RANSOMWARE

O que fazer DURANTE um ataque

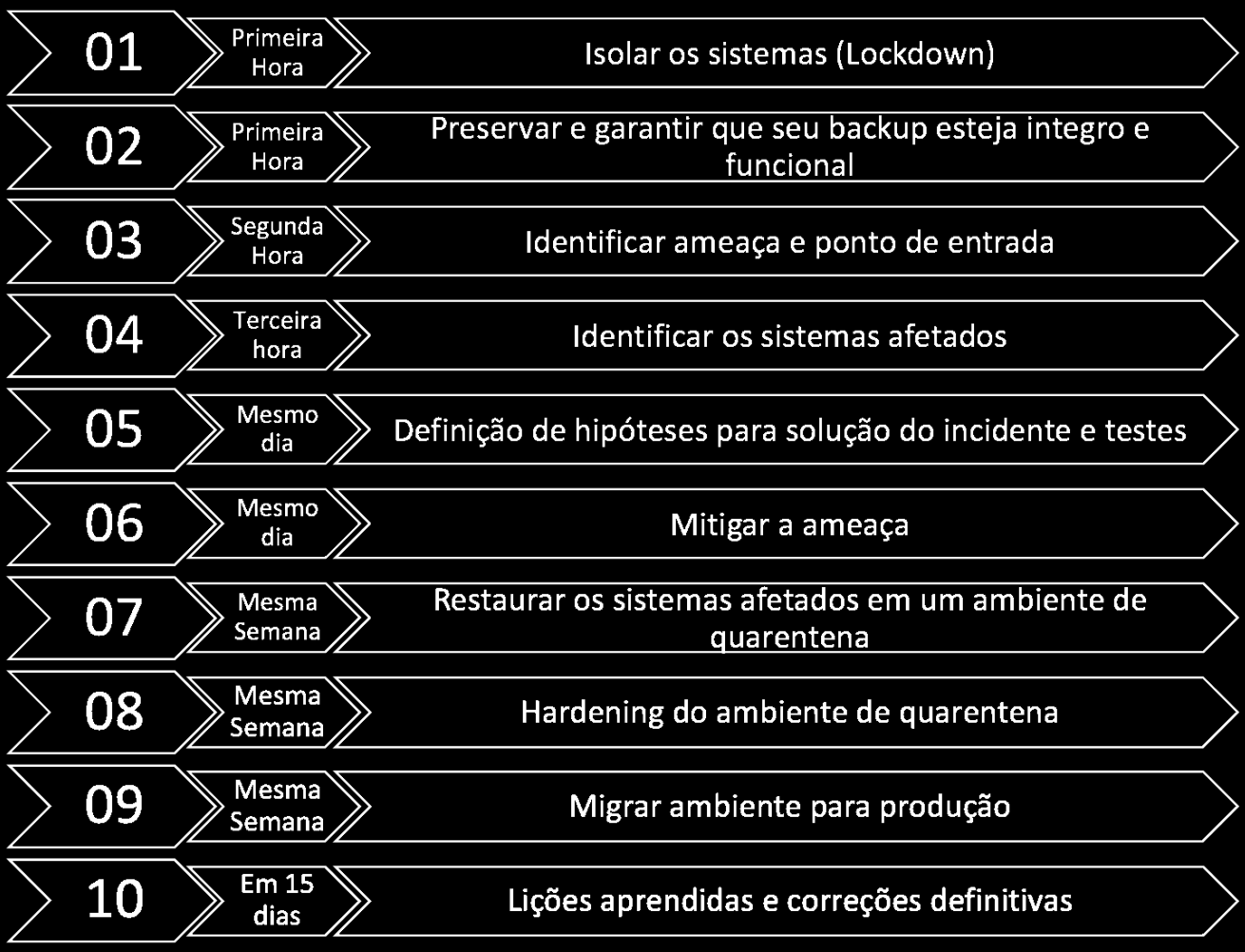
ESCRITO POR
LIERTE BOURGUIGNON

EXECUTIVE REPORT

Lierte Bourguignon – CSO da ISH Tecnologia

"Durante o ano de 2022 realizei diversas apresentações em grandes fóruns de Cyber Security no Brasil, compartilhando um pouco da minha experiência e do time de DFIR (Digital Forensics and Incident Response) do SOC da ISH Tecnologia. O tempo de apresentação é sempre muito curto, e não conseguimos nos aprofundar nos temas, e sempre encontramos uma plateia sedenta de mais informações e conhecimentos sobre resposta a incidente, desta forma o objetivo deste documento é se aprofundar nos temas em formato mais lúdico, prático e estratégico".

INTRODUÇÃO



Não é novidade que ataques de ransomware aumentaram muito em vários países, inclusive no Brasil. Só aqui, concentramos cerca de 55% dos casos de ransomware da América Latina. E isso mostra que a necessidade de segurança nas empresas está cada vez maior.

Já entendemos o que fazer antes de um incidente através do primeiro artigo "*Ransomware, o que fazer antes do ataque?*". Mas será que mesmo aplicando todos os conceitos, como a aplicação de uma arquitetura antifrágil, plano de Resposta a Incidentes e testes de defesa, ainda existe a possibilidade de sermos infectado por um malware?

Sim, é possível! Executar todas as medidas proativas diminui o risco. Entretanto, não podemos ter a sensação de que estamos 100% seguros. Apesar de não desejarmos o ataque, precisamos estar preparados para quando isso acontecer, por isso, é de suma importância, trabalharmos no tempo e na organização da resposta, minimizando o risco que seu ambiente sofrerá durante um ataque.

