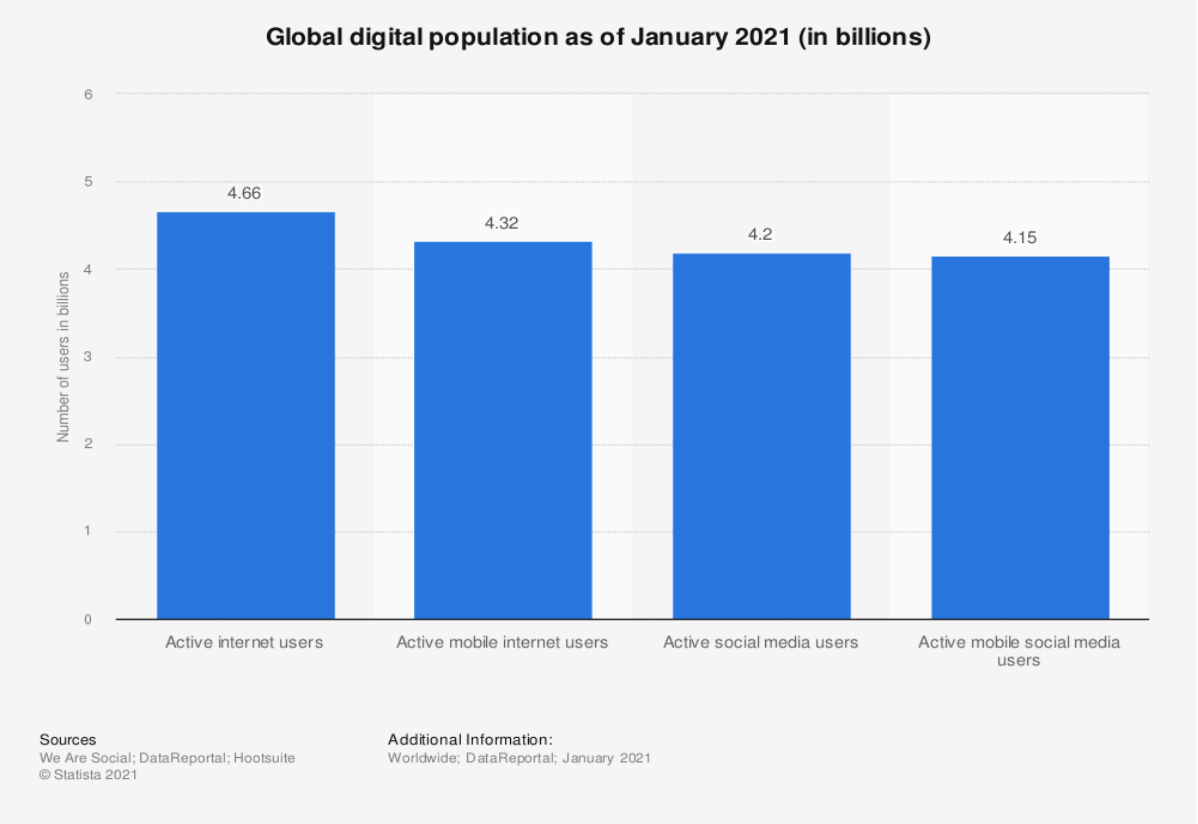
1

Como a internet funciona

A maioria das pessoas usa luz elétrica e nem imagina como ela funciona. Por que um capítulo introdutório para falar da história da internet e alguns dos fundamentos de funcionamento da rede mundial de computadores?
Nenhuma outra tecnologia se entranhou tanto na vida das pessoas e alterou tão significantemente a cultura, os comportamentos, costumes, o modo de se relacionar, ensinar, aprender, usar bancos, pedir comida, fazer política, consumir informações. Segundo por que você é o que você faz na internet, além das informações compartilhadas por vontade própria nas redes sociais, vários dados ficam registrados a cada clique em qualquer site, seu comportamento, interesses e costumes.
Entender o funcionamento básico das redes e as regras de uso dos sites é a melhor forma para buscar uma navegação segura na web. O conhecimento permite que você tenha consciência sobre os riscos a que está exposto na rede e seja um agente ativo para mais segurança e privacidade na internet, inclusive pensando melhor sobre o que compartilha. “Seus dados são você” como diz o slogan de uma campanha da Coalizão de Direitos na Rede[1] mostrando a importância da Lei Geral de Proteção de Dados(LGPD).

1 https://direitosnarede.org.br/campanha/seus-dados-sao-voce/



Segundo o site statista[2], em janeiro de 2021, havia 4,66 bilhões de usuários ativos da internet no mundo todo, o que equivale a 59,5% da população global. Desse total, 92,6 por cento (4,32 bilhões) acessaram a internet por dispositivos móveis.

A internet alcança diferentes regiões do planeta com a mesma desigualdade do mundo físico. Com exceção da Antártida (comunicações só por satélite), do deserto do Saara sem conexão alguma, o norte da Europa está em primeiro lugar, com uma taxa de penetração de 96% entre a população, seguido dos Emirados Árabes Unidos, Dinamarca e Suécia. Países grandes e populosos como China, Índia e os Estados Unidos têm mais usuários de internet do que os campeões de penetração. A China tem mais de 854 milhões de usuários e um grande firewall que controla todas as informações, mas permite que a internet funcione por razões econômicas.

2 https://www..com/statistics/617136/digital-population-worldwide/

A Índia tem cerca de 560 milhões de usuários online e outros tantos milhões offline. Algumas regiões na Ásia e na África têm baixos índices de penetração de internet, enquanto em outras a conexão é abundante. Países como Afeganistão e Paquistão são pouco conectados, enquanto países com governos autoritários como Mianmar e Coreia do Norte a conectividade é quase nula e, no caso da Coreia do Norte a internet é monitorada e apenas pessoas do governo têm acesso. Segundo o Comitê Gestor da Internet do Brasil, em 2020, havia 152 milhões de usuários, 81% da população maior de 10 anos com internet em casa. Aumento de 7% em relação ao ano anterior.
Mesmo indivíduos que não estão conectados à internet são afetados por seu alcance: bancos, comunicações, bens, serviços dependem da rede para funcionar. A internet permeia todos os aspectos da vida das pessoas, organizações, empresas e governos — estão cada vez mais dependentes da tecnologia e do acesso e da informações disponíveis na web.

Hacker é uma cultura

A palavra é entendida e usada erroneamente por quase todo mundo, inclusive a mídia, que descreve um hacker com uma pessoa com conhecimentos avançados na área de informática que faz uso desses conhecimentos para ações criminosas. Em parte é verdade, em outras não. Hack, em inglês é um verbo que significa “cortar”, e a expressão é usada por programadores todas vezes que utilizavam de truques ou artifícios de programação visando obter um comportamento diferente da programação original. As primeiras notícias do uso de hacks para obter vantagens ilícitas, foi de um grupo de programadores que identificou falhas no sistema de telefonia que permitiram-lhes fazer ligações telefônicas sem pagar por elas e isso desencadeou a ideia de que o hacker é um criminoso.

Steve Wozniak e Steve Jobs exploraram essa falha e criaram a Apple. Qualquer pessoa com conhecimentos a respeito de falhas de segurança em sistemas operacionais e navegadores é um hacker, a diferença é como esse conhecimento é usado, para fins éticos ou não.

Os hackers nasceram nos primórdios da internet, pode-se dizer serem filhos e filhas dela. Hacker é um movimento[3], um estilo de vida com uma filosofia libertária, quase anarquista, em parte se define pela rejeição dos valores normais e hábitos de trabalho. A cultura hacker é interligada de subculturas que compartilham experiências, raízes e valores. Têm um vocabulário próprio e, como todas as culturas humanas usam jargões ou gírias como uma ferramenta de comunicação, de inclusão e de exclusão, têm um código de ética baseado em código aberto e difusão de conhecimento, que deve ser livre e acessível a todos.

O termo foi criado no meio acadêmico, no prestigiado MIT[4] (Massachusetts Institute of Technology), no laboratório de inteligência artificial onde pesquisadores contornavam a escassez tecnológica para usar a ARPAnet, rede desenvolvida pelo Departamento de Defesa norte-americano e pela Agência de Desenvolvimentos de Projetos Avançados (ARPA), em plena guerra fria sob o medo de ataques nucleares. A ideia era criar uma rede com vários computadores que pudessem trocar informações através de várias conexões independentes. Se um computador ou conexão caíssem, os outros poderiam continuar a trocar informações. O plano desenhado em 1961 tornou-se realidade em 1967, mas só foi conectada à rede da ARPAnet em janeiro de 1970.

3The Jargon File" é um glossário organizado pelo hacker e escritor Eric Raymond e ficava hospedado no endereço www.tuxedo.org/~esr/jargon. No entanto, a URL redireciona para a página inicial do portal, onde se encontra uma homenagem a Aaron Swartz, famoso por ser co-autor da especificação RSS e do site Reddit. Aaron foi encontrado morto em seu apartamento no dia 11 de janeiro de 2013 após ter sido condenado pela justiça americana pelos crimes de invasão de computadores e por compartilhar arquivos acadêmicos em domínio público. O Jargon File está disponível atualmente em www.catb.org/~esr/jargon/ e também foi lançado em livro com o nome The Hacker 's Dictionary.

4 http://tmrc.mit.edu/hackers-ref.html

O uso era restrito — um consórcio com as principais universidades e centros de pesquisa para investigar a utilidade da comunicação de dados em alta velocidade para fins militares —, os recursos escassos: 13 computadores conectados em janeiro de 1971 e, dois anos depois, 38. Poucos computadores conectados à rede e muitos querendo usar daí a necessidade de contornar a burocracia para se conectar. Os criminosos digitais eram os crackers. Outra expressão criada no MIT, no mesmo contexto histórico, se referia a alunos que enganavam sistemas de segurança para escrever linhas de código. Os crackers iniciaram uma nova cultura baseada na invasão de sistemas.
Richard Stallman, hacker e programador do sistema operacional GNU e fundador da Fundação para o Software Livre, define hacker como:

> "Acesso aos computadores — e qualquer coisa que possa ensinar algo sobre como o mundo funciona — deve ser ilimitado, toda informação deve ser livre, desconfiar das autoridades e promover sua descentralização, julgar os hackers somente por suas habilidades de programação — não por critérios como formação, idade, raça ou classe social —, computadores podem criar arte, computadores podem mudar vidas para a melhor."[5]

As raízes e a ética do trabalho do hacker são acadêmicas e o compartilhamento do conhecimento é um princípio: todos devem ter acesso e utilizá-los e isso é feito usando código-aberto, resumidamente: alguém estabelece uma meta ou identifica um problema que precisa ser solucionado, propõe uma solução ou apenas aponta o problema para a comunidade. Os outros vão analisar, criticar e fazer novas mudanças, sempre dividindo os resultados com outros e dando créditos a quem fez cada parte do todo.

5 https://pantheon.ufrj.br/bitstream/11422/4104/1/DSousa.pdf

A ideia da internet como conhecemos hoje foi de Leonard Kleinrock, matemático, um dos desenvolvedores da ARPAnet, que no início dos anos 1960 era um estudante de pós-graduação do MIT, no Lincoln Lab. O perfil de Kleinrock na revista Wired[6] conta que:

> "Quando Kleinrock chegou no MIT no final dos anos 50, estava cercado por computadores enormes que não conseguiam se comunicar. Sua tese estabeleceu a noção de uma rede que trocava informações dividindo-as em pedaços minúsculos, os packet switching."

A isso deu-se o nome comutação de pacotes, pedaços de informações transmitidas individualmente entre os nós da rede, ligadas por outros nós e estabelecendo uma ligação virtual entre ambos. A comutação de pacotes otimiza o uso da largura de banda da rede e diminui o tempo que o pacote demora a atravessar a rede (latência).

A linguagem universal dos computadores

Para que os computadores se comuniquem são estabelecidas normas e padrões que definem como se dará essa comunicação, os protocolos são uma espécie de linguagem universal, interpretada por computadores de qualquer fabricante e por qualquer sistema operacional, que determinam como algo deve ser feito. Os protocolos dividem a informação em pequenos pacotes e carregam dados de endereçamento de origem e destino e são responsáveis pela sistematização das fases de estabelecimento, controle, tráfego e encerramento.

6https://www.internethalloffame.org//blog/2012/10/01/leonard-kleinrock-tx-2-and-seeds-internet

A rede é dividida em quatro camadas, cada uma com uma função específica. Os protocolos de rede variam conforme o serviço utilizado e a camada correspondente.[7]

- Camada de aplicação, a interface dos usuários

Na camada de aplicação, de interface com os usuários estão os protocolos HTTP e HTTPs, protocolos de transferência de hipertexto utilizado para requisição de páginas web. É executado na máquina do cliente e do servidor, no sistema de requisição e resposta. O HTTP se encarrega de requisitar uma página web, o servidor atende a solicitação e exibe a página ao usuário. O protocolo de transferência de hipertexto seguro, o HTTPs transmite os dados por uma conexão criptografada e a verificação da autenticidade do servidor e do cliente se dá através de certificados digitais. É o protocolo mais usado em compras online e identificado com um cadeado na barra de endereço do navegador. Para verificar a identidade do servidor basta dar um duplo clique no cadeado para exibição do certificado.
Outra forma de proteção é o Secure Shell (SSH), um protocolo de rede criptográfico para operação de serviços de rede de forma segura. Possui uma arquitetura cliente-servidor, conectando uma aplicação cliente SSH com um servidor SSH. Aplicações comuns são para login remoto de usuários a sistemas de computadores, login em linha de comando remoto e execução remota de comandos. Qualquer serviço de rede pode ser protegido com SSH.
O protocolo mais importante de segurança na camada de aplicação da rede é o TLS (Transport Layer Security), projetado para fornecer privacidade e integridade de dados entre dois ou mais aplicativos de computador que se comunicam.

7 Referência Bibliográfica: KUROSE, J. F. e ROSS, K. — Redes de Computadores e a internet — 5ª Ed., Pearson, 2010.

Várias versões do protocolo são usadas em aplicativos como navegação na web, email, mensagens instantâneas e voz sobre IP (VoIP). A conexão é segura porque usa criptografia simétrica para criptografar os dados transmitidos, as chaves de criptografia são geradas exclusivamente para cada conexão. O servidor e o cliente negociam os detalhes de qual algoritmo de criptografia e chaves criptográficas usar antes que o primeiro byte de dados seja transmitido. A identidade das partes em comunicação pode ser autenticada usando criptografia de chave pública. Essa autenticação pode ser opcional, mas geralmente é necessária para pelo menos uma das partes (geralmente o servidor). A conexão é confiável porque cada mensagem transmitida inclui uma verificação de integridade usando um código de autenticação para evitar perda não detectada ou alteração dos dados durante a transmissão. A configuração cuidadosa do TLS pode fornecer propriedades adicionais relacionadas à privacidade, como sigilo de encaminhamento, garantindo que qualquer divulgação futura de chaves de criptografia não possa ser usada para descriptografar as comunicações TLS registradas no passado.
O TLS é o sucessor do SSL (Secure Sockets Layer), um protocolo usado para criptografar e autenticar os dados enviados entre um aplicativo (como seu navegador) e um servidor da web. A criptografia faz a internet mais segura para todos. Os protocolos SSL/TLS são essenciais para sites que processam informações confidenciais, como dados de cartões de crédito, dados bancários, informações de saúde.
O Pix, o sistema de pagamentos instantâneos do Banco Central, é realizado por um canal criptografado TLS, com autenticação mútua. Os pagamentos são enviados por protocolos de segurança e certificados digitais ICP-Brasil no padrão SPB (Sistema de Pagamentos Brasileiro). A comunicação entre as instituições e o Banco Central se dá através de uma rede dedicada de alta disponibilidade tornando praticamente impossível ataque de negação de serviço (DDoS). Há ainda um mecanismo antifraude provido pelo DICT

(Diretório de Identificadores de Contas Transacionais) que informa ao prestador de serviço de Pagamento (PSP) os dados adicionais associados às chaves como data de registro, contadores de transações realizadas e relatos de infrações. A criptografia e a segurança reforçada são necessárias porque a troca de informações trafega pela rede passando por vários nós antes de chegar ao destino, e a criptografia assegura que sejam enviados e recebidos no servidor correto e garante a segurança e integridade dos dados durante o transporte. Integridade dos dados é a garantia que não haja perda ou alteração e inclui um código de autenticação de mensagem.

Na web, cada página tem um único endereço, o IP e o DNS (Domain Name System) é o protocolo responsável pela tradução dos endereços IP em nomes de domínio. Cada endereço é associado a um único domínio. Existem vários servidores DNS espalhados ao redor do mundo e nenhum deles sozinhos têm todos os endereços associados a todos os domínios na internet. Por exemplo, há 13 servidores raiz, nomeados de A a M, divididos entre América, Europa e Ásia. Por medidas de segurança cada um desses servidores é um cluster de servidores[8]. Já os domínios de alto nível como gov, edu, uk, br, são armazenados em servidores TLD. Há ainda servidores DNS autoritativos para armazenar os registros necessários para mapear os nomes de hospedeiros para endereços de IP. Por fim, há DNS local que fornece um endereço de IP do servidor local sempre que alguém se conecta à internet.

Emails são gerenciados pelo SMTP (Simple Mail Transfer Protocol) responsável pela transferência de mensagens eletrônicas. Ao escrever e enviar um email, a mensagem é enviada ao seu servidor de correio eletrônico e o SMTP envia para o servidor de correio eletrônico do destinatário e fica disponível na caixa de entrada para ser visualizado posteriormente. O correio eletrônico é gerenciado pelo IMAP(internet Message Access Protocol).

8 https://root-servers.org

Um dos mais importantes protocolos da rede mundial de computadores é o TCP (Transfer Control Protocol) que faz dois serviços principais: transporte confiável que possui um mecanismo de verificação e controle dos pacotes para não se perderem na rede. Ao ser enviado via TCP cada pacote recebe uma numeração de identificação sequencial, dessa forma quando todos os dados chegam ao seu destino o destinatário pode organizá-los na ordem correta. O TCP também é um serviço orientado para conexão segura que verifica ambos os lados da comunicação antes de iniciar a transferência de dados, isto é, quem envia e recebe têm que estar autenticados para ocorrer a troca de informações. O serviço de conexão do TCP também faz o controle de congestionamento para manter um bom fluxo de tráfego na internet. Se não houvesse esse controle seria como se todos os bits estivessem sendo transmitidos simultaneamente, congestionando os meios de transmissão, roteadores, switches, etc. O HTTP utiliza o TCP para garantir confiabilidade no recebimento das páginas web.

- Camada de rede

Na camada de rede está o IP (internet Protocol) pensado desde o início das redes para ser um serviço de internet working, ou seja, funcional para redes formadas por outras menores. Esse protocolo basicamente une toda a internet e seu principal objetivo é definir como os pacotes viajam entre sistemas finais e dispositivos de transmissão, garantindo bom desempenho independente das entidades serem da mesma rede ou de redes diferentes.
O IP Security Protocol conhecido pela sigla IPsec é uma extensão do protocolo IP que visa a ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas para bancos, lojas online), integridade dos dados (garantindo que o conteúdo que chegou ao seu destino seja o mesmo da origem) e autenticidade das informações ou prevenção de identity spoofing é um tipo de ataque que falsifica a identidade de alguém em meios digitais, se passando por outra

pessoa ou por uma empresa legítima para de roubar dados, invadir sistemas e/ou espalhar malwares. O IPsec garante que a pessoa é realmente quem diz ser, ao transferir informações através de redes IP.

VPN (Virtual Private Network) é uma conexão segura entre o usuário e a internet que oculta o endereço IP pessoal deixando que a rede o redirecione por meio de um servidor remoto. O tráfego de dados é roteado por um túnel virtual criptografado disfarçando o endereço IP e a identidade online ao navegar na internet. Não há anonimato na rede, isso é um mito comum, todas as atividades podem ser rastreadas pelo endereço IP e uma VPN oculta o endereço IP e se torna a fonte de seus dados. Isso significa que seu Provedor de Serviços de internet (ISP) e terceiros não podem ver quais sites visita ou quais dados envia e recebe online. É importante porque seu tráfego de rede é roteado pelos servidores do seu provedor de acesso que, por sua vez, pode registrar e compartilhar seu histórico de navegação com anunciantes, polícia, governo e/ou terceiros e uma VPN também deve impedir que você deixe rastros como o histórico de navegação, de pesquisa e cookies.

Cookies são pequenas informações, geralmente codificadas, usadas por servidores de internet para diferenciar sessões, usuários e para controlar os dados de navegação em um site. Serve tanto para armazenar os dados de um usuário no momento de efetuar compras online, como gerenciar permissões de acesso. Cookies colocam a privacidade em risco, ao rastrear o comportamento dos internautas no momento da navegação, captando dados e informações valiosas.

Como se proteger dos cookies
Para diminuir alguns de seus rastros digitais, você pode optar por apagar os cookies logo após cada navegação e ativar a navegação anônima, um recurso que todos os browsers têm para diminuir o número de rastreadores de conteúdos de navegação e buscas na rede. Sempre use guias anônimas no navegador quando estiver num dispositivo que não seja o seu. Exclua seu histórico em mecanismos de busca periodicamente. Use VPN ou Proxy.

Proxy — Atua como um intermediário entre o usuário e o servidor. De modo simples, o proxy faz uma ponte entre o computador e a internet, sendo aquele que autorizará aos computadores o acesso ao mundo virtual, enviando a solicitação do endereço local, o IP para o servidor, traduzindo e repassando o pedido para o computador que solicitou. Mais do que controlar o fluxo de uma rede, o proxy ajuda a proteger a navegação. Ao chegar ao site, o IP do proxy fica registrado na memória transitória (cache) do seu destino, e não o seu, pois a proxy protege a navegação do computador de origem, permitindo que os usuários naveguem de forma anônima. Com o uso de proxies é possível evitar que governos, empresas e atores maliciosos de vários espectros, inclusive políticos, realizem atividades de espionagem e vigilância. Os proxies camuflam o endereço de IP único para cada computador conectado à rede e impede que os provedores de serviços de internet vejam os sites navegados e quais dados envia e recebe online.

- Camada de transporte

A camada de rede pode não oferecer um serviço confiável por isso a camada de transporte isola as aplicações de quaisquer imperfeições no trânsito de pacotes (perdas, duplicatas) e oferece transporte de dados confiável e efetivo entre uma máquina origem até uma máquina destino com dois tipos de serviço: orientado a conexão e não-orientado a conexão. O estabelecimento de conexão garante que um lado saiba da existência do outro, que haja negociação de parâmetros e que os recursos da entidade de transporte sejam alocados. A camada de transporte permite o desenvolvimento de rotinas básicas que funcionariam em qualquer tipo de plataforma de rede, pois estabelece comunicação cliente e servidor através de diversas tecnologias de rede como o já citado modelo TCP/IP que é o modelo cliente-servidor, uma estrutura de aplicação de rede que distribui as tarefas e cargas de trabalho entre os fornecedores de um recurso ou serviço, designados como servidores, conhecido também como host, e os requerentes dos serviços, isto é, os clientes.
A camada de transporte utiliza dois protocolos: o TCP e o UDP.
O TCP (Protocolo de controle de transmissão) define como estabelecer e manter uma conversa via rede, em que programas e aplicativos podem trocar dados, portanto, é orientado à conexão e funciona com o Internet Protocol (IP), que define como computadores enviam pacotes de dados um para o outro. Também determina como dividir os dados de aplicativos em pacotes que as redes podem transmitir e mantém a conexão até que os programas de aplicação em cada extremidade termine a troca de mensagens.

O UDP (Protocolo de datagrama de usuário) recebe os dados de um processo e entrega ao processo de destino, não leva em consideração o congestionamento da rede ou uma entrega confiável dos dados, considerando apenas a multiplexação - reunir pedaços vindo de diferentes portas e encapsular para criar segmentos e entregar a camada de rede e — a demultiplexação (entrega dos dados de um segmento para a porta correta). A vantagem do TCP em relação ao UDP está na confiabilidade dos dados entregues garantindo que todos os dados repassados a camada de aplicação não estão corrompidos. Já a vantagem do UDP está na velocidade de transmissão. Nas aplicações onde velocidade é mais importante do que a ordem em que os pacotes são recebidos, como jogos, vídeos e músicas, o UDP é mais recomendado.

Portas de rede

Vários aplicativos de rede podem ser executados simultaneamente como abrir vários navegadores ao mesmo tempo ou navegar em páginas HTML baixando, um arquivo por FTP, cada um destes programas trabalha com um protocolo da camada de aplicação e o computador distingui as diferentes fontes de dados para facilitar, cada aplicação recebe um endereço único na máquina, codificada em 16 bits: uma porta. A combinação endereço IP e Porta se torna um endereço único, chamado socket. As Portas são definidas em números que variam de 0 a 65536

Porta	Serviço ou aplicativos
21	FTP
23	Telnet

25	SMTP
53	Domain Name (Nome do domínio do Sistema)
80	HTTP
110	POP3

- Camada fisíca

O objetivo da camada física é transmitir um fluxo bruto de bits da camada de enlace de dados nos meios físicos da rede. A camada de enlace de dados é responsável pela conversão dos dados em bits dos pacotes recebidos pela camada de rede e transmitindo através de cabeamento. Depende dos protocolos que entregam desde o transmissor até ao receptor em um único enlace. A camada física é responsável pelo acesso físico da rede, como especificações elétricas e mecânicas, onde é definida as taxas de dados e distancias de transmissão, nível de tensão e conectores físicos, diz respeito aos meios de conexão através dos quais irão trafegar os dados, tais como interfaces seriais ou cabos coaxiais e tem por função a transferência de dados, gerenciamento de conexões e adaptar o sinal lógico em sua transmissão.

Protocolos usados comumente na camada de enlace são:

- PPP(Point-to-Point Protocol)

A Internet consiste em máquinas individuais (hosts e roteadores) e na infraestrutura de comunicação que as conecta. Em áreas locais, as LANs são bastante utilizadas para interconexões, mas grande parte da infraestrutura geograficamente distribuída é construída a partir de linhas ponto-a-ponto.

Com frequência, estes roteadores são interconectados via backbone, mas em geral, todas as conexões com o mundo exterior passam por um ou dois roteadores que têm linhas ponto-a-ponto com roteadores distantes (regiões distantes geograficamente e são esses roteadores e suas linhas que compõem as sub-redes de comunicação, nas quais a internet se baseia. Outro uso do protocolo ponto a ponto são os milhões de indivíduos que estabelecem conexões domésticas com a Internet usando provedores (ISPs), por meio de modems ADSL, via Cabo, fibra ótica, rádio, etc. O PPP faz o tráfego de roteador para roteador, transmite dados do usuário doméstico ao seu ISP, detecção de erros, negociação de endereços IP durante a conexão, autenticação e outras características.

