OPINIÃO

Cinco técnicas para ter sucesso nas negociações

Haroldo Matsumoto (*)

Desenvolver algumas habilidades, usar táticas simples e refletir sobre os objetivos e a estratégia de negociação podem ser chaves para o sucesso.

Negociar faz parte do dia a dia de todo empresário ou líder. Em qualquer empresa, todo o tempo negociam-se prazos, salários, carga de trabalho, preços, orçamentos, contratos, investimentos. Portanto, dominar as técnicas e adquirir habilidades de negociação são pré-requisitos para o sucesso nos negócios.

Nem todo gestor, no entanto, gosta de negociações ou se sente apto e confortável no papel de negociador. Muitos até evitam ao máximo a tarefa de fechar negócios ou procurar um acordo, mesmo que essa recusa traga prejuízos ao empreendimento.

O escritor e coach David Finkel sabe dessas limitações e escreveu para a "Inc." sobre as cinco habilidades mais importantes para quem quer dominar a arte da negociação.

1. Tenha clareza de objetivos

A maioria das pessoas entra em uma negociação sem saber exatamente o que quer. Para ter metas claras, é importante responder três perguntas: qual é o melhor resultado que posso obter; qual é o meu ponto de partida, ou seja, o mínimo que considero aceitável; qual é meu plano B, isto é, o que fazer se o acordo não for possível.

Pensar sobre essas três questões antecipadamente torna as negociações muito mais fáceis.

2. Defina a estratégia de negociação

Estabelecer o ponto central da negociação antes de sentar à mesa ou pegar o telefone é outro aspecto fundamental. Uma boa estratégia fará com que você se aproxime do melhor resultado possível, enquanto uma estratégia mal pensada poderá levar ao fracasso total.

Mas o que significa definir a estratégia central? É determinar a porta de entrada na negociação. Você vai negociar com base no preço ou vai pôr o foco na confiabilidade? Vale apelar para a segurança ou explorar a questão da concorrência?

A resposta depende de cada negociação. É importante conhecer a outra parte para escolher a estratégia mais adequada.

3. Conheça seu perfil

Alguns negociadores costumam ser agressivos, enquanto outros são tímidos e quase sempre acabam aquiescendo.

Alguns são envolventes, já outros são duros e irredutíveis. Há vários tipos de negociadores e é importante que você conheça sua personalidade, seu estilo e suas preferências, reflita sobre seu comportamento em negociações passadas e como se sentiu em relação a elas.

Essa reflexão permite que você trabalhe seus pontos fracos, foque nos pontos fortes e cresça como negociador.

4. Crie motivação

Procurar descobrir o que leva a outra parte a desejar um acordo com você ou sua empresa é um exercício poderoso na negociação. Um truque é fazer perguntas que ajudem a construir uma motivação na sua contraparte.

Se você está adquirindo um serviço, por exemplo, pode questioná-la sobre seus concorrentes e em que ela se diferencia deles.

5. Mostre-se relutante

Em quase toda negociação há uma parte ansiosa e outra relutante. Com algumas táticas, é possível mostrar-se resistente, forçando sua contraparte a assumir o segundo papel. Como?

Use sua linguagem corporal para mostrar resistência. Os ansiosos ficam tensos e inclinam o corpo para a frente, parecendo que estão para disparar em uma corrida. Os relutantes, por sua vez, sentam-se mais afastados da mesa e mantém seus corpos relaxados, demonstrando que não estão aflitos para fechar o acordo.

Manipule sua voz para que soe relutante também, falando de forma pausada e suave. Pessoas ansiosas tendem a falar rápido e em alto volume.

Por último, não mostre emoção nos seus comentários e ponderações. Em vez de dizer "sim, vamos fazer isso!", diga frases como "funcionaria para você se pudéssemos fazer isso?".

(*) É sócio-diretor da Prosphera Educação Corporativa, consultoria especializada em gestão de negócios.

Vivenciamos uma onda de ataques cibernéticos

Em paralelo à pandemia de Covid-19, percebemos um aumento acentuado nas atividade de cibercriminosos. De simples ataques de phishing a um dos maiores ataques DDoS já registrados, vimos o cenário de ameaças cibernéticas evoluir.

Ivan Marzariolli (*)

Pexels

Ao mesmo tempo, observamos o crescimento da indústria de tecnologia e cibersegurança. Desde a implementação do 5G em muitas partes do mundo até o crescimento exponencial das aplicações de SaaS, vimos que a pandemia também trouxe mudanças positivas.