Conforme podemos observar no gráfico abaixo, o risco está diretamente associado ao tempo de resposta. Quanto mais rápido e efetivos formos, menor será o risco, vamos detectar e responder ao ataque ainda nas ações iniciais, onde o atacante está tentando aprender sobre a arquitetura dos nossos ambientes, agora se houver demora ou desorganização da resposta quem sabe o atacante já estará utilizando o nosso ambiente para atacar outras instituições (ultima fase do ataque), nesta altura seus dados já foram *exfiltrados*, suas defesas já foram desativadas, contas com alto privilegio de acesso já foram comprometidas.

Neste sentido, o objetivo deste e-book é compartilhar o que fazer durante um ataque, seguindo 10 passos que poderão ser feitos em 15 dias dentro do seu negócio.

1. ISOLAMENTO DOS SISTEMAS - *LOCKDOWN*

A palavra que mais ouvimos durante a pandemia do Covid-19 foi lockdown. A estratégia e analogia de ser uma medida preventiva obrigatória que consiste no bloqueio total e isolamento de sistemas, é a mesma aplicada na cibersegurança.

Quando há um ataque, o pontapé inicial na primeira hora é isolar os sistemas afetados. Neste ponto, gostaria de fazer um destaque bem importante: é bem traumático pensar que será necessário parar todo o ambiente em função de um ataque em curso. Mas, se você seguiu a estratégia de criar uma arquitetura segmentada por funções do seu ambiente, talvez não precise parar todo seu ambiente, e sim, isolar os sistemas afetados.

O que significa de fato essa ação de isolar? Seria desligar? Bloquear? Interromper? Vamos pensar em dois casos, para entendermos como seria essa ação:

Cenário 1 - Ambiente segmentado por funções: Teremos nesta arquitetura um ambiente separado para as principais aplicações da empresa, como rede dos usuários, redes de servidores de homologação, redes para servidores de produção, redes de BYOD, e, principalmente, uma rede separada para backup.

Cada serviço da empresa está em um ambiente diferente, e a interação entre eles controlada por um belo ecossistema de segurança, liberando apenas as portas e serviços que são necessárias para a comunicação e funcionamento entre eles.

