Fd-Rie
Formación docente
revista iberoamericana de educación

Artículo

Tendências e vulnerabilidades de segurança em sistemas baseados em nuvem para processos educacionais

Tendencias de seguridad y vulnerabilidades en sistemas basados en la nube para procesos educativos

Security trends and vulnerabilities in cloud-based systems for educational processes

Pamela Govin

Doctor en ciencia. Université de Reims Champagne Ardenne, Brasilia, Brasil, https://orcid.org/0000-0003-0009-1005, pamelagovin@urca.edu.br

Recebido Outubro de 2018 - Aceito em maio de 2019

Formación docente - revista iberoamericana de educación
http://www.revista-iberoamericana.org/index.php/es/index

e-ISSN: 2737-632X

Vol – 2 No. 3, julho - outubro 2019
Pags 43-54

Resumo O constante crescimento da tecnologia chegou ao ponto em que muitos serviços que eram usados anteriormente na infraestrutura física da empresa ou organização agora podem ser fisicamente hospedados em qualquer lugar do mundo e acessados pela Internet. "Serviços na nuvem". Isso leva ao aumento da segurança e devem ser tomadas medidas para evitar ataques ao serviço. Os dados estatísticos sobre eventualidades levantadas recentemente serão analisados e várias recomendações para sua prevenção serão revisadas.

Palavras-chave: Segurança, Técnicas de ataques, Serviços em nuvem

Resumen El constante crecimiento de la tecnología ha llegado al punto donde muchos servicios que antes eran usados desde la propia infraestructura física de la empresa u organización, ahora pueden estar alojados físicamente en cualquier parte del mundo y accedidos haciendo uso del internet, a esto lo conocemos como “Cloud Services”. Esto conlleva a que las seguridades se incrementen y se deban tomar medidas para evitar ataques al servicio. Se analizarán datos estadísticos sobre las eventualidades suscitadas últimamente y se revisarán varias recomendaciones para prevención de las mismas.
Palabras clave: Seguridad informática, informáticos, Técnicas de ataques informáticos, Servicios en la nube

Abstract. The constant growth of technology has reached the point where many services that were used before from the physical infrastructure of the company or organization, can now be physically housed anywhere in the world and access to use the internet, this We know it like "Services in the cloud". This leads to increased security and measures to prevent attacks on the service. Statistical data will be analyzed on the eventualities that have arisen recently and several recommendations for the prevention of these will be reviewed.
Key words: Computer security, Computer services, Techniques of computer attacks

INTRODUÇÃO

Nos últimos anos, a tecnologia evoluiu de tal forma que os equipamentos de informática dependem fortemente da Internet para se interconectar com outros equipamentos e trocar recursos. Isso dá origem ao conceito de CLOUD ou Cloud Computing, que (Reimche, 2013) o define como "computação baseada na Internet usando recursos compartilhados", que ao longo dos anos

evolui até o uso de serviços de servidor no nuvem, que para as empresas representa economia no custo de manutenção, licenciamento e até economia de recursos humanos, pois todos esses serviços são gerenciados por um provedor que cuidará de todo o trabalho.

O termo computação em nuvem se disseminou, referindo-se a soluções tecnológicas de software como serviço. O importante para o usuário é que o serviço funcione corretamente, não importa onde o servidor esteja localizado. A demanda por esses serviços aumentou nos últimos dois anos em todo o mundo por clientes corporativos e entidades públicas.

O gráfico a seguir mostra a evolução da receita de serviços de computação em nuvem em todo o mundo de 2013 a 2015, bem como previsões para 2016 e 2019. (statista.com, 2016). A estatística inclui uma distribuição por área geográfica da mesma.

Como podemos ver, na União Européia, o volume de negócios para a prestação de serviços em nuvem cresceu continuamente ao longo do período, de modo que em 2015 excedeu pela primeira vez o valor de 20.000 milhões de euros.

Existem diferentes tipos de serviços de servidor em nuvem, incluindo IaaS (Infraestrutura como Serviço), definido pelo Gartner, como “uma oferta padronizada e altamente automatizada, onde eles pertencem a recursos de computação, complementados por recursos de armazenamento e rede e realizada por um provedor de serviços e oferecida a clientes sob demanda ". (Gartner, 2017). Portanto, quem contrata esse serviço tem total controle e responsabilidade sobre a infraestrutura hospedada na nuvem.

