SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

AULA 5

Prof. Douglas Eduardo Basso

CONVERSA INICIAL

Nessa aula, vamos falar sobre conceitos relacionados ao uso dos dispositivos pessoais nos meios corporativos, o chamado BYOD, como as empresas precisam se precaver para manter a segurança com os colaboradores usando seus equipamentos pessoais dentro da organização. Outro assunto comentado são as *sandboxes*, que são plataformas utilizadas para vários tipos de testes sem afetar o ambiente de produção das organizações. Por meio dessa plataforma, é possível validar sistemas, aplicações, simular cenários de uso, entre outros.

Vamos abordar também algumas tendências corporativas, a mobilidade como variável dinâmica na mudança de processos, as tecnologias que vêm emergindo e, na sequência, o tema proposto será a segmentação da rede, as redes desmilitarizadas, como é possível melhorar a segurança criando redes separadas, isolando equipamentos e criando mecanismos de separação de redes com as VLANs, as redes locais virtuais.

Vamos falar sobre a computação em nuvem, quais são os tipos de nuvens, como o advento da computação em nuvem tem afetado as questões de segurança, as camadas de acesso à nuvem, a camada em neblina, as características de cada camada, as ameaças e riscos dentro da nuvem, recomendações e boas práticas de segurança nesses cenários. Nos temas finais, vamos falar sobre a segurança da informação no mundo IoT, como a Internet das Coisas vai aumentar a superfície de ataques e como podemos nos precaver com esse novo ecossistema de dispositivos conectados à rede, como a segmentação de rede, a autenticação e o registros de atividades e eventos podem atuar para minimizar os riscos de segurança.

TEMA 1 – BYOD, *SANDBOX*

O termo BYOD (*Bring Your Own Device*), ou "traga o seu próprio dispositivo", refere-se à propriedade de ativos, em que as organizações deixam em aberto a seus colaboradores utilizar seus próprios dispositivos para trabalhar na organização. O BYOD está vinculado à mobilidade corporativa, um tipo de fenômeno global que deve envolver vários aspectos como: serviços, políticas de segurança, usabilidade e tecnologias e deve propiciar que os funcionários de uma organização desempenhem e executem suas atividades profissionais

fazendo o uso de seus próprios meios eletrônicos, como notebooks, smartphones, tablets, entre outros.

Na atualidade, o uso de celulares, tablets e notebooks é muito comum. A utilização desses meios eletrônicos dentro de uma organização acaba melhorando o desempenho das funções e tarefas, aumentando a produtividade e a comunicação. Quando são utilizados equipamentos pessoais existe o problema de utilizar as informações corporativas em aparelhos pessoais, isso acaba criando um risco à segurança da informação, equipamentos pessoais podem ser roubados ou cair em mãos erradas.

A tecnologia hoje rege o mundo, é impossível ir contra as novas ondas digitais. Dessa forma, é preciso achar uma maneira de harmonizar essa utilização de meios tecnológicos próprios dentro das organizações, eis que surge um outro conceito correlato ao BYOD chamado de Consumerização. A Consumerização de tecnologia da informação é quando os colaboradores de uma organização fazem investimentos em recursos próprios de tecnologia, seja na compra de equipamentos, na realização de cursos, treinamentos e na utilização de aplicações e tecnologias de consumo popular para a realização das tarefas organizacionais.

Além do emprego de dispositivos pessoais para o trabalho, a Consumerização de tecnologia também envolve outros elementos como a internet, as mídias sociais, ferramentas de consumo e produção. Dessa maneira, são ampliadas as relações entre colaboradores, fornecedores, clientes, parceiros e demais envolvidos. Os funcionários das empresas querem sempre poder optar pelo uso de recursos organizacionais e seus recursos pessoais, fazendo uma espécie de combinação entre vida profissional e pessoal, o uso de dispositivos pessoais é mais familiar, mais eficiente e já é parte integrante da vida dos funcionários.

Quando falamos em transformação digital, é preciso encontrar soluções seguras e práticas que consigam suprir algumas necessidades e, dessa maneira, é essencial ter um bom ambiente de testes. O *sandbox* é uma plataforma muito utilizada por desenvolvedores e empresas de tecnologia da informação para testes sem a necessidade de executar essas rotinas de testes em ambientes de produção.

A *sandbox* é uma plataforma de testes em que é possível inserir aplicações para prototipagem e testes sem impactar o ambiente de produção.

Dentro da *sandbox* os desenvolvedores de software têm a possibilidade de testar e executar todas as operações, as mudanças experimentais e demais alterações feitas nos aplicativos, sempre com o intuito de melhorar o funcionamento e a qualidade das soluções, evitando erros e problemas que possam prejudicar os sistemas de produção.

Nesse ambiente de testes é importante utilizar dados fictícios, evitando dessa maneira qualquer tipo de dano e exposição dos dados genuínos do negócio. A *sandbox* cria uma barreira, onde esses dados ficam separados do ambiente de produção, não podendo ser enxergados e visualizados por quem está do outro lado da plataforma.

As *sandboxes* fazem a replicação das várias funcionalidades e de todos os códigos das aplicações para seja possível testar os programas de maneira devida, criando um ambiente para que os criadores e desenvolvedores de softwares possam fomentar toda a sua criatividade. Normalmente são criadas novas funções e testadas novas aplicabilidades aos softwares sem que o ambiente de produção seja impactado. Podemos apontar algumas vantagens na utilização das *sandboxes*, tais como:

- aumento da criatividade;
- criação de cenários para treinamento;
- ambiente livre para desenvolvedores;
- conformidade com regras de utilização;
- otimização e ganho de tempo; e
- execução de testes sem impacto no ambiente produtivo.

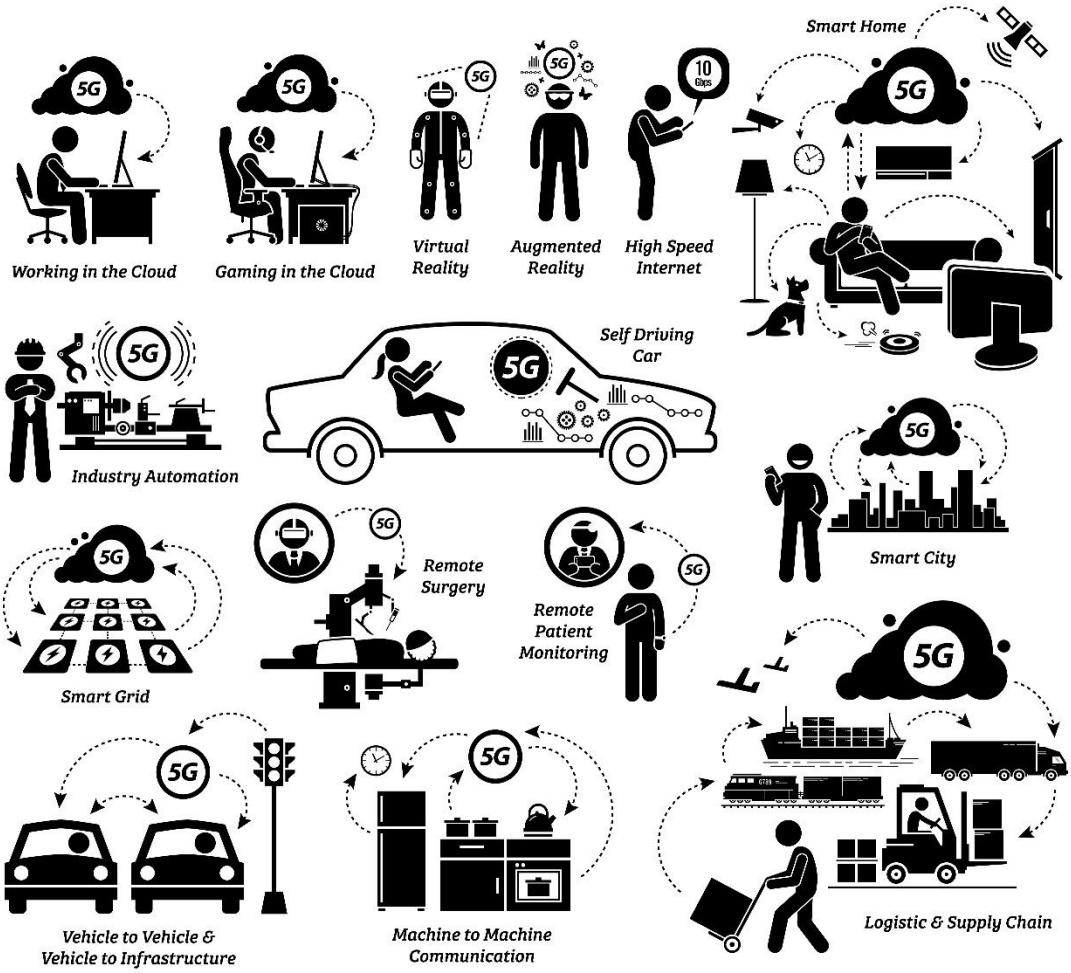
A *sandbox* é uma espécie semelhante a uma máquina virtual, tem um enfoque maior em segurança. São muito utilizadas também por empresas de segurança da informação na avaliação de ameaças virtuais como vírus e outros programas maliciosos.

1.1 Mobilidade

As tecnologias que estão sendo utilizadas nas telecomunicações estão melhorando muito a abrangência de acesso à internet e, com a chegada de novas tecnologias como a 5G, a qualidade e velocidade de acesso será ainda maior. O uso de dispositivos móveis está cada vez maior, contribuindo para o uso desses recursos para a vida profissional e pessoal em sociedade.

A partir dos anos de 2014 e 2015, o número de usuários conectados por dispositivos móveis à internet superou os acessos de usuários conectados por meio de computadores (*desktops*), atualmente o uso de dispositivos móveis ganha muito destaque, o sinal de internet móvel tem avançado, a mobilidade está alavancando muito o crescimento socioeconômico. A telefonia móvel passou por várias gerações até chegar à tecnologia 5G, que deve ser implantada no Brasil em 2022. Essa evolução da internet vem sendo empregada pelos usuários em diversas atividades cotidianas, conforme Figura 1 a seguir, fazendo o rompimento de barreiras temporais e territoriais.

Figura 1 – Tecnologia 5G e Internet das Coisas



Créditos: Leremy/ Shutterstock,

1.2 Tecnologias emergentes

Algumas tecnologias vêm criando um novo cenário, a produção de novos componentes eletrônicos proporciona novas descobertas, substituindo tecnologias obsoletas. São alguns exemplos de tendências digitais: as tecnologias vestíveis, flexíveis e a durabilidade das baterias.