- Ethernet

Outro protocolo dessa camada é o Ethernet criado em 1972 nos laboratórios da Xerox, com o pesquisador Robert Metcalfe, inicialmente utilizava uma rede onde todas as estações(LANs) compartilhavam do mesmo meio de transmissão, um cabo coaxial, com configuração em barramento e taxa de transmissão de 2,94 Mbps.
A Ethernet é a tecnologia de rede local mais utilizada graças a diferenciais como baixo custo, por ter sido a primeira tecnologia de LAN largamente usada e é, atualmente, a tecnologia predominante no mundo e seus padrões definem muitos aspetos da comunicação de rede, quando as mensagens são enviadas entre hosts em uma rede Ethernet, os hosts formatam as mensagens no layout especificado. Atualmente, a Ethernet opera de forma síncrona com quadros que possuem tamanho variável entre 64 e 1518 bytes e velocidade entre 10 Mbps a 10 Gbps. A Ethernet que define como os dados serão transmitidos através dos cabos da rede. Sua função é agrupar os dados entregues pelos protocolos de alto nível (TCP/IP, por exemplo) e inseri-los dentro dos quadros (frames) serão enviados através da rede, incluindo as informações do

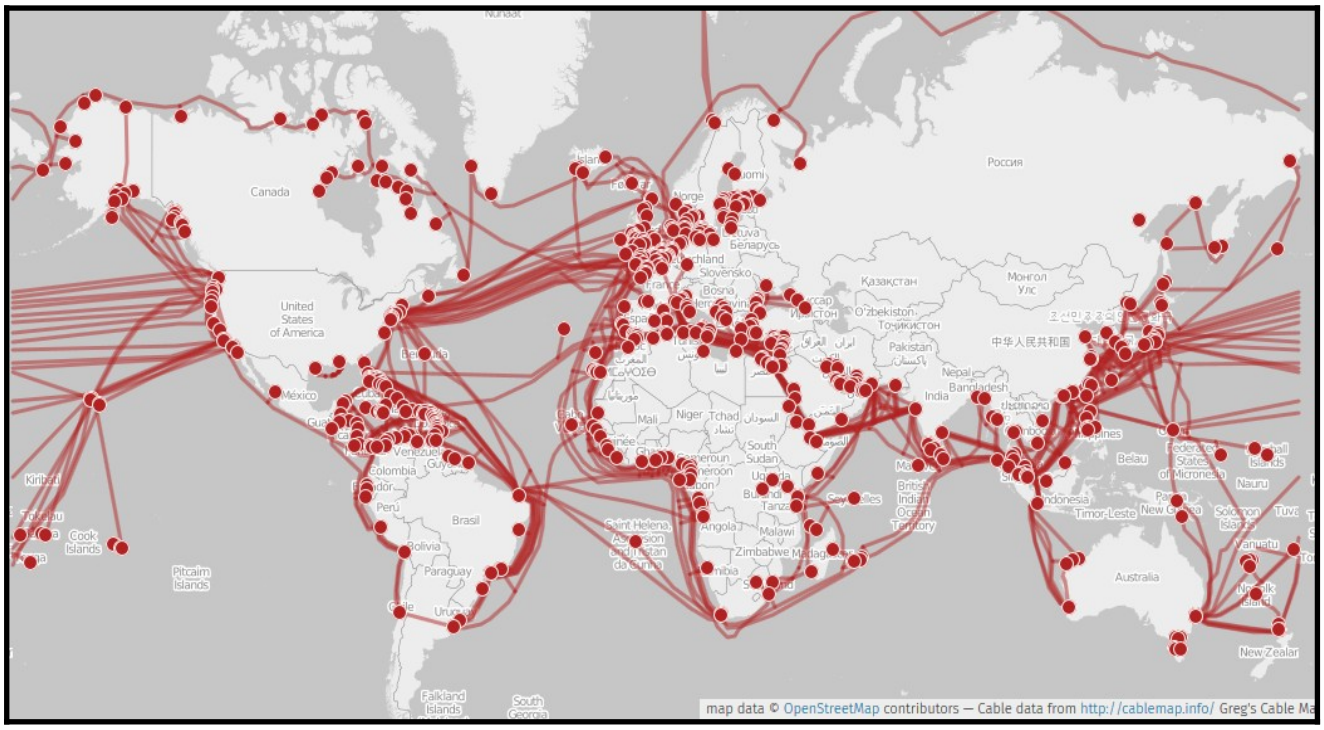
protocolo de alto nível que entregou o pacote de dados a ser transmitido. Com isso, a máquina receptora tem como saber para qual protocolo de alto nível ela deve entregar os dados de um quadro que ela acabou de receber.

- WiFi
- ATM (Asynchronous Transfer Mode) é uma tecnlogia de rede baseada na transferência de pacotes relativamente pequenos chamados de células de tamanho definido. O tamanho pequeno e constante da célula permite a transmissão de áudio, vídeo e dados pela mesma rede.

O ATM cria canais fixos entre 2 pontos para que os dados possam ser transmitidos. O que difere do sistema TCP/IP no qual as mensagens são divididas em pacotes e cada pacote pode tomar uma rota diferente para alcançar o destino. É uma tecnologia de rede tanto para redes locais como para redes geograficamente distribuídas (LANs e WANs) que suporta voz em tempo real, bem como vídeo e dados. Usa comutadores que estabelecem um circuito lógico fim-a-fim que garante a qualidade de serviço na transmissão O ATM se popularizou como a tecnologia da infra-estrutura básica das operadoras de telecomunicações e grandes corporações, mas nunca se popularizou nas redes locais (LAN).

2

Perigos da rede



Os cabos submarinos carregam 95% das informações de voz e dados transmitidos no mundo, os satélites 5%.

A foto acima é a estrutura de cabos submarinos que permitem às pessoas em todos os países e continentes (exceto a Antártida) se comunicarem, trocarem e consumirem informação. Assistir televisão aberta ou ver séries no streaming, falar ao telefone, mandar mensagens instantâneas, navegar na internet e

9 World map of submarine communication cables. cable data by Greg Mahlknecht (KML file released under GPLv3) as of 2015-07-21, world map by Openstreetmap contributors

transmitir dados de qualquer tipo depende dessa estrutura, a da foto é de 2010 e é a rede atual, o chamado ciberespaço. Não existem locais no ciberespaço fora dos nós, os pacotes de informações só podem se mover de um nó conectado para o próximo ponto predeterminado, passando por muitos outros nós por caminhos incompreensivelmente complexos.[10]

A internet nasceu pequena e flexível para mudar e se reinventar. Muitas características hoje entendidas como vulnerabilidades já existiam nos primórdios da internet que não foi projetada pensando em segurança. As ameaças eram poucas e as vulnerabilidades não eram exploradas.

Com alcance global e milhões de usuários conectados e trilhões de dólares sendo transacionados por dia, várias soluções específicas foram adicionadas ao projeto original para atender novas demandas e resolver problemas não previstos originalmente, em muitos casos, as soluções adotadas violam princípios estabelecidos pela própria concepção da rede aumentando a complexidade e problemas de interoperabilidade.

Uma vulnerabilidade é uma imperfeição ou falha que pode ser explorada por instituições e pessoas para conduzir um ataque cibernético. As vulnerabilidades existem em aplicações e nos protocolos de comunicação, por falhas de projeto, de implementação ou de configuração e em conjunto ameaçam a segurança da informação e a estabilidade da rede.

Há vários riscos na rede, embora haja uma infinidade de roteadores, firewalls e switches há falhas de estrutura física onde tudo deveria fluir com integridade, confiabilidade e segurança da informação.

O roteamento é um exemplo de elemento crítico da infraestrutura da internet. Quando se fala roteamento inclui, equipamentos, instalações, informações, protocolos e sistemas que facilitam a transmissão de comunicações em pacotes da origem ao destino. Internet Exchange Points, isto é, os sites físicos onde a

10 http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/view/349

largura de banda da internet é produzida, o peering (troca de tráfego entre redes) e os roteadores de núcleo das principais redes que transportam essa largura de banda para os usuários, além dos sistemas necessários para garantir a autenticidade do roteamento e integridade dos próprios protocolos de roteamento e seus processos de desenvolvimento, padronização e manutenção.

Há falhas nos meios de transmissão, na infraestrutura, sistemas e instalações para comunicações que atendem ao público, seja de fibra, cobre ou sem fio, em cabos terrestres, submarinos, em data centers e outras instalações físicas que hospedam servidores, conteúdo e infraestrutura de internet. Em data centers o próprio sistema usado para garantir a segurança e controle de acesso físico, operações, gerenciamento, manutenção e sistemas de redundância sistemas de comunicação usados para enviar informações de, para e dentro dos centros de dados.Celulares e outras comunicações de voz e dados sem fio são vulneráveis e trafegam por essa mesma rede. Idem dispositivos de IoT(em inglês *Internet of Things*) termo que se refere a objetos físicos ou coisas conectados à internet, todos coletando e trocando dados com outros dispositivos e sistemas. Cada componente IoT tem um Identificador Único (UID) e também pode transmitir dados sem a ajuda de humanos, exemplo comuns já presentes no dia-a-dia são os assistentes de voz do Google ou da Amazon, relógios e TVs inteligentes, óculos, entre outros.

Geopolítica da rede

A capacidade de digitalizar, armazenar, analisar e transportar dados em todo o mundo mudou a maneira como nos comportamos pessoal, comercial e politicamente. Países e milhares de pessoas se beneficiam da atividade econômica que ocorre no ciberespaço. À medida que a conectividade se espalha pelo mundo, o maior desafio para governos, empresas e pessoas é

manter a estabilidade da rede mundial com políticas de dissuasão de ataques cibernéticos que na última década atingiram sistemas governamentais e infraestruturas críticas.[11] O termo dissuasão remete a Guerra Fria e ao contexto que motivou o nascimento da internet como conhecemos atualmente: a dissuasão nuclear. As armas nucleares resultam em destruição permanente e não dá para aumentar ou reduzir a capacidade de destruição. O uso de armas nucleares é binário, são usadas ou não. O objetivo é o uso zero.

Ataques cibernéticos não são binários e fazem parte de disputas políticas, mede-se o uso da força, retaliam ações dos adversários e são usadas por governos como dos Estados Unidos, Reino Unido, Israel, China, Rússia e Irã, que usam suas capacidades cibernéticas ofensivas para causar perturbações generalizadas e até destruição física.

Como parte do combate ao estado islâmico, os Estados Unidos interromperam comunicações em alguns países do Oriente Médio. O governo russo desligou a energia elétrica na Ucrânia em dezembro de 2015 e dezembro de 2016. Em 2014, dados da Sony foram violados, o ataque ocorreu após a Coreia do Norte ameaçar os Estados Unidos de uma possível retaliação caso a Sony lançasse o filme “The Interview”, uma comédia que aborda dois jornalistas contratados pela CIA para assassinar o líder norte-coreano Kim Jong-Un.

Os governos poderiam usar ataques cibernéticos com muito mais frequência do que já fazem, no entanto, violam acordos internacionais de comportamento cibernético e potencialmente colocariam em risco a paz mundial. Ataques cibernéticos generalizados, frequentes e destrutivos contra ativos de infraestrutura crítica fora do conflito armado são autolimitados também devido a interesses econômicos.

Governos exploram vulnerabilidades, indivíduos também o fazem para roubar informações, dinheiro, para interromper, destruir ou ameaçar a entrega de serviços.

11 https://cyberstability.org/paper-series/closing-the-gap-expanding-cyber-deterrence/

Qualquer roubo de propriedade intelectual ou interrupção de negócios não chega a ameaçar a paz mundial, ou a segurança nacional, mas em conjunto e com a frequência que acontecem, se houver uma percepção que os sistemas não são confiáveis podem limitar o uso da tecnologia e restringir seus benefícios. Ransomware é um bom exemplo.

Embora a maioria dos ataques de ransomware individuais fiquem abaixo do uso da força conforme definido na lei internacional, coletivamente ameaçam a segurança nacional, prosperidade econômica, saúde e segurança públicas. A dissuasão cibernética é inútil para impedir ataques de ransomware.

A estabilidade da rede significa assegurar disponibilidade, integridade, confidencialidade e a autenticidade da informação, além de manter a cultura com que foi criada: compartilhamento, socialização, transparência, criação e difusão de conhecimento, proteção ao usuário incluindo seus direitos, liberdades de expressão, associação e privacidade.[12]

À medida que aumenta a complexidade de sistemas operacionais, software e hardware, mais vulnerabilidades eles contêm, ameaçando a segurança da informação. O conceito de segurança da informação definido pela ABNT(Associação Brasileira de Normas Técnicas) é:

> "(...) é a proteção da informação de vários tipos de ameaças (...) é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware."[13]

Outro conceito importante é privacidade que o direito define como:

12 https://cyberstability.org/report/#note-2
13 ABNT NBR ISO/IEC 17799:2005

> “o direito de ser deixado só (...) que remete à não interferência pelo Estado na vida do indivíduo (...) também como o poder de se reivindicar ao Estado a tutela da privacidade, protegendo o indivíduo de terceiros.”

Privacidade de dados está diretamente ligada à segurança da informação, mas sob a perspectiva do usuário, como os dados são utilizados, coletados e armazenados.

Em poucas palavras o que se quer na internet é:

Confidencialidade	Informação disponível só para pessoas autorizadas.
Autenticidade	Garantia sobre quem emitiu a informação.
Responsabilidade	Garantia da responsabilização por ações ocorridas na transmissão, armazenamento e processamento da informação.
Disponibilidade e confiabilidade	Garantia de que a informação está disponível quando necessário.
Não-repúdio / irretratabilidade:	Impedimento às partes da comunicação de negarem que ela ocorreu.

Ameaças

Há muitos tipos de ameaças cibernéticas para roubar dados ou perturbar de alguma forma a carga de trabalho e os serviços. Não importa o tipo ou a origem, as ameaças cibernéticas são um sério risco para a estabilidade da rede. Grande parte dos ataques usa engenharia social, ou seja, a prática de explorar emoções de um indivíduo como o medo, curiosidade, senso de urgência, ganância para enganar e fazer realizar uma ação que o atacante quer. Desde obter acesso físico a escritórios e edifícios privados e/ou acesso online aos sistemas de uma empresa para obter informações para lançar mais ataques, extorquir credenciais e/ou roubar dados, ou dinheiro.[14] É mais fácil enganar as pessoas para que caiam em armadilhas online do que na vida real, onde a desconfiança e a cautela são mais comuns.
Esses artifícios tornam a engenharia social online uma prática prevalente e perigosa, atualmente são localizados, mais personalizados e são direcionados geograficamente. A empresa Acronis, que treina equipes de TI com soluções de proteção cibernética, aponta que:

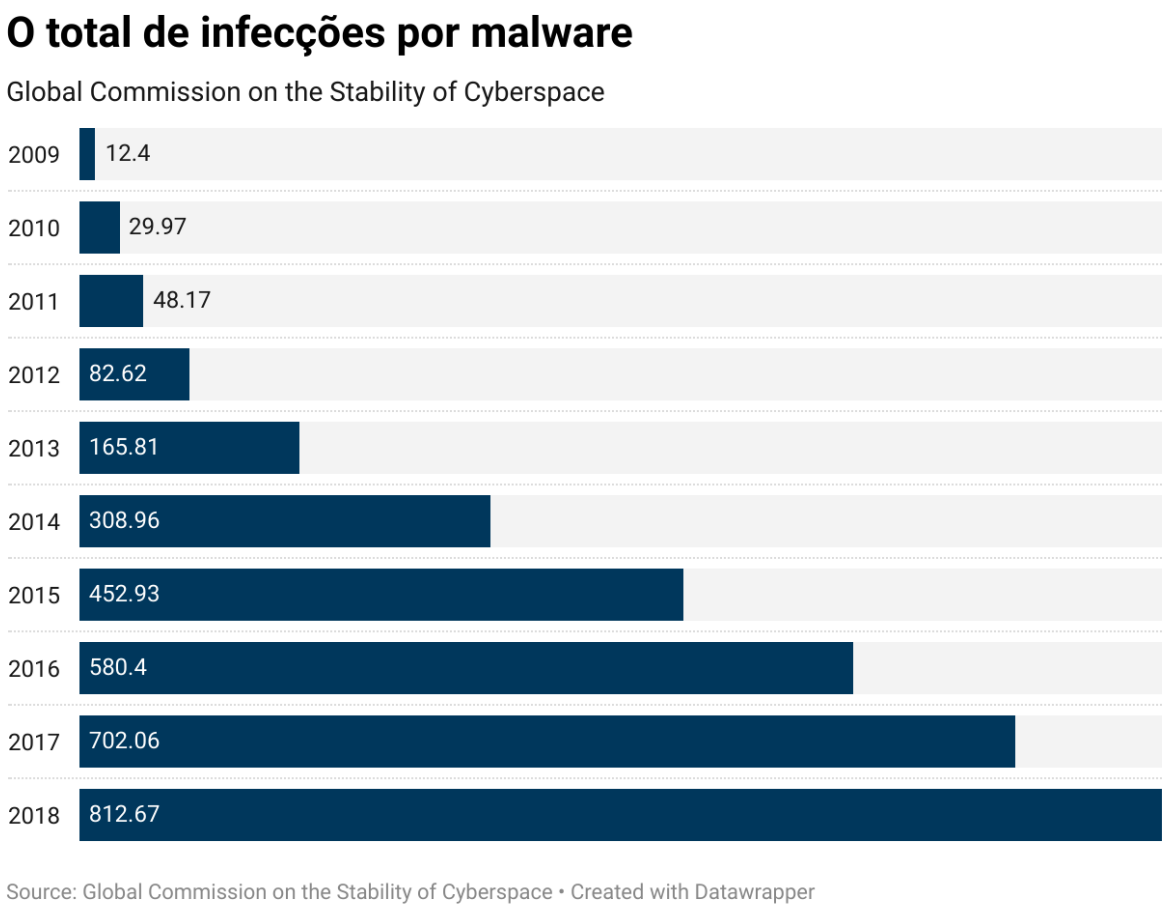
99% dos ataques cibernéticos dependem de engenharia social
43% dos profissionais de TI declararam que foram alvos de esquemas de engenharia social em 2020
21% dos funcionários atuais ou ex-funcionários usam a engenharia social para obter uma vantagem financeira, por vingança, por curiosidade ou por diversão
43% dos ataques de phishing / engenharia social visam pequenas empresas

14 https://www.acronis.com/en-us/articles/social-engineering/

Os golpes no Pix utilizam engenharia social e fizeram com que o Banco Central limitasse o valor das transações noturnas. Criminosos vão aonde o dinheiro está e com a alta adesão ao sistema — 206 milhões de chaves registradas menos de um ano após o lançamento — e a agilidade das transações tem servido aos criminosos. A vítima tem menos tempo para perceber o golpe e pode não conseguir cancelar a operação. Outro problema é que o Pix pode ser usado com QR Code. Os QR Codes são códigos de resposta rápida bidimensionais com uma URL embutida, ao escanear um QR Code os usuários estão clicando em link que não conseguem ver e pode ser phishing.

O relatório de segurança Check Point Research 2021[15], diz que o smartphone é um alvo e, de abril a setembro de 2021, 5,2% dos ataques cibernéticos no Brasil foram direcionados contra smartphones. A média global foi de 1,3%. O relatório alerta para a necessidade de aumentar os níveis de segurança nos QR Codes já que podem comprometer a confidencialidade dos dados pessoais.

15 https://www.checkpoint.com/pages/cyber-security-report-2021/



Os ataques mais comuns são de malware, aliás a palavra é abreviação de software malicioso — é uma aplicação que causa danos aos sistemas para roubar dados, obter acesso não autorizado às redes. A infecção por malwares é o tipo mais comum de ameaça cibernética e, é um termo que se refere a várias categorias de variantes de software malicioso, incluindo vírus, worms, trojans, entre outros.

Vírus é o malware mais comum, 92% é entregue por e-mail. Assim como seu nome biológico, os vírus se ligam a arquivos limpos, se replicam e se espalham para outros arquivos. Eles podem apagar arquivos, forçar reinicializações, unir máquinas a uma botnet, ou permitir acesso remoto a sistemas infectados por backdoor.

Worms são semelhantes aos vírus, mas sem a necessidade de um arquivo hospedeiro. Infectam sistemas diretamente e residem na memória, onde se auto-replicam e se espalham para outros sistemas na rede.

Backdoor é um método de contornar a autenticação ou criptografia normal e é usado para acessar remotamente sistemas infectados, ou para obter acesso não autorizado a informações privilegiadas. Alguns backdoors podem ser incorporados em hardware ou sistemas operacionais para fins legítimos, como restaurar o acesso a um usuário que esqueceu sua senha.

Trojans, o nome do famoso cavalo de madeira da história da Guerra de Tróia, se disfarça como uma aplicação legítima, ou simplesmente, se escondem em uma e dão acesso aos atores maliciosos aos sistemas infectados, muitas vezes permitindo o carregamento de outros malwares.

O ransomware também é uma forma de malware, embora mereça um foco especial devido ao conceito da computação ubíqua, termo que se refere à presença direta e constante da informática e tecnologia no dia a dia das pessoas, integrando totalmente o ser humano e a máquina. O ransomware foi projetado para criptografar dados e bloquear vítimas fora de seus sistemas até o pagamento de um resgate para restaurar o acesso.

16

Em alguns ataques, os atacantes extraem cópias dos dados da vítima e ameaça torná-los públicos se as exigências não forem atendidas, o que aumenta a pressão sobre as vítimas, pois os dados roubados muitas vezes contêm informações que identificam pessoalmente clientes e funcionários, detalhes financeiros sensíveis, ou segredos pessoais, comerciais, intelectuais e industriais. Ataques de ransomware, geralmente, dependem de técnicas de engenharia social e phishing de e-mails, em 98% dos casos são a principal forma de entrada no sistema. Outras formas de entrada são sites maliciosos, apps vulneráveis, links suspeitos em redes sociais e falsos pedidos de atualização de programas.

16 Imagen de pedido de resgate após ataque por ransomware em 2017 na Ucrânia

Uma vez no sistema, o ransomware encontra todos os arquivos de um tipo específico localmente e através da rede os criptografa. Os arquivos originais, pontos de recuperação e backups são excluídos para evitar que os usuários restaurem o sistema por conta própria. O ransomware normalmente muda a extensão do arquivo e adiciona um arquivo explicando como as vítimas podem pagar para recuperar seus dados.

Como se proteger
Evitar clicar em “avisos” que podem conter links maliciosos
Evitar abrir e-mails de desconhecidos e spam em geral
Jamais clicar em links cuja procedência é desconhecida
Instalar apenas programas de fontes confiáveis
Desconfiar de links e vídeos enviados por pessoas que não têm o perfil de enviar este tipo de conteúdo
Manter programas atualizados (inclusive antivírus)
Prever varreduras automáticas e periódicas de antivírus
Estar sempre com o backup atualizado e desconectado do computador

O phishing é uma técnica de ataque comum e é uma forma de engenharia social: a estratégia de manipular as pessoas para tomarem atitudes inseguras ou divulgarem informações sensíveis. Nas campanhas de phishing, os atacantes utilizam comunicações enganosas como e-mail, mensagens instantâneas, SMS e websites para personificar uma pessoa ou organização de

confiança, como uma empresa ou instituição governamental legítima. Aproveitando-se da confiança dos usuários, os atacantes os enganam ao clicar em links maliciosos e baixar anexos carregados de malware. Variantes do phishing nas corporações são os Business e-mail Compromise (BEC) e e-mail account compromise (EAC) fraude em que o invasor se apresenta como alguém em quem o destinatário deve confiar - normalmente um colega, chefe ou fornecedor. O remetente pede ao destinatário para fazer algo que seria indevido ou estranho pedir, mas que pelo elo de confiança o destinatário não estranha tanto (transferência eletrônica, alterar dados bancários para pagamentos futuros e assim por diante).[17]

Como se proteger
Não clicar em nenhum link sem pensar
Não responder a um e-mail suspeito de phishing
Se o e-mail/mensagem recebido é referente a algum serviço que de assinatura, entrar no site do serviço (sem usar qualquer link do e-mail) e verificar a situação
Não apagar um e-mail de phishing imediatamente, mas marcar o e-mail como “phishing”

O spear phishing utiliza e-mail, mas o foco é um pequeno grupo de indivíduos como funcionários de uma empresa. As mensagens são adaptadas com base

17 https://www.proofpoint.com/us/resources/white-papers/definitive-e-mail-security-strategy-guide

em conhecimento interno ou em informações disponíveis na web (por exemplo, das mídias sociais). Embora eles exigem um esforço extra para criar, os ataques de spear phishing tendem a ser bastante convincentes e têm mais chances de sucesso.

DDoS (Distributed Denial of Service), em português, ataques de negação de serviço distribuída é um tipo de ataque cibernético que deixa um site ou recurso de rede indisponível por causa de uma sobrecarga ou tráfego mal-intencionado, deixando-o inoperante.

Como identificar?
Quantidade suspeita de tráfego originária de um único endereço de IP ou de uma faixa de endereços IP
Grande tráfego de usuários com o mesmo perfil de comportamento, como tipo de dispositivo, geolocalização ou versão de navegador web
Aumento inexplicado de solicitações de uma mesma página
Padrões de tráfego incomuns, como picos em horários inusitados ou padrões que parecem artificiais (por ex., um pico a cada 10 minutos)

Dispositivos individuais nessas redes de segurança são chamados bots (ou zumbis) e vários deles são conhecidos como botnet. As botnets são usadas contra servidores ou redes, fazendo com que cada bot envie pedidos repetidos para o endereço IP do alvo. Isto acaba fazendo com que o servidor ou a segurança da rede fique sobrecarregada e indisponível ao tráfego normal.

A remediação é geralmente difícil, pois os bots são dispositivos legítimos da Internet — dificultando separar os atacantes dos usuários inócuos.

A prevenção passa por medidas como rotear para um black hole (rota nula), rate limiting (limitação do número de solicitações que um servidor aceitará por um período de tempo, firewall de aplicativos web (ferramenta capaz de ajudar a mitigar o ataque de DDoS na camada de aplicação). Há risco de perda de tráfego legítimo e as duas últimas medidas não são eficazes contra DDoS complexos.

Spoofing do verbo em inglês spoof (imitar, fingir), que em tecnologia da informação é um jargão usado para falsificação. Quando você recebe um e-mail estranho de um contato conhecido e confiável (pode ser um amigo, um familiar, uma empresa ou mesmo o seu banco), com todas as informações do cabeçalho aparentemente corretas (nome, endereço de e-mail, remetente, etc.) mas com um conteúdo estranho, pedindo para clicar em links encurtados e/ou enviar dados sensíveis, por exemplo, trata-se de um ataque spoofing[18]. A Clonagem de WhatsApp é um ataque de Spoofing e, segundo a PSafe, mais de 5 milhões de brasileiros já foram vítimas em 2020, em média 15 mil vítimas de spoofing por dia no Brasil.

Há vários tipos de spoofing:

Spoofing de ID: Um atacante faz uma requisição a um site ou servidor se passando por um IP legítimo, de forma que a vítima não consiga identificar o atacante. Não clique em qualquer link enviado, seja por e-mail, SMS ou através de apps de mensagens. É importante verificar o DNS do seu roteador e estar sempre atento ao endereço do site suspeito, que em geral difere em detalhes do legítimo.
Spoofing de e-mail: Um dos mais comuns, mira usuários e consiste em e-mails falsos, se passando por outra pessoa ou uma empresa real.

18 https://tecnoblog.net/299805/o-que-e-spoofing/

Geralmente ligado a golpes de phishing.
Spoofing de DNS: O hacker manipula as conexões de rede (alterando o DNS de roteadores em larga escala) e desvia acessos a um site legítimo para uma cópia falsa, de modo a roubar dados. Sites de bancos são os alvos mais comuns. Desconfie da natureza de pedidos de RG e CPF, além do número de cartão, senha e código de segurança. Os bancos não fazem isso.
Spoofing de chamadas e/ou SMS: O atacante faz chamadas ou envia mensagens SMS se passando por um número legítimo, tentando enganar outros usuários.

Como se proteger
Usar senhas fortes
Trocar de senhas regularmente
Ativar a verificação em duas etapas (de preferência, não usar o SMS ou o número de telefone como verificador)
Usar antivírus (atualizado)
Verificar o DNS do seu roteador e estar sempre atento ao endereço do site suspeito, que em geral difere em detalhes do legítimo (para Spoofing de DNS)

Outro ataque popular é conhecido como Man-in-the-Middle. Como o próprio nome sugere, o atacante “se coloca” entre duas partes que tentam se comunicar, quando o usuário entra no internet banking, nas contas de e-mail, intercepta mensagens enviadas e depois se passa por uma das partes envolvidas. O envio de contas e faturas falsas é um exemplo. Estes ataques são eficientes e difíceis de detectar.

A variante deste ataque é o Man-in-the-Browser, o agressor implementa um código malicioso no browser do computador da vítima e o malware silenciosamente grava informações. Ou usa um router WiFi para interceptar conversas de suas vítimas, uma situação comum, o agressor configura dispositivos wireless, para atuar como ponto de WiFi e o nomeia com um título comum em redes públicas. Quando um usuário se conecta ao “router” tem suas senhas roubadas.

A injeção SQL (SQLI) utiliza a linguagem padrão para a construção e manipulação de bancos de dados SQL (Structured Query Language) inserem código SQL malicioso em um servidor, manipulando-o para exibir informações de banco de dados que o atacante não tem autorização para acessar. Estas informações podem incluir dados corporativos sensíveis, credenciais de usuários e identificação pessoal de funcionários e clientes. A injeção SQL pode ser usada para atacar qualquer banco de dados baseado em SQL e visa principalmente os sites da web. Um ator malicioso poderia realizar um ataque simplesmente submetendo um comando SQL na caixa de busca de um site vulnerável, recuperando potencialmente todas as contas de usuário do aplicativo web, o mesmo acontece com Elastic Query mal configurada.

Doxxing pode envolver hacking, mas normalmente o ato é realizado por meios legais, há muitas informações sobre as pessoas expostas na internet, basta dar um Google para achar. O termo doxxing é a abreviação de “droping documents”, expressão que pode ser traduzida como liberação de documentos ou a publicização de documentos privados de alguém.