Outro tipo de serviço é o SaaS (Software como Serviço), conforme definido pelo Gartner, é um software proprietário, entregue e gerenciado remotamente por um ou mais fornecedores. (Gartner, 2017), onde é o provedor de serviços responsável pela administração total do equipamento na nuvem. Este trabalho

tratará especificamente do SAS, uma vez que, dadas as facilidades que oferece aos usuários, é o mais oferecido e, portanto, representa um desafio em termos de segurança de computadores.

Os provedores de serviços SAS têm como principal preocupação a segurança não apenas física, mas lógica de seus equipamentos e serviços; portanto, devem ser consideradas as vulnerabilidades às quais os servidores estão expostos, dentre elas temos

DoS: Negação de serviço.

SPAM: Entrega em massa

Roubo de identidade.

Nessa situação, a pergunta a ser feita é: quais são os níveis de percepção de risco nos sistemas de computação baseados em nuvem?

Isso influencia bastante o desenvolvimento do negócio de serviços em nuvem, especialmente na área de servidores, uma vez que o nível de valorização da segurança pelos clientes afetará a decisão de comprar ou não o serviço, portanto, é um problema. Ele deve ser tratado com os requisitos do caso para o desenvolvimento e evolução do uso da tecnologia em nuvem.

Tudo isso nos leva à seguinte hipótese: "O aumento no uso de serviços em nuvem é exigente para maximizar os níveis de segurança pelos fornecedores"

Se a segurança das informações não for oferecida, as pessoas dificilmente decidirão confiar as informações a um serviço em nuvem; portanto, as diferentes circunstâncias que enfraquecem a segurança das informações nesses serviços devem ser analisadas.

O objetivo deste trabalho é determinar os métodos de segurança para impedir ataques a servidores hospedados na nuvem.

MÉTODOS E MATERIAIS

O estudo foi realizado analisando dados estatísticos de diferentes empresas comerciais especializadas em segurança, analisando a demanda por serviços em nuvem e analisando software estratégico para evitar ataques.

As empresas na América Latina estão fazendo mais uso dos servidores em nuvem, de acordo com (TI, 2017) “Uma pesquisa global da IBM, realizada com mais de 1.000 executivos de 18 setores, indica que quase todas as empresas pesquisadas estão usando a nuvem , mas apenas em algumas áreas de seus negócios ”.

Você pode ver o crescimento do investimento nos diferentes tipos de serviços em nuvem que as empresas equatorianas contrataram entre 2015 e 2016, o serviço de software como serviço (SAAS), em que o provedor é responsável por fornecer todos os a facilidade de uso de seus clientes em conjunto com o PAAS (Platform as a Service), no qual o cliente é responsável pelo gerenciamento do servidor na nuvem, mostra um aumento de 6,2 pontos percentuais em 2016, o mesmo Esse aumento é refletido no serviço de infraestrutura como serviço (IAAS).

Evidências do crescimento no uso de serviços em nuvem, o crescimento de ataques a eles é demonstrado. O principal ataque ao qual eles estão expostos é o Denial of Service (DoS) (Brito, 2009) explica que estes "consistem em tirar proveito de um gerenciamento incorreto dos recursos de um aplicativo para fazer solicitações massivas e causar sua saturação", o O gráfico a seguir indica o aumento durante o segundo trimestre de 2016 desse tipo de ataque:

Isso é corroborado pelo digitalattackmap.com, um site especializado em monitorar ataques de negação de serviço em colaboração com o Google e a Arbor Networks, onde os ataques são setorizados

O Equador está nessas estatísticas com uma porcentagem de ataques de 14,34% durante 2016, o que mostra que as vulnerabilidades às quais os servidores em nuvem estão expostos não podem ser detectadas e é preciso tomar precauções.

RESULTADOS

Os números apresentados denotam a insegurança à qual os serviços e servidores em nuvem estão expostos; portanto, é necessário melhorar sua segurança e proteção.

O desenvolvedor interno do software de segurança ModSecurity recomenda que os valores mobiliários a serem utilizados nos servidores em nuvem incluam:

• Monitoramento de segurança de aplicativos em tempo real e controle de acesso

• Registro de tráfego HTTP completo

• Monitoramento de segurança passivo contínuo

• Restrições em aplicativos da web

Embora não exista 100% de segurança na Internet, é necessário que, nos procedimentos básicos de segurança da Web, seja monitorado constantemente a segurança de todos os aplicativos, incluindo o tráfego que utiliza o protocolo HTTP, também é necessário hospedá-lo em o sistema operacional é um antivírus com monitoramento constante do comportamento do arquivo para detectar tentativas de infecção no computador. Por fim, é importante que os aplicativos desenvolvidos para trabalhar na Web, a partir de seu código-fonte, incluam títulos que impeçam o acesso fácil ao banco de dados ou a qualquer outra instância do servidor.