- Tecnologia vestível – hoje, alguns relógios, pulseiras e óculos conseguem informar uma série de dados como data e hora, ritmos cardíacos, mensagens instantâneas, recursos complementares, aceitam comandos de voz, realidade virtual e aumentada, entre outros, além de que conseguem ser utilizados como tokens para pagamentos. Essa tecnologia vestível já faz parte da Internet das Coisas. Esses dispositivos podem ser utilizados na indústria, setor de transportes, na saúde, auxiliando no controle de dados e informações.
- Tecnologia flexível – a construção de componentes que conseguem se moldar no formato desejado e se adaptarem ao ambiente em que estão devem melhorar muito a usabilidade e atender as necessidades de qualquer usuário, a evolução de materiais e condutores mais leves, com maior potência e força, devem acelerar o crescimento das tecnologias flexíveis, caso do grafeno e nióbio.
- Baterias duráveis – com o consumo de energia cada vez maior dos dispositivos móveis e os diversos aplicativos que utilizamos diariamente, surge a necessidade de criação de baterias com maior durabilidade e poder elétrico, as primeira baterias era feitas de níquel e cadmio, mais tarde foram evoluindo para o lítio, que era um material mais leve com grande potencial energético, e existem pesquisas sendo realizadas com o nióbio, que promete revolucionar, sendo utilizado em baterias seguras, de rápido carregamento, com maior vida útil e densidade energética.

1.3 O polivalente celular

Hoje, com os celulares e as redes móveis podemos acessar qualquer tipo de serviço em qualquer momento, em qualquer lugar, muitas necessidades aparecem e várias oportunidades são criadas em diversos ramos de atuação. Os celulares apresentam um leque com muitas utilidades como: máquina fotográfica, câmera de vídeo, GPS, serviços de localização, televisão, navegador

de internet, sistemas mensageiros, rádio, carteira eletrônica, tocador de música, você pode efetuar uma série de pagamentos, o celular é hoje o dispositivo que retrata e representa toda essa convergência digital.

Para alguns especialistas, o celular é um dispositivo utilizado de maneira muito massiva e está presente em todos os grupos sociais, em todas as classes, atende pessoas de todas as unidades em qualquer meio geográfico, são incorporados a nossa vida pessoal e profissional. Existe uma grande variedade de celulares cada vez mais sofisticados e a variedade dos aplicativos desenvolvidos tem crescido bastante, desenvolvidos para atender as mais diversas finalidades.

A Figura 2 a seguir apresenta as várias funções que os celulares possuem.

Figura 2 – Funções dos celulares

Créditos: Ksyu Deniska/ Shutterstock.

1.4 Mudanças no ambiente corporativo

Com toda essa evolução digital, melhoria dos processos de comunicação, das redes e dispositivos móveis e essa possibilidade de estar sempre conectado, possibilitou algumas mudanças no ambiente corporativo, na possibilidade de poder responder uma mensagem eletrônica a qualquer momento, sem estar presente na organização, nas vantagens em poder acessar qualquer informação corporativa durante uma viagem, uma visita a um cliente, acompanhar projetos em tempo real, surge um conceito chamado mobilidade corporativa.

Entendemos como mobilidade corporativa a possibilidade de os colaboradores poderem atuar de maneira remota, executando suas funções pela empresa, sem que seja necessário estar presencialmente na organização. Os colaboradores podem desempenhar suas atividades utilizando dispositivos móveis, com recursos computacionais ajustados para atender esse serviço remoto.

A mobilidade corporativa tem ganhado muito espaço a cada dia, está sendo empregado em diversos ramos de negócio, com as novas tecnologias de comunicação, a computação em nuvem e a virtualização, é possível que os colaboradores possam acessar qualquer aplicação empresarial de qualquer lugar e momento.

TEMA 2 – SEGMENTAÇÃO DE REDE

Nas últimas décadas temos presenciado um crescimento muito grande no número de dispositivos conectados às redes de comunicações e, dessa maneira, um incremento de conexões nas redes locais das organizações. O tráfego de dados e as trocas de informações de sistemas e serviços deste número grande de dispositivos compartilhados em um mesmo segmento de rede tem como consequência a geração de tráfego muito grande dentro desse mesmo segmento, esse tráfego grande acaba ocasionando lentidões na comunicação entre os dispositivos, muitas informações de controle são utilizadas, a gestão e segurança acabam sendo comprometidas e até mesmo ocorrem indisponibilidades da rede, serviços e sistemas que operam nesse segmento, gerando uma complexidade para gerenciamento de rede e seus administradores.

Com a modernização dos equipamentos de rede nos últimos anos, houve a possibilidade de melhorar a gestão e administração das redes, tornando estas mais eficientes, com melhor desempenho e mais seguras. Os computadores (*switches*) que interligam os dispositivos de rede mantendo a comunicação o tempo todo fazem todo o tratamento, o recebimento e a entrega de pacotes de dados em toda a rede de computadores.

Gerenciar de maneira adequada as redes corporativas não é uma tarefa muito simples, a segurança de um ambiente computacional deve ser bem estruturado e organizado. Uma boa prática é realizar uma separação dessas redes em segmentos, isso pode ser importante sobre vários aspectos como:

gestão, organização, segurança, propriedade, finalidade, localidade e desempenho.

Quando utilizamos mecanismos de segmentação de rede, é essencial que sejam empregadas técnicas de proteção, contenção e filtragem de acessos externos à rede local, com o intuito de manter a integridade, a disponibilidade de acesso a dados e serviços de rede com níveis seguros.

2.1 DMZ

Um dos meios mais utilizados para aumentar a segurança da uma rede de computadores é a criação da chamada DMZ (Zona Desmilitarizada), fazendo uma separação física e lógica de serviços restritos de alta prioridade de outros com características de vulnerabilidade. Essa rede normalmente é criada para separar os dispositivos e serviços de uma rede local e a internet.

Uma DMZ também é conhecida como rede de perímetro, é uma sub-rede física ou lógica que contém e expõe serviços de fronteira externa de uma organização a uma rede maior e não confiável, normalmente a internet. Qualquer situação nessa área – isto é, entre a rede confiável (geralmente a rede privada local) e a rede não confiável (geralmente a internet) – está na zona desmilitarizada (Fraga, 2019).

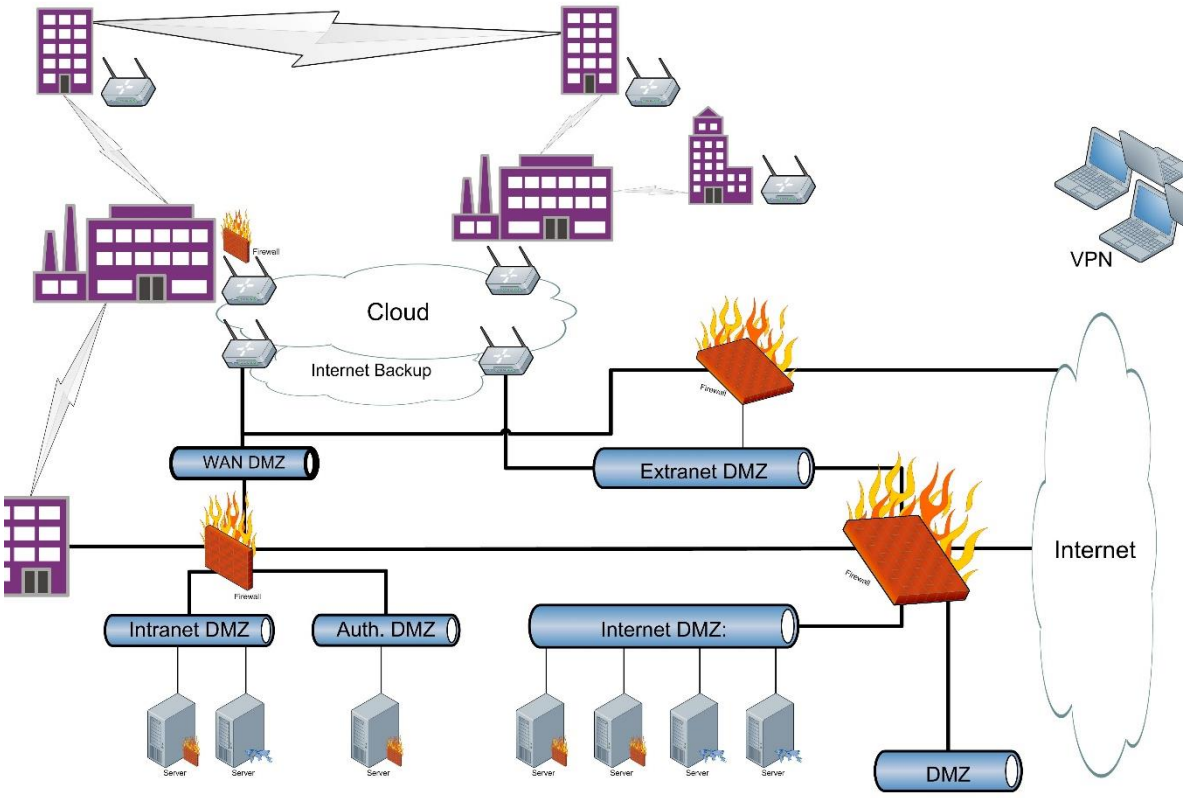
A criação e a configuração de uma zona desmilitarizada (DMZ) são boas soluções para a segurança de rede. Com um controle eficaz de acesso permitindo que todo o tráfego entre os servidores corporativos e a internet estejam devidamente isolados por um *firewall* e pela DMZ, com regras de segurança específicas para cada equipamento de rede, geralmente são servidores de páginas, aplicações que são acessadas pela internet.

Segundo Fraga, a função de uma DMZ é manter todos os serviços que possuem acesso externo, tais como servidores web, transferência de arquivo, correio eletrônico, aplicações com acesso pela internet, entre outros. Esses servidores ficam juntos em uma mesma rede, limitando assim o potencial dano em caso de comprometimento de algum desses serviços por um invasor. Para atingir esse objetivo, os dispositivos presentes em uma DMZ não devem conter nenhuma forma de acesso à rede privada local.

Por mais que possa parecer um tanto quanto complexa a criação de uma DMZ, podemos definir que a elaboração de uma zona desmilitarizada nada mais é que um grupo de servidores que tem acesso externo (internet), configurados

de maneira separada da rede privada local para uma maior segurança. A Figura 3, a seguir, apresenta um diagrama de rede em que são empregadas estruturas de rede DMZ.

Figura 3 – Diagrama de rede DMZ



Créditos: Natascha Kaukorat/ Shutterstock.

