



OWASP

Open Web Application
Security Project

Segurança em Nuvem: a ameaça fantasma

fazer seu trabalho seu provedor
não irá

AGENDA

- O que é owasp
- O que é CSA
- O que é computação em nuvem
- Principais vulnerabilidades
- Boas práticas
- About me



O que é owasp

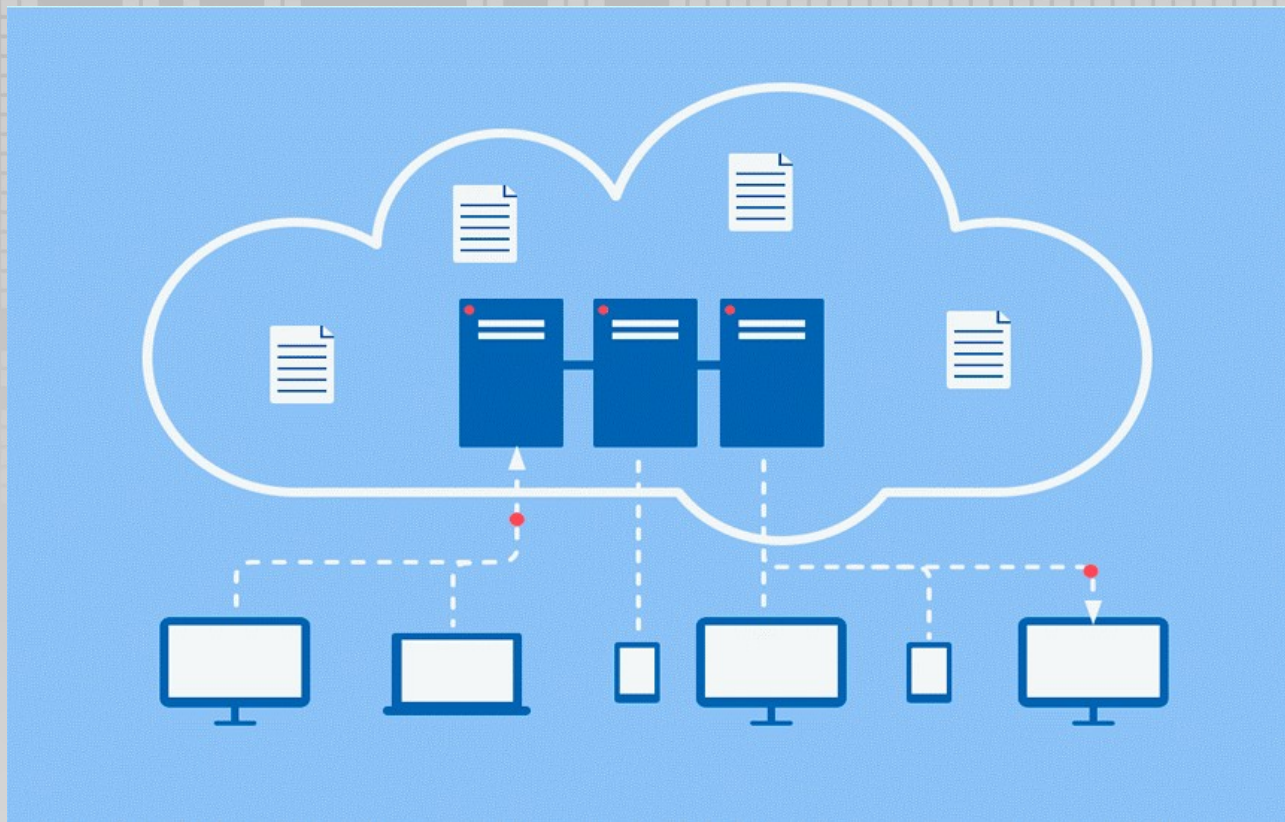
A OWASP Foundation ficou on-line em 1º de dezembro de 2001 e foi estabelecida como uma organização de caridade sem fins lucrativos nos Estados Unidos em 21 de abril de 2004, para assegurar a disponibilidade contínua e suporte para nosso trabalho na OWASP. OWASP é uma organização internacional e a OWASP Foundation apoia os esforços do OWASP em todo o mundo. OWASP é uma comunidade aberta dedicada a permitir que as organizações concebam, desenvolvam, adquiram, operem e mantenham aplicações confiáveis.