A ação é comum em círculos de hacktivismo para expor autores de crimes ou políticos corruptos, por exemplo, mas é comumente utilizada como forma de assédio na web, propagação de discurso de ódio e perseguição. Jornalistas, professores e outros atores da sociedade civil podem ser alvos de doxxing por fazerem seus trabalhos ou simplesmente por se manifestarem.

Como se proteger[19]
Limitar as informações pessoais disponíveis online.Remova todos os endereços, locais de trabalho e locais específicos de suas contas. Certifique-se de que seus perfis, nomes de usuário / identificadores sejam mantidos privados
Usar uma VPN (virtual private network) para proteger seu IP, se usar wi-fi público, desative a funcionalidade de compartilhamento de rede pública em seu dispositivo
Evitar responder quizzes online (muitas vezes eles perguntam por informações “inofensivas” e mapeiam preferências
Requerer remoção de informações pessoais do Google (uma pessoa pode requisitar que suas informações saiam dos mecanismos de busca e outras plataformas / redes sociais)

A controvérsia dos proxies

O uso de proxy vem sendo discutida como uma das políticas de dissuasão contra o crime cibernético pela Comissão Global de Estabilidade do Ciberespaço (Global Commission on the Stability of Cyberspace) que desencoraja seu uso de pelo anonimato e falta de rastreabilidade, permitindo

19 https://ethics.berkeley.edu/privacy/protect-yourself-doxxing

que indivíduos e máquinas se conectem a dados e sistemas sem declarar identidade e aproveitar para cometer crimes cibernéticos com impunidade. A GCSC quer que os países sejam responsabilizados financeiramente por ataques cibernéticos feitos em seu território, independentemente de saberem de tal atividade antes que ela ocorra. Essa responsabilização aumentaria a pressão internacional e multissetorial para reduzir o uso de proxies pelo impacto econômico que traria.
Dados da empresa de consultoria alemã Roland Berger, prevê que o prejuízo das empresas em todo mundo com crimes cibernéticos em 2021 deve ser três vezes o valor do Produto Interno Bruto (PIB) brasileiro — US $6 trilhões. O Brasil ocupa o 5.º lugar com mais registros de ataques hackers contra empresas, atrás apenas dos Estados Unidos, Reino Unido, Alemanha e África do Sul.

Os Estados Unidos sofreram 18,2% de todos os ataques de ransomware do mundo, segundo a Symantec.

O relatório da Kaspersky “Panorama de Ameaças na América Latina” (set/2020) apontou em média 5 mil tentativas de ataque com ransomware por dia, quase metade (46,7%) era contra alvos no Brasil.

A estimativa do prejuízo que os ataques de ransomware causaram em 2020 e 2021 é alta e subnotificada. Uma pesquisa da Keeper Security[20] com mais de 2000 profissionais estadunidenses aponta que 49% das organizações que sofreram ataque de ransomware pagaram o resgate e 22% não divulgaram essas informações. O que significa que a porcentagem de empresas que pagam resgates pode ser maior do que se pensa e os prejuízos também.

20 https://www.keepersecurity.com

Dado significativo da pesquisa aponta que 29% dos funcionários entrevistados disseram que não estavam familiarizados com o ransomware até ser vítima. É bom lembrar que ataques de ransomware são desencadeados por um e-mail de phishing.

“É importante compartilhar informações que ajudem a corrigir vulnerabilidades de segurança ou ajudem a prevenir, limitar ou mitigar um ataque", recomenda a Global Commission on the Stability of Cyberspace, a não notificação de vulnerabilidades e ataques é que as falhas podem afetar vários produtos e serviços de diferentes produtores e em diferentes ambientes. Corrigir um produto sem revelar a vulnerabilidade subjacente a outros pode proteger esse produto, mas não proteger a estabilidade do ciberespaço. Produtos e serviços bem projetados e construídos, bem gerenciados por profissionais de TI e usuários de computador aumentarão a segurança, mas mesmo o melhor desenvolvimento e operações não serão suficientes, um invasor persistente pode derrotar as medidas de segurança. É importante focar não apenas na tecnologia, mas nos comportamentos dos países e das pessoas. Medidas de prevenção de segurança cibernética são diferentes para cada tipo de ataque, boas práticas de segurança e higiene básica de TI que incluem práticas de codificação seguras, manter sistemas e software de segurança atualizados, aproveitar firewalls e ferramentas e soluções de gerenciamento de ameaças, instalar software antivírus em sistemas, controlar acesso e privilégios de usuário, sistemas de backup frequentementes, e caçar proativamente ameaças desconhecidas (riscos, vulnerabilidades, etc.).

3

Criptografia

Desde o surgimento da humanidade sempre houve a necessidade e o desejo de manter conversas em segurança e com privacidade.

A máquina Enigma (Foto: Thiago Tanji)

Criptografia (palavra derivada do grego kryptós, escondido e gráphein – escrita) é a arte ou a ciência de escrever em cifra ou em código para tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e a compreenda. Mensagens criptográficas envolvem conjuntos de valores matemáticos para cifrar dados e ocultá-los promovendo o embaralhamento ou a inserção de códigos ou cifras entre as palavras para não permitir sua leitura caso sejam interceptadas. A chave criptográfica é uma informação usada para controlar o funcionamento de uma cifra de modo que apenas quem detém essa informação pode decifrar o texto criptografado.

A criptografia antecede em muito a era tecnológica, desde o início dos tempos o ser humano sempre teve preocupação em manter e promover o envio de mensagens de forma secreta, seja por interesse político, guerras ou poder.

A criptografia protege dados sigilosos, promove o tráfego de mensagens com segurança, mantém sigilo de informações e guarda documentos importantes. A técnica é utilizada desde a Antiguidade, o relato mais antigo de que se tem conhecimento é do Egito há cerca de 4.000 anos e, posteriormente, na Mesopotâmia, Grécia e Roma.[21] Em 100 a.C, Júlio César usava uma forma de criptografia para transmitir mensagens secretas a seus generais do exército na frente de guerra. A cifra de substituição, conhecida como cifra de César, era o um deslocamento de 3 cifras, cada caractere era deslocado em 3 lugares, o caractere 'A' era substituído por 'D', 'B' foi substituído por 'E' e assim por diante. Outro registro da criptografia remota aos anos 450 a.C., os militares gregos faziam uso do bastão de Licurgo ou Scytale, uma técnica de criptografia que utilizava uma mensagem escrita em uma tira de couro sobre um bastão de largura definida, apenas o destinatário que possuía um bastão do mesmo tamanho conseguia ler a mensagem.

21 https://jornal.usp.br/artigos/criptografia-de-arma-de-guerra-a-pilar-da-sociedade-moderna/

22

Os métodos para preservar as comunicações evoluíram com o passar dos séculos e, em 1918, o engenheiro alemão Arthur Scherbius patenteou a Enigma, a máquina capaz de encriptar informações de modo avançado para os padrões da época. Composta de 26 teclas do alfabeto romano, quando uma letra é pressionada, por exemplo, “A” poderia se transformar em “Z” com a criptografia. O segredo para que as combinações se tornassem quase impossíveis de ser quebradas estava na composição de três rotores do equipamento, conjunto de fios que serviam para alterar as posições das letras. Na II Grande Guerra Mundial o exército nazista avançou por vários países sem serem detido graças a Enigma.

Diariamente os alemães alteravam a ordem dos rotores e as informações modificadas eram transmitidas via rádio, as mensagens chegavam a outro operador da Enigma, que tinha as mesmas posições definidas que o remetente. Mesmo que as Forças Aliadas interceptassem o sinal de rádio, a mensagem não fazia sentido. Para complicar, estima-se que existiam ao menos 1.054.560 combinações diferentes possíveis de serem realizadas com a Enigma. Durante o esforço de guerra, os britânicos convocaram centenas de cientistas que deveriam criar uma tecnologia capaz de superar as comunicações nazistas e coube ao matemático, cientista da computação e criptoanalista Alan Turing (1912–1954) chefiar a equipe responsável por criar o modelo computacional que é a base das máquinas que usamos ainda hoje. A máquina inventada por Alan Turing ficou pronta em 1943 e desempenhou um papel importante que permitiu aos Aliados derrotar os nazistas. A criptografia desenvolvida pelos alemães foi desvendada por conta de erros como usar senhas fáceis e reutilizar as mesmas senhas. Turing identificou que uma letra nunca era cifrada como ela própria, graças à automação computacional foi possível realizar comparações de mensagens similares, boletins de tempo e textos longos para diminuir as possibilidades de combinações, calcular probabilidades até que conseguiam decifrar as mensagens em poucos segundos. A conquista de Turing e dos cientistas da equipe encurtou a guerra em pelo menos dois anos. A vida de Alan Turing e esse período histórico é contado no filme O Jogo da Imitação(2014)[23].

Criptowars

No pós Segunda Guerra Mundial até a década de 1970 o uso de criptografia era quase inteiramente militar e um monopólio do estado. Em 1973, o Nation Bureau of Standards (agora chamado NIST) nos Estados Unidos fez um

23 https://www.imdb.com/title/tt2084970/?ref_=ttpl_pl_tt

pedido de propostas para uma cifra de bloco que se tornaria um padrão nacional. A cifra escolhida foi desenvolvida pela equipe de Horst-Feistel da IBM e foi chamada Lúcifer. Foi a escolhida pelo governo e rebatizada de DES ou Data Encryption Standard. Nos anos seguintes, o DES foi quebrado, o principal problema era o tamanho pequeno da chave de criptografia. À medida que o poder de computação aumentou, tornou-se fácil forçar todas as diferentes combinações da chave para obter uma possível mensagem de texto simples.

Ao tempo programadores independentes passaram a desenvolver sistemas de criptografia. Em 1976 foi desenvolvido um método de distribuição de chaves, o método Diffie-Hellman, capaz de permitir a criação de diversos sistemas sem que ninguém além do remetente e destinatário conseguissem acessar o conteúdo, nem mesmo o provedor. O método de criptografia assimétrica garante o sigilo necessário para transações comerciais e bancárias pela internet. O modelo usa pares de chaves criptográficas para aumentar a segurança durante a troca de informações: uma chave pública, que pode ser amplamente disseminada, e uma chave privada conhecida apenas pelo seu detentor. As chaves são diferentes, uma é utilizada para cifrar a mensagem e a outra para decifrá-la.

Até o início dos anos 1990, os regulamentos de exportação do governo dos Estados Unidos não permitiam a exportação de sistemas de criptografia. Para derrubar as restrições à criptografia e as tentativas dos governos de controlá-la, programadores ativistas criaram o movimento cypherpunk.

A palavra é a junção dos termos: Cipher(escrita cifrada) e punk, grupo de ativistas ligados a noções como antiautoritarismo, pensamento livre e revolução, grupos que lutavam pela privacidade e pela utilização de criptografia contra o vigilantismo do governo e das grandes corporações, para eles:

O governo não deve ser capaz de espionar as atividades das pessoas
É considerado um direito básico a proteção de conversas e negociações entre as pessoas.
Esses direitos podem ser assegurados não somente pelas leis, mas também pela tecnologia.
O poder da tecnologia, muitas vezes, cria novas realidades políticas.

A pressão contra o controle da criptografia se intensificou na década de 1990 com a introdução do computador pessoal, do surgimento do comércio eletrônico e quando o ciberativista Philip Zimmermann criou o PGP(Pretty Good Privacy), uma ferramenta usada até hoje para criptografar. O código foi disponibilizado na internet em 1991, gratuitamente e para todos que quisessem usar. Detalhe curioso é que Zimmermann publicou seu código fonte em um livro, pois sabia que a legislação dos EUA garantia a liberdade de expressão para materiais impressos.
O PGP é um software que fornece autenticação e privacidade criptografica para comunicação de dados e é utilizado para assinar, encriptar e descriptografar textos, e-mails, arquivos, diretórios e partições inteiras de disco e para aumentar a segurança de comunicações via e-mail. A encriptação do PGP usa uma combinação serial de hashing, compressão de dados e criptografia assimétrica. Pouco depois, a Netscape desenvolveu a tecnologia SSL, amplamente adotada como um método para a proteção de transações de cartão de crédito que usavam criptografia de chave pública.

Apenas no ano 2000 foram implementadas regras para simplificar a exportação de programas proprietários e de código aberto de criptografia, após um embate pelo direito à privacidade que chegou à Suprema Corte estadunidense em 1999. De um lado, o governo dos Estados Unidos e países aliados se esforçando sistematicamente para enfraquecer e sabotar a criptografia disponível comercialmente usada por indivíduos e empresas mundo afora e ameaçando instalar backdoors como entradas especiais para atividades investigativas ou implementação de sistemas de chave-reserva. Do outro lado, ativistas de direitos humanos afirmam que a criptografia é essencial para a proteção da privacidade, liberdade de expressão e associação. A Suprema Corte determinou que a criptografia não pode ser controlada por entidades, por ser uma garantia da liberdade de expressão.

A segunda fase da criptowar, ficou conhecida como going dark (em tradução livre, fique no escuro) envolveu um embate entre o FBI e a Apple em 2015. Um ano antes, a Apple criou uma criptografia individual para cada aparelho e o usuário deve criar uma senha de quatro ou mais dígitos para desbloquear o smartphone. A codificação é armazenada no próprio dispositivo e a empresa não tem acesso a essa senha. Assim, se recusou a cumprir ordens judiciais e quebrar a criptografia do iPhone pertencente ao atirador de San Bernardino, Califórnia, alegando não ter como desbloquear o aparelho.

No Brasil já houve disputas judiciais envolvendo o Whatsapp e a Polícia Federal, em dezembro de 2015, o aplicativo chegou a ficar 13 horas fora do ar, após decisão judicial que ordenava que as operadoras de celulares do Brasil suspendessem o acesso ao WhatsApp. O bloqueio e uma multa milionária foi uma retaliação a ordem judicial que obrigava o Facebook (agora Meta), controlador do WhatsApp, para que entregasse dados e históricos de conversas de pessoas investigadas de um caso de latrocínio e tráfico de drogas ocorrido em 2013.

Em 2018, novamente a Polícia Federal solicitou que se entregasse os números de telefone celular utilizados para disparar conteúdos em massa sobre o processo eleitoral brasileiro e o WhatsApp removeu o acesso de contas vinculadas aos disparos em massa no aplicativo. A eleição presidencial de 2018 com desinformação e disparos em massa motivou o WhatsApp a limitar o encaminhamento de mensagens para apenas cinco conversas por vez, reduzindo o encaminhamento em mais de 25%. Mensagens encaminhadas frequentemente tem limites mais rígidos. Essas mensagens são identificadas com uma etiqueta de setas duplas para indicar que elas não foram criadas por quem as enviou e podem ser encaminhadas para apenas uma conversa por vez. Essa medida reduziu a viralização desse tipo de mensagens em mais de 70%.[24] Para Carlos Liguori, coordenador de projetos e pesquisador do Centro de Ensino e Pesquisa em Inovação da FGV Direito São Paulo, qualquer tipo de acesso excepcional a sistemas criptográficos é prejudicial à privacidade e à liberdade de expressão[25]. "Há tentativas de soluções regulatórias em diferentes países, como a proibição de criptografia, a licença governamental para fornecer criptografia, a obrigação de uma assistência para tecnologia e o estímulo ao desenvolvimento de sistemas criptográficos na forma de políticas públicas. Mas qualquer mecanismo que busque limitar ou fragilizar o uso da criptografia significa uma ameaça para a privacidade e liberdade de expressão no mundo digital." Para Liguori, as autoridades judiciais não estão no escuro e há alternativas para o acesso a conteúdos em consonância com as normas jurídicas. Além da quebra da criptografia, o pesquisador cita o uso da nuvem para investigações com possíveis dificuldades quanto a jurisdição ou a uma nuvem encriptada, o uso de metadados também seria uma alternativa, porém esses podem ser bastante invasivos à privacidade e, por fim, o hackeamento governamental dentro de

24 https://faq.whatsapp.com/general/security-and-privacy/about-whatsapp-and-elections/?lang=pt_br
25https://lapin.org.br/2020/09/04/relatorio-do-webinario-privacidade-nao-hackeada-como-a-criptografia-protege-seus-dados/

um escopo limitado e medidas de transparência e devido processo para acesso aos dados pessoais.

Criptografia para se adequar a LGPD

A criptografia é relevante para garantir a proteção de dados, uma boa prática a ser seguida pelas empresas e pela administração pública que deveriam aplicar conceitos de privacidade por design, isto é, desenvolver plataformas e aplicativos que colocariam temas de privacidade desde a concepção da tecnologia e a implementação de criptografia.
Além disso, é uma forma de cumprir a LGPD por garantir que as informações do sistema de um computador não sejam roubadas e lidas por alguém que deseja usá-las para fins maliciosos. Criptografar interações e comunicações é uma forma de manter os dados pessoais seguros e protegidos. Com isso, um possível vazamento de dados teria efeitos menores quando criptografados, já que não haveria acesso à informação sem a chave de acesso. A criptografia é adequada à Lei Geral de Proteção de Dados(LGPD), sendo um mecanismo que gera mais confiança entre os diferentes atores e pode ser considerada um direito fundamental do usuário na internet já que as formas de comunicação e de expressão da personalidade dos indivíduos também estão no mundo digital.

> A criptografia é necessária para que haja maior privacidade, proteção de dados e liberdade de expressão dos cidadãos[26].

26https://lapin.org.br/2020/09/04/relatorio-do-webinario-privacidade-nao-hackeada-como-a-criptografia-protege-seus-dados/

Para a segurança cibernética a criptografia é um elemento fundamental da segurança de dados e usada por indivíduos e grandes corporações para proteger as informações dos usuários enviadas entre um navegador e um servidor. Quaisquer informações, desde dados de pagamento até informações pessoais. Os softwares de criptografia para a proteção de dados pessoais tem sistema de criptografia forte, teoricamente, mais difícil de ser desvendado já que demandaria dos atacantes muito tempo e grande capacidade de processamento para ser bem sucedido. Quanto mais complexa for a chave criptográfica, mais segura será a criptografia, pois é menos provável que terceiros descriptografar por meio de ataques de força bruta, ou seja, tentativa e erro de números aleatórios até que a combinação correta seja encontrada.

Técnicas mais comuns

Os dois métodos mais comuns são a criptografia simétrica e assimétrica.
A criptografia simétrica também conhecida como criptografia de chave privada é considerada a mais simples porque envolve a utilização de uma única chave usada pelo codificador e decodificador. É uma boa opção para usuários individuais e sistemas fechados, caso contrário a chave deve ser enviada ao destinatário, a troca constante das chaves para autenticação tem o risco de interceptação durante a transmissão. Também é um método mais rápido do que o assimétrico.
Chaves de criptografia assimétrica usam duas chaves diferentes, uma pública e uma privada, que são vinculadas matematicamente. Essencialmente, as chaves são apenas grandes números que foram emparelhados um ao outro, mas não são idênticos, daí o termo assimétrico. A chave privada é mantida em segredo pelo usuário, e a chave pública pode ser compartilhada entre destinatários autorizados ou disponibilizada ao público em geral. Os dados criptografados

com a chave pública do destinatário só podem ser descriptografados com a chave privada correspondente.

Algoritmos de criptografia são desenvolvidos para diferentes objetivos, entre os mais conhecidos:

- DES - Data Encryption Standard é um algoritmo de criptografía de chave simétrica. Ela trabalha com blocos de 64 bits com chaves também de 64 bits, embora a chave real seja de 56 bits, já que 8 desses bits são redundantes. Assim, são possíveis 256 chaves diferentes, algo como 1016 chaves. O DES é atualmente considerado inseguro para muitas aplicações por causa de uma pequena chave de 56 bits. Recentemente o DES foi substituído pelo AES.
- Criptografía 3DES - Triple Data Encryption Standard, algoritmo de chave simétrica e os dados passam pelo algoritmo DES três vezes durante o processo de criptografia. O Triple DES está sendo lentamente substituído, mas continua sendo uma solução de criptografia de hardware confiável para serviços financeiros e outros setores.
- Criptografia AES - Advanced Encryption Standard é comumente usada de várias maneiras, incluindo segurança sem fio, segurança do processador, criptografia de arquivo e SSL / TLS. É o algoritmo usado em aplicativos de mensagens, como o Signal ou WhatsApp e o programa de compactação de arquivos WinZip.
- Criptografia RSA - O primeiro algoritmo de criptografia assimétrica amplamente disponibilizado ao público e é popular devido ao tamanho da sua chave e amplamente utilizado para transmissão segura de dados . RSA significa Rivest, Shamir e Adleman, os sobrenomes dos matemáticos que descreveram o algoritmo de criptografia assimétrica por usar um par de chaves.

- Criptografia Twofish - Usado tanto em hardware quanto em software, o Twofish é considerado um dos mais rápidos do seu tipo é um programa gratuito e disponível gratuitamente para quem quiser usá-lo.
- Criptografia RC4 - É usado em WEP e WPA que são protocolos de criptografia comumente usados em roteadores sem fio e usa criptografia simétrica

Além dos algoritmos de criptografia, há um conjunto de orientações internacionais para verificar se demandas de segurança do produto resistem a uma análise, conhecidos como Critérios Comuns (CC). As orientações foram criadas para oferecer supervisão de produtos de segurança de fornecedores neutros e terceiros. Os produtos são enviados para análise voluntariamente por fornecedores e funcionalidades testadas de acordo com um conjunto definido de padrões por tipo de produto.

As soluções de criptografia de dados são projetadas para dados em repouso, na nuvem, ou em trânsito.

- Criptografia de dados em trânsito se movendo entre dispositivos, em redes privadas ou na web estão expostos a um maior risco devido às vulnerabilidades do método de transferência e a necessidade de serem criptografados antes da transferência. A criptografia de dados durante a transferência é referida como criptografia de ponta a ponta, garantindo que mesmo se os dados forem interceptados, a privacidade é protegida.
- Criptografia de dados em repouso estão em um dispositivo de armazenamento de dados e não estão sendo ativamente usados ou transferidos. Normalmente, os dados em repouso são menos vulneráveis do que quando estão em trânsito, já que os recursos de segurança do dispositivo restringem o acesso, mas não são imunes, geralmente,

contêm informações mais valiosas, por isso são um alvo mais atraente para atores maliciosos

A criptografia de dados em repouso reduz as oportunidades de roubo de dados de dispositivos perdidos ou roubados, compartilhamento inadvertido de senha ou concessão acidental de permissão. Ela aumenta o tempo necessário para acessar informações e dá um tempo valioso para o proprietário dos dados descobrir perda de dados, ataques de ransomware, dados apagados remotamente ou credenciais alteradas.

Os dados em repouso são protegidos por intermédio do Transparent Data Encryption, uma tecnologia usada pela Microsoft, Oracle e IBM para criptografar arquivos de banco de dados. A TDE protege dados em repouso, criptografando bancos de dados no disco rígido e, consequentemente, em mídias de backup, mas não protege dados em trânsito.

Dados criptografados de ponta a ponta se referem a sistemas em que somente dois usuários se comunicam, ambos possuem chaves e podem descriptografar a conversa. Até mesmo o provedor de serviços não pode acessar os dados criptografados de ponta a ponta.

A criptografia ajuda a manter a integridade dos dados de atacantes que podem roubar informações ou alterar dados para cometer fraudes. Embora atacantes habilidosos consigam alterar dados criptografados, os destinatários conseguem detectar a intrusão e dar uma resposta mais rápida. A criptografia ajuda as organizações a atender a padrões normativos, a cumprir as regulamentações e garantir a conformidade em setores como serviços financeiros ou serviços de saúde que possuem regulamentações rigorosas sobre como os dados do consumidor são usados e armazenados.

A criptografia protege quem usa vários dispositivos e transfere dados entre eles mesmo durante a transferência, por exemplo, ao mover dados para armazenamento em nuvem. Lógico que a segurança na nuvem é essencial e o armazenamento criptografado ajuda a manter a privacidade desses dados, mas

os usuários devem garantir a criptografia em trânsito, enquanto são usados e no armazenamento. Especialmente no pós a pandemia, muitas empresas foram para o home office, outras já tinham profissionais espalhados por diferentes lugares e isso representa riscos à segurança, pois os dados estão sendo acessados de vários locais diferentes. A criptografia ajuda a proteger contra roubo ou perda acidental de dados.
A criptografia protege a propriedade intelectual e o gerenciamento de direitos digitais quando criptografam os dados em repouso para evitar a engenharia reversa e o uso ou a reprodução não autorizados de material protegido por direitos autorais.
A criptografia pode e deve ser usada para apagar dados. Como as informações excluídas podem ser recuperadas usando ferramentas de recuperação de dados, se forem criptografados antes de serem excluídos, basta jogar fora a chave, a única coisa recuperável será o texto cifrado e não os dados originais.

O direito à privacidade

O livro 1984, de George Orwell, escrito entre 1947 e 1948, no pós II Guerra Mundial, retrata uma sociedade governada por um governo totalitário, que controla os pensamentos, bem como todos os dados, imagens e sons dos cidadãos. O protagonista, Winston Smith, trabalha no Ministério da Verdade, setor responsável por alterar a história a seu bel prazer e moldar a narrativa geral em favor da ditadura vigente. Esta última frase traz alguma lembrança? O livro entrou em domínio público e, só no Brasil, foi relançado por 14 editoras. Também figurou nas listas de best-sellers mais vendidos nos EUA logo após Donald Trump tomar posse como presidente e, no Brasil, em 2020 foi o livro mais vendido na categoria ficção. Uma explicação para o longevo sucesso do livro é o medo e a preocupação que os indivíduos têm em relação a própria privacidade e da liberdade de exercer pleno controle sobre suas

informações mais íntimas, bem como o direito de escolher como e para quem quer transmiti-las. O direito à proteção da privacidade é inerente ao direito à autodeterminação individual e nesse direito fundamental está implícito o direito à proteção dos dados, também previsto genérica e implicitamente no artigo 12 da Declaração Universal de Direitos Humanos da ONU(Organização das Nações Unidas), de 1948 que trata do princípio da dignidade humana. Por fim, contemplada no artigo quinto da Constituição Federal do Brasil, de 1988.

> O indivíduo deve ter o controle sobre suas informações. E deve exercer esse controle com base nos seus interesses e valores

Uma vez que o usuário aceita a política de utilização de um site, a obtenção desses dados são juridicamente legais, mas com a LGPD agora é lei que as empresas que coletam dados informem aos usuários o que será feito com eles, se serão compartilhados com outras empresas, vendidos ou se serão apagados do banco de dados depois de um determinado período ou não.
Além das informações que estão disponíveis publicamente na internet, existe outro mercado em que esses dados são comercializados de forma ilícita. Em reportagem da Folha de São Paulo[27] o jornal mostrou que páginas reúnem em painéis cadastros vazados do CadSUS, da Senatran (Secretaria Nacional de Trânsito), da Receita Federal, do INSS (Instituto Nacional de Segurança Social), da Boa Vista - empresa privada de informações de crédito que administra um banco de dados que reúne informações comerciais e cadastrais de mais de 130 milhões de empresas e consumidores com abrangência nacional - e do Sinarm (Sistema Nacional de Armas), da Polícia Federal.

27https://www1.folha.uol.com.br/cotidiano/2021/12/criminosos-vendem-por-r-200-acesso-a-dados-completos-de-milhoes-de-brasileiros.shtml

Os sites encontrados pela reportagem não estão na deep web, mas na chamada surface web, a camada da internet em que os conteúdos podem ser encontrados com facilidade por qualquer usuário, nesse caso as conversas foram no Facebook, para acessar basta pagar cerca de R$ 200/mês para obter login e senha. Os dados disponíveis incluem nome completo, endereço, CPF, RG, nome dos pais e irmãos e até dos vizinhos, renda aproximada, foto, CNH e benefícios sociais, entre outros. As informações permitem o cruzamento dos dados e as buscas podem ser qualquer informação que o criminoso tenha sobre uma pessoa, seja o CPF, nome completo, a empresa em que trabalha.
Os vazamentos criam riscos consideráveis para as pessoas que vão desde fraudes bancárias ou práticas como perseguição, coação e extorsão.
Mas não só a população “civil” corre risco: as bases permitem saber quem faz parte das forças policiais, onde mora, dados de familiares, etc. Os dados vazados da Polícia Federal pertencem ao Sinarm, o registro de armamentos vinculados ao CPF facilitando furto, roubo e desvio de armas de fogo.
Os vendedores disseram à reportagem que puxam os dados por meio de logins de funcionários dos órgãos públicos, gerando acessos indevidos nos sistemas das instituições.
O Estado, como maior repositório de dados pessoais, deveria em primeiro lugar colocar todas as barreiras necessárias a esses dados tratá-los com anonimização e criptografia e limitar o acesso dos funcionários, mas segurança da informação não é uma preocupação, tanto que muitos sites .gov nem usam o protocolo de transferência de hipertexto seguro (https).
Tanto os que vendem os acessos como os que compram, podem ser acusados com base nos artigos 153 e 154 do Código Penal que tratam da divulgação de conteúdo particular e invasão de dispositivos digitais.

