EDUARDO RIBEIRO TOLEDO

SEGURANÇA EM COMPUTAÇÃO EM NUVEM: UM ESTUDO DE CASO DAS COMUNICAÇÕES UNIFICADAS DE UMA UNIVERSIDADE DE GRANDE PORTE

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para a conclusão do curso de MBA em Tecnologia de Software.

Área de Concentração: Tecnologia de Software

Orientador: Prof. Dr. Marcos A. Simplício

São Paulo
2014

FICHA CATALOGRÁFICA

Toledo, Eduardo Ribeiro
Um estudo de caso das comunicações unificadas de uma universidade de grande porte / E.R. Toledo. -- São Paulo, 2014.
56 p.

Monografia (MBA em Tecnologia de Software) – Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1.Computação em nuvem I.Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia II.t.

DEDICATÓRIA

Dedico este trabalho aos meus pais e às minhas irmãs que sempre me deram apoio para que continuasse meus estudos e tiveram muita paciência comigo durante os últimos anos.

AGRADECIMENTOS

Ao professor Marcos A. Simplício pela preciosa orientação, confiança e dedicação dados durante a elaboração deste trabalho.

À Universidade de São Paulo – USP que forneceu a infraestrutura e recursos necessários ao bom aproveitamento do curso de pós-graduação.

À Escola Politécnica da Universidade de São Paulo – EPUSP e ao Programa de Educação Continuada em Engenharia – PECE que disponibilizam cursos de altíssima qualidade.

Aos meus amados pais, Renê Júlio de Lima Toledo e Arlete Ribeiro Toledo, que me apoiaram da melhor forma que se possa imaginar por toda minha vida e por fazerem sempre o possível para me fornecer a melhor educação possível.

Ao meu amigo Gercel de Araújo e Silva que me indicou o curso de MBA em Tecnologia de Software e motivou a fazê-lo.

Aos meus amigos de trabalho que sempre foram prestativos e atenciosos ao fornecer detalhes e sanarem dúvidas sobre detalhes do projeto de comunicações unificadas na nuvem da universidade de grande porte.

RESUMO

Este é um trabalho sobre a computação em nuvem e as preocupações de segurança introduzidas ou diretamente afetadas por essa tecnologia. São apresentados e discutidos resultados de pesquisas sobre as principais preocupações de segurança relacionadas à computação em nuvem e então são discutidas em maiores detalhes algumas dessas preocupações. Dentre os principais pontos discutidos, destacam-se, no ambiente de computação em nuvem, a segurança de redes e a segurança de dados. As discussões e resultados obtidos são então aplicados no estudo de caso de um projeto de comunicações unificadas baseada em nuvem de uma universidade de grande porte.

ABSTRACT

This is a work on cloud computing and security concerns introduced or directly affected by this technology. Research findings on the major security concerns related to cloud computing are presented and discussed and then some of these concerns are presented in details. Among the main points discussed, network and data security in the cloud computing environment are of special interest. The discussions and results found are then applied in the case study of a proposed cloud-based unified communications project of a large university.

LISTA DE ILUSTRAÇÕES

Pág.

Figura 1 – Taxonomia da Segurança em Nuvem..... 24
Figura 2 – Problemas de segurança agrupados por categoria.....25
Figura 3 – Domínios de segurança antes e depois da virtualização..... 29
Figura 4 – Comunicação entre máquinas virtuais.....30
Figura 5 – Exemplo de Ataque de Envelopamento..... 33
Figura 6 – Componentes de uma localidade..... 43

LISTA DE TABELAS

Pág.

Tabela 1 – Resumo dos modelos de serviço identificados..... 44
Tabela 2 – Resumo das questões de segurança do modelo IaaS..... 46
Tabela 3 - Resumo das questões de segurança dos modelos PaaS e SaaS..... 48
Tabela 4 – Resumo das questões de segurança de dados..... 49

SUMÁRIO

1. INTRODUÇÃO 11
1.1. Motivações 11
1.2. Objetivo 12
1.3. Justificativas 12
1.4. Estrutura do Trabalho 13
2. REVISÃO BIBLIOGRÁFICA 15
3. FUNDAMENTAÇÃO TEÓRICA 17
3.1. Computação em Nuvem: Uma definição 17
3.2. Características Essenciais da Computação em Nuvem 17
3.3. Os Modelos de Serviço da Computação em Nuvem 19
3.4. Os Modelos de Implantação da Computação em Nuvem 20
3.5. Virtualização 21
3.6. Segurança na web 22
4. SEGURANÇA EM COMPUTAÇÃO EM NUVEM 23
4.1. Segurança de Rede 26
4.1.1. Modelo IaaS 27
4.1.1.1. Fronteiras de rede quebradas 28
4.1.1.2. Tráfego invisível de dados 29
4.1.1.3. Gerenciamento da segurança no tráfego de rede 31
4.1.2. Modelos PaaS e SaaS 32
4.1.2.1. Serviços web 32
4.1.2.2. Navegadores web 33
4.2. Segurança de Dados 34
4.2.1. Espionagem da Agência Nacional de Segurança 36
5. ESTUDO DE CASO 39
5.1. O Projeto de Comunicações Unificadas na Nuvem 40
5.1.1. Particularidades e Detalhes Técnicos do Projeto 42
5.1.2. Identificando os Modelos de Serviço 43
5.2. Segurança em Comunicações Unificadas na Nuvem 45
6. CONSIDERAÇÕES FINAIS 51
6.1. Trabalhos Futuros 52
REFERÊNCIAS 53
GLOSSÁRIO 55

1. INTRODUÇÃO

A computação em nuvem está se tornando cada vez mais presente no dia a dia tanto de corporações quanto de usuários comuns. O termo *computação em nuvem* é amplo e abrange diversos conceitos de computação distribuída, tais como armazenamento remoto de arquivos pela Internet, execução de aplicações remotas, hospedagem de banco de dados em servidores externos, virtualização de infraestrutura de hardware etc. (CARROLL; VAN DER MERWE; KOTZE, 2012).

Entre os atrativos da computação em nuvem estão a terceirização de recursos físicos computacionais permitindo a utilização de recursos que de outra forma estariam indisponíveis, a redução de custos operacionais na virtualização de infraestrutura de hardware. A computação em nuvem também introduziu ou reformulou modelos de negócios, como a terceirização de infraestruturas de hardware, software e aplicações.

Como toda nova tecnologia que se encontra em fase de introdução ou evolução, existem preocupações cabíveis por parte daqueles que as adotam. Enquanto as preocupações dos usuários comuns normalmente se restringem a capacidade/limitações do serviço, disponibilidade e preço, as preocupações das corporações são mais complexas e abrangentes. Em especial, como as corporações possuem maior exposição e, portanto, são alvos potenciais de atacantes, a segurança se torna um item de extrema importância.

1.1. Motivações

O estudo de itens relacionados à segurança em ambientes computacionais é importante, independentemente da aplicação final. Afinal, a possibilidade de perdas é grande ao se abdicar ou dar pouca atenção à segurança. Além de perdas financeiras imediatas, problemas decorrentes de falta de segurança levam a situações complexas, como a avaliação total do impacto quando informações confidenciais de uma empresa são roubadas e como a credibilidade de uma empresa é afetada e seus concorrentes são beneficiados pelo fato.

A introdução da computação em nuvem introduziu novas variáveis no tocante a questões de segurança. Por exemplo, a virtualização possibilitou que diversas máquinas virtuais compartilhassem o mesmo servidor físico. Desta forma, o cenário que antes era composto por soluções hospedadas em servidores distintos começou a apresentar soluções que precisam dividir recursos de processamento, memória RAM, interfaces de rede, etc. Este compartilhamento de recursos é uma variável nova que demanda novos estudos para que se tenha maior compreensão de suas vulnerabilidades e como amenizá-las.

Além destas novas preocupações, questões de segurança antigas precisam ser revistas com as novas possibilidades de cenários para abranger e atender novos paradigmas impostos pela nova tecnologia. Entre outros casos, a computação em nuvem introduziu a possibilidade de empresas utilizarem um banco de dados hospedado em um ambiente externo à intranet da empresa como seu banco de dados corporativo. Os dados que antes trafegavam pela intranet agora são transmitidos pela Internet e podem conter informações sensíveis que não devem estar acessíveis a terceiros.

1.2. Objetivo

Este trabalho tem como objetivo discutir algumas das preocupações relacionadas à segurança, tanto as que são específicas desta nova tecnologia como aquelas que são derivadas das alterações que a computação causou no ambiente da computação. É dado especial destaque a questões de segurança de redes e segurança de dados. Adicionalmente, o trabalho tem também como objetivo analisar a aplicabilidade destas questões no projeto de comunicações unificadas de uma universidade de grande porte, que está sendo implantado por uma empresa multinacional especializada em comunicações.

1.3. Justificativas

Os estudos sobre segurança em ambiente computacionais são importantes no ambiente interconectado e competitivo no qual a computação em nuvem está inserida. A computação em nuvem se encontra em processo de expansão, de modo

que vem sendo adotados entre instituições como empresas, órgãos públicos, indivíduos etc.

Entre as mudanças que a computação em nuvem introduziu, uma das mais importantes é a que diz respeito à **rede** (GONZALEZ et al., 2011). Diversas tecnologias de computação em nuvem fazem uso intenso e/ou diferenciado dos recursos na rede de computadores. Por exemplo, a virtualização de infraestrutura pode utilizar a rede intranet para armazenamento de máquinas virtuais enquanto outra empresa pode terceirizar toda sua solução de banco de dados na nuvem. Além disso, a computação em nuvem introduziu alguns modelos que permitem que todos os **dados** de uma pessoa ou organização estejam armazenados em uma nuvem remota e, desta forma, necessitem trafegar pela rede pública de dados. Quando esses dados são sigilosos, gera-se uma preocupação que demanda atenção, tanto que o controle sobre dados está entre os três itens individuais mais citados entre as preocupações de segurança na computação em nuvem (GONZALEZ et al., 2011). O tema segurança de dados se tornou particularmente mais evidente após a divulgação dos casos de espionagem da NSA (*National Security Agency*, a agência de segurança nacional dos Estados Unidos da América), prejudicando muito a confiança dos usuários de computação em nuvem quanto à segurança de dados.

Neste contexto, a escolha do ambiente de comunicações unificadas de uma universidade de grande porte se mostrou um estudo de caso interessante por utilizar dois conceitos de computação em nuvem: o lado da empresa e o lado do usuário. Especificamente, a infraestrutura do projeto utiliza a nuvem em sua hospedagem e os usuários utilizam a solução em outra nuvem, de modo que diversas questões sobre segurança surgem naturalmente neste cenário.

1.4. Estrutura do Trabalho

O restante deste documento está organizado da seguinte forma.

O Capítulo 2 apresenta o resumo dos estudos realizados durante a elaboração deste documento.

O Capítulo 3 apresenta conceitos básicos que são mencionados ou discutidos ao longo deste documento sobre a computação em nuvem.

No Capítulo 4 são analisadas as questões de segurança em nuvem que são o foco do presente estudo, a saber: (1) a camada de rede, e (2) a segurança de dados, com atenção no caso de espionagem da NSA.

O Capítulo 5 apresenta uma análise de como os conceitos de segurança da computação em nuvem se aplicam ao cenário de comunicações unificadas na nuvem de uma universidade de grande porte.

