- **Incidentes de ransomware estão aumentando à medida que criminosos utilizam a exfiltração de dados e ataques à cadeia de suprimentos para maximizar sua influência.**
- **Análise da Allianz Commercial mostra que número de ataques cibernéticos que se tornam públicos também está aumentando.**
- **Violações cibernéticas que não são detectadas e contidas precocemente podem ser até mil vezes mais caras do que aquelas que são.**
- **As prioridades de segurança cibernética das empresas devem incluir o reforço de suas capacidades de detecção e resposta.**

O número de casos de ransomware e extorsão aumentou em 2023, segundo o relatório da Allianz Commercial, Tendências de Segurança Cibernética 2023: As últimas ameaças e as melhores práticas de mitigação de riscos - antes, durante e após um hack.

De acordo com o documento, os hackers aumentaram o direcionamento às cadeias de suprimentos de TI e, por meio de ataques cibernéticos em massa, estão encontrando novas formas de extorquir dinheiro de grandes e pequenas empresas. A maioria dos ataques de ransomware envolve o roubo de dados pessoais ou comerciais sensíveis, com o propósito de extorsão, aumentando o custo e a complexidade dos incidentes, assim como o dano à reputação. A análise da Allianz Commercial sobre as grandes perdas cibernéticas mostra que o número de casos em que ocorre exfiltração de dados está aumentando a cada ano – dobrando de 40% em 2019 para quase 80% em 2022, com 2023 significativamente mais alto.

"Este ano, a frequência de reclamações cibernéticas aumentou novamente, à medida que grupos de ransomware continuam a evoluir suas táticas", diz **Scott Sayce, Chefe Global de Cyber da Allianz Commercial.** "Com base nas reclamações ocorridas durante o primeiro semestre de 2023, esperamos ver cerca um crescimento de 25% nas reclamações até o final do ano. Os hackers estão focados novamente nas economias ocidentais, com ferramentas mais poderosas, processos aprimorados e mecanismos de ataque. Dada essa dinâmica, uma empresa bem protegida é necessária para enfrentar a ameaça e, cada vez mais, o elemento mais importante disso é o desenvolvimento de capacidades fortes de detecção e resposta".

Como está evoluindo o risco de ransomware?

De acordo com o relatório da Allianz Commercial, a frequência de reclamações cibernéticas se estabilizou em 2022, refletindo a melhoria da segurança cibernética e das ações de gerenciamento de riscos entre as empresas seguradas. Agências de aplicação da lei visando gangues, juntamente com o conflito Rússia-Ucrânia, também ajudaram a conter a atividades de ransomware. No entanto, os ataques de ransomware sozinhos aumentaram 50% durante o primeiro semestre de 2023. Os chamados kits de Ransomware como, por exemplo, o serviço (RaaS), com preços a partir de apenas US□40, continuam sendo um fator chave na frequência dos ataques. As gangues de ransomware também estão realizando ataques mais rápidos, com o número médio de dias para executar caindo de cerca de 60 dias em 2019, para quatro.

"Incidentes de dupla e tripla extorsão - usando uma combinação de criptografia, exfiltração de dados e ataques de Negação de Serviço Distribuído - para obter dinheiro não são novos, mas agora são mais prevalentes", diz **Michael Daum, Chefe Global de Reclamações de Cyber da Allianz Commercial**. "Vários fatores são combinados para tornar a exfiltração de dados mais atraente para os atores de ameaças. O escopo e a quantidade de informações pessoais coletadas estão aumentando, enquanto as regulamentações de privacidade e violação de dados estão se tornando mais rigorosas globalmente. Ao mesmo tempo, a tendência para a terceirização e o acesso remoto leva a mais interfaces para os atores de ameaças explorarem".

A exfiltração de dados pode aumentar significativamente o custo de uma perda ou reclamação cibernética. Tais incidentes podem levar mais tempo para serem resolvidos, enquanto os serviços

jurídicos e de forense de TI podem ser extremamente caros. Se dados foram roubados, as empresas devem saber exatamente quais dados foram exfiltrados e provavelmente terão que notificar os clientes, que podem buscar compensação ou ameaçar litígio.

Este ano, aconteceram vários grandes ataques cibernéticos em massa, à medida que os hackers aproveitaram as vulnerabilidades em software e fraquezas nas cadeias de suprimentos de TI para atingir múltiplas empresas. Por exemplo, o ataque cibernético em massa MOVEit, que explorou um produto de software de transferência de dados, impactou milhões de indivíduos e milhares de empresas, contribuindo para o aumento da frequência de reclamações em 2023 até o momento, afetando múltiplos segurados simultaneamente.

