CyberTech Report

Desafios da Cibersegurança no Brasil

#1 | JULHO | 2021

Sua opinião é muito importante para nós

Queremos saber quais foram as suas impressões, críticas e sugestões sobre este relatório. Além disso, também gostaríamos de saber quais outros estudos você teria interesse que o dataminer realizasse.

Quer falar com a gente? É só encaminhar um e-mail para: inside@distrito.me

Metodologia

As startups delineadas no report foram selecionadas a partir de um trabalho minucioso de pesquisa e consulta ao banco de dados de startups proprietário do Distrito. Também foram realizadas consultas a bancos abertos e informações públicas do governo. As startups foram examinadas individualmente para verificar adequação ao tema do report e informações públicas do governo.

As startups foram examinadas individualmente para verificar adequação ao tema do report e aos critérios de seleção estabelecidos. São eles:

- Ter a inovação no centro do negócio, seja na base tecnológica, no modelo de negócios ou na proposta de valor.
- Estar em atividade no momento da realização do estudo, medido pelo status do site e atividade em redes sociais.
- Desempenhar atividade diretamente relacionada ao setor estudado.
- Ter nacionalidade brasileira e operar atualmente no Brasil.

O trabalho de definição das categorias foi baseado em análise da literatura relevante e das classificações utilizadas amplamente no mercado, no Brasil e no mundo. A definição da categoria a que pertence cada startup foi feita por nossa equipe, e, quando operada em mais de uma categoria, a situamos na que interpretamos como sua atividade principal ou de maior visibilidade.

Também temos uma preocupação em incluir somente aquilo que consideramos startups - e por mais que nosso critério para defini-las seja bastante amplo, excluímos alguns tipos de negócio que, embora muitas vezes se autodenominem startups, acabam fugindo do conceito. Isso inclui empresas que têm como característica principal serem:

- Software Houses (desenvolvimento de software sob demanda)
- Consultorias
- Agências de marketing, publicidade e design

Enfatizamos aqui que os números expostos podem sofrer alterações conforme a evolução da acurácia das informações e maior capacidade de interação com as próprias startups ao longo do tempo.

Entrevistados

Fernando Zamai
Regional Sales Leader Cybersecurity
Cisco

Leonardo Militelli
CEO
GAT Infosec

Kaique Bonato
Founder & CEO
Sentinela

Josemando Sobral
Co-Founder
Unxpose

Daniel Ibri
Co-Founder & Managing Partner
Mindset Ventures

Sumário

Para navegar pelos capítulos deste estudo, **clique nos botões na margem superior**. A qualquer momento, **clique no logo do Distrito no canto inferior direito para voltar a esta página**.

Introdução

Introdução

O ano de 2020 foi extremamente difícil e transformador. Em meio a crise sanitária e econômica que foi agravada em diferentes frentes do país e no mundo, o momento se transformou em gatilho de aceleração digital que agilizou ainda mais o processo de digitalização das estruturas produtivas e da economia de uma forma geral. Com a vasta adoção do modelo de home office desde o ano passado, não só nossa maneira de trabalhar mudou, como também,as formas de nos protegermos de ataques cibernéticos. Dessa forma, os investimentos em Cybersecurity das companhias tiveram de acompanhar essa transformação, tendo em vista a maior exposição de seus dados devido ao compartilhamento entre diversos computadores que não possuem necessariamente os mesmos padrões de segurança. Com isso, diversos meios de proteção foram adotados, tais como a contratação de redes virtuais privadas (VPN), simulações de ataques virtuais, automação de diversos processos, entre outros.

O mercado global de Cibersegurança atualmente é estimado em US$ 176,5 bilhões e é esperado crescer aproximadamente 12,5% anualmente nos próximos 5 anos, conforme exposto no portal Ciso Advisor. O Brasil ainda está em processo de desenvolvimento e amadurecimento, mas a pandemia acelerou o processo de crescimento de um ecossistema que está presente em cada vez mais setores produtivos.

Nesse primeiro Inside Cybertech, focamos em contextualizar a importância da temática, principalmente frente a realidade trazida pela pandemia. Iremos trazer informações desse novo contexto e explicar melhor como o setor funciona e quais são as tendências para o futuro. Ademais, vamos introduzir o ecossistema de cibersegurança no Brasil, bem como colocar em pauta o que está acontecendo no panorama internacional e quais são as tendências do setor.

Esperamos que esse estudo traga visibilidade para uma área que não para de crescer e cada dia se torna mais importante na realidade da economia digital. Agradecemos mais uma vez a colaboração e o apoio da Cisco em todo o projeto.

Boa leitura!

Contextualização

O que é cibersegurança e como ela se tornou uma das pautas mais importantes na era da economia digital?

Categorias

NETWORK & INFRASTRUCTURE SECURITY
Companhias que apliquem processos de proteção da infraestrutura de rede, instalando medidas preventivas para negar acesso não autorizado, modificações, exclusões e roubo de recursos e dados. Essas medidas de segurança podem incluir controle de acesso, segurança de aplicativos , firewalls, redes virtuais privadas (VPN), análise comportamental, sistemas de prevenção de intrusão e segurança sem fio. Se relaciona com a camada física de transmissão e conexão. Também englobamos soluções de endpoint e messaging security nesta categoria

WEB SECURITY
Medidas e protocolos de proteção que empresas utilizam para proteger suas organizações de cyber criminosos e ameaças que usam a web como canal. Se relaciona com a camada não física de segurança, o que engloba internet e segurança de sites.

APPLICATION SECURITY
Medidas de segurança que impedem roubo/sequestro de dados e códigos dentro de dentro de aplicativos e plataformas.

DATA PROTECTION
Data protection engloba empresas responsáveis pela proteção de informações sensíveis à empresa (Banco de Dados, Informações de Corporações) e enquadram às corporações na LGPD.

MOBILE SECURITY
Empresas que atuam com produtos e serviços voltados a garantir a segurança do device (dispositivo móvel), IoS, Android. Via de regra, são companhias que visam a proteção contra ameaças associadas à conexões wireless.

SECURITY OPERATIONS & INCIDENT RESPONSE
Empresas que desenvolvem soluções estruturadas para responder a vazamentos de dados ou ciberataques. A solução visa minimizar os impactos de ataques cibernéticos já realizados, possibilitando um controle da situação com o menor tempo e custo.

IOT SECURITY
Empresas que atuam com segurança relacionada a internet das coisas, aparelhos e networks que estão conectados entre si.

IDENTITY & ACCESS MANAGEMENT
Empresas que desenvolvem soluções que garantem a veracidade das informações e identidades de todas as partes envolvidas em um processo. Aqui se encontram empresas de Identidade as a Service, que capturam, armazenam e asseguram a veracidade do usuário, e companhias de assinatura digital, que trazem inovação e segurança para todo o ciclo de documentos.

Categorias

BLOCKCHAIN
Blockchain as a Service (BaaS) são empresas que possibilitam o desenvolvimento de produtos digitais com a tecnologia blockchain, instalando, hospedando e/ou mantendo redes desse tipo em nome de outras organizações.

FRAUD & TRANSACTION SECURITY
Empresas que aplicam tecnologias de análise de dados para gerar avaliações e insights sobre clientes, permitindo mapear riscos, analisar a conformidade com leis e regulamentações e se prevenir contra perdas, desvio, fraude e ataques cibernéticos.

CLOUD SECURITY
Cloud Secutiry refere-se às startups que atuam com políticas, tecnologias, aplicativos e outros mecanismos de controle utilizados para proteger IP virtualizado, dados, aplicativos, serviços e a infraestrutura associada de computação em nuvem.

SECURITY CONSULTING & SERVICES
Security Consulting and Services refere-se a startups que prestam serviços para testar ou aprimorar serviços de cibersegurança. Um exemplo aqui são empresas que atuam com simulações de ataques cibernéticos como forma de identificar possíveis falhas nos sistemas.

Economia Digital já movimenta 25% dos negócios no mundo

O progresso tecnológico experimentado pela sociedade no século XXI é seguido por uma disseminação em massa de novas tecnologias digitais, com o crescimento da importância dos dados e uma democratização crescente da internet. Essas transformações permitiram uma conexão maior entre pessoas, empresas e organizações, de forma que a comunicação se tornou mais eficiente. A incorporação todos os agentes em um novo modelo social junto a essas práticas já citadas são as características fundamentais da Economia Digital. Como consequência, os processos de transformação e produção, infraestrutura das corporações e os próprios modelos de negócio buscam se adaptar à realidade digital. Aproximadamente 25% dos negócios no mundo já acontecem na nova economia digital, e estima-se que aproximadamente US$ 100 trilhões serão movimentos nos próximos dez anos em todas as cadeias produtivas.

Nesse cenário, as maiores empresas do mundo, antes pautadas em modelos de negócio tradicionais, como General Motors e Stantand Oil, foram substituídos por gigantes tecnológicos, como Google, Amazon, Microsoft e Facebook. No Brasil, a Nubank se tornou o maior exemplo de digitalização de um modelo de negócios antes tradicional no segmento bancário, e recentemente captou US$ 400 milhões em sua Series G , se tornando a 7º startup mais valiosa do mundo. Ademais, deve-se destacar que as práticas de isolamento social e os efeitos da pandemia no Brasil e no mundo aceleraram ainda mais o processo natural de digitalização da economia em praticamente todos os setores. Entretanto, em um mundo cada vez mais digital e conectado, torna-se cada vez mais essencial discussões e soluções sobre cibersegurança e privacidade de dados

Cibersegurança se tornou essencial em um mundo conectado

Em um mundo de economia digital, a cibersegurança se apresenta como prática de proteger sistemas e ativos de informação, tais como computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados. Segundo o *Framework do National Institute of Standards and Technology*, ameaças em *cybersecurity* exploram a complexidade e conectividade dos sistemas críticos de infraestrutura digital. Suas competências são resumidas em: identificar, proteger, detectar, responder e recuperar.

Soluções complexas e diversas surgem e ganham cada vez mais força em um contexto de cadeia produtiva digital, como *firewalls*, antivírus, monitoramento remoto de rede de corporações, criptografia, confirmação e gerenciamento de identidade, dentre outras. De acordo com um levantamento realizado pela PWC, o fator principal de limitação de crescimento do mercado de segurança frente às demandas crescentes é justamente a formação de profissionais, que são disputados entre as corporações. Nesse estudo, estima-se que em 2021 cerca de 3,5 milhões de potenciais empregos em segurança da informação ficarão vagos, devido a falta de profissionais qualificados na área.

Home Office se tornou a forma de trabalho mais utilizada pelas empresas na pandemia

O ano de 2020 transformou o universo corporativo, as organizações tiveram que readequar o modelo de trabalho e continuar garantindo produtividade, sustentabilidade e segurança para seus colaboradores. Ao mesmo tempo que os horizontes de trabalho foram expandidos, não mais se limitando às fronteiras geográficas, as mudanças repentinas trouxeram novas adversidades que precisaram ser consideradas. A virtualização do ambiente de trabalho gerou mudanças no dia a dia das empresas, e a segurança dos dispositivos não teriam mais as mesmas garantias como no ambiente de trabalho tradicional, com firewalls, VPN's e antivírus corporativos.

No trabalho remoto, muitas empresas viram na tecnologia em nuvem uma opção para sua operação acontecer. Porém essa transformação radical com pouco ou quase nenhum planejamento abriu uma janela de vulnerabilidades. No Brasil, entre janeiro e setembro de 2020, foram registradas mais de 3,4 bilhões de tentativas de ataque cibernético. Como resposta, em um estudo realizado pela empresa Check Point em 2020 com cerca de 600 executivos da área de segurança de informação, 95% dos entrevistados afirmaram que suas estratégias de segurança mudaram para a segunda metade do ano. Desse montante, 67% respondeu que o motivo que justificava essas mudanças seriam a necessidade de se adaptar rapidamente ao trabalho remoto e 61% disse que esse deve continuar a ser motivo de preocupação até 2023.