> As informações pessoais são qualquer coisa que possa ser usado para identificar o indivíduo, não se limitando a, mas incluindo nome, endereço, data de nascimento, documentos, IP, informação de crédito e seus gostos pessoais.

No manifesto do movimento cypherpunk, o matemático Eric Hughes, que junto com Timothy C. May e John Gilmore foram os articuladores da comunidade, escreveu que: “A privacidade em uma sociedade aberta também exige criptografia. Não podemos esperar que os governos, empresas ou outras grandes corporações sem rosto nos conceda a privacidade por caridade, assim cabe aos usuários defender o anonimato e a privacidade por si sós.”
O argumento mais falacioso usado por pessoas que não se preocupam com a segurança de seus dados pessoais é: — “Não tenho nada a esconder.” O vigilantismo não as afeta ou incomoda, mas dados pessoais são compartilhados entre empresas, por serviços de marketing abusivos. Você dá seu CPF para ganhar descontos na farmácia ou ganhar pontos e prêmios em programas de fidelidade de supermercados. Nada impede que seus dados de compras de supermercado sejam compartilhados com companhias de seguro, por exemplo, e que a franquia de seguro do seu carro aumente por estar comprando muitas bebidas alcoólicas no supermercado. Ou seus dados de saúde sejam usados por empresas que podem não lhe contratar por conta dos medicamentos que você toma.

Não existe mais anonimato

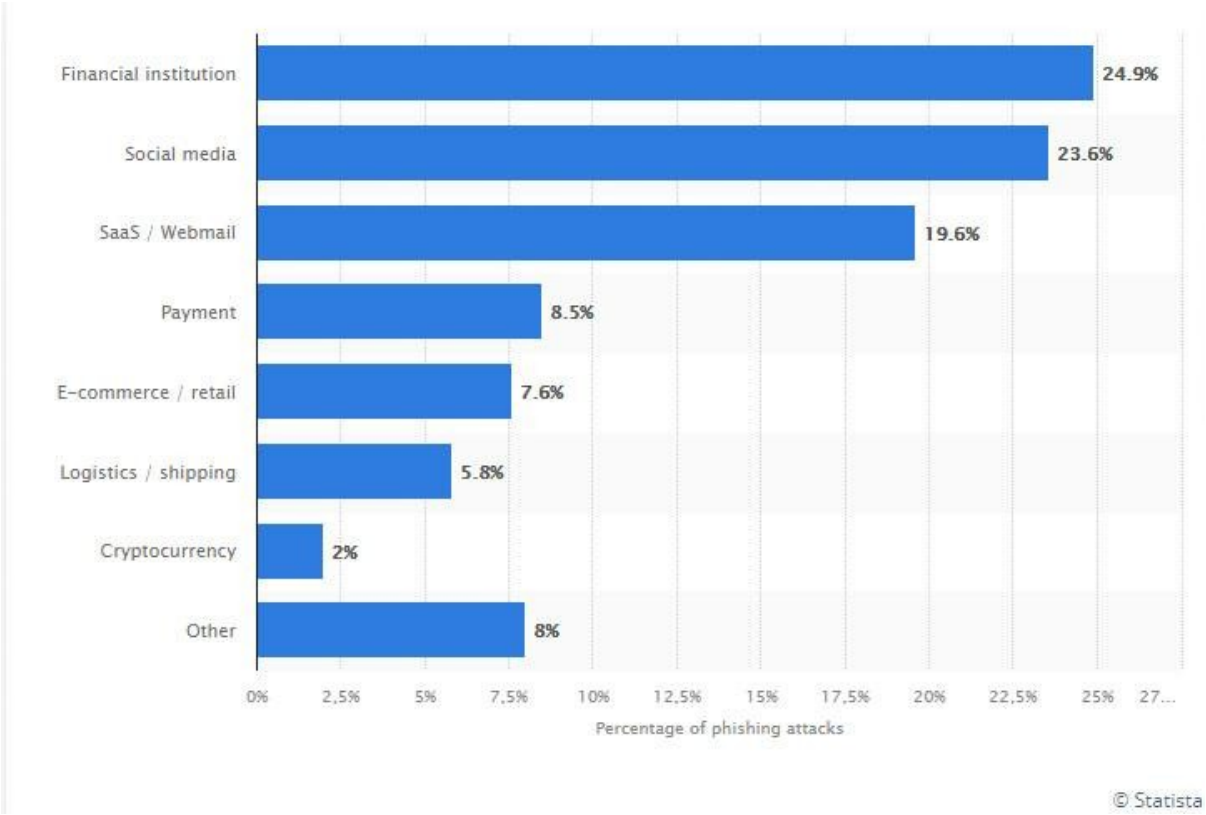
Há alternativas além da criptografia, a rede TOR um browser de internet possibilita que pessoas possam navegar na internet de maneira anônima e segura, preservando assim sua privacidade. O TOR foi elaborado pelos matemáticos Michael R. Reed e David Goldschlag (1996) do Laboratório de Pesquisa Naval dos Estados Unidos, em 1997 a "*onion routing*" foi efetivamente desenvolvido pela DARPA. A primeira versão do navegador TOR foi lançada em 2002, e dois anos depois, o Laboratório de Pesquisa Naval dos Estados Unidos liberou o código sob licença livre. Atualmente, o "*The TOR Project" é financiado pelo* Google, Universidade de Princeton, Universidade de Minnesota, Drexel University, Human Rights Watch, Reddit entre outros. O objetivo de sua criação foi a necessidade de se esconder o tráfego dos dados na internet, possível através dos cabeçalhos que eles possuem, onde contém informações como a origem e o destino dos pacotes de dados. A arquitetura que esconde essas informações de roteamento é conhecida como *Onion Routing* por se basear na construção de várias camadas de circuitos virtuais, bidirecionais, anônimos e criptografados, para dificultar a análise do tráfego das informações. Qualquer pessoa pode usar o TOR para navegação, protegendo sua privacidade, seja dos serviços de marketing abusivos ou de eventuais roubos de dados fornecidos via internet.
Outro lado da moeda, é a utilização por criminosos que buscam o mesmo anonimato na internet como uma maneira de se esconder da lei, o mesmo argumento usado contra a criptografia.

4

Novo normal

"Este não é um fenômeno de curto prazo. É um problema de longo prazo ... este é o novo mundo em que vivemos."

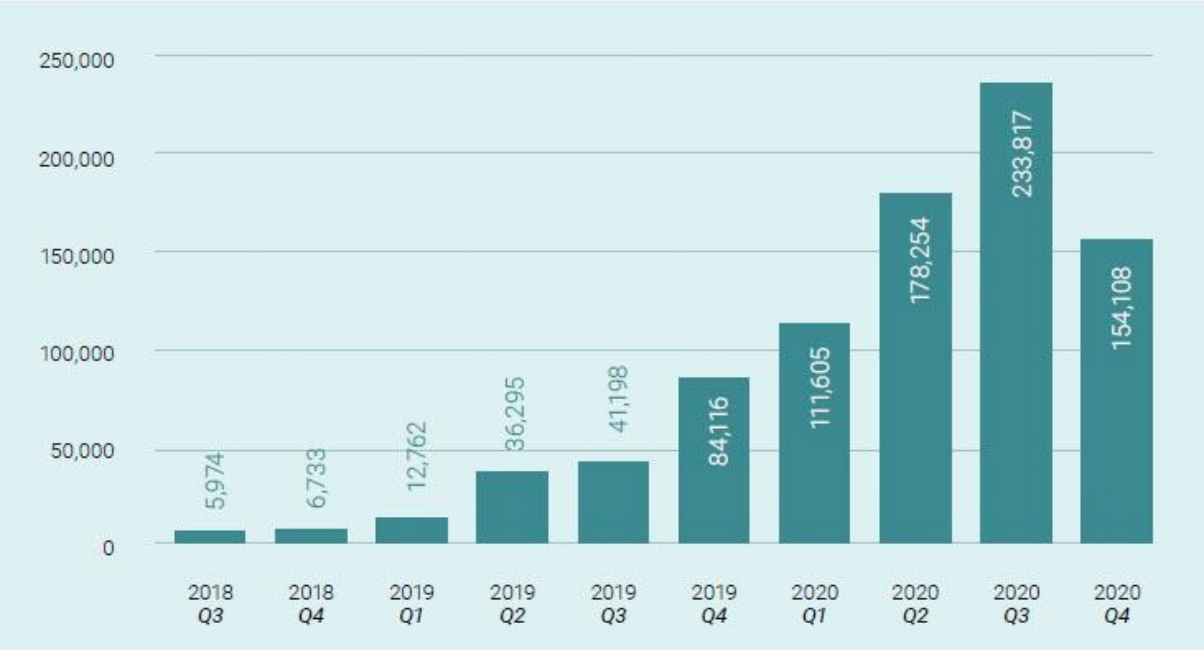
A frase é de Henry Trevelyn-Thomas, da Tessian, empresa de segurança cibernética estadunidense focada em proteger dados pessoais, referindo-se ao aumento e sofisticação dos ciberataques e do efeito pandemia do coronavírus na segurança cibernética.



Fonte: Statista. Durante o primeiro trimestre de 2021, 24,9% dos ataques de phishing em todo o mundo foram direcionados a instituições financeiras. A mídia social foi responsável por 23,6% dos ataques.

A engenharia social explorou o medo, a busca de informações sobre a pandemia durante seus estágios iniciais com ataques de phishing (veja no gráfico acima os setores mais afetados), no final de 2020 e em 2021, com os ataques de ransomware que se multiplicaram explorando as brechas criadas pela implementação apressada do trabalho remoto. Vários negócios migraram para o digital, empresas que já estavam online expandiram e introduziram processos inteiramente novos em seus fluxos de trabalho, novas iniciativas digitais se aceleraram, profissionais trabalhando em casa e acessando a rede das empresas em computadores domésticos, o cibercrime explodiu. Pesquisa da Tessian aponta que mais de 1.000 multinacionais tiveram dados confidenciais roubados e vazados publicamente por ataques de ransomware em 2020. Os prejuízos financeiros aumentaram 311% em relação ao ano anterior foram pagos cerca de US$350 milhões em moedas criptográficas.

FIGURE 1 Average ransom in USD



From The Coveware Quarterly Ransomware Report

“A pandemia mostrou que a maioria das empresas tem dados desprotegidos e más práticas de segurança cibernéticas, tornando-as vulneráveis à perda de dados. É imperativo que as empresas se conscientizem da importância da segurança cibernética, atuem na prevenção e adotem melhores práticas de segurança como parte da cultura empresarial.”

Em relação ao primeiro ano da pandemia, nada mudou no segundo ano, em 2021 uma seguradora pagou US$40 milhões por ataque de ransomware de uma única vítima. De acordo com a seguradora Coalition, o ransomware foi responsável por 41% de todos os sinistros de ciber seguro nos três primeiros trimestres de 2021. O seguro de segurança cibernética se tornou uma parte do gerenciamento de riscos corporativos, mas ataques de ransomware descontrolados e outras falhas de violação fizeram com que muitas seguradoras aumentassem drasticamente as taxas de seguro, ou simplesmente, abandonaram a cobertura de empresas de alto risco de segurança ou saíram do mercado de seguros cibernéticos.

Empresas que trabalham com produtos de segurança cibernética apontam que os ataques de ransomware estão se reinventando e evoluindo para incluir extorsão de dados com base em informações vazadas perpetradas para compradores específicos. As organizações devem esperar que o ransomware se torne personalizado envolvendo diferentes tipos de ativos, como IoT e os funcionários das empresas.

Diante desse cenário, o combate a crimes na internet entrou na agenda de prioridades do presidente dos EUA, Joe Biden. Em outubro de 2021, Biden se reuniu com 30 países e a União Europeia, aliados da OTAN e do G7, para discutir questões de cibersegurança, melhorar a colaboração policial, impedir o uso ilícito de criptomoedas e facilitar questões diplomáticas em casos de

ataques de ransomware.[28] Especialistas em cibersegurança afirmam que o combate eficaz a esse tipo de crime requer cooperação internacional, os cibercriminosos não estão no mesmo país das suas vítimas. Identificar, localizar e extraditar exige coordenação entre os países.

As preocupações do governo Biden se intensificaram após o ciberataque ao oleoduto Colonial Pipeline. Além do compartilhamento de dados entre agências federais, eles estão trabalhando para dificultar o pagamento de resgate a ataques de ransomware por meio de criptomoedas. O Departamento de Tesouro dos EUA também planeja novas regras contra lavagem de dinheiro e financiamento ao terrorismo que devem dificultar os pagamentos aos atacantes. As sanções serão para indivíduos e transações específicas, não para todo setor de criptomoedas, e deverão prejudicar organizações ligadas a ataques anteriores e desencorajar plataformas de criptomoedas de processarem os pagamentos no futuro. Empresas envolvidas com ataques e sistemas financeiros que permitem aos atacantes receberem fundos sem serem rastreados serão alvo de multas e outras sanções.

Para pagar o resgate uma empresa retira fundos de uma instituição financeira para comprar moedas criptográficas que é transferida para uma wallet (carteira) da vítima, a transferência para o atacante se dá por intermédio de um quiosque privado(uma espécie de terminal de autoatendimento de cripto ativos) ou transferindo para uma carteira sob controle do atacante. Essas carteiras de cripto não estão em nenhuma exchange que trata e monitora as transações.

As moedas criptográficas, em tese, estão fora do controle de qualquer organização ou órgão governamental. Em tese porque estão em uma cadeia de blocos de informação, a tão falada blockchain, com a tecnologia adequada e conhecimento podem ser analisadas.

28 https://www.poder360.com.br/tecnologia/biden-planeja-reuniao-com-30-paises-para-combater-cibercrimes/

A grosso modo blockchain é uma espécie de livro-razão com blocos de informação conectados em cadeia. Cada bloco possui dados, a identificação única(hash) mais informação da hash do bloco anterior ao qual está conectado. A cadeia de blocos utiliza uma rede “peer-to-peer”, com computadores interligados onde os próprios nós validam as transações, o que elimina a necessidade de terceiros para proteger e autenticar os dados. A maioria das criptomoedas é executada em um blockchain público controlado por regras ou algoritmos de consenso e qualquer nó pode se juntar à rede e acessar, ou gravar dados no livro-razão como, por exemplo, no blockchain bitcoin ou no blockchain ethereum público. O fato de que toda transação ficar registrada no histórico e gravada nos blocos permite a análise e o rastreio de agências governamentais, cryptocurrency exchanges e instituições financeiras, com tecnologias adequadas, podem entender quais pessoas e entidades do mundo real transacionam entre si rastreando a blockchain. O que não invalida a segurança das informações no blockchain, todas criptografadas e com transações validadas por lógicas e algoritmos de computadores públicos, e não por banco de dados de uma corporação e pessoas que operam esses sistemas em data centers.

Força tarefa contra o ransomware

A preocupação com os ataques de ransomware também motivou a reunião de 60 especialistas da indústria, governos, juristas, organizações da sociedade civil e ONGs internacionais trabalhando em campanhas anti-ransomware unificadas, agressivas, abrangentes e público-privadas.[29] [30]

29 https://securityandtechnology.org/ransomwaretaskforce/report/
30 https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

“Criminosos com conhecimentos técnicos estão conduzindo ataques cada vez mais sofisticados. Não será com esforços isolados que o problema será atenuado, será preciso uma abordagem abrangente que influencie o comportamento de todos no ecossistema e cooperação internacional.” aponta o relatório.

A maioria dos ataques tem origem em países que não podem ou não querem levar os atacantes à justiça. Um desses países é a Rússia que tem sofrido sanções impostas pelos EUA desde abril de 2021, após a descoberta de operações de espionagem conduzidas do país para o resto do mundo. Apenas duas semanas após a reunião para discutir segurança cibernética, para a qual a Rússia não foi convidada, a agência de inteligência russa lançou uma campanha de invasão de milhares de redes de computadores do governo dos Estados Unidos, empresas e grupos de pesquisa americanos. O alerta feito por funcionários da Microsoft[31] que afirmaram que o objetivo era capturar dados armazenados na nuvem. “Este ataque de ransomware se enquadra na categoria de espionagem (em busca de segredos industriais ou farmacêuticos) e não na de sabotagem.”

O relatório da força-tarefa contra ransomware aponta que os criminosos estão expandindo os ataques para incluir dupla extorsão: primeiro exigem um resgate para descriptografar os dados de uma organização, depois ameaçam liberar os dados na internet se um resgate adicional não for pago. “No início de 2020, apenas um desses grandes ataques exigiu pagamento extra para os dados vazados, mas ao final do ano, pelo menos 17 outros grupos usaram essa tática.

31 https://www.canalmeio.com.br/edicoes/2021/10/26/cpi-pedira-banimento-de-bolsonaro-das-redes-sociais/

“A exposição potencial dos dados pessoais e sensíveis e a consequente responsabilidade legal, em países com leis de segurança de dados pessoais, é um dos fatores que levam as empresas a pagar o resgate.” Outros são: se têm ou não seguro contra ataque cibernético, a qualidade dos backups de dados e os custos estimados de interrupção do sistema.

Outra tendência apontada pela empresa de segurança cibernética Group-IB é o ransomware como um serviço (RaaS), em 2020, dois terços dos ataques de resgate analisados foram perpetrados usando um modelo RaaS que não requer sofisticação técnica. É um modelo que fornece recursos, um desenvolvedor escreve o programa malicioso que encripta e potencialmente rouba a vítima e um afiliado que paga uma taxa fixa ou uma parte dos resgates de sucesso. O afiliado executa o ataque e cobra o resgate, esse modelo, potencialmente, envolve um comprador, uma corretora de cryptocurrency ou especialistas em lavagem de moedas criptográficas.

A mentalidade de gerenciamento de emergência é uma aliada da segurança cibernética que ajudaria as indústrias que tradicionalmente preferem pagar o resgate em vez de tomar quaisquer outras medidas como preparar suas respostas cibernéticas. O setor industrial paga e é o setor que recebe o dobro dos ataques do que os segmentos de construção, tecnologia e varejo juntos. As indústrias não podem se dar ao luxo de desligar os sistemas por qualquer período de tempo. A preparação para os ataques cibernéticos pode construir resiliência e ajudar a criar resistência.

As medidas de prevenção e reação a ataques de ransomware da força tarefa contra os ataques requer cooperação internacional. Primeiro, os governantes devem deixar claro ações e medidas contra os ataques, isso inclui, definir como prioridade internacional diplomática que inclui cooperar de forma mais intencional e pública para enviar um sinal eficaz para os atacantes. Assumir compromissos com as medidas definidas internacionalmente e criar planos de contenção no âmbito doméstico.

Liderar novos esforços conjuntos com a indústria também é crucial: nenhum ator é totalmente capaz de interromper esta ameaça por si mesmos. É imprescindível que os governos trabalhem com parceiros internacionais tanto em nível político como operacional. Os participantes privados poderiam incluir fornecedores de infra-estrutura, fornecedores de plataforma/CA, registradores, endpoint empresas de segurança, empresas de inteligência de ameaças, redes de entrega de conteúdo (CDNs), operadores de rede, organizações sem fins lucrativos e nós da indústria. Usando APIs para a interoperabilidade.

Os Estados Unidos lideram a força tarefa e defendem priorizar e adotar sanções mais duras aos ataques de infraestruturas críticas ou por ataques que ponham em perigo a saúde e a segurança públicas. Para agir com mais força, os ataques de ransoware teriam o status de crime organizado e terrorismo o que permitiria confiscar os bens dos atacantes. EUA e parceiros internacionais devem trabalhar juntos para desenvolver uma comunidade internacional de inteligência responsável pela coordenação internacional, coleta global de informações contra os atacantes, e exercer pressão sobre as nações que são cúmplices ou coniventes. As punições seriam sanções econômicas e comerciais; restringir a atividade do país nos mercados financeiros internacionais e usando provas de cumplicidade, nomeá-los em fóruns públicos para perturbar a liberdade de atividade, retenção de ajuda militar ou de assistência estrangeira, ou ainda, negação de vistos a cidadãos que procuram viajar para os Estados Unidos ou outras nações.

Ransomware tem motivações financeiras, e desde que os lucros superem os riscos, os ataques continuarão. Para minimizar estes ataques, governos e partes interessadas do setor devem trabalhar em colaboração além das fronteiras para reduzir a rentabilidade e aumentar o risco de execução dos ataques. Entre as ações que os governos podem adotar estão:

1. Incomodar os sistemas de pagamento para tornar os ataques de resgate menos rentáveis,

2. Mexer com a infraestrutura utilizada para facilitar os ataques, exemplo: nuvem e Cloud Computing,

3. Interromper os atacantes com processos criminais e outras táticas,

4. Criar incentivos para compartilhar indicadores de pagamento de moeda criptográfica nas exchanges em tempo hábil e acionável para viabilizar a lei,

5. Apreender pagamentos de resgate quando possível. Estas informações podem incluir a carteira endereços, hashes de transação e notas de resgate. Em troca destas informações, as vítimas devem ser capazes de denunciar anonimamente.

6. Regular e penalizar as bolsas de troca de moedas, quiosques criptográficos e comércio de balcão (OTC) para cumprir com as leis existentes. Essas opções permitem a compra e venda de moedas criptográficas em troca de moedas tradicionais, e também as convertem em outras moedas virtuais. Estas entidades não estão em conformidade com ou sujeitas ao Know Your Customer (KYC), a due diligence de lavagem de dinheiro e Combate ao Financiamento do Terrorismo (CFT). As cryptocurrencies que estão sujeitas a essas leis ficam obrigadas a relatar transações suspeitas, trocas não conformes, de quiosques e balcões OTC.

7. A Receita Federal e a Europol se engajam em esforços para identificar os contribuintes que não revelaram renda da moeda criptográfica, serão incluídos nas sanções de evasão fiscal .

Tudo isso deve ser feito minimizando os danos às vítimas de resgate e não interferindo com sua capacidade de recuperar seus sistemas.

Leis de proteção de dados pessoais

A regulamentação das leis de proteção de dados pessoais e do direito à privacidade da União Europeia, em 2016, a GDPR (General Data Privacy Regulation) é um dos desenvolvimentos mais significativos na regulamentação de privacidade de dados e está tendo um grande impacto nos requisitos globais de proteção de dados. Embora a lei tenha origem na União Europeia e valha para os países do bloco, qualquer empresa que comercializa bens ou serviços para residentes na UE precisa cumprir a nova regulamentação, independentemente de sua localização. A regulamentação de como as empresas devem tratar a coleta, o processamento e armazenamento de dados, e de fixar multas de valor significativo em casos de não conformidade têm obrigado organizações em todo o mundo a, gradualmente, implementar mudanças e reestruturações para cumprir a lei e fugir das multas.

Nos Estados Unidos não há uma regulamentação para a proteção de dados válida para todo país, mas o estado da Califórnia tem o California Consumer Privacy Act of 2018 (CCPA) que funciona como método de defesa do consumidor, que entrou em vigor em 2020 no mesmo ano em que a Lei Geral de Proteção de Dados (LGPD) brasileira. Há leis semelhantes no Canadá, no Japão, Nova Zelândia e na Argentina, sendo que a lei de proteção de dados pessoais dos hermanos argentinos é de 2000 e limita o uso dos dados apenas com consentimento do cidadão.

No Brasil, o quinto país com o maior número de vítimas de ataques cibernéticos no mundo e com enormes vazamentos de dados[32], antes da LGPD os vazamentos eram ocultados pelas empresas que agora devem comunicar à Autoridade Nacional de Proteção de Dados, além de adotar medidas para reduzir ou mitigar o risco.

32 https://www.consumidormoderno.com.br/2021/02/05/procon-megavazamento-dados/

É crucial definir as permissões aos arquivos, atualizar o consentimento dos usuários e se livrar de dados obsoletos ou dos dados que o cliente pede para excluir. Indústrias que armazenam informações valiosas como saúde e finanças são os maiores alvos para roubar registros médicos, financeiros e outros dados pessoais.

A confiança do público deve estar no foco das empresas devido ao impacto do crime cibernético nos clientes. Assim como no mundo físico estabelecemos diferentes níveis de confiança com outras pessoas, na web também especialmente com empresas com as quais fazemos negócio, quando essa confiança é quebrada e dados sensíveis são expostos ficamos mais relutantes em confiar em outros relacionamentos e esse trauma quando acontece em sociedade, todo mundo começa a desconfiar de todo mundo. As violações de dados produzem reações negativas devido ao estresse envolvido com a perda de privacidade. Individualmente, as pessoas são frequentemente deixadas deprimidas, envergonhadas e confusas após terem sido vítimas de crimes cibernéticos como fraudes bancárias com dados pessoais vazados. A percepção de que as informações pessoais não são mais privadas pode ter um efeito bastante prejudicial sobre a psique.

Em uma pesquisa da PricewaterhouseCoopers[33], uma em cada quatro pessoas dizem que deixariam de lidar com uma marca que sofreu uma violação, e as repercussões para as empresas são enormes, tanto que cerca de 60% das pequenas e médias empresas saem do mercado seis meses após serem vítimas de uma violação de dados. Empresas maiores como Ebay, Equifax e LinkedIn são gigantes e podem não sentir tanto as violações de dados, os danos são na reputação e na perda de confiança dos consumidores e de opinião pública negativa.

A proteção de dados pessoais não é mais opcional para as empresas. Com a entrada da LGPD o crescente número de ataques cibernéticos expondo milhões de registros de informações de dados pessoais, as preocupações com a privacidade, gerenciamento, segurança e a privacidade de dados pessoais deve ser tratada como prioridade. Os clientes são as principais vítimas de crimes cibernéticos, suas informações são expostas pelos atacantes, perde-se a privacidade, e principalmente, o direito do sigilo bancário. Além de adotarem medidas para fortalecer a segurança dentro da empresa e proteger os clientes, é importante conscientizar os usuários para identificar e prevenir hacks de rede. A conscientização dos usuários e funcionários das empresas é uma boa prática para proteger a reputação da empresa e para prevenir tais ataques.

Como proteger o ecossistema cibernético?

Em duas palavras: security by design[34]

Security by design é a segurança preventiva de boas práticas de segurança da informação para diminuir as vulnerabilidades desde o início do desenvolvimento de software, nos processos internos, no desenvolvimento de aplicativos e dispositivos de IoT. Propõe uma relação de trabalho positiva entre os desenvolvedores e a equipe de segurança, com requisitos claros e apropriados, além da possibilidade de testar a segurança do código-fonte desde o planejamento inicial e concepção.

Desenvolvedores, produtores de produtos e serviços dos quais depende a estabilidade do ciberespaço devem priorizar a segurança e a estabilidade, tomar medidas razoáveis para garantir que seus produtos ou serviços estejam livres de vulnerabilidades significativas e adotar medidas para mitigar vulnerabilidades que são descobertas e ser transparente sobre seus processos.

34 https://owasp.org/

Todos os atores têm o dever de compartilhar informações sobre vulnerabilidades, a fim de ajudar a prevenir ou mitigar atividades cibernéticas maliciosas.

Um programa de segurança cibernética bem-sucedido tem camadas de proteção espalhadas por redes, servidores, computadores e aplicações. Firewalls, filtros DNS, antivírus e software de proteção contra malwares, treinamento aos funcionários sobre como lidar e compartilhar dados corporativos confidenciais.

A Inteligência Artificial está sendo utilizada para detectar intrusões, o papel do Aprendizado de Máquina (Machine Learning) torna a segurança cibernética mais simples, mais eficaz e, ao mesmo tempo, menos cara. A partir de um volumoso conjunto de dados, o ML desenvolve padrões e os manipula com algoritmos. Dessa forma, ele pode antecipar e responder a ataques ativos em tempo real. Essa tecnologia depende fortemente de dados de qualidade para produzir algoritmos eficazes. Os dados devem vir de todos os lugares e representar tantos cenários potenciais quanto possível. Machine Learning permite que os sistemas de segurança cibernética analisem os padrões de ameaça e aprendam os comportamentos dos cibercriminosos. Isso ajuda a evitar ataques semelhantes no futuro e também reduz o tempo necessário para que os especialistas em segurança cibernética executem tarefas de rotina.