O Capítulo 6 apresenta conclusões e considerações finais sobre a análise apresentada neste documento.

2. REVISÃO BIBLIOGRÁFICA

Devido à importância que a área de computação em nuvem vem acumulando durante os últimos anos, diversos estudos vêm sendo realizados sobre o assunto. Exemplos incluem as mais de 50 referências pesquisadas por Gonzalez et al. (2011) em seu estudo sobre as maiores preocupações de segurança na computação em nuvem. Esses estudos são amplos e ainda não existe um ponto de convergência, sendo que muitos deles apresentam temas relacionados a questões políticas e de negócios, enquanto outros analisam questões técnicas. Mesmo os estudos de natureza técnica discutem temas que vão desde tecnologias que sofreram alterações com o advento da computação em nuvem até aqueles que discutem as questões que foram introduzidas com a computação em nuvem. A seguir são apresentados alguns dos documentos mais relevantes para o presente estudo.

O artigo 'A quantitative analysis of current security concerns and solutions for cloud computing', de Gonzalez et al. (2011) apresenta um estudo sobre as maiores preocupações de segurança na computação em nuvem. Assim, ele realiza um estudo quantitativo e propõe uma classificação das preocupações de segurança em categorias. Esta classificação serviu como base para identificar algumas das principais linhas de estudo que poderiam ser utilizadas neste trabalho.

O artigo 'On technical security issues in cloud computing' de Jensen et al. (2009) apresenta um estudo sobre questões técnicas de segurança relacionadas aos modelos de nuvem PaaS e SaaS. A maioria dos artigos com discussões específicas sobre tais modelos de nuvem discutem principalmente questões relacionadas a políticas e normas de segurança, mas Jensen et al. (2009) apresenta um estudo mais técnico, adequada ao nível proposto por este trabalho.

O artigo 'Security for networks virtual access of cloud computing', de Sun e Hu (2012), discute os problemas relacionados a redes na computação em nuvem e apresenta as soluções que estão sendo desenvolvidas e adotadas pelo mercado. Esse trabalho apresentou discussões e preocupações técnicas sobre a segurança de redes na computação em nuvem, influenciando nas decisões tomadas no estudo de caso do presente trabalho.

Finalmente, as publicações de Green (2013) em seu blog de segurança contribuíram nas discussões sobre a segurança de dados na nuvem pública deste estudo. Green é um autor reconhecido no campo de segurança e apresentou discussões importantes sobre o caso de espionagem promovido pela Agência de Segurança Nacional do governo dos Estados Unidos da América.

3. FUNDAMENTAÇÃO TEÓRICA

A computação em nuvem é um conceito de computação que está cada vez mais presente no dia a dia das pessoas. Entretanto, a definição do que consiste a computação em nuvem ainda é muitas vezes confusa, não sendo incomum que usuários de computação em nuvem não conheçam os conceitos envolvidos. Assim, com o objetivo de facilitar a discussão, neste capítulo são discutidos brevemente os principais componentes e conceitos envolvidos nestes sistemas.

3.1. Computação em Nuvem: Uma definição

A virtualização de servidores é um dos principais componentes que viabilizou a computação em nuvem e que está ajudando a difundi-la (ARMBRUST et al., 2010). No entanto, a computação em nuvem não se restringe apenas à virtualização. A definição de computação em nuvem de acordo com o Instituto Nacional de Padrões e Tecnologia do Ministério do Comércio dos Estados Unidos da América, NIST, é:

> *"A computação em nuvem é um modelo para habilitar o acesso por rede ubíquo, conveniente e sob demanda a um conjunto compartilhado de recursos de computação (como redes, servidores, armazenamento, aplicações e serviços) que possam ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços"* (MELL; GRANCE, 2011).

O NIST também define que seu modelo de computação em nuvem inclui cinco características essenciais, três modelos de serviço e quatro modelos de implantação, os quais são detalhados nas seções a seguir.

3.2. Características Essenciais da Computação em Nuvem

As características essenciais da computação em nuvem afetam tanto os consumidores quanto os fornecedores de computação em nuvem. Enquanto os

fornecedores são afetados pela necessidade de prover tais características, os consumidores desejam utilizá-las.

As cinco características essenciais da computação em nuvem segundo o NIST são (MELL; GRANCE, 2011):

- **Autosserviço sob demanda** (*on-demand self-service*) – Um usuário consegue provisionar funcionalidades computacionais unilateralmente e automaticamente, sem intervenção humana do fornecedor de serviços.
- **Amplo acesso à rede** (*broad network access*) – As funcionalidades são disponibilizadas pela rede e acessadas através de mecanismos padrão, permitindo o uso através de diferentes plataformas, sejam elas clientes magros (*thin clients)* ou gordos (*thick clients).*
- **Recursos compartilhados** (*resource pooling*) – Os recursos do provedor de serviços são compartilhados para atender múltiplos consumidores no modelo de locação múltipla (*multitenant*), com diferentes recursos físicos e virtuais dinamicamente distribuídos e redistribuídos de acordo com a demanda dos consumidores. Existe um senso de independência de localização dos recursos provisionados, de modo que o consumidor não tem controle ou conhecimento da localização dos recursos além de um nível de abstração elevado (por exemplo, país, estado ou datacenter).
- **Elasticidade veloz** (*rapid elasticity*) – Funcionalidades podem ser provisionadas e liberadas rapidamente e até automaticamente em alguns casos, permitindo expansão ou retração conforme a demanda. Para o consumidor, a capacidade de provisionamento parece ilimitada e pode ser alterada em qualquer quantidade a qualquer momento.
- **Serviço mensurável** (*measured service*) – Sistemas de computação em nuvem controlam e aperfeiçoam o uso de recursos através de uma capacidade de medição em algum nível de abstração adequado ao tipo de serviço fornecido (e.g., armazenamento, processamento, banda de rede, contas de usuários ativos, etc.). A utilização de recursos é monitorada, controlada e reportada, fornecendo transparência tanto para o fornecedor quanto para o consumidor do serviço utilizado.

3.3. Os Modelos de Serviço da Computação em Nuvem

Os modelos de serviço definem a forma como a computação em nuvem é comercializada entre os fornecedores e consumidores. A comercialização pode ser simples, como a disponibilização de máquinas virtuais do setor de tecnologia de informação a outras equipes da mesma empresa. Mas elas também podem ser complexas, incluindo contratos com níveis de serviço, regras de provisionamento e envolvendo diversas empresas.

O NIST define três modelos de serviço (MELL; GRANCE, 2011):

- **IaaS** – Infraestrutura como serviço, do inglês *Infraestructure as a Service*. O recurso fornecido ao consumidor é provisionar processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais. O consumidor pode então usar tais recursos para instalar e executar softwares em geral, incluindo sistemas operacionais e aplicativos. O consumidor não gerencia nem controla a infraestrutura na nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento, e aplicativos instalados, e possivelmente um controle limitado de alguns componentes de rede, como firewalls.
- **PaaS** – Plataforma como serviço, do inglês *Plataform as a Service*. O recurso fornecido ao consumidor é instalar na infraestrutura da nuvem aplicativos criados ou adquiridos pelo consumidor, desenvolvidos com linguagens de programação, bibliotecas, serviços e ferramentas suportados pelo fornecedor ou compatíveis. O consumidor não gerencia nem controla a infraestrutura na nuvem subjacente, incluindo rede, servidores, sistema operacional ou armazenamento, mas tem controle sobre as aplicações instaladas e possivelmente configurações do ambiente de hospedagem de aplicações.
- **SaaS** – Software como serviço, do inglês *Software as a Service*. O recurso fornecido ao consumidor é o uso de aplicações do fornecedor executando em uma infraestrutura na nuvem. As aplicações podem ser acessadas por vários dispositivos clientes através de interfaces magras ou gordas, tais como um navegador web (como em serviços de e-mail baseados na web), ou por uma interface de acesso proprietária. O consumidor não gerencia nem controla a

infraestrutura na nuvem subjacente, incluindo rede, servidores, sistemas operacionais, armazenamento, ou mesmo recursos individuais da aplicação, com a possível exceção de configurações limitadas por usuário.

3.4. Os Modelos de Implantação da Computação em Nuvem

Os modelos de implantação definem a forma como a computação em nuvem é apresentada aos consumidores. Também permite definir os responsáveis pelos elementos que compõe determinada implantação da computação em nuvem.

O NIST define quatro modelos de implantação (MELL; GRANCE, 2011):

- **Nuvem privada** – A infraestrutura da nuvem é provisionada para o uso exclusivo de uma única organização constituída de múltiplos usuários e/ou unidades de negócio. A nuvem pode pertencer, ser gerenciada e operada pela própria organização, um terceiro ou uma combinação de ambos. Pode existir com ou sem premissas acordadas entre fornecedores e usuários.
- **Nuvem comunitária** (community cloud) – A infraestrutura da nuvem é provisionada para o uso exclusivo de uma comunidade de consumidores de uma organização que compartilham alguma preocupação (e.g., missão, segurança, política, etc.). A nuvem pode pertencer, ser gerenciada e operada por um ou mais membros da organização, um terceiro ou uma combinação de ambos. Pode existir com ou sem premissas acordadas entre fornecedores e usuários.
- **Nuvem pública** – A infraestrutura de nuvem é provisionada para uso aberto do público em geral. A nuvem pode pertencer, ser gerenciada e operada por empresas, meio acadêmico, órgão governamental ou uma combinação destes. A nuvem existe segundo premissas definidas pelo fornecedor da nuvem.
- **Nuvem híbrida** – A infraestrutura de nuvem é uma composição de dois ou mais modelos de implantação (privada, comunitária ou pública) que continuam como entidades únicas, mas que estão compromissadas por algum padrão ou tecnologia proprietária que permita portabilidade de dados e/ou

aplicações (e.g., fragmentação de nuvem para balanceamento de carga entre nuvens).

3.5. Virtualização

A virtualização não é um elemento novo no meio computacional. Elementos como mainframes, máquinas virtuais Java, redes virtuais etc. utilizam conceitos de virtualização presentes e difundidos há muito tempo.

A virtualização de servidores é um conceito antigo, que surgiu na década de 1960 com a IBM (SEO, 2009). A partir dos anos 2000, a virtualização ganhou maior foco do mercado, com a intenção de aproveitar recursos computacionais ociosos presente nos servidores modernos, execução de software legados em hardwares modernos, etc.

A virtualização de servidores permite a execução simultânea de diversas máquinas virtuais da família x86 num mesmo servidor físico. Sistemas operacionais completos são executados nestas máquinas virtuais como se estivem sendo executados por hardware reais. Desta forma, a virtualização cria uma camada de 'hardware' compatível com diversos hardwares existentes. A compatibilidade de hardware fornecida pelas máquinas virtuais permite que elas sejam movidas entre diferentes servidores físicos facilmente. Tecnologias existentes permitem migração de máquinas virtuais entre servidores físicos em tempo real.

A virtualização transformou a tecnologia da informação, alterando a forma como aquisição de hardware é feita. Com ela, não há necessidade de alto comprometimento financeiro inicial com a aquisição de hardware: a aquisição pode ser escalonada e crescer sob demanda.