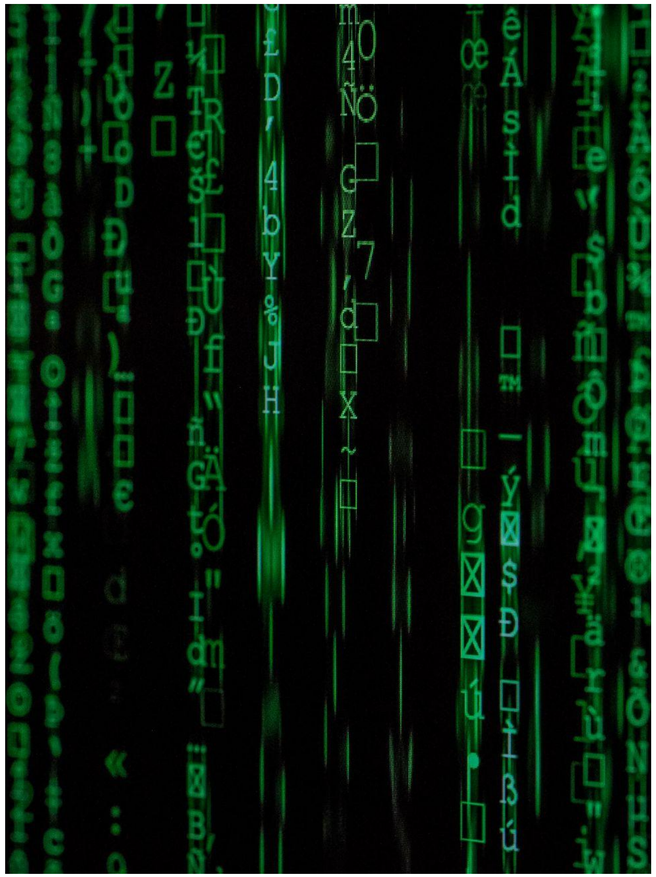
A apreensão vista pelos executivos têm sua argumentação embasada em dados. Das 5000 tentativas de ataque diárias realizadas na América Latina, 67% são direcionados a empresas e organizações. Entre elas, os setores-alvo são os de saúde, mídia, lazer e entretenimento, que que carregam grandes quantidades de dados pessoais. Além disso, percepções internacionais seguem a mesma preocupação: na França, foi constatado que pelo menos 25% das empresas sofreram um ataque de Ransamware.

É essencial frisar que criminosos cibernéticos estão cada vez mais habilidosos, e apenas em 2019 o FBI já recebia 1.300 denúncias por dia de crimes cometidos pela internet nos Estados Unidos. No Brasil, só em 2020 foram mais de 8 bilhões de tentativas e ameaças de ataques. Nesse contexto, os desafios da cibersegurança são constantes, e necessitam de soluções constantemente atualizadas para frear o impacto do crime cibernético.

Desenvolvimento tecnológico traz um alerta para os times de segurança digital

Quando olhamos para o futuro, temos um cenário de alerta pela frente. O desenvolvimento tecnológico traz uma série de vantagens em diversos setores, mas também traz consigo uma série de vulnerabilidades para o dia a dia. Uma exemplificação é o avanço do sistema operacional Windows 10 e versão beta do Windows 11, que trouxe consigo o fim do suporte para quem usa o sistema operacional do Windows 7. Esse ainda é a versão muito popular entre os brasileiros, tornando diversas máquinas defasadas e vulneráveis a ataques. Algumas tendências, que vêm ganhando cada vez mais tração no mercado, como serviços de Open Banking, IoT e 5G também são possíveis portas de entrada para invasores mal intencionados.

Este último vem como uma tecnologia que possibilita a transmissão de dados de forma incrivelmente rápida e pode ser conectada a diversas soluções, mas paralelamente aumenta o número de vetores pelas quais um ataque pode ocorrer e dificulta o controle pelos times de cyber segurança. Em outra análise, feita pela empresa Check Point com mais de 400 profissionais de segurança e TI, foi levantado que 90% dos entrevistados sofrem com o fenômeno de Shadow IoT, que consiste na existência de dispositivos não gerenciados oficialmente pela equipe de tecnologia dentro do ambiente corporativo, abrindo espaço para possíveis falhas de segurança. Agravando este fato, apenas 11% responderam que usam alguma solução de segurança para dispositivos IoT, e 52% afirmou não possuir recursos de proteção adicionais além daqueles oferecidos pelo próprio aparelho, que em sua maioria se limita a um login, com senha alfanumérica.



© UNSPLASH

Transformações em cibersegurança

Fernando Zamai
Regional
Sales Leader
Cybersecurity
Cisco

Com a pandemia, diversos mercados entraram em ascensão digitalmente e passaram a coletar mais dados, aumentar o número de transações financeiras no ambiente online, entre outras práticas. Quais os principais setores que vocês atenderam e quais tecnologias surgiram ou foram intensificadas em cibersegurança para atender a essas demandas?

O mercado se reinventou e buscou alternativas para sua continuidade ao mesmo tempo que explora novas formas de fazer negócio. Os setores de varejo, finanças e saúde lideram a demanda e impulsionam a adoção de soluções em nuvem (IaaS, PaaS e SaaS), e nesta jornada as soluções de segurança também evoluíram para oferecer soluções de conectividade e proteção consumíveis como serviços em nuvem "SASE". Quando comparados às soluções tradicionais, esses novos serviços oferecem inúmeras vantagens, como simplicidade, desempenho, eficiência.

Quando falamos de avanços em cibersegurança, qual o patamar que o mercado brasileiro está em comparação aos *players* internacionais? Quais são nossos maiores destaques e onde podemos evoluir?

Em geral, a maturidade em cibersegurança no Brasil é baixa e infelizmente ainda somos um dos países mais afetados pelos ciberataques. São inúmeros os desafios, então hoje destacarei a efetividade das proteções. Historicamente as organizações investem de forma fragmentada adquirindo soluções pontuais para problemas pontuais ,culminando numa operação complexa e pouco eficiente. As empresas de maior maturidade buscam a simplificação através da consolidação de fornecedores, o que também facilita a integração entre as soluções. Cria-se então uma arquitetura que detecta e responde de forma automática no menor tempo possível.

Como a inovação aberta, e a integração entre corporações e startups, pode auxiliar nos desafios atuais de cibersegurança?

Um estratégia de defesa eficiente depende de Inteligência de ameaças e da cooperação entre soluções onde integração, automação e orquestração são elementos críticos, abrindo oportunidades desde o desenvolvimento de algoritmos que detectam novas ameaças por aprendizado de máquina até sistemas de orquestração que simplificam as investigações e automatizam as respostas via RestAPI.

Categorias de ativos que são expostos a ameaças

INFRAESTRUTURA
Ativos encontrados na infraestrutura de TI da organização, envolvendo hardware e software.

USUÁRIOS
Pessoas com credenciais de usuário na rede corporativa que tenham acesso a terminais, servidores, sistemas e softwares.

COMPLIANCE
Procedimentos e processos relacionados a frameworks, normativas e políticas internas de práticas de Gestão da Segurança da Informação cuja ausência pode trazer riscos à organização.

APLICAÇÕES
Aplicações web, APIs e Apps expostos à camada pública da internet ou redes internas.

Principais ameaças de cyber no Brasil

MALWARE
É um software mal intencionado, um programa de computador destinado a se infiltrar em um sistema de computador de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações.

PHISHING
É uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais como nome de usuário, senha e detalhes do cartão de crédito. Para realizar o ataque os criminosos utilizam mensagens aparentemente reais, porém com scripts que roubam as informações desejadas.

ATAQUES DDoS
Distributed Denial of Service, ou ataque de negação de serviço, é o ataque voltado a inutilizar um sistema. Alvos típicos são servidores web, onde diversos acessos sobrecarregam o servidor, que fica incapaz de processar os acessos reais. Vale ressaltar que não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

RANSOMWARE
É um tipo de malware que encriptografa os dados do sistema infectado, bloqueando-o e cobrando um resgate para ter o acesso aos dados de novo. Caso não ocorra, os arquivos podem ser perdidos e até mesmo publicados.

Falta de informação e atenção dos colaboradores das empresas é alarmante

Os usuários são o principal ativo procurado para ataques de cibersegurança, já que, no geral, não há uma conscientização efetiva dos colaboradores dentro das corporações para assegurar uma cultura de proteção de dados. Isso culminou em um aumento considerável de ataques que exploram o fator humano como principal elemento para ataques cibernéticos, sendo o elo mais frágil de ataque. Dessa forma, existe uma preocupação dos profissionais em segurança de informação de propagar entre seus colaboradores uma cultura de proteção e atenção à sensibilidade das informações que precisam ser protegidas. Dessa forma, além de documentos, mensagens e treinamentos convencionais, muitas empresas estão aplicando no cotidiano atividades de conscientização recorrentes, principalmente focado em novos colaboradores, para que se inicie uma conscientização ampla da importância das informações que são tratadas diariamente e como ataques à elas podem ser extremamente danosos.

Além dos usuários, outro fator que exemplifica a falta de preocupação com a *cybersecurity* por parte das corporações é o fato de 59% das falhas de infraestrutura que são exploradas por criminosos tem correção disponível a mais de 1 ano. Em outras palavras, simples atualizações podem evitar ameaças que podem infectar o sistema e ter acesso a informações sigilosas, visto que 28% das falhas de aplicação são relacionadas com vazamento de dados. Por fim, apenas 27% entre todas as falhas identificadas são corrigidas, o que reforça que ainda há muito a ser melhorado no setor de uma forma geral por parte das corporações.

A importância do conhecimento em cibersegurança

Leonardo Militelli
CEO
GAT Infosec

A GAT explicita em seus posicionamentos a importância da proteção do Usuário como elemento mais vulnerável a ameaças cibernéticas. Como a empresa atua para corrigir as falhas dos colaboradores dentro das organizações?
Atualmente, o fator humano é considerado o elemento mais vulnerável e a maior ameaça à segurança cibernética, especialmente devido ao crescente número de ataques de ransomware, além da complexidade e criatividade observadas nos ataques de Engenharia Social. As técnicas são tão diversas quanto a prática, mas os objetivos são quase sempre os mesmos: aplicação de golpes e fraudes, sequestro de dados e pedidos de resgate, espionagem industrial, roubo de identidade ou credenciais, interrupção de serviços, motivação política e até por pura diversão.

O ato de manipular as pessoas com o objetivo de obter informações relevantes e úteis para uma fraude ou um ataque não é novidade, mas as formas como isso vem ocorrendo sim. Atualmente, é muito representado pelo crime de *phishing*, que tem como objetivo enganar usuários e obter informações sensíveis como credenciais de acesso, dados pessoais, senhas e até informações que, em um primeiro momento, não parecem sensíveis ou relevantes, mas que podem ajudar um cibercriminoso a compor um perfil mais detalhado de uma eventual vítima. Tais dados são coletados para utilização futura (endereço de e-mail, hábitos pessoais, telefone, endereço, marca do carro, escola onde estudou, nome do pet etc.).

Nesse cenário, é cada vez mais comum a incidência de mensagens de E-Mail, SMS e WhatsApp contendo links para sites fraudulentos com o intuito de obter informações pessoais e profissionais. Evitar tais riscos depende do nível de conscientização dos usuários sobre os tipos de fraudes para, então, possam saber como evitá-las e a melhor forma de evitar estes riscos é por meio de treinamentos constantes e conscientização das equipes em relação aos riscos.

Para sanar tais riscos, a GAT InfoSec oferece em suas ferramentas o monitoramento de vazamento de senhas dos e-mails corporativos. Também é possível aplicar questionários nos colaboradores de uma empresa para medir o nível de conscientização e eficácia dos treinamentos realizados, identificar, mapear e medir os riscos de fator humano enfrentados pela organização. Tais funcionalidades são o primeiro passo para a utilização das ferramentas oferecidas, transformando informações em indicadores e dashboards, apontando o

progresso e as falhas em processos realizados internamente. As soluções também englobam avaliações de risco de terceiros, com a possibilidade da aplicação de tais pesquisas em fornecedores e potenciais stakeholders que sejam relevantes para a atuação da organização em seu mercado.

A GAT se destaca na produção de conteúdo dentro do mercado de cibersegurança no Brasil. Qual a importância da geração de conteúdo e da democratização desse conteúdo dentro do ecossistema de cyber?

O ecossistema de cibersegurança no Brasil é composto por diversas desenvolvedoras multinacionais e nacionais atuando no mercado e atingindo níveis de atuação e expressão relevantes, conquistando clientes importantes para seu sucesso e relevantes para a economia nacional. Entre as nacionais, poucas se equiparam em termos de oferta e quantidade de produtos e serviços, quando comparadas às multinacionais, estas com mais estrutura, tempo de experiência e dinheiro em caixa.

Desta forma, as multinacionais saem na frente na corrida da produção de conteúdo, mesmo que esta seja apenas apenas uma tradução do conteúdo original, pois já têm sua posição consolidada no mercado e um tamanho permitiu acumularem uma quantidade imensa de dados, publicando seus achados regularmente e tornando-se fontes de informação para estudos, pesquisas de terceiros e notícias, entre outros. No entanto, uma vez que o número de multinacionais atuantes em solo nacional ainda não é tão numeroso quanto, por exemplo, nos Estados Unidos, a imensa maioria dos materiais na área de cibersegurança ainda estão disponíveis apenas em inglês, criando certa barreira por causa da linguagem. Prova disso é uma recente pesquisa do portal Catho, um dos maiores sites de busca de empregos do país, que mostra que apenas 5% dos brasileiros têm o inglês como segundo idioma e os fluentes na língua são apenas 3%. Neste cenário, as empresas nacionais lutam para manter sua relevância, muitas vezes por meio da realização de eventos (atualmente virtuais) e, ocasionalmente, por meio da produção de relatórios e conteúdos ricos sobre cibersegurança.

