A nova face dos processos cibernéticos de 2021

Um estudo sobre sinistro de seguro cibernético na Europa Continental

Agosto de 2021

Índice

Introdução

As oportunidades oferecidas às empresas pela digitalização e pelas tecnologias emergentes continuam a crescer em um ritmo veloz pelo mundo. Essas oportunidades, contudo, andam lado a lado com um aumento no risco cibernético, e isso tem levado a um forte aumento na compra de seguro cibernético.

Em nosso relatório inaugural no ano passado, o rápido aumento no entendimento do seguro cibernético para 2019 foi evidente, assim como a alta nos processos cibernéticos pela Europa Continental.

O relatório deste ano demonstra que essas tendências continuaram em 2020. O crescimento continuado dos processos cibernéticos, em especial aqueles relacionados a ransomware, trouxe uma nova dimensão ao mercado de seguro cibernético de rápido amadurecimento.

Há uma série de consequências positivas para essas tendências:

- As organizações cada vez mais vêm o seguro cibernético como uma forma confiável e econômica não somente de obter suporte técnico caso ocorra um evento cibernético, mas também de transferir os riscos financeiros enfrentados do uso ampliado de dados e tecnologia nas operações comerciais. Eles incluem sinistros e despesas associados a um conjunto crescente de perigos cibernéticos, como ataques mal-intencionados, violações de privacidade e eventos acidentais. As políticas cibernéticas e a cibersegurança deverão ser vistas como complementares: Enquanto o seguro identifica o impacto financeiro, a cibersegurança administra a frequência do ataque, por exemplo, mantendo o malware fora do sistema de TI de uma organização.

- Tem havido desenvolvimentos nos serviços de prevenção referentes à gestão de incidentes cibernéticos – durante o processo de subscrição, em que vemos mais e mais seguradoras pedindo por controles de segurança específicos e, durante o prazo da apólice, que se informe aos segurados sobre as ameaças emergentes. O seguro cibernético é agora visto como um importante componente para um mundo mais resiliente.

Contudo, nem todas as consequências têm sido positivas; o aumento da gravidade e da frequência dos processos cibernéticos também tem levado a um reposicionamento significativo do mercado.

O mercado está vivenciando o seguinte com o seguro cibernético pela Europa Continental:

- Aumento agressivo nos prêmios.
- Redução da capacidade.
- Subscrição mais rígida.
- Limitação da exposição a processos relacionados a ransomware.

O seguro cibernético, então, está sendo oferecido para empresas com uma alta maturidade de segurança cibernética.

Com estas tendências em mente, tanto o mercado quanto seus clientes precisarão trabalhar juntos para amenizar o avanço dos processos de ransomware. Assim, nos concentramos neste risco específico no relatório deste ano. Evidentemente, a COVID-19 também causou um profundo impacto na sociedade, nas organizações e nos padrões de trabalho e, por sua vez, em seus riscos cibernéticos relacionados. Também exploraremos como os cibercriminosos estão se aproveitando dos problemas contemporâneos atuais.

Assim como no compartilhamento de insights coletados de dados de processos da Marsh e de dados, experiência e expertise da Microsoft, Kivu e CMS, este relatório se atém às formas práticas de administrar e mitigar o risco cibernético e os processos, ajudando na construção de resiliência nas suas práticas de trabalho.

1 Tendências do processo cibernético

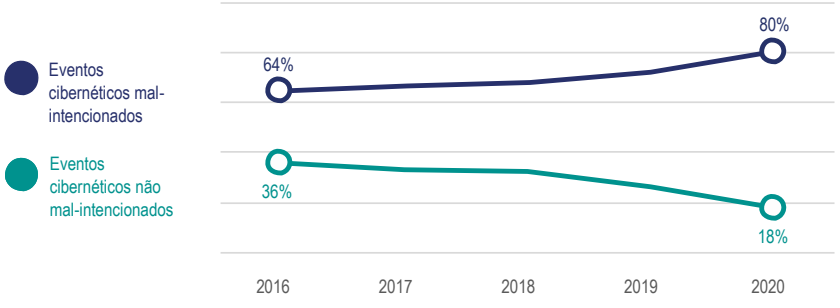
De acordo com as taxas de notificação na Marsh, embora o número de processos cibernéticos pela Europa Continental tenha continuado a aumentar, o nível de crescimento é bem menor do que foi testemunhado de 2018 até 2019. Contudo, os dados de 2020 revelaram um foco maior nos eventos cibernéticos mal-intencionados. Deve-se notar que isto não significa que o número de notificações de processos cibernéticos não mal-intencionados esteja diminuindo, pois eles também mostraram um crescimento estável nos anos analisados, muito embora a taxa de crescimento esteja diminuindo.

Os processos de ransomware responderam por **32%** dos processos cibernéticos em 2020. Isso representou um aumento significativo. Com efeito, os processos de ransomware responderam por **14%** das notificações de processos cibernéticos em 2016-2019; as notificações de 2020 empurraram o percentual global para **24%** – quase o dobro do que foi relatado nos quatro anos anteriores.

Este número seria até maior se os eventos de processos cibernéticos mal-intencionados não tivessem sido interrompidos em seu curso: Para muitos ciberataques, o objetivo final é a extorsão de um pagamento de resgate. Entretanto, quando um departamento de TI competente ou uma equipe de resposta de emergência externa é capaz de interromper o ataque antes que seja identificada uma demanda de resgate efetiva, o evento não será registrado como um ransomware.

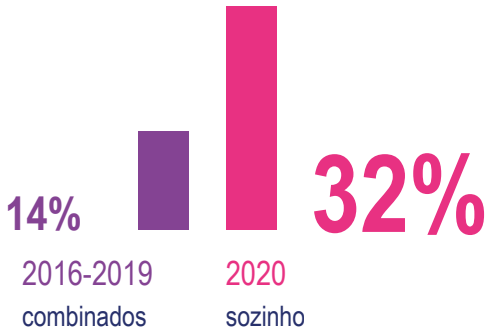
80% dos eventos cibernéticos são mal-intencionados, um aumento de 10% em comparação com 2019

01 | **Eventos cibernéticos mal-intencionados vs não mal-intencionados**



***Fonte**: Marsh*

02| Notificações de processos cibernéticos de ransomware



Os setores mais afetados continuam sendo de **instituições financeiras, fabricação, comunicação, mídias e tecnologia** e **serviços profissionais** nesta ordem – e isso não mudou desde 2019. Contudo, as taxas entre esses setores mudaram significativamente, com as empresas de fabricação dobrando sua taxa de incidentes cibernéticos e as empresas de serviços profissionais aumentando três vezes as suas. Embora as instituições financeiras continuassem sendo o setor mais afetado, a grande lacuna na taxa de incidentes entre os setores estacionou consideravelmente.

Quando se focaliza exclusivamente os eventos cibernéticos mal-intencionados, percebe-se que o setor de fabricação sofreu a frequência mais alta de ataques. Um possível motivo para isso poderia ser os altos custos vinculados à interrupção do negócio, que tornam o setor de fabricação muito sensível a ataques de ransomware – e, portanto, um alvo atraente.