Tendências para as empresas

Abaixo um compilado de recomendações para proteção contra ataques de ransomware.

1. Conscientização do usuário

Os clientes são as principais vítimas de crimes cibernéticos, pois suas informações são expostas. As empresas devem propor medidas para fortalecer a segurança e proteger seus clientes. É importante conscientizar os usuários sobre os métodos de um ataque cibernético para identificar e prevenir hacks de rede. E também treinar os funcionários sobre como lidar e compartilhar dados corporativos confidenciais.

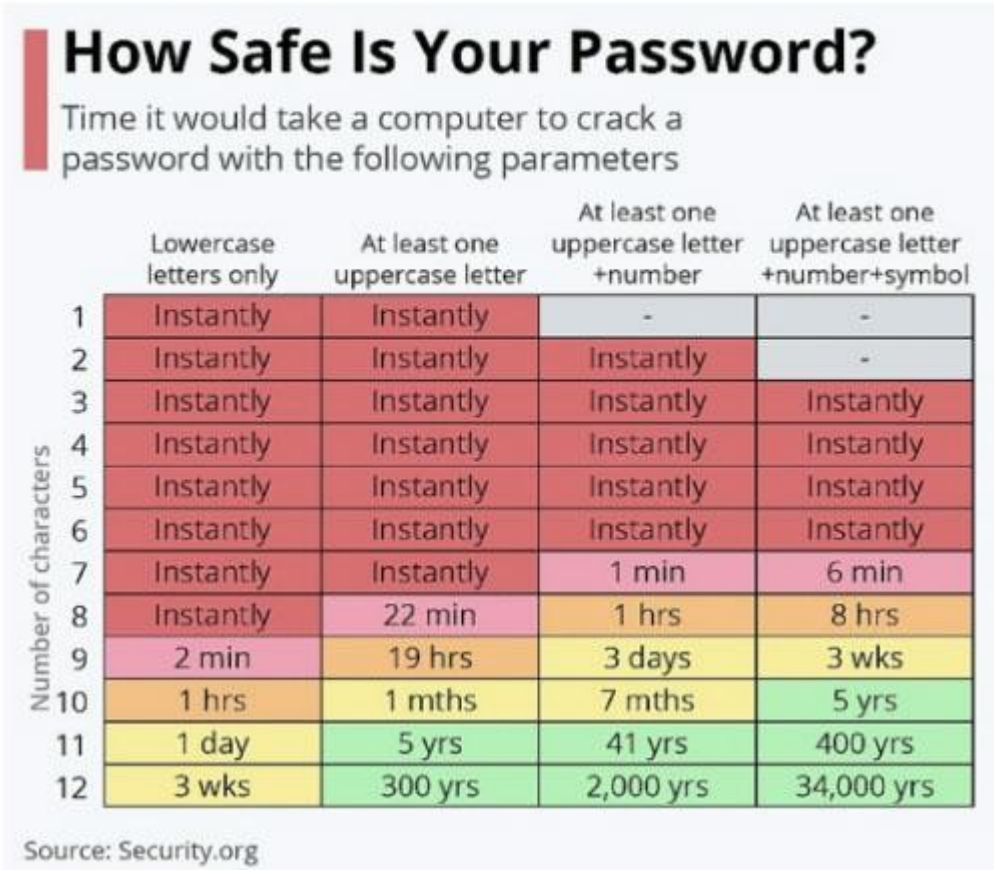
Um dos exemplos mais importantes de educação e conscientização de segurança digital é o uso de senhas. De acordo com uma pesquisa[35] feita pelo Google em 2019, 24% dos estadunidenses usam senhas fracas (por exemplo, “abc123”, “Password”, “123456”, “Admin”, etc.) e 59% dos indivíduos incorporaram um nome ou data de aniversário em suas senhas, o que os torna suscetível a ataques de força bruta. Outra pesquisa do Precise Security.com, aponta que as senhas fracas foram responsáveis por 30% das infecções de ransomware em 2019. A senha não é uma forma muito eficaz de proteger os dados pessoais, a memória humana não é tão boa e as pessoas tendem a usar a mesma senha fácil em todas as ocasiões. Reutilizar senhas é uma péssima prática do ponto de vista da segurança. Se um invasor tiver acesso a uma senha utilizada em diversos serviços diferentes, poderá ter acesso a muitas contas. É por isso que é tão importante ter senhas fortes, únicas e distintas, de preferência com mais de um fator de segurança e senhas descartáveis.

Outra dificuldade inerente ao ser humano é a dificuldade em fazer escolhas aleatórias e imprevisíveis. Uma forma eficiente de criar uma senha forte e que possa ser memorizada é utilizar dados numéricos e uma lista de palavras para escolher palavras de maneira aleatória.

35https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

Juntas, estas palavras formarão sua “frase-chave”. Uma frase-chave é um tipo de senha mais comprida, com o objetivo de ser mais segura. Recomenda-se utilizar um mínimo de seis palavras, o ideal é doze quanto mais comprida e mais aleatória for a senha, mais difícil será para computadores e humanos adivinhá-las.[36]

Senhas com símbolo, número, letra maiúscula e doze dígitos são as mais seguras



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

Como criar senhas fortes?

36 https://ssd.eff.org/pt-br/module/criando-senhas-fortes

Não usar informações pessoais Exemplos: datas de nascimento, aniversário, casamento, falecimento; nomes (próprio, de filho(a)(s), animais, etc.); favoritos (filme, livro, comida, etc.)
Não usar sequências de números ou letras e não usar repetições ou espelhamentos
Busque formas de criar senhas sem sentido ou aleatórias
Use senhas longas (com mais de 12 caracteres)
Use senhas que não sejam palavras que estão no dicionário
Mesclar tipos de caracteres: letras (MAIÚSCULAS e minúsculas), núm3ros e esp&c!4i$
Cuidado com as “perguntas de segurança” que sites utilizam para confirmar identidade. A resposta verdadeira são fatos públicos fáceis de descobrir se a pergunta for: “Qual era o nome de seu primeiro animal de estimação?” A resposta deve ser uma senha aleatória e fictícia. Tente lembrar dos sites em que você utilizou perguntas de segurança e nunca utilize as mesmas senhas ou respostas às perguntas de segurança para diversas contas em sites ou serviços diferentes.

2. Muitas empresas estão migrando para a autenticação sem senha, é preferível pelas recomendações acima. As empresas que optam por autenticação sem senha adotam os padrões fornecidos pela FIDO Alliance[37] , incluindo Universal Authentication Framework (UAF), Universal 2nd Factor (U2F) e mecanismo FIDO 2 (cujo componente principal é a Autenticação da Web, ou WebAuthn[38] , publicada pelo World Wide Web Consortium), que

37 https://fidoalliance.org/
38 https://en.wikipedia.org/wiki/WebAuthn

permite fazer login com dados biométricos, chaves de segurança física (token), entre outras.

3. Ameaças de phishing direcionadas geograficamente

Os ataques de phishing são atualmente a ameaça de segurança mais extensa para o setor de TI, os e-mails de phishing e URLs maliciosos continuam prevalecendo na web, exceto que agora são localizados, mais personalizados e direcionados geograficamente. Mais uma vez a dica é treinar funcionários e clientes, um estudo identificou que pessoas informadas têm cinco vezes menos probabilidade de abrir um e-mail de phishing. O treinamento também deve informar sobre ataques cibernéticos e as abordagens de defesa e compartilhar seus erros e conhecimento (especialmente o primeiro) em vez de escondê-los

4. Segurança na nuvem

Não existe nuvem (etéreo) são só computadores de outra pessoa que não o seu. A nuvem possibilita que serviços online expandam as capacidades de armazenamento, processamento, etc, de um computador ou celular.

Soluções de Cloud Computing permitem que pequenas empresas possam escalar seus negócios com muita velocidade, isso porque o custo de implementar novas tecnologias são mais acessíveis do que antigamente. Computação na nuvem facilita ter ferramentas, instrumentos, tecnologias, estruturas escalabilidade, servidores flexíveis, suporte, etc. A computação em nuvem viabilizou a sobrevivência de várias empresas que migraram para o home office e nunca esteve tão presente como na pandemia de Covid 19. Não seria possível oferecer tantos serviços para quem estava em isolamento para manter o distanciamento social sem a nuvem. É necessário avaliar o impacto no seu modelo de negócio, riscos, jurisdição, histórico de compromisso com segurança e privacidade.

Amazon Web Services(AWS), Google Cloud, VMware Cloud e outros serviços em nuvem fornecem o básico de segurança, a maioria não fornece criptografia segura e não dá para achar que está 100% seguro. E evitar armazenar dados sensíveis desnecessariamente, exclua ou mantenha apenas uma cópia fora da internet.

6. Conformidade com as leis de proteção de dados pessoais.

7. Vulnerabilidade de IoT

Os problemas de segurança afetam a maioria dos dispositivos IoT que dominam o mercado. Dispositivos de computação embutidos em produtos IoT permitem o envio e recebimento de dados pela internet. Isso representa ameaças de segurança significativas para os usuários, expondo-os a ataques cibernéticos como DDoS ou dispositivos sequestrados. À medida que a IoT conecta o espaço virtual e o mundo físico, as intrusões domésticas estão

aumentando a lista das ameaças mais assustadoras possíveis que a IoT traz. Os dispositivos IoT são uma boa oportunidade para empresas e cibercriminosos.

8. Dispositivos móveis como vetores de ataque

A maior parte do software de comércio eletrônico e outras plataformas podem ser acessados por meio de plataformas móveis. Os smartphones são alvos de cibercriminosos que os consideram um meio fácil de atacar. No celular os usuários fazem negócios e comunicação pessoal, compras, reservas em hotéis, bancos, etc. Mais de 70% das transações fraudulentas ocorrem usando dispositivos móveis.

9. A proteção com blockchain

A CIA, confidencialidade, integridade e autenticidade, a tríade do blockchain é um modelo que orienta as políticas de segurança da informação de uma organização. Uma empresa que pretenda mitigar o risco cibernético precisa construir uma política de segurança focada nestas três propriedades.

9.a A confidencialidade é a proteção de dados contra acesso não intencional, ilegal ou não autorizado, divulgação ou roubo. Os blockchains podem ser usados para apoiar a confidencialidade por meio do gerenciamento de direitos de acesso ou registros, por exemplo, em identidade auto-soberana.

9.b A integridade significa a manutenção e garantia da precisão e consistência dos dados ao longo de todo o seu ciclo de vida. A tecnologia blockchain pode apoiar a integridade por meio de propriedades como carimbo de data/hora e reconhecimento de firma da data, por exemplo, na certificação de documentos.

9.c Já a autenticidade diz respeito à veracidade dos dados, certificando-se de que os dados recebidos no servidor de coleta são originais e foram recebidos exatamente como enviados. Resolvendo o problema do Man in the middle (MITM). Qualquer sistema baseado em protocolos de acordo-chave e no armazenamento e troca de segredos é vulnerável a ataques de de uma forma ou de outra, e a melhor maneira de evitar ataques é usar sistemas de autenticação já que esses ataques têm como objetivo fazer com que a Autoridade de Certificação (CA) forneça ao usuário chaves públicas falsificadas que pode levar à descriptografia de informações confidenciais. Um blockchain permite redes de permissão e IDs digitais seguros e personalizados e combate fraudes porque o livro-razão é constantemente atualizado se ambas as partes forem verificadas. Além disso, os participantes podem ver o histórico e a transferência de ativos, para que as transações fraudulentas sejam mais fáceis de identificar. Uma abordagem de blockchain pode oferecer suporte à autenticidade fornecendo credenciais digitais em sistemas de identidade, rastreamento e pagamentos.

Empresas como a IBM e a Accenture já usam o blockchain para prevenção de fraudes em seus processos de negócios. Recursos como razão distribuída, imutabilidade, segurança, transparência, sistema descentralizado, permissão, etc., evitaria a ocorrência de fraudes em setores como saúde, bancos, imóveis, segurança e seguros.

Com pandemia do coronavírus, a autenticação de documentos em serviços notariais[39] ganhou impulso. Uma plataforma que permite acessar serviços de cartórios de todo o Brasil digitalmente, usa a função de autenticação digital do blockchain, os documentos são verificados e guardados permanente com dados criptografados e públicos. O documento certificado pela rede é imutável e ficam salvos dentro de blocos criptográficos conectados entre si permitindo rastrear todas as transações feitas. Cerca de 156 mil páginas de documentos já foram autenticados.

39 https://www.e-notariado.org.br/

Para combater a pirataria, a Disney criou uma patente de um sistema de distribuição de mídia baseado em blockchain que visa prevenir vazamentos e pirataria de conteúdo ainda não lançado, principalmente, nas produções cinematográficas, a parte do processo mais vulnerável, permitindo que pessoas com as conexões certas possam fazer cópias durante ou após a entrega do conteúdo finalizado.

Outro recurso de autenticação em blockchain é o MetaMask, desenvolvido em 2016, foi criado inicialmente como uma carteira para realizar negócios com Ethereum e NFTs, é uma carteira não custodial, isto é, somente o proprietário possui a chave de acesso privada. Com foco na segurança dos usuários foi programada com a biblioteca oficial Ethereum, a web3.js e usa a interface e a API da web Ethereum. O MetaMask permite o desenvolvimento de aplicativos descentralizados(Dapp), que são softwares baseados em blockchain, um mecanismo capaz de validar e preservar transações por meio de um registro protegido por criptografia de alta segurança, qualquer alteração só é executada depois que se atinge um consenso entre os participantes. Protocolos e informações também são armazenados em blockchain e acessíveis à rede descentralizada.

O MetaMask controla cada interação do usuário com o Dapp e executa as operações necessárias para que as transações sejam realizadas, em um meio de comunicação seguro e com a capacidade de gerar suas próprias chaves assimétricas, salvá-las localmente e gerenciar seu acesso. Os aplicativos descentralizados, os Dapp, tem código aberto e operam de modo autônomo, sem uma autoridade no controle. Qualquer alteração só é executada depois que se atinge um consenso entre os participantes. São emitidos tokens, uma espécie de ficha virtual com valor atribuído, para permitir acesso à rede, recompensar usuários e incentivar a contribuição dos membros da rede.

O MetaMask ultrapassou a marca de 10 milhões de usuários ativos mensais e é mantido pela Consensys e é muito utilizado em protocolos de DeFi e marketplaces de NFTs, dois setores que tiveram crescimento expressivo nos últimos meses. Esse aplicativo está disponível para todos os navegadores e também nas plataformas mobile, sistemas Android e iOS (Apple). O Brasil é o oitavo país com mais usuários no mundo do MetaMask, cerca de 140.000 usuários ativos por mês.

5

Economia digital

Em 2013, o então Secretário-Geral das Nações Unidas, Ban Ki-moon, escreveu no prefácio do relatório da UNCTAD(em inglês, United Nations Conference on Trade and Developm), organização intergovernamental para ajudar países em desenvolvimento a serem mais eficientes para se integrarem à economia global, que a computação em nuvem (cloud computing), "(...) tem um grande potencial para o desenvolvimento econômico e social."

Por muitos anos, os fornecedores de tecnologia estiveram focados nos grandes clientes com orçamentos vultuosos. Mainframes, redes privadas de alta velocidade, arquiteturas de alta disponibilidade, computação distribuída. O que tornava a tecnologia praticamente inacessível às pequenas e médias empresas por alto custo e complexidade de implantação. A computação em nuvem mudou o jogo ao possibilitar que empresas, independentemente do porte, usem a mesma infraestrutura e recursos tecnológicos do que as grandes sem os investimentos vultosos, sem custos fixos somente custos variáveis conforme o uso (pay-per-use), possibilitando a competição entre todos.

Essa é a grande revolução que vêm sendo proporcionada pela nuvem e o motivo pelo qual o cloud computing é considerado o motor da indústria 4.0.

Um parênteses: a indústria 4.0 se refere menos "as coisas", mas sim como são feitas, uma série de mudanças nos procedimentos e na maneira como os produtos são fabricados visando aumentar o valor da cadeia organizacional e do ciclo de vida das mercadorias. Nesse contexto, tudo o que está envolvido com a metodologia de trabalho da indústria deve ser conectado, uma cadeia de

valor integrada, onde a interconectividade é a principal inovação. Sem a computação na nuvem essa interconexão seria impossível.

O que é cloud computing? Segundo o NIST[40]Instituto Nacional de Padrões e Tecnologia do departamento de comércio norte-americano: a computação em nuvem é um modelo que permite acesso ubíquo, conveniente e sob demanda, via rede, para um conjunto compartilhado de recursos computacionais configuráveis. Na prática é a evolução e a reunião dos fundamentos técnicos de áreas como virtualização de servidores, grid computing (modelo computacional com alto processamento que divide as tarefas entre diversas máquinas, podendo ser em rede local ou rede virtual), software como serviço, gestão de grandes instalações (data centers).

De modo simples, cloud é a migração de sistemas computacionais físicos para uma base virtual de grandes empresas de tecnologia que proporcionam Infraestrutura de TI, hardware, software, centros de dados e informação, acessados pela internet, por qualquer browser e qualquer tipo de equipamento. Todo mundo conectado acessa algum serviço em nuvem várias vezes ao dia: Webmail, Google, Facebook, YouTube, Twitter, Netflix para citar só alguns. A Netflix[41], o maior utilizador de largura de banda nos Estados Unidos, migrou os conteúdos de streaming para fornecedores de serviços de rede como a Comcast, Verizon e AT&T para armazenar e atender as requisições dos clientes, a Amazon Web Services (AWS) para pesquisa e fornecimento do sistema de recomendação e até faturamento e pagamentos estão em centros de dados na nuvem.

A disseminação dos computadores pessoais na década de 1990, o preço da computação e das tecnologias caindo, maior poder de processamento e armazenamento de dados e velocidades de transmissão mais altas aliadas a larguras de banda mais rápidas para os usuários provocaram a migração de muitas estruturas para a nuvem.

40 https://csrc.nist.gov/publications/detail/sp/800-145/final

41 Brodkin, J. 2016. “Netflix finishes its massive migration to the Amazon cloud.” ARS Technica, Biz and IT

A principal motivação para adoção do cloud computing é econômica e essa vantagem advém da economia de escala resultante do uso mais eficiente dos recursos computacionais. Fernando Arbache[42], empreendedor, consultor de educação independente trabalhando com o MIT e professor em instituições como FGV, Fundação Dom Cabral, FATEC, trabalha com computação em nuvem desde 1998 e explica a importância: “É poder ter ferramentas, instrumentos, tecnologias com preços mais acessíveis e poder concorrer com outras empresas, inclusive grandes.” Cloud computing fornece soluções para empresas iniciantes entrarem no mercado com seus produtos e serviços digitais, ganharem tração e exponenciar rapidamente o negócio, isso muda a competitividade, as relações de força e a concorrência em todos os setores da economia. Muitos dos novos modelos de negócios só são viáveis através do uso da tecnologia que se torna mais crítica na execução das estratégias e o cloud oferece serviços de TI avançados com economia, infraestrutura elástica, capacidade de armazenamento, processamento conforme a demanda, mobilidade de dados e serviços, atualização imediata e gratuita de software, suporte técnico, manutenção e serviços de assistência técnica. “Starups têm o potencial de inovar e gerar rupturas em setores tradicionais e se transformem em empresas de um bilhão de dólares, as tais unicórnios, graças as oportunidades para agilizar processos, possibilitar a inovação, ganhar eficiência e escalabilidade, com custos mais acessíveis e competitivos.” Muitos players da indústria de tecnologias de informação e computação consideram as nuvens como a próxima fase do desenvolvimento da internet, similar ao modelo de computação cliente/servidor que precedeu a popularização da computação pessoal.

42 https://vimeo.com/529265754/7fa05fd125

A expectativa é que a nuvem se tornará cada vez mais o recurso predominante para empresas. Como toda nova tecnologia transformadora que atinge o patamar de produtividade e viabilidade econômica, a computação em nuvem abre novas possibilidades que permite ampliar o alcance e melhorar o desempenho das mais diversas atividades empresariais, diminuindo os custos de implantação de soluções de processamento de dados e mecanismos de interação com os clientes por intermédio de canais digitais. Já o consumidor final adota serviços em nuvem, principalmente, para armazenamento online, backup e sincronização entre dispositivos.

Acelerando a transformação digital

Um relatório da International Data Corporation (IDC) aponta que os investimentos em transformação digital crescerão a uma taxa anual de 15,5% até 2023, aproximando-se de US$ 6,8 trilhões. Segundo o estudo do IDC, 70% de todos os gastos com tecnologia e serviços será em operações baseadas em nuvem. “As empresas terão acelerado o uso de tecnologias digitais e mais da metade da economia global será baseada (e influenciada) pela digitalização, até por que, a maioria das empresas de produtos e serviços já utiliza esse modelo em suas entregas ou precisa investir mais em ferramentas digitais para manter as suas atividades em funcionamento.”
Fernando Arbache explica que cloud computing acelera a economia digital gerando oportunidades em diversas áreas. “Já estamos vivendo na economia digital, tudo está no digital ou migrando, a pandemia de Covid-19 nos mostrou isso claramente. Foi o digital que viabilizou a continuação dos negócios, do home office e da adoção massiva de tecnologias de comunicação como o Zoom, o Teams que possibilitaram fazer reuniões em vários lugares do mundo de uma forma muito simples. Serviços de teleconferência já existiam

vide o Skype, mas não eram usados por tantas pessoas e possibilitaram além das reuniões, a continuidade de eventos, congressos, etc. Sem o cloud não seria possível oferecer tantos serviços quantos foram oferecidos para viabilizar que - quem podia - ficasse em casa."

Outro fator citado por Arbache foi o crescimento de empreendedores e microempresários digitais. Para exemplificar cita o iFood que possibilitou que pequenos empreendedores da área de alimentos pudessem fornecer seus produtos com a mesma infraestrutura de uma grande rede de alimentação. "Um microempresário em um canto que ninguém conhecia, produtores de alimentos de com mais diversidade, produtos mais caseiros, artesanais, de nicho conseguiram sobreviver por meio desse hub digital. Esses microempresários vão se tornar grandes e competir com uma Pizza Hut, por exemplo, provavelmente não, mas em conjunto esses microempresários estão reduzindo a escala das grandes redes alimentação."

O iFood é uma plataforma, uma empresa de tecnologia e distribuição, não de alimentação e conectou pessoas e microempresários que tiveram mais oportunidade de venda e de ficarem conhecidos. Essa concorrência de todos com todos é o que gera as inovações disruptivas permitindo que uma nova população de consumidores na base do mercado tenha acesso a um produto ou serviço que, historicamente, só era acessível a consumidores endinheirados ou com muita habilidade, no caso de tecnologias. O termo 'inovação disruptiva' foi cunhado por Clayton Christensen, no livro The Innovator's Dilemma[43] e descreve esse movimento propiciado pela tecnologia existente, predominantemente, nas nuvens e que muda a cultura econômica e permite fazer algo escalável, mais barato e que atenda diversos nichos. Um não faz nenhuma diferença, mas milhares de pessoas migrando para esses pequenos empresários, o impacto nas grandes gera disruptura do mercado.

43 https://www.amazon.com.br/Innovators-Dilemma-Revolutionary-Change-Business/dp/0062060244

Um conceito da transformação digital são os benefícios de primeira e segunda ordem. Os benefícios primeira ordem são a adoção e democratização da tecnologia. O benefício de segunda ordem é a oferta de tecnologia. Um exemplo é o Zoom ao descobrir seu público alvo empresas com menos de 10 funcionários, em 2020 ano I da pandemia, conquistou 370.200 novos clientes, o que gerou um crescimento de 438% em relação a 2019. Ao se tornar uma tecnologia popular chegou ao ponto de inflexão, o crescimento continua, mas em ritmo menor porque a tecnologia ofertada se tornou commodity e foi copiada por outras empresas. Apenas adotar tecnologias não tornam as empresas mais competitivas nem proporcionam um crescimento exponencial por não oferecerem nenhum diferencial competitivo, justamente, por causa do cloud e das vantagens econômicas na adoção de tecnologias.
Já o iFood obtêm benefícios de segunda ordem oferecendo a vários usuários a utilização da plataforma, um negócio que não é simples de copiar, o desenvolvimento de tecnologia que exige investimentos vultosos e mão de obra altamente especializada e cara.
Os benefícios de segunda ordem são o contrário dos de primeira ordem: impulsionam pouco até serem adotadas em grande escala, ter milhões de usuários, daí o crescimento é exponencial e a curva permanece alta. As empresas de segunda ordem são grandes empresas de e-commerce e desenvolvedores de plataforma que capturam os benefícios das commodities digitais. Os unicórnios são de segunda ordem por criarem tendências tecnológicas. Empresas que capturam benefícios de primeira ordem adotando tecnologia estão em países em desenvolvimento e até em algumas economias de alta renda. As empresas que usufruem dos benefícios de segunda ordem estão em economias avançadas como Alemanha, Japão, Suécia, Estados Unidos e China. Empresas de serviços em nuvem são um pequeno número de

empresas globais de TI como Google, Amazon, Microsoft, Alibaba, Apple, entre outras sediadas nos Estados Unidos e China.

> "Estamos testemunhando uma divisão na economia global entre aqueles que usam e aqueles que desenvolvem, distribuem e gerenciam tecnologias digitais e estabelecem padrões. Neste contexto global é preciso distinguir uso do desenvolvimento, distribuição e gerenciamento. A maioria dos negócios são usuários, uma pequena parte são os desenvolvedores."
>
> Fernando Arbache

Estados Unidos e China são os grandes usuários de cloud e adoção dos serviços de nuvem continua crescendo, mas apostam no desenvolvimento, tanto que 75% de todas as patentes relacionadas à blockchain são registradas nos Estados Unidos e na China. Países que perceberam os benefícios de segunda ordem e respondem por até 85% de todos os data centers que oferecem esses serviços.

As nuvens

A nuvem não é etérea, mas uma série de servidores localizados em várias partes do mundo, que podem ser alocados e desalocados dinamicamente, e rodam como máquinas virtuais no hardware do fornecedor de serviços. Quando em execução, as máquinas virtuais são chamadas instâncias e podem ter diferentes tipos em função do modelo de cobranças e forma de alocação.

Esses servidores são elásticos, isto é, se adaptam às alterações de carga de trabalho pela alocação e liberação de recursos, automaticamente, conforme a variação da carga. Um site será elástico se for capaz de alocar e liberar recursos como servidores, discos, banda de comunicação à medida que o número de usuárdios simultâneos aumenta ou diminui.
O fato de um sistema rodar na nuvem não garante que ele seja escalável. Alocar e liberar recursos automaticamente seja de capacidade de processamento, espaço, memória e banda com desempenho adequado para cargas de trabalho crescentes e adicionar novos recursos computacionais se houver necessidade define a escalabilidade é um pré-requisito para a elasticidade. Um sistema só pode ser elástico se for escalável.

Diferentes tipos de nuvem

✔ Nuvem pública é oferecida pela internet por um provedor de serviços. Os recursos computacionais são compartilhados por diversos clientes e o controle das instâncias, máquinas virtuais e recursos de processamento e armazenamento ficam completamente delegados ao provedor. Os principais players são Amazon (AWS), Microsoft Azure e Google Cloud Platform.

✔ Nuvem privada é aquela em que os recursos computacionais alocados são isolados dos recursos compartilhados pela nuvem pública com os mesmos benefícios, via de regra, dedicados a uma empresa específica. Se estiver configurada em um provedor público, a infraestrutura é controlada pelo provedor de serviços com alocação e liberação dos recursos computacionais sob demanda e pagamento pelo uso. A nuvem privada também pode ser criada na rede interna da empresa que controla a infraestrutura física e tem menos problemas relacionados à segurança, em tese, já que o tráfego de informações e migração de dados entre servidores virtuais e físicos é limitada aos recursos que estão sob controle da empresa cliente.

A segurança dos sistemas está relacionada à sua arquitetura, mecanismos de proteção e técnicas de sigilo de dados.

✔ As nuvens híbridas são a combinação das duas anteriores, a decisão de executar em nuvem pública ou privada depende de vários parâmetros, como sensibilidade dos dados e aplicativos, certificações do setor, padrões e regulamentos. A empresa pode manter algumas aplicações na nuvem privada e outras em serviços de nuvem pública ou privada virtual.

✔ Multi Cloud, dois ou mais fornecedores de nuvem pública e podem incluir uma nuvem privada no data center da empresa.