Após identificar essas tendências, percebemos que existe uma dominância na geração de conteúdo por parte das grandes multinacionais que, na maioria das vezes, apenas têm o conteúdo original traduzido para o português por seus escritórios locais e oferecem ao mercado informações de relevância global. Muitas vezes, isto significa que a realidade local não é tão relevante para os materiais que surgem como resultados de tais pesquisas e observações.

Decidimos, assim, optar pela criação de conteúdo na área de cibersegurança como forma de democratização da cultura de Segurança da Informação em território nacional, com o objetivo de ajudar a criar uma sociedade mais segura frente ao mundo digital, rompendo com as barreiras que ela normalmente enfrenta. Além das postagens em nosso blog e dos checklists disponibilizados em nosso website, decidimos lançar a série GAT Cyber Talks com especialistas e gerentes de segurança da informação do mercado (CSO/CISOs) e iniciar o desenvolvimento de materiais ricos (relatórios, infográficos e e-books), além de datasheets sobre tais materiais, sobre a empresa e nossos produtos. Desta forma conseguimos atingir um público maior e difundir as informações da melhor forma possível, sempre adequadas às diversas mídias e canais utilizados.

A importância do conhecimento em cibersegurança

Leonardo Militelli
CEO
GAT Infosec

Conseguimos, assim, conquistar uma posição relevante no mercado em pouco mais de um ano como empresa, alcançando destaque na grande mídia e em veículos de comunicação especializados em cibersegurança, o que só contribuirá para a difusão das informações que estamos divulgando constantemente. Milhares de pessoas, das mais diversas áreas, costumam consultar nosso website regularmente em busca de informações, muitas delas direcionadas a um público que precisa de um alto grau de conhecimento em cibersegurança para saber o que fazer com tais informações.

Acreditamos que a geração e a democratização deste tipo de conteúdo só trará benefícios a todos pois está auxiliando, dia após dia, estudantes e profissionais em todos os estágios de suas carreiras, além de empresas de todos os portes e segmentos. Pretendemos atingir o maior número possível de pessoas com conteúdo de qualidade, sempre claro e objetivo, ajudando todos a compreender os desafios enfrentados e saber como superá-los.

Percebemos que tal democratização pode ajudar a sanar um dos maiores problemas enfrentados pelo mercado de cibersegurança atualmente: a falta de profissionais. Um estudo global da IBM estima que, atualmente, há uma defasagem na casa de 3 milhões de profissionais para detecção, diagnóstico e solução de ataques cibernéticos. Este é um problema enfrentado por empresas de cibersegurança ao redor do mundo que não se torna mais fácil no Brasil. Em território nacional, a falta de profissionais é evidenciada pela alta rotatividade e remuneração cada vez mais alta, praticada como forma de atrair talentos.

E assim, a cada conteúdo produzido, pretendemos colaborar com a democratização da informação e com o ecossistema de cibersegurança, levando cada vez mais informação relevante a todos.

A importância do conhecimento em cibersegurança

Leonardo Militelli
CEO
GAT Infosec

Brasil entra na rota global de *cybersecurity* em um contexto de ataques com prejuízo trilionário

O setor de cibersegurança está em uma crescente, assim como a quantidade de ataques e ameaças cibernéticas. Em 2018 o prejuízo global causado por cibercrimes já era relevante e atingiu um patamar de US$ 522,5 bilhões. Já em 2020 ,esse número quase dobrou, totalizando US$ 945 bilhões,beirando a marca de 1 trilhão de dólares em prejuízos por ciberataques. Esse valor representa mais de 1% do PIB mundial.

O setor de cibersegurança não está evoluindo da mesma maneira. Apesar da taxa de crescimento anual composta (CAGR) do mercado global ser estimado em 12,5%, atingindo US$ 403 bilhões até 2027. Os ciberataques estão evoluindo de forma mais acelerada. Segundo relatório da Chainnalysis, os ataques por *ransomware* cresceram 311% entre 2019 e 2020, sendo este um dos que causam maiores prejuízos para as empresas.

Temos que lembrar que essas despesas não se encontram apenas na área financeira, mas em toda a operação. Ataques podem causar quedas no sistema, gerando interrupções na produtividade e inatividades não planejadas. Na América Latina e no Brasil o contexto é o mesmo. Estima-se que dos 41 bilhões de ataques realizados na América Latina em 2020, mais de 20% tenham ocorrido apenas no Brasil. O assunto chama tanto a atenção que o país irá fazer parte do estudo global de soluções e serviços de segurança cibernética, realizado pela TGT Consult, ao lado de Estados Unidos, Reino Unido, Alemanha, Suíça, França, Austrália e países nórdicos.

O país entra para o estudo por chamar a atenção em três aspectos que devemos prestar atenção. São eles a LGPD, o trabalho remoto e o aumento dos crimes cibernéticos. Vale lembrar que além dos crimes de ransomware, cada vez mais comuns, vemos um crescente número de ataques relativos à roubo de criptomoedas, sequestro de e-mails, spyware e phishing, sendo necessário todo o cuidado dos usuários para se protegerem dessas ameaças.

Soluções internacionais já estão buscando o Brasil como potencial mercado consumidor no segmento de cibersegurança. Um exemplo é a startup argentina VU Security, que atua para melhorar a identificação digital e prevenção de fraudes, e que recentemente captou uma rodada de R$60 Milhões para manter sua expansão internacional e prepara para entrar no mercado brasileiro. Além disso, o país recebeu pela primeira vez um convite para participar do *Cyber Security Challenge* (ICSC), competição global organizada pela *European Cyber Security Challenge* (ECSC), que visa aumentar a conscientização da cibersegurança mundial promovendo competições entre talentos do setor.

Ataques cibernéticos no Brasil durante a pandemia

FLEURY

No dia 23 de junho deste ano, o Grupo Fleury, referência em medicina diagnóstica no país, sofreu um ataque hacker via *ransomware*. Responsável pelo ataque, o grupo REvil sequestrou os dados da empresa exigindo um pagamento de aproximadamente US$ 5 milhões por meio da criptomoeda *monero* (XMR). Dentre os danos causados à companhia, foram notados tanto a queda de seu sistema, quanto de seu site e aplicativo aos clientes que queriam acessar resultados de exames. Contudo, o principal foi a ameaça dos hackers de publicar 450 GB de informações médicas, financeiras e pessoais de clientes do Grupo. Embora a empresa não tenha confirmado o pagamento do resgate, pouco mais de uma semana após o ataque, os acessos a seu site e app foram retomados normalmente. As investigações sobre o ocorrido mantêm-se de forma interna com o auxílio de outras empresas no setor de cibersegurança.

STJ

No dia 3 de novembro do 2020, por meio do *ransomware* RansomEXX, o Superior Tribunal de Justiça teve seus dados sequestrados, culminando na interrupção dos julgamentos em todos os seus colegiados, além da suspensão de prazos processuais e da queda de seu sistema. A volta do sistema ocorreu apenas duas semanas após o ataque. Não houve divulgação quanto ao grupo responsável pelo crime ou a qualquer pedido/pagamento de resgate. As investigações foram feitas pela Polícia Federal.

TJRS

O Tribunal de Justiça do Rio Grande do Sul (TJRS) foi atingido por um ataque cibernético entre os dias 28 de abril e 10 de maio de 2021. O acesso aos diversos sistemas e processos do TJRS foi impedido, somado à suspensão dos prazos processuais do tribunal, devido ao sequestro de diversos dados via ransomware pelo grupo REvil. Entretanto, mesmo após a volta de seu funcionamento, diversos usuários das plataformas do Tribunal alegaram falta de transparência na resolução do problema. Embora um resgate de US$ 5 milhões em moneros (XMR) tenha sido pedido pelos hackers, o TJRS não confirmou seu pagamento. A Polícia Civil foi designada a cargo das investigações.

JBS

A multinacional brasileira JBS S.A, maior processadora carne bovina e suína do mundo, também não ficou impune dessa onda de ciberataques. No dia 30 de maio deste ano, a empresa sofreu um ataque de ransomware do grupo REvil que resultou no fechamento de suas unidades produtivas em países como Austrália, Canadá e EUA por quase quatro dias. A JBS, no entanto, optou por pagar o resgate de US$ 11 milhões em bitcoin pedido pelos sequestradores e logo retomou suas atividades. As investigações desse ataque foram feitas pelo FBI e por companhias contratadas.

Reações do ecossistema brasileiro

Kaique Bonato
Founder & CEO
Phanter

Com o início da pandemia e a transição para o trabalho remoto, os ataques hackers ficaram cada vez mais complexos e agressivos. Quais são as tecnologias de cibersegurança que hoje em dia já estão defasadas, e quais foram as novas soluções que o mercado trouxe?

Com a chegada da pandemia, o home-office tornou-se uma alternativa praticamente obrigatória para as organizações, e as equipes de T.I/Segurança precisaram se adaptar rapidamente a esse novo cenário. Porém, fazer isso com pressa e sem planejamento gerou diversos problemas de segurança e percebeu-se a necessidade de novas tecnologias para tal. As organizações acabaram perdendo o controle dos seus ativos e funcionários e logo foi necessário adotar soluções existentes e que tiveram maior aderência após a pandemia, tais como a utilização de múltiplos fatores de autenticação nos sistemas e plataformas, soluções de proteção e monitoramento de notebooks/computadores durante o home-office. As soluções convencionais que eram utilizadas dentro das organizações, como firewall, foram defasadas, uma vez que os funcionários já não estão mais conectados a eles para trabalhar.

Sabemos que o mercado brasileiro de cibersegurança ainda está muito atrasado quando colocado em escala global. Quais são os desafios de criar empresas nessa área no país, e qual a sua previsão para o mercado brasileiro no futuro?

Cibersegurança é um tema sensível nas organizações principalmente quando falamos em grandes empresas. Um dos desafios que estamos enfrentando é a falta de abertura para apresentarmos soluções para essas corporações, e, quando termos abertura, logo somos questionados em diversos fatores. Por sermos uma startup, é complicado assumir todos os riscos, mesmo que nossa solução atendendo as necessidades da companhia.

Temos diversas empresas de Segurança da Informação/Cibersegurança que prestam consultoria, mas poucas que possuem soluções/produtos. Com o dólar em alta e todas as soluções vindo de fora, é muito provável que venhamos a ter diversas iniciativas para criação de soluções brasileiras no combate a ciberataques. O mercado nunca esteve tão aquecido como agora e só tende a aumentar, e o próprio Gartner estimou que para esse ano o investimento de Segurança da Informação/Cibersegurança chegue a U$ 150 Bilhões e até 2026 tende a duplicar. Para o Brasil ainda vemos um movimento mais devagar, mas a tendência é que com a LGPD e as multas sendo aplicadas a partir de agosto deste ano o mercado pode abrir novas oportunidades para todos.

Dentro do ambiente corporativo brasileiro, quais são as maiores vulnerabilidades na defesa digital que você consegue identificar?

Nossa solução de monitoramento detectou alguns pontos em grandes corporações, sejam elas de pequeno porte ou até que já estão na bolsa de valores. Esses são os 5 principais fatores de vazamentos de dados:

-Fornecedores;
-Credenciais comprometidas;
-Falta de visibilidade dos ativos;
-Configurações incorretas da nuvem;
-Vulnerabilidades de segurança antigas e não corrigidas. ●

Ecossistema brasileiro

Como está configurando o ecossistema de inovação brasileiro dentro do universo de cyber?