Cenário 2 - Ambiente sem segmentação: Todas as aplicações críticas da organização ocupam o mesmo segmento que o ambiente de usuário. Neste cenário, não existe preocupação em isolar ou controlar o acesso ao ambiente de backup, ou quem sabe, até existir uma segmentação de redes internas. De qualquer ponto da rede é possível acessar, sem grandes esforços, as principais aplicações da organização.

Um dos primeiros passos do atacante após alcançar sucesso na invasão é aplicar técnicas avançadas de persistências para permanecer no ambiente, tentando se movimentar lateralmente nas diversas redes e aplicações.

O hacker encontrará bastante facilidade em ambientes sem segmentação ou controles internos. Logo, este ambiente será diretamente impactado. Como consequência, a ação de lockdown será traumática. Uma vez que entendermos que o atacante impactou todo o parque e pode estar em qualquer ponto da rede, o lockdown sugerido será para todo o parque da empresa. Porém, se o atacante afetou apenas uma parte do sistema e temos confiança que os demais segmentos estão íntegros, o isolamento pontual será apenas para o segmento afetado.

2. PRESERVAR E GARANTIR QUE O BACKUP ESTEJA ÍNTEGRO

Feito o lockdown total ou em partes do ambiente, o próximo passo ainda na primeira hora é garantir que o backup esteja íntegro e funcional.

É de conhecimento que a Segurança da Informação envolve três pilares básicos: Disponibilidade, Integridade e Confidencialidade. O objetivo final do atacante é tentar quebrar estes pilares.

Se o cibercriminoso obteve acesso aos dados, provavelmente ele fará uma exfiltração, ou seja, um vazamento, e este, é um fator impossível de resolver pós impacto. Todavia, ainda é possível recuperar os pilares de disponibilidade e integridade, e talvez o backup seja a única ferramenta capaz de realizar tal recuperação com sucesso. Uma vez realizado o *lockdown* imediatamente, precisamos garantir que o backup esteja isolado, íntegro e funcional e que de maneira alguma o atacante conseguirá alcançá-lo.

O papo sobre arquitetura, rotinas e modelos de backup é grande, e não é nosso objetivo através deste documento explorá-lo. Mas recomendo fortemente que sua organização mantenha um backup off-line. Por mais que esteja seguindo todas as boas práticas de backup, lembre-se que talvez esta seja a sua única alternativa para garantir que seu ambiente volte à normalidade. O exagero nunca é demais quando falamos de backup. Outro ponto, é que algumas famílias de Ransomware e demais malwares desenvolveram táticas e técnicas para encontrar onde está seu backup e criptografá-lo.

Neste processo de checagem de integridade do backup, é importante parar as rotinas de backup do seu ambiente.

“Imagina o cenário onde as rotinas estão funcionando e sobrescreve o seu backup com cópias dos servidores criptografados?”

Por isso, é necessário ser uma ação casada com o lockdown! Se você parou as rotinas de backup de um segmento do seu ambiente, ele precisa estar em isolamento, porque também não queremos que os usuários continuem a criar e/ou alterar dados sem que o

backup daquele segmento esteja sendo realizado. Lembre-se que o atacante tentará fazer movimentações laterais.

O atacante precisa de poder de negociação para te convencer a pagar bitcoins. A primeira forma que ele fará isso, é te prometendo devolver seus dados sequestrados. Se você tiver o backup íntegro e funcional, ele vai perder essa primeira ferramenta de negociação.

Um ponto importante aqui é que desaconselhamos o pagamento de resgates. Pois, não há garantia de que você receberá o acesso aos seus arquivos se pagar. Logo, isso apenas incentiva mais ataques desse tipo.

Na possibilidade do cibercriminoso não conseguir impactar seu backup, ele vai usar a segunda ferramenta que ele tem: a chantagem da divulgação dos seus dados! O backup não vai te livrar desta segunda ameaça, porém, apesar da gravidade, é importante não depositar, neste momento, a sua força de trabalho em tentar mitigar este problema. A estratégia é ganhar tempo para retornar o ambiente.