3.6. Segurança na web

Várias tecnologias podem ser combinadas na criação das ferramentas de acesso aos ambientes de computação em nuvem. Entretanto, dois mecanismos de segurança comumente usados em aplicações web são especialmente importantes para a segurança do acesso aos recursos da nuvem (JENSEN et al., 2009): *WS-Security* e TLS.

A segurança de serviços web (*web services*) conhecida como WS-Security é a principal especificação de segurança de tais serviços (JENSEN et al., 2009). O WS-Security define como prover integridade, confidencialidade e autenticação na troca de mensagens SOAP. É através da definição de um item para o cabeçalho SOAP que se permitem as extensões WS-Security. O WS-Security também define como os padrões XML para assinatura digital (*XML Signature*) e cifração (*XML Encryption*) são aplicados às mensagens SOAP (JENSEN et al., 2009).

O protocolo TLS (*Transport Layer Security*, ou segurança na camada de transporte) surgiu em 1999 como sucessor do protocolo SSL (*Secure Sockets Layer*) que havia sido implementado em 1996 pela Netscape. O TLS é o protocolo de segurança mais utilizado no mundo, disponível em todo navegador de Internet. Basicamente, o protocolo consiste nos processos de cifração e decifração de dados TCP utilizando algoritmos e chaves definidos durante o início da comunicação, que também são utilizados para autenticar o servidor e opcionalmente o cliente da comunicação.

4. SEGURANÇA EM COMPUTAÇÃO EM NUVEM

Acadêmicos, organizações governamentais e iniciativa privada de uma forma geral compartilham a visão de que a segurança é considera a funcionalidade chave para a consolidação da computação em nuvem como uma solução robusta (GONZALEZ et al., 2011). Entretanto, um desafio no contexto de computação em nuvem é que a preocupação com segurança não se restringe apenas à soma das questões de segurança herdadas das tecnologias subjacentes, pois novas questões de segurança são inerentes desta nova tecnologia.

A computação em nuvem é uma tecnologia recente e em evolução. Porém, como ela já se encontra adotada em ambientes de produção, existe um esforço em identificar pontos onde a segurança pode ser considerada digna de atenção e na identificação de pontos de vulnerabilidades.

Gonzalez et al. (2011) afirma que a preocupação com tópicos relacionados à segurança é crescente e importante a ponto que alguns órgãos dedicam grupos de estudos para melhor explorar os temas e sugerir soluções. Entre estes órgãos, pode-se citar a ENISA, que não apenas estuda e analisa os riscos da nuvem como também fornece uma lista de estudos e recomendações correlatas. Outro exemplo é a CSA (CSA 2011 apud GONZALEZ et al. 2011), que define e correlaciona domínios de segurança.

Através da análise das preocupações de segurança dos documentos da ENISA (ENISA 2011 apud GONZALEZ et al. 2011) e CSA, Gonzalez et al. (2011) propuseram uma taxonomia para definir um modelo que auxilie tanto nos estudos sobre a segurança na computação em nuvem quanto no suporte a decisões em questões que a envolvam. A taxonomia proposta agrupa as questões de segurança em três grupos fundamentais. A Figura 1 apresenta a taxonomia proposta e o primeiro nível de classificação das questões de segurança.

Figura 1 – Taxonomia da Segurança em Nuvem. Adaptado de Gonzales et al. (2011)

Os três grupos principais de classificação propostos nessa taxonomia são *arquitetura*, *compliance* e *privacidade*. O grupo *arquitetura* abrange itens como configuração de rede, servidores e virtualização; o grupo *compliance* envolve questões administrativas e responsabilidades legais e; o grupo *privacidade* cobre questões sobre a geração, trânsito e armazenamento de informações, bem como melhores práticas sobre este tema. Os grupos principais de classificação são subdivididos em subconjuntos que agrupam questões com afinidade.

Enquanto as subdivisões diretas propostas por Gonzales et al. (2011) para *privacidade* e *compliance* são muito abrangentes (respectivamente, preocupações e princípios; implementação de controles de ciclo de vida e GRC), as subdivisões de *arquitetura* são mais diretas: rede, servidor, aplicação, segurança de dados e armazenamento, gerenciamento de segurança e gerenciamento de acesso e identidade.

Com as classificações e subclassificações definidas, Gonzales et al. (2011) analisam as preocupações relacionadas à computação em nuvem nos meios acadêmico, organizacional e empresarial. O resultado destas análises é uma contabilização das quantidades de referências a grupos de cada classificação, o que indica o grau de preocupação com cada um deles. O resultado é apresentado na Figura 2:

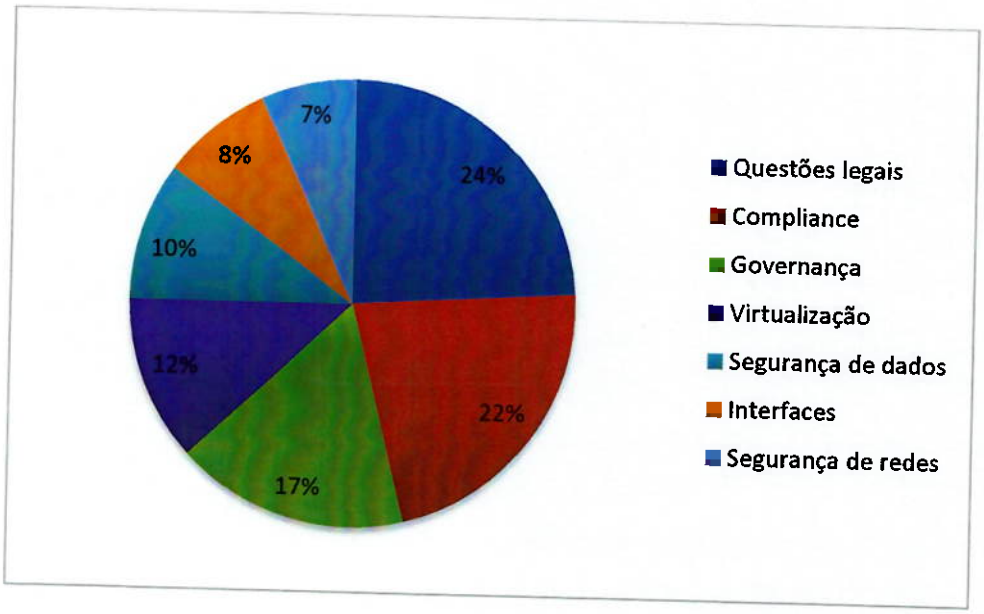

Figura 2 – Problemas de segurança agrupados por categoria. Extraído de Gonzales et al. (2011)

A Figura 2 mostra que os problemas de segurança mais referenciados são de natureza teórica e/ou política (*questões legais*, *compliance* e *governança* com 63% das referências) e não com ligação técnica direta (*virtualização*, segurança de dados, *interfaces* e segurança de redes com 37% das referências). Excluindo-se *virtualização*, os demais problemas de natureza técnica são questões de segurança já existentes antes da adoção da computação em nuvem e que atualmente estão recebendo maior atenção da comunidade devido aos impactos e alterações que a computação em nuvem causou na abordagem clássica da resolução dos problemas de segurança.

Dentro dos problemas de segurança com natureza técnica direta, percebe-se que os problemas de segurança convergem em menor ou maior grau em segurança de rede: segurança de dados, interfaces e segurança de redes. Portanto, conclui-se que as maiores preocupações de segurança na computação em nuvem segundo Gonzalez et al. (2011) que não são nativas desta tecnologia são as alterações de conceitos e na forma de realização de negócios e na infraestrutura de rede.

A partir dos estudos da ENISA e CSA, os estudos de Gonzalez et al. (2011) correlacionam os pontos de segurança na computação em nuvem nos seguintes tópicos, que são discutidos com maior atenção neste documento:

- Segurança de rede: a segurança do ambiente de rede abrange as comunicações na rede e as configurações relacionadas à infraestrutura da computação em nuvem. A segurança de rede ideal é ter a computação em nuvem como uma extensão da rede interna atual (GONZALEZ et al., 2011), permitindo que as mesmas políticas locais sejam aplicadas em qualquer recurso ou processo remoto.
- Segurança de dados: a segurança de dados é definida em termos de confidencialidade, disponibilidade e integridade (GONZALEZ et al., 2011). A segurança de dados será discutida principalmente sob o aspecto da espionagem da NSA, assunto que entrou em evidência em setembro de 2013 a partir de reportagens vinculadas em grandes jornais dos Estados Unidos da América. Esta abordagem é aqui adotada porque, embora a NSA não seja a única fonte de ameaças aos dados na nuvem, os casos envolvendo essa agência são emblemáticos das possíveis consequências da terceirização de dados e serviços.

Como o objetivo deste documento é discutir principalmente os pontos segurança de redes e segurança de dados, os mesmos são apresentados em detalhes a seguir.

4.1. Segurança de Rede

Se fosse necessário resumir a preocupação com a segurança de rede na computação em nuvem num único ponto, poder-se-ia dizer que isto significa aplicar as mesmas regras e restrições da infraestrutura de rede local no ambiente remoto (GONZALEZ et al., 2011). Esta afirmação se aplica a cenários nos quais as nuvens se encontram fora de seu local de utilização final, mas a partir de tal afirmação pode-se entender que as funcionalidades introduzidas ou alteradas pela computação em nuvem no âmbito de segurança de rede são num primeiro momento tratadas de forma equivalente ao já praticado em ambientes tradicionais.

É importante entender e mapear as questões de segurança de rede segundo os conceitos clássicos para, assim, melhor entender suas particularidades. Os estudos de Gonzalez et. al (2011) dividem a segurança de rede em três aspectos principais:

- Segurança de transferência *(transfer security)*: as funcionalidades fornecidas pela computação em nuvem tais como arquiteturas distribuídas, recursos compartilhados e sincronização entre máquinas virtuais demandam transferência massiva de dados;
- Aplicação de firewalls *(firewalling)*: o desenvolvimento de técnicas mais efetivas de firewall e de novas tecnologias para a segurança de dados é uma das urgências para o paradigma de computação em nuvem;
- Configuração de segurança *(security configuration)*: configuração de protocolos, sistemas e tecnologias que forneçam níveis de segurança e privacidade para a computação em nuvem sem prejudicar o desempenho e eficiência.

A análise dos três aspectos de segurança de redes propostos por Gonzalez et al. (2011) evidencia que apenas os pontos que são puramente relacionados à rede foram inclusos em sua classificação. Aspectos relacionados à segurança de redes que possuem pontos em comum com outras categorias foram incluídos em categorias próprias como, por exemplo, aspectos que fazem referências aos limites da rede e à segurança dos dados que estão trafegando por ela. Entretanto, visando uma maior aderência à classificação do NIST para a computação em nuvem (MELL; GRANCE, 2011), o presente estudo busca analisar os diversos aspectos de segurança da nuvem considerando o modelo de computação em nuvem (IaaS, PaaS ou SaaS) no qual ele tem maior relevância.

4.1.1. Modelo IaaS

O IaaS é o mais básico dos modelos de computação em nuvem por ser aplicado diretamente na infraestrutura computacional e, consequentemente, seus aspectos de segurança estão próximos dos componentes tradicionais da computação: *switches* e *switches virtuais* (vSwitches), interfaces de rede e interfaces de rede virtuais (vNICs), servidores e máquinas virtuais (VMs), etc.