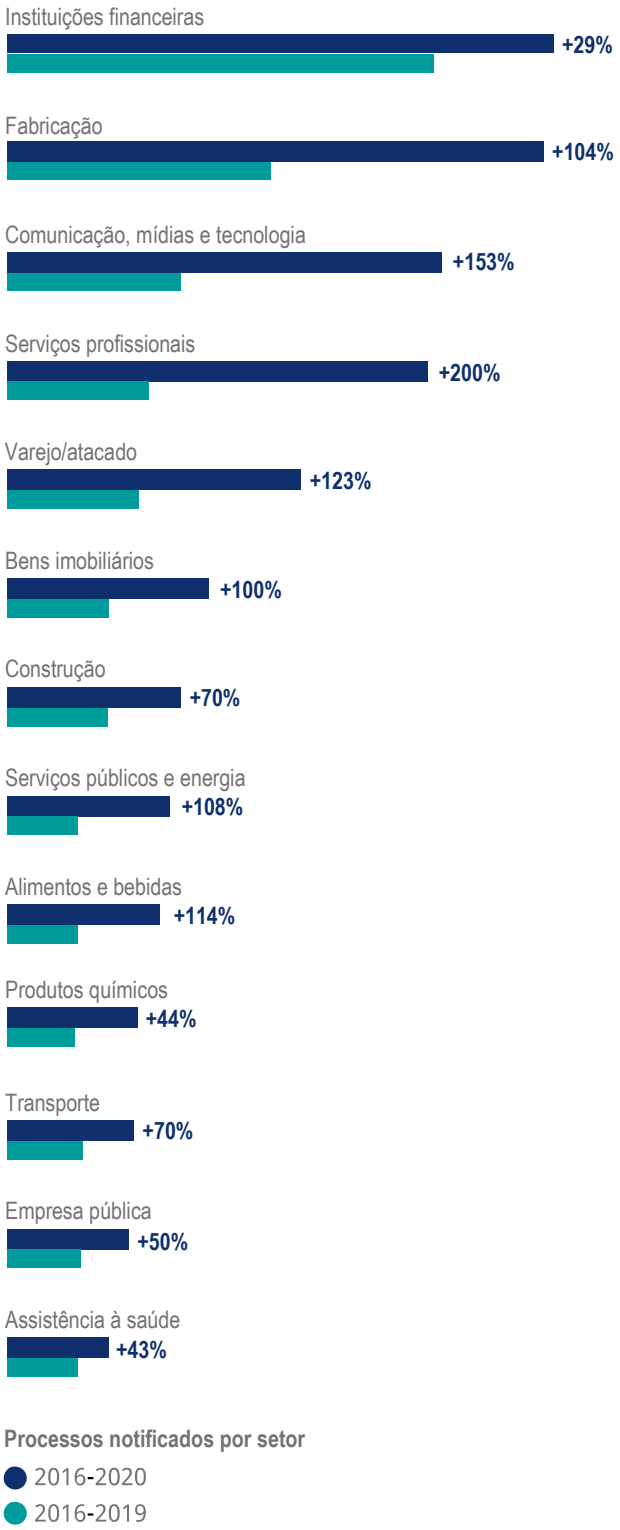
Além disso, a vulnerabilidade deste setor tem aumentado significativamente nos últimos anos, pois agora avanços comuns, como automação aumentada e implantação de processos baseados em software, aumentaram a superfície de ciberataques.

Enquanto a grande maioria dos clientes da Marsh que adquiriram apólices cibernéticas é composta por pequenas e médias empresas **(74%)**, os clientes mais afetados em termos de frequência de notificação cibernética são as empresas muito grandes. Isso poderia ser interpretado como as maiores empresas sendo alvo de eventos cibernéticos mal-intencionados em um grau mais alto; e também poderia ser devido a elas notificarem com maior frequência e maior consistência devido a processos mais fortes de gestão de riscos internos ou capacidades de TI.

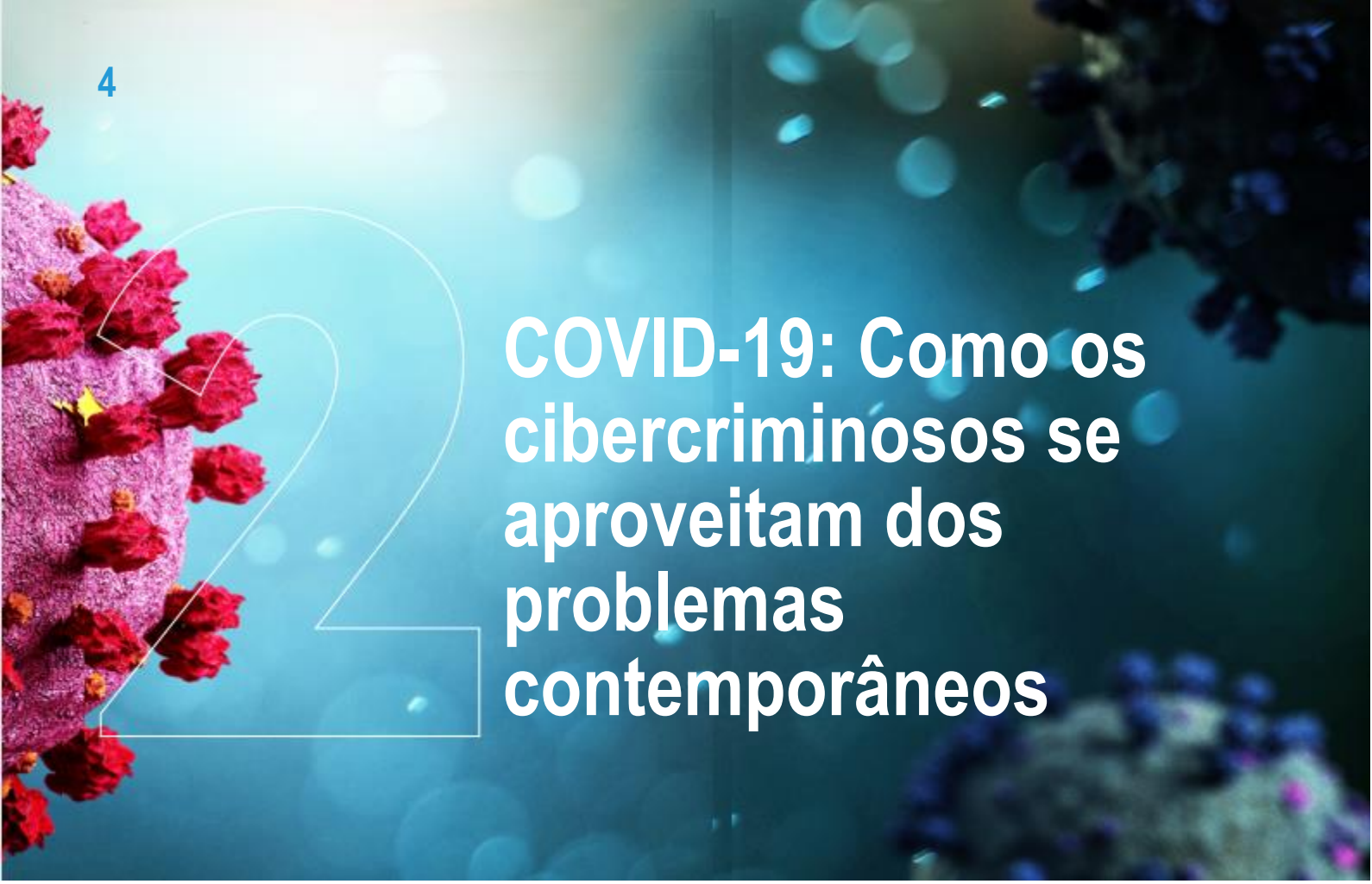
Com base em nossos prêmios contabilizados em 2020 para apólices cibernéticas e na última estimativa total de sinistros de processos cibernéticos relatados, uma estimativa aproximada da taxa de sinistros seria de cerca de **74%***. Por este motivo, as seguradoras primárias tenderiam a ser um pouco não lucrativas enquanto as seguradoras excedentes permanecem lucrativas.