A dica é manter uma comunicação com o atacante de maneira amistosa, deixando a entender que em algum momento você pagará pelo resgate. Enquanto seu ambiente estiver off-line e isolado, você ainda é uma fonte que poderá ter ganhos financeiros.

3. IDENTIFICAR AS AMEAÇAS E O PONTO DE ENTRADA

Chegamos a segunda hora pós impacto. Aqui você será tentado a cometer um dos pecados capitais no processo de resposta a incidente: retornar o backup antes de identificar com qual situação e ameaça você está lidando.

Vamos pensar em um cenário. Você saiu cedo para trabalhar e deixou a porta da sua casa aberta e esqueceu de ligar o alarme da sua casa. O ladrão passa em frente e vê sua casa como alvo em potencial. Logo ele entra e nota que nada aconteceu. Rouba sua televisão e vai embora. Ao final do dia, você volta e percebe que foi roubado. O que você faz primeiro? Vai correndo para a loja comprar uma nova televisão ou fecha a porta e liga o alarme?

Bom, o ideal primeiramente é fechar a porta e ligar o alarme. A porta foi um ponto de entrada e o ladrão explorou a vulnerabilidade do alarme já que não estava ligado. Então por que sem saber de fato o que aconteceu, você já vai querer retornar o backup?

Já acompanhei várias Respostas a Incidentes, e posso garantir que, quase em 100% das vezes que o cliente que voltou o backup antes de identificar a ameaça, ele foi alvo mais uma vez e teve todo seu ambiente impactado.

Outro ponto a ser lembrado é que para retornar o ambiente, é preciso colocar o segmento de backup conectado ao ambiente de produção para realizar a restauração. Isso quer dizer que, além de ser uma possível tentativa errada de restauração, você ainda poderá estar colocando em risco seu ambiente de backup ao conectá-lo em um cenário ainda comprometido. É preciso manter a calma e não tentar acelerar o processo. É necessário seguir o plano de resposta a incidente estabelecido.

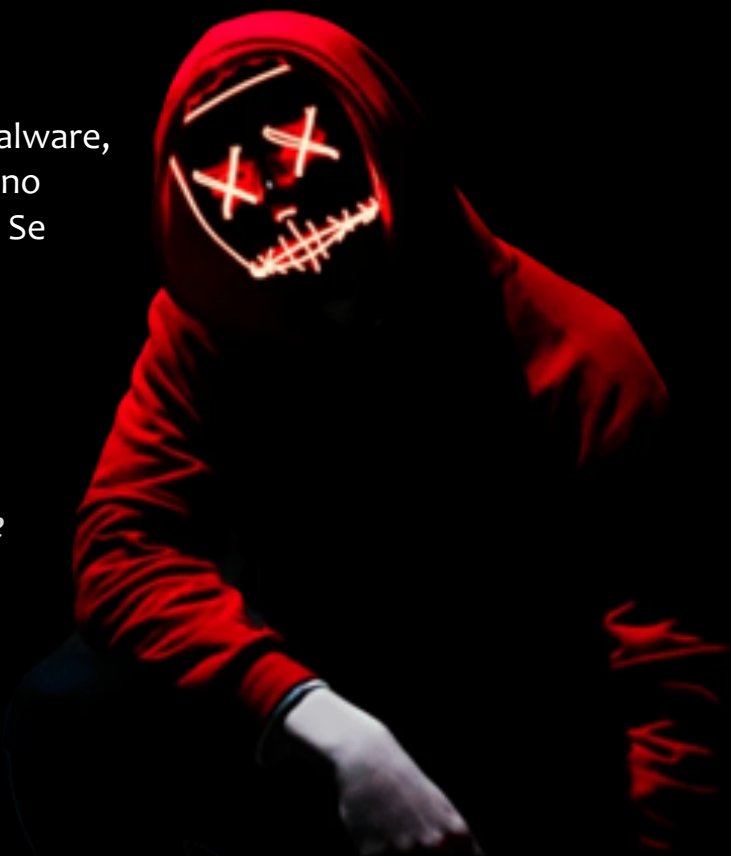
Vencida a vontade de tentar restaurar o backup, vamos para o passo correto: identificar com qual ameaça estamos lidando. Nesta fase, não desligue os servidores e máquinas afetadas! Aqui você deve estar pensando que essa ação conflita com a primeira recomendação deste artigo. Porém realizar lockdown não significa desligar os ambientes afetados, e sim isolar. Mas como não desligar?

