Relatório Cyber de Allianz Global Corporate & Specialty mostra que o custo crescente dos ataques de ransomware impactam empresas de todos os tamanhos

O ransomware continua a ser um dos principais riscos cibernéticos para as organizações em todo o mundo, enquanto os incidentes de comprometimento de e-mails comerciais vem crescendo e aumentarão ainda mais na era dos "deep fakes". Ao mesmo tempo, a guerra na Ucrânia e tensões geopolíticas mais amplas são uma grande preocupação, pois as hostilidades podem se espalhar pelo espaço cibernético e causar ataques direcionados contra empresas, infra-estrutura ou cadeias de abastecimento, de acordo com um novo relatório da Allianz Global Corporate & Specialty (AGCS).

A análise anual da seguradora sobre o cenário de risco cibernético também destaca as ameaças emergentes decorrentes da crescente dependência dos serviços em nuvem, um cenário de responsabilidade civil em evolução que significa maiores indenizações e penalidades, bem como o impacto da escassez de profissionais de segurança cibernética. Tais vulnerabilidades potenciais significam que hoje a resiliência da segurança cibernética de uma empresa é examinada por mais gente do que nunca, incluindo investidores globais, o que significa que muitas empresas agora a classificam como sua maior preocupação relacionada a riscos ambientais, sociais e de governança (ESG), observa o relatório.

"O cenário de risco cibernético não permite que uma empresa durma no ponto. Ransomwares e esquemas de phishing estão tão ativos como sempre e, além disso, há a perspectiva de uma guerra cibernética híbrida", diz **Scott Sayce, Diretor Global de Cyber na AGCS e Diretor de Grupo do Centro Cibernético de Competência**. "A maioria das empresas não será capaz de escapar de uma ameaça cibernética". Entretanto, é claro que as organizações com boa maturidade no assunto estão mais bem equipadas para lidar com incidentes. Mesmo quando são atacadas, as perdas são tipicamente menos graves devido aos mecanismos de identificação e resposta estabelecidos.

"Embora vejamos bons progressos, nossa experiência também mostra que muitas empresas ainda precisam fortalecer seus controles cibernéticos, particularmente no que diz respeito a treinamentos em segurança de TI, melhor segmentação de rede para ambientes críticos e planos de resposta a incidentes cibernéticos e governança da segurança. Como seguradora atuante no ramo cyber, estamos dispostos a ir além da pura transferência de riscos, ajudando os clientes a se adaptarem a um cenário em constante mudança e a elevar seus níveis de proteção".

Em todo o mundo, a freqüência dos ataques de ransomware permanece alta, assim como os custos de sinistros relacionados. Houve um recorde de 623 milhões de ataques em 2021, o dobro e 2020. Embora a freqüência tenha caído em 23% globalmente durante o primeiro semestre de 2022, o total acumulado no ano ainda excede o montante dos anos de 2017, 2018 e 2019, quando a Europa viu os ataques aumentarem durante este período. Prevê-se que os ransomwares causarão US$ 30 bilhões em danos a organizações em todo o mundo até 2023. Do ponto de vista da AGCS, o valor dos sinistros de ransomware nos quais a empresa esteve envolvida juntamente com outras seguradoras, representou bem mais de 50% de todos os custos de sinistros cibernéticos durante 2020 e 2021.

Dupla e tripla extorsão são agora a regra

"O custo dos ataques de ransomware aumentou à medida que os criminosos visavam empresas maiores, infra-estrutura crítica e cadeias de abastecimento. Os criminosos aperfeiçoaram suas táticas para extorquir mais dinheiro", explica Sayce. "Ataques duplos e triplos de extorsão são agora o padrão - além da criptografia dos sistemas, dados sensíveis são cada vez mais roubados e utilizados como uma alavanca para demandas de extorsão a parceiros comerciais, fornecedores ou clientes". É provável que a severidade do resgate continue sendo uma ameaça chave para as empresas, alimentada pela crescente sofisticação dos criminosos e pelo aumento da inflação, o que se reflete no aumento do custo dos especialistas em TI e segurança cibernética.

Cada vez mais, empresas de pequeno e médio porte, que muitas vezes carecem de controles e recursos para investir em segurança cibernética, estão sendo alvo de criminosos, pois estão mais expostas que as grandes companhias. As gangues cibernéticas também estão usando uma ampla gama de técnicas de assédio, adaptando suas demandas de resgate a empresas específicas e utilizando negociadores especializados para maximizar os retornos.

Esquemas sofisticados

Os ataques a e-mails comerciais (BEC) continuam a aumentar, facilitados pela crescente digitalização e disponibilidade de dados, a mudança para o trabalho remoto e, cada vez mais, a tecnologia 'deep fake' e as conferências virtuais. De acordo com o FBI, os golpes BEC totalizaram 43 bilhões de dólares no mundo inteiro de 2016 a 2021, com um pico de 65% entre julho de 2019 e dezembro de 2021 apenas. Os ataques estão se tornando mais sofisticados e direcionados com os criminosos agora utilizando plataformas de reuniões virtuais para enganar os funcionários e conseguir que transfiram fundos ou compartilhem informações sensíveis. Cada vez mais, estes ataques são possibilitados pela inteligência artificial com "deep fakes" de imagem e voz que imitam os executivos das empresas. No ano passado, um funcionário de um banco dos Emirados Árabes Unidos fez uma transferência de 35 milhões de dólares após ter sido enganado pela voz clonada de um diretor da empresa.

