Pela CT Leste de Governança e Riscos da Abrapp (*)

Não adianta chorar sobre o leite derramado!

Aposto que você já ouviu essa frase muitas vezes e em muitos contextos... Mas e então? Não há o que se fazer diante do leite derramado?

Essa frase visa nos levar à reflexão de que não adianta ficar apenas arrependido e frustrado por não ter evitado a ocorrência de um fato não desejado. Ela pretende nos levar à busca pela solução do problema e, claro, à identificação das oportunidades de melhorias para que o fato não ocorra novamente.

Sendo assim, se você não conseguiu evitar que o leite fosse derramado, chamemos o gato!

Durante a pandemia em curso houve um aumento massivo no número de ataques cibernéticos e em 2021 tivemos um dos maiores vazamentos de dados da história, dados de 223 milhões de brasileiros no sistema nacional de saúde, crime este ainda sob investigação.

Se você já implementou tudo que sugerimos até aqui, nessa série de posts, para se proteger de um ataque cibernético, certamente a probabilidade de um incidente desta natureza em sua empresa está muito reduzida e, ainda que ocorra, a chance de danos também está reduzida.

Mas é importante estar ciente de que, mesmo com todas as precauções, a possibilidade de ser alvo de um crime cibernético continua existindo. Ao mesmo tempo em que os desenvolvedores de sistemas de segurança digital e especialistas no combate aos ataques cibernéticos seguem avançando, os criminosos fazem o mesmo.

Invasão dos servidores, vazamento de dados, bloqueio ao acesso às informações, pedidos de “resgate” dos cibercriminosos... são muitas as formas como os hackers podem alvejar o nosso negócio. Nesse sentido, se a natureza dos ataques é determinante para definir a conduta, certas providências podem e devem ser tomadas em todas as situações.

Sendo assim, caso sua entidade sofra um desses ataques, há ações que podem ser feitas para minimizar os impactos da ação criminosa.

Portanto, se apesar de todas as ferramentas de mitigação desse risco, você se ver em um ciberataque, ao invés de se desesperar e pagar um resgate ou ceder à extorsão, saiba o que fazer:

1. Identifique os sinais do possível ataque e comunique a área de TI

Um dos indícios de alerta é o processamento lento de um ou mais computadores. Isso pode acontecer caso os hackers estejam utilizando os recursos das máquinas nos “bastidores”, enviando dados ou e-mails infectados para outro computador.

2. Notifique o incidente às autoridades

Como qualquer outra ação ilegal, o crime cibernético deve ser comunicado à polícia. A partir daí, pode-se empreender a correta investigação do caso. Para fundamentar o incidente, deve-se primeiro coletar evidências do ataque hacker no negócio, incluindo capturas de telas, e-mails, arquivos e outros materiais. Se possível, registre também o IP do criminoso. E claro: se houver vazamento de dados, comunique também à Agência Nacional de Proteção de Dados – ANPD.

3. Identifique as causas

É essencial descobrir qual foi a brecha de segurança, ou seja, como os hackers conseguiram

acessar e invadir a rede.

As principais causas de violação e vazamento de dados são: roubo ou perda de dispositivos, desatualização de softwares ou sistemas de TI, malware (softwares maliciosos), senhas fracas ou roubadas e uso de redes inseguras (incluindo o wi-fi público).

Nesse cenário, como mencionamos, é preciso contar com o apoio de um profissional especializado para a detecção da causa, caso a entidade não tenha essa expertise na equipe interna. Depois de determinado o "porquê", é preciso investigar outros aspectos, tais como quais dados foram roubados ou acessados, quais contas e computadores foram comprometidos e quem foi afetado.

4. Reduza os danos nos sistemas internos

Algumas medidas imediatas são importantes para iniciar a contenção de danos. Isso envolve desconectar o servidor e/ou computadores afetados do roteador ou rede empresarial. Caso a conexão seja via wireless, desabilite as funcionalidades de wi-fi no dispositivo em questão. Se o website da entidade foi alvo dos hackers, contate o serviço de hospedagem do portal o quanto antes.