2.2 *Honeypots*

Já as *honeypots* (pote de mel) nada mais são que sistemas e dispositivos que têm por objetivo criar alguns ambientes computacionais falsos, muito semelhantes aos reais, e têm por finalidade servir como armadilha e atrair possíveis ataques para que dessa maneira seja possível mapear, monitorar e estudar esses ataques. É um sistema computacional sacrificial que pretende atrair ataques cibernéticos, como uma emboscada.

As *honeypots* fazem a emulação de alguns alvos para os *hackers* e usa suas tentativas de intrusão para obter informações sobre criminosos virtuais e a maneira como eles estão operando ou para distraí-los de outros alvos. Essa rede parece um verdadeiro sistema computacional, com aplicativos e dados, enganando os *hackers* a pensarem que são um alvo legítimo.

A *honeypot* é uma ferramenta de coleta de informações que pode ajudar a compreender e entender as várias ameaças existentes ao seu negócio e identificar o surgimento de novas ameaças. Com o conhecimento obtido de uma *honeypot*, os estudos e esforços de segurança podem ser priorizados e focados.

Existem diferentes maneiras de criar uma *honeypot*, podem ser utilizadas para mapear diferentes tipos de ameaças. Dentre as diversas configurações de honeypot, podemos elencar algumas delas.

- Armadilhas de mensagens – também são chamadas de armadilhas de *spam* e mensagens eletrônicas, nesse método são colocados um endereço de e-mail falso em uma área oculta, na qual apenas um coletor de endereços automatizado será capaz de localizá-lo. Dessa forma, como o endereço não é utilizado para nenhum outro fim, a não ser a armadilha de *spam*, é quase certo que qualquer mensagem que chegue nesse endereço de eletrônica seja *spam*. Assim, é possível identificar todas as mensagens que contenham os mesmos dados e conteúdo que as enviadas para a armadilha de spam, e estas podem ser automaticamente bloqueadas nos sistemas antispam, e o endereço eletrônico de origem dos remetentes pode ser adicionado a uma lista de bloqueio ou lista negra.
- Armadilha de banco de dados – a utilização de uma base de dados falsa pode ser criada e configurada para mapear e monitorar vulnerabilidades de softwares a possíveis ataques de exploração a uma determinada arquitetura de sistema insegura ou usando ferramentas de injeção para linguagens de banco de dados como o SQL, exploração de serviços, ou até mesmo tentativas de invasão, quebras de senhas e escalação de privilégios de acesso.
- Armadilhas para vírus – uma *honeypot* para vírus (malwares) cria uma imitação de aplicativos de software e APIs de desenvolvimento para atrair ataques de malware. Dessa maneira, é possível mapear as características e estrutura dos malwares, que podem então ser analisadas para a criação e desenvolvimento de soluções antimalware ou para identificar e corrigir vulnerabilidades nos sistemas.
- Armadilhas para Web – tem o intuito de capturar todo o tipo de rastreadores da Web por meio da criação e elaboração de páginas Web e links acessíveis apenas a rastreadores. A detecção de rastreadores tem

como objetivo ajudar a conhecer e aprender mais como bloquear sistemas maliciosos, assim como os rastreadores de rede de anúncios.

Em todo esse mapeamento e monitoramento do tráfego que entra no sistema *honeypot* podem ser avaliado elementos como: de onde os criminosos virtuais estão atacando (qual país, por exemplo), os níveis de ameaça, como é o *modus operandi* desses invasores, quais são os dados e aplicativos mais atacados (que despertam maior interesse) e como as suas medidas de segurança estão respondendo e funcionando para impedir esses tipos de ataque. Uma *honeypot* tem a função de fornecer informações e conhecimento para auxiliar os analistas de segurança a priorizarem os seus esforços de segurança cibernética.

2.3 Isolamento de rede

A virtualização de redes é uma nova tecnologia apontada como uma solução promissora para o gerenciamento de redes. Com a virtualização, a rede física é subdividida em fatias chamadas de redes virtuais, cada uma com suas próprias características, como pilha de protocolos e sistema de endereçamento. Com isso, o núcleo da rede é flexibilizado e passa a dar suporte à inovação. Alguns aspectos principais que devem ser providos para as redes virtuais são o isolamento, de forma que uma rede virtual não interfira nas demais, o desempenho no encaminhamento de pacotes e o provimento de qualidade de serviço ficam mais efetivos e eficazes.

Quando falamos de isolamento de rede podemos destacar também alguns equipamentos de rede sem fio em que possíveis é possível ativar algumas funcionalidades de isolamento de rede e dispositivos, é uma forma de evitar que usuários de uma rede com fio consigam ter comunicação com usuários de uma rede sem fio dentro de uma mesma organização, por exemplo. Alguns roteadores de rede sem fio têm recursos e algumas configurações que apresentam essas funcionalidades.

- Isolamento de ponto de acesso ativado + isolamento de rede ativado: ocorre o isolamento entre os usuários da rede sem fio (eles não podem se comunicar) e o acesso à rede principal não é permitido.

- Isolamento de ponto de acesso ativado + isolamento de rede desativado: apresenta isolamento entre os usuários da rede sem fio (eles não podem se comunicar) e o acesso à rede principal é permitido.
- Isolamento de ponto de acesso desativado + isolamento de rede ativado: os usuários da rede sem fio podem se comunicar uns com os outros, mas o acesso à rede principal não é permitido.
- Isolamento de ponto de acesso desativado + isolamento de rede desativado: nesse método, os usuários da rede sem fio podem se comunicar entre si e o acesso à rede principal é permitido.

2.4 VLAN

O conceito e a utilização das VLANs (*Virtual Lan Area Network*) em organizações, nas universidades e em outras grandes redes estão intimamente relacionados a uma forma de redução de custos e à melhoria nos processos de mudanças e alterações constantes nos setores, na estrutura da rede e na utilização dessas redes por seus usuários.

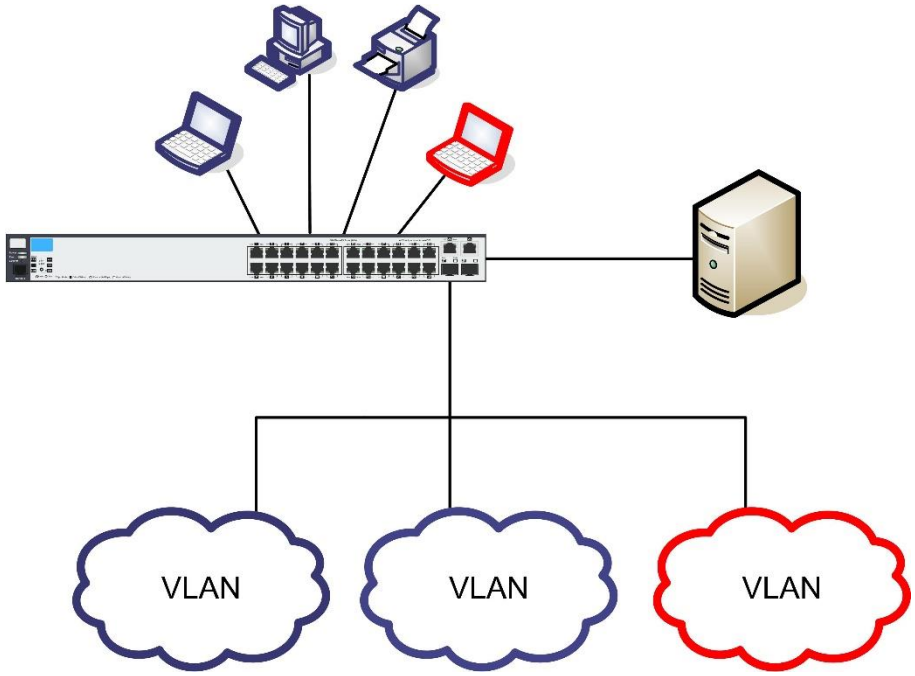
Como argumentado anteriormente, com crescimento e maior complexidade das redes de computadores tem sido muito comum nos dias de hoje que as redes físicas sejam separadas em vários segmentos lógicos, o recurso utilizado pelos *switches* para fazer essa segmentação é chamado de VLANs. Podemos considerar uma VLAN com sendo basicamente uma rede lógica em que é possível agrupar vários dispositivos seguindo algum tipo de critério, como: localização, grupos de trabalhos, por departamentos, pelo tipo de tráfego, pela finalidade, pela propriedade, entre outros.

As VLANs conseguem fazer a segmentação das redes físicas, sendo que a comunicação entre dispositivos de VLANs diferentes deverá ser feita obrigatoriamente por um roteador ou outro equipamento capaz de realizar roteamento e encaminhamento de pacotes, este equipamento será incumbido por fazer todo o encaminhamento de tráfego entre essas redes (VLANs) distintas.

As VLANs podem ser criadas e configuradas de diversas maneiras, entre elas a configuração baseada a nível de protocolo, normalmente por endereçamento lógico (IP), mas também pode ser configurada baseada nos endereços físicos dos dispositivos (*mac-address*), ou até por uma porta de comunicação de modo específico do *switch*.

A segmentação da rede com a utilização das VLANs é a forma mais eficaz para um melhor controle a nível de gerenciamento da infraestrutura de grandes redes de computadores, faz uma grande contribuição em relação à: escalabilidade, confiabilidade, qualidade e disponibilidade da rede, tornando a rede mais resiliente e tolerante a falhas. As VLANs oferecem ainda outras vantagens, como maior segurança, flexibilidade, redução de custos etc. Na figura a seguir, é mostrado um cenário de utilização de VLAN, em que parte dos computadores faz parte da rede azul (VLAN Azul) e parte dos equipamentos faz parte da rede vermelha (VLAN Vermelha).

Figura 4 – Cenário de uso VLAN



Créditos: Bildagentur Zoonar GmbH/ Shutterstock.

TEMA 3 – SEGURANÇA DE NUVEM PRIVADA, PÚBLICA E MISTA

A expressão "computação em nuvem" foi empregada pela primeira vez em 2005 por Eric Schmidt, um gerente do Google. A computação em nuvem pode ser definida de várias formas. A computação em nuvem é o conjunto de recursos virtuais facilmente utilizáveis e acessíveis, tais como hardware, software, plataformas de desenvolvimento e serviços. Esses recursos podem ser dinamicamente reconfigurados para se ajustarem a uma carga de trabalho variável, permitindo a otimização do seu uso. Esse conjunto de recursos é tipicamente explorado por meio de um modelo em que o pagamento é feito pelo

uso, com garantias oferecidas pelo provedor por meio de acordos de nível de serviços. A computação em nuvem é substituir ativos de TI que precisam ser gerenciados internamente por funcionalidades e serviços contratados oferecidos por provedores, pagando pelo seu uso a preços de mercado (Veras, 2015).

