQL permite que os clientes implantem/executem código, configurações ou dados persistidos com credenciais. Recomenda-se implementar o *Credential Scanner* para identificar credenciais dentro de {código, configurações ou dados persistidos}. O Credential Scanner também incentivará a mudança de credenciais descobertas para locais mais seguros, como o Azure Key Vault.

LIMITE O NÚMERO DE USUÁRIOS PRIVILEGIADOS

Você deve limitar o número de contas ou funções altamente privilegiadas e proteger essas contas em um nível elevado. Os usuários com esse privilégio podem ler e modificar direta ou indiretamente todos os recursos do seu ambiente.

Você pode ativar acesso privilegiado just-in-time (JIT) aos recursos do Azure e ao Azure AD usando o Azure AD PIM. O JIT concede permissões temporárias para executar tarefas privilegiadas somente quando os usuários precisam. O PIM também pode gerar alertas de segurança quando há atividades suspeitas ou inseguras em sua organização Azure AD.

REVISE E REVOGUE ACESSOS REGULARMENTE

Revise contas de usuários e acesse atribuições regularmente para garantir que as contas e seu acesso sejam válidos. Você pode usar o Azure AD e acessar avaliações para revisar membros do grupo, acesso a aplicativos corporativos e atribuições de papéis. Os relatórios do Azure AD podem fornecer logs para ajudar a descobrir contas obsoletas.

Você também pode usar o PiM (Azure AD Privileged Identity Management) para criar fluxos de trabalho de relatório de revisão de acesso para facilitar o processo de revisão.

UTILIZE O PIM (AZURE AD PRIVILEGED IDENTITY MANAGEMENT)

O PIM (Privileged Identity Management) é um serviço no Azure AD (Azure Active Directory) que permite gerenciar, controlar e monitorar o acesso a importantes recursos na sua organização. Esses recursos incluem os recursos no Azure AD, no Azure e em outros Microsoft Online Services, como o Microsoft 365 ou o Microsoft Intune.
O Privileged Identity Management fornece ativação de função baseada em tempo e aprovação para atenuar os riscos de permissões de acesso excessivas, desnecessárias ou que foram indevidamente utilizadas em recursos importantes.

3 – HARDENING

Garanta que as contramedidas abaixo estejam implementadas em seu servidor de Banco de Dados. Responda "*sim*" caso as contramedidas de segurança estejam implementadas e forneça maiores detalhes técnicos junto à resposta. Responda "*não*" caso as contramedidas de segurança não estejam implementadas no ambiente e considere como um gap de segurança.

1. Aplique os patches de segurança mais recentes do Sistema Operacional.
2. Garanta que o software de Banco (*db*) esteja atualizado com as últimas versões estáveis do fabricante.
3. Garanta que o servidor possui um Endpoint de segurança instalado, EDR, Antivírus ou outros. Especifique no caso de outros.
4. Garanta que o servidor foi submetido à testes de segurança, invasão (Pentest) ou vulnerabilidade. Exemplifique especificando datas.
5. Desative o acesso do database à Rede Pública.
6. Utilize Networking Peerings para conectar duas ou mais redes virtuais.
7. Padronize o Azure AD como padrão de identidade e autenticação e elimine credenciais locais.
8. Certifique-se que a autenticação MFA/2FA está habilitada
9. Habilite a criptografia dos dados em repouso (criptografia TDE)
10. Habilite a criptografia dos dados em trânsito (segurança da cama de transporte)
11. Implemente MTLS (Mutual Transport Layer Security) garantindo a autenticação à nível de máquina para que somente o servidor da aplicação e administradores de Banco de Dados a partir do jumpserver possuam acesso ao database.
12. Implemente o Azure Credential Scanner para identificar credenciais expostas dentro de código, configurações ou dados persistidos.
13. Utilize o Azure Bastion, jumpservers ou jumpbox para garantir que o acesso seja realizado somente a partir deste ponto de extremidade seguro e altamente hardenizado.
14. Utilize o PIM (Azure AD Privileged Identity Management)
15. Certifique-se de que as zonas e registros de DNS estejam protegidas contra modificações acidentais ou maliciosas usando o Azure RBAC e bloqueios de recursos.
16. Habilite a Microsoft Azure Defender para detecção de ameaças dos recursos do Azure.
17. Habilite o Microsoft Anti-malware for Azure Cloud Services
18. Configure retenção de armazenamento de log para ao menos 90 dias
19. Garanta backups e testes de restore realizados regularmente.
20. Solicite reautenticação de sessões inativas.
21. Garanta que sessões idle sejam desconectadas.
22. Habilite a auditoria de logs para sucesso e falha de autenticação.
23. O servidor de Banco de Dados é dedicado para a brMalls ou compartilhado com outros clientes?
24. Existem instâncias de outras aplicações ou de outros clientes neste database?
25. Informe o IP e Portas utilizados pelo Banco de dados, para realização de um assessment de vulnerabilidades.

26. Qual a arquitetura da infraestrutura ou onde o servidor está posicionado na rede? Por favor envie um desenho ilustrando o servidor de Database na infraestrutura.

4 – LEITURA ADICIONAL

- https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/sql-database-security-baseline
- https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts
- https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware
- https://docs.microsoft.com/pt-br/azure/active-directory/privileged-identity-management/pim-configure
- https://secdevtools.azurewebsites.net/helpcredscan.html
- https://azure.microsoft.com/pt-br/services/azure-bastion/
- https://csrc.nist.gov/publications/detail/sp/800-81/2/final
- https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F7698e800-9299-47a6-b3b6-5a0fee576eed
- https://portal.azure.com/#blade/Microsoft_Azure_Policy/PolicyDetailBlade/definitionId/%2Fproviders%2FMicrosoft.Authorization%2FpolicyDefinitions%2F1b8ca024-1d5c-4dec-8995-b1a932b41780