Por estar muito próxima do modelo tradicional, a segurança de rede da computação em nuvem no modelo IaaS possui parâmetros bem definidos para comparação

direta. Como a segurança de rede é importante nos cenários tradicionais, espera-se que os mesmos aspectos sejam tratados de forma equivalente na ambiente da computação em nuvem. De fato, conforme afirma Sun e Hu (2012), segurança de rede é um dos aspectos chave para o modelo IaaS ser bem sucedido na computação em nuvem.

Alguns dos principais desafios da segurança em rede no que se refere ao modelo IaaS são (SUN; HU, 2012): as fronteiras de rede quebradas, tráfego de dados invisíveis à rede e o gerenciamento da segurança no tráfego de dados na rede.

4.1.1.1. Fronteiras de rede quebradas

A segurança de rede tradicional se baseia em domínios de segurança obtidos a partir das fronteiras da rede. Essas fronteiras estão geralmente baseadas nas fronteiras físicas dos servidores. Porém, na computação em nuvem, é comum que vários sistemas compartilhem a mesma fronteira física. De fato, VMs hospedadas num mesmo servidor podem pertencer a diferentes domínios lógicos de segurança, enquanto VMs hospedadas em hosts distintos podem estar no mesmo domínio lógico de segurança.

A Figura 3 mostra um exemplo dos domínios de segurança antes e depois da virtualização. Antes da virtualização, cada porta de switch se conectava a uma interface de rede de um servidor. Assim, aquela interface de rede representava uma fronteira física que garantia que, através daquela porta do switch, só trafegariam dados sujeitos a uma única regra de segurança. Após a virtualização, cada porta do switch continua se conectando a uma interface de rede de um servidor, mas a fronteira física que a interface representa não é mais garantia de que todos os dados daquela porta de switch estão sujeitos às mesmas regras. Isto ocorre porque através daquela interface de rede estarão uma ou mais máquinas virtuais, cada qual podendo estar sujeita a regras específicas de segurança.

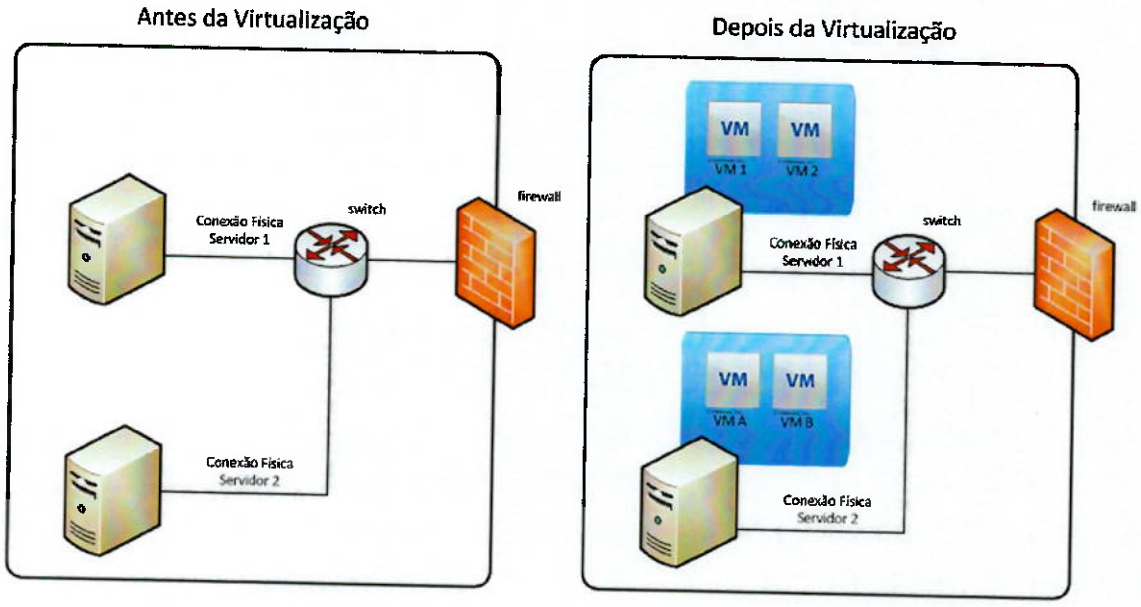

Figura 3 – Domínios de segurança antes e depois da virtualização. Adaptado de Sun e Hu (2012)

A solução para estes casos é adotar estratégias que levem em consideração as alterações introduzidas pela computação em nuvem. Uma destas estratégias é reconstruir o domínio de segurança, isolando as máquinas virtuais lógica ou fisicamente.

Para atingir o isolamento lógico, as máquinas virtuais devem ser classificadas de acordo com suas características de negócio, níveis de segurança de negócio e atributos de rede (SUN; HU, 2012). Segmentação de IP e VLAN também pode ser utilizada no isolamento lógico.

Para atingir o isolamento físico, as máquinas virtuais devem utilizar elementos de hardware dedicados, tais como servidores de armazenamento (*storage*), CPUs e VLANs.

4.1.1.2. Tráfego invisível de dados

Nos ambientes tradicionais, todo tráfego de rede é transportado ao switch físico no qual as máquinas físicas estão conectadas. Portanto, o switch é capaz de aplicar as políticas de segurança de rede, monitorar e gerenciar a rede. Entretanto, num ambiente virtualizado, duas VMs comunicando-se entre si podem estar hospedadas

num mesmo servidor. Assim, sua comunicação pode não ser encaminhada para o switch adjacente e as políticas de segurança desse equipamento não são aplicadas, caracterizando um tráfego invisível à rede em si (SUN; HU, 2012). Esta situação de tráfego invisível também tem o inconveniente adicional de deixar obscuras as responsabilidades dos administradores de rede e administradores de servidores.

A Figura 4 ilustra dois cenários onde a máquina virtual A precisa se comunicar com a máquina virtual C. No primeiro cenário, A está num servidor físico diferente de C, o que obriga o tráfego de dados a passar tanto pela interface de rede quanto pelo switch adjacente para chegar ao seu destino. No segundo cenário, tanto A quanto C estão no mesmo servidor físico, o que permite que o tráfego de dados chegue diretamente ao destino sem passar pelo switch adjacente, caracterizando desta forma a ocorrência de tráfego invisível de dados.

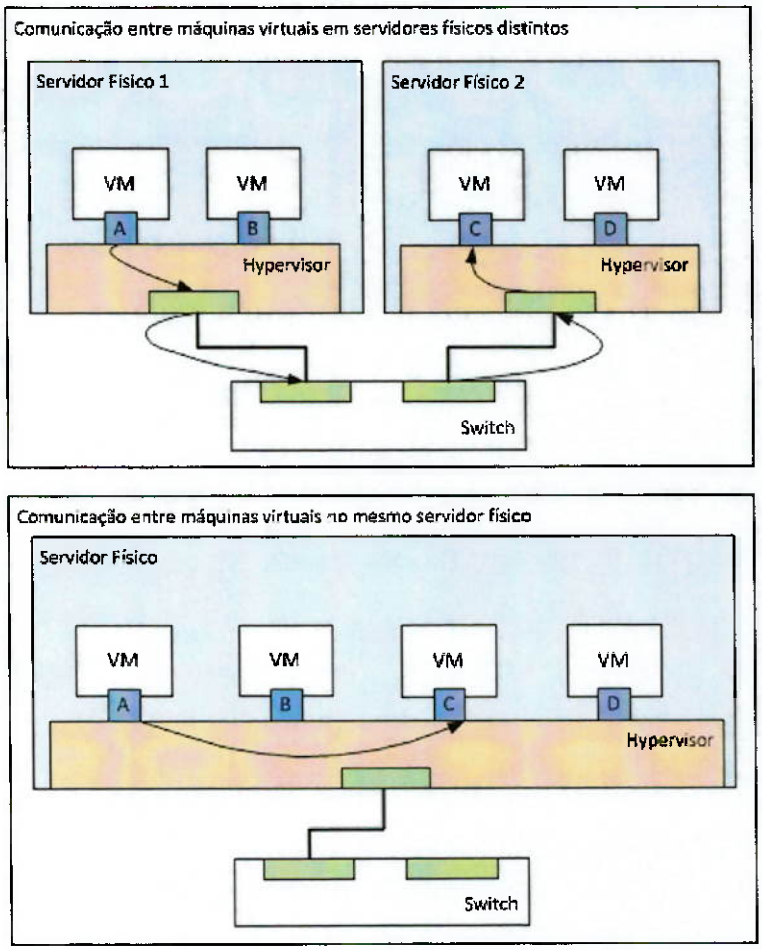

Figura 4 – Comunicação entre máquinas virtuais
Adaptado de Sun e Hu (2012)

A solução para estes casos é proteger o tráfego entre as máquinas virtuais (SUN; HU, 2012). Esta proteção pode ser obtida, por exemplo, no próprio ambiente de virtualização, através de uma terceira máquina virtual que analisaria todo tráfego entre as VMs do mesmo servidor físico. Outra alternativa para obter efeito semelhante é através de técnicas que forcem o tráfego entre as VMs do mesmo host a utilizar o switch adjacente.

A opção de forçar o tráfego pelo switch adjacente é muitas vezes preferível à utilização de uma terceira máquina virtual, pois esta abordagem apresenta duas grandes vantagens: não consome recursos de virtualização e retorna a responsabilidade de segurança ao administrador de redes.

4.1.1.3. Gerenciamento da segurança no tráfego de rede

O gerenciamento da segurança no tráfego de rede envolve a aplicação e migração de regras de segurança tais como ID da VLAN e QoS. Além das dificuldades em aplicar essas regras com relação ao tráfego de dados invisíveis na rede explicado na seção 4.1.1.2, a computação em nuvem também adiciona a dificuldade da migração síncrona das configurações de segurança conforme as VMs são movidas entre servidores físicos.

Uma possível solução para este problema é o modelo *Virtual Network Management Model* (VNMM), desenvolvido pela *Distributed Management Task Force* (DMTF), e baseado em padrões definidos pelo IEEE (THALER et al., 2011). O interesse desse modelo é que ele define claramente os papéis que cada componente deve executar na inicialização ou na migração das máquinas virtuais. Desta forma, os componentes individuais da virtualização são responsáveis pelos ajustes necessários para manter as regras da rede quando as migrações ocorrem.

4.1.2. Modelos PaaS e SaaS

O modelo PaaS é o modelo de computação em nuvem onde os usuários recebem o acesso a uma plataforma que pode ser por eles personalizadas, enquanto o modelo SaaS é o modelo onde os usuários recebem o acesso a uma aplicação que pode ser acessada por um ou mais aplicativo cliente. Em ambos os modelos, a maior responsabilidade sobre a segurança de rede costuma ser do fornecedor da nuvem (SABAHI, 2011). Isto ocorre porque as particularidades desses dois modelos de entrega de computação em nuvem não permitem que os usuários tenham acesso direto às configurações físicas de rede: no modelo SaaS, não há qualquer acesso a configurações de rede, enquanto no modelo PaaS existe acesso apenas a configurações lógicas. Portanto, os usuários de nuvens no modelo SaaS não exercem responsabilidades diretas sobre aspectos técnicos de segurança de rede, enquanto as suas responsabilidades em nuvens PaaS são restritas. Entretanto, ambos os modelos compartilham a responsabilidade sobre o controle de acesso à nuvem através de usuários e senhas.