A computação em nuvem (*Cloud Computing*) é resultado de uma grande evolução e da união de vários métodos, fundamentos e elementos técnicos da área de tecnologia da informação: a virtualização de servidores, os sistemas distribuídos, os *grids* e *clusters* computacionais, os softwares orientados a serviços, a melhor gestão de grandes instalações e centros de informática, as evoluções dos equipamentos, do hardware e dos sistemas de gerenciamento e controle, dentre tantas outras.

Trata-se da gestão e utilização muito mais eficiente e eficaz da infraestrutura de TI, questões relacionadas aos softwares de controle, as maneiras de acessar, armazenar e processar dados por meio de diferentes dispositivos e tecnologias voltadas à internet. De maneira prática, a computação em nuvem seria a transformação dos sistemas computacionais físicos para um ambiente virtualizado. A proposta da computação em nuvem é de alguma maneira otimizar a utilização dos recursos computacionais, de uma maneira que torne as operações de tecnologia e os gastos com infraestrutura menores e mais econômicos, conforme Figura 5 a seguir:

Figura 5 – Computação em nuvem

Créditos: GoodStudio/ Shutterstock.

A computação em nuvem possui algumas características e entre elas podemos destacar:

- autoatendimento sob demanda;
- amplo acesso a serviços de rede;
- variedade de recursos;
- elasticidade rápida;
- serviços mensuráveis.

3.1 Virtualização

Segundo Veras, a virtualização ajudou as empresas a usar os recursos de hardware com mais eficiência. Ela possibilitou desvincular o ambiente de software e do hardware. Agora os servidores existem como se fossem um único arquivo, uma máquina virtual. É possível movê-los de um hardware para o outro, duplicá-los quando desejar e criar uma infraestrutura mais escalonável e flexível.

3.2 Modelos de computação em nuvem

Os ambientes utilizados na computação em nuvem podem ser classificados e compostos por três modelos de serviços que apresentam um padrão de arquitetura para aplicações e soluções que utilizam a computação em nuvem. Os benefícios e riscos globais serão diferentemente tratados, dependendo do modelo de serviço e tipo de implantação que atenderão as necessidades da empresa contratante. É importante notar que, ao se considerar os diferentes tipos de serviços e modelos de implantação, as organizações devem considerar os riscos e ameaças que os acompanham. Esses modelos são classificados como se segue.

- Software como serviço (*Software as a Service* - SaaS) – nesse modelo, os aplicativos são ofertados como serviços pelos provedores e acessados por diversos usuários por aplicações que utilizam os navegadores de internet. Todo a parte de controle e gerenciamento da rede, sistemas operacionais, serviços e armazenamento, é de responsabilidade dos provedores de serviço. O modelo de serviço de SaaS possui uma série de desafios a serem vencidos, dentre os quais podemos destacar os problemas regulatórios, a integração com os recursos internos das

organizações, a disponibilidade e, mais especificamente, a segurança das informações.

- Infraestrutura como Serviço (*Infrastructure as a Service* – IaaS) – nesse modelo, os provedores de serviços oferecem sua infraestrutura de armazenamento e processamento de uma maneira transparente. Os utilizadores não têm o controle da infraestrutura física, porém com as funcionalidades da virtualização é possível fazer o controle de suas máquinas virtuais, aplicativos instalados e controles relacionados à conectividade e rede. Nesse modelo de serviço, o fornecimento de infraestrutura computacional (geralmente em ambientes virtualizados) é o principal objetivo. Possui algumas características básicas como o fornecimento de uma interface para administração da infraestrutura; provisionamento dinâmico de recurso e serviços, destaque para a alta disponibilidade e o balanceamento de carga.
- Plataforma como serviço (Platform as a Service - PaaS) - nessa modelagem, o provedor oferece uma estrutura para o desenvolvimento de aplicações e softwares que serão hospedados e executados na nuvem. Essas plataformas na nuvem têm modelos de computação, armazenamento e comunicação para aplicativos na nuvem. Tem como característica a entrega de uma plataforma para desenvolvimento, teste e disponibilização de aplicativos web com a finalidade de facilitar a implantação de aplicações sem os custos e complexidade de gerenciamento do hardware.

3.3 Tipos de computação em nuvem

A computação em nuvem oferece quatro tipos básicos para sua gestão e propriedade. A definição do tipo que melhor se adapta às particularidades de cada organização depende muito das características de cada negócio, os tipos de informação e dos níveis de acesso, utilização e controle. Os principais tipos de computação em nuvem serão listados a seguir.

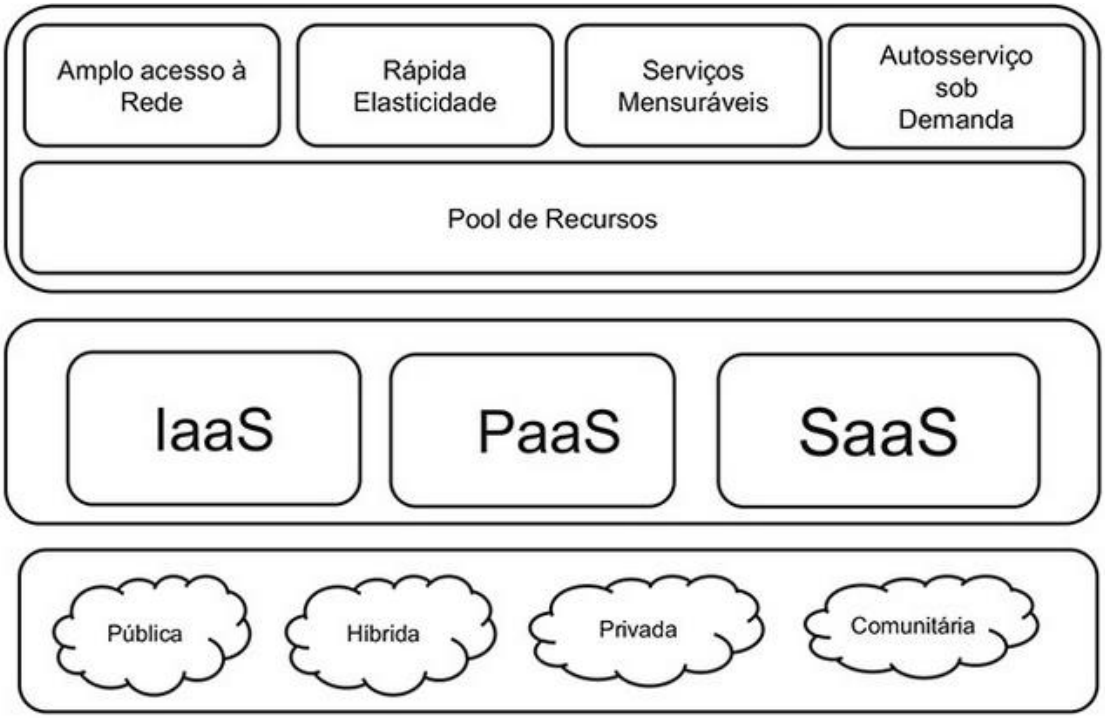
- Computação em nuvem privada (*Private Cloud*) – neste tipo de nuvem privada, é permitido que as organizações ou equipe de parceiros administrem a infraestrutura. Nessa forma de utilização, as políticas de segurança de acesso a serviços são empregadas. Os métodos utilizados

para prover tais características podem ser a nível de gerenciamento de redes e as configurações desses serviços são realizadas pelos provedores de serviços, são empregadas algumas tecnologias de autenticação e autorização. Em comparação com outros tipos de modelos de implantação de nuvem, esse modelo é o que apresenta um menor risco, pois tem sua natureza de domínio privada. Esse cenário traz uma série de facilidades por ser um ambiente da organização, porém esse modelo exige uma gestão interna, o que atrapalha a premissa de economia de recursos.

- Computação em nuvem pública (*Public Cloud*) – neste tipo de computação em nuvem, toda a infraestrutura é disponibilizada para o público em geral, sendo utilizado por qualquer usuário que conheça a forma de acesso e localização do serviço. Nesse cenário, podem ser criadas algumas restrições de acesso quanto ao gerenciamento de redes e aplicadas técnicas de autenticação e autorização. O conceito de computação em nuvem pública apresenta às organizações uma maior economia de escala, pois existe o compartilhamento de recursos. Todavia, possui uma série de limites de recursos e customização, recursos, a falta de segurança e sigilo das informações, acordos de nível de serviço e políticas de acesso, pois dessa forma todos os dados podem ser armazenados em locais desconhecidos e não podem ser de difícil recuperação em caso de falhas.
- Computação em nuvem comunitária (*Community Cloud*) – nesse tipo de nuvem a comunidade de usuários faz o compartilhamento por vários provedores de serviços na nuvem, sendo esta administrada e suportada por uma grande comunidade que faz o compartilhamento de temas e interesses da comunidade, existem alguns desafios em relação aos requisitos de segurança, política e considerações sobre flexibilidade. Este tipo de modelo de implantação pode existir localmente ou remotamente e pode ser administrado por alguma empresa da comunidade ou por parceiros, semelhante ao tipo de computação em nuvem privada em relação à definição de políticas de acesso e à utilização de tecnologias de autenticação e autorização. Outra característica que merece destaque é a possibilidade de os dados serem armazenados com os dados de outros concorrentes pertencente à mesma comunidade.

- Computação em nuvem híbrida (*Hybrid Cloud*) – este tipo de computação em nuvem tem como característica a composição de dois ou mais tipos de computação em nuvem (comunidade, privada ou pública), que mantém como entidades únicas, sendo interligadas por uma tecnologia padronizada ou proprietária que traz a portabilidade de dados e de aplicações. A adoção desse tipo de computação exige uma classificação, mapeamento e modelagem dos dados, para garantir que estes sejam atribuídos ao tipo de nuvem correto. Um fator negativo nesse tipo de nuvem é o alto risco de ameaças, pois acaba sendo vinculado e concatenado com diferentes tipos de computação em nuvem.

Figura 6 – Modelos e tipos de computação em nuvem



Fonte: Veras, 2015.

3.4 Segurança na computação em nuvem

Será que a nuvem é segura? Será que as minhas informações estarão seguras? Quem vai garantir que os provedores de serviços de nuvem estão tratando os meus dados de maneira segura? Bem, essas são perguntas que recebemos diariamente. Quando se decide usar um provedor de serviços na nuvem ou terceirizar os recursos de TI, questões desse tipo sempre geram preocupação (Donda, 2020).

Quando falamos de segurança da informação na computação em nuvem, podemos relacionar vários riscos. Com os modelos de entrega de soluções e sistemas hospedados em provedores, surgem as questões relacionadas à privacidade e segurança das informações que estão hospedadas na nuvem.