As mudanças trazidas não vão parar de um momento para o outro. Os efeitos dessa pandemia serão duradouros para indústria de TI. Além disso, alguns dos desafios introduzidos em 2020 continuarão a afetar a cibersegurança. A seguir, algumas das tendências de segurança em alta:

Uma onda de crimes cibernéticos

O ano de 2020 foi movimentado para invasores e hackers, bem como para as equipes de cibersegurança. Com a eleição norte-americana em 2020, houve um aumento nas atividades cibernéticas antigovernamentais, um exemplo disso foi o ataque à FireEye, supostamente por uma entidade patrocinada por uma nação estrangeira, onde muitas ferramentas foram roubadas para uso em ataques posteriores.

Em 2021, além de frequentes, essas invasões serão muito específicas em relação aos seus alvos. A espionagem internacional será um dos principais motivadores dos ataques cibernéticos e os fornecedores de segurança serão atacados e afetados em um ritmo ainda maior. Mesmo os incidentes que aconteceram em 2020, como o envolvendo a FireEye ou o ataque Sunburst que visou a cadeia da SolarWinds, terão efeitos duradouros. Percebemos apenas o início. Os investigadores suspeitam, por exemplo, que até 250 organizações podem ter sido comprometidas no ataque da SolarWinds. Os resultados reais ainda estão por vir.

Esses incidentes propiciam oportunidades para outras variantes/ramificações nos já existentes, só que também impulsionarão a inovação da segurança em 2021.

A Intelligent Edge será armada

Uma inovação impulsionada pelo 5G é a implementação da edge computing multiacesso (MEC). Construir inteligência na edge (borda) aumentará a disponibilidade e a eficiência das redes 5G. No entanto, mantendo as tendências de cibersegurança global em mente, podemos ver que a borda inteligente pode ser sequestrada por invasores para lançar diferentes tipos de ataques, tanto nas redes centrais (core) móveis, como nas vítimas fora do domínio do provedor de serviços que foi comprometido. A MEC pode ser usada para propagar malware em diferentes redes, para recrutamento de drones em botnets IoT (Internet das Coisas).

Ataques DDoS de baixo volume serão frequentes

Em 2020, embora tenhamos visto um dos maiores ataques DDoS já registrados cujo alvo foi um nome conhecido na indústria de TI, também percebemos que vários ataques DDoS passaram despercebidos pois apesar da frequência ter sido muito alta, felizmente o volume não foi. Esse tipo de ataque manterá a indústria de segurança ocupada em 2021 e podem ser instrumentais para desabilitar as infraestruturas de segurança ou apenas atuar como uma cortina de fumaça para ataques de malware expressivos, como o ataque Sunburst.

Cinco milhões de armas DDoS serão adicionadas ao arsenal global de DDoS

Os pesquisadores de segurança observam que o número de armas DDoS dobrou de cerca de seis milhões em 2019 para 12,5 milhões em 2020. Essa tendência se mantém em 2021, pois mais dispositivos IoT estarão online a cada dia, ou seja, haverá uma estimativa de aumento de, pelo menos, cinco milhões de armas.

Esse número elevado de armas permitirá que os invasores lancem outro ataque DDoS recorde ainda em 2021. E vamos aguardar para ver se uma ocorrência como essa será tornada pública ou não.

O ano da confiança zero

Em 2020 compreendemos o que é o modelo Zero Trust na prática. Ao longo dos meses, vimos fornecedores de segurança alinharem suas soluções, ajustar o modelo e as políticas internas conforme obtiveram mais clareza sobre o que significa ser um usuário de rede ou de dispositivos móveis coerente com o conceito Zero Trust. A pandemia de COVID-19 acelerou a mudança para SaaS e tornou o modelo de "trabalho a partir de casa" uma alternativa viável.

As organizações compreenderam que Zero Trust não é adotar um fornecedor ou dispositivo específico, mas sim uma série de políticas estratégicas e mudanças na prática para melhorar a segurança. Uma implementação bem-sucedida requer uma boa compreensão do que é o modelo Zero Trust, assim como quais as diversas soluções que precisam funcionar em uníssono para permitir sua implementação.

Por ter atingido o nível de maturidade e clareza, acreditamos que o conceito de Zero Trust será efetivamente adotado e implementado por muitas organizações em 2021, e se tornará o ideal de segurança para todos os tipos e tamanhos de empresas.

Adoção SASE vai acelerar

Com uma parte expressiva das pessoas trabalhando de forma remota, os invasores têm experimentado novos jeitos de explorar brechas ou deficiências de segurança evidenciadas por essas rápidas mudanças. O que acelerou o desenvolvimento e a adoção de soluções SASE - Secure Access Service Edge.

Porém, a mudança para a nuvem não acontece de um dia para o outro, pois muitas organizações mantêm a maior parte de seus recursos hospedados on-premise (localmente). Por outro lado, é provável que continuem a manter o trabalho remoto e voltem ao modelo anterior de negócios assim que a vacina para COVID-19 se tornar disponível.