RADAR: CYBERTECHS

DISTRITO

Application Security

Berghem Smart Information Security
BugHunt
CONVISO APPLICATION SECURITY

BLOCKCHAIN

amachains
bit shopp
BLOCKc
BlockNobre Blockchain Solutions
COSMOS BLOCKCHAIN
CRIPTONOMIA
original
EOSRIO
Go Blockchain
GoBlock
GoLedger
growthTech
HubChain
InspireIP PROPRIEDADE INTELECTUAL
InterAg
health
multiledgers
ORIGINAL MY BLOCKCHAIN
QUAN DIGITAL

Data Protection

a2f
C²LAW
CIAware
CLAVIS segurança da informação
CleanCloud
DADOS LEGAIS
dogma
DPO Center
ethquo ETHICAL QUOTIENT
GLOBAL DATA BANK
guardSI Cybersecurity
ID ESSENTIALS
Intelivix
LOGS360
MODULO
NETTIME SISTEMAS
OWL DOCS
Privacy tools
PRIVALLY
riskex
SAFE WAY
senhasegura
SENSR.
Simply.
ST3TAILOR SISTEMAS E SERVIÇOS
unxpose

Cloud Security

ADTsys
baxtru | cloud backup
BrasilCloud Nuvem Corporativa
skalena
DDMX
nuvic cloud solutions
RedeHost

Fraud & Transaction Security

akaer
B2e Group
bankSe
bigdatacorp.
BrScan
COMBATE A FRAUDE
deepen
CQuantt
datarisk.io
EXATO DIGITAL BETA
HUPDATA Data Analysis Solutions
infodatos
konduto
legiti
MOST SPECIALIST TECHNOLOGIES
NeuralMind
MaChiron
NeuroBanco Banco de Desenvolvimento Comunitário
NEXTCODE
REFINARIA DE DADOS
Owli
v/certo
inlocomedia
TRANSFERO SWISS AG
ZAIG

IoT Security

LATOS
POLSEC
PREVISIOWN Technology for better decisions
Ochain
ROBBIoT
TrackerThings

RADAR: CYBERTECHS

DISTRITO

Identity & Acess Management

DAITAN · acert · AIKNOW · akiyama · autentique · AutoSeg · My BeCloudx Customer Experience · BRyTecnologia · CH tecnologia · Chico High Intelligence · Computer ID · CRED DEFENSE · GO! FIVE · Formalizar e-signature · FULLFace A sua segurança é você · griaule big data biometrics · GrupoCloud · GRYFO · ha tecno · HOOBOX · ID ESSENTIALS · idwall · INCOGNIA · INOVACODE RFID SOLUTIONS · Let's Work · MEERKAT · MULTIFACE BIOMETRIA · NATOSAFE BORN TO BE UNIQUE · nexti SOLUÇÕES INTELIGENTES · nTokens · OITI · payface · qriar · QualiSign · PONTO marcação móvel · SHIELDER · SimpleID IDENTIDADE CONFIRMADA! · SVATECH smart video analytics · T-SHIELD · acesso digital · unike TECHNOLOGIES · UNISEC Segurança, tecnologia e conforto · VSOFT · welcome

Security Consulting and Services

ANDRADESOTO INFORMATION SECURITY · BLAZE INFORMATION SECURITY · CECyber Center of Excellence in Cybersecurity · Collision INTELLIGENCE LABS · CROMISOFT · Deep.bbl R&D, Technology & Services · ESTUARIO TI · HACK3R_RANGERS · IBLISS 10 anos DIGITAL SECURITY · InfoSafe · SOLVIMM · nova8 CYBERSECURITY · OPTRA SECURITY · PHISHX · REDBELT · RUSTCON · STRONG SECURITY · TEMPEST security intelligence · Unbroken Cyber Security

Mobile Security

BluePex

Security Operations & Incident Response

gocache next-gen CDN · AXUR

Network & Infrastructure Security

BluePex · CONNECT · ISH · lumiun CLOUD MANAGED NETWORK · munic SECURITY · oktopus · ProFUSION embedded systems · StartLink INFORMÁTICA CORPORATIVA · TI Safe · Virti · Ztec

Web Security

apura · AuditSafe · CromiWAF cyber defense · DESEC · EARLYSEC · GAT InfoSec · Gatefy · XLabs | ON SECURITY · SITE BLINDADO · UPX TECHNOLOGIES · XLabs security

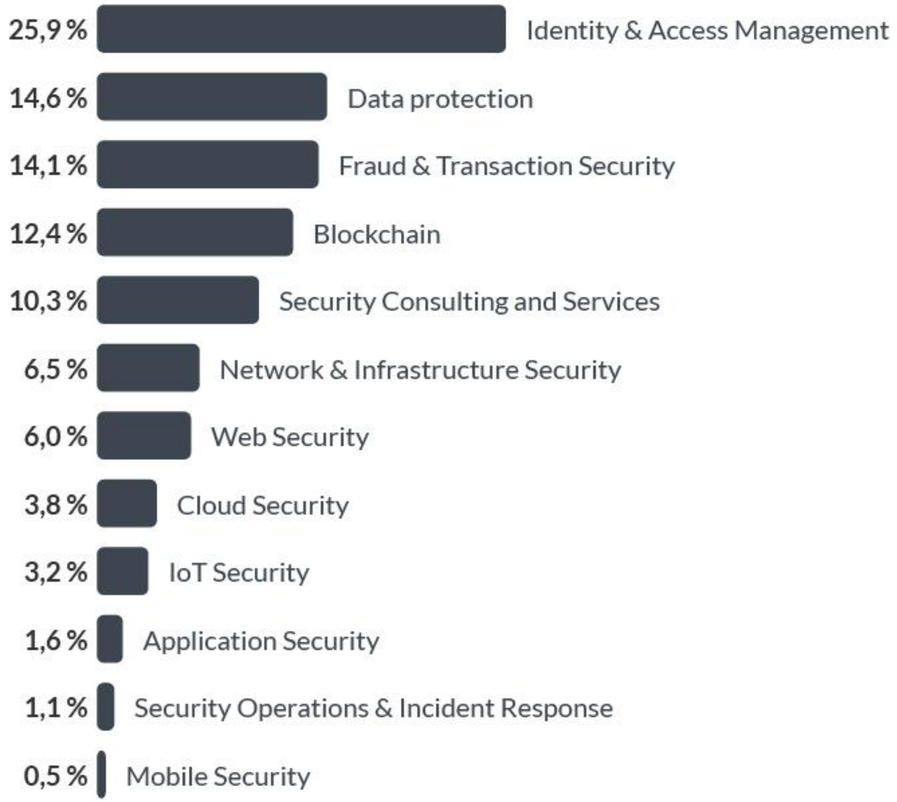
Zoom: Categorias

186 startups

48 startups de Identity & Access Management

Soluções de Identity & Access Management são foco no crescente cenário de transformação digital e se tornaram destaque no ambiente de home office. Essas soluções também são impulsionadas, por exemplo, pela digitalização de abertura de contas financeiras e serviços pessoais, que é necessário a validação de identidade, seja através de reconhecimento facial ou por validação de impressão digital. Outros nichos que também se beneficiam são os de recursos humanos, principalmente na etapa de onboarding e acesso a credenciais. Outra vantagem desses sistemas é no de compliance, pois, com as questões de adequação a LGPD, é cada vez mais necessário ter o controle de quem tem acesso a arquivos contendo informações sensíveis.

Porcentagem de startups por categoria

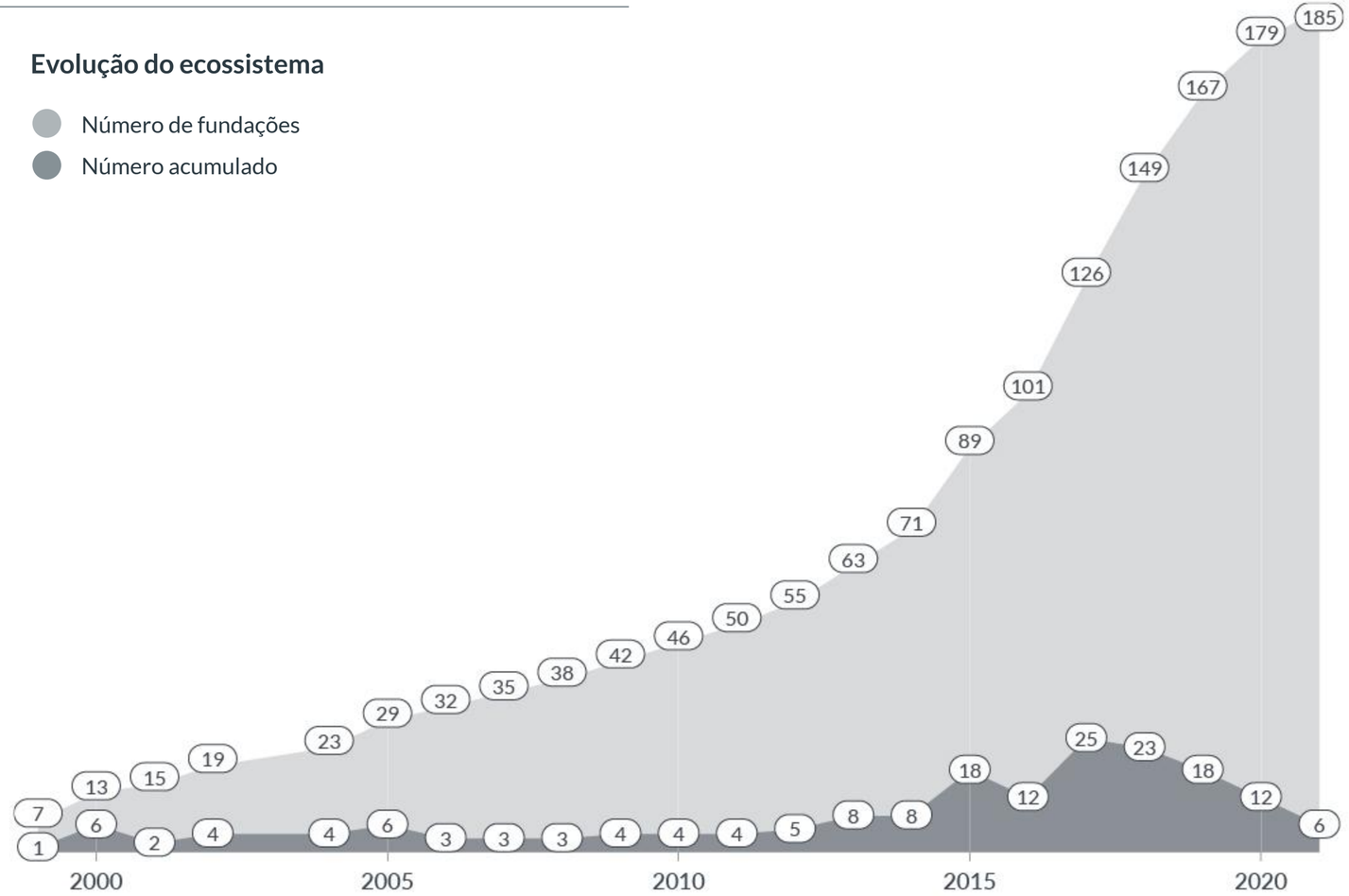


2017 e 2018 se destacam como anos de criação de empresas de cibersegurança

Entre 2015 e 2020, observa-se o nascimento de mais de 90 empresas de cibersegurança no Brasil. Só entre 2017 e 2018 nasceram 48 delas. Esse movimento é acompanhado pela transformação digital das empresas brasileiras, que já vinha ocorrendo mesmo antes da pandemia.

Apesar da crescente preocupação das empresas por conta de ataques cibernéticos, observa-se que não há um crescimento expressivo de novas startups no período de pandemia. Ao mesmo tempo que isso significa um risco, visto que muitas corporações acabam buscando empresas de segurança mais tradicionais e consolidadas no mercado ou mesmo soluções internacionais, isso também se reflete em oportunidade em um cenário de aceleração contínua da digitalização da economia e crescente olhar para o tema de segurança digital.

Evolução do ecossistema



Soluções exclusivamente B2B representam 83% das startups

Era esperado que soluções de segurança cibernética tivessem maior foco em corporações, visto que são os focos de ameaças de ataques. Além disso, todas elas precisam de soluções para guardar informações sensíveis de forma segura e evitar ataques que podem gerar prejuízos milionários, como já foi caso de algumas corporações brasileiras no ano de 2020.

Dessa forma, 98% das soluções encontradas oferecem serviços para corporações, que necessitam otimizar a segurança de suas empresas, principalmente aquelas que tem pretensões de expansão por meio de contratação de colaboradores em home office.

Do outro lado, apenas 4 soluções levantadas neste mapeamento são responsáveis pela segurança individual do usuário. Essa pode ser uma oportunidade de mercado, uma vez que ataques de *phishing* e de engenharia social estão sendo cada vez mais observados. No entanto, vale ressaltar a necessidade de educação deste mercado B2C, que muitas vezes não está ciente dos riscos que suas ações despretensiosas podem causar a si mesmo.

Representatividade por Público

Com o crescimento dos acessos descentralizados, o uso do *Multi-factor authentication* (MFA) virou uma boa prática cada vez mais obrigatória em empresas de todos os tamanhos. MFA consiste de mais uma camada de proteção para conseguir se autenticar em sites e aplicações. Exemplo comuns são o uso de apps de autenticação que geram senhas de uso único ou aparelhos físicos de Token de segurança.

Mas nem todos os tipos de MFA são igualmente seguros. Já existem técnicas que permitem aos atacantes usarem falhas nos processos de empresas telefônicas para burlá-lo baseados em ligações ou mensagens de texto, ao ponto de fazer a Microsoft emitir um comunicado recomendando a seus usuários que não utilizem mais esses tipos de MFA. O uso de biometria como um fator de autenticação é uma tendência cada vez maior, e recentemente a Transmit Security, especializada em biometria facial, recebeu um investimento recorde de US$ 543 milhões.

A velocidade na migração para o modelo remoto de trabalho forçou também a adoção massiva de serviços em nuvem. De acordo com a Cybersecurity Ventures, o mundo vai armazenar 200 zettabytes (que significa Duzentos trilhões de Gb) de dados até 2025, e metade disso vai estar na nuvem. A complexidade do cloud torna cada vez mais comum falhas de configuração que podem gerar acessos não autorizados e, consequentemente, vazamentos de dados. As empresas também têm tido dificuldade em encontrar um equilíbrio capaz de conciliar a velocidade para os times de desenvolvimento com a segurança necessária para diminuir a exposição a ataques. Nesse cenário, torna-se cada vez mais importante adotar um monitoramento contínuo das configurações de segurança da nuvem.