Para evitar esse tipo de ataque, um sistema IPS de prevenção de intrusões, definido pela Panda Security (PANDA SECURITY, 2017), deve ser implementado para controlar o acesso em uma rede de computadores para

proteger os sistemas de ataques e abusos. Ele foi projetado para analisar os dados do ataque e pará-lo no momento em que está sendo produzido e antes de ser bem-sucedido.

As soluções baseadas na nuvem, como o Kona Site Defender, oferecem escalabilidade integrada e alcance global para se defender dos tipos mais comuns de ataques DoS, além de ataques contra aplicativos da Web (injeções de SQL, scripts entre sites etc.) e ataques diretos a origem.

O DoS Kona Site Defender atenua os ataques de DoS absorvendo o tráfego de DoS direcionado no nível do aplicativo, desviando todo o tráfego de DoS direcionado no nível da rede, como inundações SYN ou UDP, e autenticando o tráfego válido no fim da rede. Essa solução de proteção interna está "sempre ativada" e apenas o tráfego é permitido na porta 80 (HTTP) ou na porta 443 (HTTPS). Os serviços associados ao tráfego de DoS podem ser limitados, e o recurso de cache flexível maximiza o download da fonte. (AKAMAI.COM, 2017).

O gerenciamento dessa ferramenta de segurança permite manter a disponibilidade de sites sem redirecionar o tráfego e sem afetar o desempenho, pois possibilita o gerenciamento de Tb // s do tráfego diário.

Os recursos de mitigação de DoS são implantados no caminho para fornecer proteção apenas a um salto de rede a partir do ponto de solicitação do servidor em nuvem.

É uma solução flexível, configurando um número ilimitado de regras personalizadas para proteção de aplicativos em nuvem.

O Kona Site Defender inclui uma coleção completa de proteções de firewall predefinidas, mas configuráveis, para a camada de aplicativos, que periodicamente mantém com atualizações em diferentes categorias, como: protocolo, violações da política HTTP e limites de solicitação, robôs

maliciosos, ataques genéricos injeção de comando, Trojans backdoor e vazamento de conteúdo de saída.

Esta solução é mais eficiente do que o IDS atual, sistema de detecção de intrusão, age de maneira reativa. Evitando maiores perdas econômicas para empresas que optam por um sistema IPS.

Algumas vantagens sobre os serviços IDS são mencionadas:

• Integração simples com a infraestrutura de TI existente.

• Maximização do tempo de atividade e disponibilidade durante ataques de DoS.

• Defesa da infraestrutura de aplicativos da web.

Escalabilidade.

• Manutenção de desempenho, mesmo em caso de ataque.

No Equador, está iniciando a implementação desses sistemas de prevenção de ataques, a fim de impedir o crescimento de intrusões no nível de serviços fornecidos por servidores em nuvem, como é o caso de serviços bancários, compras on-line, serviços gerais de marketing na web.

CONCLUSÕES

O objetivo dos ataques DDoS é tentar bloquear e se infiltrar nos sites inundando o servidor de origem do site com solicitações falsas, de vários locais e redes. Globalmente, os ataques de negação de serviço (DoS) estão aumentando em aproximadamente 28%, de acordo com as informações de mapeamento apresentadas pelo portal www.digitalattackmap.com, se os números da China e dos EUA forem tomados como referência. , principais países de destino para esse tipo de ataque. No Equador, deve-se impedir o crescimento desse tipo de ataque, que em 2016 apresentou 14,34% do total

mundial, com a implementação de soluções em nuvem para o desvio do tráfego de DoS.

Devido ao crescente número e escala de ataques de DoS, os provedores de serviços em nuvem devem considerar o planejamento para a detecção e mitigação de ataques de DoS, bem como a implementação de sistemas de defesa para proteger a nuvem, dentro de suas políticas comerciais. servidor de nome de domínio que enfrenta sobrecargas e ataques de negação de serviço.

Para empresas com serviços em nuvem e grandes volumes de vendas ao consumidor, transações entre empresas, usuários de aplicativos SaaS e jogos online. É imperativo que eles adotem soluções de segurança em nuvem que lhes permitam se proteger e garantir acesso ininterrupto a sites e aplicativos.

A implementação de ferramentas como o Kona Site Defender, para proteger sites e APIs de ataques sofisticados com um kit de ferramentas multicamada, é essencial para mitigar esse tipo de ataque. Os recursos de defesa do DoS estão sempre ativos, portanto, não há necessidade de redirecionar o tráfego antes do início do processo de mitigação.