o que é CSA

A Cloud Security Alliance (CSA) é a organização líder mundial dedicada a definir e conscientizar sobre as melhores práticas para ajudar a garantir um ambiente seguro de computação em nuvem.





O que é computação em nuvem

Paradigma para habilitar o acesso à rede para um pool escalável e elástico físico ou virtual compartilhável recursos com provisionamento de autoatendimento e administração sob demanda.(ISO/IEC)



Principais Vulnerabilidades

A CSA publica anualmente um relatório sobre as vulnerabilidades mais comuns daquele ano, ao decorrer dos próximos slides vamos discuti-las.



Caso de Estudo Linkedin(2012)

- Causa interna
 - ignorar boas práticas de segurança
- Causa externa
 - Hackers maliciosos do leste europeu
- TT11 DoS
- TT12 vulnerabilidades em tecnologias compartilhadas
- TT2 Gerenciamento insuficiente de credenciais e acesso



- TT1 Violação de dados e/ou perda de credenciais de usuários PT2
- TT5 Sequestro de conta utilizando senhas roubadas



Impactos Financeiros

- Processos de usuarios U\$ 1.25M (exclusas taxas legais)
- Forense e limpeza custou U\$ 1M



Impacto Operacional

Duas chamadas para usuários trocarem as senhas



OWASP
Open Web Application
Security Project

Controles Preventivos

- EKM-02: Geração de chaves - funcionários devem ter bastante cuidado com ferramentas de gerenciamento de acesso, chaves, senhas e sistemas criptográficos
- IAM-12: credenciais de ID de usuários
- GRM-03: Supervisão de gestão
- GRM-06: Política



Boas Práticas

Nos próximos slides iremos discorrer sobre o conjunto de boas práticas publicado pela CSA

Security Guidance (Atualmente em sua 4ª versão)

