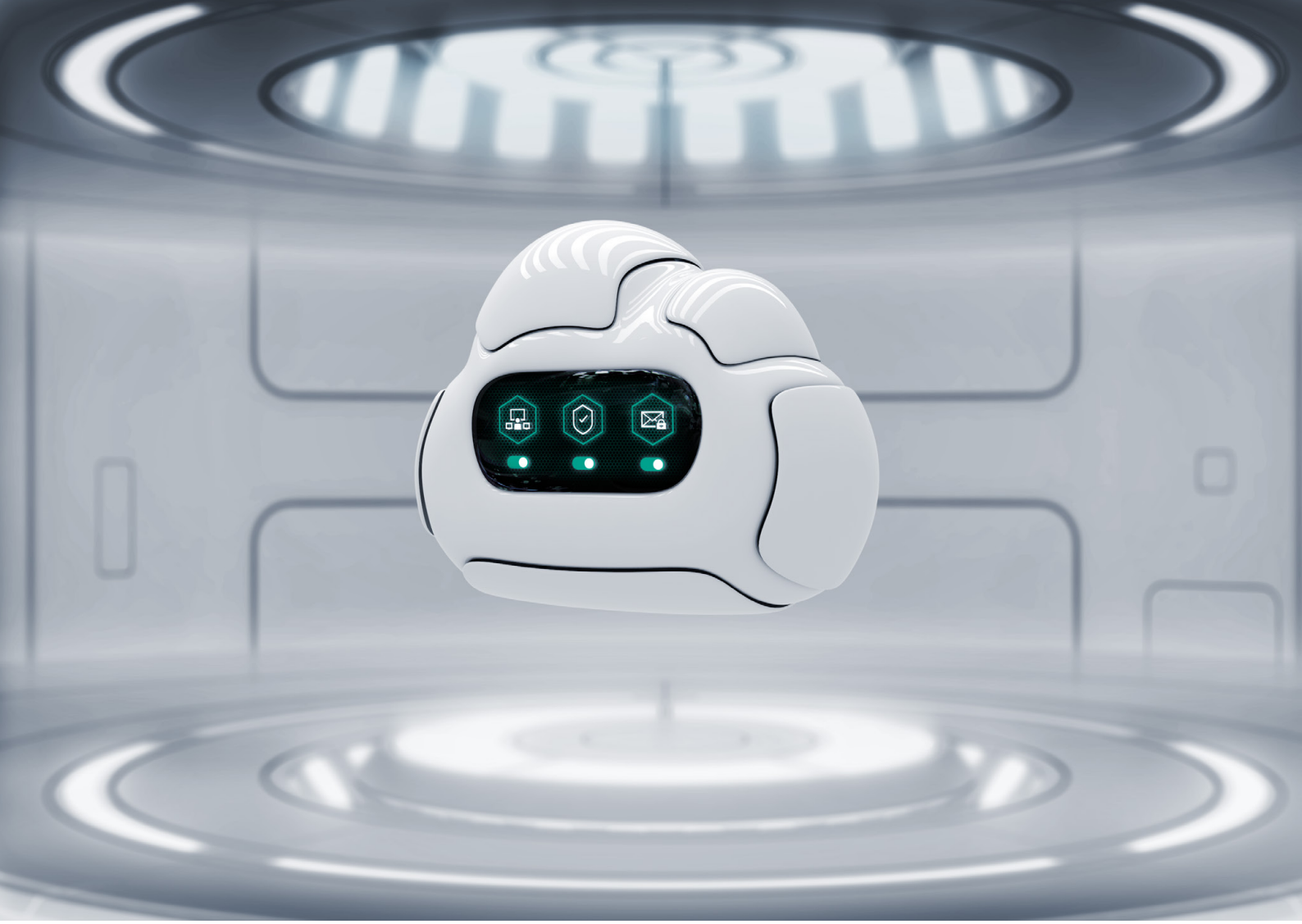

Reputação e cibersegurança: do risco à oportunidade

kaspersky

Reputação e cibersegurança: do risco à oportunidade

"São necessários 20 anos para construir uma reputação e cinco minutos para destruí-la. Pense nisso e você fará as coisas de maneira diferente". (Warren Buffett)

Os limites do medo como motivador – percepções da psicologia
O medo é útil. De acordo com os neurocientistas do Hospital Karolinska, em Estocolmo, "a função do medo é motivar os organismos a lidar com as ameaças que prejudicaram a sobrevivência ao longo da evolução".