Em última análise, os processos cibernéticos ocorrem em todos os níveis. Não importa o setor, a área geográfica ou o tamanho da empresa, é essencial que as empresas estejam preparadas e invistam na sua resiliência cibernética.

03| Processos cibernéticos por setor



* As estimativas de sinistro usadas para esses cálculos podem não responder por todos os custos relacionados aos processos, pois alguns deles estão cobertos diretamente pelas seguradoras (custos de assistência, etc.).



2 COVID-19: Como os cibercriminosos se aproveitam dos problemas contemporâneos

A maioria das pessoas terá ouvido uma das muitas notícias de ataques de ransomware atingindo empresas pelo mundo. Esses ataques estão ocorrendo no contexto de um novo normal em que a pandemia da COVID-19 causou impacto na gestão de risco cibernético de suas organizações.

A questão é: como os cibercriminosos estão fazendo uso de problemas contemporâneos na sociedade e nas organizações?

O crime cibernético é um crime organizado que funciona como um negócio. E como qualquer outro negócio, existe uma necessidade de inovar para ser lucrativo e bem-sucedido. Alguns tipos de crime cibernético persistem independentemente das mudanças econômicas, políticas ou sociais, enquanto outros tipos são alimentados por essas mudanças. Isso foi comprovado mais uma vez ao constatarmos a natureza oportunista dos cibercriminosos quando capitalizaram no interesse e no temor relacionados à pandemia da COVID-19 e outros eventos perturbadores. À medida que o vírus se alastrou globalmente, os cibercriminosos articularam suas iscas para imitar fontes confiáveis como a OMS (Organização Mundial da Saúde) e outras organizações nacionais de saúde, em um esforço para fazer com que os usuários clicassem em links e anexos mal-intencionados.

A falta de higiene de segurança básica em qualquer ecossistema continua a permitir que cibercriminosos usem as vulnerabilidades tão conhecidas – ou novas variantes delas – para explorar esses ambientes. Eles também são capazes de se aproveitar do temor e da incerteza associados à COVID-19 com grande sucesso. Embora os ataques relacionados à COVID-19 representem um percentual pequeno do número total de malware, eles mostram como os cibercriminosos agem rapidamente para adaptar suas iscas aos tópicos do dia.

Um entendimento comum entre os profissionais de cibersegurança é “jamais desperdiçar uma crise” e usar as informações obtidas para ajudar a embasar as necessidades de investimento. Os cibercriminosos compartilham a mesma filosofia; eles buscam unir táticas bem estabelecidas e malware com a curiosidade humana e a nossa necessidade de informações tópicas. Assim, os cibercriminosos usaram com eficácia o tema COVID-19 para engendrar socialmente iscas para a ansiedade e a torrente de informações associadas à pandemia.

AJUSTANDO-SE AO NOVO NORMAL

Da noite para o dia, a força de trabalho de milhares de organizações pelo mundo tornou-se totalmente remota. Os fechamentos de escolas forçaram milhões de estudantes a passar imediatamente a estudar em casa, acrescentando desafios significativos para pais e cuidadores.

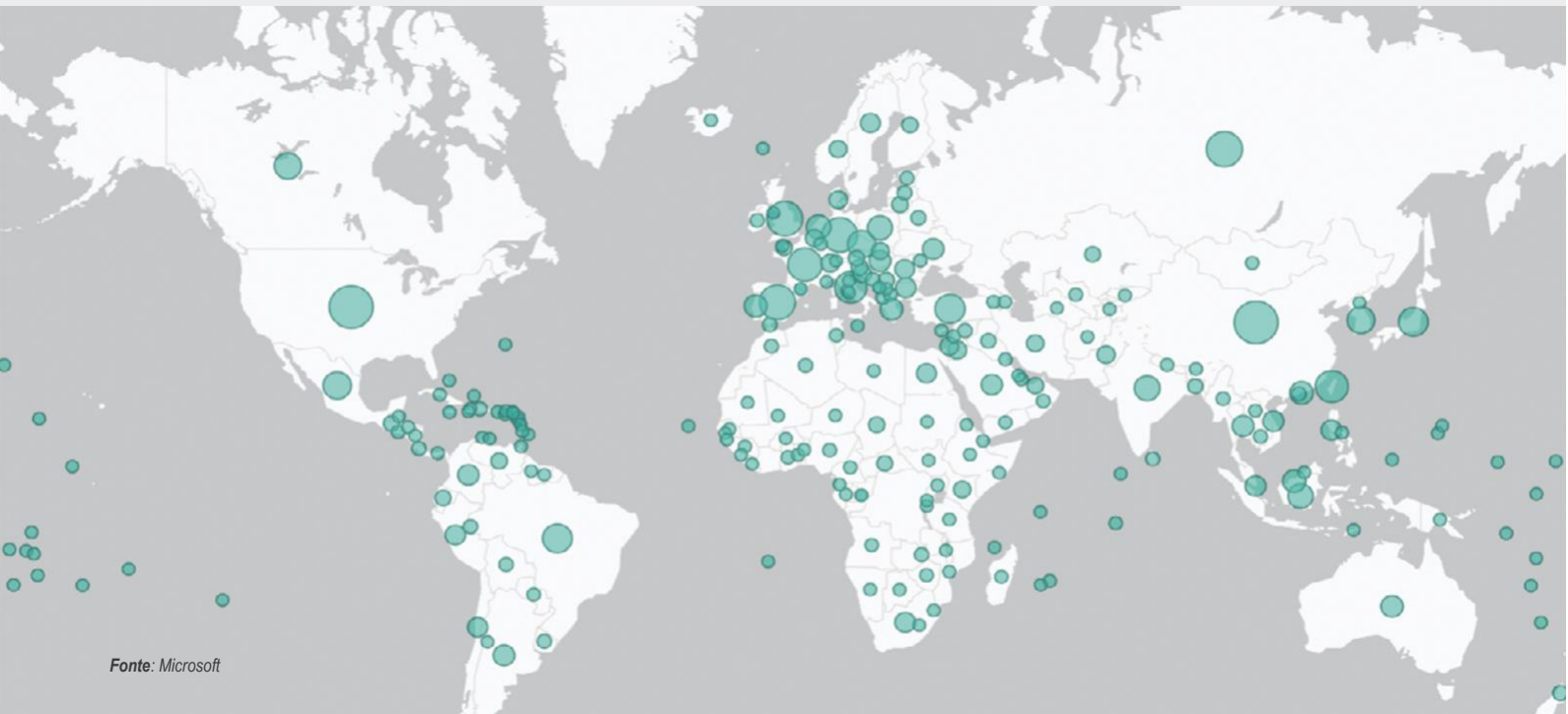
Embora as forças de trabalho pelo mundo, não importando o tamanho, estejam se inclinando para a mobilidade em alguns aspectos de suas operações, poucas empresas e instituições de ensino estavam preparadas para funcionar 100% remotamente. Tarefas operacionais como software ou patch de dispositivo e atualizações tinham sido previamente consumadas quando os trabalhadores remotos retornassem rotineiramente para o escritório. Depois do surgimento da COVID-19, esta opção desapareceu temporariamente.