Com todas essas preocupações sobre os riscos que a computação em nuvem muitas vezes ignorada, cresce a importância de criar planos de redundância e contingência de acordo com níveis de serviço, a premissa de garantia de confiabilidade e a certeza de que os processos de negócios não sofreram nenhum tipo de dano ou interrupção no caso de problemas e incidentes computacionais. Os riscos e ameaças referentes à segurança e privacidade de dados na nuvem e a portabilidade desses dados criam um cenário de alta criticidade e preocupação para as organizações.

Todas essas questões acabam impulsionando os analistas de segurança a mudarem antigos paradigmas e a buscarem cada vez mais a adoção das melhores práticas em segurança, caso suas organizações pretendam desfrutar dos benefícios da computação em nuvem. Para Donda, os provedores de soluções em nuvem possuem muitos controles de segurança em seus sistemas, que dão aos clientes a garantia de que os dados serão tratados conforme os principais padrões de segurança. Vamos elencar alguns exemplos de recursos.

- Segurança física de centros de informática – com monitoramento 24 horas por dia, durante toda a semana, com câmeras de segurança internas e externas e um controle de acesso restrito, garantindo a segurança física dos centros de processamento.
- Restrições baseadas em geolocalização – faz o filtro em relação aos acessos conforme a escolha do cliente em relação a sua localização geográfica, criando regras de utilização, armazenamento e controle de maneira geral.
- Criptografia de dados em repouso e transporte – são recursos utilizados para garantir a confidencialidade dos dados armazenados para que não sejam legíveis por qualquer usuário ou aplicativo não autorizado. Essa criptografia também deve ser empregada quando os dados estão sendo comunicados e em trânsito, principalmente quando falamos de transmissão em meios não seguros como a internet.

Alguns modelos de gestão de riscos e ameaças foram elaborados para tentar minimizar essas preocupações com a segurança da informação na nuvem. É um grande desafio ter esses dados disponíveis o tempo todo, ao mesmo tempo, de maneira protegida e segura. Os processos de negócios e procedimentos precisam levar em conta a segurança, e os administradores de sistemas e equipe de segurança da informação devem alinhar suas políticas e procedimentos de segurança para atender às necessidades do negócio. Alguns exemplos de riscos de computação em nuvem para a empresa que precisam ser gerenciados incluem o que se segue.

- A escolha de um bom provedor de computação em nuvem como sendo o passo inicial. Reputação, origem, história, portfólio de produtos, sustentabilidade são alguns fatores considerados na escolha.
- A responsabilidade na gerência e manipulação dos dados é um ponto de atenção. Acordos de nível de serviço devem ser combinados, é um aspecto crítico ao negócio.
- O dinamismo da computação em nuvem pode dificultar a identificação do local onde as informações estão armazenadas.
- Acesso de parceiros e terceiros a informações críticas pode causar algum tipo de comprometimento, segredos corporativos e propriedades intelectuais devem ser blindadas e protegidas.
- Atender as legislações e os aspectos legais em relação aos dados, conformidade com regras e regulamentos fica um pouco mais difícil, porque a computação em nuvem nem sempre respeita barreiras geográficas e temporais.
- A recuperação de desastres, planos de continuidade de negócios, são outros pontos a serem levados em conta.
- Como as informações ficam todas armazenadas na computação em nuvem, abre-se uma superfície maior de ataques para hackers, ambientes em nuvem são explorados de maneira maior pelos criminosos virtuais.
- Segregação de dados, criptografia de dados armazenados e em transporte. A nuvem precisa prover isso.
- Apoio a investigações, pelo dinamismo dos acessos e pela forma como a tecnologia evolui, é necessário ter mecanismos de auditoria para a descoberta de ações ilegais e acessos indevidos.

TEMA 4 – SEGURANÇA EM *FOG CLOUD* (IOT)

A Internet da Coisas (*Internet of Things* – IoT) é um conjunto computacional que reúne componentes de hardware, software e conectividade com o intuito de interligar objetos físicos com infraestruturas e comunicação e a internet. Esses objetos, que são chamados de dispositivos IoT, são formados por sensores e atuadores e têm, de maneira geral, baixo poder computacional de armazenamento e processamento, todavia são dispositivos que quando conectados são capazes de realizar processamento, coletar informações, reagir a estímulos e podem fornecer um valor agregado. Com esses dispositivos mais baratos e a sua capacidade de promover inovação, a tendência é um crescimento na utilização de IoT e a criação de várias aplicações que façam uso desses elementos.

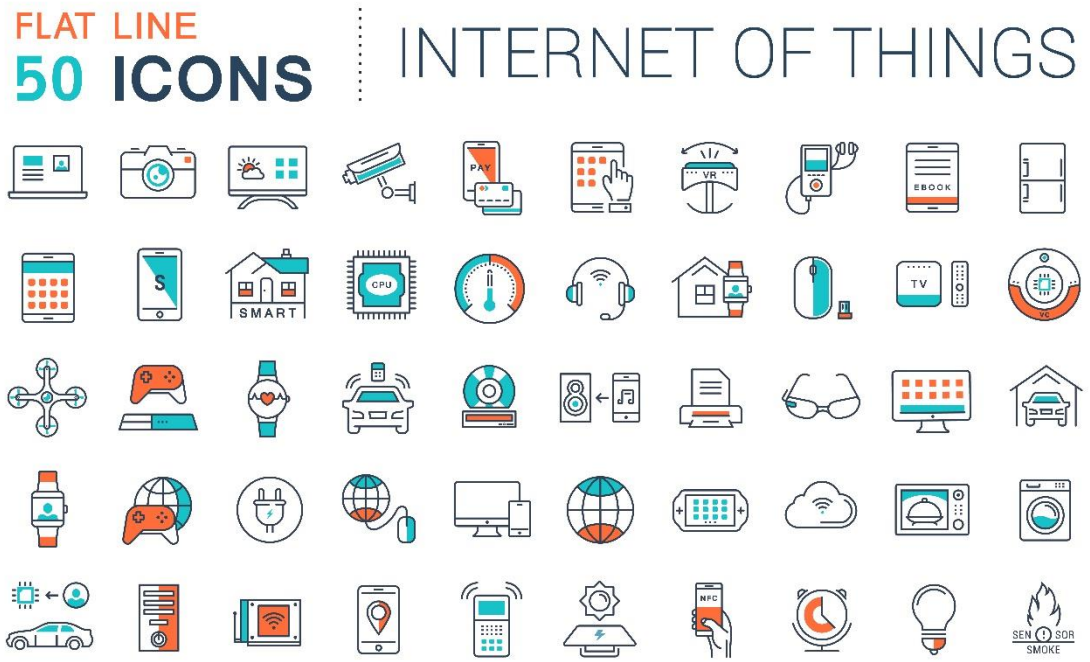
A Internet das Coisas (IOT) pode ser considerada “um ecossistema computacional de sensores e recursos interconectados, que permitem a tomada de decisões inteligentes”. Com base nessa definição, temos o fato de que as informações estão no coração da IoT, alimentando um ciclo contínuo de detecção, tomada de decisões e ações. A IoT está fortemente ligada aos sistemas computacionais e, a esse respeito, é um facilitador de infraestruturas inteligentes, como a Indústria 4.0, rede inteligente, transporte inteligente, entre outros. Permitindo serviços de maior qualidade e facilitando o fornecimento de funcionalidades avançadas (Alves, 2021).

Dessa forma, a Internet da Coisas é um novo paradigma que surgiu nos últimos anos. Tudo isso faz parte de uma evolução natural da tecnologia da informação e carrega consigo uma série de desafios. Os riscos e ameaças que têm relação com esses dispositivos, serviços e sistemas IoT são diversos, dinâmicos e evoluem de maneira muito rápida. A IoT vai causar um grande impacto na área de segurança da informação e proteção de dados, a superfície de ataque será mais ampla. Portanto, é essencial ter os entendimentos em relação ao que precisa ser protegido e elaborar medidas de segurança específicas para a IoT contra-ataques cibernéticos.

Segundo Alves, a IoT promete sistemas complexos que detectam o ambiente externo e tomam decisões sem a necessidade de intervenção humana. Isso significa que muito mais informações sobre a vida humana serão coletadas e processadas por esses sistemas, como alguns ambientes controlados sendo

capazes de detectar e gerenciar dados pessoais e muito sensíveis. Isso torna a proteção de dados um recurso obrigatório nos sistemas de IoT, colocando o quesito privacidade dos dados e sua consequente proteção cada vez mais em pauta. A Figura 7 a seguir apresenta um grupo de vários elementos e dispositivos do ecossistema IoT.

Figura 7 – Dispositivos IoT



Créditos: M.Style/ Shutterstock.

Com a Internet das Coisas será possível combinar a utilização de sensores do mundo real com o poder da internet. Os sensores fazem a coleta de informações do ambiente externo e os dados são concatenados com dados que estão armazenados na computação em nuvem, depois esses dados são analisados e processados de modo geral para gerar conhecimentos e contextos referentes àquele domínio de atuação. Essa combinação e integração sinergética entre IoT e a nuvem é chamada *de Cloud of Things* (CoT).

Com todos esses novos desafios criados por essas novas tendências tecnológicas, as corporações, indústrias e as universidades estão elaborando uma série de soluções viáveis para atingir o pleno potencial da IoT. Com essa mobilização em torno da migração da computação para a nuvem, seja para processamento ou armazenamento, surge um outro paradigma chamado

computação em neblina, também denominada computação de borda ou nevoeiro.

4.1 Premissas de segurança de dispositivos IoT

Para Alves, em um mundo cada vez mais conectado surgem riscos relacionados às ameaças virtuais, vulnerabilidades e ataques cibernéticos que a IoT pode trazer consigo. Além dos riscos relacionados, também será necessário o envolvimento dos fabricantes de tecnologia com objetivo de aprimoramento dos níveis de segurança de seus produtos a fim de evitar possíveis violações, ataques e consequências aos seus consumidores. Prejuízos financeiros e de imagem à organização também serão suscetíveis de acontecer, devido à possibilidade de aplicação de sanções administrativas, estipuladas em leis de privacidade que já existem, justamente para a proteção das pessoas e de seus dados.

Existe uma série de dispositivos eletrônicos de IoT: sistemas de alarme, câmeras de segurança, relógios inteligentes, sensores diversos, computadores, notebooks, roteadores, *switches*, entre outros equipamentos que podem ser utilizados pela Internet das Coisas. Dessa forma, é essencial tomar cuidados que garantam a segurança da informação, integridade, privacidade e a minimização dos riscos. De antemão, vamos abordar algumas práticas de segurança que podem colaborar na proteção de dados e equipamentos.