REFERÊNCIAS

AKAMAI.COM. (Enero de 2017). *https://www.akamai.com/es/es/resources/protect-against-ddos-attacks.jsp*. Recuperado el 22 de Mayo de 2017, de https://www.akamai.com/es/es/resources/protect-against-ddos-attacks.jsp: https://www.akamai.com/es/es/resources/protect-against-ddos-attacks.jsp

AppArmor.com. (Octubre de 2016). *wiki.ubuntu.com/AppArmor*. Recuperado el 17 de Mayo de 2017, de wiki.ubuntu.com/AppArmor: wiki.ubuntu.com/AppArmor

Barros-Bastidas, C., & Turpo, O. (2020). La formación en investigación y su incidencia en la producción científica del profesorado de educa- ción de una universidad pública de Ecuador. *Publicaciones, 50*(2), 167–185. doi:10.30827/publicaciones.v50i2.13952

Barros Bastidas, C., & Turpo Gebera, O. (2018). Factors influencing the scientific production of university professors: a systematic review . *Pensamiento Americano*, *11*(22). https://doi.org/10.21803/pensam.v11i21-1.276

Brito, N. (2009). *Manual de Desarrollo Web con GRAILS.* Imaginaworks.

Clamav.net. (Octubre de 2016). *https://www.clamav.net/documents/installing-clamav*. Recuperado el 17 de Mayo de 2017, de https://www.clamav.net/documents/installing-clamav: https://www.clamav.net/documents/installing-clamav

Gartner. (Febrero de 2017). *http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas/*. Recuperado el 15 de Mayo de 2017, de http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas/: http://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas/

Gartner. (Febrero de 2017). *http://www.gartner.com/it-glossary/software-as-a-service-saas/*. Recuperado el 15 de Mayo de 2017, de http://www.gartner.com/it-glossary/software-as-a-service-saas/: http://www.gartner.com/it-glossary/software-as-a-service-saas/

MODSECURITY. (Noviembre de 2016). *https://modsecurity.org/about.html*. Recuperado el 17 de Mayo de

2017, de https://modsecurity.org/about.html: https://modsecurity.org/about.html

Nixory. (Noviembre de 2013). *http://nixory.sourceforge.net/about.html*. Recuperado el 17 de Mayo de 2017, de http://nixory.sourceforge.net/about.html: http://nixory.sourceforge.net/about.html

PANDA SECURITY. (Enero de 2017). *http://www.pandasecurity.com/spain/support/card?id=31463*. Recuperado el 22 de Mayo de 2017, de http://www.pandasecurity.com/spain/support/card?id=31463: http://www.pandasecurity.com/spain/support/card?id=31463

Reimche, T. (2013). Tecnology Briefing. *Alberta Goverment*.

statista.com. (Octubre de 2016). *https://es.statista.com/estadisticas/573149/facturacion-por-servicios-de-cloud-a-nivel-mundial-por-area-geografica/*. Recuperado el 15 de Mayo de 2017, de https://es.statista.com/estadisticas/573149/facturacion-por-servicios-de-cloud-a-nivel-mundial-por-area-geografica/: https://es.statista.com/estadisticas/573149/facturacion-por-servicios-de-cloud-a-nivel-mundial-por-area-geografica/

TI, D. (2017). *Diario Ti.* Obtenido de diarioti.com.

von Feigenblatt, Otto Federico, Garcia Marquez' Magical Realism as a Representation of Latin America's Socio-Political Reality: Developmental Simultaneity and Exceptionalism in Latin America as Expressed in Historiographic Metafiction

(December 27, 2009). The Expression, Vol. 2, No. 1, pp. 1-6, 2009, Available at SSRN: https://ssrn.com/abstract=1596690

von Feigenblatt, Otto Federico, A Socio-Cultural Analysis of Romantic Love in Japanese Harem Animation: A Buddhist Monk, a Japanese Knight, and a Samurai (September 16, 2010). Journal of Asia Pacific Studies, Vol. 1, No. 3, pp. 636-646, 2010, Available at SSRN: https://ssrn.com/abstract=1760643

von Feigenblatt, Otto Federico, Costa Rica's Foreign Policy: Can 'Right' Become 'Might'? (November 27, 2008). Journal of Alternative Perspectives in the Social Sciences, Vol. 1, No. 1, pp. 11-15, 2008, Available at SSRN: https://ssrn.com/abstract=1308245