Allianz: Empresas precisam reforçar os controles cibernéticos para combater a pandemia de ransomware

## Allianz: Empresas precisam reforçar os controles cibernéticos para combater a pandemia de ransomware

- O relatório da AGCS destaca as tendências cibernéticas de risco que impulsionam o aumento de incidentes de resgate, tais como dupla ou tripla extorsão e ataques à cadeia de suprimentos.
- A interrupção e recuperação dos negócios são as principais causas de perdas financeiras para as empresas.
- Muitos ataques poderiam ser evitados se as empresas reforçassem sua segurança e controles cibernéticos - muitas vezes com medidas simples.

**São Paulo - 19 de outubro de 2021 Du**rante a crise da Covid-19, outro surto aconteceu no espaço cibernético: uma pandemia digital impulsionada por ransomwares. Ataques de malware que codificam dados e sistemas da empresa e exigem um pagamento de resgate por sua liberação estão surgindo globalmente. A crescente frequência e gravidade dos incidentes é impulsionada por vários fatores: o número crescente de diferentes padrões de ataque, tais como campanhas de extorsão 'duplas' e 'triplas'; um modelo de negócio criminoso em torno de 'ransomware as a service' e criptomoedas; a recente disparada das exigências de resgate; e o aumento dos ataques à cadeia de suprimentos. Em um novo
relatório
, a seguradora Allianz Global Corporate & Specialty (AGCS) analisa os últimos desenvolvimentos de risco em torno de ransomware e descreve como as empresas podem fortalecer suas defesas com boas práticas de higiene cibernética e segurança de TI.

"O número de ataques de resgate pode até aumentar antes que a situação melhore", diz Scott Sayce, Diretor Global de Cyber na AGCS. "Nem todos os ataques têm um alvo. Os criminosos também adotam a ‘abordagem do regador’ para explorar os negócios que não estão interpelando ou entendendo as vulnerabilidades que possam ter. Como seguradoras, devemos continuar a trabalhar com nossos clientes para ajudar as empresas a entender a necessidade de fortalecer seus controles. Ao mesmo tempo, no atual mercado de seguros cibernéticos em rápida evolução, a prestação de serviços de resposta a emergências, bem como a compensação financeira, é agora o padrão".

A atividade de intrusão cibernética global saltou 125% no primeiro semestre de 2021 em comparação com o ano anterior, segundo a Accenture , sendo o ransomware e as operações de extorsão um dos principais contribuintes por trás desse aumento. De acordo com o FBI , houve um aumento de 62% nos incidentes de resgate nos EUA no mesmo período que se seguiu a um aumento de 20% para o ano 2020. Estas tendências de riscos cibernéticos estão espelhadas na própria experiência de sinistros da AGCS. A seguradora esteve envolvida em mais de mil reclamações cibernéticas em 2020 , contra cerca de 80 em 2016; o número de sinistros de ransomware (90) aumentou 50% em comparação com 2019 (60). Em geral, as perdas resultantes de incidentes cibernéticos externos, como os ataques de resgate ou de Negação de Serviço Distribuído (DDoS), representam a maior parte do valor de todas os sinistros cibernéticas analisados pela AGCS ao longo dos últimos seis anos.

A crescente dependência da digitalização, o aumento do trabalho remoto durante o Covid-19 e as restrições de orçamento de TI são apenas algumas das razões pelas quais as vulnerabilidades de TI se intensificaram, oferecendo incontáveis pontos de acesso para os criminosos explorarem. A adoção mais ampla de criptomoedas, como o Bitcoin, que permite pagamentos anônimos, é outro fator chave para o aumento de ransomwares.

**Cinco áreas de foco**

**N**o relatório , a AGCS identifica cinco tendências no universo do ransomware, embora estas estejam em constante evolução e possam mudar rapidamente na corrida "gato e rato" entre cibercriminosos e empresas:

- O desenvolvimento de **'ransomware como serviço' fa**cilitou a realização de ataques por parte dos criminosos. Correndo como um negócio comercial, grupos hackers como REvil e Darkside vendem ou alugam suas ferramentas de hacking para outros. Eles também fornecem uma gama de serviços de suporte. Como resultado, muitos mais agentes de ameaças maliciosas estão operando.

- **De simples a dupla e a tripla extorsão... As tá**cticas de "dupla extorsão" estão a crescendo. Os criminosos combinam a criptografia inicial de dados ou sistemas, ou até mesmo seus back-ups, com uma forma secundária de extorsão, como a ameaça de liberação de dados

sensíveis ou pessoais. Em tal cenário, as empresas afetadas têm que gerenciar a possibilidade de uma interrupção importante do negócio e um evento de violação de dados, o que pode aumentar significativamente o custo final do incidente. Os incidentes de 'extorsão tripla' podem combinar ataques DDoS, criptografia de arquivos e roubo de dados - e não visam apenas uma empresa, mas potencialmente também seus clientes e parceiros de negócios. Um caso notável foi uma clínica de psicoterapia na Finlândia - um resgate foi exigido do hospital. Ao mesmo tempo, também foram exigidas somas menores aos pacientes em troca da não divulgação de suas informações pessoais.