A revolução do cloud computing proporcionou mudanças do produto físico para serviços:

✓IaaS - Infrastructure as a Service

Computação em nuvem baseia-se na alocação de recursos de acordo com a demanda. Na infraestrutura como serviço, alocam-se recursos para processamento e armazenamento de dados. Antes da tomada de decisão por esse tipo de serviço é preciso definir o tipo e o tamanho das máquinas virtuais, capacidade de processamento, como os dados serão armazenados e a integração entre diferentes tipos de recursos. Outra questão a ser considerada é a região geográfica onde o servidor será criado, primeiro por causa da latência que impacta diretamente no desempenho de uso, quanto mais distante for a região, maior o tempo de resposta. Além disso, a região precisa ser avaliada em relação aos custos, impostos e legislação, principalmente, em relação à proteção de dados dos usuários em conformidade com as leis locais. Os três maiores fornecedores de IaaS são Amazon, Google e Microsoft.

Na Amazon Web Services(AWS), por exemplo, as regiões estão distribuídas por vários locais, nos estados da Virgínia, Califórnia, Oregon nos Estados Unidos, em São Paulo, Irlanda, Tóquio, Singapura e Sidney. Cada região oferece duas ou mais zonas de disponibilidade. Cada uma é um data center completo com infraestrutura independente conectadas por links de baixa latência, isto é, velozes com tempo de resposta baixo. As nuvens do Google estão em três regiões, Estados Unidos, Europa e Ásia, cada região possui pelo menos três ou mais zonas de disponibilidade possibilitando a redundância dos recursos para garantir alta disponibilidade dos serviços e dados hospedados na nuvem. O Google guarda sigilo sobre a localização dos seus data centers. A Microsoft Azure possui data centers distribuídos em cinco áreas geográficas e 13 regiões: Iowa, duas na Virgínia, Illinois, Texas e Califórnia nos Estados Unidos, Irlanda e Holanda na Europa, Hong Kong e Singapura na região da Ásia- Pacífico, duas no Japão, e uma em São Paulo.

✓PaaS - Platform as a Service

Plataforma como serviço oferece um ambiente de desenvolvimento de software para desenvolver aplicações para rodar na nuvem. Ao usar o PaaS os desenvolvedores não precisam cuidar da administração do sistema operacional e da gestão de infraestrutura. Alguns fornecedores de PaaS oferecem serviços especializados, por exemplo, desenvolvimento de aplicações em linguagem Java ou múltiplas linguagens de programação com suporte para PHP, Ruby, Python e outras para o desenvolvimento de aplicações web. Antes de escolher o fornecedor é importante dimensionar as necessidades de armazenamento e disponibilidade de dados. Se a aplicação exigir baixa latência considera-se uma solução com capacidade de prover grande número de operações por segundo. Se o negócio for tratamento de dados, a escalabilidade, a escolha deve ser uma plataforma que suporte bancos de

dados NoSQL. Os players principais são: Google App Engine, Heroku, Red Hat OpenShift, Microsoft Azure Cloud Services, Tsuru e etc.

✓SaaS - Software as a Service

Comprar software como serviço significa comprar o acesso a uma aplicação sem se preocupar da infraestrutura por trás dela sendo apenas um usuário do software, sem nenhuma tarefa de gerenciamento de infraestrutura para executá-lo. Um exemplo de software como serviço é o Google Apps com ferramentas como email, agenda, a suíte Google Docs que são acessadas pelo navegador em qualquer dispositivo. Isso para usuários finais, empresas podem fazer uso do Google Apps For Work e os aplicativos podem ser personalizados para a empresa. O SalesForce, sistema de gestão de relacionamento com clientes(CRM) é outro exemplo.

✔Content Delivery Network

Para otimizar a entrega de conteúdo para o usuário final há empresas que oferecem serviços de Content Delivery Network (CDN), um sistema de servidores distribuídos ao redor do mundo para oferecer alta disponibilidade e alta velocidade do conteúdo. Cópias do conteúdo são entregues ao usuário que fez a requisição a partir do data center mais próximo. Entre os fornecedores de serviços de nuvem que têm seu próprio serviço de CDN estão a Amazon CloudFront e o Microsoft Azure CDN.

Segurança na nuvem

Cloud computing cresce exponencialmente e pode ser uma boa solução, entretanto, questões de segurança e gestão de riscos preocupa especialistas em

segurança pela integridade e controle reduzido sobre os dados e aplicativos, privacidade, segurança da informação e crimes cibernéticos.

A responsabilidade da segurança na nuvem é de ambas as partes, provedores e clientes. Os provedores garantem uma segurança básica, porém a maioria dos serviços em nuvem não fornece criptografia segura. Se a configuração da segurança da nuvem for ruim, isso pode ser um convite para cibercriminosos. É um problema que atinge, principalmente, empresas que conseguem trabalhar com a nuvem, mas nem sempre conseguem aplicar configurações de segurança para atuar nesse ambiente.

Relatório 2021 X-Force Cloud Security Threat Landscape Report da IBM[44] aponta que cibercriminosos estão entrando pelas portas abertas que os usuários deixam em aplicativos, bancos de dados e podem ter interrompido dois terços dos ambientes de nuvem violados observados pela IBM. O relatório com dados de 2020 até o segundo trimestre de 2021 que aponta que dois em cada três ambientes de nuvem as violações foram causados por APIs (Application Programming Interface) configuradas incorretamente, APIs sem controles de autenticação que permitem que qualquer pessoa, incluindo atores maliciosos, acessem informações potencialmente confidenciais, APIs com acesso a muitos dados também podem resultar em divulgações inadvertidas. Na grande maioria dos testes de penetração na nuvem realizados pela IBM, a equipe observou um crescimento de 150% nos últimos cinco anos das vulnerabilidades em aplicativo. “Com quase 30.000 contas de nuvem comprometidas à venda na dark web e o Remote Desktop Protocol representando 70% dos recursos de nuvem à venda, os cibercriminosos têm opções prontas para automatizar o acesso a ambientes de nuvem.” aponta o relatório, ressaltando que a mineração de bitcoins e ransomware são os principais malwares em ambientes de nuvem, respondendo por mais de 50% dos sistemas comprometidos. Os testes de penetração em vários ambientes de nuvem encontraram problemas com senhas ou aderência a políticas, tanto que

44 https://securityintelligence.com/posts/x-force-report-hacking-cloud-environments/

dois terços das violações nas nuvens, provavelmente, teriam sido evitadas por sistemas robustos como a implementação adequada de políticas de segurança e aplicação de patches.

"As organizações precisam gerenciar sua infraestrutura distribuída como um único ambiente para eliminar a complexidade e obter melhor visibilidade da rede da nuvem à borda e vice-versa e adotar uma abordagem de confiança zero com urgência.", aconselha a IBM.

A segurança na nuvem(cloud security) é a proteção de dados, aplicações e infraestruturas. Em muitos aspectos segurança na nuvem (pública, privada ou híbrida) são os mesmos de qualquer arquitetura de TI tradicional, envolvem exposição e vazamento de dados não autorizados, controles de acesso fracos, suscetibilidade a ataques e interrupções na disponibilidade. As principais ameaças são:

✔ Quebra de perímetros

A segurança está relacionada ao acesso e são controladas nos ambientes tradicionais usando um modelo de segurança por perímetro. Em cloud computing estão altamente conectados, o que facilita a passagem do tráfego pelas defesas tradicionais de perímetro. Interfaces de programação de aplicações (APIs) não seguras, gerenciamento fraco de identidades e credenciais, invasões de conta e usuários internos mal-intencionados são ameaças ao sistema e aos dados. Para impedir o acesso não autorizado à nuvem, uma abordagem centrada nos dados pressupõe criptografia, processo de autorização, senhas fortes e a autenticação em dois fatores. Crie segurança em cada nível.

✔ Software

Cloud está relacionada aos recursos hospedados entregues ao usuário por meio de um software. As infraestruturas e todos os dados processados são dinâmicos, escaláveis e portáteis. Seja como partes inerentes das cargas de trabalho (por exemplo, criptografia) ou de forma dinâmica por meio de APIs e sistema de gerenciamento de nuvem, os controles de segurança precisam responder às variáveis do ambiente e acompanhar as cargas de trabalho e os dados tanto em repouso quanto em movimento.

✔ Malwares

Malwares cada vez mais sofisticados e outros ataques, como as ameaças persistentes avançadas (APTs), foram projetados para burlar as defesas de rede, tendo como alvo as vulnerabilidades no stack de computação. As violações de dados podem resultar em adulteração e divulgação não autorizada de informações. A responsabilidade dos usuários de nuvem é de se manter atualizado sobre as práticas de segurança e acompanhar os novos riscos.

✔ Responsabilidades compartilhadas

Independente do tipo de implantação de nuvem, uma das principais causas das falhas na segurança é a falta de diligência prévia e isso inclui usar

softwares confiáveis, entender a conformidade e governança dos dados, gerenciar os ciclos de vida, considerar a portabilidade, monitorar continuamente e manter uma equipe competente.

✔ “As nuvens públicas são seguras?”

As nuvens públicas oferecem a segurança apropriada para diversos tipos de carga de trabalho, mas não são adequadas para tudo, principalmente, por não ter o isolamento das nuvens privadas. As nuvens públicas oferecem suporte a múltiplos locatários, ou seja, aluga-se a capacidade de computação (ou espaço de armazenamento) do fornecedor de serviços de nuvem junto com outros. Cada um deles assina um SLA com o fornecedor, que documenta quem é responsável pelo quê. O fornecedor da nuvem se compromete a manter a infraestrutura, cuidar do acesso e proteger a privacidade. O usuário se compromete a não fazer nada que afete negativamente a integridade, por exemplo, executar aplicações não seguras. Embora a equipe de segurança de infraestrutura do fornecedor da nuvem fique de olho nos eventos incomuns, as ameaças escondidas ou agressivas – como ataques distribuídos de negação de serviço (DDoS) maliciosos podem afetar todos os usuários.
Há padrões de segurança, regulamentos e estruturas de controle aceitos pelo setor, como o Cloud Controls Matrix[45] da Cloud Security Alliance. Também é possível se isolar em um ambiente de vários usuários ao implantar medidas de segurança, como criptografia e técnicas de redução de DDoS, que protegem as cargas de trabalho contra uma infraestrutura comprometida. Se não for suficiente, recomenda-se implantar brokers de segurança de acesso[46] à nuvem

45 https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/
46 https://en.wikipedia.org/wiki/Cloud_access_security_broker

para monitorar as atividades e aplicar políticas de segurança em funções corporativas de baixo risco. Para setores que operam sob regulamentos rígidos de privacidade, segurança e conformidade e usam nuvens híbridas, as medidas de segurança estão muito relacionadas à tolerância a riscos e à análise do custo-benefício. Como os possíveis riscos e benefícios afetam a integridade geral da organização? O que é mais importante? Nem toda carga de trabalho requer o mais alto nível de criptografia e segurança. Por isso, cada vez mais empresas estão adotando as nuvens híbridas e a combinação de dois ou mais ambientes de nuvem (pública ou privada) interconectados. Com as nuvens híbridas é possível escolher a localização das cargas de trabalho e dos dados com base nos requisitos de conformidade, auditoria, política ou segurança. Mantendo as cargas confidenciais protegidas na nuvem privada e as operações mais comuns na nuvem pública. Desafios de segurança específicos da nuvem híbrida, como migração de dados, maior complexidade e extensa superfície de ataque. No entanto, a presença de vários ambientes é uma das defesas mais fortes contra os riscos à segurança.

Uma alternativa é a rede definida por software (SDN) que separa o plano de controle de rede do encaminhamento para permitir provisionamento automatizado e gerenciamento baseado em políticas de recursos de rede. A programabilidade é a base para a definição do que é SDN: as arquiteturas de data center com sobreposições definidas por software ou controladores separados do hardware de rede subjacente, oferecendo gerenciamento baseado em política ou intenção da rede como um todo. Isso resulta em uma rede de data center mais alinhada com as necessidades de cargas de trabalho de aplicativos por meio de provisionamento automatizado e mais rápido, gerenciamento de rede programática, visibilidade orientada a aplicativos abrangentes e, onde necessário, integração direta com plataformas de nuvem.

O desenvolvimento do SDN separa os planos de controle e dados, além de ter uma visão completa da rede, toma decisões de roteamento e comutação com base nessa visão, torna a automação das funções de rede mais fácil e permite o provisionamento e gerenciamento mais simples de recursos de rede.
Roteadores e switches de rede sabem apenas sobre os equipamentos de rede vizinhos, mas um ambiente SDN devidamente configurado torna-se uma entidade central que pode controlar tudo, desde a alteração de políticas até a simplificação da configuração e automação em toda a empresa. Os clientes podem ver todos os seus dispositivos e fluxos TCP, o que significa que eles podem dividir a rede do plano de dados ou gerenciamento para suportar uma variedade de aplicativos e configurações. Alguns controladores SDN são inteligentes para ver se a rede está ficando congestionada e, em resposta, aumentam a largura de banda ou o processamento para garantir que os componentes remotos e de borda não sofram latência. Há soluções SDN que centralizam e abstraem o controle e automatizam os fluxos de trabalho em muitos locais da rede e seus dispositivos aumentam a confiabilidade operacional, a velocidade e melhoram a experiência, além de permitir uma variedade de benefícios de segurança. Um cliente pode dividir uma conexão de rede entre um usuário final e o data center e ter diferentes configurações de segurança para os vários tipos de tráfego de rede. Uma rede pode ter baixa segurança voltada para o público que não toque em nenhuma informação sensível. Outro segmento poderia ter um controle de acesso remoto muito mais refinado com firewall baseado em software e políticas de criptografia que permite que dados confidenciais passem por ele.
SDN e a rede de longa distância definida por software (SD-WAN) permite às as empresas agreguem uma variedade de conexões de rede - incluindo MPLS, 4G LTE e DSL - em uma filial ou localização de ponta de rede e tenha uma plataforma de gerenciamento de software que pode ativar novos sites, priorizar o tráfego e definir políticas de segurança. O SD-WAN permite que as redes roteiam o tráfego com base em funções e regras gerenciadas

centralmente, independentemente dos pontos de entrada e saída, otimização de WAN avançada e firewalls com reconhecimento de aplicativo com total segurança. Para muitas empresas, a implementação de SD-WAN é parte de uma iniciativa maior de transformação digital que move funções de desenvolvimento de aplicativos, aplicativos de missão crítica, armazenamento, backups, recuperação de desastres e análise de dados na nuvem, além de permitir acessar esses recursos na nuvem de forma rápida, segura e eficiente.

6

Blockchain muito além do bitcoin

A maioria das pessoas associa a criptomoeda a cadeia de blocos, a confusão é natural, pois são termos muito próximos. Originalmente, a blockchain foi concebida como uma tecnologia financeira aplicada na criação do bitcoin, que foi o primeiro uso da blockchain, mas é errado pensar que blockchain e bitcoin são indivisíveis. O bitcoin é uma aplicação e blockchain uma tecnologia que vai muito além das criptos moedas e consegue gerar transformação em vários negócios e seu impacto deve se estender por toda a economia global graças à possibilidade de estabelecer novas formas de confiança de forma distribuída. O modelo de confiança atual é baseado em sistemas centralizados como no caso dos governos ou descentralizados como o sistema financeiro global, a blockchain permite a criação de confiança que não é centralizada nem descentralizada, é distribuída e por isso que esse sistema foi chamado de “confiança sem confiança”, ou "truthless trust”, no original em inglês.
As blockchains de maior impacto são as desenvolvidas por comunidades

abertas e mantidas como um projeto open source, descentralizado, transparente e auditável. É uma solução que não tem dono e precisa da comunidade para desenvolver os blocos e de cada vez mais pessoas se interessando pela tecnologia para prover soluções para vários segmentos econômicos.
De acordo com a multinacional de consultoria e auditoria PwC (PricewaterhouseCoopers) a tecnologia blockchain tem o potencial de aumentar o PIB global em US$ 1,76 trilhão na próxima década. A empresa acrescenta que a maior atividade do setor privado que se beneficiará do blockchain é rastreamento e logística com US$ 962 bilhões, mas funções públicas, como administração governamental, educação e saúde serão as que mais se beneficiarão. A tecnologia surgiu para gerar ganhos econômicos, e promove ganhos de eficiência e redução dos custos de transações, além de desafiar o papel dos intermediários nas mais diversas áreas, especialmente quando este intermediário é um depositário de confiança que se organiza de

forma centralizada ou descentralizada, por exemplo, desafiando o sistema financeiro tradicional.

Um pouco de história…

O bitcoin surgiu em 2008, após a crise financeira internacional, originada em meados de 2007 no mercado norte-americano de hipotecas de alto risco (subprime) que acabou por se transformar, após a falência do banco de investimentos Lehman Brothers, numa crise de confiança sistêmica. O desenrolar da crise colocou em xeque a arquitetura financeira internacional. Foi nesse cenário que surgiu o bitcoin, uma moeda virtual, com um funcionamento muito diferente de moedas como o dólar ou real, não existe de forma física e as transações não são controladas por instituições governamentais nem por bancos centrais de países, nem passa pelo Swift (Sociedade de Telecomunicações Financeiras Mundial) que faz a compensação de 70% das transações bancárias globais.

Criado por Satoshi Nakamoto, um pseudônimo que não se sabe se remete a uma única pessoa ou várias sem identidade conhecida, como um movimento anárquico com novas regras e formatação transgredindo os termos de negócios estabelecidos pela sociedade, possibilitando transações financeiras entre pessoas tirando a intermediação dos bancos, quebrando o *status quo* de quem detêm o poder de manter a sociedade do jeito que é.
Satoshi Nakamoto publicou um paper[47] tratando a questão da dependência bancária, escreveu o código do primeiro bloco do bitcoin, o Gênesis com a plataforma blockchain, mas o bitcoin só ganhou tração em 2011 devido ao processo de mineração que, de forma descentralizada a partir de cálculos matemáticos criados por computadores de alto desempenho fez com que o sistema financeiro dos bitcoins funcionasse.

Em 2014, um novo protocolo aberto para a construção de aplicações descentralizadas generalizadas (e não somente financeiras) foi inteiramente construído em torno da tecnologia blockchain: a Ethereum. Nesta, tornou-se possível também a criação do que se conhece hoje por contratos inteligentes, trechos de códigos capazes de operacionalizar registros mais complexos de propriedade e primeiras organizações autônomas (DAOs). Este feito evidenciou um mercado que cresce exponencialmente e o potencial das plataformas distribuídas, com a possibilidade de ir muito além dos sistemas de pagamento ou registros permitidos pela aplicação original da tecnologia no protocolo bitcoin.
Nakamoto foi o precursor da tecnologia ao juntar uma série de tecnologias desenvolvidas por outros cientistas ao longo dos séculos. Blockchain envolve criptografia, livro-razão, hash, assinatura digital, rede peer-to-peer (ponto a ponto), algoritmos de consenso e outras tecnologias que em conjunto fornecem a solução do blockchain. Por exemplo, em 1494 o frei franciscano

47https://bitcoin.org/bitcoin.pdf

Luca Pacioli (1445-1517) desenvolveu os primeiros estudos de matemática para serem utilizados em contabilidade e criou o livro-razão ou ledger que é o sistema padrão universal de débito, crédito e a composição de um balanço financeiro utilizado até hoje pelas empresas, governos, mercados mundiais e pela blockchain.
À medida que a internet deixou de ser utilizada apenas por militares e acadêmicos e, pouco a pouco, mais pessoas tiveram acesso e começaram a fazer transações na web ficou claro os problemas de segurança da rede e para minimizá-los, em 1971, Horst Feisel, um engenheiro da IBM criou um algoritmo de criptografia, denominado Lúcifer, baseado em um elevado nível de segurança e uma chave de codificar e decodificar. Três anos depois os colegas de Feisel da IBM melhoraram o Lúcifer para aumentar a segurança e criaram o Data Encryption Standard (DES).

Na década seguinte o DES foi adotado pela American Standard Institution para promover padronização de cifragem e procedimentos para serem utilizados em instituições financeiras. O DES algoritmo de criptografia de chave simétrica trabalha com chaves de 64 bits, embora a chave real seja de 56 bits, dos quais 1 em cada 8 bits servem de teste de paridade, para verificar a integridade da chave e para testar um dos bytes da chave por paridade ímpar, ou seja, cada bit de paridade é ajustado para ter um número ímpar de 1 no byte ao qual ele pertence. Já que 8 desses bits são redundantes são possíveis 256 chaves diferentes. O algoritmo executa várias operações, como combinações, substituições e permutações, para criptografar dados onde um conjunto de operações é aplicado 16 vezes em cada bloco de dados e, se tornou o principal algoritmo de chave única em 1981. Era inseguro e não evitava fraudes, vazamentos de informações e disponibilizava muitas informações pessoais do usuário do cartão.

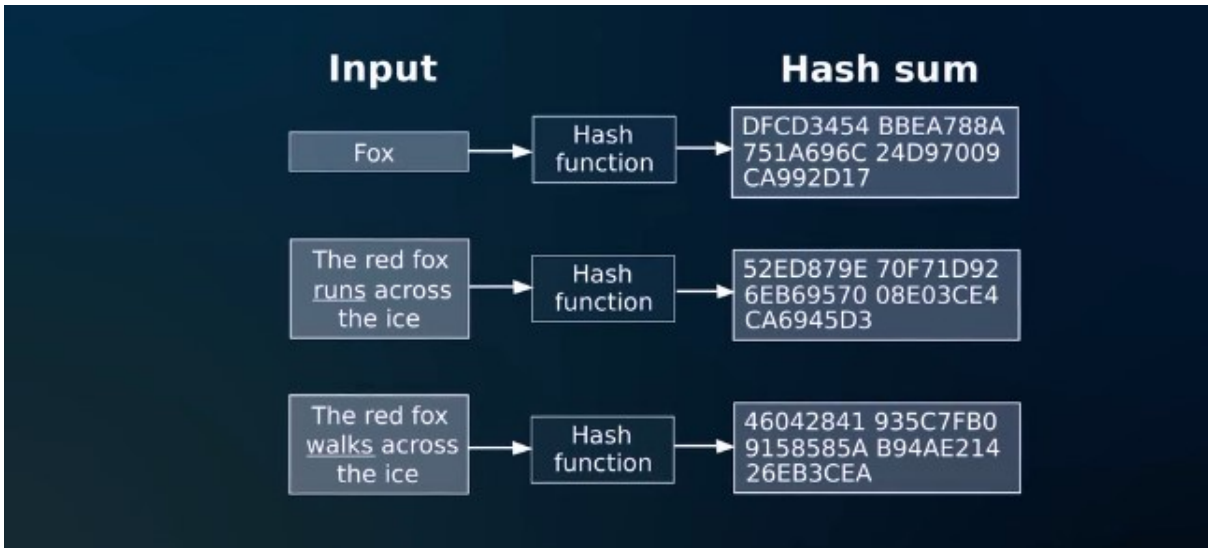
Em meados de 1983, David Chaum, cientista e entusiasta da criptografia, fundou a DigiCash, uma moeda eletrônica criptografada, chamada E-cash. A ideia era que os usuários obtivessem moedas digitais de um banco e não pudessem ser mais rastreados. A E-cash faria do papel-moeda, o dinheiro tangível em uma moeda digital que pudesse mudar de mãos de maneira segura e sigilosa. Um dos desafios das moedas digitais é justamente evitar o problema do gasto duplo, ou seja, que um ativo digital seja gasto duas vezes. Em um sistema centralizado, como uma instituição bancária tradicional, é simples resolver esse problema, mas em um sistema distribuído o grande salto dessa tecnologia havia dificuldades na solução do gasto duplo. Essa tecnologia foi tão precursora e libertária que praticamente fundou o movimento anarquista cypherpunk, no final da década de 1980. A ferramenta era boa e as grandes empresas de tecnologia se mostraram interessadas em adquiri-la. Chaum colaborou com vários outros estudos, propôs sistemas peer-to-peer (ponto a ponto) com criptografia e segurança.

Apesar dos avanços, a DigiCash faliu em 1998 e Chaum disse à época que “a tecnologia entrou no mercado antes que o comércio eletrônico fosse totalmente integrado na internet”.
A partir daí houve avanços em algoritmos de criptografia associada à expansão da internet para, de certa maneira, compensar a falta de segurança do protocolo ethernet. Na rede, a transmissão se dá por pacotes fragmentados e nas camadas da internet é possível haver perda de parte da informação dos pacotes e a criptografia de 64 bits de chave simétrica ou assimétrica válida integridade da informação é uma das tecnologias utilizadas para fazer blockchain funcionar.
A criptografia de chave simétrica ou de chave única utiliza a mesma chave para codificar e descriptografar os dados. É o procedimento mais simples de criptografia, já que o emissor e o receptor partilham somente uma chave de

transação. Oferece maior rapidez, simplicidade e menor segurança. Outro tipo de chave é a de criptografia de chave assimétrica, também denominada criptografia de chave pública que utiliza duas chaves distintas: uma pública, que pode ser divulgada, e outra privada, mantida em sigilo pelo seu dono, dessa forma a chave pública é utilizada para criptografar e a chave privada é utilizada para descriptografarc

Algoritmos de criptografia de chave assimétrica
RSA
DAS
ECC

Função hash



Fonte: Nano curso Blockchain Advanced - Fiap (https://www.fiap.com.br)

A criptografia tem uma função específica conhecida como hash. Este tipo de função é usado como bloco fundamental em muitas aplicações criptográficas e tem como comportamento básico receber um conjunto de dados de tamanho arbitrário, uma string de qualquer tamanho, podendo ter poucos ou muitos os caracteres, bytes ou gigabytes como input e produzir um valor hash de um tamanho fixo como output como forma de representação do dado de entrada, um identificador digital chamado valor hash.
O valor hash, geralmente, é formado por 16 bytes (no caso do MD-2, MD-4 e MD-5) ou 20 bytes (no caso do SHA-1), mas pode ser maior, embora não passe de 512 bytes.

O conceito teórico por trás do hash é a transformação de uma grande quantidade de dados, por um algoritmo matemático, em uma sequência de bits, representada em base hexadecimal, se porventura algum dado dessa base for adulterado, no momento do cálculo do hash haverá incompatibilidade, indicando que os dados foram adulterados.
O hash pode ser comparado a um dígito verificador, ou algoritmo de controle, promovendo um mecanismo que assegura a autenticidade das informações, integridade e a autenticidade das mesmas.

Exemplos de algoritmos de hash
MD4 ➔ 128 Bits
MD5 ➔ 128 Bits
SHA-1 ➔ 160 Bits

RIPEMD-160 ➔ 160 Bits

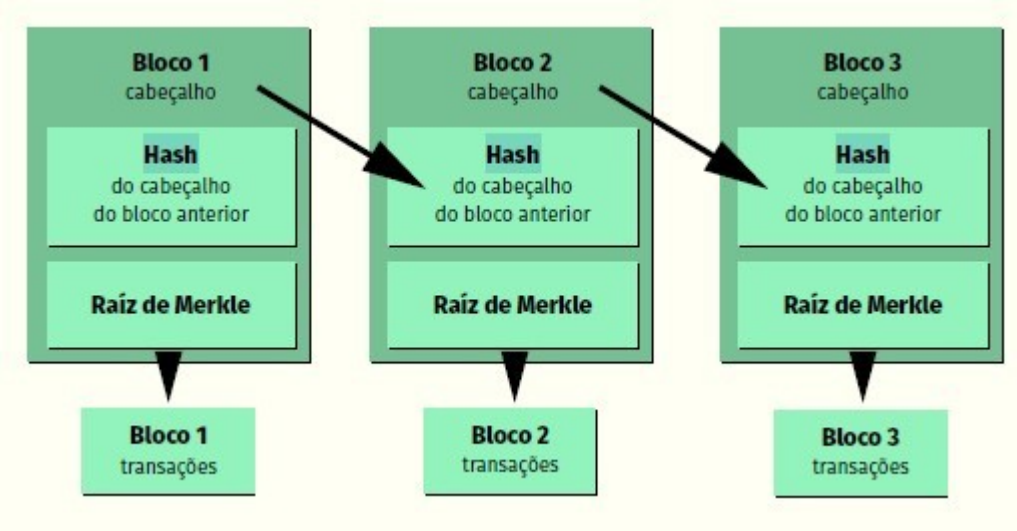
A origem do termo blockchain advém do fato da plataforma armazenar as transações em blocos interligados entre si, formando uma cadeia. A plataforma Blockchain usa a função hash (identificação exclusiva do bloco) em cada bloco processado, e todos os blocos processados e os que serão processados no futuro se baseiam no hash do bloco anterior e assim sucessivamente. Cada bloco processado gera um hash próprio uma cadeia de processamento interligada, ou seja, se qualquer informação for alterada em um bloco, irá denunciar o conflito com o hash do bloco e dos blocos antecessores e sucessores e é justamente todo esse processamento em blocos que torna a cadeia inviolável com o atributo de chave de imutabilidade.