A ameaça da guerra cibernética

A guerra na Ucrânia e as tensões geopolíticas mais amplas são um fator importante para remodelar o cenário da ameaça cibernética, pois aumenta o risco de espionagem, sabotagem e ataques cibernéticos destrutivos contra empresas com laços com a Rússia e a Ucrânia, bem como contra aliados e países vizinhos. Os atos cibernéticos patrocinados pelo Estado poderiam ter como alvo potenciais infraestruturas críticas, cadeias de abastecimento ou corporações. "Até agora, a guerra entre a Rússia e a Ucrânia não levou a um notável aumento nos sinistros de seguros cibernéticos, mas aponta para um risco potencialmente maior por parte dos Estados-nação", explica Sayce. Embora atos de guerra sejam tipicamente excluídos dos produtos de seguros tradicionais, o risco de uma guerra cibernética híbrida acelerou os esforços no mercado de seguros para tratar a questão da guerra e dos ataques cibernéticos patrocinados pelo Estado em clausulados e fornecer clareza de cobertura para os clientes.

Os especialistas da AGCS identificam uma série de outras tendências no relatório Cyber: O cenário de ameaças em mudança, inclusive:

- Os ataques às cadeias de abastecimento - seja em infraestruturas críticas como o Gasoduto Colonial ou em serviços de nuvem - surgiram como um risco significativo. Cada vez mais, as gangues de ransomware usam a ameaça de perturbação para pressionar as empresas a pagar resgates, sendo as empresas fabricantes particularmente vulneráveis.

- As empresas continuam a transferir seus serviços e armazenamento de dados para a nuvem, apesar da crescente preocupação com a segurança e a agregação de riscos. Ao depender de um pequeno número de provedores para serviços em nuvem ou segurança cibernética, a sociedade está criando grandes concentrações em torno de poucos pontos de falha. É um equívoco comum que a terceirização ou o fornecedor da nuvem assumirá total responsabilidade no caso de um incidente.

- A responsabilidade civil de terceiros, incluindo multas e penalidades, está se tornando mais relevante com os avanços da tecnologia, organizações que coletam mais informações e a regulamentação de privacidade de dados aplicada. Praticamente qualquer incidente cibernético - incluindo ransomware de dupla-extorsão - pode levar a litígios e demandas de indenização das partes afetadas.

- **A escassez de profissionais** está dificultando os esforços para melhorar a segurança cibernética. Embora haja uma conscientização crescente entre os conselhos administrativos, o

número de empregos de segurança cibernética não preenchidos no mundo todo cresceu 350% nos últimos oito anos para 3,5 milhões, estimativas mostram, o que significa que muitas empresas lutam para contratar, impactando sua capacidade de melhorar sua postura de segurança cibernética.

- **Segurança cibernética cada vez mais vista através da lente ESG.** Hoje, a resiliência da segurança cibernética das empresas é examinada por muito mais grupos do que no passado. Cada vez mais, considerações de segurança cibernética são incorporadas às estruturas de análise de risco ESG de provedores de dados, que examinam as práticas das empresas para avaliar sua preparação com o crime cibernético. Garantir que os processos e políticas cibernéticas de uma empresa sejam compreendidos em nível de diretoria e que os processos de monitoramento de risco estejam em vigor nunca foi tão importante.

Em resposta a um ambiente de risco mais complexo e ao aumento da atividade de sinistros cibernéticos, o setor de seguros está avaliando mais diligentemente os perfis de risco cibernéticos das empresas em uma tentativa de incentivar as empresas a melhorar sua segurança e seus controles de gerenciamento de risco.

"A boa notícia é que agora estamos vendo uma conversa muito diferente do que há alguns anos atrás sobre a qualidade do risco cibernético", diz Sayce. "Estamos ganhando muito melhores percepções e apreciamos os clientes que vão mais longe a fim de nos fornecer dados abrangentes". Isto também nos ajuda a fornecer mais valor e oferecer informações e conselhos úteis aos clientes, tais como quais controles são mais eficazes ou onde melhorar ainda mais a gestão de riscos e as abordagens de resposta. O resultado deve ser menos eventos cibernéticos (ou menos significativos) para nossos clientes e menos sinistros para nós. Tal colaboração também ajudará a criar um mercado de seguro cibernético sustentável a longo prazo que não apenas se baseia em coberturas tradicionais, mas, cada vez mais, na integração de riscos cibernéticos em programas cativos e outros conceitos alternativos de transferência de riscos".

Sobre a Allianz Global Corporate & Specialty

A Allianz Global Corporate & Specialty (AGCS) é uma seguradora corporativa líder global e uma unidade de negócios chave do Grupo Allianz. Fornecemos consultoria de risco, soluções de seguros Property-Casualty e transferência alternativa de risco para um amplo espectro de riscos comerciais, corporativos e especiais em nove linhas de negócios dedicadas e seis hubs regionais.

Nossos clientes são tão diversos quanto os negócios podem ser, desde empresas da Fortune Global 500 até pequenas empresas. Entre eles estão não apenas as maiores marcas de consumo do mundo, instituições financeiras, empresas de tecnologia, as indústrias globais de aviação e transporte marítimo, mas também operadoras de satélite ou produções cinematográficas de Hollywood. Todos buscam a AGCS para soluções inteligentes e programas globais para seus maiores e mais complexos riscos em um ambiente de negócios multinacional dinâmico e nos confiam para oferecer uma experiência excepcional em sinistros.

Em todo o mundo, a AGCS opera com equipes próprias em mais de 30 países e por meio da rede e parceiros do Grupo Allianz em mais de 200 países e territórios, empregando cerca de 4.250 pessoas. Como uma das maiores unidades de Property-Casualty do Grupo Allianz, somos respaldados por classificações financeiras fortes e estáveis. Em 2021, a AGCS gerou um total de € 9,5 bilhões de prêmios brutos globalmente.

Para mais informações acesse www.agcs.allianz.com ou siga nossos perfis no Twitter @AGCS_Insurance e LinkedIn.

Fonte: AGCS, em 26.10.2022.