As práticas de proteção de dados continuam a aumentar, à medida em que as forças de trabalho se tornam remotas e as equipes alimentam ativos vitais sem estar fisicamente juntas. Na mesma ocasião, observamos o aumento continuado do uso de gerenciamento de direitos de informação na aplicação de políticas voltadas para a proteção das informações confidenciais e da propriedade intelectual.

Encorajamos que todas as organizações sejam vigilantes nessa questão e percebam como seu perfil de empresa mudou no curto e no longo prazo como resultado da COVID-19. É essencial adaptar sua abordagem de gestão de risco cibernético de forma condizente. As mudanças operacionais podem significar uma mudança no seu perfil de risco, como um incidente cibernético agora causando um impacto maior na interrupção do negócio.

Em uma perspectiva mais ampla, todas as organizações devem estar cientes de que o antigo adágio “a oportunidade faz o ladrão” ainda é pertinente. Os cibercriminosos buscam e agem ativamente nas oportunidades que lhes são apresentadas.

04| **Impacto relativo dos ataques ligados à COVID-19 pelo mundo por contagem de arquivos (em 1° de julho de 2020)**



***Fonte**: Microsoft*

3 Análise aprofundada do ransomware

Embora nossa análise detalhasse um aumento nos incidentes relacionados ao ransomware, é provável que a real dimensão desta tendência seja significativamente maior do que tem sido retratada.

Isso se deve ao número de casos de ransomware que não estão incluídos nos dados porque os cibercriminosos foram interceptados antes do pedido de um pagamento de resgate.

Assim, é razoável dizer que os incidentes cibernéticos relacionados ao ransomware são um dos maiores riscos no panorama cibernético – tanto hoje quanto no futuro. Para entender melhor este panorama, faremos uma análise aprofundada dos incidentes cibernéticos relacionados ao ransomware, o modus operandi dos criminosos e as lições aprendidas de prevenção e resposta a esses tipos de ataque.

O QUE É DARKSIDE?

Declaração de missão do DarkSide

Darkside

Vamos começar!

Somos um novo produto no mercado, mas isso não significa que não temos experiência e que surgimos do nada.
Recebemos milhões de dólares de lucro em parcerias com outros cryptolockers bem conhecidos.
Criamos o DarkSide porque não encontramos o produto perfeito para nós. Agora temos isso.
Com base nos nossos princípios, não atacaremos os alvos a seguir:
* Medicina (hospitais, hospícios)
* Educação (escolas, universidades)
* Organizações sem fins lucrativos
* Setores do governo
Apenas atacaremos as empresas que podem pagar o valor pedido; não queremos acabar com o seu negócio. Antes de qualquer ataque, analisamos cuidadosamente sua contabilidade e determinamos quanto vocês podem pagar com base no seu lucro líquido. Vocês podem fazer todas as perguntas no chat antes de pagar e o nosso suporte responderá.
Damos as seguintes garantias para os nossos alvos:
* Garantimos a descriptografia de um arquivo de teste.
* Garantimos fornecer descriptografadores após o pagamento, assim como suporte no caso de problemas.
* Garantimos apagar todos os dados carregados dos TOR CDNs após o pagamento.
Caso vocês se recusem a pagar:
* Publicaremos todos os seus dados e os armazenaremos em nossos TOR CDNs durante pelo menos 6 meses.
* Enviaremos notificação sobre o seu vazamento para as mídias e para seus parceiros e clientes.
* JAMAIS forneceremos descriptadores para vocês.
Levamos muito a sério a nossa reputação, então se vocês pagarem, todas as garantias serão cumpridas.
Caso não paguem, vocês entrarão na lista de empresas publicadas no nosso blog e se tornarão um exemplo para as outras.

Fonte: DarkSide

RANSOMWARE É CRIME ORGANIZADO

O ransomware tem sido uma ameaça crescente durante anos, mas os eventos de ransomware de 2020 apresentaram um aumento na frequência e na sofisticação. O ransomware é perpetrado através de uma economia informal altamente ativa que se parece e funciona como um comércio legítimo. É uma comunidade constituída por desenvolvedores de malware, afiliados e parceiros, e aqueles que fornecem serviços adjacentes como venda de acesso à rede ou serviços de hospedagem.

Como vimos no ataque do DarkSide em 2020, os operadores do grupo de ransomware tentaram recrutar afiliados em publicidade e comunicados à imprensa. Eles também podem publicar uma declaração de missão – ver na pág. 6 – que se parece com um contrato social.

Para que os operadores do ransomware sejam bem-sucedidos, eles tentarão recrutar afiliados talentosos, que podem ser responsáveis pela distribuição do ransomware para as vítimas em potencial. Os afiliados podem ficar com 60% e 80% do resgate, dependendo da variável, com o restante do resgate ficando com os operadores, negociadores e outros provedores de serviço. Determinados grupos de ransomware até têm atendimento ao cliente e suporte de TI para resolução de problemas com a descriptografia na rede, bem parecido com um negócio legítimo.

A hierarquia e a estrutura

Provas de blockchain coletadas de pagamentos de resgate corroboram que existe uma estrutura e uma hierarquia nos diferentes grupos de ransomware. A Kivu rastreou ataques de ransomware do grupo de ransomware Egregor e seguiu a trilha dos pagamentos de resgate pelo blockchain. Ao seguir o dinheiro extorquido desembolsado pela carteira paga original, a Kivu descobriu parcelas predeterminadas do lucro entre cada ordem dos desembolsos, aludindo a uma hierarquia de membros.

A análise forense de blockchain sugere que o grupo Egregor pertence e é operado por não mais do que 10-12 membros principais. Os membros principais distribuem seus ataques através de não mais do que 20-25 membros semiexclusivamente avaliados que são denominados de afiliados.