Enquanto as tecnologias de acesso à nuvem podem variar entre clientes gordos (*thick clients*) e clientes magros (*thin clients*) no modelo IaaS, os modelos PaaS e SaaS utilizam quase que exclusivamente clientes magros através de serviços web (*web services*) (JENSEN et al., 2009). Portanto, o acesso à nuvem nos modelos PaaS e SaaS se dá quase que exclusivamente através de navegadores web. A utilização de navegadores web e serviços web implica que uma série de vulnerabilidades inerentes a essas tecnologias pode afetar a segurança de rede da computação em nuvem nos modelos PaaS e SaaS mais intensamente do que no modelo IaaS.

4.1.2.1. Serviços web

A tecnologia de serviços web é baseada em XML (*eXtensible Markup Language*) e na troca de mensagens conforme protocolo SOAP (sigla inglesa para Protocolo Simples de Acesso a Objetos). A especificação de segurança mais importante e amplamente utilizada para os serviços web é o WS-Security (brevemente discutida

na Seção 3.6). Uma forma de ataque conhecida ao WS-Security é o *XML Signature Element Wrapping* (que será referido no restante deste documento como ***ataque de envelopamento***), que consiste no envelopamento de uma requisição verdadeira, proveniente de uma fonte confiável, após sua captura por algum elemento espião (JENSEN et al., 2009). O elemento espião substitui a requisição verdadeira por uma requisição maliciosa e aproveita as informações de autenticação do usuário autêntico para ignorar a segurança do sistema. A Figura 5 ilustra um exemplo no qual a mensagem original de uma fonte confiável que solicitava o arquivo 'me.jpg' foi envelopada por um atacante para obter o arquivo 'cv.doc'.

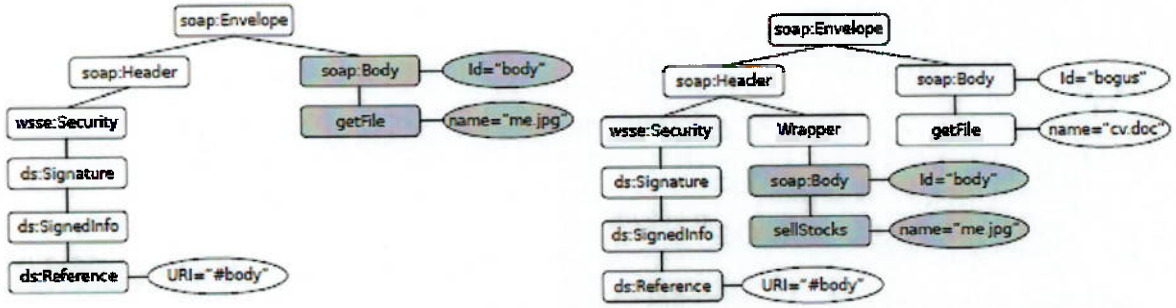

Figura 5 – Exemplo de Ataque de Envelopamento
Fonte: Jensen et al. (2009)

Os ataques por envelopamento foram descobertos por McIntosh e Austel em 2005 e desde então várias variações do ataque original foram propostas, bem como medidas de segurança para preveni-las. Entretanto, como o uso de WS-Security em aplicações de negócios eram raros, esses ataques eram tidos como teóricos e não práticos até que, em 2008, descobriu-se que os serviços de nuvem da Amazon eram vulneráveis a esse tipo de ataque (JENSEN et al., 2009).

4.1.2.2. Navegadores web

O cliente magro dos modelos PaaS e SaaS não realiza processamento local, pois toda a carga de computacional é realizada em sistemas remotos. Portanto, não há necessidade de desenvolvimento de um sistema proprietário para executar apenas

as finalidades de autenticação e envio de comandos quando uma ferramenta multiplataforma já se encontra disponível: os navegadores web (JENSEN et al., 2009).

Embora a utilização de navegadores web facilite a disseminação e utilização de soluções PaaS e SaaS, a segurança do sistema pode ficar comprometida devido a vulnerabilidades de tais ferramentas. De fato, os dados recebidos por um navegador web não são protegidos de forma que sejam acessíveis apenas pela origem da requisição: linguagens de script (como Javascript) podem acessar informações de outras origens uma vez que tenham conhecimento da existência dessas informações (JENSEN et al., 2009), por exemplo, através de vulnerabilidades do serviço de DNS (*Domain Name Service*). Isto pode dar origem a violações de uma política de segurança chamada Política da Mesma Origem (SOP – *Same Origin Policy*). Além disso, a própria autenticação através de navegadores web também não é segura, pois o *token* de autenticação é protegido pela mesma política SOP. Mesmo a utilização direta de web services com WS-Security não ajuda a resolver esse problema devido à incapacidade dos navegadores em processar diretamente a criptografia de dados XML através de WS-Security. Apesar dessas deficiências, existem alternativas com o uso de TLS e chaves públicas que aumentam a segurança dos navegadores, o que é feito através da autenticação segura e, assim, métodos que permitem a proteção do *token* de autenticação (JENSEN et al., 2009).

4.2. Segurança de Dados

A segurança de dados é definida em termos de confidencialidade, disponibilidade e integridade (GONZALEZ et al., 2011) (CHEN; ZHAO, 2012), termos estes que se aplicam a diversos cenários, incluindo computação em nuvem.

O serviço de confidencialidade de dados visa garantir que as informações sejam acessíveis ou inteligíveis apenas para os detentores de fato daqueles dados. Enquanto dados sigilosos podem permanecer a todo o momento dentro dos limites de um ambiente controlado (e.g., uma intranet) no modelo IaaS, o mesmo cenário é impraticável nos modelos PaaS e SaaS. Isto ocorre porque nesses últimos modelos

todos os dados estão armazenados remotamente e necessitam transitar pela Internet. Portanto, a confidencialidade de dados é de extrema importância na computação em nuvem e a criptografia é a tecnologia mais aplicada para garantir a confidencialidade de dados importantes (GONZALEZ et al., 2011).

Já a disponibilidade dos dados é um elemento importante principalmente pelo fato de que a maioria dos negócios atualmente se baseia na tecnologia da informação e processamento de dados para a execução de seus processos e funcionalidades (GONZALEZ et al., 2011). A principal técnica utilizada para garantir disponibilidade de dados é através da redundância (GONZALEZ et al., 2011). Os ataques externos são a principal ameaça à disponibilidade de dados na computação tradicional, mas na computação em nuvem há preocupações além dos ataques externos, como a disponibilidade dos serviços de nuvem, a política de armazenamento dos dados, a continuidade da operação do serviço de nuvem, etc. (CHEN; ZHAO, 2012).

Finalmente, a integridade de dados na computação em nuvem necessita de uma abordagem diferente da computação tradicional: na computação em nuvem, não é prático realizar o download de todos os dados, verificar a integridade das informações, realizar as operações e alterações desejadas e então fazer o upload dos dados; a verificação dos dados precisa ser realizada dinamicamente e de forma paralela à confidencialidade, mantendo-se os dados sendo processados na própria nuvem na medida do possível (CHEN; ZHAO, 2012).

A relevância dos aspectos de integridade e confidencialidade dos dados implica na importância do uso de criptografia. O uso de criptografia eficiente depende da escolha de bons algoritmos e da geração de chaves altamente aleatórias, o que, consequentemente levam a outro problema: o gerenciamento de chaves criptográficas (CHEN; ZHAO, 2012). O gerenciamento de chaves supostamente deveria ser realizado pelos donos das informações, mas a atual falta de experiência dos usuários implica no gerenciamento de chaves ser realizado pelo próprio fornecedor da nuvem. Uma preocupação neste contexto, entretanto, é que este cenário onde um serviço tão importante como a criptografia dos dados é administrada pelo fornecedor da nuvem foi profundamente abalado em 2013 com a

divulgação de casos de espionagem pela Agência Nacional de Segurança dos Estados Unidos, conforme discutido a seguir.

4.2.1. Espionagem da Agência Nacional de Segurança

O caso de espionagem de dados promovido pelo governo dos Estados Unidos através da NSA (National Security Agency) divulgados pelos jornais The New York Times (PERLROTH; LARSON; SHANE, 2013) e The Guardian (GREENWALD; BORGER; BALL, 2013) em setembro de 2013 gerou uma onda de desconfiança sobre a segurança dos sistemas de comunicação. O efeito de tais revelações foi especialmente impactante no que se refere à computação em nuvem porque a data de divulgação foi uma época onde a computação em nuvem estava se tornando cada vez mais comum em projetos diversos no mundo todo. Em especial, este é o caso dos projetos de comunicações unificadas da empresa que realiza a implantação do projeto que é foco do estudo de caso discutido mais adiante no capítulo 5. Especificamente, enquanto a implantação de projetos em clientes utilizando uma nuvem privada já era uma realidade na empresa responsável por tal projeto e crescia o número de clientes interessados em conhecer com maiores detalhes a utilização de nuvens públicas ou híbridas em projetos de comunicações unificadas, de repente a utilização de nuvens passou a ser considerada alternativa perigosa. Enquanto a maior parte das percepções de perigo dos clientes é baseada no título da notícia em si ("espionagem promovida pela NSA") e não nos detalhes da espionagem, alguns clientes fundamentam suas conclusões em fragmentos de informações (e.g., "protocolo TLS comprometido") que apontavam que qualquer tráfego de informações na nuvem estaria comprometido. Seja por razões reais ou apenas impressões errôneas, o fato é que diversos usuários passaram a observar a tecnologia da nuvem com desconfiança.

A NSA vem realizando ações que violam a privacidade com um orçamento dedicado de 250 milhões de dólares por ano (PERLROTH; LARSON; SHANE, 2013). Dentre as ações realizadas, aquelas mais graves no que diz respeito à violação de privacidade são (GREEN, 2013):

- Trabalhar em conjunto com entidades dos Estados Unidos responsáveis por protocolos (o NIST é especificamente mencionado) para promover padronização de criptografia fraca ou vulnerável;
- Influenciar entidades de padronização para enfraquecer protocolos;
- Trabalhar com fabricantes de hardware e software para enfraquecer algoritmos de criptografia e geradores de números aleatórios;
- Atacar a criptografia utilizada pela 'próxima geração' de telefones 4G;
- Obter acesso ao texto às claras de 'um grande sistema de comunicação ponto-a-ponto da Internet', supostamente o Skype;
- Identificar e quebrar chaves vulneráveis;
- Estabelecer uma divisão de inteligência para se infiltrar na indústria de telecomunicações.
- Decifrar as conexões seguras que utilizam o protocolo SSL, ação esta que seria a ação de espionagem mais grave da NSA.

Sem enumerar de acordo com a relevância, as três formas de quebrar um sistema de criptografia são (GREEN, 2013):

1) Atacar a criptografia – é difícil e improvável de funcionar com os algoritmos que são utilizados atualmente. Entretanto, existem protocolos com falhas conhecidas, como o RC4 (GREEN, 2013), e existem diversos algoritmos complexos que possuem vulnerabilidades;
2) Influenciar a implementação – a criptografia normalmente é implementada em software, mas também pode ser implementada em hardware. Para obter grande escala na espionagem, seria necessário trabalhar com os grandes fornecedores de software e hardware para inserir neles vulnerabilidades desde o início (as chamadas *backdoors*[1]);
3) Engenharia social – não há necessidade de invasão se é possível fazer o usuário legítimo fornecer a chave de acesso.