"Podemos esperar mais ataques cibernéticos em massa no futuro. As empresas e suas seguradoras precisam entender melhor a interconectividade e as dependências que existem entre organizações e dentro das cadeias de suprimentos digitais ", diz Daum.

Aumento de casos públicos

No passado, o número de incidentes cibernéticos que se tornaram públicos foi baixo. Atualmente, a história diferente, pois, com a exfiltração de dados, os hackers ameaçam publicar os dados roubados online. A análise da Allianz Commercial sobre grandes perdas cibernéticas (€1 milhão+) mostra que a proporção de casos que se tornaram públicos aumentou de cerca de 60% em 2019, para 85% em 2022, com previsão ainda maior para 2023.

"Hoje, se você tem exfiltração de dados, é provável que se torne público, e toda empresa precisa estar preparada para isso", diz **Rishi Baviskar, Chefe Global de Consultoria de Risco Cibernético da Allianz Commercial.**

Com potenciais consequências financeiras e de reputação custosas, as empresas podem se sentir mais pressionadas para pagar resgates quando os dados foram roubados. O número de empresas que pagam um resgate aumenta ano após ano, passando de apenas 10% em 2019 para 54% em 2022, novamente com base na análise apenas de grandes perdas (€1 milhão+). As empresas estão duas vezes e meia mais propensas a pagar um resgate se os dados forem exfiltrados, além da criptografia.

No entanto, pagar um resgate por dados exfiltrados não resolve necessariamente o problema. A empresa ainda pode enfrentar litígios de terceiros por violação de dados, especialmente nos Estados Unidos. Existem poucos casos em que uma empresa deva acreditar que não há outra solução além de pagar o resgate para poder recuperar o acesso aos seus sistemas ou dados. Qualquer parte afetada deve sempre informar e cooperar com as autoridades.

A importância da detecção precoce e resposta rápida

Proteger uma organização contra invasões cibernéticas continua sendo um jogo de gato e rato, no qual os cibercriminosos têm a vantagem. A análise da Allianz Commercial de mais de 3 mil reclamações cibernéticas nos últimos cinco anos, mostra que a manipulação externa de sistemas é a causa de mais de 80% de todos os incidentes. Os hackers usam a inteligência artificial (IA) para automatizar e acelerar os ataques, criando malwares, phishing e simulações de vozes mais eficazes. Combinado com a explosão de dispositivos móveis conectados – o relatório mostra um número crescente de incidentes causados por má segurança cibernética nessa área -, os caminhos de ataque parecem propensos a aumentar.

As capacidades e ferramentas de detecção e resposta precoces estão se tornando cada vez mais importantes. Cerca de 90% dos incidentes são contidos precocemente. No entanto, se um ataque não for interrompido nas fases iniciais, as chances de evitar que ele se torne algo muito mais sério e caro diminuem consideravelmente.

"A segurança cibernética tradicional tem se concentrado na prevenção, com o objetivo de manter

os ataques fora de uma rede. Embora o investimento em prevenção reduza o número de ciberataques bem-sucedidos, sempre haverá um 'hiato' que permitirá que os ataques passem. Por exemplo, não é possível impedir que todos os funcionários cliquem em e-mails de phishing cada vez mais sofisticados ", diz Baviskar.

As empresas devem direcionar gastos adicionais em segurança cibernética para detecção e resposta, em vez de apenas adicionar mais camadas de proteção e prevenção. Apenas um terço das empresas descobre uma violação de dados por meio de suas próprias equipes de segurança. No entanto, a tecnologia de detecção precoce está, prontamente, disponível e eficaz.

"Os sistemas de detecção estão constantemente melhorando e podem evitar muita dor, reduzindo os tempos de detecção e resposta. Isso é algo que procuramos em nossas avaliações e subscrições de risco cibernético", acrescenta Baviskar.

Violações cibernéticas que não são detectadas e contidas precocemente podem ser até mil vezes mais caras do que aquelas que são e a a detecção e resposta precoces podem evitar que uma perda de €20.000 se transforme em uma de €20 milhões, destaca o relatório.

"A prevenção impulsiona a frequência dos ataques e a resposta é responsável pelo quão significativa será a perda - seja um incidente de TI menor ou uma crise corporativa. Acreditamos que as empresas podem se preparar de maneira significativa e há espaço para melhorias em como elas respondem a essas ameaças de atacantes. Em última análise, as capacidades de detecção precoce e resposta serão essenciais para mitigar o impacto dos ciberataques e garantir um mercado de seguros cibernéticos sustentável no futuro”, conclui Daum".

Fonte: Allianz Commercial, em 06.11.2023.