Para onde vai o dinheiro quando chega às mãos dos afiliados?

Os afiliados lavam o dinheiro extorquido através de uma série de mecanismos, inclusive câmbios de alto risco em vários países e mercados da Darknet. A maior parte dos lucros nos mercados da Darknet é enviada para o Hydra, o mercado russo mais famoso para produtos e serviços ilegais.

Além disso, a equipe da Kivu descobriu uma coincidência entre os afiliados do Egregor e grupos de ransomware conhecidos como DoppelPaymer e NetWalker. Os afiliados do ransomware operam entre múltiplos grupos de RaaS (Ransomware-as-a-Service) em que a oportunidade econômica está presente.

Qual o seu efeito sobre o tamanho do pedido de extorsão?

O grupo de RaaS Egregor se expande em um nível contratual com base no tamanho do ataque, a saber o tamanho e a complicação da rede da vítima. A economia no uso de afiliados contratados e tempo dispendido na rede de uma vítima afeta diretamente o tamanho do pedido de extorsão buscado pelo grupo. Isso demonstra o amplo ecossistema comercial por trás dos ataques. Esta capacidade de expandir levou a ataques em empresas maiores, um crescimento na frequência e um aumento nos pedidos de extorsão.

EM 2020 OS EVENTOS DE RANSOMWARE APRESENTARAM UM AUMENTO NA FREQUÊNCIA E NA SOFISTICAÇÃO

Os afiliados dos operadores do ransomware podem ficar com

60-80%

do resgate

A análise forense de blockchain sugere que o grupo Egregor pertence e é operado por

10-12

membros principais

Esses membros principais distribuem seus ataques através de

20-25

membros avaliados que são denominados de afiliados.

MODUS OPERANDI

O phishing de e-mail no contexto empresarial continua a crescer e tornou-se um método de infiltração predominante. Dado o aumento de informações disponíveis com respeito a esses esquemas, e os avanços técnicos na detecção, os criminosos por trás desses ataques agora estão dispendendo tempo, dinheiro e esforços significativos no desenvolvimento de golpes que sejam suficientemente sofisticados para ludibriar até profissionais perspicazes. As técnicas de ataque de phishing e comprometimento de e-mail comercial (BEC) estão evoluindo rapidamente.

Antes, os cibercriminosos concentravam seus esforços nos ataques de malware; agora, passaram a se concentrar no ransomware, bem como nos ataques de phishing, com o objetivo de extrair as credenciais do usuário. As gangues de ransomware operado por humanos estão realizando varreduras amplas da internet, buscando pontos de entrada vulneráveis que permitam o acesso, esperando por um momento que seja vantajoso para o seu objetivo.

EXEMPLO DE PHISHING DE CREDENCIAL

1 Configuração da infraestrutura criminosa

Criar domínios falsos ou comprometer os legítimos

Obter informações sobre as vítimas potenciais

2 Mensagens mal-intencionadas

3 As vítimas são incitadas a clicar

O clique envia a vítima para um domínio falso (site falso)

4 As credenciais da vítima são roubadas

A vítima insere as credenciais em um formulário web falso

Ou o malware é baixado no dispositivo da vítima para pegar as credenciais

5 Os dados da vítima são enviados para uma "conta suspensa" (*drop account*)

Os cibercriminosos usam as credenciais da vítima ou outros sites legítimos

Ou usam os dados para ganhar acesso a redes e dados corporativos

RANSOMWARE DE BIG GAME

Ransomware operado por humanos, algumas vezes denominado como "ransomware de big game", é quando os cibercriminosos selecionam redes específicas para sua proposição de valor e então procuram por vetores de entrada. De modo geral, os cibercriminosos executam uma varredura ampla e considerável da internet, buscando pontos de entrada vulneráveis, ou entram nas redes via cavalos de Tróia de commodities, e então se depositam neste acesso por um tempo e um propósito que sejam vantajosos para eles.

Por exemplo, os cibercriminosos exploravam as vulnerabilidades em dispositivos de VPN e acesso remoto para obter credenciais, e então salvavam seu acesso para usar pedindo resgate a hospitais e provedores de serviços médicos durante a pandemia da COVID-19.

Nesses ataques, os cibercriminosos agem ativamente, tomando decisões à medida em que vão caminhando, controlando cada etapa do ataque com base nas configurações que encontram na rede. Eles decidem que dados exfiltrar, que mecanismos de persistência usar para futuro acesso à rede e, por fim, que carga de ransomware vão atacar.

Este cenário está longe de ser uma commodity ou ameaça automatizada. Este tipo de ataque é chamado de "ransomware operado por humanos" para refletir o atual panorama de ameaça de forma mais exata.

Embora esta abordagem tenha sido a exceção, não a regra, na maioria dos principais ataques de ransomware no ano passado, isso mostra que o crime cibernético evoluiu para além do modelo de "lobo solitário". O ransomware virou crime organizado.

COMO SE TORNAR MAIS RESILIENTE

Os provedores de gestão de risco cibernético, corretores e seguradoras em geral podem oferecer proteção econômica e uma série de recursos e serviços para ajudar na preparação, resposta, recuperação e ressarcimento das perdas dos ataques de ransomware. Isso pode incluir:

Preparação

- Planejamento e atualização de resposta a incidente cibernético.
- Avaliação do preparo para ransomware.
- Avaliações da estrutura e da vulnerabilidade da cibersegurança.
- Treinamento e aprendizado do colaborador.
- Melhores práticas de cibersegurança.
- Suporte ao pagamento de resgate em criptomoeda.
- Análise do impacto financeiro.
- Identificação do fornecedor.

Recuperação

- Parceria e suporte a evento, inclusive suporte e defesa de processos.
- Seguro cibernético para cobrir perda de receita, despesas extras e custos de ransomware associados.
- Preparação e suporte de comprovação de sinistro.
- Atualização/reavaliação de planos de resposta a incidente.

Resposta

- Obter serviços de gestão de incidente.
- Identificação do fornecedor, incluindo: assessoria jurídica, peritos forenses, suporte de relações públicas e provedores de serviço de restauração de dados.
- Serviços de notificação de violação.
- Suporte ao pagamento de resgate em criptomoeda.
- Suporte de processos para recuperação de seguro.

Cobertura de seguro

- Receita perdida e despesas extras para continuar em operação.
- Restauração ou recriação de dados corrompidos ou destruídos e outros ativos intangíveis.
- Restauração ou reparo de rede ou hardware.
- Multas e penalidades regulatórias.
- Eventos de privacidade.
- Danos à reputação.