Todas essas mudanças ocorrem ao mesmo tempo em que as leis de proteção de dados se tornam uma realidade em diversos países, inclusive no Brasil. As possíveis sanções legais a vazamentos de dados intensifica a preocupação com a privacidade de dados. Isso requer das empresas a implementação de uma estratégia robusta de dados que integre áreas como o marketing, jurídico, produto e RH.

A proteção precisa ser elevada a assunto corporativo não restrito às áreas de tecnologia.

Independente das mudanças trazidas pelo home office, há 3 aspectos sobre os quais as empresas não podem abrir mão para se manterem protegidas: cultura, processos e tecnologia. O primeiro ponto diz respeito à necessidade conscientizar os colaboradores para que se tornem agentes de cibersegurança. O segundo versa sobre a importância da criação de políticas claras de segurança e da contração de profissionais especialistas no tema. O terceiro fala sobre a necessidade da adoção de uma infraestrutura tecnológica de cibersegurança capaz de proteger os ativos digitais de uma empresa. Com esses 3 aspectos cobertos, empresas de todos os tamanhos estarão prontas para enfrentar os desafios do home office e de outras mudanças que o mundo pós-pandemia vai trazer.

Para qual direção estamos indo?

Josemando Sobral
Co-Founder
Unxpose

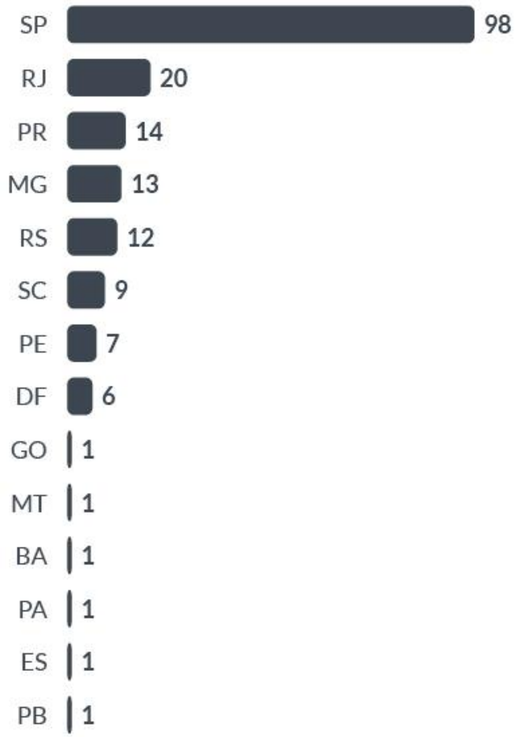
São Paulo se destaca por sediar mais da metade das startups de cyber segurança

Assim como em outros setores, o eixo São Paulo / Rio de Janeiro se destaca por possuir o maior número de startups de CyberTech.

Com 98 empresas, São Paulo se sobressai, concentrando 53% do total dessa categoria de empresas. Em seguida vem o Rio de Janeiro com 20 startups, praticamente um quinto do total quando comparado à São Paulo.

A concentração se explica pelo grande número de empresas que se localizam neste eixo, sendo natural startups que atendem no modelo B2B buscarem maior aproximação por haver mais chances de conversão de oportunidade de negócios.

Startups de Cyber pelo Brasil



Radar: Número de funcionários e empregabilidade por categoria

Porcentagem de empregados por categoria

Quantidade de startups por faixa de funcionários

Como era de se esperar, a categoria Identity & Access Management possui um dos maiores quadros de colaboradores, assim como ocupa o maior número de startup do setor. Porém, o destaque fica para a categoria de Fraud & Transaction Security, que ocupa primeiro lugar em número de funcionários. Isso se deve ao fato de que as startups da categoria são mais consolidadas no mercado e têm um porte e robustez maior, reflexo dos parceiros com quem atuam. Ou seja, empresas do setor financeiro que historicamente têm boa aderência com novas tecnologias e os e-commerces, que precisam dessas estruturas para viabilizarem o modelo de negócio.

Em relação à faixa de funcionários geral, era esperado que tivessem mais empresas com porte reduzido, dado ao cenário ainda em crescimento do setor de cyber segurança no Brasil.

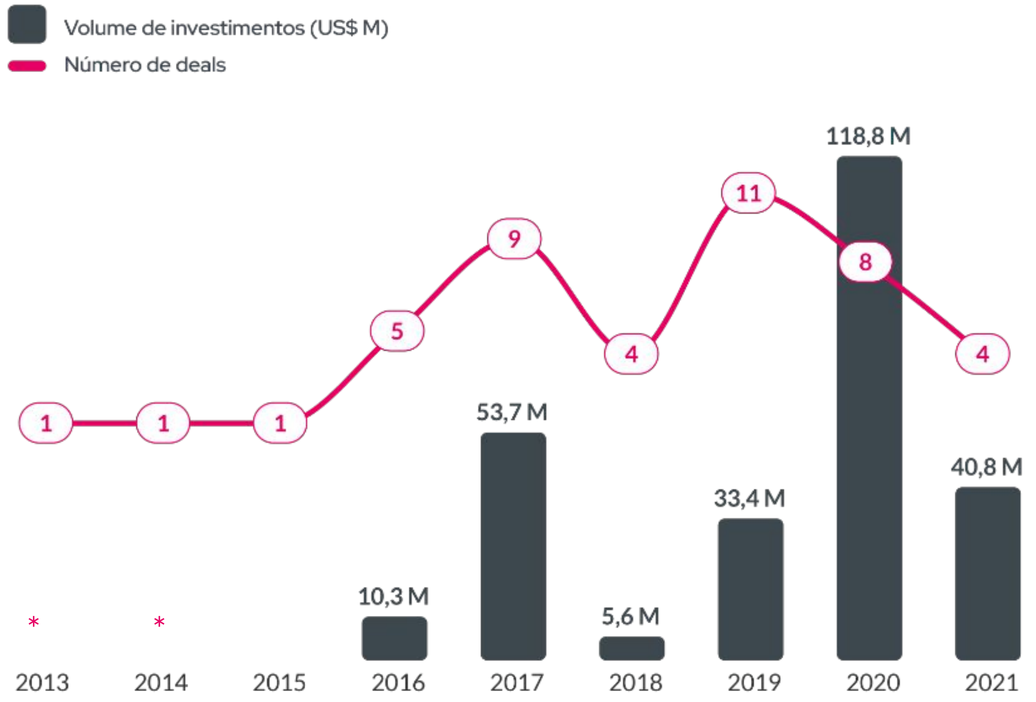
Financiamento de Cyber no Brasil ainda é pequeno, e 2020 destoa por uma rodada

A startup UNICO, antiga Acesso Digital, recebeu um aporte de US$ 110 milhões em 2020, o que classificou o ano como destaque no quesito financiamento de startups de cibersegurança no Brasil. Entretanto, também se destaca o baixo número de deals, mesmo em um ecossistema crescente desde 2018. Outro ponto a ser observado é a falta de dados sobre deals e investimentos no ano de 2015, que não foram encontrados.

Visando um desenvolvimento maior do ecossistema de cibersegurança brasileira, é esperado que conforme o mercado vá se desenvolvendo, ocorram cada vez mais investimentos. Vale salientar que a maioria das startups de Cyber brasileiras ainda estão em estágios iniciais e metade delas foram fundadas nos últimos 5 anos, o que confirma que o ecossistema ainda está longe de estar maturado.

Não existe ainda uma tendência de alta marcante em volume de investimento e número de deals. Até o momento, poucas empresas conseguem se destacar dentro do ecossistema e crescer para chegar ao ponto de serem investidas, mesmo em early stage.

Volume investido e número de deals em Cybersecurity no Brasil



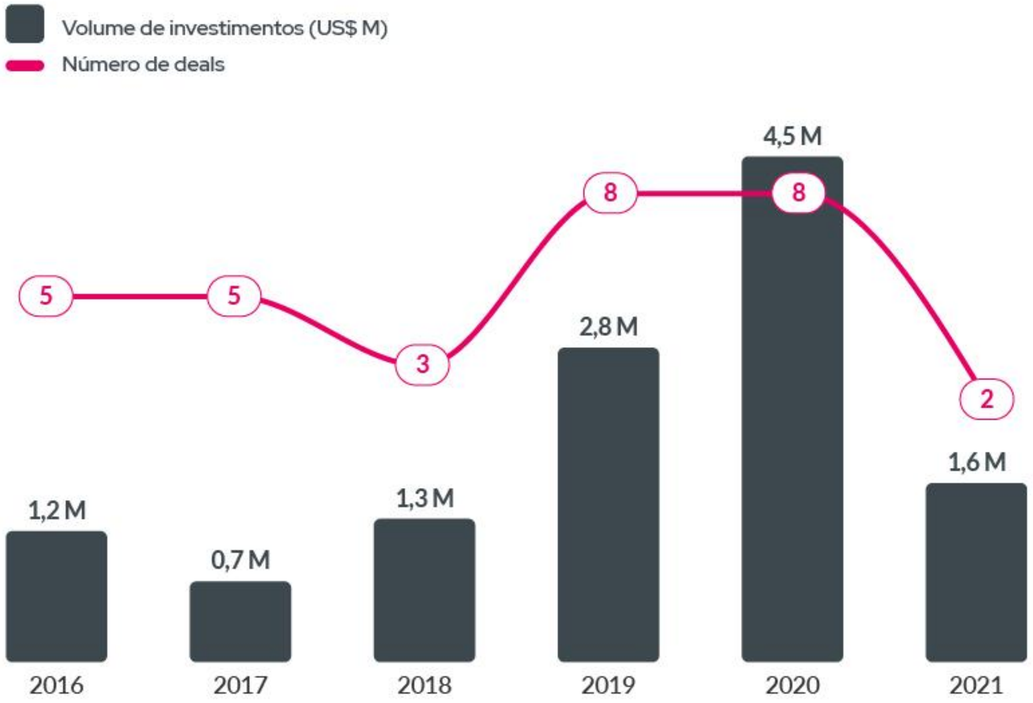
* Volume de investimento não informado.

Investimentos iniciais apresentam leve tendência de crescimento em 2020

Investimentos em estágios iniciais (Anjo, Pré-Seed e Seed) são bons indicadores de desenvolvimento do ecossistema no geral, indicando futuros aportes maiores nos anos subsequentes e criação de novas soluções. Isso é evidenciado em outros setores, em que startups atingem níveis de investimento elevados e colaboradores da empresa buscam uma nova etapa na carreira, criando novas soluções para o mercado. No setor de cibersegurança, observa-se uma leve tendência de crescimento em número de aportes e volume investido nos últimos anos, mas os números não apontam que haverá um grande número de grandes investidas no país.

É nítido que o ecossistema brasileiro de cibersegurança ainda está em estágios iniciais, porém espera-se que o crescimento do número de soluções acompanhe um aumento do número de investidas em estágio inicial nos próximos anos, para a continuidade da criação de soluções melhores e mais escaláveis. Além disso, a quantidade relevante startups fundadas nos últimos 5 anos que começam a se consolidar no mercado podem iniciar um novo ciclo de financiamento da cyber brasileira, frente a demanda trazida pelas grandes corporações, necessitadas de soluções efetivas de segurança da informação.

Valor investido e número de rodadas em investimentos Anjo, Pré-Seed e Seed

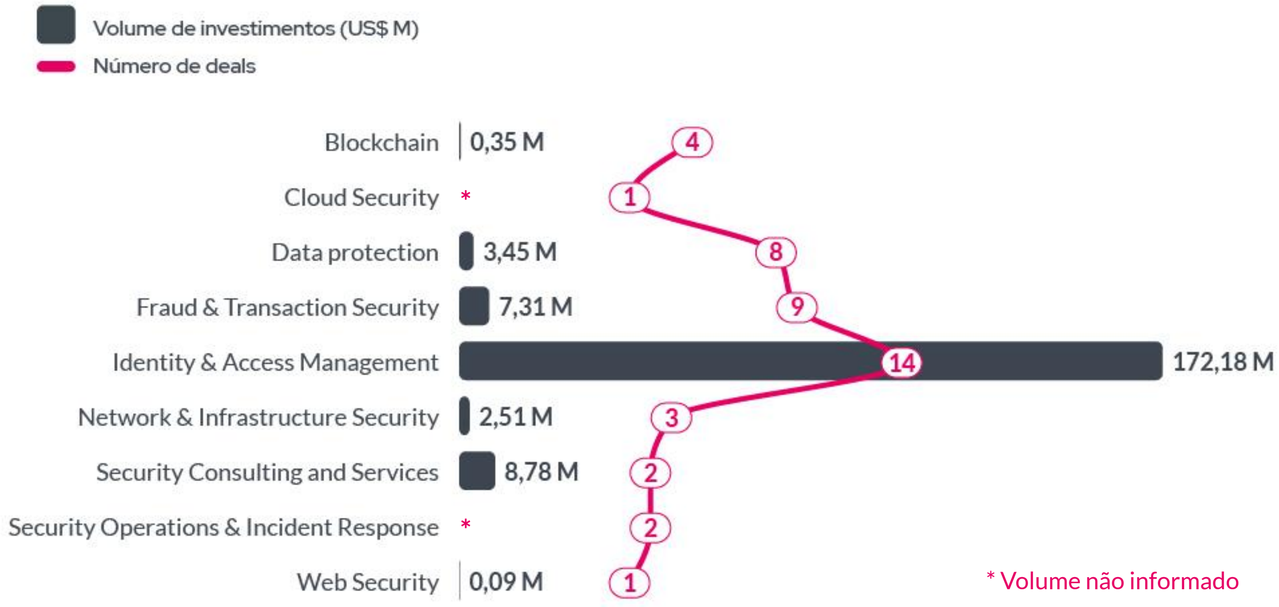


Identity & Acess Management segue como destaque absoluta em funding

1º Identity & Access Management

2º Identity & Access Management

3º Identity & Access Management



A categoria de Identity & Access Management é destaque absoluto em financiamento da cibersegurança brasileira, puxada por grandes rodadas recebidas pelas top 3 startups que mais receberam investimento no setor historicamente. Para soluções da mesma categoria, infere-se que possa haver ainda espaço em um mercado que está sendo bastante demandado, porém a concentração dos investimentos reflete a falta de soluções consolidadas no mercado em diferentes categorias de segurança da informação.