Muitos quando se deparam com um ataque Ransonware, querem desligar tudo o mais rápido possível, com receio que o mal se alastre pelo ambiente. Fazendo isso, entretanto, você pode perder a possibilidade de conhecer o malware que está afetando seu ambiente.

Algumas ameaças cibernéticas mais avançadas, após executados no ambiente, aplicam rotinas de autodestruição dos executáveis. Em algumas ocasiões, o malware em si, abre a possibilidade de execução de comando remoto pelo atacante. Isso quer dizer que a única possibilidade de você descobrir o que afetou sua empresa é com análise de memória. Se você desligar os dispositivos afetados, perderá essa chance.

Lockdown não significa desligar todo seu ambiente, e sim isolar o problema! Isso pode ser através de criação de políticas de firewall que controla o segmento ou desconectando a placa de rede dos ativos afetados.

Além da análise de memória para identificar o malware, também é recomendado realizar uma varredura no ambiente, a fim de buscar possíveis executáveis. Se encontrado, o passo seguinte será realizar uma análise deste malware em alguma Sandbox para entender o comportamento do mesmo.



> *“Outra dica valiosa: nunca execute este malware fora da Sandbox.”*

E você deve pensar, “eu criei uma máquina virtual só para isso, e ela está totalmente isolada do ambiente”. Não é o recomendado! Alguns malwares possuem estratégia de movimentação lateral via hipervisor e poderá afetar toda sua farm. Além de ser extremamente custoso uma análise de malware de maneira artesanal, o mais rápido e efetivo é usar uma Sandbox.

Além de promover uma execução mais segura, a maioria já vai gerar um relatório de todo comportamento do executável, agilizando assim o seu trabalho. Lembre-se que quanto mais rápido for, menos impacto sua empresa terá.

Outros dois pontos devem ser observados. É a característica da mensagem com pedido de resgate que foi deixado pelo atacante. Foi um texto ou um papel de parede que foi alterado? Qual a cor e mensagem? Está em qual idioma?

Isso é importante para identificar o grupo hacker que está atacando seu ambiente. Isso acelera o entendimento. Em geral, cada um deles possuem um comportamento específico, e sua maioria repete as mesmas armas e estratégias durante os ataques.

O segundo ponto é a extensão dos arquivos pós serem criptografados. Isso também fala com o tipo de malware que está afetando sua empresa.

Se você seguiu os passos acima é bem provável que a esta altura você já sabe qual o comportamento do malware, e qual vulnerabilidade do seu ambiente ele explorou para conseguir sucesso. Antes de avançar para os próximos, é importante preservar a cadeia de custódia para uma futura forense. Não estamos preocupados, ainda, em realizar uma forense completa do ambiente. Queremos apenas entender com o que estamos lidando e seus comportamentos. No futuro, serão necessárias mais respostas e isso vai exigir uma forense completa.

A Cadeia de Custódia é uma prática antiga nas Ciências Forenses. Independente da área de atuação, todas as amostras são recebidas como evidências e analisadas. O seu resultado é apresentado na forma de laudo, objetivando dissertar um parecer sobre a evidência examinada.

As evidências devem ser manuseadas de forma cautelosa, e todo o manuseio na evidência deverá ser registrada na Cadeia de Custódia. Considerada um conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

4. IDENTIFICAR OS SISTEMAS AFETADOS

Chegamos então na terceira hora pós impacto.

A esta altura, já devemos saber com qual malware estamos lidando e por onde entrou. O próximo passo é entender a dimensão do estrago que ele causou.