Mas as respostas defensivas do medo (congelamento/combate/fuga) não foram criadas para enfrentar os problemas no local de trabalho moderno. O combate desempenha um papel no contexto de um incidente virtual imediato, mas a resposta do combate pode ser um instrumento pouco preciso e sempre focado no curto prazo.

Psicóloga
Christine Tappolet (Université de Montréal) faz este ponto de forma breve: "O medo influencia o que fazemos, restringindo o foco do agente [ou seja, o nosso]". Agora, estamos focados apenas na ameaça à nossa frente, às custas de ver o cenário mais amplo.

Na psicologia, é feita uma distinção entre a Motivação por aproximação (atração por algo positivo, impulsionado pela esperança) e a Motivação por afastamento (distanciamento de algo negativo, guiado pelo medo). Ambos têm um papel a desempenhar mas, como afirma o psicólogo Andrew Elliot (Universidade de Rochester), "a Motivação por afastamento foi feita para possibilitar a sobrevivência, ao passo que a Motivação por aproximação foi feita para facilitar o crescimento".

Neste artigo, convidamos você a se juntar a nós na transição da sobrevivência para o crescimento, aproveitando a oportunidade de trabalhar em direção a um objetivo extremamente positivo: conquistar uma reputação poderosa e magnética, reforçada por uma abordagem de segurança virtual confiante.

Começamos com um fato muito básico e incontestável: os incidentes cibernéticos podem (e causam) prejuízos à reputação da empresa. É muito simples: seus clientes esperam que você mantenha os dados seguros e as operações em execução; se você não puder, eles encontrarão alguém que possa. Além do mais, o risco de danos à reputação de incidentes virtuais está aumentando.

O valor da reputação não é novidade: sempre foi um dos recursos mais importantes que uma empresa pode possuir (isso também vale para as pessoas, pense nisso). Os clientes não compram apenas uma solução, um serviço ou um produto; eles compram uma marca, uma ideia, uma promessa de algo maior. A confiança é muitas vezes o que fecha o negócio.

Na era digital, dois principais fatores tornaram a defesa da reputação ainda mais urgente do que nunca. O primeiro é o crime cibernético, que expõe as empresas ao ataque de agentes maliciosos remotos e invisíveis, cujas ações podem tornar empresas vulneráveis. O segundo é o contexto digital mais amplo das mídias sociais, notícias instantâneas e sites públicos de análise, como Trustpilot, G2, Feefo e mais. Combinadas, essas duas forças representam não só uma frente de batalha maior e mais ampla do que nunca, como também o desafio de conter qualquer notícia negativa (incluindo rumores) se tornou interminável.

Junte-se a nós para explorar as oportunidades de gerenciamento de reputação e segurança virtual

Precisamos conversar sobre o risco da reputação em incidentes virtuais e, neste artigo, faremos isso, com fatos reais que você precisa saber para se comprometer a defender e proteger a preciosa (e merecida) reputação de sua empresa por um futuro lucrativo.

Mas também vamos olhar para a interação entre a segurança virtual e a reputação de um ângulo completamente novo, que, infelizmente, falta no discurso moderno sobre o tema. Além de fornecer conhecimentos críticos sobre o combate, também convidamos você a explorar a riqueza de oportunidades que o desafio de reputação representa, no contexto de segurança virtual e além.

Acreditamos que uma posição meramente defensiva é lamentavelmente ambiciosa: falha em fazer justiça aos seus negócios, clientes, missão ou valores. Em vez disso, estamos propondo um conceito totalmente novo: o orgulho cibernético. O medo desempenha um papel muito válido, obrigando-nos a tomar as ações necessárias, mas queremos levá-lo muito além dessa posição defensiva e entrar em um mundo em que a reputação seja estimada, cultivada, celebrada e não seja mais guardada com zelo como uma princesa em uma torre.