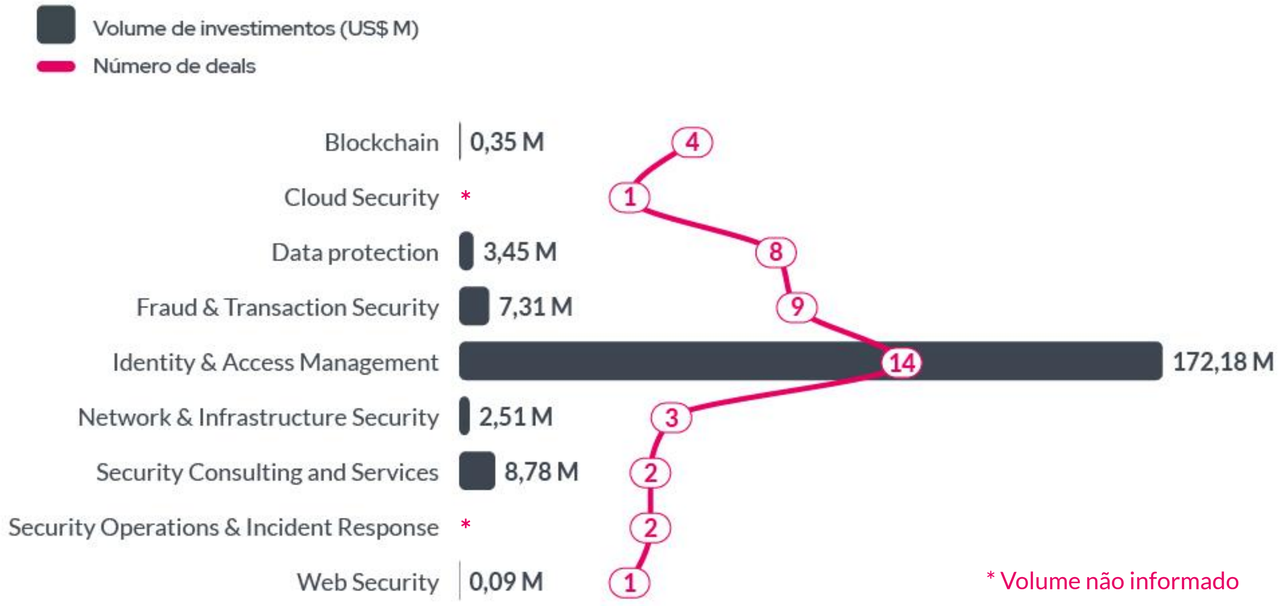
Identity & Acess Management segue como destaque absoluta em funding

1º UNICO — Identity & Access Management

2º idwall — Identity & Access Management

3º INCOGNIA™ — Identity & Access Management

Investimento por categoria



* Volume não informado

A categoria de Identity & Access Management é destaque absoluto em financiamento da cibersegurança brasileira, puxada por grandes rodadas recebidas pelas top 3 startups que mais receberam investimento no setor historicamente. Para soluções da mesma categoria, infere-se que possa haver ainda espaço em um mercado que está sendo bastante demandado, porém a concentração dos investimentos reflete a falta de soluções consolidadas no mercado em diferentes categorias de segurança da informação.

Panorama Internacional

Como o ecossistema de cyber está sendo avaliado em um contexto internacional e o que deve ser destacado?

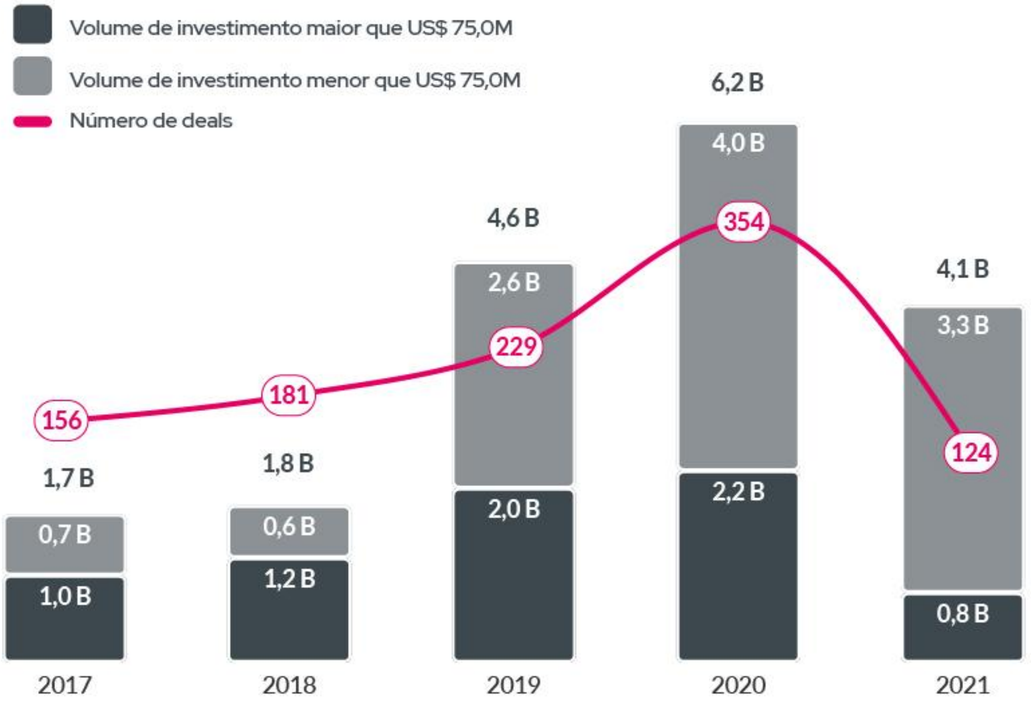
Investimentos globais em 2020 e 2021 se destacam

O setor de cibersegurança se tornou peça essencial para todas as indústrias e mercados modernos, e ser capaz de se defender de ataques cibernéticos tem se tornado uma necessidade cada vez mais urgente. Desta forma, as soluções desenvolvidas para resolver importantes dores do mercado de cibersegurança vem atraindo cada vez mais a atenção dos investidores globais.

Soluções que utilizam inteligência artificial para detectar comportamentos anômalos e soluções para proteção de mensagens e mídias digitais foram algumas das principais tendências olhadas pelos venture capitalists em 2020. As soluções voltadas para a identificação e a verificação de identidades digitais também vem crescendo bastante no último ano.

Segundo dados do RegTech Analyst o mercado de cybertech recebeu mais de US$ 6,2 bilhões em investimentos no ano passado, um crescimento de 31% em comparação com 2019. A pandemia acelerou o processo de digitalização e a necessidade de soluções de segurança digital, logo, no primeiro trimestre de 2021 já foram investidos mais de US$ 4 bilhões, indicando uma forte tendência de recorde para esse ano.

Investimentos e número de deals globais em Cybersecurity



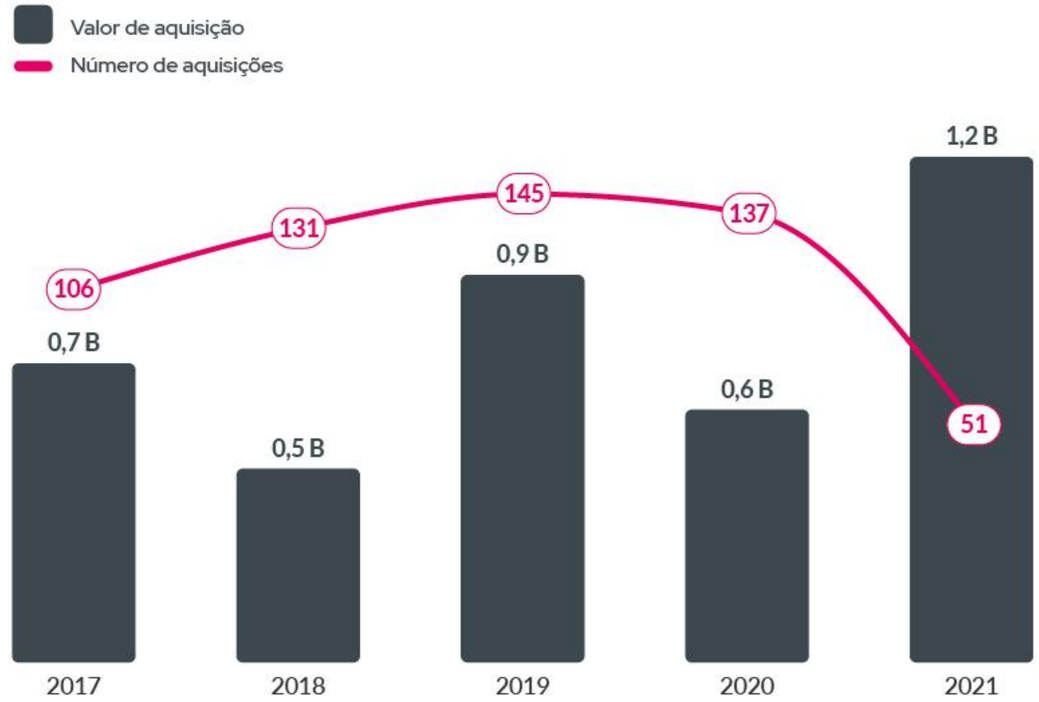
M&As estão presentes no mercado de Cybersecurity internacional

As transações de M&As no mercado cyber nos mostram um mercado agitado, com grandes players buscando as novas tecnologias e buscando consolidar suas posições.

Os EUA se destacam como sede das empresas que mais adquiriram startups de cybersecurity em 2021, com as 9 primeiras corporações mais ativas na procura de soluções para serem incorporadas. Com relação às startups, o país segue como sede da maior quantidade de soluções adquiridas, entretanto, Israel e Canadá também merecem destaque.

As principais companhias visadas para as transações atuam no setor de identificação, *zero trust*, *cloud security* e *security services*. O aquecido mercado de cyber não parece dar indícios de reduzir o número de investimentos ou de transações em M&As. O expressivo número de novas empresas surgindo também indicam uma tendência de crescimento dos investimentos e das oportunidades de aquisição.

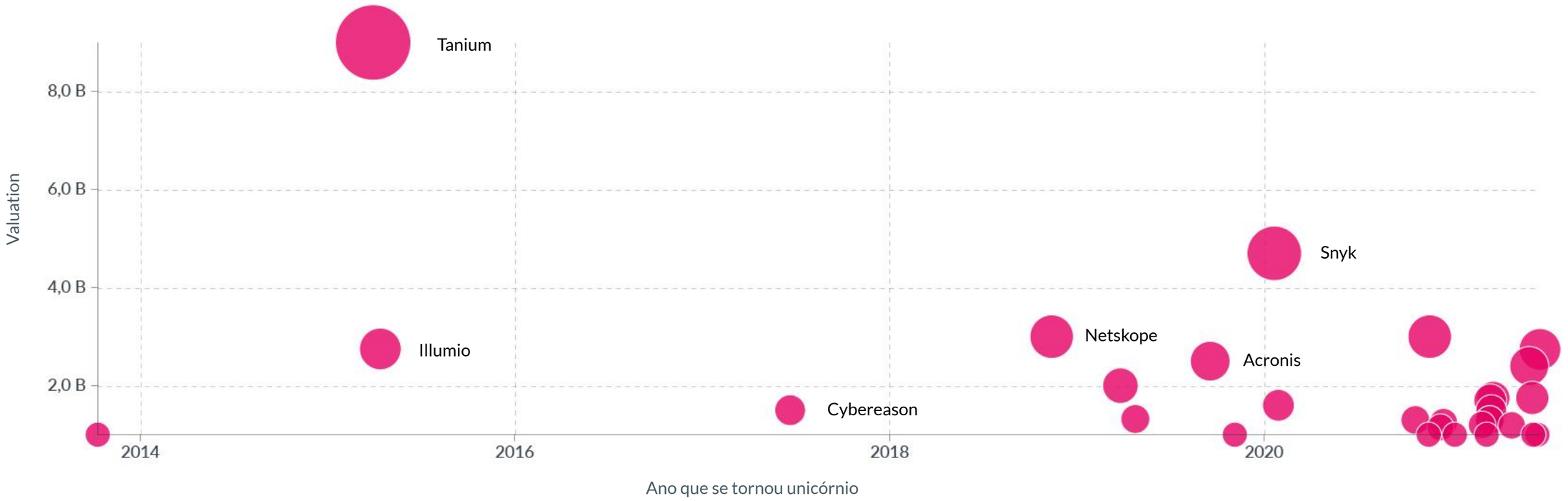
Aquisições em Cybersecurity



Dos 750 unicórnios ao redor do mundo, 30 são empresas de cibersegurança

O crescimento que o mercado cyber vem apresentando nos últimos anos é refletido diretamente no número de startups que atingiram o patamar de unicórnio (empresas com valor de mercado acima de US$ 1 B). Não à toa, o setor representa cerca de 5% do total de unicórnios. Interessante notar que 21 das 30 empresas alcançaram este patamar em 2020 ou 2021, o que evidencia a crescente preocupação com a segurança digital.