[1] **Falha de segurança que permite a invasão de um sistema computacional possibilitando que o invasor assuma o controle e/ou tenha acesso às informações do sistema.**

Assumindo que os documentos são verdadeiros, a quebra de segurança seria através da implementação (2) e do fator humano (3), ou seja, através de "trapaça" e não de matemática (SCHNEIER, 2013).

Mais precisamente, para quebrar a segurança através da implementação, a NSA precisaria trabalhar em conjunto com os fornecedores de criptografia que detêm grandes fatias de mercado, tanto de hardware quanto de software. Segundo Green, os maiores fornecedores de criptografia SSL em software são a Microsoft e os membros do projeto OpenSSL, a principal biblioteca de código aberto para SSL. Também segundo Green, o maior fornecedor no mercado de hardware seria a Intel.

Quebrar a segurança através do fator humano abrange a quebra através da implementação (pois precisa da colaboração dos fornecedores de hardware e software para tanto), mas não está restrito apenas a estes tipos de fornecedores. De fato, os documentos revelam que a NSA trabalha em duas frentes: enfraquecendo ou adicionando vulnerabilidades na definição dos padrões de criptografia e com a colaboração de grandes fornecedores de telecomunicações que não são citados. Enquanto protocolos vulneráveis facilitariam o trabalho de espionagem, a colaboração de fornecedores de serviços de telecomunicações facilita muito mais a espionagem.

5. ESTUDO DE CASO

Para uma discussão mais concreta dos conceitos apresentados no Capítulo 4, neste capítulo os mesmos são debatidos no contexto do projeto de comunicações unificadas na nuvem que se encontra em processo de implantação numa universidade de grande porte. Tal projeto já se encontra em um estado avançado e diversos dos aspectos discutidos neste documento se aplicam a tal cenário, o que justifica o interesse nesse projeto como alvo da presente análise. Entretanto, é importante mencionar que o projeto de comunicações unificadas não estava finalizado, podendo ter sofrido alterações durante a execução deste trabalho. Portanto, é importante ter em mente que algumas das considerações aqui apresentadas podem não se aplicar inteira ou parcialmente caso o projeto final seja diferente do aqui apresentado.

O projeto de comunicações unificadas na nuvem desta universidade de grande porte apresenta elementos que contribuem para sua complexidade, o que torna a análise do projeto ainda mais interessante. Dentre esses elementos, destacam-se:

- Nuvem local, hospedada no campus principal da universidade e administrado por equipe da própria universidade;
- Nuvem remota, hospedada e administrada por um fornecedor terceiro;
- Tráfego de voz protocolos como SIP (Session Initiation Protocol) e VoIP (Voice over Internet Protocol), os quais requerem a alta disponibilidade fornecida pela computação em nuvem e proteção adicional através do uso da convencional rede pública de telefonia comutada (PSTN) numa eventual pane na rede de dados;
- Salas de conferência web usando protocolo HTTP, que podem utilizar tráfego de voz tanto dentro da própria conferência quanto através de telefones comuns;
- Comunicações unificadas com serviço por número único, funcionalidade pela qual o usuário precisa divulgar um único número de telefone e todos os contatos telefônicos que receber poderão ser atendidos em qualquer de seus dispositivos (telefone residencial, escritório, escritório remoto, celular, etc.);
- Central de atendimento a usuários com suporte a voz ou bate-papo web

- Correio eletrônico de voz

Os serviços utilizados pelo projeto e suas respectivas interligações demandam a utilização dos conceitos de segurança previamente discutidos a fim de permitir sua elevada disponibilidade, tanto numa eventual falha de componentes individuais quanto no caso de ataques virtuais através da Internet.

5.1. O Projeto de Comunicações Unificadas na Nuvem

Um sistema de comunicação unificada pode ser entendido como uma estrutura em que há a convergência entre sistemas de telecomunicações e de tecnologia da informação, permitindo a integração entre mídias (voz, texto, vídeo) e dispositivos (telefones, celular, computadores) com informações de presença e funcionalidades de colaboração (RIEMER; TAING, 2009).

O projeto de comunicações unificadas na nuvem da universidade de grande porte envolve diversos serviços com funções específicas que, trabalhando em conjunto, atendem aos objetivos do projeto. Especificamente, os serviços ou componentes principais do projeto são:

- Central telefônica software (*softswitch*)
- Servidores de mídia (*media servers*)
- Serviços de comunicações unificadas (*Unified Communications* - UC)

O software de central telefônica provê serviços de comunicação de voz através dos protocolos VoIP e SIP, sendo também responsável pelo roteamento dos contatos de voz. É o softswitch que localiza o dispositivo que se deseja contatar em sua tabela de roteamento e apresenta seu endereço ao dispositivo de origem. De posse dessa informação, o dispositivo de origem utiliza o protocolo SIP para negociar os detalhes da sessão de comunicação, para então iniciar a comunicação através de VoIP.

O servidor de mídia possui duas atribuições principais que, apesar de semelhantes, apresentam requisitos computacionais distintos: disponibilizar mídias para o sistema de voz (com alto número de requisições de baixa demanda computacional) e

disponibilizar mídias para sistemas multimídia (baixo número de requisições, mas cada uma delas com alta demanda computacional). No contexto do sistema de voz, tal servidor permite que elementos de áudio comuns de um sistema de telefonia convencional sejam apresentados aos dispositivos clientes. Exemplos de elementos de áudio de sistema são: tom de ocupado, tom de telefone de destino sendo chamado, música de espera etc. Nos sistemas multimídia, o servidor disponibiliza vídeo e áudio das sessões de colaboração web, i.e., sessões interativas transmitidas a múltiplos clientes, permitindo, por exemplo, que apresentações e aulas sejam realizadas em tempo real e remotamente.

Os serviços de comunicações unificadas proveem as funcionalidades de estado de presença, sessões de colaboração web, interoperabilidade transparente entre dispositivos de comunicação, etc. A funcionalidade de "estado de presença" permite aos usuários configurar em tempo real se estão disponíveis ou indisponíveis para o recebimento de uma chamada enquanto outra já estiver em curso (e.g., permite evitar o recebimento de uma requisição de chat enquanto um contato telefônico está em curso). É desta forma que o controle de estado de presença, em conjunto com a interoperabilidade de dispositivos, permite aos usuários controlar as formas disponíveis para estabelecimento de comunicação, que podem ser e-mail, voz, colaboração web, etc. Ela permite também a migração de uma comunicação em curso entre dispositivos semelhantes sem a interrupção da sessão (e.g., transferir um contato telefônico em curso no telefone de trabalho para um telefone celular de forma transparente e ininterrupta).

Além dos componentes principais, o projeto também conta com outros componentes que desempenham funcionalidades específicas:

- Correio de voz (voice mail)
- Central de atendimento (contact center)
- Unidades de resposta audível (URA)

5.1.1. Particularidades e Detalhes Técnicos do Projeto

Entre os principais usuários finais do projeto estão alunos e professores que desejam assistir ou ministrar cursos remotos com a possibilidade de colaboração ativa entre os participantes. As características destes usuários e a previsão de demanda de uso realizada para o projeto implicam na necessidade de alta disponibilidade a fim de prover um nível adequado de experiência para os usuários.

Esta necessidade de alta disponibilidade do projeto levou à decisão de distribuir os componentes do sistema em dois ou mais datacenters geograficamente separados. Esta abordagem minimiza danos na eventualidade de catástrofes que afetem a região geográfica onde um datacenter esteja instalado, como uma queda de energia ou de rede. Porém, para obter tais benefícios é necessário arcar com custos relativos a tráfego de dados entre os datacenters, componentes para realizar o balanceamento de carga, etc. Cabe notar que, no contexto das comunicações unificadas na nuvem da universidade de grande porte, esses datacenters serão utilizados simultaneamente, de modo que não se aplicam conceitos de datacenters principal e de backup.

As localizações geográficas dos datacenters não serão levadas em consideração para os fins deste estudo. Desta forma, as referências aos datacenters serão feitas através dos termos 'Datacenter 1' e 'Datacenter 2'. Todos os componentes do projeto de comunicação unificada mencionados no capítulo 5.1 (O Projeto de Comunicações Unificadas) se encontram duplicados e distribuídos em ambos os datacenters. Entretanto, alguns desses elementos possuem mais de uma instância presente em um único datacenter, sendo que as cópias adicionais devem fornecer balanceamento de carga ou executar funções dedicadas.

A Figura 6 apresenta os componentes do projeto de comunicações unificadas na nuvem de cada datacenter, agrupados de acordo com suas finalidades. O projeto prevê que as máquinas virtuais destinadas ao mesmo objetivo ou aplicação devem ser alocadas na nuvem dentro de um mesmo grupo.

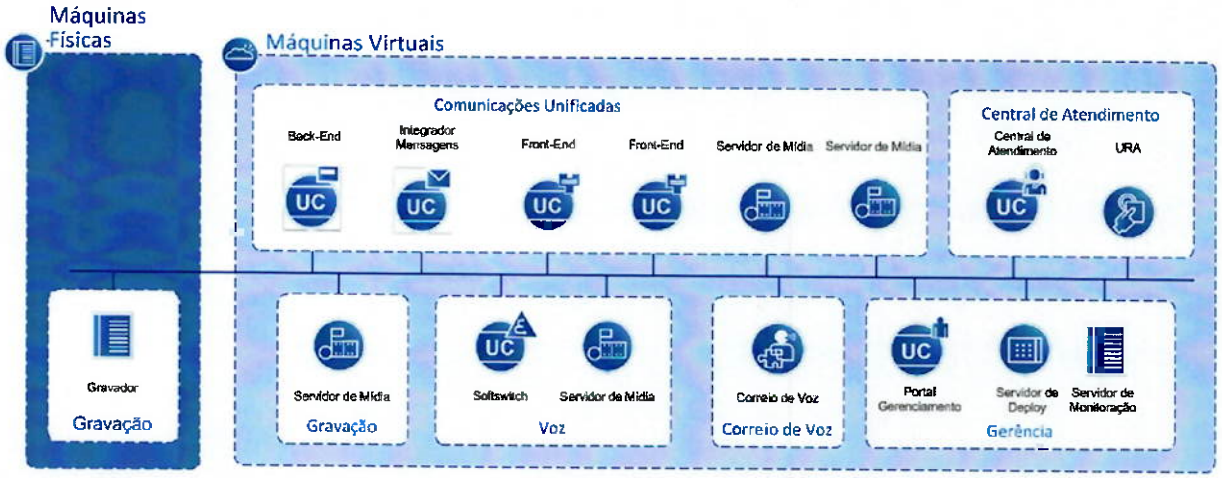

Figura 6 – Componentes de uma localidade

A Figura 6 também evidencia os elementos que possuem mais de uma instância dentro do mesmo datacenter:

- Front-end de comunicações unificadas – são os componentes que irão receber e gerenciar as conexões dos usuários e suas respectivas requisições. Cada instância permite uma capacidade maior de usuários simultâneos e fornece uma melhor experiência de uso.
- Servidores de Mídia – são os componentes por onde trafegam os dados multimídia (áudio e vídeo). Cada instância permite isolar o tráfego de determinada aplicação (e.g., apenas áudio das gravações da central de atendimento, áudio e vídeo das videoconferências, etc.).

