Evento generalizado

Um único ataque e/ou falha de uma tecnologia amplamente utilizada pode criar um risco agredado que excede a capacidade do setor segurador para segurar. A fim de proporcionar aos segurados clareza de cobertura e estabilidade de mercado, a Chubb prevê limites, retenções e cosseguros afirmativos e específicos para esses eventos generalizados. Seguem-se uns exemplos hipotéticos de eventos generalizados.

- Ataque cibernético a sistema operativo global

1

1. O evento

A empresa Exemplo tem mais de 500 000 clientes individuais e 5000 clientes empresariais. Um dia, os seus funcionários descobriram que não conseguiam aceder a nenhuma das suas estações de trabalho, aplicações críticas ou dados que dependiam de um sistema operativoconhecido . Felizmente, havia alguns usuários na equipa de TI que conseguiam aceder usando dispositivos com um sistema operativo diferente, o que lher permitiu analisar o problema. Uma investigação inicial revelou problemas críticos no sistema operativo do servidor que tinham afetado vários sistemas internos e portais de contas de clientes.

2

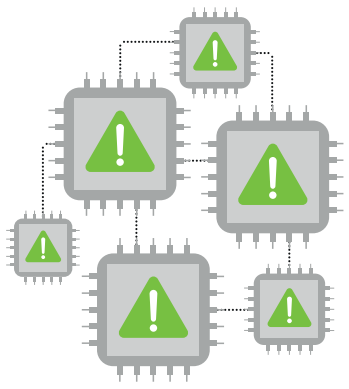
2. O problema

A empresa Exemplo comunicou o incidente assim que o descobriu, recorrendo rapidamente a um Gestor de Resposta a Incidentes (GRI) que efetuou a triagem do incidente com base nos factos iniciais. O GRI recorreu a uma empresa forense especializada em TI para ajudar a empresa Exemplo na investigação. O GRI recorreu também a advogados e especialistas em relações públicas.

No mesmo dia, vários meios de comunicação social noticiaram que empresas de todas as dimensões e de diversos setores tinham sido vítimas de um ataque cibernético e que o problema parecia estar a alastrar-se. Vários relatórios afirmavam que todas as vítimas pareciam utilizar o mesmo sistema operativo de servidor. No dia seguinte, as agências governamentais de cibersegurança emitiram declarações oficiais, explicando que o ataque explorava uma vulnerabilidade de dia zero num sistema operativo específico, que se propagava através de uma porta de rede informática comummente utilizada e aberta ao público. As aplicações de software dependem do sistema operativo, pelo que a funcionalidade das aplicações em muitasempresas mundiais foi gravemente afetada, independentemente da geografia, dimensão ou indústria.

A equipa de resposta a incidentes também contribuiu com uma estratégia de mitigação. A equipa de relações públicas criou comunicações cuidadosamente elaboradas para os clientes da empresa Exemplo para os informar da causa da interrupção do serviço. Os consultores jurídicos ajudaram a notificar os organismos jurídicos e regulamentares relevantes e os especialistas em TI trabalharam para identificar possíveis soluções alternativas, utilizando outros sistemas operativos enquanto aguardavam pelos conselhos de recuperação do fornecedor do sistema operativo e dos investigadores de segurança.

3



3. A solução

Nos dias seguintes, investigadores de segurança, agências governamentais de cibersegurança e o programador do sistema operativo divulgaram informações sobre o ataque e a vulnerabilidade. Também forneceram conselhos às empresas afetadas pelo incidente e medidas que todos os seus utilizadores deveriam tomar, mesmo que ainda não tenham sido afetados. O National Institute of Standards and Technology classificou a vulnerabilidade como Common Vulnerability and Exposure (CVE) com uma pontuação base de 10,0 devido à gravidade do potencial impacto e à possibilidade de exploração. Esta é a pontuação mais elevada do Common Vulnerability Scoring System (CVSS), atribuída apenas a incidentes “críticos”. Os relatórios também referiram que o ataque se propagou através de uma ferramenta integrada que procurou portas abertas vulneráveis e explorou a vulnerabilidade do sistema operativo em todas as correspondências positivas.

Esta foi uma vulnerabilidade de dia zero porque foi conhecida e explorada por piratas informáticos antes de o programador do sistema operativo ter conhecimento da vulnerabilidade e ter criado uma correção. O evento foi generalizado porque o ato único afetou entidades e indivíduos fora do grupo de impacto limitado da empresa Exemplo. O grupo de impacto limitado pode ter incluído os clientes individuais e empresariais da empresa Exemplo devido à sua utilização do sistema operativo afetado e de portas abertas. No entanto, os relatórios dos especialistas realçaram que várias outras entidades sem qualquer relação com a empresa Exemplo foram afetadas por esta exploração, excluindo assim estas partes do grupo de impacto limitado.