Unicórnios em cybersecurity



Trulioo

A plataforma da Trulioo fornece verificação em tempo real para seus clientes, de forma totalmente integrada e digital, com o objetivo de mitigar os riscos de fraudes e garantir maior conformidade regulatória. A empresa foi fundada em Vancouver e hoje possui escritórios em Dublin, San Diego e Austin.

Para garantir produtos de extrema qualidade e alinhados com as expectativas de seus clientes, a companhia acessa mais de 450 fontes de dados diferentes, incluindo informações de órgãos governamentais e agências de crédito, bem como registros telefônicos. De acordo com Steve Munford, CEO da Trulioo, existe uma combinação entre fontes tradicionais e não não tradicionais.

Neste ano a startup anunciou o recebimento de US$ 394 milhões em uma rodada de financiamento liderada pela TCV, o que avaliou a companhia em US$ 1,75 bilhão. A mega rodada de investimento ocorreu no momento em que a pandemia acelerou a digitalização de negócios e empresas de comércio eletrônico, fazendo com que os players precisassem de meios para verificar a identidade dos clientes a fim de manter as transações seguras.

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2011	Vancouver **Canadá**	US$ 474,8 M	American Express Ventures, Goldman Sachs Growth

Aura

Liderada e fundada por Hari Ravichandran, a Aura é uma empresa de tecnologia de segurança digital dedicada a criar uma Internet mais segura para todos. Seu produto carro-chefe recém-lançado, Aura, combina o uso de diferentes ativos para fornecer segurança digital de forma mais abrangente aos consumidores, apresentando roubo de identidade, fraude financeira e proteção de dispositivos em uma única plataforma, apoiada por uma unidade de atendimento ao cliente. Os produtos da empresa são utilizados por mais de 1,7 milhão de clientes, gerando mais de US $ 220 milhões em receita em 2020.

Fundada em 2019, a companhia teve um crescimento bastante acelerado, e dois fatores nos ajudam a explicar o movimento: o volume de investimento recebido e as aquisições realizadas. Ao todo, mais de U$ 450 milhões foram investidos na companhia por fundos como Accel, General Catalyst e WndrCo, além de Warburg Pincus. Grande parte deste capital foi utilizado na estratégia de expansão inorgânica, adquirindo a Intersections, Pango, FigLeaf e Privacy Mate, empresas de privacidade digital e segurança pessoal.

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2019	Burlington **Estados Unidos**	US$ 450 M	Accel, General Catalyst e WndrCo. e Warburg Pincus.

Sift

Para empresas como a Sift — que visa prever e prevenir fraudes online mais rápido do que os cibercriminosos adotam novas táticas — o aumento nos crimes cibernéticos também levou a um aumento nos negócios.

No ano passado, a empresa sediada em São Francisco avaliou o risco em mais de US$ 250 bilhões em transações, o dobro do que fez em 2019. A comapnhia tem mais de centenas de clientes, incluindo Twitter, Airbnb, Twilio, DoorDash, Wayfair e McDonald's, e também possui uma rede de dados global de 70 bilhões de eventos por mês.

Embora a empresa não revele números concretos de receita, o presidente e CEO Marc Olesen disse que os negócios triplicaram desde que ele ingressou na empresa em junho de 2018. A Sift foi fundada na Y Combinator em 2011 e arrecadou um total de $ 157 milhões ao longo de sua vida .

Um dos produtos da companhia, a plataforma "Digital Trust & Safety" visa ajudar os comerciantes a não apenas combater todos os tipos de fraudes e abusos na Internet, mas também a "reduzir o atrito" para clientes legítimos. Aparentemente, existe uma linha tênue entre cuidar de um comerciante e chatear um cliente que está legitimamente tentando conduzir uma transação.

A Sift usa aprendizado de máquina e inteligência artificial para supor automaticamente se uma tentativa de transação ou interação com um negócio online é autêntica ou potencialmente problemática.

FUNDAÇÃO	LOCALIZAÇÃO	TOTAL FUNDING	PRINCIPAIS INVESTIDORES
2011	São Francisco **Estados Unidos**	US$ 157 M	Insight Partners, Stripes, Spark Capital, Union Square Ventures.

Israel: Um polo de destaque

Israel se tornou lar de um ecossistema de cibersegurança avaliado em US$ 82 Bilhões, diversas soluções em diferentes segmentos, além de referência em atrair talentos que se interessam por segurança da informação. Recentemente, durante a 7º conferência anual de Cibersegurança promulgada pela Universidade de Tel Aviv, o então Primeiro Ministro do país reforçou que cyber security é um business que cresce geometricamente e que não existe uma solução permanente, o que a deixa com um valor imensurável.

O ecossistema israelense de cyber se desenvolveu com um apoio governamental extremamente presente. O Parque de tecnologias avançadas, sediado em Beer-Shiva abriga atualmente multinacionais gigantes, tais como Oracle, Dell EMC, IBM, e Deutsche Telekom, que trazem consigo centros de desenvolvimento dentro da área de segurança da informação. Dessa forma, o governo é agente primordial na transformação de Israel como um dos principais polos globais, e utiliza o apoio de instituições como a agência espacial israelita em cooperação nos trabalhos de desenvolvimento do ecossistema. Destaca-se que Israel é um país que nasceu com uma cultura militar enraizada, isso foi grande fator no desenvolvimento de políticas de segurança de uma forma geral, o que induziu o crescimento do polo de Cyber.

Atualmente, o país atrai talentos do mundo inteiro, sendo o primeiro país a oferecer um programa de PhD em segurança da informação, além de ter um ecossistema de inovação extremamente desenvolvido no setor.

© UNSPLASH

Investindo em Cyber: tese

Daniel Ibri
CIO
Mindset Ventures

A Mindset Ventures se posiciona como um fundo de Venture Capital Internacional. Qual é o mindset de investimento da Mindset Ventures?
Quando iniciamos a Mindset Ventures, nossa intenção era proporcionar aos investidores brasileiros a possibilidade de investirem em empresas disruptivas fora do Brasil e auxiliar essas empresas a expandirem suas operações para nosso país. Apesar de continuarmos focados em startups B2B desde o início, nossa tese foi se aperfeiçoando ao longo dos anos. Hoje, por exemplo, continuamos investindo em empresas *early stage*, mas de forma mais concentrada em Series A do que em seed. O fundamento por trás das empresas também permanece o mesmo (empresas voltadas para tecnologia), mas com o passar dos anos notamos que alguns segmentos oferecem oportunidades mais atrativas do que outros. E hoje já conseguimos entregar às nossas startups oportunidades de conexão em nível global, e não apenas com parceiros no Brasil, por exemplo. Em linhas gerais, nosso mindset nunca mudou estruturalmente, mas se aperfeiçoou muito desde que formamos a empresa. Ou seja, somos focados em empresas de tecnologia B2B, fundadas por empreendedores experientes, com soluções significativamente diferenciadas e com tração já comprovada.

Ao mesmo tempo em que permitimos aos nossos investidores acessarem empresas dos dois maiores hubs de tecnologia do mundo (EUA e Israel), proporcionamos às nossas startups ajuda em diversas vertentes, inclusive na expansão internacional.

A Mindset Ventures se destaca como um investidor institucional dentro do mercado de cibersegurança. O que vocês avaliam em startups que estão no setor?
Nossos critérios de avaliação de empresas são extremamente rigorosos, o que nos permite utilizá-los de forma uniforme para todas as empresas que analisamos, inclusive para startups de cyber. Este, no entanto, é um setor que exige um diferencial tecnológico muito claro para que a empresa tenha maior probabilidade de sucesso, talvez mais do que em outros setores, pois é um mercado significativamente concorrido. Seria difícil, por exemplo, apostarmos em uma empresa que desenvolveu mais um antivírus sem vantagens competitivas muito claras, afinal o mercado está inundado com este tipo de solução. Por outro lado, alguns segmentos dentro do mercado de cyber ainda são pouco explorados, e dentro deles vemos empresas com grande potencial de desenvolvimento. Há algum tempo, por exemplo, investimos na Eclypsium,

que oferece uma solução de proteção de firmwares de forma automática em larga escala. A Eclypsium é a única (ou uma das únicas) empresa até hoje que desenvolveu algo do tipo. Para o mercado de cyber especificamente, talvez até mais do que para todos os outros segmentos, olhamos muito para as dores dos clientes na hora de analisar uma startup. Ou seja, dado que o budget para cyber costuma ser menor do que para diversas outras frentes dentro das empresas, apenas investimos em startups de cyber cuja solução se mostra realmente necessária para seus clientes, e que não seja algo apenas desejável ou complementar.

O que nos permitiu ter tanto sucesso neste segmento foi a qualidade do dealflow que conseguimos gerar nos últimos anos. Como hoje temos uma presença muito forte em Israel, que é considerado um dos maiores hubs de startups de cyber do mundo, acabamos conseguindo desenvolver um acesso constante a empresas de enorme qualidade deste tipo. Por meio de uma análise criteriosa similar à que fazemos para empresas de outros setores (mas obviamente levando em consideração as peculiaridades de cada setor separadamente), conseguimos identificar os deals mais atrativos e investimos nas empresas de cyber que hoje temos em nosso portfólio. O mercado de cyber também requer empreendedores muito experientes, com grande conhecimento técnico do setor. Essa mão de obra qualificada é grande em Israel, principalmente pela influência do exército e capacitação desses empreendedores nas forças de segurança do país.

Como vocês avaliam o desenvolvimento do mercado de cyber no mundo e a ascensão de Israel como um dos principais polos do setor?

O mercado de cyber surge para suprir uma necessidade de proteção gerada pelos ataques cibernéticos e é de certa forma completamente dependente disso. Hoje, os ataques cibernéticos crescem exponencialmente ano a ano em quantidade e sofisticação, sendo cada vez mais difícil combatê-los e trazendo consequências cada vez mais graves e tangíveis. Anos atrás, por exemplo, mal existiam os ransomwares, que hoje estão gerando um estrago significativo em empresas ao redor do mundo todo. Mas, da mesma forma que os ataques evoluem a uma velocidade cada vez maior, os meios de combatê-los também se desenvolvem em velocidade similar. Curiosamente, apesar de muito se discutir sobre quem está à frente (os hackers ou as empresas de proteção), pouco se discute sobre o quanto as empresas e pessoas estão dispostas a adotar meios de proteção, sendo este o tema mais importante atualmente quando se discute formas de combater ataques cibernéticos. Em meio a isso, Israel tem se destacado nos últimos anos como um dos maiores polos de startups de segurança cibernética em função de algumas razões. A primeira delas é o fato de que quase todos os israelenses passaram anos servindo o exército após terminarem o estudo médio, o que de certa forma incentiva o empreendedorismo de forma geral, não apenas dentro do mercado de segurança cibernética. Ou seja, após cumprir o serviço militar obrigatório, muitos israelenses decidem empreender imediatamente depois, pois estudar em uma faculdade poderia tomar muitos outros anos e postergar a entrada no mercado de trabalho. Mesmo para os que prestam o serviço militar após a faculdade (em grande parte profissionais ligados ao campo de programação), o profissional acaba entrando no mercado de trabalho mais tarde do que na maior parte dos outros países, de

Investindo em Cyber: tese

Daniel Ibri
CIO
Mindset Ventures

certa forma incentivando o empreendedorismo. Em segundo lugar, enquanto estão servindo o exército, muitos israelenses acabam passando por atividades com cunho de proteção tecnológica, seja ela bélica ou totalmente digital. Desta maneira, cria-se um ambiente muito forte de incentivo natural ao empreendedorismo com exposição à proteção cibernética, e disso acabam surgindo iniciativas de segurança cibernética em quantidade e qualidade maiores que em outros países. Enquanto essa continuar sendo a realidade de Israel, o país deve continuar sendo referência no setor de segurança cibernética.