ADMINISTRANDO O RISCO LEGAL ALÉM DO GDPR

O ransomware continua sendo um risco cibernético generalizado e persistente que representa inúmeros desafios legais. Há mais a se considerar, embora a conformidade com as obrigações de notificação do GDPR já possa ser uma prioridade no fluxo de trabalho da gestão de incidentes legais. Conflitos e disputas podem surgir com clientes, fornecedores ou seus parceiros comerciais: Quando a extorsão resulta no pagamento de um resgate, ou quando esse pagamento é levado em consideração ou planejado, as organizações devem estar cientes das leis antiterrorismo e de lavagem de dinheiro, bem como das sanções e da conformidade interna, como a regra de julgamento de negócio. A abordagem a alguns desses aspectos de uma perspectiva prática permitirá que as empresas verifiquem seus planos de emergência em busca de consistência e completude.

GDPR e o cronômetro de 72 horas

O ataque de ransomware médio afeta regularmente os sistemas de TI que, de alguma forma, são usados para o processamento de dados pessoais. Isso leva o ataque ao escopo do Regulamento Geral de Proteção de Dados da UE (GDPR). O GDPR contém obrigações de notificação de violação tanto para as autoridades supervisoras ("sem atraso indevido", mas no máximo 72 horas após a descoberta do incidente) e para as pessoas impactadas (apenas "sem atraso indevido"). A definição de "violação de dados" do GDPR é ampla e cobre qualquer incidente de segurança com um impacto negativo na disponibilidade, integridade ou confidencialidade dos dados pessoais, já indicando a sobreposição necessária entre fluxos de trabalho jurídicos e de TI/forenses na gestão de incidentes.

Ao lidar com situações usuais de ransomware – cronometrando as 72 horas do GDPR enquanto se administra uma situação complexa e incerta – o seguinte deverá ser levado em conta: De uma perspectiva do GDPR, a notificação para a autoridade de proteção de dados é em geral a ação mais urgente. Como dispõe o Artigo 33 do GDPR, que estabelece um limite comparavelmente baixo – de notificação salvo quando a violação dificilmente resulte em um risco para as pessoas – uma notificação "melhor prevenir do que remediar" é geralmente aconselhável. As autoridades supervisoras determinaram altos padrões para a comprovação de qualquer conclusão de não notificar e podem, por exemplo, presumir que essa avaliação foi posterior a uma análise forense de TI minuciosa. Ao mesmo tempo, a conclusão de tal investigação dentro de 72 horas é praticamente impossível, devido à falta inicial de dados de registro suficientes.

No relatório do ano passado, destacamos que a falta de dados de registro parecia ser um desavio significativo à avaliação confiável dos requisitos de notificação de violação, principalmente porque muitas organizações simplesmente não implantaram capacidades suficientes de registro em log. Parece que essa situação não melhorou de forma substancial durante o último ano.

Da mesma forma, com respeito às notificações preliminares, as organizações deverão estar cientes de que problemas de segurança preexistentes podem emergir durante um incidente. As organizações deverão perceber que elementos como aqueles citados acima de não disponibilidade de dados de registro apropriados podem, por si só, servir como um indicativo de não conformidade com a obrigação do GDPR de implantar medidas de segurança.

As multas do GDPR após esses indicativos nada mais são do que um mito: A primeira multa do GDPR já expedida, imposta na Alemanha, se referia a uma falta de medidas de segurança descoberta com base na notificação de uma violação de dados. Nesse sentido, observe que mais de 20% de todas as multas do GDPR conhecidas publicamente se referem a uma falta de implantação de medidas adequadas de segurança da informação, ocupando o segundo lugar quando classificadas por tipo de violação (fonte: Rastreador de Aplicação do GDPR).

Por fim, a avaliação de risco do GDPR deverá levar em conta a variedade e a dinâmica dos vetores de ataque dos agentes da ameaça de ransomware: 2020 mostrou um aumento significativo de incidentes de ransomware em que os invasores foram além da "abordagem de assinatura" de ransomware dos dados criptografados, acrescentando esforços persistentes para exfiltrar dados pessoais fora da infraestrutura de TI, geralmente seguidos por uma ameaça de publicar ou vender esses dados quando a vítima do ataque se recusa a atender aos pedidos de resgate. Em outras palavras: fora a encriptação que afeta a disponibilidade dos dados, a exfiltração normalmente representa um risco até mais grave para as pessoas.

Fique de olho em seus parceiros comerciais

Nas economias em rede, as organizações e seus processos comerciais estão altamente conectados e integrados. Uma interrupção na infraestrutura de TI de uma organização pode facilmente levar a graves impactos na infraestrutura das organizações associadas, e os incidentes de ransomware raramente passam despercebidos por clientes, fornecedores ou outros parceiros comerciais. Qualquer organização, portanto, deverá tomar as medidas apropriadas para considerar os terceiros pertinentes em todas as etapas da gestão de incidentes – caso contrário, haverá um risco crescente de perda de controle da narrativa, resultando não somente em dano à reputação, mas também em perda de negócio – ou até um escalonamento legal, como a rescisão de contratos ou processos de indenização civil.

Mais de

20%

de todas as multas de GDPR publicamente conhecidas se referem a uma falta de implantação de medidas adequadas de segurança da informação

"De acordo com peritos em cibersegurança, não é uma questão de **SE** uma organização estará envolvida em um incidente cibernético, mas de **QUANDO**

As organizações que passam por um ataque de ransomware devem esperar uma onda de pedidos de informação dos peritos em segurança de TI de seus parceiros para sua própria avaliação do impacto e do risco. Manter a transparência apropriada pode ser essencial para conservar e restaurar a confiança do cliente, mesmo quando não existe obrigação legal de fazer isso. A análise preventiva de potenciais obrigações contratuais relacionadas ao incidente é sempre aconselhável na preparação para a comunicação do incidente ao parceiro comercial.

Em termos de riscos de B2B, vale a pena destacar a gestão dos serviços de TI, em especial os serviços de nuvem que operam em uma infraestrutura compartilhada. Os clientes geralmente têm uma alta dependência em seu provedor de serviço quando se trata de obter disponibilidade, integridade e confidencialidade de serviços comerciais e de TI sediados na nuvem.

A despeito da prática comum de grande limitação dos provedores de serviço com respeito à sua responsabilidade nos contratos de serviços de TI, houve jurisprudência na Europa em que os clientes tiveram sucesso ao pedir indenização de seu fornecedor de TI após um ataque de ransomware.

Isso tem se baseado, por exemplo, em supostas falhas em observar as obrigações de segurança ou mesmo uma falha em observar um princípio geral do dever de cuidar dos fornecedores. O alto nível de dependência dos clientes em seu provedor de serviço de nuvem, em geral combinada com um grande volume de clientes atendidos em infraestruturas de TI compartilhadas, cria um risco multiplicador potencial para o provedor de serviço, que deverá ser levado em conta de uma perspectiva de seguro.

Quando o pagamento do resgate é a única saída...