- **A cadeia de suprimentos: o próximo grande negócio. E**xistem dois tipos principais - aqueles que têm como alvo os provedores de software/serviços de TI e os utilizam para espalhar o malware (por exemplo, os ataques da Kaseya ou Solarwinds). Ou aqueles que têm como alvo cadeias de suprimento físicas ou infra-estruturas críticas, como a que teve impacto sobre o Gasoduto Colonial. Os prestadores de serviços provavelmente se tornarão alvos principais, pois freqüentemente fornecem soluções de software a centenas ou milhares de empresas e, portanto, oferecem aos criminosos a chance de um pagamento maior.

- **Dinâmica do resgate:** As exigências de resgate dispararam ao longo dos últimos 18 meses. De acordo com Palo Alto Networks , a demanda média de extorsão nos EUA foi de US$ 5,3 milhões no primeiro semestre de 2021, um aumento de 518% em relação à média de 2020; a maior demanda foi de US$ 50 milhões, acima dos US$ 30 milhões do ano anterior. A quantia média paga aos hackers é cerca de 10 vezes menor do que a demanda média, mas esta tendência geral de aumento é alarmante.

- **Pagar ou não pagar:** O pagamento do resgate é um tópico controverso. As agências de aplicação da lei normalmente desaconselham o pagamento de pedidos de extorsão para não incentivar ainda mais os ataques. Mesmo quando uma empresa decide pagar um resgate, o dano pode já ter sido feito. Restaurar os sistemas e permitir a recuperação do negócio é uma tarefa enorme, mesmo quando uma empresa tem a chave de decifração.

**A interrupção do negócio e os custos de recuperação são os principais motores das perdas**

**A** interrupção dos negócios e os custos de restauração são os maiores motores por trás das perdas cibernéticas, como os ataques de resgate, de acordo com a análise de sinistros da AGCS. Eles são responsáveis por mais de 50% do valor de cerca de 3.000 sinistros cibernéticos do setor de seguros no valor de cerca de 750 milhões de euros (885 milhões de dólares) que o mercado observou em mais de seis anos.

O custo médio total da recuperação e do tempo parado - em média 23 dias - de um ataque de ransomware mais que dobrou no ano passado, aumentando de $761.106 para $1,85mn em 2021
.

O aumento dos ataques de ransomware nos últimos anos desencadeou uma grande mudança no mercado de seguros cibernéticos. As taxas têm aumentado, segundo a corretora Marsh , enquanto a capacidade vem se restringindo. Os subscritores estão colocando um escrutínio crescente nos controles de segurança cibernética empregados pelas empresas.

"Três em cada quatro empresas não atendem aos requisitos da AGCS para segurança cibernética", explica Marek Stanislawski, Diretor Global de Subscrição Cibernética da AGCS. "As empresas precisam investir em segurança de TI. As perdas podem ser evitadas se as organizações seguirem as melhores práticas. Uma casa com uma porta aberta tem muito mais probabilidade de ser assaltada do que uma casa trancada. ”

**Lista de verificação com as melhores práticas de segurança de TI**

**A** AGCS publicou uma lista de verificação com recomendações para a gestão eficaz do risco cibernético. "Em cerca de 80% dos incidentes de ransomware, a perda de informação poderia ter sido evitada se as organizações tivessem seguido as melhores práticas. A aplicação regular de patches, a autenticação multi-fator, assim como o treinamento de segurança da informação e conscientização e o planejamento de resposta a incidentes são essenciais para evitar ataques de resgate e também constituem uma boa higiene cibernética", diz Rishi Baviskar, Diretor Global de Peritos Cibernéticos da AGCS Risk Consulting. "Se as empresas aderirem às recomendações de melhores práticas, há uma boa chance de não se tornarem vítimas de ransomware. Numerosas falhas de segurança podem ser eliminadas, muitas vezes com

medidas simples". ”

No caso de um ataque, a cobertura do seguro cibernético evoluiu para fornecer serviços de resposta a incidentes de emergência que normalmente incluem acesso a um gerente de crise profissional, suporte forense de TI e assessoria jurídica. Outras ofertas incluem treinamento de segurança de TI para funcionários e assistência no desenvolvimento de um plano de gerenciamento de crise cibernética.

**Fonte: AG**CS, em 20.10.2021.