Conheça os três caminhos da reputação

Reputação não é indestrutível Ela é construída pelas ações cumulativas das três vias principais, e igualmente pode ser destruída por incidentes em qualquer uma dessas mesmas vias. Eles (em nenhuma ordem específica) são os seguintes:

1. Novidades sobre produtos
2. Marca
3. Segurança

Neste artigo, nossa principal preocupação é o terceiro caminho da reputação, a segurança, mas é bom dizer algumas coisas sobre os outros dois primeiro, porque há uma interação significativa entre os três.

Caminho da reputação 1: produto

Este parece muito simples: o seu produto é bom, os seus clientes sabem que é bom, e por isso você é escolhido em vez dos seus concorrentes. Num mundo ideal, a reputação dependeria apenas do produto isoladamente. Afinal, não seria maravilhoso se tudo que tivéssemos que fazer fosse criar um produto bonito e esperar as vendas chegarem?

Crédito em seu devido lugar: por que acreditar é tudo?
Quando seus clientes compram de você, eles creditam sua conta com dinheiro em troca de produtos ou serviços. A palavra "crédito" vem do latim "credere", que significa acreditar. Essa crença (ou falta dela) é o que impulsiona as decisões de compra em todos os lugares, do indivíduo às grandes empresas. Seus clientes escolhem seus produtos porque acreditam (crédito) que você pode entregar de uma maneira que seus concorrentes não. Essa crença está por trás da transação financeira, que incorpora a confiança que seus clientes depositam em você. Essa confiança é conquistada e fortalecida por meio de um dos ativos mais fenomenais que sua empresa pode cultivar: reputação.

... e não são apenas seus clientes que lhe dão crédito
Não devemos esquecer que seus clientes não são o único grupo para quem sua reputação é importante quando se trata de crédito, crença e reputação. Sua empresa precisa ter acesso ao crédito financeiro real, e os danos à reputação podem afetar negativamente sua classificação de crédito, dificultando o investimento e o crescimento. Os prêmios de seguro também podem ser impactados negativamente por danos à reputação, com as seguradoras cobrando somas maiores às empresas cujas reputações de segurança virtual são consideradas mais fracas.

Caminho da reputação 2: marca

Um caminho particularmente moderno, a marca tem um grau de influência sobre a reputação da sua empresa, que só cresce à medida que o mundo se torna maior (pelo tamanho potencial do mercado) e menor (pelo poder da Internet) do que nunca. A marca aborda o fato de que os clientes compram mais do que apenas um produto, compram uma ideia ou até um sentimento (às vezes por meio de tribos) que desejam. Se seu produto é bom, mas sua marca é ruim, você pode criar, criar e criar com todas as suas forças, mas os clientes simplesmente não vai vê-lo.

Caminho da reputação 3: segurança

O que você geralmente ouve sobre o caminho da reputação de segurança é que a sua ausência tem o poder de destruir qualquer um dos benefícios alcançados por um produto ou marca de uma única vez por um criminoso virtual. Vamos inverter completamente essa forma de ver a segurança virtual neste artigo, mas não podemos evitar o fato, cada vez mais lamentável, de que os incidentes causados a este caminho podem e causam enormes danos a qualquer bom trabalho realizado por meio dos outros.

Vamos virar o jogo o mais rápido possível. O caminho da reputação de segurança representa as três áreas importantes, que acompanhamos abaixo com as principais perguntas trazidas pelos seus clientes:

- Dados do cliente – você me respeita?
- Fornecimento contínuo e seguro (vs. latência) – posso confiar em vocês em não atrasar entregas?
- Competência – vocês sabem o que estão fazendo?

Conhecendo melhor alguns fatos reais

A reputação não pode ser deixada pra depois quando se trata das estratégias de segurança de TI (ou qualquer estratégia de negócios, pense nisso). A reputação é a âncora que faz nossos clientes acreditarem no poder de nossos produtos e serviços, não apenas por entregar, mas por entregar além dos de nossos concorrentes. A mensagem primordial da reputação é a **confiança.**

Como sabemos tudo isso: Pesquisa de riscos corporativos internacionais de segurança de TI da Kaspersky

Há nove anos, anualmente a Kaspersky realiza uma enorme pesquisa internacional sobre riscos corporativos de segurança de TI para descobrir exatamente o que as empresas passam quando sofrem com um incidente de segurança. A pesquisa abrange 23 países e inclui dados de quase 5.000 entrevistas com líderes de negócios em todo o espectro. Os dados deste estudo impressionante informam tudo o que fazemos, garantindo que nossos produtos e serviços continuem resolvendo problemas reais para um mundo mais que real.