Como vocês enxergam os efeitos da pandemia dentro do setor de cibersegurança? Isso mudou de alguma forma a visão dos investidores no setor?

Apesar de a pandemia ter causado efeitos tanto a favor quanto contra as empresas de segurança cibernética, acreditamos que as contribuições para o desenvolvimento deste setor sejam maiores do que os impactos negativos.

A primeira grande causa da epidemia é, naturalmente, a adoção em massa do trabalho remoto. Apesar das vantagens desta política de trabalho, os funcionários passam a trabalhar em ambientes muito mais vulneráveis a ataques cibernéticos do que quando trabalhavam no escritório, muitas vezes em computadores pessoais sem qualquer tipo de antivírus ou dispositivo/software que lhes entreguem algum tipo de proteção. Esse aumento da vulnerabilidade é claramente negativo para a sociedade, mas ao mesmo tempo fomenta o surgimento de empresas voltadas justamente para a proteção nessas circunstâncias. No nosso portfólio, por exemplo, temos uma empresa que faz exatamente isso: a SAM. A startup israelense possibilita a proteção de diversos dispositivos a partir do roteador ao qual eles estão conectados.

O segundo grande efeito da pandemia é o surgimento de mais ataques cibernéticos. Algumas fontes indicam que os EUA passaram a ser uma das maiores origens deste tipo de ataque depois do início da pandemia, muito em função do desemprego gerado pela crise (o que incentiva este tipo de atitude criminosa) e do aumento da vulnerabilidade mencionada acima, encorajando a atividade de hackers. Como o mercado de segurança cibernética se desenvolve tão rapidamente quanto a atividade de ataques, podemos dizer que a circunstância acelerou o surgimento de startups que combatem este tipo de crime.

Por fim, a terceira grande consequência da pandemia foi a redução ou estabilização dos orçamentos das empresas para investimento tecnológico, o que de certa forma afeta negativamente este mercado. Apesar disso, hoje já notamos uma discussão muito grande acerca deste mercado, e a própria mídia vem retratando diariamente ataques de grande escala que poderiam ser facilmente evitados por meio de softwares relativamente simples de proteção, inclusive no Brasil. Dito isso, muito provavelmente nos próximos anos teremos uma grande ênfase para empresas deste setor, cuja importância deve se tornar cada vez mais clara e que deve passar a ser compreendido pelas empresas como investimento crucial para o bom andamento das operações. Com este destaque, é natural se esperar que ainda mais investidores sejam atraídos pelo setor, o qual deve se valorizar ainda mais na medida em que se tornar mais reconhecido.

Investindo em Cyber: tese

Daniel Ibri
CIO
Mindset Ventures

Como vocês enxergam o futuro do setor de cibersegurança no mundo?

A tecnologia estará presente cada vez mais intensamente em nossas vidas, e a pandemia mostrou o quão verdadeira essa afirmação realmente é. Hoje, dependemos da tecnologia mais do que nunca para todos os aspectos da nossa vida. Quando trabalhamos, estamos praticamente o tempo todo em contato com computadores. Nos momentos de lazer, não raramente também temos a tecnologia como centro das atenções (streaming de vídeo, redes sociais, videogames). E, como se não bastasse, estamos o tempo todo com um celular no bolso, com potência de processamento igual a computadores de poucos anos atrás. Este contato deve se tornar cada vez mais frequente e intenso. O problema, no entanto, é que, da mesma forma que a tecnologia foi criada por nós, ela também pode ser desconstruída por nós. Isso significa que a tecnologia é vulnerável a ataques e, quanto mais intensamente vivemos com ela e mais dependemos de suas funcionalidades, mais frequentes e maiores são os estragos causados por estes ataques mal-intencionados.

Neste sentido, dado que a tendência de adoção tecnológica é clara e aparentemente irreversível, empresas de segurança cibernética passam a ganhar uma importância enorme na sociedade, evitando que a tecnologia se vire contra nós no sentido de causar mais problemas do que soluções. Em nossa visão, este setor se desenvolverá tão aceleradamente quanto os ataques cibernéticos crescerem, e empresas deste tipo terão que estar sempre um passo a frente dos hackers para que possam combatê-los efetivamente. Acreditamos que este seja um caminho sem volta. Da mesma forma que hoje não conseguimos, por exemplo, conceber a ideia de uma sociedade sem forças policiais, em alguns anos não conseguiremos enxergar a sociedade sem presença de empresas voltadas para proteção cibernética.

Investindo em Cyber: tese

Daniel Ibri
CIO
Mindset Ventures

Tendências

O que deve ser destacado no futuro da cibersegurança no Brasil?

Para qual direção estamos indo?

Josemando Sobral
Co-Founder
Unxpose

A pandemia de COVID-19 alterou significamente a maneira como o mundo opera em diversos aspectos e serviu para impulsionar mudanças no formato de trabalho de empresas de todos os tamanhos. O trabalho remoto, que sempre foi uma dúvida, acabou virando uma norma do dia para a noite, e vários negócios tiveram que se adaptar na mesma velocidade. Um ano depois os efeitos da pandemia começam a diminuir em alguns países por causa da vacinação, e enquanto algumas empresas começam a falar sobre a volta aos escritórios, várias pesquisas mostram que uma parcela grande da força de trabalho deseja continuar trabalhando de casa ou em um modelo misto de presencial. Um levantamento realizado em junho de 2020 com os empregados de uma grande mineradora brasileira identificou um grau de favorabilidade ao trabalho remoto de 73% de seus colaboradores.

Essa mudança de comportamento traz benefícios, mas também novos riscos. Home offices são normalmente menos protegidos do que escritórios, já que não possuem equipamentos de proteção, como firewalls, gerenciados por times de TI corporativo.

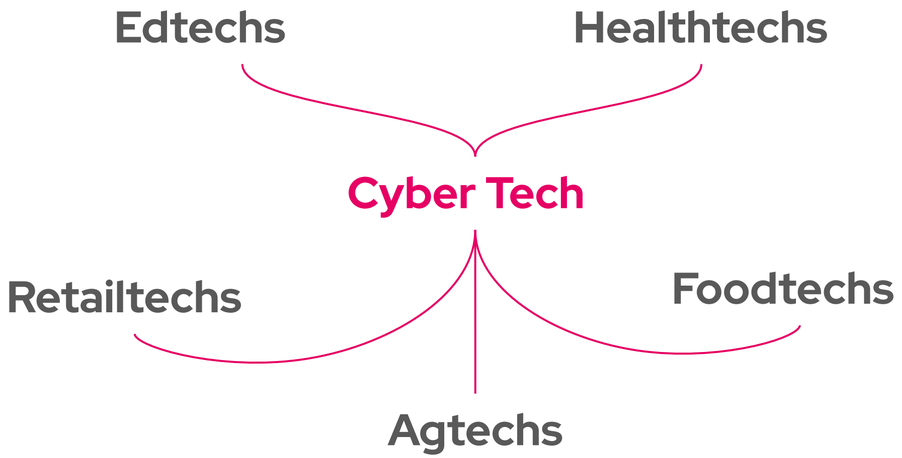
Dados sensíveis das empresas trafegam por meio de roteadores wifi domiciliares de forma não criptografada. Via de regra, esses equipamentos são configurados com senhas fracas, facilitando a interceptação dos dados por cibercriminosos. Além disso, houve uma redução ainda maior da divisão entre equipamentos pessoais e corporativos, com o uso comum de aplicativos de comunicação corporativa como Slack, Teams e Zoom em smartphones pessoais.

Nesse cenário, o trabalho remoto aumentou a superfície de ataques e hackers possuem mais oportunidades para explorar dispositivos e redes vulneráveis de funcionários. Isso aumenta consideravelmente a chance de vazamento de dados sensíveis. Um levantamento da Fortinet revela que apenas no primeiro trimestre de 2020 o Brasil sofreu 3,2 bilhões de tentativas de ataque, com investidas constantes na execução de código remoto em roteadores domésticos.

Setor da Saúde é destaque negativo como alvo de ataques cibernéticos

O setor de saúde se tornou um grande alvo de crimes cibernéticos, o que fez com o que a Organização Internacional de Polícia Criminal (INTERPOL) enviasse um alerta direcionado à hospitais e empresas que atuam diretamente contra a COVID 19. Na Alemanha, houve caso de óbito em um hospital de Dusseldorf por uma falta de atendimento em decorrência da inacessibilidade dos sistemas durantes uma ataque de ransomware , enquanto no Brasil o ataque ao grupo Fleury se tornou destaque por paralisar completamente as atividades da empresa durante dias.

De toda forma, todas as corporações lidam com dados sensíveis, sejam de clientes ou de colaboradores, que precisam estar seguros da melhor forma possível. Cibersegurança é necessária desde o princípio de uma cultura de proteção de dados na corporação até soluções complexas de proteção. Identificação e manutenção de identidade (ID and Access Management, em inglês) se torna destaque no ecossistema brasileiro por uma demanda latente das corporações de garantir, principalmente em uma realidade de trabalho remoto, que apenas pessoas autorizadas tenham acesso a informações, pois uma simples quebra de protocolo pode abrir uma brecha para ataques que trarão prejuízos milionários, além de diminuir a confiança dos clientes na empresa atacada. Entretanto, reforça-se a necessidade de novas soluções brasileiras consolidadas nas categorias voltadas às barreiras de proteção de ataques diversos, como N*etwork & Infrastructure Security* e *Web Security*.



Trabalho remoto deve permanecer como tendência

Apesar de gradativamente muitas atividades estarem retornando ao trabalho presencial, muitas corporações já utilizam o home-office ou o trabalho híbrido como forma definitiva. Um levantamento realizado pela FIA Employee Experience (FEEx) mostrou que 90% das empresas entrevistadas adotaram alguma forma de trabalho remoto durante o ano de 2020, e o resultado foi uma resposta de 90% dos colaboradores avaliando o home-office como ótimo ou bom, embora 60% das empresas tenham relatado algum tipo de problema na implementação ou no dia a dia de trabalho.

O trabalho remoto permite a quebra de fronteiras, busca de talentos no mundo todo e mão de obra qualificada muito mais rapidamente. Dessa forma, observa-se movimentos de grandes empresas como o Twitter de adotarem permanentemente o home office. Além disso, brasileiros capacitados estão sendo procurados por empresas estrangeiras devido a desvalorização do real frente ao dólar. Movimentos semelhantes estão ocorrendo em diversos segmentos, que perpetuam a continuidade de trabalho remoto como relevante dentro do mercado.

Dessa forma, como já exposto neste report, o trabalho em home office necessita de uma série de protocolos de segurança para garantir a proteção de dados de uma corporação. Espera-se que esse movimento de tendência seja positivo para o mercado de segurança global e brasileiro.

LGPD mudou a preocupação das empresas com informação

A Lei 13.709, mais conhecida como Lei Geral de Proteção de Dados, passou a valer em 2020 e impôs uma gama de desafios às empresas brasileiras, que por necessidade passaram a ter um olhar diferenciado para segurança da informação e o tratamento de dados pessoais dos clientes e dos colaboradores. Um dos principais méritos dessa lei é induzir as empresas a de fato terem uma cultura que preza pela segurança de informações sensíveis, como exposto neste report.

Ademais, a LGPD prevê que empresas adotem medidas de segurança técnicas e administrativas que estejam aptas a de fato protegerem os dados da corporação, e prevê mitigação de sanções para empresas que adotarem mecanismos e procedimentos internos que minimizem eventuais danos causados por ataques cibernéticos, o que **estimula empresas a investirem em Cyber Security**. Ademais, diversas soluções surgem no intuito de ajudar corporações a se encaixarem nas conformidades da nova lei, que precisam se adaptar à nova realidade.

Dessa forma, a LGPD surge em um momento em que o ecossistema brasileiro de Cibersegurança precisa de um incentivo, e a obrigatoriedade de um olhar diferenciado para segurança da informação tende a ser um estimulante notável.

Glossário

Se você não entendeu alguma coisa...

Glossário

Ameaça: Causa potencial de um incidente.

Ativo: Tudo aquilo que possui valor.

Ativo de Informação: Patrimônio intangível da corporação,, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a organização por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da organização ou por infraestrutura externa, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Confidencialidade: Propriedade dos ativos da informação da corporação, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Controle: Medida de segurança adotada pela corporação para o tratamento de um risco específico.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da corporação

Integridade: Propriedade dos ativos da informação da corporação, de serem exatos e completos.

Risco de Segurança da Informação: Efeito da incerteza sobre os objetivos de segurança da informação da corporação.

Segurança da Informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da corporação.

Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da corporação

Engenharia Social: Manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais.

Acha que faltou algum termo? Manda pra gente!

Corporates members