Pagar um resgate é geralmente percebido como sendo o último recurso para recuperar-se de um ataque de ransomware. Em 2020, foi comprovado que muitas organizações foram forçadas a atender às demandas de seus invasores quanto ao pagamento em criptomoedas devido à eliminação ou criptografia dos dados de backup que, de outra forma, podiam ter sido usados para restaurar a infraestrutura de TI afetada. As organizações que consideram o pagamento desse resgate devem levar em conta as restrições legais potenciais, que podem incluir as instituições envolvidas na troca de criptomoedas e as empresas de seguro cibernético que cobrem os pagamentos de resgate. Os pagamentos de resgate são frequentemente regulados por leis nacionais e internacionais proibindo pagamentos aos chantagistas, inclusive cibercriminosos em listas de sanções ou quando eles se qualificam como sendo uma organização terrorista.

Será necessária uma auditoria legal em qualquer situação: contudo, em geral é impossível estabelecer a identidade do chantagista graças ao anonimato no ciberespaço.

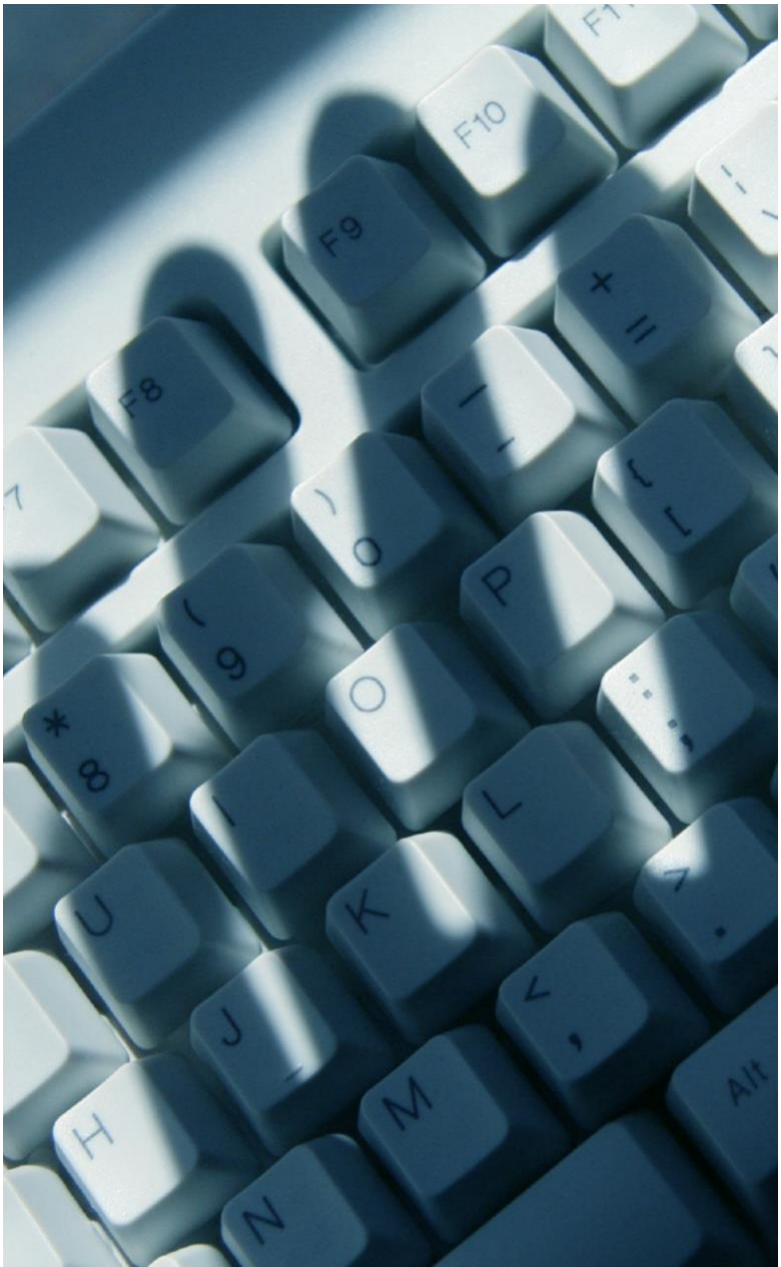
Na prática, isso significa que as organizações deverão confiar nos relatórios de inteligência publicamente disponíveis dos agentes da ameaça, por exemplo. Caso tais informações não resultem em um grau razoável de certeza, ou façam suspeitar de que o pagamento pretendido é ilícito, a legislação pertinente pode não ser capaz de impossibilitar que seja feito o pagamento do resgate.

O pagamento do resgate também pode estar relacionado a regulamentos contra a lavagem de dinheiro (AML). Embora os pagamentos de resgate das organizações extorquidas possa não violar essa legislação, os bancos e as seguradoras continuam a se distanciar tanto quanto possível do envolvimento direto nesses pagamentos. Uma orientação futura das autoridades competentes seria útil para determinar o risco de AML e os limites dos pagamentos de resgate.

Por fim, a alta administração provavelmente desejará entender os possíveis riscos referentes aos requisitos internos de conformidade, para minimizar os riscos causados por decisões inadequadas ou precipitadas que poderiam levar a uma avaliação da regra de julgamento de negócio. Atender aos requisitos correspondentes exigirá uma abordagem holística, levando em conta as informações de todos os fluxos de trabalho envolvidos.

Esteja preparado

De acordo com peritos em cibersegurança, não é uma questão de se a organização estará envolvida em um incidente cibernético, mas de quando. Recomendamos fortemente que se faça uma reflexão sobre o risco aumentado de um ataque de ransomware, com seu impacto operacional potencialmente alto, quando do estabelecimento de planos e protocolos de emergência. Quanto mais tempo uma organização economizar com uma criação rápida de equipes de resposta a incidentes, mais efetivamente os advogados internos e externos podem dar suporte e administrar os desafios jurídicos diversificados.



4 Lições aprendidas: Gestão de incidentes e de processos

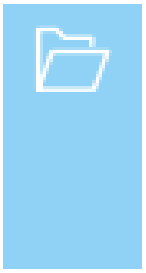
Imprimir seu plano de ação para ameaça cibernética e as informações de contato das principais partes interessadas. O melhor manual existente não o ajudará caso não possa acessá-lo quando precisar.

Notificar sua corretora e/ou seguradora sobre todos os eventos suspeitos, e na evidência de incidentes de segurança, violação de dados e extorsão cibernética.

Obter o **consentimento prévio** de sua seguradora para quaisquer despesas que você possa incorrer para restaurar e/ou resolver o incidente – salvo aquelas despesas necessárias para conter e mitigar um evento de segurança (nas primeiras 72 horas).

Em geral não estão cobertos durante a primeira resposta:

- Despesas para atualizar ou melhorar controles, políticas ou procedimentos de privacidade ou de segurança de rede além daqueles já existentes.
- Impostos, multas pecuniárias, multas contratuais, medidas cautelares ou sanções.
- Ordenados de horistas, salários, custos e despesas operacionais internos ou taxas.

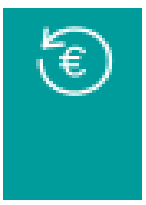


Mantenha registos apropriados e estabeleça um relatório offline (por exemplo, em Excel) com dados diários sobre:

- Horas extras do pessoal.
- Horas inativas do pessoal.
- Impacto sobre as vendas.
- Todas as despesas (inclusive valores, fornecedores e sua natureza).
- Comunicações com terceiros sobre processos potenciais.