O caminho da reputação de segurança e o resultado final – fatos de nossa pesquisa

É muito fácil se empolgar falando sobre o valor da reputação e flutuar nas nuvens de conversas fofas de marketing (não que o marketing não tenha um papel a desenvolver), mas é o resultado final que conta. É por isso que nossa pesquisa indica o custo financeiro exato dos incidentes de segurança. Precisamos saber o tamanho da fera com a qual estamos lidando, se quisermos derrotá-la.

Para os fins deste artigo, analisamos quatro categorias que comprovam as perdas financeiras específicas relacionadas à reputação que ocorrem no caso de um incidente virtual:

1. Perda de negócios
2. Prejuízo na classificação de crédito e aumento do prêmio de seguros
3. Custos de RP para limitação de incidentes e reparo da reputação
4. Custos de compensação (o ato se desculpas por meio de reparação financeira)

Veja como cada uma dessas quatro áreas é afetada pela média de incidentes virtuais de pequenas, médias e grandes empresas:

Categoria de perda	PMEs 2019	Grandes empresas 2019
Perda de negócios	US$ 13.000	US$ 163.000
Classificação de crédito/prêmios de seguro	US$ 13.000	US$ 179.000
Custos RP	US$ 12.000	US$ 161.000
Compensação	US$ 5.000	US$ 72.000
TOTAL de perda de reputação	US$ 43.000	US$ 575.000
TOTAL de perda por incidente virtual	US$ 108.000	US$ 1.400.000
% de perda causada à reputação	40%	41%

O impacto de perdas financeiras devido a questões relacionadas ao PR
Além de definir a escala da perda financeira no caso de um incidente virtual, queremos saber o impacto dessas perdas nos negócios. Perguntamos aos entrevistados da pesquisa se sua organização havia enfrentado problemas relacionados a RP (escândalos, crises públicas) relacionados a incidentes de segurança em geral e violações de dados em particular nos últimos 12 meses, e se eles poderiam estimar quão significativas eram as perdas. para a empresa deles.

Dos que sofreram algum tipo de incidente de segurança, 77% disseram que as perdas financeiras relacionadas às RP eram significativas ou muito significativas, enquanto que para os que sofreram uma violação de dados, 80% disseram que as perdas eram significativas ou muito significativas. Essas porcentagens eram as mesmas para pequenas, médias e grandes empresas.

Não é surpresa que as companhias de seguros estejam começando a oferecer suporte de RP como parte de seus pacotes de serviços para correções após incidentes virtuais. A Hiscox (Reino Unido) inclui isso em sua cobertura:

Custos de relações públicas:
Os custos adequados incorridos com nosso contrato prévio por escrito:

1. **um consultor de relações públicas ou gerenciamento de crises, para ajudar a restabelecer a reputação de sua empresa e responder a relatórios da mídia, incluindo o desenvolvimento e a comunicação de uma estratégia para reparar sua reputação;**
2. **emitir declarações através de e-mail ou do seu site e contas de redes sociais, incluindo o gerenciamento e acompanhamento dos seus sites e redes sociais; e**
3. **por quaisquer outras medidas cabíveis e proporcionadas tomadas para proteger ou restabelecer a reputação da sua empresa.**

O que é realmente chocante nesses números é o fato de que 40% de todas as perdas financeiras citadas por uma empresa após um incidente virtual se resumem apenas a danos à reputação. Para referência, os 60% restantes são perdidos devido à necessidade de empregar profissionais externos, salários adicionais de colaboradores internos, punições e multas, melhorias de software e infraestrutura, treinamento e contratação de novos colaboradores.

Se isolássemos o dano à reputação como um indicador de perda, poderíamos dizer ingenuamente que, ao garantir sua reputação, uma empresa poderia reduzir a perda no caso de um incidente virtual em 40%. Obviamente, essa abordagem não faz sentido prático (porque a reputação de segurança virtual sólida só pode ser construída com base em fatos, não em arrogância), mas é uma forma útil colocar os dados à reputação em seu devido lugar como uma área de risco que exige uma atenção séria e urgente.