4

4. O resultado

As cláusulas de seguro de resposta a incidentes, custos de recuperação de dados e sistemas, bem como perdas por interrupção da atividade foram todas inicialmente acionadas em resposta ao incidente cibernético. As informações disponíveis em poucas horas mostravam que se tratava de um evento generalizado, pelo que o sinistro estava sujeito à secção da apólice aplicável a eventos generalizados. As perdas ao abrigo dos contractos de seguro para resposta a incidentes, custos de recuperação de dados e sistemas, bem como perdas por interrupção da atividade foram cobertas até aos limites disponíveis para eventos generalizados, após aplicação da franquia e do cosseguro aplicáveis.

Evento generalizado

- Interrupção mundial de uma solução de software comum

1

1. O evento

A empresa Exemplo tinha instalações no Reino Unido, em França e na Alemanha. As suas unidades de produção e venda dependiam de uma subscrição comum de uma solução de Planeamento de Recursos Empresariais (PRE) baseada na nuvem de um grande fornecedor de software. A solução de PRE permitia o processamento de encomendas, a gestão de stocks, a definição de prioridades de produção, a gestão logística e o processamento de salários.

Há duas semanas, a empresa Exemplo atualizou o seu sistema de PRE da versão 2.3.2 para a versão 3.0 depois de realizar um teste de penetração e de executar a nova versão num ambiente de teste para garantir a inexistência de problemas de desempenho resultantes da atualização.

Na semana passada, o sistema de PRE avariou, restringindo o acesso da empresa Exemplo. A empresa Exemplo contactou a equipa de apoio ao cliente do fornecedor de software e descobriu que vários clientes na Europa tinham sido afetados pela interrupção. A empresa Exemplo contactou também o Centro de Resposta a Incidentes Cibernéticos da Chubb para contratar um Gestor de Resposta a Incidentes e notificar a Chubb Claims do incidente. No espaço de duas horas, foi publicado um aviso no website do fornecedor de software a pedir desculpa pelos problemas. Informou que estava a investigar um comprometimento do sistema no seu ambiente de produção e recomendou a consulta regular à disponibilização de informações adicionais e conselhos de recuperação.

2

2. O problema

No dia seguinte, o fornecedor de software enviou um e-mail aos seus clientes com uma descrição do que deveriam verificar para saberem se tinham sido afetados pelo evento, bem como conselhos sobre o que fazer a seguir. O e-mail indicava o seguinte: “Se utilizou as versões 2.3 ou 3.0 do PRE nas últimas três semanas e está com problemas de acessibilidade, o problema foi causado por atividade maliciosa nos sistemas de produção do serviço na nuvem e as nossas tentativas de recuperação estão a decorrer.”

A indisponibilidade do sistema de PRE da empresa Exemplo durou cinco dias. Entretanto, passaram a receber encomendas manualmente por telefone e e-mail, a produção continuou parcialmente com uma capacidade significativamente reduzida e as entregas tiveram de ser interrompidas porque os dados das encomendas estavam inacessíveis. Quando o sistema ficou finalmente disponível, todos os dados históricos relativos às encomendas, ao inventário, ao estado da produção e às entregas tinham sido eliminados e não era possível recuperá-los. A última notificação do fornecedor de software, enviada por e-mail e publicada no seu website, confirmou que o malware destrutivo tinha corrompido os dados de produção dos clientes, bem como as cópias de segurança. A notificação detalhava também que o evento tinha afetado mais de 30 000 clientes de PRE na Europa e em partes da América do Norte.

3

3. A solução

Para determinar se as secções de cobertura de evento de impacto limitado ou de evento generalizado se aplicavam à apólice da empresa Exemplo, foi necessário avaliar quem foi afetado por este evento e o motivo de ter sido afetado. As declarações do fornecedor de software indicavam que 30 000 clientes, que utilizavam as versões de PRE na nuvem em causa, foram afetados devido a um código malicioso nos sistemas de produção do fornecedor. As outras empresas foram afetadas não devido à sua relação com a empresa Exemplo, mas sim devido à sua escolha do sistema de PRE. Teriam sido afetadas por este evento mesmo que a empresa Exemplo não fosse um cliente.

4

4. O resultado

A informação que indicava que este evento afetava clientes em toda a Europa foi enviada à empresa Exemplo duas horas após a interrupção, o que constituiu a primeira indicação de que este evento era generalizado. Por este motivo, os limites, a franquia e o cosseguro de eventos generalizados aplicavam-se aos montantes das perdas cobertas. Isto incluía a eventual perda por interrupção da atividade, custos de recuperação de dados e sistemas, como o custo de soluções manuais alternativas e esforços de recuperação de dados, custos para os Gestores de Resposta a Incidentes e o custo de contratação de outras entidades para gerir as relações públicas e comunicações com os clientes da empresa Exemplo que tinham de voltar a enviar as suas encomendas ou gerir envios atrasados.