Sintetizando:

- Blockchain gera uma cadeia de registros imutáveis, distribuídos e públicos.
- Cadeia, pois os registros processados no blockchain encontram-se encadeados uns aos outros.
- Imutáveis, uma vez que o registro é inserido em uma cadeia não pode ser alterado.
- Público, disponível na internet.
- Distribuídos, por tratar-se de uma rede P2P que se trata de uma estrutura distribuída sem um servidor central.

As transações na Blockchain são como de Árvores de Merkle, em criptografia e ciência da computação árvores de Merkle, também denominada Merkle Root, são o hash raiz de uma estrutura de dados, ou estruturas de dados utilizadas para criar um resumo de dados com integridade criptograficamente verificável de forma eficiente quando em poder da raiz de Merkle - que vai no cabeçalho

de cada bloco - e de um caminho de Merkle. Para formar a raiz desta árvore binária com as transações, cada transação tem o seu id (o hash da transação) concatenado ao id da transação vizinha na árvore é submetida a uma dupla rodada da função hash SHA- 256 sucessivamente até chegar à raiz.



Fonte:https://itsrio.org/pt/publicacoes/blockchain-para-aplicacoes-de-interesse-publico

Cada bloco que compõe a estrutura do blockchain possui uma área destinada às transações que são feitas nele e outra área destinada ao armazenamento do cabeçalho, que por sua vez possui o hash do bloco anterior e a raiz da árvore de Merkle das transações presentes no bloco.

ACs

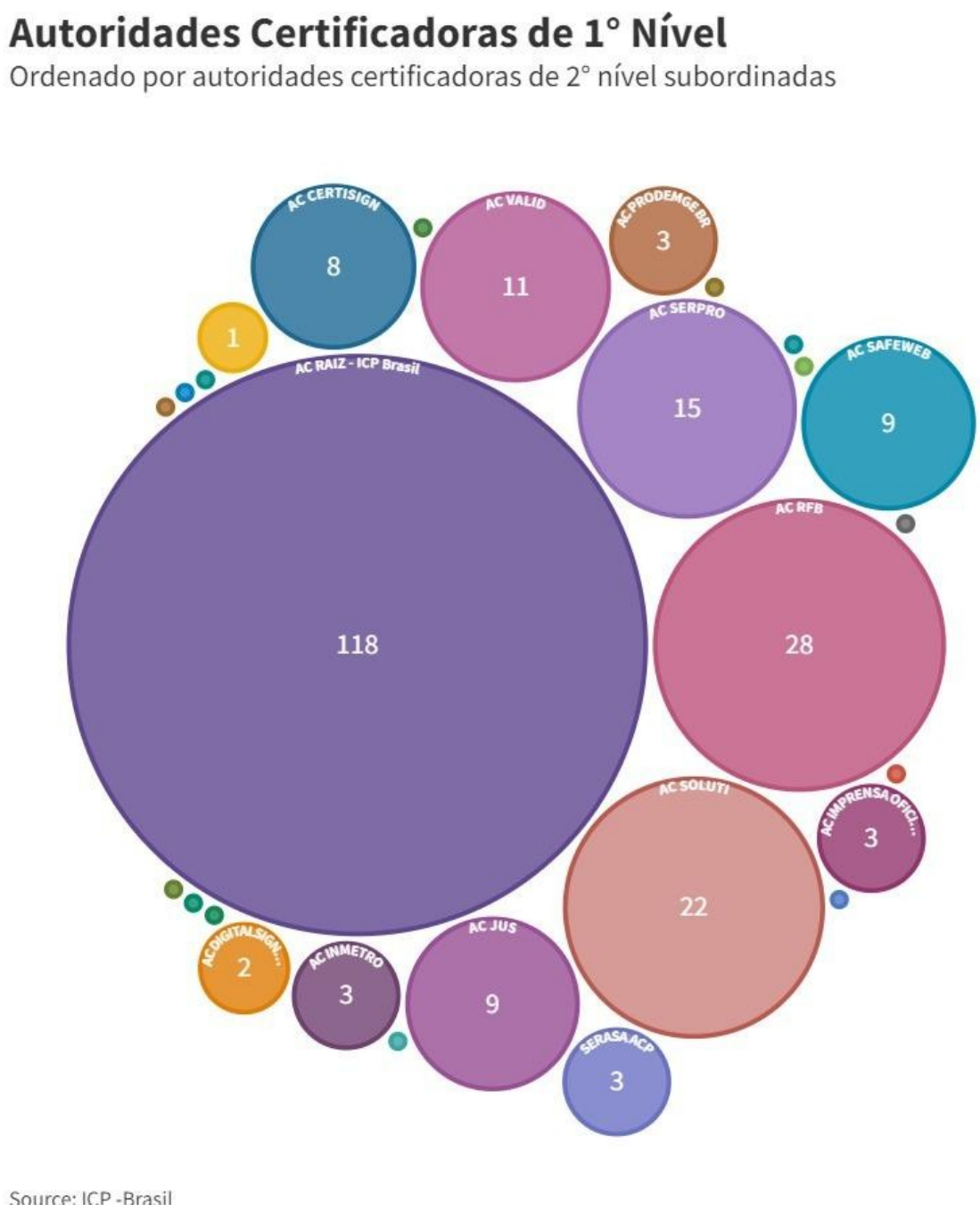
O Certificado Digital é a identidade digital da pessoa física e jurídica no meio eletrônico. Ele garante autenticidade, confidencialidade, integridade e não repúdio nas operações realizadas por meio dele, atribuindo validade jurídica. Por identificar no meio digital permite que diversos serviços sejam realizados sem a necessidade da presença física, significando agilidade nos processos, sustentabilidade e redução de custos. No sistema criptográfico brasileiro[48], a

48 https://estrutura.iti.gov.br/

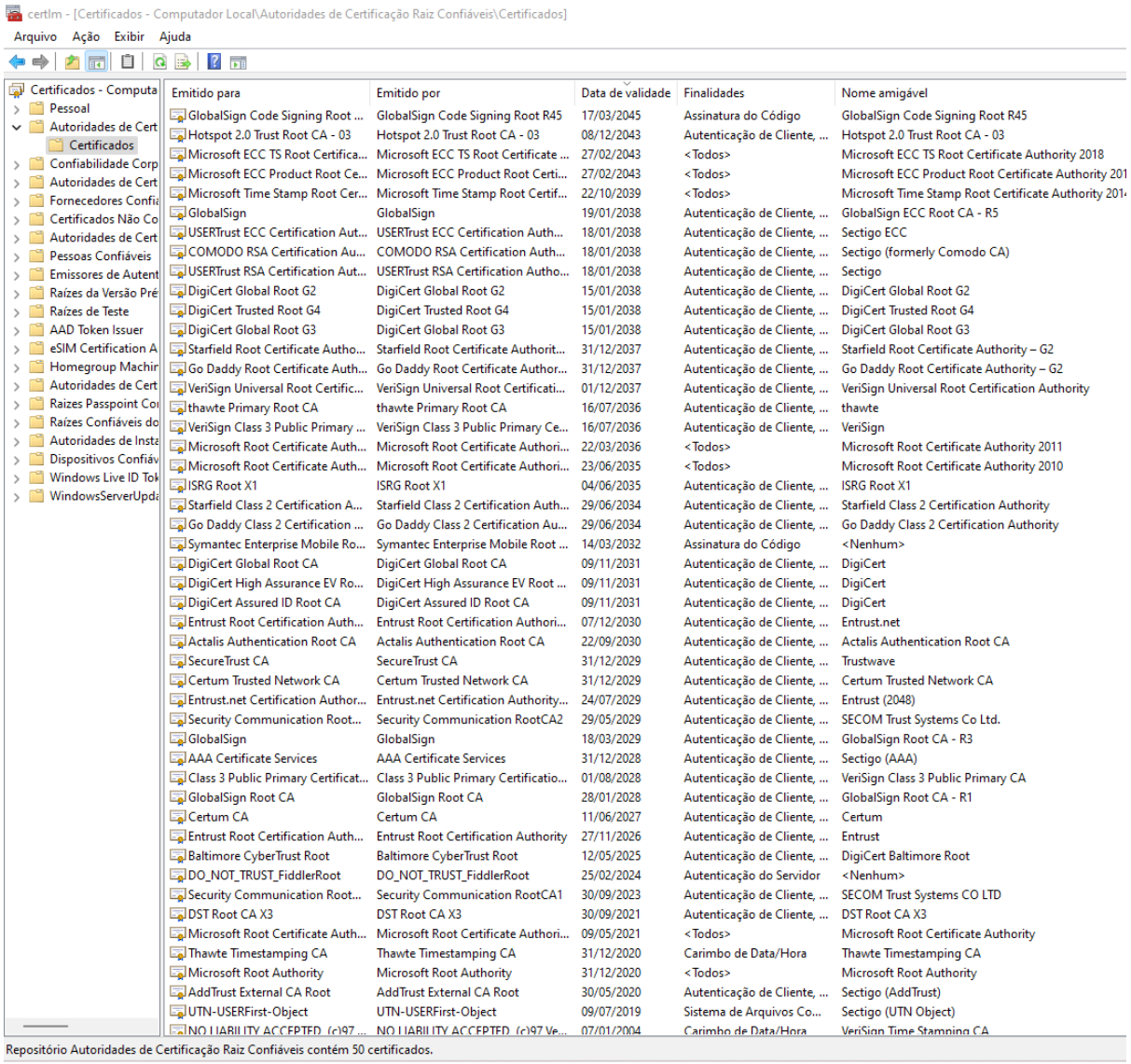
infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é a principal autoridade em certificação digital, é um conjunto de entidades, regulamentos e procedimentos criados para sustentar o sistema criptográfico e a base da segurança dos certificados definidos em conjunto com o Instituto Nacional da Tecnologia da Informação (ITI).

O ICP-Brasil é a Autoridade Certificadora Raiz (AC-Raiz) responsável por definir as regras seguidas pelas por outras ACs subordinadas a ela. Uma autoridade certificadora é uma entidade, pública ou privada, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais dos solicitantes. Sem autoridade certificadora sem certificado digital.
As ACs de primeiro nível emitem certificados para as ACs de segundo nível e estas emitem certificados digitais para pessoas físicas, jurídicas e para páginas da internet. Porém, a lei permite que entidades sem vínculo com a ICP-Brasil elaborem suas próprias normativas de segurança para emitir certificados digitais para uso interno em empresas ou órgãos públicos, para uso externo as

ACs exercem o monopólio, assim como, os cartórios no mundo físico nos serviços registrais.



As ACs controlam certificados emitidos e revogados, estes vão para uma Lista de Certificados Revogados (LCR) e também devem manter os registros das operações de cada certificado seguindo as normas do ITI para garantir a credibilidade e a segurança do certificado digital.



O ano de 2021 terminou com quase 11 milhões de certificados ativos no país graças à expansão da digitalização de processos no centro das estratégias de negócio. A certificação digital usa chaves criptográficas e permite aos usuários da rede realizarem transações eletrônicas com segurança, integridade e privacidade.

ICP BRASIL	A ICP-Brasil é uma cadeia de confiança, que viabiliza a emissão de Certificados Digitais para a identificação do cidadão.
ITI — Instituto Nacional da Tecnologia da Informação (ITI)	Tem o papel de credenciar e descredenciar os participantes da cadeia, supervisionar e fazer a auditoria dos processos. Ele faz interface direta com as Autoridades Certificadoras (AC).
AC — Autoridade Certificadora	AC tem como responsabilidade emitir, renovar ou revogar os Certificados Digitais e credenciar as ARs para o atendimento aos clientes.
AR — Autoridade de Registro	A AR está abaixo da Autoridade Certificadora (AC) e tem como missão receber o cliente para realizar conferência da documentação e emissão do Certificado.

A AC-Raiz possui o selo Webtrust SSL Baseline – Secure Socket Layer for Certification Authorities. ACs de todo mundo passam por processos de auditoria e recebem este selo que garante a segurança na aplicação da tecnologia de Infraestrutura de Chaves Públicas, mundialmente reconhecida por PKI (Public Key Infrastructure) que garante a conformidade e a manutenção dos certificados da AC-Raiz nos repositórios dos navegadores de internet.

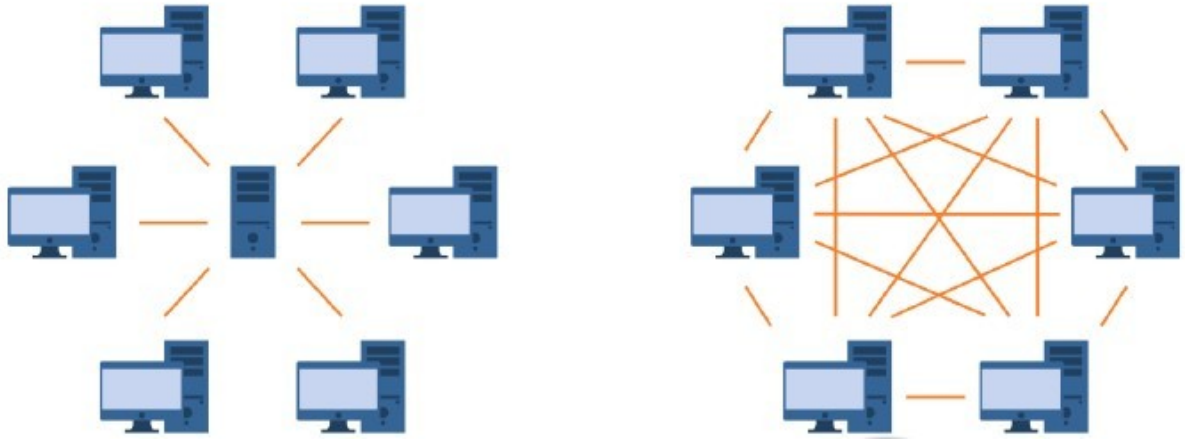
Nem tudo é tão seguro e autêntico nos certificados digitais. Ao acessar sites que envolvam troca de informações sensíveis como internet banking, serviços de pagamento, armazenamento em nuvem, os usuários estão garantindo a criptografia dos dados trafegados em rede, mas não assegura a autenticidade do site acessado. Basta que um ator mal-intencionado crie um clone do site original para ter acesso aos dados e nesse caso não adianta o conteúdo ser embaralhado se a troca não está acontecendo com o site correto.

Outro problema é o compartilhamento de tokens, senhas e e-CPFs que ameaça ainda mais a segurança e leva a questionamentos e dúvidas se o documento foi realmente assinado pela pessoa que detém o certificado. Outro ponto falho dos certificados digitais é a quantidade de erros e bugs que ocorrem por problemas de compatibilidade entre o certificado digital e as versões de sistema operacional, de navegadores de internet, de PDFs e arquivos incompatíveis e até mesmo incompatibilidade de drivers que atrapalha o funcionamento dos sistemas.

As ACs realizam a assinatura digital de certificados digitais atestando a identidade é um processo matemático que garante ao navegador web que a AC realmente garantiu a autenticidade do certificado, mas quem decide quais autoridades certificadoras são reconhecidas é o próprio navegador. Quando um certificado digital não tem a assinatura de uma AC confiável ou simplesmente não tem uma assinatura, o navegador exibirá uma mensagem informando que o site não é seguro.

Nem todos os navegadores confiam nas mesmas ACs. Além disso, existem listas de revogações de certificado distribuídas pelas ACs e interpretadas pelos navegadores. Daí tantas mensagens de aviso de sites não seguros.

Rede P2P



Fonte: Nano curso Blockchain Advanced - Fiap (https://www.fiap.com.br)

Na imagem, a esquerda representa uma rede cliente-servidor e a direita uma estrutura P2P (ponto a ponto), uma estrutura de redes de computadores e internet em que não há um servidor definido para armazenamento e compartilhamento das informações, ou seja, todos os computadores que participam da estrutura exercem o papel de cliente e servidores. A principal função técnica é a transmissão e compartilhamento de arquivos em grande escala de forma descentralizada, em que cada estação é um nó da rede.

Os dados existentes nesse nó podem ser compartilhados com outros vários nós conectados, sendo que cada nó possui uma parcela de responsabilidade pelos recursos de processamento e tráfego das informações. Dessa forma, todos os participantes são responsáveis por armazenar e manter a base de dados existente. A arquitetura Blockchain, utiliza a estrutura de rede P2P justamente por ser uma tecnologia:

- Descentralizada
- Compartilhada
- Com vários nós participando do processamento
- Distribuída
- Segura

Diferentemente dos sistemas contábeis tradicionais, a blockchain trabalha com o conceito de contabilidade de tripla entrada, na qual a variável tempo é inserida e anexada a todas as transações, de modo que estas sejam localizadas e ordenadas em uma ordem específica. Cada transação é codificada e carimbada com data e hora, permitindo o rastreamento de todos os blocos da corrente, além de garantir que as transações não sejam alteradas. Essa lógica de encadeamento de blocos que possuem informações de transações passadas, somada ao caráter de imutabilidade do sistema permite que qualquer transação possa ser rastreada.
A segurança do sistema é garantida pela criptografia, no caso da blockchain do bitcoin, os dados presentes no bloco não são criptografados.
As informações são armazenadas abertas, sendo possível acompanhar o bitcoin desde sua geração, passando por todas as carteiras até o presente momento. Não existe sigilo bancário: todas as movimentações são públicas, para quem quiser olhar. O que é mantido em segredo é a identidade dos donos das carteiras, que são identificados com um identificador alfanumérico longo, a chave pública do par de chaves.

O sigilo na rede bitcoin é, portanto, parcial, pois o proprietário da carteira é anônimo, mas suas transações são todas conhecidas. É possível identificar o dono da carteira ao cruzar informações adicionais: por exemplo, compras pagas com bitcoins.
Em síntese a arquitetura é de uma grande rede sincronizada de transação de dados, um banco de dados único, público, compartilhado, sincronizado, disponível para acesso por qualquer nó da rede que tem uma cópia das transações. Esse banco de dados contém informações entrelaçadas entre si, cada bloco criado é registrado e são vinculados uns aos outros para aumentar a confiabilidade das informações. O fato de ser imutável cria um vínculo entre as partes envolvidas sem a necessidade de uma instituição que garante a integridade ou faça a intermediação dessas transações e tudo isso é feito através de uma rede P2P que redireciona os conteúdos para esse banco de dados público.
É possível fazer uma analogia com um cofre transparente, todos podem ver o que está dentro do cofre e ele continua seguro porque ninguém consegue alterar ou retirar a informação dele.

A tecnologia blockchain está baseada em quatro pilares:

- Segurança das operações realizadas.
- Descentralização do armazenamento.
- Integridade de dados.
- Imutabilidade de transações

A tecnologia blockchain também é conhecida como “ledger of facts” ou livro de fatos, sendo que:

- O Ledger pode ser denominado o livro de registro digital, e uma vez validado um registro inserido neste livro, ele não poderá ser mais removido.

- O Fact (fato) denomina as transações que ocorrem dentro da plataforma.
- Os nós são os membros/integrantes da rede blockchain e podem ser anônimos ou não.
- Bloco que constitui um conjunto de fatos.
- Cadeia de blocos ou um conjunto de blocos encadeados.

Toda transação que ocorre dentro da blockchain é protegida pelas tecnologias que compõem a plataforma, isto é, criptografia, assinatura digital, certificado digital, hash, redes P2P.

Públicas e privadas

As redes blockchain podem ser privadas (permissioned) ou públicas (permissionless). As redes privadas são plataformas fechadas que atendem à demanda de um grupo, para participar do bloco, precisa ser convidado ou ter permissão para ter acesso a ele. Por se tratar de uma estrutura privada a atualização dos blocos é mais ágil, uma vez que existe um número limitado de participantes que concorrem ao fechamento e atualização dos blocos. Suas principais aplicações são voltadas a ambientes corporativos e fechados.
As redes blockchain públicas são plataformas abertas, ou seja, qualquer pessoa pode se tornar membro e armazenar, enviar e receber dados, após baixar o software compatível.

Algoritmo de Consenso

Um mecanismo de consenso é um algoritmo que serve para criar um novo bloco num ambiente descentralizado de forma consensual entre os nós da rede P2P. Como todos os nós que participam do blockchain compartilham a mesma base de dados, quando uma nova transação é efetuada, precisa ser validada e

sincronizada com os demais nós que participam da estrutura, para que isso ocorra dentro da plataforma, deve-se eleger um líder, ou seja, um dos nós que atualizará o Ledger, o restante dos nós acompanham o líder. O algoritmo de consenso é um dos pilares da atualização blockchain, pois é ele que promoverá a decisão de quem será o líder para cadeia de blocos. Graças a descentralização é possível criar ambientes em que as partes envolvidas em uma transação podem fazê-lo diretamente, sem a necessidade de um terceiro de confiança, as partes realizam suas atividades diretamente (ponto a ponto) e as outras dezenas, centenas ou milhares de partes servem de testemunhas de que aquilo realmente aconteceu. As atividades realizadas ou valores mudando de mãos são registradas simultaneamente por todas as partes em um livro-razão idêntico para todos.

A confiabilidade das operações é garantida por consenso. Mesmo que haja partes maliciosas que queiram fraudar as operações registradas, elas são uma minoria que será desconsiderada. A descentralização de uma rede de Blockchain é um dos princípios inegociáveis para o pleno funcionamento da tecnologia. Quanto mais membros independentes uma rede blockchain possuir, mais segura será. Se alguém possuir mais de 51% dos membros de uma rede, pode confirmar operações fraudulentas ou mesmo reescrever o livro-razão. O nome que se dá a isso é de ataque dos 51%.

Cada membro da rede P2P do blockchain possui uma cópia idêntica e completa desse livro-razão que não é estático, mas escrito a todo instante. O ledger é dividido em blocos que contêm as transações, operações ou dados que devem ser registrados. Sempre que novas informações precisam ser registradas, um novo bloco deve ser criado, preenchido, validado é posicionado no final do livro-razão, incrementando esse grande documento. Esses blocos são encadeados de tal maneira que a assinatura usada para validar o bloco anterior é necessária para validar o novo bloco. É esse encadeamento é o que torna o blockchain imutável, já que a alteração ou

remoção de um dado já registrado necessitaria de uma revalidação do bloco em que o dado está e todos os blocos gerados posteriormente.

A cada novo bloco é eleito um membro que ganha o direito de registrar os dados no bloco, cabendo aos demais a função de validá-lo.

São vários os algoritmos de consenso aplicados para esse fim, cada um com suas vantagens e desvantagens:

Uma das formas da blockchain criar consenso é por meio de um processo chamado prova de trabalho (Proof of Work [PoW]), que consiste em resolver um desafio matemático, que é então demarcado no tempo, assinado criptograficamente e distribuído ao longo de toda a rede, o que impede sua adulteração. Aplicado no consenso de Nakamoto é um protocolo criptográfico criado para prevenção de ataques cibernéticos de negação de serviço (denial of service) e spam. Satoshi Nakamoto adaptou os conceitos de prova de trabalho para que funcionasse como um algoritmo de consenso que passou a ser conhecido posteriormente como consenso de Nakamoto (Nakamoto consensus). No consenso de Nakamoto a cada bloco um líder é eleito de modo randômico, uma abordagem de loteria por ser totalmente aleatória. Na rede bitcoin, um enigma criptográfico é proposto pelo protocolo, e os membros que participam dessa rede se propõem a decifrá-lo. Basicamente, o enigma é a execução de uma função hash SHA-256 utilizando alguns dados específicos do bloco atual e um número aleatório(também conhecido como nonce), que, aliado às informações do bloco, deve resultar em um hash iniciado por um número de zeros. Se o número de zeros em questão não for obtido, a função hash deve ser testada utilizando outro número aleatório.
Esse processo de adivinhação exige milhões de tentativas em um único segundo e esse processo de descoberta leva em torno de dez minutos para

acontecer. Os participantes de rede competem entre si para ser o primeiro a adivinhar esse número.

O nó que conseguir primeiro comunica imediatamente a todos os demais participantes qual é o número aleatório que, por sua vez, param de utilizar números aleatoriamente e usam o número informado para validar a vitória do reclamante. Confirmada a solução do enigma, os participantes da rede, em consenso, elegem esse nó como líder.

O líder eleito tem o direito de determinar quais transações de bitcoin não confirmadas irão compor o novo bloco; as transações realizadas e não confirmadas do bitcoin formam uma fila que o membro líder deve consultar. Em 2019, o tamanho exato do bloco era de apenas 1MB, espaço capaz de armazenar aproximadamente três mil transações por vez. Todas as demais transações não escolhidas para confirmação no novo bloco permanecem na fila de espera e serão confirmadas nos blocos seguintes.

Escolhidas as transações, o vencedor propaga o bloco formado pelos demais participantes e eles armazenam o bloco no final da corrente e se preparam para o próximo. O conceito de prova de trabalho está na solução do enigma criptográfico, para encontrar o número um alto poder computacional empregado.

Por se tratar de um blockchain público, membros podem entrar e sair da rede de bitcoin a qualquer momento, sendo assim, é possível que novos membros façam esse processo de validação. O líder do bloco (e somente o líder) ganha uma recompensa em bitcoins. Para não inundar o sistema econômico gerando todos os bitcoins de uma vez, novas unidades são geradas e inseridas no sistema a uma taxa constante.

São essas novas unidades da moeda que são entregues aos líderes do consenso seguindo o princípio econômico que diz que para algo ser considerado valioso, ele precisa ser finito e escasso. Os bitcoins não poderiam ser gerados

indefinidamente e, por essa razão, o sistema foi programado para parar de gerar novas unidades quando o total atingir 21 milhões de unidades.

Para tal, como pode ser visto no próprio código-fonte do bitcoin no Github[49], a seguinte linha:
Consensus.nSubsidyHalvingInterval = 210,000
O que significa que a cada 210 mil blocos gerados, acontece um evento conhecido como halving, que faz a recompensa cair pela metade. A rede começou com a recompensa de 50 BTC por bloco, caindo para 25 BTC em quatro anos, 12,5 BTC quatro anos seguintes e, a partir de 2020, a recompensa passou a ser 6,25 BTC. Nakamoto considerou a condição desses validadores de rede aos mineradores de ouro, que empregam recursos para adicionar mais ouro em circulação no mercado, e é por essa razão que os participantes são chamados de mineradores (miners), mas o principal papel dos mineradores é a validação das transações no blockchain.
Quando o último bitcoin for gerado em algum momento no ano de 2140, Nakamoto prevê que a mineração continuará graças às taxas de rede, um valor que os emissores de transação pagam para ter prioridade em suas confirmações. Os mineradores investem em equipamentos que adivinhem o nonce cada vez mais depressa, aumentando suas chances de serem escolhidos. Existem hardwares especializados conhecidos como ASICs (Application Specific integrated circuit, ou circuito integrado de aplicação específica) que, diferentemente de desktops ou laptops criados para múltiplos propósitos, são concebidos especificamente para mineração de bitcoins.
Os altos preços atingidos pelo bitcoin tornaram a atividade altamente rentável e a corrida criptográfica se tornou uma corrida por hardware. Se em seu início a mineração de bitcoin era possível utilizando as placas de vídeos de computadores comuns, há vários anos isso se tornou inviável.

49 https://github.com/bitcoin/bitcoin

Agora usa-se equipamentos como a Bitmain Antminer S9i com 189 chips é capaz de chegar a 14.5 TH/s, ou seja, ela pode chutar mais de 14 trilhões de nonces em um único segundo

As ASICs custam, em média, dois mil dólares a unidade. É possível formar um cluster com esse tipo de equipamento, aumentando as chances de se tornar líder do bloco.