Uma abordagem abrangente, baseada na realidade e tratando o futuro com confiança

Sabemos que os três caminhos da reputação estão intimamente conectados e que nenhum pode ser tratado isoladamente dos outros. É uma boa notícia, uma fonte de imenso poder que as empresas podem aproveitar para aumentar sua reputação e seus resultados, confiantes de que o investimento em um caminho gera retorno nos outros dois. Mas isso exige que nos afastemos de uma forma atenuada e negativa de pensar a segurança virtual como uma "mera" tática defensiva, ou uma tática que se encontra apenas na área de TI.

A segurança virtual pode ser uma questão relativamente nova, mas a maior parte da forma **como as empresas enfrentam os riscos a seu favor** é mais antiga do que as montanhas. Ao aperfeiçoar nossa abordagem à segurança virtual, não é necessário reinventar a roda. Para comprovar nosso argumento, analisaremos outro setor que enfrentou seus problemas de risco e saiu vitorioso, resiliente e lucrativo.

O que a indústria automobilística tem a ensinar às empresas sobre segurança virtual e reputação

Em 1869, a cientista irlandesa Mary Ward se tornou a primeira pessoa a morrer em um acidente de carro. Pouco mais de 150 anos depois, os acidentes de carro são agora a 9ª causa mais comum de morte, com 1,2 milhão de pessoas morrendo em todo o mundo a cada ano. É incrível dar um passo para trás e considerar esses riscos no contexto dos estimados 1,4 bilhão de carros no mundo atualmente, com mais de 74 milhões vendidos todos os anos.

Os riscos que os fabricantes de automóveis e seus clientes enfrentam são muito maiores do que aqueles que ocorrem com incidentes virtuais: estamos falando de nada menos que morte e ferimentos graves, que tornam uma violação de dados insignificante. A partir dessa perspectiva, deveria ser surpreendente que os fabricantes de automóveis agora priorizem suas campanhas de anúncios e RP falando que a segurança é um dos principais recursos. Imagine seu próprio negócio agora e os riscos que você enfrenta quando se trata de incidentes virtuais, você estaria disposto a liderar com segurança? Muitas empresas preferem rezar para que os seus clientes ignorem os riscos da segurança virtual ao tomarem decisões de compra, rezando também para que não ocorra qualquer incidente e, se acontecer, serão resolvidos da melhor forma possível.

Claramente, a indústria automobilística nem sempre foi tão ousada. Por décadas, durante as quais os riscos (ou mortes, para não exagerar) aumentaram exponencialmente, os fabricantes de automóveis preferiram impressionar seus clientes com a paixão de outros valores e características, como: glamour, liberdade, diversão, luxo e potência do motor. Somente nos anos 80, as empresas de automóveis assumiram que a segurança precisa estar no centro das atenções, mostrando assim suas tecnologias de defesa proativa como parte integrante não só dos seus produtos, mas também das suas plataformas de marca.

Muitas empresas modernas também estão presas a uma atitude movida pelo medo em relação à segurança virtual e ao gerenciamento da reputação, ecoando o atraso da indústria automobilística em ver a segurança como um fator decisivo nas vendas. Este medo, agravado pela incerteza num cenário de risco cibernético em rápida evolução, pode levar as empresas a perderem oportunidades de crescimento incrivelmente poderosas.

Veja, por exemplo, o caso da Volvo: amplamente considerada e classificada de forma independente como um das fabricantes de automóveis mais seguros do mundo por várias décadas. E, se você permitem o trocadilho - essa reputação segura não foi por acidente: A Volvo foi uma das primeiras empresas de automóveis a entender o relacionamento positivo e lucrativo entre segurança e reputação, liderando e se diferenciando com uma campanha publicitária ousada, apresentando manequins em testes de colisão. Vale a pena assistir ao anúncio do Volvo 340 de 1987, um elegante comercial de 43 segundos que serve como uma lição perfeita de como empresas precisam levar suas referências de segurança (o chefe de segurança virtual) para o centro do palco.