Assim como no artigo anterior, *Ransomware, o que fazer antes do ataque*, ressalto aqui a importância de se ter um BIA (Business Impact Analysis). Ele será seu fio condutor para definir suas prioridades, e você usará a mesma estratégia para identificar os sistemas afetados que usou para construir um BIA. A primeira parte para se construir um BIA é identificar os processos essenciais para o negócio da sua organização para então construir um plano de recuperação. Use este mesmo método para descobrir os sistemas afetados.

> *"Eu quero descobrir os sistemas afetados, não os processos afetados, por que deveria seguir neste caminho?"*

A resposta é que as pessoas consomem os sistemas através de processos. São os processos da sua organização que determinam a prioridade de um sistema e seus dados. O fio condutor para identificar os sistemas afetados são os processos essenciais para o seu negócio que foram mapeados pelo BIA.

Comece dos mais importantes para os menos relevantes. É muito importante que quem participe desta validação seja os usuários de tais processos. Provavelmente, o usuário executa este processo quase que diariamente, então saberá te informar com velocidade se tem algo que não está funcionando como antes. Não se arrisque tentando testar o processo sozinho, já que alguma rotina ou procedimento poderá passar despercebido.

Uma vez identificados os sistemas afetados, vamos usar duas ferramentas do Lean Six Sigma para definir a ordem de atuação do time, Matriz GUT e Matriz Esforço vs Impacto. Essas duas ferramentas vão te ajudar a direcionar o time para investir o tempo em ações que irão obter o melhor resultado no menor tempo possível.

A Matriz GUT é uma ferramenta da qualidade que visa priorizar ações, ela possui três pilares principais que irá auxiliar na tomada de decisão: gravidade, urgência, tendência.

A ideia básica da matriz é que você atribua notas de 1 a 5 para cada pilar relacionando a cada problema encontrado (sistema afetado), e, posteriormente, multiplique o resultado de cada linha. Quanto maior resultado, mais atenção o problema merece. Veja na imagem abaixo:

Resumidamente, faremos uma adaptação da ferramenta para que a definição de gravidade e urgência não fique subjetiva, uma vez que se perguntarmos para os usuários ou donos dos sistemas afetados qual a urgência todos responderam que “precisa de ação imediata”. Resposta parecida, imagino, que também teremos para a gravidade, onde provavelmente todos responderão que é “extremamente grave”. Sendo assim, a adaptação passa por ter critérios tais definições.

Para definir a gravidade vamos usar o mesmo método que frameworks com ITIL usa para definir gravidade de um ticket de suporte. Quantos e quais usuários estão sendo afetados?

Vamos imaginar uma organização com 1000 usuários. Teríamos algo parecido com o que segue abaixo:

Gravidade	Quantidade de usuários afetados
Extremamente grave	100% dos usuários foram afetados
Muito Grave	Até 50% dos usuários foram afetados
Grave	Até 25% dos usuários foram afetados
Pouco Grave	Até 10% dos usuários foram afetados
Sem gravidade	Até 1% dos usuários foram afetados

Veja como isso é rico! imagina que você tem um CRM e um Serviço de diretório (Active Directory) totalmente impactados pelo ataque. No primeiro instante parece que a gravidade maior é do CRM, uma vez que se trata de um sistema de vendas da organização. Porém, em geral, a área de venda representa menos do que 10% dos funcionários. Logo, seria classificado como pouco grave. O serviço de diretório é utilizado por 100% da organização, então receberia classificação de extremamente grave.

Ponto de atenção: a maioria dos frameworks de serviço ressaltam a importância de tratar os usuários VIPs, C-Level por exemplo, com pesos de gravidade diferente dos demais. Minha sugestão é dar peso de 25% a cada VIP impactado.

Uma vez definida a gravidade utilizando o método acima, seguimos para a urgência, e aqui minha sugestão é que você busque esta informação do seu BIA, pois a urgência está relacionada ao negócio, o quanto de dinheiro que a empresa está perdendo ou deixando de ganhar com aquele sistema parado, em geral tais definições já estão presentes no seu BIA. Não canso de descrever e apontar a importância que um BIA tem para as organizações.