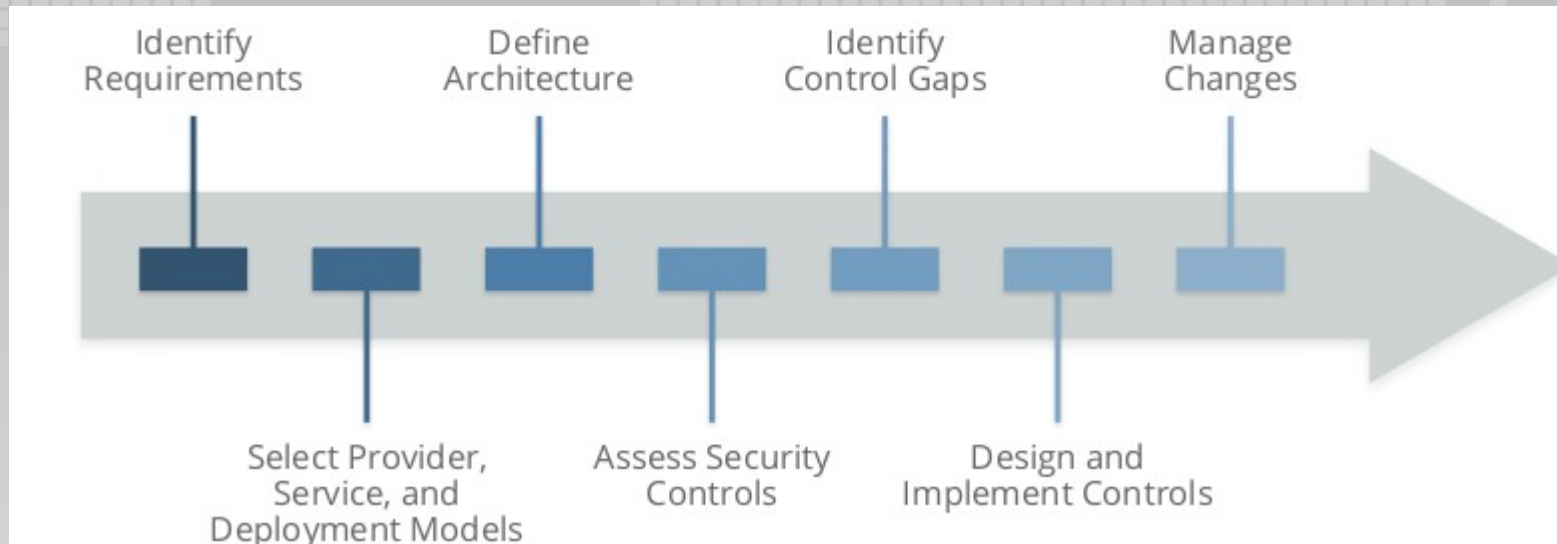











Recomendações iniciais

- Provedores devem documentar de forma clara seus controles internos e segurança de seus clientes
- Provedores também devem projetar e implementar estes controles
- Usuários devem para cada projeto criar uma matriz de responsabilidades onde indique quem está implementando que controle e como



Arquitetura de segurança



Domain	Title	Description
6	 Management Plane and Business Continuity	Securing the management plane and administrative interfaces used when accessing the cloud, including both web consoles and APIs. Ensuring business continuity for cloud deployments.
7	 Infrastructure Security	Core cloud infrastructure security, including networking, workload security, and hybrid cloud considerations. This domain also includes security fundamentals for private clouds.
8	 Virtualization and Containers	Security for hypervisors, containers, and Software Defined Networks.
9	 Incident Response, Notification and Remediation	Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident-handling program.
10	 Application Security	Securing application software that is running on or being developed in the cloud. This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS).
11	 Data Security and Encryption	Implementing data security and encryption, and ensuring scalable key management.
12	 Identity, Entitlement, and Access Management	Managing identities and leveraging directory services to provide access control. The focus is on issues encountered when extending an organization's identity into the cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based Identity, Entitlement, and Access Management (IdEA).
13	 Security as a Service	Providing third-party-facilitated security assurance, incident management, compliance attestation, and identity and access oversight.
14	 Related Technologies	Established and emerging technologies with a close relationship to cloud computing, including Big Data, Internet of Things, and mobile computing.



Recomendações

- Entender as diferenças entre computação em nuvem e infraestrutura tradicional ou virtualização, e como a abstração e a automação impactam a segurança.
- Familiarize-se com o modelo NIST para computação em nuvem e a arquitetura de referência do CSA.
- Usar ferramentas como o CAIQ (Questionário de Iniciativa de Avaliação de Consenso) do CSA para avaliar e comparar provedores de nuvem.



- Os provedores de nuvem devem documentar claramente seus controles e recursos de segurança e publicar usando ferramentas como o CSA CAIQ.
- Usar ferramentas como a Matriz de controles de nuvem da CSA para avaliar e documentar a segurança do projeto em nuvem e requisitos e controles de conformidade, bem como quem é responsável por cada um.
- Usar um modelo de processo de segurança na nuvem para selecionar fornecedores, arquiteturas de design, identificar controle lacunas e implementar controles de segurança e conformidade.



About me

Profissional formando em Redes de Computadores, certificado pela CompTIA Linux+. Cofundador da empresa de consultoria Vault Cyber Security. Entusiasta de software livre e de segurança da informação. Líder no capítulo Natal da OWASP, organização internacional que visa fomentar segurança em aplicações web.



OWASP
Open Web Application
Security Project