No ano passado, a nova campanha publicitária da Toyota deu seguimento ao papel do boneco de testes de colisão na divulgação da segurança como produto central e característica da marca. Desta vez, o boneco de teste de colisão fica desanimado por se encontrar desempregado, graças às características de segurança automatizadas da Toyota que impedem que os acidentes aconteçam em primeiro lugar.

As exigências de segurança da Volvo são baseadas na tecnologia de segurança sólida como uma rocha, e é por isso que estimulam o crescimento

A reputação da Volvo em termos de segurança não se tornou realidade apenas por causa de uma simples campanha publicitária. A campanha só funcionou porque as suas afirmações eram verdadeiras, e as classificações de segurança independentes as apoiaram repetidamente desde então. De fato, em 2017, o Volvo XC90 foi audaciosamente chamado de "o carro mais seguro do mundo" pelos mais altos avaliadores independentes possíveis, o Instituto de Seguros de Segurança Rodoviária (IIHS, sigla em inglês).

A segurança virtual não é diferente da segurança do carro quando se trata de garantir que você não está apenas falando, mas fazendo acontecer também. É a verdade pelos dois lados. Em primeiro lugar, saber que o seu negócio é seguro transmite a confiança necessária para promover realmente a segurança como um valor fundamental, apoiado pela ação. Em segundo lugar, e talvez mais obviamente, os clientes sabem quando seu fornecedor está realmente fazendo (ou apenas falando), seja devido a um incidente virtual que tem impacto no serviço ou vaza dados, ou porque eles estão se tornando cada vez mais especializados em descobrir a falsificação dos valores empresariais, das falar bobagens e exigir provas de ações significativas.

Antes de começarmos a falar sobre como a Kaspersky pode dar a você a confiança necessária para promover o compromisso de sua empresa com a segurança de uma maneira que impulsiona o crescimento e inspira a confiança de seus clientes, achamos justo apresentar algumas evidências claras, portanto, que você sabe que estamos agindo. É fácil fazer declarações sobre eficácia mas, a menos que essas reivindicações sejam apoiadas por testes independentes (como o IIHS no Volvo XC90), elas não têm sentido.

Temos orgulho em afirmar com confiança que somos a empresa de segurança virtual mais testada e premiada do mundo, com um desempenho estável em vários testes independentes que dão uma avaliação muito mais significativa do que apenas as vitórias pontuais.

Dentro desse recorde mundial de desempenho estável, existem alguns elogios recentes importantes que estamos particularmente orgulhosos de apresentar hoje:

- A Iniciativa Global de Transparência da Kaspersky foi recentemente aprovada pelo Paris Call for Trust and Security in Cyberspace (veja à esquerda)
- A AV-Comparatives recentemente parabenizou a Kaspersky por receber seu prêmio de produto com melhor classificação, além de outros prêmios por testes individuais em 2019
- A Kaspersky Anti Targeted Attack Platform foi a única solução a demonstrar 100% de taxa de detecção e zero falsos positivos no teste de Defesa Avançada contra Ameaças executado pelo ICSA Labs no terceiro trimestre de 2019
- Este ano, a Kaspersky conquistou a certificação ISO/IEC 27001:2013; o padrão internacional que descreve as melhores práticas para sistemas de gerenciamento de segurança da informação

Essas são apenas algumas das referências que nos dão a confiança de estar diante dos 400 milhões de usuários e 270.000 clientes corporativos e dizer: **estamos te protegendo, você está seguro.**

Gostaríamos de compartilhar com você um pouco dessa confiança, para que a voz da sua empresa possa se destacar na multidão e falar com ousadia sobre o respeito que você investe nos dados do cliente e sobre sua capacidade de entrega pontual, sempre. Às vezes, particularmente no contexto da crise de talentos de segurança virtual, ou quando os orçamentos e o tempo estão apertados, pode ser difícil incorporar essa confiança, ou orgulho cibernético, de uma maneira que repercuta com sua base de clientes.

Por isso, projetamos o Kaspersky Endpoint Security Cloud, oferecendo proteção excepcional moderna que não poderia ser mais fácil de gerenciar. Repleto de tecnologias de proteção avançadas, estamos ansiosos para falar sobre elas, mas primeiro precisamos nos aprofundar no que consideramos uma das maiores oportunidades perdidas na história dos negócios.