Uma premissa de projeto estabeleceu que uma das localidades fosse administrada pela equipe de infraestrutura do campus da universidade enquanto a outra fosse administrada por um fornecedor terceiro.

5.1.2. Identificando os Modelos de Serviço

A identificação de elementos segundo os modelos de serviço IaaS, PaaS e SaaS no projeto de comunicações unificadas permitem uma aplicação mais rápida e direta dos itens discutidos no capítulo 4. Com a exceção da máquina Gravador da solução de Gravação por questões técnicas, todos os demais elementos do projeto são máquinas virtuais. As máquinas virtuais são elementos típicos do modelo IaaS, mas

apenas o seu uso não implica diretamente que o modelo de serviço adotado será o IaaS. A forma como as máquinas virtuais são hospedadas e disponibilizadas para uso são determinantes para identificar o modelo de serviço a que estão sujeitas no projeto de comunicações unificadas de grande porte.

O projeto de comunicações unificadas na nuvem da universidade de grande porte alvo do presente estudo utiliza duas abordagens distintas para questão de hospedagem e disponibilização das máquinas virtuais segundo a localidade: o datacenter do campus e o datacenter remoto. A abordagem utilizada no datacenter do campus da universidade foi a aquisição de uma solução de virtualização por esta instituição, sendo que desta forma é a equipe de tecnologia de informação da universidade deve se preocupar com todas as questões de segurança das máquinas virtuais, caracterizando o modelo IaaS. Já a abordagem utilizada no datacenter remoto foi através da contratação de um terceiro, sendo que desta forma o terceiro solicita a quantidade de recursos computacionais necessários para o projeto e é responsável pela disponibilização e administração destes recursos, caracterizando o modelo PaaS.

A operação dos ambientes distintos também implica na identificação de elementos em outros modelos. Enquanto a operação do ambiente no datacenter do campus da universidade utiliza as ferramentas de acesso do fornecedor do ambiente virtual, caracterizando elementos do modelo IaaS (ferramentas gordas e magras de acesso), a operação do ambiente remoto utiliza ferramentas desenvolvidas pelo próprio terceiro, caracterizando elementos SaaS.

A Tabela 1 apresenta um resumo dos modelos de serviço identificados.

Elemento do Projeto	**Responsável**	**Modelo de Serviço**
Máquinas virtuais	Equipe de TI da universidade	IaaS
Máquinas virtuais	Fornecedor terceiro	PaaS
Ferramenta de acesso	Equipe de TI da universidade	IaaS
Ferramenta de acesso	Fornecedor terceiro	SaaS

Tabela 1 – Resumo dos modelos de serviço identificados

5.2. Segurança em Comunicações Unificadas na Nuvem

O fato de o projeto utilizar dois datacenters geograficamente separados exige atenção para a necessidade de comunicação entre os componentes que executam funcionalidades semelhantes e que estão alocados em diferentes localidades. Enquanto algumas tecnologias permitem que cada elemento trabalhe de forma totalmente isolada, outras exigem alguma forma de inteligência centralizada que seja acessível acessada por outros elementos. Essa centralização é obtida através da clusterização de serviços, o que implica em comunicação e sincronização de altas quantidades de dados entre as diferentes localidades. Assim, faz-se necessário permitir na camada de computação em nuvem transferências de dados de baixa plataforma em altos volumes e com baixo tempo de espera a fim de garantir ambas as formas de redundância nas aplicações. Entretanto, essa necessidade é obtida diretamente na infraestrutura de rede e não na camada de computação em nuvem. Esta necessidade na infraestrutura de rede não viola as questões de segurança do modelo IaaS de Fronteiras de rede quebradas (seção 4.1.1.1), o Tráfego invisível de dados (seção 4.1.1.2) e Gerenciamento da segurança no tráfego de rede (seção 4.1.1.3), pois se trata do tráfego de dados que já são tipicamente tratados em ambientes que não utilizam a computação em nuvem.

Embora as questões de segurança de computação em nuvem no modelo IaaS não sejam diretamente afetadas em ambientes de múltiplos datacenters, o mesmo não ocorre dentro de cada datacenter: é exatamente neste cenário que as regras pertinentes ao modelo IaaS devem ser observadas. Especificamente, a premissa de projeto de que os elementos que executam funcionalidades de uma determinada aplicação sejam agrupados na nuvem (necessidade exposta na seção 5.1.1) levam à necessidade de atenção aos aspectos de segurança discutidos sobre o modelo IaaS (seção 4.1.1). Tal preocupação surge porque é exatamente dentro de um ambiente localmente delimitado, que possui uma relação mais próxima das infraestruturas de servidores, rede, etc., que o modelo IaaS possui maior aplicabilidade. Primeiramente, as questões das Fronteiras de rede quebradas (seção 4.1.1.1) e do Tráfego invisível de dados (seção 4.1.1.2) são diretamente influenciadas pela decisão de hospedar máquinas virtuais que irão trocar

informações entre si dentro de um mesmo elemento de processamento (e.g., um mesmo servidor físico padrão ou lâmina de processamento).

Uma segunda preocupação neste contexto refere-se ao Gerenciamento da segurança no tráfego de rede (seção 4.1.1.3), que também precisa ser observado devido à necessidade de alta disponibilidade do projeto. Portanto, como é de se esperar que servidores adicionais estejam disponíveis no ambiente para garantir continuidade na eventualidade de uma falha de hardware, as possíveis de rotas de rede alternativas precisam estar mapeadas e configuradas com as mesmas regras de segurança padrão da rota principal.

A Tabela 2 faz um resumo dos cuidados e comentários sobre segurança do modelo IaaS discutidos.

Questão de segurança	**Razão para o problema**	**Sugestão de melhoria de segurança**
Fronteiras de rede quebradas	Gerado ao agrupar VMs em um mesmo elemento de processamento físico.	Realizar o isolamento lógico proposto por Sun e Hu (2012) através de um projeto que leve em consideração a topologia do projeto. Cabe notar que o isolamento físico em si não é recomendado por exigir hardware dedicado e, assim, prejudicar a alta disponibilidade ou exigir alto investimento financeiro.
	Premissas do projeto podem gerar violação deste quesito.	Analisar o motivo da premissa e os impactos de uma possível alteração.
Tráfego invisível de dados	Gerado ao agrupar VMs em um mesmo elemento de processamento físico.	Forçar o tráfego das máquinas virtuais a utilizar o switch adjacente conforme proposto por Sun e Hu (2012). Esta opção permite que equipes de infraestrutura de rede possam colaborar efetivamente com o projeto através da correta configuração de roteadores.

Tabela 2 – Resumo das questões de segurança do modelo IaaS

Questão de segurança	Razão para o problema	Sugestão de melhoria de segurança
Tráfego invisível de dados	Premissas do projeto podem gerar violação deste quesito.	Analisar o motivo da premissa e os impactos de uma possível alteração.
Gerenciamento da segurança no tráfego de rede	Gerado ao movimentar VMs entre elementos de processamento físicos	Verificar se o modelo Virtual Network Management Model é adotado pelos fornecedores de hardware. Caso não seja adotado, analisar se upgrade de software permitiria o suporte a tal tecnologia.
	Premissas do projeto podem gerar violação deste quesito.	Analisar o motivo da premissa e os impactos de uma possível alteração.

Tabela 2 (cont.) – Resumo das questões de segurança do modelo IaaS

A interface de gerenciamento utilizada para acessar e administrar as máquinas virtuais em um dos datacenters é baseada em navegadores web, enquanto no outro se utiliza tanto um navegador web quanto um aplicativo gordo (*thick application*). Esta particularidade do ambiente implica na importância de se atentar à segurança dos serviços web (seção 4.1.2.1) utilizados, a fim de garantir que as normas e atualizações de segurança mais recentes de serviços web (WS-Security) sejam utilizadas. Quanto à segurança no uso dos navegadores web (seção 4.1.2.2), é importante garantir a utilização de protocolos de segurança como o TLS, com uma configuração adequada (e.g., evitando o uso de RC4 e outros algoritmos considerados vulneráveis) para garantir o mínimo de segurança (JENSEN et al., 2009). Uma forma interessante para se evitar o uso de RC4 é através da implementação do TLS 1.2 com suporte aos algoritmos de criptografia com cifração autenticada, tanto no lado cliente quanto servidor da conexão (PATERSON et al., 2013).

A Tabela 3 faz um resumo dos cuidados e comentários sobre segurança do modelo PaaS e SaaS discutidos.

Questão de segurança	Razão para o problema	Sugestões de melhoria de segurança
Serviços web	Utilização de aplicativo gordo como ferramenta de acesso	Utilização de segurança de serviços web (WS-Security) (JENSEN et al., 2009).
	Utilização de navegador web como ferramenta de acesso	Utilização de protocolos de segurança como TLS com configuração adequada (JENSEN et al., 2009). Utilização do TLS 1.2 sem RC4 (PATERSON et al., 2013)
Navegadores web	Utilização de navegador web como ferramenta de acesso	Utilização de protocolos de segurança como TLS com configuração adequada SSL (JENSEN et al., 2009). Utilização do TLS 1.2 sem RC4 (PATERSON et al., 2013)

Tabela 3 - Resumo das questões de segurança dos modelos PaaS e SaaS

No tocante à segurança de dados (seção 4.2), o aspecto de confidencialidade é parcialmente atendido a partir das recomendações da Tabela 3 através do uso do protocolo de segurança TLS. Como é premissa do projeto que um datacenter será administrado pela equipe de TI da universidade, é importante que as chaves criptográficas sejam geradas a partir de fontes de entropia adequadas. O datacenter administrado por terceiros necessita de acordos comerciais para que a mesma política seja adotada.

Já o aspecto de disponibilidade pode ser obtido através do uso de dispositivos de armazenamento de dados redundantes em conjunto com configurações de rede que permitam rotas múltiplas de acesso a esses dispositivos (GONZALEZ et al., 2011). Isso se aplica dentro do ambiente administrado pela equipe de TI da universidade e também ao outro datacenter. A comunicação entre os dois datacenters também deve possuir rotas múltiplas de acesso.

Finalmente, o aspecto de integridade pode ser obtido através do uso de técnicas de verificação de dados que devem ser disponibilizados pelos seus respectivos fornecedores. No ambiente administrado pelo pela equipe de TI da universidade, isto

implica na utilização de soluções dos fornecedores dos dispositivos de armazenamento que utilizem técnicas como sistema de arquivos autenticado, protocolos que permitam auditoria contínua dos arquivos e verificação em tempo real da integridade dos dados (STEFANOV et al., 2011). No ambiente do outro datacenter deve-se exigir que o fornecedor disponibilize ferramentas que forneçam a integridade equivalente ao modelo PaaS.

A Tabela 4 faz um resumo dos cuidados e comentários sobre segurança de dados discutidos.

Questão de segurança	**Sugestões de melhoria de segurança**
Confidencialidade	Uso de segurança na camada de transporte (TLS) (GONZALEZ et al., 2011) (CHEN; ZHAO, 2012)
	Escolha de chaves de criptografia adequadas (CHEN; ZHAO, 2012)
Disponibilidade	Uso de dispositivos de armazenamento redundantes (CHEN; ZHAO, 2012)
	Uso de múltiplas rotas de rede no acesso aos dispositivos (CHEN; ZHAO, 2012)
Integridade	Uso de soluções disponibilizadas por fornecedores (CHEN; ZHAO, 2012)

Tabela 4 – Resumo das questões de segurança de dados

Não há referências diretas aos fornecedores de computação em nuvem no caso de espionagem da NSA. Entretanto, fornecedores de hardware e software da computação em nuvem, tais como a Microsoft e a Intel, e serviços que são infraestrutura de nuvem pública, tais como provedoras de telecomunicações, são explicitamente citados em documentos que discutem a espionagem da agência. Além disto, se grandes empresas estabelecidas no mercado colaboram com a NSA, empresas relativamente novas e de menor tradição no mercado teoricamente poderiam ser envolvidas mais facilmente.