Modificar as senhas dos serviços tende a evitar o agravamento do problema. Isso porque pode levar um tempo entre a notificação do ataque e a ação efetiva do hacker. Na hora da troca, invista em senhas fortes, que reúnam letras, números e caracteres especiais, além de totalizarem ao menos 8 dígitos. Vale a pena ressaltar que senhas fracas são uma causa comum de invasão. Adicionalmente à força dessas credenciais, nunca utilize a mesma senha para diversos serviços. Caso ocorra um vazamento, afinal, diversas soluções corporativas serão prejudicadas em cadeia.

5. Acione os equipamentos reserva

Após um ataque, caso um dispositivo da infraestrutura de TI tenha suas operações interrompidas, é primordial restabelecer os serviços com agilidade. O tempo de inatividade não acarreta somente perda de produtividade da equipe, mas também prejudica a experiência do cliente.

É preciso ter em mente, ainda, que a desinfecção e o restabelecimento dos equipamentos podem demandar horas, dias ou até mesmo semanas. Nesse sentido, é recomendado contar com reservas dos equipamentos mais críticos para os processos de trabalho.

6. Investigue os impactos na entidade e nos clientes

Como o ataque impactou sua empresa? Os dados de clientes estão envolvidos no incidente de segurança?

Aqui, além da análise dos desdobramentos da ação hacker, é preciso restaurar os sistemas e informações afetados. É aí que entra em cena a enorme importância de um bom backup, que permita recuperar dados íntegros e garantir a continuidade do negócio.

Outro ponto de atenção: se houver vazamento e exposição dos dados corporativos ou informações pessoais dos clientes, deve-se entender as implicações legais do evento.

Além das etapas de notificação policial que já abordamos acima, é necessário informar os clientes sobre o incidente, esclarecendo que todas as medidas cabíveis já estão em andamento.

7. Revisite sua cibersegurança e aprenda com os erros!

Por fim, e não menos importante, é crucial não deixar a experiência "passar em branco". Quando o assunto é a pergunta "ataque hacker: o que fazer?", a prevenção e os ajustes contínuos de segurança são elementos-chave para evitar que novos incidentes aconteçam.

Garanta que as soluções de proteção estejam funcionando da forma apropriada, assim como a execução periódica dos backups. Verifique se as atualizações de todos os sistemas estão em dia, além de revisar o plano de disaster recovery e as demais políticas de segurança da organização, cuja importância já mencionamos aqui nessa série de posts.

Identifique, ainda, se há necessidade de treinamento da equipe acerca das melhores práticas de cibersegurança.

Nesse cenário, muito mais do que remediar, a prevenção é a chave. A jornada não é fácil, mas nada se compara aos potenciais danos devastadores que as ciberameaças podem representar, afetando a reputação, a própria sobrevivência dos negócios e até mesmo as vidas dos indivíduos cujos registros pessoais podem ser impactados.

Portanto, se você seguir, em resumo, essas etapas, você não só terá a sua entidade mais protegida de um ataque cibernético, ou seja, menos vulnerável, como também conseguirá identificar mais rapidamente o ataque, caso o ocorra:

Verificação de Erros	Certificar que a verificação explícita de erros seja realizada para todos os softwares desenvolvidos internamente
Tratamento de Incidentes	Designar equipe de gerenciamento para dar suporte ao tratamento de incidentes e documentar procedimentos de resposta a incidentes
Resposta a Incidentes	Elaborar padrões que abranjam toda a organização para reporte de incidentes
Contatos para Reportes	Manter informações de contato para reportes de incidentes de segurança e publicar informações sobre reportes de anomalias e incidentes de computador
Scan de Vulnerabilidades	Utilizar ferramentas de scan de vulnerabilidades e testes de penetração (pentest) em conjunto
Classificação	Criar sistema de pontuação, classificação e priorização de incidentes

E lembre-se: aprender com o incidente é uma importante etapa do processo! Não perca, então, a nossa próxima edição do Saiba Como, que trará como tema processos robustos de gestão das aplicações e dispositivos.

Fontes:

- https://strati.com.br/blog/saiba-o-que-fazer-se-sua-empresa-for-vitima-de-ataque-cibernetico/
- https://digital.futurecom.com.br/transformao-digital/crime-ciberntico-o-que-fazer-no-caso-de-um-ataque-indstria
- https://www.microserviceit.com.br/ataque-hacker/

(*) Comissão Regional Leste de Governança e Riscos da Abrapp.

Fonte: Abrapp em Foco, em 23.03.2022.