—

A The Paris Call for Trust and Security in Cyberspace foi lançado em 2018 pelo Presidente Emmanuel Macron durante o Fórum de Governança da Internet realizado pela UNESCO e o Fórum de Paz de Paris. O apelo convida todos os atores do ciberespaço a trabalharem juntos e incentivar os Estados a cooperar com parceiros do setor privado, o mundo da pesquisa e a sociedade civil e define o Centro de Transparência Global da Kaspersky como uma resposta modelo ao Princípio 6 (Segurança do Ciclo de Vida).

"A Kaspersky implementa uma abordagem única para maior transparência e confiança que pode ser verificada na segurança virtual: A Iniciativa Global de Transparência (GTI) da Kaspersky colocam em prática um conjunto de medidas claras de verificação e minimização de riscos para aumentar a confiança dos usuários e garantir que as soluções de segurança virtual atendam e excedam os padrões corporativos de segurança e proteção de dados".

Por que as empresas não lideram com suas referências de segurança virtual e privacidade? Por que eles não tem orgulho cibernético?

De acordo com Forrester, dentre as pessoas on-line, 32% dos adultos britânicos, 35% dos americanos e alemães classificados e 38% dos adultos franceses não confiam em nenhuma empresa para manter as suas informações pessoais seguras. Também sabemos que essa confiança (ou a falta dela) é um dos principais fatores nas decisões de compra, que se resumem ao mérito. Com isso em mente, é difícil entender por que as empresas em todo o mundo estão perdendo a oportunidade de colocar suas preocupações com privacidade e segurança virtual na linha de frente de comunicação com seus clientes.

Avisos de privacidade e a prisão pouco ambiciosa das entrelinhas

Existem joias preciosas confinadas à prisão das entrelinhas acessadas por um link <Aviso de privacidade>, situado na parte inferior das páginas da Web de empresas de todas as categorias. Estas joias devem ser mineradas, polidas e expostas.

Em média o Aviso de privacidade da empresa apresenta uma breve declaração descritiva de abertura que fala das preocupações muito válidas com os clientes sobre o uso de informações pessoais, mas desce imediatamente para uma enxurrada de informações jurídicas: pouco atraente e intercalada apenas com a garantia explícita ocasional do valor que a empresa coloca nos dados e na segurança de seus clientes.

Não estamos sugerindo que cada página da Web ou material de marketing deve orientar com declarações sobre segurança virtual e confidencialidade dos dados, mas que elas precisam ir além da prisão sombria das entrelinhas. A segurança virtual e a confidencialidade dos dados devem ser integradas em toda a empresa de uma forma abrangente, que reconheça a importância de tais preocupações como uma oportunidade para impulsionar o crescimento das empresas, e não como uma tentativa pouco ambiciosa de cumprir os requisitos regulamentares.

A regulamentação não deve ser o único guia das políticas de segurança virtual e de proteção da vida privada

Muitas empresas acreditam na ilusão de que as regulamentações são suficientes como guia para a tomada de decisões em matéria de segurança virtual e privacidade. Isso, novamente, representa decisões motivadas pelo medo e pela busca de indenização, em vez de excelência ética e crescimento dos negócios.

Em primeiro lugar, as regulamentações lutam para acompanhar o ritmo do avanço tecnológico, tanto do lado dos negócios quanto do lado dos criminosos virtuais e seus métodos em constante evolução de causar estragos maliciosos. Embora a regulamentação deva ser claramente respeitada, os verdadeiros líderes empresariais devem sempre olhar além das condições atuais, guiados pela realidade das inovações tecnológicas, por um lado, e pelos imutáveis princípios éticos eternos que (deveriam) conduzir as regulamentações, em primeiro lugar.

A boa notícia aqui é que se, as empresas aceitarem e defenderem a centralização da ética na segurança virtual e na privacidade, como fizeram analistas como a Forrester, elas naturalmente terão uma poderosa oportunidade para promoverem o valor ético da sua marca de uma forma que seja apoiada por uma ação sólida. Este é um exemplo prático da interação entre os caminhos da reputação da marca e da segurança.