É possível elencar e destacar cinco principais premissas de cibersegurança para a adoção da Internet das Coisas em ambientes corporativos, fazendo a mitigação dos maiores riscos.

- Levar em consideração todas as recomendações e requisitos de segurança dos fabricantes e fornecedores de IoT.
- Testar, avaliar e homologar as soluções de IoT em um ambiente criado para prototipagem e testes, segmentado do ambiente de produção.
- Fazer a desativação de todos os serviços que não são utilizados ou que apresentem vulnerabilidades, fazer a alteração de senhas geradas de maneira padrão pelos fabricantes de equipamentos de IoT.
- Fazer a inclusão de todos os dispositivos IoT nas atividades de gerenciamento de rede, gestão de vulnerabilidades das organizações. Criar rotinas de atualizações de software e segurança.

- Fazer a separação da rede de dispositivos IoT, criar um ambiente segregado onde seja possível criar mecanismos de controle, autenticação e emprego de criptografia.

4.2 Práticas de segurança de dispositivos IoT

Embora todo esse crescimento e expansão do uso de dispositivos e aplicações IoT apresentem uma gama muito grande de benefícios para melhora da nossa qualidade de vida, com um número cada vez mais alto de dispositivos conectados à rede, com grande tráfego de dados, temos que entender que essas características criam uma superfície maior para ataques e acabam expondo os usuários de dispositivos IoT.

Dentro desse aspecto, apresentamos uma lista de boas práticas de segurança relacionadas com os dispositivos e a Internet das Coisas.

- Televisores – as TVs armazenam várias informações pessoais, algumas possuem até câmeras para monitoramento de usuários, a atualização de software deve ser feita periodicamente, as senhas redefinidas (evitar senhas padrões de fabricantes) e não conectar a TV em redes desconhecidas. As TVs possuem interfaces de rede com cabos e sem fio. Caso não utilize alguns serviços que a TV oferece, a recomendação é desativar a função.
- Roteadores, modens e demais equipamentos de rede – são dispositivos bem comuns nas residências, em muitos casos apresentam falhas na configuração, permitindo acessos remotos, com várias funções habilitadas, é importante manter o equipamento atualizado, revisar as configurações, desativar serviços não utilizados, enviar compartilhar dados de acesso, criar senhas de acesso mais robustas e habilitar a criptografia de dados.
- Câmeras de segurança – são um dos dispositivos que apresentam maior risco, muitas vezes essas câmeras são conectadas diretamente à internet, acessos indevidos e não autorizados a câmeras de vigilância podem ser uma grande ameaça, seja para a execução de um roubo, espionagem, entre outros. A câmeras devem estar com o software atualizado (atualizações automáticas habilitadas), verificar com os fornecedores se existem times de segurança que podem auxiliar em caso de eventos

maliciosos que impactem na segurança, mudança de senhas, a fim de mitigar possíveis brechas e vulnerabilidades.

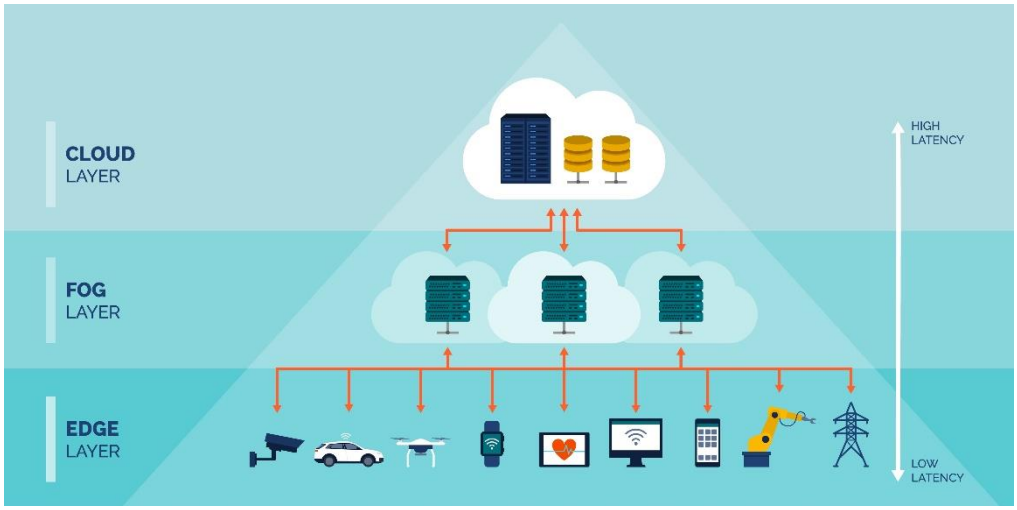
- Dispositivos removíveis – existe a possibilidade de alguns dispositivos complementares, como *pendrives*, discos rígidos internos e externos, tokens, entre outros dispositivos, virem acoplados a dispositivos de IoT, esses componentes complementares podem estar infectados com vírus e outras ameaças como malwares.

4.3 *Fog computing* ou computação em neblina

O computação em neblina, conforme mencionado anteriormente, é um novo paradigma da computação que consegue trazer as características e todas as funcionalidades da computação em nuvem para mais perto dos seus usuários e aplicações, com a melhoria das redes de comunicações com melhor latência, mais largura de banda, qualidade de serviços, maior disponibilidade, alta confiabilidade e promovendo ampla mobilidade, fica claro que o desenvolvimento de sistemas será muito mais eficiente com a computação em neblina.

A figura a seguir apresenta a estrutura, no topo a camada de *cloud computing* (*cloud layer*), no meio a camada de *fog computing* (fog layer) e na base a camada de acesso a aplicações (*edge layer*), a latência da rede varia de acordo com cada camada da estrutura.

Figura 7 – Camadas de acesso, neblina e nuvem



Créditos: elenabsl/ Shutterstock.

Os dispositivos IoT geralmente são compostos por atuadores e sensores e não possuem comunicação direta com os serviços hospedados na nuvem,

existem elementos nesse caminho como *gateways*, roteadores e servidores, todos esses contidos na camada *fog*, devem estar geograficamente próximos. Os elementos que estão na camada *fog* têm a função de efetuar o armazenamento e processamento temporário de dados, de maneira que os serviços que são necessários para executar esse processamento estejam na camada *fog*, e não mais na nuvem. Por mais que a nuvem tenha um papel reduzido nessa estrutura, ela é muito importante, pois hospeda os servidores de banco de dados e faz todo o gerenciamento de aplicações.

Cabe lembrar ainda que a computação em neblina possui alguns requisitos para atender os propósitos e prover as funções que ela promete. Dentre as características necessárias da computação em neblina estão as que se seguem.

- Distribuição geográfica – refere-se às diferentes posições geográficas dos equipamentos que fazem parte da computação em neblina e que são necessários para o gerenciamento, controle, armazenamento, processamento e acesso de usuários e suas fontes de dados. Utilizam instalações mais distribuídas, diferente da computação em nuvem.
- Suporte à aplicação de baixa latência – a computação em neblina deve prover latências bem reduzidas para aplicações que necessitem latência ultrassensíveis. Essa premissa envolve um serviço sofisticado de estrutura e suporte nas extremidades da rede.
- Portabilidade – retrata a capacidade de gerenciar diversos dispositivos IoT, mesmo estes apresentando recursos diferentes e heterogêneos, e deve conseguir interpretar essas diferenças e prover um serviço para os desenvolvedores de maneira que não seja necessário ajustar detalhes técnicos.
- Interoperabilidade – usar todo o potencial da IoT oferecendo vários tipos de serviços com a colaboração de vários fornecedores e provedores de computação em nuvem, existem desafios nesse quesito como coexistência de muitos dispositivos no mesmo ambiente trocando informações, a variedade de dispositivos de fabricantes diferentes com domínios de uso diversos, as mudanças em relação a novos protocolos de comunicação e novas capacidades, a existência de muitos formatos de dados que necessitam de tratamento e modelagem. Esse quesito é essencial para o funcionamento da computação em neblina.

- Uso eficiente de largura de banda – filtrar a utilização dos recursos de conectividade e transmitir apenas o necessário para a computação em nuvem.
- Suporte à localização – a computação em neblina deve conhecer a localização física de seus elementos, sua topologia dos dispositivos e dos equipamentos que fazem parte da estrutura, o uso de estratégias de localização e descoberta são importantes para a gestão e funcionamento.
- Suporte a contexto – refere-se à capacidade de recuperar dados e informações a respeito de alterações e mudanças de estado das diferentes variáveis contextuais do ambiente dinâmico, seus componentes e entidades.
- Suporte à mobilidade – a computação em neblina pode possuir elementos fixos e móveis. Dessa maneira, é necessário que a estrutura garanta a comunicação, a disponibilidade, as mudanças de canais de comunicação, a identificação dos dispositivos, o endereçamento e a localização.
- Disponibilidade – característica que assegura a oferta de serviços mesmo sob condições adversas de operação, com escalabilidade sem degradar a qualidade do serviço ao longo do tempo, técnicas de clonagem, duplicação e redundância, isolamento de falhas são boas práticas nesse quesito.
- Eficiência energética – essa característica está alinhada com o conceito de sustentabilidade, com a distribuição do processamento e armazenamento, a solução acaba atendendo com um custo mais baixo de consumo energético se comparado à computação em nuvem.
- Privacidade e segurança – a proteção e sigilo de dados e informações são essenciais, mas como a computação em neblina tem como premissas a heterogeneidade, distribuição, mobilidade, esse ambiente se torna muito vulnerável e mesmo seguro. Algumas medidas serão discutidas nos próximos tópicos.
- Escalabilidade – como mencionado anteriormente, é primordial que a computação em neblina incorpore novos elementos, com a adição de mais hardware, mais softwares e mais usuários, a estrutura precisa se manter em boas condições de uso, fazer um bom provisionamento e otimização de recursos são um caminho a ser trilhado.

4.4 *Edge computing* ou computação de borda

A computação de borda (*edge computing*) é a camada de rede que faz a conexão dos dispositivos finais e aos seus usuários. Ela oferece todos os recursos computacionais e é nessa camada que acontecem os processamentos locais (ou mais próximos) do usuário e suas fontes de dados. Dessa forma, com os recursos na borda, mais perto dos usuários os serviços ficam muito mais rápidos e confiáveis, e é uma maneira em que as organizações conseguem distribuir uma gama de recursos em um grande número de locais.

Em outras palavras, a computação de borda aproxima as aplicações corporativas de suas fontes de dados, como servidores de borda local e seus dispositivos IoT. Com esses recursos mais próximos serão gerados uma série de benefícios, com acessos mais rápidos, melhores tempos de resposta, maior disponibilidade e largura de banda mais aprimorada.