Por último não menos importante está a tendência. Essa etapa virá do parecer técnico dos engenheiros envolvidos no processo de resposta a incidente, pois estão relacionados a investigações iniciais do problema. Apenas eles saberão informar se em função do tempo aquele problema vai piorar ou não.

Terminando a matriz GUT com todos os sistemas afetados, chegou o momento de buscar onde vamos depositar energia para ter os melhores resultados. Neste momento, usamos a outra matriz conhecida como matriz de Esforço Vs Impacto. Ela é dividida em quatro quadrantes, sendo as atividades divididas entre eles de acordo com o tempo gasto em cada ação, e com o impacto que ela trará. A matriz possui ainda dois eixos principais: o eixo vertical e o horizontal.

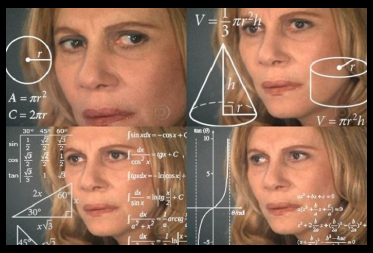
O impacto virá da GUT, e o nível de esforço para recuperação será uma definição pós avaliação técnica dos problemas enfrentados.

Quando chegar a hora de mitigar o incidente ou recuperar o ambiente, é necessário começar sempre da maior gravidade pelo menor esforço, conforme tabela demonstrada acima.

5. DEFINIÇÃO DE HIPÓTESES

Um dos desafios mais comuns enfrentados durante uma resposta a incidente ou qualquer tipo de resolução de problemas que precisamos encontrar uma solução muito rápida, é que sempre vamos usar o método de tentativa e erro.

Ou seja, várias tentativas são feitas para chegar a uma solução. Considero que não existe problema aplicar este método. O problema é que não aplicamos o método corretamente!



Observo que na maioria das Respostas a Incidentes, engenheiros tendem sob pressão repetir as mesmas ações que não deram certo. Para que o método possa dar certo, precisamos definir as hipóteses prováveis para mitigar a ameaça, que a esta altura você já a conhece (através da fase 3), conforme segue os passos abaixo:

a) Defina as possíveis hipóteses para mitigar a ameaça;
b) Toda hipótese deve ter um resultado esperado após ser aplicada;
c) Um plano de ação deve ser criado para aplicação da hipótese.

A indicação é consumir todas as informações geradas pela fase de identificação de ameaça (fase 3) e classificar a ameaça seguindo o framework MITRE.

MITRE ATT&CK foi criado em 2013, como uma ferramenta para descrever e categorizar os comportamentos dos adversários. O ATT&CK é uma lista estruturada de comportamentos conhecidos de invasores que foram compilados em táticas e técnicas, expressos em várias matrizes. Tal estratégia vai te ajudar a definir as hipóteses mais eficientes para mitigar o problema.

Por exemplo, se estiver lidando com ataques do tipo exfiltração de dados é bem provável que a criação de uma política no seu DLP (Data Loss Prevention) vai fazer parte da solução. Ao passo que se estivermos lidando com um ataque do tipo movimentação lateral a solução passará também pelo seu EDR (Endpoint Detection and Response).

Todas estas hipóteses servirão como insumo para a próxima fase, sendo a mitigação da ameaça. Para a mitigação ser assertiva precisamos entregar para a próxima fase, a solução correta. Por isso, é necessário realizar a prova de conceito das hipóteses que temos mapeadas.

Não é indicado sair aplicando em todo o ambiente as soluções (hipóteses) que acreditamos que resolverá o problema. Precisamos fazer a prova de conceito em parte do ambiente. Caso o resultado esperado for alcançado, essa hipótese deve ser considerada como possível solução e entregue como informação de entrada para a próxima fase.