Afinal, uma coisa é dizer que "tratamos seus dados com o máximo respeito, e é assim que cumprimos todos as regulamentações importantes", e outra é recuar, criando uma abordagem ética e abrangente da segurança virtual e da privacidade em uma das principais características do seu produto e da sua marca. Quando as decisões de segurança virtual e privacidade são orientadas por valores éticos profundamente enraizados e não por regulamentações, as mensagens públicas a respeito de uma empresa deixam a atitude simbólica das regulamentações para trás e, em vez disso, transparece sua verdadeira imagem para atuais e futuros clientes.

Em resumo, se você deseja aproveitar a segurança virtual e a privacidade para impulsionar o crescimento dos negócios, não diga apenas que se importa, mostre isso com ousadia em todas as oportunidades (relevantes). É o ar que você respira, são os produtos que você constrói, é a cultura da sua organização como um todo e todos têm um papel a desempenhar. A organização que atinge este objetivo possível de ser alcançado (como a Volvo fez com a segurança em automóveis) assegura um poderoso e duradouro fator de diferenciação em relação ao resto da multidão, que permanece paralisada por seu foco excessivo na regulamentação ao contrário da ação ética positiva.

Aproveite a grande oportunidade desperdiçada hoje e use sua reputação para impulsionar o crescimento, com o Kaspersky Endpoint Security Cloud

O Kaspersky Endpoint Security Cloud elimina riscos, dando à sua empresa a confiança necessária para aproveitar a segurança virtual para impulsionar o crescimento, rumo a um futuro seguro, lucrativo e promissor. Além de saber que sua empresa é defendida pelo **fornecedor de segurança virtual mais testado e premiado do mundo**, você poderá compartilhar essa confiança em tudo o que se comunica com seus clientes e partes interessadas. Essa confiança resulta em um claro divisor dos concorrentes que ficam para trás em alavancar o caminho da reputação de segurança, como os fabricantes de automóveis antes da ousada e lucrativa ação da Volvo nos anos 80.

O Kaspersky Endpoint Security Cloud é ideal para a era da nuvem, trabalho remoto e BYOD. Uma solução do mundo real fácil de usar, colocando poderosos controles e proteção nas mãos de empresas cujas metas são definidas de maneira decisiva no crescimento.

Particularmente, uma das tecnologias mais interessantes é a NOVA Cloud Discovery, que impede automaticamente que seus colaboradores se entreguem ao uso não autorizado de serviços em nuvem. Isso elimina completamente o estresse causado pela necessidade de gerenciar minuciosamente a crescente variedade de serviços em nuvem que podem potencialmente ameaçar a segurança da sua empresa.

Você também receberá o Kaspersky Security for Microsoft Office 365 como parte do pacote: nossa solução de defesa dedicada para todo o pacote do Office é particularmente importante, pois os produtos Microsoft ainda são o alvo número um dos criminosos virtuais.
Agora que o trabalho remoto está se tornando cada vez mais comum, adicionamos duas licenças para dispositivos móveis gratuitas por usuário, para que você tenha uma defesa cibernética sólida que reconheça que você emprega pessoas e não dispositivos. Você pode até mesmo aplicar políticas de segurança remotamente, para que seus colaboradores estejam protegidos onde quer que eles trabalhem, mesmo em uma cafeteria ou na praia.

O Kaspersky Endpoint Security Cloud é hospedado na nuvem, portanto você não precisa de hardware ou software, nem mesmo pagar pelo provisionamento ou manutenção. Você recebe proteção instantânea com políticas de segurança predefinidas desenvolvidas por nossos profissionais e conta com uma assinatura mensal para aliviar seus recursos financeiros.

Para nossos 4.000 especialistas internacionais, **segurança é realmente tudo.** Vivemos, respiramos e amamos a segurança virtual para que as empresas de todo o mundo possam levar a nossa paixão e os elogios que a acompanham para construir uma base sólida para avançar, explorar e descobrir o futuro.

Fale conosco sobre como você pode se tornar orgulhoso cibernético e construir uma reputação segura para impulsionar o crescimento com o **Kaspersky Endpoint Security Cloud**.

Notícias sobre ameaças virtuais: securelist.lat
Notícias sobre segurança de IT: business.kaspersky.com/br

www.kaspersky.com.br

kaspersky BRING ON THE FUTURE