Num outro cenário, muitas organizações já começaram o processo de mudança de um modelo de negócios on-premise para aquele baseado em SaaS - Software as a Service, o que está se acelerando com a pandemia. Em resumo, o SASE é uma parte essencial da infraestrutura de segurança corporativa.

Esse é o ano do protocolo TLS 1.3 brilhar

O protocolo TLS 1.3 finalmente começará a ter uma adoção generalizada, em parte, impulsionado pela adoção do QUIC/HTTP3, visto que o TLS 1.3 está integrado nele. Muitos fornecedores já oferecem suporte ao TLS 1.3 e isso ajudará a conduzir esse protocolo para que predomine. Mudanças também serão feitas no TLS 1.3 standard conforme a demanda por SNIs criptografados se acelere.

Dito isso, o TLS 1.2 ainda será a escolha mais amplamente utilizada como protocolo de criptografia na Internet, já que mudar para a versão recente pode ser caro para muitas organizações. Mas, à medida que o QUIC/HTTP3 se tornar mais amplamente utilizado até o final do ano, podemos verificar essa mudança.

Se 2020 nos ensinou algo, é que não podemos considerar nossa segurança e daqueles que nos rodeiam como garantida. Temos que estar vigilantes em tempos de crise. O que se aplica também à cibersegurança. Enfrentamos ameaças novas e persistentes de todas as formas e tamanhos, e precisamos nos certificar de que as enfrentaremos da melhor maneira possível. 2021 está se configurando como o ano das ciber ameaças, o que traz impulso às inovações em segurança como não tínhamos visto anteriormente.

(*) É Country manager da A10 Networks.

Schneider Electric agora disponível na Amazon

Seguindo a tendência de mercado 2021 de investimento em e-commerce e em transformação digital, a Schneider Electric estreia sua "brand page" na Amazon (https://www.amazon.com.br/stores/Schneider+Electric+Brasil/page/CBAE8921-D3A6-46EC-A098-21E3232FE278), um dos maiores e mais conhecidos marketplaces do mundo.

A loja oficial da Schneider Electric na Amazon é calcada no conceito #CustomerFirst, ou seja, na ideia do cliente ter mais uma opção de compra, que proporciona agilidade e comodidade, tanto de acesso quanto de entrega.

News @TI

ricardosouza@netjen.com.br

Adistec Brasil fortalece parceria com a Imperva

@A Adistec, distribuidora de valor agregado com foco em infraestrutura para Data Centers e Segurança da Informação, reforça parceria no Brasil com a Imperva®. Com 18 anos de experiência no mercado de TIC, a Imperva® é uma empresa especializada no desenvolvimento soluções de segurança cibernética, que fornece proteção a dados e aplicações para mais de 6.200 clientes e 150 países. Para Emerson Lima, Product Sales Manager da Adistec Brasil, a parceria com a Imperva® chega para potencializar a operação da empresa. "Uma das nossas estratégias para 2021 é o fortalecimento da nossa rede de revendas para expandir nossa presença em todo o país, especialmente nas regiões Centro-Oeste, Norte e Nordeste. Nesse sentido, a Imperva® completa nosso portfólio com sua tecnologia de ponta, nos dando a chance de oferecer aos canais uma solução de segurança cada vez mais completa", comenta Lima (www.adistec.com).

ISH Tecnologia monitora deep e dark web em busca de vazamento de dados

@A ISH Tecnologia, líder nos segmentos de cibersegurança, infraestrutura crítica e nuvens blindadas, anuncia o primeiro produto totalmente desenvolvido pelo ISH LABS, seu braço de desenvolvimento de novas tecnologias. O Mantis é uma plataforma de Proteção e Monitoramento de Riscos Digitais, que varre a internet em busca de informações sensíveis de seus clientes, especialmente na deep e dark web. "Nossos clientes podem contar com a inteligência embarcada no Mantis para manter um monitoramento permanente de seus ativos digitais mais sensíveis, sendo imediatamente alertados caso alguma informação seja vazada em qualquer camada da Internet, como deep e dark web", afirma Allan Costa, diretor de inovação e alianças da ISH Tecnologia (https://ish.com.br/).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)**

Publisher: **Lilian Mancuso** (lilian@netjen.com.br)

Editorias

Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);

Comercial: Tatiana Sapateiro – tatiana@netjen.com.br

Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza. *Revisão:* Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Jornal Empresas & Negócios Ltda

Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080 – Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br) – Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90 - JUCESP, Nire 35218211731 (6/6/2003) - Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

RIO DE JANEIRO: **J.C. REPRESENTAÇÕES E PUBLICIDADES EIRELI**
Av. Rio Branco, 173 / 602 e 603 – Centro - Rio de Janeiro - CEP 20040-007
Tel. (21) 2262-7469 – CNPJ 30.868.129/0001-87