As maiores proteções contra a espionagem da NSA para o projeto de comunicações unificadas na nuvem da universidade de grande porte seriam evitar ou minimizar a utilização de objetos que possam ser diretamente influenciados pela NSA no escopo

da nuvem ou utilizar softwares de código aberto após devidamente auditados. Cada localidade do projeto pode estar dentro de um tipo de nuvem, mas não foram obtidas certezas sobre o tipo de nuvem de cada localidade. Portanto, independente do tipo de nuvem presente em cada localidade (privada, pública ou híbrida), a maior proteção seria a escolha de fornecedores apropriados (hardware, software, serviços e telecomunicações) sem origens nos Estados Unidos ou devidamente auditados.

6. CONSIDERAÇÕES FINAIS

A computação em nuvem é a tecnologia que nos últimos anos deixou de ser um negócio promissor para se tornar um dos componentes da indústria de Tecnologia da Informação que mais cresce (SABAHI, 2011). Entretanto, as preocupações relacionadas à segurança são as principais barreiras que impedem uma adoção mais ampla e rápida da tecnologia (SHAIKH; HAIDER, 2011).

O presente trabalho discutiu os aspectos de segurança relacionados à segurança de rede e à segurança de dados nos ambientes de computação em nuvem. Com base na discussão exposta, foram feitas sugestões para melhoria da segurança de um estudo de caso, a saber, o projeto de comunicações unificadas na nuvem de uma universidade de grande porte. É importante ressaltar que as sugestões de melhorias devem ser encaradas exatamente como possibilidades de melhoria e não necessariamente como as melhores opções possíveis. Isto ocorre porque as discussões sobre segurança nunca se esgotam por completo, mesmo quando a discussão se restringe a temas com o escopo reduzido. Novas tecnologias surgem a cada momento e também podem inserir novas vulnerabilidades. Além disto, novas possibilidades de ataque são descobertas com frequência, exigindo a revisão contínua da segurança de qualquer sistema.

Apesar dos aspectos segurança de rede e segurança de dados não serem os únicos possíveis no escopo da computação em nuvem, eles são importantes de acordo com a literatura especializada (GONZALEZ et al., 2011) (SABAHI, 2011) (SHAIKH; HAIDER, 2011). A aplicação das sugestões de melhorias contidas neste documento deverá aumentar sensitivamente a segurança do projeto de computação em nuvem do ambiente proposto no estudo de caso. Entretanto, estas mesmas sugestões de melhorias poderão ter um impacto reduzido caso outras medidas de segurança para finalidades semelhantes já estejam em vigor.

As sugestões de melhorias de segurança aqui propostas são independentes e não conflitantes entre si. Elas podem, portanto, ser aplicadas na ordem desejada, de acordo com critérios de prioridade ou viabilidade. Essas características permitem às sugestões de melhorias maior flexibilidade no momento de aplicá-las.

6.1. Trabalhos Futuros

As discussões de segurança sobre a computação em nuvem presentes neste trabalho podem se expandir em duas vertentes principais: aprofundamento nas discussões dos tópicos já citados ou discussão de novos tópicos. A primeira vertente pode proporcionar um grau de segurança mais elevada dentro do tópico discutido, sendo uma opção interessante caso o tópico seja considerado de especial importância dentro do projeto cuja segurança deseja se analisar. Já a discussão de novos tópicos tem interesse para cobrir aspectos importantes negligenciados no presente estudo, os quais, mais uma vez, podem ter grande importância em cenários diferentes do sistema de comunicações unificadas na nuvem aqui estudado.

A aplicação dos aspectos de segurança discutidos neste trabalho em outro cenário também é uma opção interessante para trabalhos futuros. Características distintas de outro estudo de caso podem proporcionar conclusões diferentes das aqui obtidas e, assim, contribuir para uma melhor discussão.

REFERÊNCIAS

ARMBRUST, M; FOX, A; GRIFFITH, R; JOSEPH, A D; KATZ, R; KONWINSKI, A; LEE, G; PATTERSON, D; RABKIN, A; STOICA, I; ZAHARIA, M. **A View of Cloud Computing**. Communications of the ACM, v. 53, n. 4, p. 50-58, 2010.

CARROLL, M.; VAN DER MERWE, A.; KOTZE, P.. **Secure cloud computing: Benefits, risks and controls**. 2011Information Security South Africa (ISSA), vol., no., pp.1,9, 15-17 Aug. 2011

CHEN, D; ZHAO, H.. **Data Security and Privacy Protection Issues in Cloud Computing**. 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE). vol.1, no., pp.647,651, 23-25 March 2012

GONZALEZ, N.; MIERS, C.; REDIGOLO, F.; CARVALHO, T.; SIMPLICIO, M.; DE SOUSA, G.T.; POURZANDI, M.. **A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing**. 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom)., vol., no., pp.231,238. Nov. 29 2011-Dec. 1 2011

GREEN, M. **On the NSA.** Disponível em <http://blog.cryptographyengineering.com/>. Acesso em 17 de janeiro de 2014

GREEN, M. **Attack of the week: RC4 is kind of broken in TLS.** Disponível em <http://blog.cryptographyengineering.com/>. Acesso em 24 de janeiro de 2014

GREENWALD, G; BORGER, J; BALL, J. **Revealed: how US and UK spy agencies defeat internet privacy and security**. Disponível em <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em 19 de janeiro de 2014

JENSEN, M.; SCHWENK, J.; GRUSCHKA, N.; IACONO, L.L.. **On Technical Security Issues in Cloud Computing**. CLOUD '09. 2009 IEEE International Conference on Cloud Computing,., vol., no., pp.109,116, 21-25 Sept. 2009

MELL, P.; GRANCE, T.. The NIST definition of cloud computing. National Institute of Standards and Technology, v. 53, n. 6, p. 50, 2009

PATERSON, K; BERNSTEIN, D; POETTERING, B; SCHULDT, J. **On the Security of RC4 in TLS and WPA**. Disponível em <http://www.isg.rhul.ac.uk/tls>. Acesso em 26 de janeiro de 2014

PERLROTH, N; LARSON, J; SHANE, S. **N.S.A. Able to Foil Basic Safeguards of Privacy on Web**. Disponível em <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>. Acesso em 20 de janeiro de 2014

SUN, Q; HU, Z.. **Security for Networks Virtual Access of Cloud Computing**. 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES), vol., no., pp.749,752, 2-4 Nov. 2012

RIEMER, K.; TAING, S.. **Unified communications**. Business & Information Systems Engineering, v. 1, n. 4, p. 326-330, 2009.

SABAHI, F.. **Cloud computing security threats and responses**. 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN). vol., no., pp.245,249, 27-29 May 2011

SCHNEIER, B.. **The NSA Is Breaking Most Encryption on the Internet**. Disponível em <https://www.schneier.com/blog>. Acesso em 17 de janeiro de 2014

SEO, C. E.. **Virtualização – Problemas e desafios**. IBM Linux Technology Center. 2009

SHAIKH, F.B.; HAIDER, S.. **Security threats in cloud computing**. 2011 International Conference for Internet Technology and Secured Transactions (ICITST). vol., no., pp.214,219, 11-14 Dec. 2011

STEFANOV, E.; VAN DIJK, M.; OPREA, A.; JUELS, A.. **Iris: A Scalable Cloud File System with Efficient Integrity Checks**. In: Proceedings of the 28th Annual Computer Security Applications Conference. ACM, 2012. p. 229-238.

THALER, P.; FINN, N.; FEDYK, D.; FARKAS, J.; PARSONS, G; GRAY, E.. IEEE 802.1 Q. 2013.

GLOSSÁRIO

Clientes Gordos – O mesmo que *thick clients*.

Clientes Magros – O mesmo que *thin clients*.

CSA – Cloud Security Alliance, organização criada a fim de definir e promover melhores práticas em computação em nuvem.

Datacenter – Centro de processamento de dados, nome dado aos locais onde são concentrados equipamentos de processamento e armazenamento de uma empresa

ENISA – European Network and Information Security Agency, entidade européia de estudos sobre ameaças tecnológicas.

GRC – Governança, Risco e Compliance

HTTP – Protocolo de transferência de hipertexto, do inglês ***HyperText Transfer Protocol***. É um protocolo de comunicação e base da comunicação de dados na World Wide Web.

IaaS – Infraestrutura como serviço, do inglês ***Infrastruture as a Service***. Um dos três modelos de computação em nuvem definido pelo NIST.

NIC – Adaptador de rede, do inglês ***Network Interface Card***. Dispositivo responsável pela comunicação de computadores numa rede.

NIST – ***National Instutite of Standards and Technology***, é o Instituto Nacional de Padrões e Tecnologia do Ministério do Comércio dos Estados Unidos da América.

QoS – Qualidade de serviço, do inglês ***Quality of Service***. Tecnologia de rede que permite priorizar determinados tráfego de dados a fim de quarantir sua qualidade.

PaaS – Plataforma como serviço, do inglês ***Plataform as a Service***. Um dos três modelos de computação em nuvem definido pelo NIST.

PSTN – Rede pública de telefonia comutada, do inglês Public Switched Telephone Network. É a rede mundial de telefonia comutado por circuitos.

SaaS – Software como serviço, do inglês ***Software as a Service***. Um dos três modelos de computação em nuvem definido pelo NIST.

SIP – Protocolo para início de sessão, do inglês ***Session Initiation Protocol***.

SSL – Protocolo de camada de sockets segura, do inglês ***Secure Sockets Layer***. Protocolo de criptografia utilizado para segurança na Internet. Predecessor do TLS.

SOAP – Protocolo utilizado para troca de informações, do inglês ***Simple Object Access Protocol***.

Thick clients – Clientes gordos, onde a carga de processamento fica no lado cliente da conexão.

Thin clients – Clientes magros, onde a carga de processamento fica no lado servidor da conexão.

TI – Tecnologia da Informação. Sigla normalmente utilizada para designar equipes responsáveis pela administração dos elementos computacionais de uma empresa.

TLS – Segurança da Camada de Transporte, do inglês *Transport Layer Security*. Protocolo de criptografia utilizado para segurança na Internet. Sucessor do SSL.

UC – Comunicações Unificadas, do inglês **U**nified **C**ommunications.

URA – Unidade de Resposta Audível, componente que realiza o atendimento eletrônico de contatos telefônicos.

VLAN – Virtual Local Area Network, tecnologia de rede virtual que permite que diferentes redes lógicas compartilhem o mesmo meio físico.

VM – Máquina virtual, do inglês *Virtual Machine*.

VoIP – Voz sobre protocolo de Internet, do inglês *Voice over Internet Protocol*.

vNIC – Adaptdor de rede virtual, do inglês *Virtual Network Interface Card*.
Equivalente virtual de uma NIC.