Com a computação de borda surgem novos desafios, como a complexidade de gerenciamento, a segurança de rede, a limitações de largura de banda e latência de rede. Nessa camada de computação é viável que sejam cumpridas algumas premissas como:

- gestão e gerenciamento adequado de cargas de trabalho em toda a nuvem com qualquer número de dispositivos;
- prover a estrutura para criação e desenvolvimento de aplicativos para locais de borda de maneira contínua e confiável;
- disponibilizar a flexibilidade e abertura de adaptação das necessidades de desenvolvimento; e
- operação da infraestrutura de maneira segura, eficiente e eficaz.

4.5 Segurança na computação em neblina

A computação em neblina apresenta grande inovação ao realizar uma computação mais distribuída, oferecendo serviços de rede, armazenamento e processamento, além da conectividade com a computação em nuvem, os grandes centros de informática e todos os dispositivos interligados nessa mesma estrutura. Essa comunicação aumenta as operações e serviços inerentes à computação em nuvem, permitindo uma geração nova de aplicativos.

O principal objetivo da computação em neblina é filtrar e agregar dados para os centros de dados e para a nuvem, aplicando uma série de mecanismos de inteligência lógica e seus dispositivos finais. A computação pode ser entendida como uma pequena nuvem, porém apresenta muitos desafios na parte de segurança. Em relação à segurança da computação em nuvem, podemos destacar alguns itens.

- Técnicas de detecção de intrusão – essas técnicas devem ser aplicadas na computação em neblina. As invasões e tentativas de ataques as redes inteligentes podem ser alertadas e detectadas utilizando métodos com base em suas assinaturas, os padrões de comportamento são analisados e comparados em um banco de dados. A intrusão também pode ser capturada por meio de métodos que utilizam como base anomalias, em que o comportamento analisado é comparado com o comportamento esperado para checar se houve desvio de conduta.
- Autenticação e autorização – em se tratando de autenticação e autorização, ainda não existem muitas soluções de segurança consolidadas para a computação em neblina. Essas etapas de autenticação e autorização acabam ficando por conta dos dispositivos que funcionam na camada de acesso e extremidades das redes. Esses dispositivos normalmente têm algum tipo de conexão com servidores de autenticação remota da nuvem, esses processos de autenticação acabam coletando logs e eventos para auditoria, como a autenticação precisa ser feita a partir da nuvem pode haver lentidão. Esse cenário de autenticação central da nuvem não é o ideal, a autenticação deve ser aplicada aos usuários que acessam os dispositivos localmente, quando a comunicação do servidor de autenticação remota estiver desativada. A criação de redundâncias e contingências locais podem ser uma saída. O importante é ter uma provisão que garanta que o acesso necessário esteja disponível em situações anormais, mesmo que isso que isso acabe impactando nos controles, auditorias e monitoramento de eventos.
- Segurança de rede e infraestrutura – com o crescimento das redes sem fio e a comunicação móvel houve um aumento nos incidentes de segurança da informação. A computação em neblina é afetada igualmente, como qualquer outra tecnologia sem fio. Os ataques são diversos (inundação, enumeração, coleta de dados, negação de serviço,

invasões, escalação de privilégios). Um controle centralizado acaba consumindo muitos recursos computacionais para a gerência de rede. Criar algumas regras de acesso nas extremidades da rede pode melhorar a escalabilidade e reduzir o custo computacional por meio da computação em neblina.

- Segurança de dados – o controle do usuário para os dados é executado pelo equipamento da computação em neblina, dessa forma, os mesmos problemas de segurança surgem da computação em nuvem. A integridade dos dados será difícil de ser garantida caso esses dados forem perdidos ou modificados. Os dados que são hospedados pela computação em neblina também podem ser manipulados por terceiro. Existem várias técnicas capazes de fornecer a integridade de dados, confidencialidade e veracidade como o uso de réplicas, cópias de segurança, criptografia, entre outras. Garantem que os usuários não armazenem dados em servidores não confiáveis.
- Privacidade – um dos pontos de atenção nesse quesito são os acessos de prestadores de serviço e órgão governamentais. Devido ao grande tráfego de dados entre os dispositivos e a estrutura da computação em neblina, é muito mais fácil coletar todas as informações importantes dos usuários. Em muitos casos, a estrutura fica vulnerável a ataques. Manter a privacidade de dados de usuários é um dos principais problemas da computação em neblina.
- Protocolos seguros e eficientes – as regras de utilização de protocolos existentes são baseadas geralmente em métricas de tempo, sincronização e transmissões de pacotes em redes sem fio. Isso nem sempre é adequado para dispositivos IoT com recursos escassos e limitados na computação em neblina. As comunicações sem fio e os cálculos utilizados para garantir a segurança consomem muitos recursos computacionais e de energia. Projetar mecanismos seguros e eficazes no IoT sem causar muito impacto ao desempenho e consumo de energia é um grande desafio.
- Verificação de localização – em ambientes mais críticos, como no caso de veículos, ferrovias, hospitais, os dispositivos IoT nessa computação em neblina precisam se movimentar de maneira rápida e dinâmica, o que pode dificultar na verificação de localização. Esquemas de checagem e

validação de localização segura precisam estar bem alinhados nesses ambientes voláteis, da mesma maneira que devem estar adequados às limitações de recursos dos dispositivos IoT.

TEMA 5 – SEGMENTAÇÃO DE REDE PARA IOT, AUTENTICAÇÃO, REGISTRO E AUTORIZAÇÃO

Com as mudanças e os benefícios proporcionados pela Internet das Coisas, novos riscos de segurança estão surgindo, é necessário proteger o funcionamento desses dispositivos, é preciso criar uma estrutura segura e confiável. Dentro desse contexto, uma das alternativas para melhorar nesse aspecto é a adoção de uma boa segmentação de rede.

Dessa forma, com o crescimento do tráfego dessas redes, conectividade cada vez maior de dispositivos a aplicações com diferentes funcionalidades em várias localidades, com o progresso da IoT é preciso estabelecer um plano dessa segurança digital com conectividade de rede segmentada, com bloqueios, a comunicação não segura ou maliciosa limita a disseminação e proliferação de *malwares* por toda a rede.

Com a segregação de recursos de rede é possível aos administradores de rede criarem e elaborarem uma série de políticas de segurança em relação a acessos, servidores, equipamentos de rede e a internet. A segmentação se torna um grande obstáculo aos criminosos virtuais, pois seu raio de ação fica menor, limitando possíveis danos, contendo tentativas de invasão e ajudando na identificação de ataques por meio de sistema de monitoramento e alertas.

Nesse mundo da IoT, manter a segurança requer que as redes estejam segregadas, com muito mais conexões de entrada, com a infinidade de aparelhos isso se torna um grande desafio, com a segmentação é possível separar os diferentes tipos de tráfegos, criar regras de aceso, isolar os dispositivos uns dos outros, em caso de ataque somente o segmento atacado será danificado e infetado. Quando isso ocorre em uma rede sem fio, é importante isolar essas redes da rede principal, mapear todos os dispositivos também é uma boa prática, essa segmentação deve ser feita com base na análise do cenário de uso, o fluxo normal das atividades sem afetar negativamente os processos de negócio.

De forma conceitual, no contexto da segurança da informação, a autenticação e autorização têm um papel fundamental. No mundo IoT, a

autenticação tem a missão de tratar e especificar se um dispositivo é dentro da rede o que realmente ele diz ser, e em muitos casos isso é dificultado. Parte dessa dificuldade se refere à comunicação entre os controladores centrais e os dispositivos IoT, os métodos de autenticação devem ser seguros, porém existem muitas limitações por parte desses dispositivos IoT, alguns algoritmos de autenticação mútua e troca de chaves como o RSA (Rivest-Shamir-Adleman) e o DH (Diffie-Hellman) podem ser utilizados nesses processos, além do emprego de criptografia assimétrica e simétrica, para serem empregados na origem e destino das comunicações.

5.1 Mecanismos de autenticação e autorização para IoT

Os mecanismos de autenticação e autorização são pontos fundamentais para o bom funcionamento da rede de dispositivos IoT. Cada elemento dessa rede possui um identificador (ID), o qual deve ser único no sistema que controla essa rede. Se esses métodos de autenticação que devem ser utilizados forem fracos ou apresentarem falhas, um atacante pode estanciar um dispositivo válido, obtendo, assim, um ID para a conexão de um dispositivo malicioso, um intruso dentro do sistema com autenticação válida. Seria possível gerar dados falsos ou até mesmo efetuar algum tipo de proliferação e infecção de ameaças e malwares em todo o sistema com o intuito de tornar o sistema inoperante, causar mau funcionamento e coletar dados sigilosos.

Um outro ponto de atenção é a privacidade e a segurança na IoT, diferentes visões sobre esses problemas podem ser listadas, como: avaliação e análise de erros e falhas de segurança nas camadas de comunicação (física, enlace e rede), checagem dos métodos de autenticação e autorização, enumeração e classificação de ameaças e ataques físicos e lógicos, controle e limitação de recursos para melhorar a segurança, recursos de processamento, gasto de energia e verificação de uso de criptografia.

A autenticação deve prover acesso apenas a dispositivos autorizados. Elementos não autorizados não podem participar da comunicação e de atividades da rede.

As atividades de autenticação devem atender duas propriedades:

- garantia de autenticação da origem, isso valida ao receptor que a mensagem recebida foi enviada por um dispositivo confiável; e
- garantia de autenticação de dados, que faz a prevenção a violação da integridade e confidencialidade no transporte dos dados.

Os dispositivos IoT devem prover e atender requisitos relacionados à responsabilidade e rastreabilidade, alguns elementos de operação precisam estar presentes nesses dispositivos.

- Finalidade – apresentar proteção a dados pessoais e ativos.
- Prioridade – atender a tríade de segurança: integridade, confidencialidade e disponibilidade.
- Tolerância a falhas de dispositivos – não comprometer o sistema, sem consequências críticas.
- Reação a ameaças – regras de desligamento ou recuperação à ameaça.
- Suporte técnico – atualizações periódicas de software, gerenciamento de correções, sem impactar na disponibilidade.
- Tempo de vida do dispositivo – renovação e atualização constante de dispositivos.
- Locais de utilização – ambientes regulares e severos.

Seguindo um manual de boas práticas para segurança IoT existem algumas atividades básicas que podem ser implementadas pelos fabricantes de dispositivos IoT para aprimorar a proteção e segurança na criação e desenvolvimento de seus produtos, seria uma espécie de linha de base, uma regra ou norma a ser adotada, entre elas podemos elencar:

- Identificação de dispositivo – criar ID físico e lógica de maneira única;
- Configurações de dispositivo – gerenciamento e alterações de configurações previstas apenas para administradores e equipe autorizada;
- Proteção de dados – blindar os dados transmitidos e armazenados de ataques e acessos indevidos;
- Acesso lógico a interfaces – filtrar e restringir acessos a recursos, serviços e protocolos das conexões de rede apenas para administradores e equipe autorizada;

- Atualizações de software – criar e elaborar políticas periódicas de atualizações de software e de segurança; e
- Reportar status de segurança – ter disponível informações de estado de segurança, colaborando também na auditoria de segurança e eventos.