Junte as suas informações para poder responder a essas típicas perguntas comuns nas etapas iniciais do processo de gestão de incidente:

- Quando você tomou ciência do evento?
- Como você tomou ciência dele?
- Quem tomou ciência dele? Qual a função deles?
- O que está sendo afetado (por exemplo, e-mail, drives, sistemas operacionais, sistemas financeiros e sistemas de RH)?
- Qual a natureza dos dados afetados (clientes, fornecedores, colaboradores)?
- Existe um impacto imediato nas suas operações?
- Houve uma perda de recursos, fraude no pagamento ou pagamento de extorsão?
- Qual é o nível de envolvimento ou infecção dos sistemas de terceiros ?
- O que tem sido feito até agora para mitigar as perdas?



Abstenha-se de qualquer reconhecimento formal de obrigação perante terceiros e de qualquer promessa de remuneração.

5 Entendendo o novo mercado de seguro cibernético

Em alinhamento com o mercado do seguro cibernético de rápido amadurecimento, o mercado também está se reestruturando. Essas mudanças oferecem um relance do futuro e algum insight sobre que ações deverão ser praticadas agora para manter a sua segurabilidade.

No primeiro trimestre de 2021, as taxas cibernéticas aumentaram uma média de **39%** para todos os setores na base de clientes da Marsh na Europa Continental.

Como os preços na Europa são tradicionalmente baixos, as seguradoras estão se empenhando em alinhá-los mais aos preços globais.

A taxa de sinistros estimada aumentou para **74%** em 2020 (excluindo custos de gestão da crise pagos pelas seguradoras diretamente) e as seguradoras primárias estão nos dizendo que sua taxa de sinistros é até mais alta do que consta aqui.

A falta de apetite para novos negócios das seguradoras que estão voltadas para renovações significa que existe menos concorrência no mercado.

Insights mais profundos sobre números de processos e seu impacto mudaram o mercado de seguros em termos de prêmio e demanda de seguradora.

8%

Aumento nos processos relatados em 2020 (vs 2019)

37%

Aumento da taxa média no 4° trimestre de 2021

74%

Taxa de sinistros estimada na Europa Continental em 2020

39%

Aumento da taxa média no 1° trimestre de 2021

Fonte: *Dados internos e análise da Marsh.*

Conclusão

Estamos no meio de uma onda significativa de ransomware, que está deixando as empresas até mais conscientes do quanto são dependentes da tecnologia. Essa dependência somente aumentará na medida em que a tecnologia continua a avançar na nossa sociedade, especialmente em termos de eficiência e qualidade de vida. Certamente é essencial ter uma melhor gestão de risco.

Nosso relatório de processos também demonstra como os cibercriminosos estão tirando vantagem dos problemas contemporâneos, como a pandemia da COVID-19.

Mas há boas notícias para compartilhar nesse ambiente obscuro: Vemos a eficácia de alguns controles de cibersegurança, na redução tanto da frequência quanto da gravidade dos ataques.

É por isso que as seguradoras estão constantemente se concentrando nos controles de cibersegurança nas organizações, bem como na resiliência cibernética intensificada. Poderíamos até afirmar que o setor de seguro cibernético é um catalisador de melhores controles de cibersegurança e resiliência cibernética.

Como resultado:

- A aquisição do seguro cibernético garante maturidade cibernética acima da média.
- O seguro agora é visto como uma ferramenta que comprova que as empresas têm instaladas defesas cibernéticas entre as melhores da categoria.
- O seguro cibernético é uma maneira comprovada de melhorar a resiliência cibernética das organizações.

Na Marsh, somos capazes de oferecer um diagnóstico de segurabilidade sem custo, de modo que você esteja bem preparado para a sua colocação ou renovação de seguro cibernético.

Indo adiante, nós da Marsh, junto com nossas parceiras Microsoft, Kivu e CMS, continuaremos a aprender com as necessidades e perguntas de nossos clientes, e com os processos com que lidamos, para ajudar as organizações a se tornarem mais resilientes à cibernética.

Sobre a Marsh

A Marsh é a principal corretora de seguro e consultora de risco do mundo. Com cerca de 40.000 colaboradores operando em mais de 130 países, a Marsh atende a clientes comerciais e individuais com soluções de risco controlado por dados e com serviços de consultoria. A Marsh é uma empresa da Marsh McLennan (NYSE: MMC), a empresa líder na prestação de serviços profissionais no mundo nas áreas de risco, estratégia e pessoas. Com uma receita anual de mais de US$ 18 bilhões, a Marsh McLennan ajuda os clientes a navegar em um ambiente cada vez mais dinâmico e complexo através de quatro empresas líderes no mercado: Marsh, Guy Carpenter, Mercer e Oliver Wyman. Para mais informações, visite mmc.com, siga-nos no LinkedIn e noTwitter, ou subscreva o BRINK.

Sobre a Microsoft

A Microsoft é a plataforma e a empresa de produtividade líder para priorizar dispositivos móveis e a nuvem, e a sua missão é capacitar todas as pessoas e todas as organizações no planeta para que obtenham mais.

Sobre a KIVU

A Kivu é uma empresa líder em cibersegurança global voltada para restaurar a liberdade de operação e minimizar a interrupção do negócio. O objetivo da Kivu é trazer de volta os nossos clientes de forma rápida e segura.

Sobre a CMS

A CMS é um escritório de advocacia voltado para o futuro. Com mais de 70 escritórios em mais de 40 países e mais de 4.800 advogados, combinamos um profundo entendimento do mercado local com uma visão geral global, o que nos dá a capacidade não somente de ver o que está por vir, mas de podermos ajustar isso. Com uma equipe de especialistas em proteção de dados e cibersegurança totalizando pouco mais de 200 pessoas, incorporamos a mentalidade da próxima geração em toda a nossa assessoria – desde a resposta à violação cibernética até investigações regulatórias e acompanhamentos de processos, bem como a conformidade. Nossa equipe inclui ex-reguladores que estiveram no centro do desenvolvimento da legislação de proteção de dados. Em um mundo de mudanças sempre aceleradas, em que a tecnologia é cada vez mais importante no desenvolvimento das estratégias globais, nossa assessoria voltada para o negócio ajuda clientes de todos os tamanhos a enfrentar o futuro com confiança. Visite http://cms.law.

Esta é uma comunicação de marketing.

As informações aqui contidas estão baseadas em fontes que acreditamos serem confiáveis e deverão ser entendidas como sendo tão somente informações gerais sobre gestão de risco e seguro. As informações não pretendem ser consideradas como recomendações com respeito a qualquer situação individual e não podem ser vistas como tal.

As declarações pertinentes a questões legais, tributárias ou contábeis deverão ser entendidas como observações gerais com base exclusivamente em nossa experiência como corretores de seguro e consultores de risco, não devendo ser consideradas como orientação legal, tributária ou contábil, que não estamos autorizados a fornecer.