ASICs para a mineração de bitcoin

Fazenda de mineração, provavelmente, na Ucrânia com centenas de ASICs

Se por um lado a escala de hardware torna o blockchain do bitcoin mais seguro ao obrigar provas de trabalho cada vez mais complexas, por outro, torna-o inseguro ao centralizar cada vez mais a atividade na mão de poucos participantes. O altíssimo custo da prova de trabalho da blockchain do bitcoin também é sua principal força. Em agosto de 2018, somente a rede de blockchain do bitcoin consumiu 1% da energia elétrica gerada no planeta.
A rede de blockchain do bitcoin consome entre 55,63 e 73,12 TeraWatts/h de eletricidade por ano, se o bitcoin fosse um país, o consumo energético seria compatível com países como a Colômbia ou o Chile.
No caso específico do bitcoin há um problema de escalabilidade.
Cada bloco minerado possui apenas 1 megabyte de espaço disponível para registrar as transações financeiras, o que possibilita três mil transações em média. Como cada bloco é minerado a cada dez minutos (e cada vez que o poder computacional sobe a dificuldade para adivinhar o nonce também sobe proporcionalmente), a rede dessa criptomoeda seria capaz de validar apenas

sete transações por segundo, o que o inviabilizaria para uma série de aplicações. O consenso de Nakamoto é, por concepção e design, um consenso mais lento para maior controle da geração sistemática de blocos encadeados.

Proof of Stake (PoS)

Em 2011, um usuário do fórum bitcoin talk chamado Quantum Mechanic propôs um novo algoritmo de consenso chamado Proof of Stake. Embora a abordagem também envolva a eleição de um líder de forma aleatória os candidatos a líder deixam de fazer investimentos em hardware e passam a fazer investimentos no próprio cripto ativo que deve ser validado.
O candidato a líder se compromete a trancar na rede uma quantidade de cripto ativos que servirá de garantia das transações que ele se propõe a validar. Dessa forma, caso o líder eleito valide transações fraudulentas, ele é punido pois sua garantia (stake) será utilizada para sanar eventuais prejuízos. Trata-se de uma evolução em relação à prova de trabalho aplicada no consenso de Nakamoto: embora a rede possua mecanismos para rejeitar transações fraudulentas, o responsável pela fraude não é punido, ele está livre para realizar novas tentativas no futuro. O stake que permitisse o gasto duplo ou ataques de 51%, abalaria a credibilidade do cripto ativo o que se refletiria rapidamente em desvalorização, logo, os validadores são os maiores interessados em manter a saúde do sistema. Proof of stake também recompensa os validadores com mais cripto ativos. Seja um algoritmo de consenso proof of work ou proof of stake há sempre a tendência à centralização. Manter o sistema descentralizado é um desafio para qualquer ecossistema de blockchain.

A rede Ethereum[50] procura manter esse equilíbrio com um conjunto de smart Contracts e o consenso dessa plataforma é chamado de Casper PoS.
E se o dinheiro fosse programável? E se uma o dinheiro pudesse vir atrelado a às suas próprias regras ou condições? A rede Ethereum foi concebida para responder essas perguntas, mantido pela Ethereum Foundation, uma organização sem fins lucrativos na Suíça, o Ethereum é uma plataforma descentralizada que roda contratos inteligentes, permitindo que aplicações rodem exatamente conforme foram programadas previamente, sem a possibilidade de atraso, censura, fraude ou interferência de terceiros.
Para manter o incentivo de mineração da rede criou-se um token chamado ether para viabilizar seu funcionamento.

Smart Contracts

A tecnologia do blockchain traz uma variedade de outras propostas de aplicação, uma das mais promissoras são os smart contract ou contratos inteligentes que seriam uma evolução para a prevenção de fraude. Publicado na plataforma Ethereum, os contratos inteligentes herdaram uma característica da blockchain: não pode ser alterado ou modificado.
O contrato inteligente é um acordo entre as partes cuja execução é automática, e essa automação é realizada por um código de computador, escrito na linguagem de programação Solidity[51], que traduz um discurso legal em um programa executável.

50 https://ethereum.org/
51 Solidity, a linguagem usada na plataforma Ethereum é uma linguagem de programação orientada a objetos e em alto nível. Influenciada por C + +, Python e JavaScript. Assim como a linguagem Java, o Solidity é uma linguagem compilada e interpretada ao mesmo tempo: o código-fonte escrito na linguagem é armazenado em arquivos .sol e são submetidos a um compilador chamado Solidity Compiler (solc) e se transformam em bytecode; esse contrato compilado e publicado na plataforma Ethereum, que possui um interpretador conhecido como Ethereum Virtual Machine (EVM), que é responsável por interpretar este bytecode.

O algoritmo verifica com suas estruturas condicionais se determinadas condições foram satisfeitas e, caso tenham sido, automaticamente executa os termos estipulados no contrato. Os Smart Contracts permitem que as partes interessadas se comprometam previamente com os termos a serem executados sem, no entanto, determinar uma autoridade central (um sistema judicial) para fazer valer sua execução.
Como não pode ser modificado, o contrato precisa ser destruído (rescindido) ou abandonado e um novo deve tomar o seu lugar. Dessa maneira, há garantias de que o contrato será executado exatamente com as condições que foram previamente estabelecidas, de forma compulsória.
Essa tecnologia tornou possíveis novas aplicações com por exemplo:

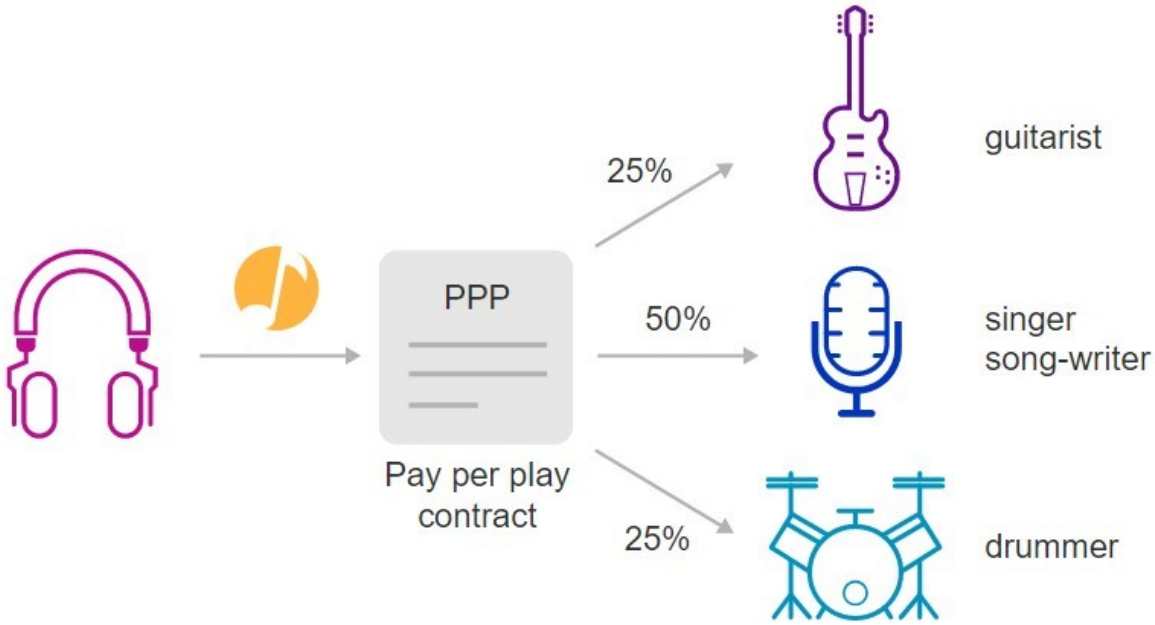
- OpenBazaar

Em funcionamento desde 2014, o OpenBazaar uma plataforma de comércio eletrônico ponto a ponto (P2P), ligando compradores e vendedores diretamente sem intermediários, taxas ou restrições para seu uso.
Por funcionar em uma rede descentralizada, as informações dos anúncios e das transações realizadas não ficam em servidores centrais ou sites, funcionando em uma rede similar à rede Onion, do navegador Tor. Para acessar o marketplace, existe um navegador web capaz de acessar os anúncios e, para comodidade, possui uma carteira de criptomoedas embutida, a fim de realizar os pagamentos em bitcoin, Bitcoin Cash ou Zcash (o vendedor escolhe em qual criptomoeda quer receber).
Quando acontece uma venda, é estabelecido um contrato inteligente entre comprador e vendedor para a garantia das partes envolvidas. O sistema permite o ranqueamento de seus membros e a qualificação de vendedores após as compras, como em qualquer e-commerce. O OpenBazaar não é uma empresa, é uma comunidade de software livre promovendo a inovação na forma de comprar produtos pela internet.

- Arcade.city, o Uber sem o Uber

O Arcade.city é a primeira iniciativa bem-sucedida de uma rede de viagens P2P, ou seja, motoristas e passageiros são conectados ponto a ponto. A iniciativa em Austin já está em funcionamento há alguns anos, prestando o serviço de deslocamento seguro sem incidentes.
Por consequência desse modelo, os motoristas são livres para definirem suas próprias tarifas, criar sua própria rede de clientes frequentes ou oferecer serviços adicionais, como entregas ou viagens. Assim como os concorrentes, o Arcade.city permite a avaliação de motoristas e passageiros, formando um sistema de reputação que garante mais segurança aos envolvidos.

- Musicoin, direitos autorais fonográficos



A indústria musical sofreu várias revoluções ao longo das décadas: desde o

fonógrafo de Thomas Edison, que gravou a primeira voz humana, passando pelo walkman da Sony, os CDs, o iTunes e, finalmente, no modelo vigente, os streamings como o Spotify, YouTube Music, Amazon Music, Deezer e vários outros. Entretanto, essas novas gigantes, por vezes, acabam ditando "suas regras para o mercado" e, assim, vários artistas acabaram declarando guerra ao Spotify e à Apple Music queixando-se do baixo valor de repasse desses grandes serviços. Outro fator a ser levantado são os números apresentados pelos serviços, afinal, quando o Spotify diz ao artista que sua música foi executada X milhões de vezes e, por consequência irá receber Y, pergunta-se até onde esses números correspondem à realidade, afinal, são esses mesmos serviços que realizam as apurações. Não resta ao artista outra alternativa senão confiar no intermediário.

O Musicoin que propõe um modelo de remuneração ao artista com base em um contrato PPP (pay-per-play, ou pagamento por execução), ou seja, toda vez que uma música for executada, um valor será enviado para a remuneração dos artistas, o contrato autogerenciável já faz a divisão financeira automaticamente. Cada música tem o seu próprio contrato com uma distribuição diferente, ou seja, em outra música do mesmo álbum, podemos ter outra pessoa como compositor da letra, recebendo 10%, um produtor recebendo 15% e assim por diante. Os ouvintes não precisam necessariamente pagar por execução, embora os artistas sejam remunerados dessa maneira. Em seu modelo de negócio existe uma criptomoeda que é minerada, conhecida como Musicoin (MUSIC), e 15% da recompensa pela mineração vai para um fundo chamado Universal Basic Income (UBI) que remunera o artistas quando a música é gratuita no streaming do Musicoin e esse fundo remunera o artista.

- Smart Governance, votação 2.0

Há sempre suspeitas de fraude em qualquer eleição realizada em qualquer

lugar do mundo, há muita coisa em jogo, os vencedores têm acesso a dinheiro e muito poder, assim, os sistemas de votação sempre levantaram suspeitas, especialmente dos perdedores. Existem várias propostas para o uso de smart contracts em sistemas de votação inteligentes e suas propriedades de imutabilidade sem que haja controle por nenhuma das partes tornam as eleições uma aplicação perfeita para a tecnologia.
A Open Vote Network[52] (Rede de Votação Aberta) é para as eleições de diretoria e está escrita como um contrato inteligente para a Ethereum.
É a primeira implementação que não depende de qualquer autoridade confiável para calcular o registro ou proteger a privacidade do eleitor. Trata-se de um protocolo auto-organizado, e cada eleitor está no controle da privacidade de seus próprios votos, de tal forma que só podem ser violados por uma conclusão completa envolvendo todos os outros eleitores. A execução do protocolo é aplicada usando o consenso mecanismo que também protege o blockchain da rede Ethereum. Além de garantir a privacidade, o contrato traz transparência ao processo de apuração, pois, ao verificar as condições em que os votos foram apurados, é possível garantir que 1 pessoa = 1 voto. Ao utilizar um blockchain como infraestrutura para que o sistema de votação seja realizado, reduz-se drasticamente quaisquer fraudes que possam hoje ser realizadas em sistemas eleitorais tradicionais. A tecnologia garante transparência e auditabilidade.

Outras aplicações da blockchain

52 MCCORRY, P.; et al. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. https://eprint.iacr.org/2017/110.pdf

As blockchains e smart contracts são tecnologias relativamente novas, cerca de uma década, mas estão em ascensão em outros setores além das criptomoedas, a aplicação como moeda e sistema financeiro sem intermediários ainda é a aplicação mais famosa da tecnologia há várias outras possibilidades e novas iniciativas de uso das blockchain são anunciadas e, muitas prometem causar disrupção no mercado em que estão inseridas.

- Cópias de segurança

A Redundância de informações é fundamental para evitar perdas de dados e nada tem mais backups do que uma blockchain, o caso do bitcoin é o melhor exemplo com todos os nós da rede têm a posse de uma cópia completa, atualizada e integral de todos os blocos e informações registradas por ele. Para a informação se perder, todos os nós teriam que ser comprometidos de alguma forma e, sendo assim, quanto mais membros o blockchain tiver, mais segura a informação estará.

- Registros virtualmente inalteráveis com hash

As informações em um blockchain são incrementais e acumulativas, armazenadas de forma a não ser alteradas ou apagadas.Tecnicamente é possível alterar ou apagar informações, no caso do bitcoin o esforço financeiro e consenso da rede descentralizada composta por milhares de nós independentes, torna as alterações praticamente impossíveis.

- Resiliência do sistema

A rede peer-to-peer, sem servidores centrais, torna a rede extremamente resiliente. O BitTorrent, que trabalha com o mesmo tipo de rede descentralizada, é um exemplo. Embora esteja sob fogo cruzado das

gravadoras e estúdios de cinema por causa dos direitos autorais, em uma rede P2P é virtualmente impossível proibir esses compartilhamentos.
Enquanto uma rede possuir pelo menos dois participantes, continuará funcionando.

- Eliminação de intermediários

Permitir a troca de informações (ou valores) de maneira direta, seu funcionamento elimina a necessidade de intermediários ou um terceiro de confiança. Estas características podem ser aproveitadas para dezenas de aplicações diferentes como:

- Autenticidade de documentos

Garantir a autenticidade de documentos é algo custoso, especialmente no Brasil, e ser caro não garante que o processo é à prova de falhas ou fraudes, pois sempre que houver um fator humano que possa ser corrompido e subverter o sistema, a fraude será possível. A startup brasileira OriginalMy[53] tem com uma proposta: registrar documentos em um Blockchain, beneficiando-se de, pelo menos, duas características importantes: o fato de que o registro do documento não possa ser alterado ou removido e a transparência que um blockchain público provê, permitindo a verificação deste registro sem burocracias e a um custo menor. Documentos oficiais, ideias, patentes, letras de música ou livros podem ser registrados em um blockchain para comprovação de autoria posteriormente, ou seja, desempenha um dos papéis de um cartório de registro.
Como os serviços de cartório no Brasil exercem monopólio dos registros cartoriais e sem legislações que acompanhem as inovações tecnológicas, a OriginalMy possui um serviço adicional de registro notarial em um cartório tradicional.

53 https://originalmy.com/

De acordo com a Legal Architect Camila Rioja Arantes no programa Legal Talks[54] da OriginalMy, já existem ganhos de causas na justiça brasileira da qual as provas estavam registradas em blockchain.
Caso um sistema notarial de algum país fosse implementado integralmente em um único blockchain, além de mitigar fraudes por adulteração ou remoção de informações, todos os documentos poderiam ser verificados e confrontados.
Existem outras iniciativas de autenticação de documentos na internet, como é o caso do site LexisNexis[55], que também registra os documentos de maneira a comprovar sua autoria futura.

- Protegendo direitos autorais fotográficos

Fotografias são copiadas na internet e garantir os direitos autorais dos fotógrafos é um desafio enorme graças a fotografia digital e a facilidade para compartilhamento de dados que possibilitou o livre trânsito de textos, fotos e vídeos sem pagamento de direitos autorais para os profissionais que criaram as obras. A Kodak que, em 2012, declarou falência por ter ignorado o advento da fotografia digital, criou o Kodak moment propondo o uso o uso de cripto ativos e o blockchain para garantir direitos autorais para fotógrafos que podem registrar seus trabalhos em uma blockchain, que impede o registro seja alterado ou apagado. O registro da foto em um blockchain pode comprovar um eventual plágio fotográfico, permitindo identificar o autor da obra com facilidade. A solução que foi batizada de KodakOne[56] também possibilita um marketplace para licenciamento o uso da imagem, comprovando o direito de uso da imagem e também garantindo que os royalties cheguem às mãos certas. Para tal, ambas as partes utilizarão um cripto ativo chamado de Kodak Coin.

54 https://www.youtube.com/watch?v=qCeMLTK6ncM
55 https://risk.lexisnexis.com.br/
56 https://kodakone.com

A empresa também promete fazer uso de big data, inteligência artificial e web crawling para raspar a web verificando o uso devido ou não destas imagens. O site Binded.com é outra iniciativa para proteger os direitos fotográficos utilizando Blockchain de maneira simples e rápida.

- Registros imobiliários

Os custos da intermediação da compra e venda de imóveis são elevadíssimos, no Brasil e há em muitos países sistemas de registros imobiliários frágeis e, por sua, vez fraudes que vão desde a falsificação de registros, imóveis vendidos para múltiplos compradores e até funcionários corruptos que fraudam registros ao fazê-los de forma retroativa. A Costa Rica é um dos países da América Central que mais sofrem com fraudes imobiliárias, embora não seja o único. Por que não utilizar a blockchain para registros imobiliários? Um blockchain único utilizado por todas as partes que realizem registros imobiliários em um país tornaria este processo muito mais seguro e verificável do que é hoje e os custos para tal poderiam ser drasticamente diminuídos. A empresa Ubitquity[57] criou o primeiro blockchain para realizar registros imobiliários de maneira segura. O sistema foi testado nas cidades de Pelotas e Morro Redondo no Rio Grande do Sul. Outros testes pilotos têm sido realizados por outras startups em outros países, como a startup ChromaWay na Suécia.

- Alternativa ao Seguro tradicional

Os seguros são caros por diversas razões, entre elas, a quantidade de assaltos, furtos, acidentes e fraudes envolvendo os bens segurados. A brasileira Mutual.Life é uma insurtech que usa a tecnologia de blockchain e inteligência artificial para garantir a segurança dos valores e transparência dos processos

57 https://www.ubitquity.io

envolvidos. A empresa promove o chamado “seguro peer-to-peer”, uma vez que o membro do grupo atua como segurador e segurado ao mesmo tempo. A falta de regulação é um obstáculo em busca de respaldo jurídico aos membros dessa rede, o excesso de regulamentação, nesses casos, representa um obstáculo à inovação.

- Segurança na cadeia logística

Uma das grandes aplicações do blockchain é para a cadeia logística de suprimentos. Entre outros riscos, há a possibilidade do bem ser falsificado ou extraviado. Quais as garantias de que o suprimento chegou a uma determinada unidade de distribuição ou que alguns passos do itinerário tenham sido removidos para facilitar o extravio ou falsificação? A empresa Blockverify[58] faz uso do Blockchain para registrar a movimentação de produtos de alto valor (como bolsas de grife, diamantes, entre outros produtos) em um blockchain, desta forma, o itinerário dos bens não pode ser alterado ou mesmo apagado. Além disso, a empresa se utiliza de IoT, utilizando RFID para registrar os itens para evitar falsificações. As tags também permitem registrar a movimentação do item automaticamente, tornando o processo logístico mais eficiente e rápido, mitigando as possíveis fraudes no processo.

- Aplicações descentralizadas (DAPP)

58 http://www.blockverify.io

Quem usa smartphone usa aplicativos para as mais diferentes necessidades: serviços bancários, pedir comida, chamar carros por aplicativo e muitas outras aplicações, com o advento dos contratos inteligentes surgiu uma nova proposta de arquitetura para aplicações, chamada de DAPP(decentralized application), em português, aplicações descentralizadas. Em DAPP, as aplicações possuem parte de sua programação, o front-end (instalados nos smartphones, como geralmente o são), mas a programação mais pesada, conhecida como back-end, roda em um blockchain em uma rede descentralizada P2P. Desta forma, as DAPPs se tornam verdadeiras aplicações compartilhadas e não é possível, nem aos próprios desenvolvedores, modificar condições e regras já estabelecidas. Embora seja algo recente, o site State of the Dapps[59] já traz mais de mil e seiscentas aplicações descentralizadas.

- DAO e as Smart Nations

Uma DAO (Decentralized autonomous organization) ou Organização Autônoma Descentralizada), possibilita criar empresas e organizações em que as regras e os processos sejam codificados em contratos inteligentes. A internet tornou nossa comunicação veloz e a distância e as fronteiras geopolíticas irrelevantes para trabalhar, fazer compras, consumir entretenimento, fazer negócios e, talvez o conceito de nação precise ser revisto ou expandido com o conceito de DAO para as Smart Nations
Algumas pessoas, especialmente libertários com a filosofia “Imagine all the people sharing all the world”[60], começam a se organizar em nações virtuais, ou seja, as nações físicas (com suas fronteiras geopolíticas) e verdadeiras nações lógicas, em que as pessoas escolhem se organizar de maneira diferente, escolhendo assim o conjunto de regras que deseja seguir. O exemplo mais amigável para entender as smart nations seria de uma empresa com dois ou mais sócios morando e operando em diferentes países. Qual legislação seguir?

59 https://www.stateofthedapps.com/
60 Verso da música Imagine de John Lennon

E se houver conflitos onde resolvê-los? Essas e outras questões são definidas pelos sócios em contratos inteligentes.

Tokens não fungíveis, os NFTs

Um artista digital anônimo chamado Pak fez história em 2 de dezembro de 2021 ao vender sua série de obras de arte digitais intitulada The Merge por US$ 91,8 milhões. Um total de 28.983 colecionadores compraram 312.686 tokens não fungíveis, ou NFTs, da obra.

Mas o que é um NFT, um token não fungível? O termo “não fungível” significa que um NFT não pode ser substituído. Uma nota de um dólar, por exemplo, é fungível porque pode ser trocada por outra nota idêntica de um dólar. Uma carta Pokémon rara não é fungível, pois é única e não pode ser substituída por outra carta Pokémon genérica. NFTs são como cartas de Pokémon raras porque não são fungíveis ou substituíveis.

As NFTs são uma tecnologia disruptiva porque são únicas, escassas e fornecem rastreamento seguro de propriedade. Um NFT é único porque contém assinaturas digitais da mesma maneira que a arte da vida não virtual exibe a assinatura de um artista ou é autenticada por especialistas. As pessoas podem simplesmente realizar uma captura de tela de um NFT, mas o NFT original permanece autêntico para sempre graças à assinatura digital. A assinatura digital de um NFT é o equivalente virtual de uma assinatura física sob uma pintura. NFTs são escassos e não podem ser substituídos por algo semelhante porque não existe nada semelhante. A escassez, por sua vez, tem sido um dos principais fatores impulsionadores da demanda por NFTs.

É uma situação ganha-ganha: os criadores podem tornar seu trabalho mais valioso e monetizá-lo, e os usuários podem possuir um ativo digital com um conjunto exclusivo de tecnologia digital. Alguns argumentam que os NFTs escassos e de edição limitada vão contra os princípios de ampliar o acesso e promover o acesso a domínio público. NFTs podem ser oferecidos ao público sob uma licença Creative Commons, assim como NFTs de edição limitada. Isso permite que os artistas se beneficiem financeiramente e o público tenha acesso gratuito.

Um conjunto exclusivo de tecnologia de dados NFT também acompanha a propriedade. Isso é feito através do blockchain. Uma vez que o conteúdo digital é adicionado ao blockchain, cada transação ou venda do NFT é registrada na cadeia. A maioria dos NFTs faz parte do blockchain Ethereum, mas outros blockchains podem implementar sua própria versão de NFTs. Isso significa que há um registro de preço e histórico de propriedade facilmente acessível e imutável para o NFT. Antes era mais difícil para os artistas digitais protegerem seus trabalhos ou maximizarem seus lucros, com a inovação do NFT, artistas digitais podem proteger seus trabalhos exclusivos por meio do blockchain. Em vez de se preocupar com a reprodução de seus trabalhos sem a devida compensação, os artistas podem investir mais tempo na criação de suas peças.

NFTs são essencialmente contratos inteligentes que vivem em blockchains. Eles contêm informações criptografadas. As informações criptografadas tornam o NFT único: uma impressão digital exclusiva, um hash do item, seu nome, seu símbolo e muito mais. Quando o NFT é armazenado no blockchain o criador da arte e do NFT, e o único detentor do acesso ao hash exclusivo que o trabalho representa, torna-se o proprietário final desse token exclusivo.

O blockchain, por sua vez, torna o NFT imutável e permite que o token seja comprado/vendido entre pessoas na blockchain, também acompanhando todas as transações realizadas sobre o NFT criado.

Como criador, as informações armazenadas na blockchain são um fator determinante, pois além de armazenar as propriedades do NFT, ele acompanha tanto o proprietário atual quanto todos os proprietários anteriores do NFT, permitindo que o criador inicial, monetize cada transação feita em seu NFT.

NFTs abrangem o mundo das representações digitais, como música, arte, GIFs, etc. A aplicação mais popular de NFTs é a arte digital e a memória esportiva. À medida que muitas indústrias se tornam cada vez mais digitais, quase tudo tem o potencial de se tornar um NFT. Jack Dorsey, fundador do Twitter, vendeu seu primeiro tweet como NFT por quase US$ 3 milhões e o Top Shot agora está vendendo momentos da NBA como NFTs. Usuários individuais agora estão gerando NFTs de forma criativa: um par de tênis, uma redação, um nome de domínio, um ingresso que dá acesso a um evento e até mesmo um imóveis.

Os NFTs também estão ligados ao metaverso, mundos digitais onde NFTs representam ativos digitais. Imagine que cada edifício, território ou mesmo objeto no metaverso seja um NFT. Isso significa que os NFTs não apenas representam e comprovam a propriedade dos itens, mas também conduzem todas as transações monetárias que podem ocorrer dentro do metaverso. Atualmente, games são o aspecto mais popular do metaverso, mas o metaverso está destinado a expandir seu uso para todos os cantos de nossas vidas. Especialistas da Bloomberg Intelligence estimam que o metaverso global gerará cerca de US$ 800 bilhões em receita até 2024.

Os NFTs também fazem parte do desenvolvimento de interações gratuitas e acessíveis no metaverso e continuarão a crescer juntos. Embora digitais, ainda são uma classe de ativos semelhante a imóveis ou arte física. Portanto, os NFTs estão sujeitos a restrições legais, como direitos de propriedade, requisitos de direitos autorais, prevenção de fraudes, precauções de segurança cibernética e responsabilidades contratuais. Dois dos problemas mais comuns na arena dos NFTs são fraude e regulamentação de valores mobiliários.

Fraudes e golpes complexos em plataformas NFT são uma preocupação crescente. Embora as NFTs reduzam a barreira de entrada para artistas e criadores, elas também representam um desafio de responsabilidade.
Por exemplo, plataformas como Open Sea, o maior mercado de NFT do mundo, têm um processo relativamente rápido para se inscrever e criar NFTs. Os processos da Open Sea incluem requisitos de autenticação e verificação menos onerosos em comparação com outras plataformas tradicionais de transações online que exigem que os usuários comprovem sua identidade, forneçam informações de conta bancária e enviem outros documentos. As contas do Open Sea não são todas verificadas, portanto, os golpes são mais prováveis do que outras plataformas com processos de registro mais rigorosos. Muitos especialistas dizem que são necessários mais protocolos de segurança e diligência para evitar fraudes no espaço NFT.
A classificação de um ativo como títulos é fundamental porque os títulos são um instrumento financeiro que tem um preço e pode ser negociado como ações e títulos. A maioria dos NFTs não são classificados como títulos, mas isso pode mudar com o tempo ou com decisões judiciais. Complicações legais também surgem quando falamos sobre NFTs e questões de segurança cibernética. Por exemplo, o Open Sea também foi envolvido em uma controvérsia em setembro de 2021, quando os usuários de repente perderam dinheiro em carteiras digitais porque alguém postando arte NFT incorporou a arte com código malicioso. Os usuários clicavam no NFT e aceitavam um "presente" que roubava dinheiro das contas dos usuários. Ameaças como essas precisam ser rigorosamente investigadas e remediadas por plataformas NFT como a Open Sea. É necessário mais orientação legal e regulatória para promover a confiança e a segurança das plataformas NFT. Há muitas questões não resolvidas, mas o ambiente legal e regulatório crescerá rapidamente para acomodar o uso crescente de NFTs.