5.2 Riscos e ameaças às redes IoT

Com esse grande número de dispositivos IoT conectados na internet, aumentam também os riscos e ameaças cibernética de serviços de segurança para esses ambientes. Com todos esses dispositivos sendo controlados e organizados, é possível ter grande poder de ação e as consequências de um ataque podem impactar em muitos danos severos na infraestrutura, aplicações e usuários dos sistemas.

Dentro desse cenário, as principais ameaças e riscos às redes IoT que podem ser destacadas são as que se seguem.

- Ataques físicos: todo o tipo de ocorrência, incidente e ataque que cause algum tipo de dano ou avarias, acessos não autorizados que possam comprometer a integridade do hardware dos dispositivos.
- Ataque de rede: são os ataques feitos sobre toda a infraestrutura de rede de comunicação, geralmente são executadas coletas, enumeração e captura do tráfego, depois que conseguem o controle e acesso, esses dispositivos são utilizados para a execução de outros ataques, contra outros elementos e aplicações.
- Ataques aos softwares e aplicativos: o intuito desses tipos de ataques é coletar, identificar e explorar falhas e vulnerabilidades nos softwares, em execução nos dispositivos da rede IoT.
- Ataques aos canais de comunicação: nessa modalidade de ataque, os atacantes colocam escutas do canal de comunicação dos dispositivos IoT, com a finalidade de espionar e coletar informações de interesse do atacante. Em ambiente onde são implementados a comunicação criptografada o criminoso virtual tenta identificar alguns padrões e obter dados de dispositivos responsáveis pelos processos de cifragem e decifragem das informações com o intuito da quebra e obtenção das chaves de segurança utilizadas na criptografia dos dados.

- Ataque de análise de criptografia: nesse ataque, segue-se praticamente o mesmo princípio do ataque anterior aos canais de comunicação, todavia se diferencia apenas no seu objetivo final, que é capturar a chave de criptografia para que dessa maneira seja possível decifrar os dados e ler as informações capturadas.

5.3 Ataques às redes IoT

Dentro desse contexto, é possível classificar, categorizar e identificar as ameaças de maneira mais específica, são alguns dos ataques mais comuns no mundo IoT.

- *Jamming*: é uma modalidade de ataque contra equipamentos IoT sem fio, que tem o intuito de provocar danos à disponibilidade dos meios de comunicação, inundando ou anulando a utilização do meio de comunicação pelos dispositivos da rede. Esse tipo de ataque explora vulnerabilidades encontradas em instalações e implementações de infraestruturas de IoT, geralmente são estruturas que não apresentam nenhum tipo de monitoramento de dispositivos da IoT.
- *Tampering*: nessa modalidade de ataque, são exploradas vulnerabilidades relacionadas à confidencialidade e disponibilidade dos dispositivos, por meio da violação dos dados, na qual os criminosos virtuais conseguem obter o acesso físico ao dispositivo, efetuar modificações, fazendo a exclusão ou modificação dos dados no próprio dispositivo. Após isso, o dispositivo adulterado é registrado novamente na rede para ser utilizado em um possível ataque interno ou servir de espião para a coleta de dados do ambiente IoT.
- Desativação: é quando o dispositivo é corrompido ou até mesmo destruído de maneira física e não autorizada. Esse ataque tem impacto direto na disponibilidade da rede IoT, quase como um vandalismo.
- Colisão: a colisão pode ser considerada um ataque em que há falha de comunicação causada pela existência de sinais em um canal muito disputado e concorrido, e isso pode ser fruto de um planejamento de rede mal-feito, ou pela influência de um ataque cibernético. Os dados transmitidos pelo atacante podem ser executados, interrompidos e retomados, criando uma transmissão assíncrona e fora do padrão. Isso

pode causar uma incompatibilidade, em que os mecanismos de verificação de mensagens efetuados por alguns protocolos não consigam interpretar e validar essas trocas de mensagens. Com a repetição de ciclos de mensagens estando em colisão, a disponibilidade de uma aplicação é impactada, podendo chegar a se tornar um ataque de negação de serviço.

- Exaustão: nesses ataques, o alvo são os dispositivos que utilizam baterias, a finalidade desse ataque é criar um esgotamento de recursos de energia, podendo ser relacionado à energia ou mesmo à capacidade de resposta do dispositivo, consumindo todos os recursos computacionais por meio do aumento de funções ou requisições de execução.
- Dessincronização e repetição: esse ataque utiliza meios de retransmissão de quadros perdidos, criando contextos de repetição de mensagens para retransmissão e sincronização de dados. Neste tipo de ataque, o criminoso virtual armazena dados antigos, estados de rede anteriores, pacotes já transmitidos anteriormente, e cria um laço de repetição para um dispositivo receptor, com o objetivo de enganar o receptor com dados falsos.
- *Hello flood:* esse ataque explora vulnerabilidades de modos de operação de protocolos de roteamento, alguns protocolos de roteamento dinâmico requerem que roteadores pertencentes a mesma rede transmitam uma mensagem (*hello*) para se anunciarem a seus vizinhos e trocarem tabelas de roteamento. Um hacker nesse ambiente pode simular transmissões de mensagens de anunciação para todos os roteadores pertencentes dessa rede, criando um descompasso entre esses roteadores, criando uma série de problemas de roteamento, com atualizações erradas ou incompletas e, dessa forma, causando impacto nas comunicações e replicação de dados entre esses equipamentos de rede.
- *Sinkhole*: esse ataque é mais comum em redes de sensores sem fio e consiste no comprometimento e inviabilização de um equipamento central de rede. Sem esse equipamento cérebro para controlar e comandar a rede e as trocas de mensagens, estas acabam sendo perdidas, podendo resultar em um ataque de negação de serviço nas aplicações da rede.
- *Sybil*: é um tipo de ataque executado em ambientes IoT em que são empregadas algumas regras de reputação e testa a confiabilidade dos

dispositivos. O hacker cria, edita e forja um número grande de identidades, com o intuito de instanciar e se apresentar como uma boa opção entre todos os dispositivos (equipamento de maior importância da rede). Quando consegue ser ingressado às tabelas de roteamento, pode ocasionar uma remoção de todos os equipamentos originais da tabela, criando um colapso dos ativos de rede nas tabelas de roteamento dos roteadores.

- Encaminhamento seletivo: nessa modalidade, o ataque consiste em uma ação feita de modo orquestrado entre dispositivos que foram infectados em uma rede, fazendo uma espécie de ataques de negação de serviços de dispositivos IoT, causando inoperância e atrasos no sistema, com sobrecarga na largura de banda da rede, impactando na disponibilidade da rede IoT.
- *Eavesdropping*: não é um ataque, mas um método utilizado. O *eavesdropping* pode ser classificado de modo passivo ou ativo. No modo passivo, os criminosos virtuais fazem coletas, enumeração e análise do meio de transmissão da rede, capturam e extraem dados, configurações e informações vitais do tráfego de rede. No modo ativo, os criminosos virtuais enviam mensagens de controle gerando uma série de consultas para fazer a inicialização de processos, e após essas requisições fazem toda a análise das respostas dos dispositivos de destino. Os resultados dos dois modos de ataque são utilizados para criar outros ataques.
- *Flooding*: nesse ataque, o hacker tem o objetivo de utilizar todos os recursos do dispositivo ou aplicação IoT. Isso é feito com o envio de várias solicitações para estabelecimento de conexão.
- *Malware*: os malwares são criados e anexados a pequenos programas maliciosos e dessa maneira são instanciados dentro do sistema de um dispositivo de rede IoT, esse ataque tem impacto na confidencialidade das informações e no funcionamento do dispositivo.
- *Spoofing and message forging*: são ataques que criam e forjam identidades de acesso falsas, tentam registro na rede, com intuito de se passar por outro dispositivo.
- Interseção: faz a coleta e obtenção de informações complementares sobre o sistema ou dispositivos IoT. Esses dados são capturados em registros públicos de endereços na internet, domínios em servidores de

DNS, entre outros. Nessa modalidade de ataque, o objetivo é atentar contra a privacidade do sistema, uma vez que se pode coletar várias informações sobre o funcionamento do sistema por meio desses meios.

FINALIZANDO

Iniciamos com os conceitos de BYOD e as *sandboxes*, o primeiro relacionado ao uso de dispositivos pessoais no ambiente de trabalho profissional, o segundo muito utilizado nos ambientes de testes de aplicações e sistemas, destacamos a mobilidade, as tecnologias emergentes e enfatizamos as multifuncionalidades do celular, comentamos também sobre as mudanças no ambiente corporativo. Na sequência, o tema foi a segmentação de rede, no qual elencamos os conceitos de rede desmilitarizada (DMZ), as redes falsas e armadilhas criadas pelas *honeypots*, as VLANs, como o isolamento e a segmentação de rede podem ser úteis na gestão, gerência e segurança de rede.

No tópico posterior, a abordagem foi sobre a segurança na computação em nuvem, como ela é entregue, os modelos e as classificações da computação em nuvem, além de que falamos também sobre conceitos de virtualização. Em seguida, no tema de segurança em computação de neblina, elencamos as premissas e práticas de segurança para IoT, o conceito de computação em neblina (*fog computing*), as camadas de borda, nevoeiro e nuvem, como a segurança pode ser implementada na computação em neblina e como esses elementos se relacionam. Finalizando a aula com segmentação de rede para IoT, autenticação, registro e autorização. Indicamos os principais mecanismos de autenticação e autorização para IoT, os riscos e ameaças dessas redes e quais são os ataques mais encontrados nesse cenário.

REFERÊNCIAS

ALVES, D.; PEIXOTO, M.; ROSA, T. **Internet das Coisas (IoT):** segurança e privacidade de dados pessoais. Rio de Janeiro: Alta Books, 2021.

DONDA, D. **Guia Prático de Implementação da LGPD:** conheça estratégias e soluções para adequar sua empresa em conformidade com a Lei. São Paulo: Labrador, 2020.

FRAGA, B. **Técnicas de invasão:** aprenda as técnicas usadas por hackers em invasões reais. Compilação de Thompson Vangller. São Paulo: Labrador, 2019.

VERAS, M. **Computação em nuvem:** nova arquitetura de TI. Rio de Janeiro: Brasport, 2015.