6. MITIGAR A AMEAÇA

A missão nessa fase é garantir que o atacante não tenha mais controle do seu ambiente e que a ameaça não poderá gerar novos impactos.

É comum confundirmos e iniciarmos aqui fase de recuperação do ambiente. Portanto, devemos tomar bastante cuidado para não trocarmos as ações. Conforme já mencionei anteriormente, iniciar qualquer processo de recuperação no momento errado, pode gerar novos incidentes, incluindo o comprometimento do backup.

Abandonada a ideia de querer recuperar o ambiente neste momento, vamos iniciar a aplicação das hipóteses de solução recebida pela fase anterior, ainda que para cada hipótese tenha sido feito uma prova de conceito e um plano para aplicar no parque.

É bem importante que se a solução passar por aplicação que vai gerar uma grande alteração no seu parque isso seja feito em camadas, principalmente se a mitigação passar por alterações nos endpoints dos usuários. Costumo dizer que o efeito colateral do remédio não pode ser pior do que a doença do paciente. Por isso, tenha bastante cuidado em aplicar algo que pode gerar impacto ou indisponibilidade.

Aprimorar o monitoramento do seu ambiente também é importante! Se você estiver lidando com um incidente do tipo campanha, no qual o atacante desenvolveu um ataque em larga escala e indefere qual empresa será impactada, é bem provável que após a mitigação ser realizada ele vai desistir da organização.

Porém, se você estiver lidando com um hackerativismo ou um ataque patrocinado para impactar sua empresa, o atacante não vai parar, pelo contrário, quando ele perceber que sua primeira estratégia de ataque não foi eficiente ele vai mudar a estratégia de ataque.

Recomendo fortemente que neste período o time de hunt esteja 100% focado em monitorar todos os eventos do SIEM, e criando novos casos de uso para as possíveis ameaças que forem encontrando. Não avance para a fase de recuperação sem que tenha total certeza que o ataque parou e todas as frentes de mitigação funcionaram.

Nesta fase você também receberá informações de que existe uma tecnologia milagrosa que irá resolver o problema. Volto a enfatizar que para a resposta a incidente para inserir uma nova tecnologia no parque, na maioria das vezes gera mais problemas do que soluções, pois os ambientes ficaram complexos suficientes para não ser possível da noite para o dia inserir algo novo.

Outro fator relevante, é que para implantar uma nova tecnologia seu time vai precisar parar para apoiar o processo de implantação. Fazendo isso, você pausa o processo de

resposta a incidente para o implantar uma nova tecnologia que provavelmente vai mudar sua arquitetura. Neste caso, o melhor é você usar o que já tem no seu ecossistema. Levamos um ponto:

“Mas, se fui invadido é bem provável que não tenho a tecnologia que resolveria meu problema...”

A maioria dos ataques estão mais relacionados a políticas, práticas e postura de segurança, como por exemplo, uma aplicação de um patch de segurança que não havia sido feito, do que a ausência da tecnologia A, B, C ou D.

É bem comum durante um processo de resposta a incidente buscar novas empresas e profissionais. Reforços e mais cabeças pensantes são bons, porém estes novos integrantes ajudam bastante nas fases iniciais do processo de resposta a incidente, a qual é exigido pouco conhecimento do parque e mais conhecimento sobre a ameaça.

Quanto mais avançamos para o final do plano, menos eficiente eles vão se tornando. Novos profissionais vão precisar de conhecimento sobre seu parque, arquitetura, acesso as ferramentas, o que é relevante para seu negócio. Por isso, será necessário parar para repassar todo este conhecimento, e criar os devidos acessos ao ambiente destes novos integrantes.

É preciso ter em mente que o tempo é crucial! O melhor modelo é que estes profissionais ou empresas já tenham conhecimento do seu ambiente antes do ataque. Se isso não for possível, combine força para chegar ao resultado mais rápido.

Por exemplo, se você já tem um time operando seu ambiente de segurança (MSS) e tem um time trabalhando para responder ao ataque (CSIRT), o CSIRT deve identificar a ameaça e informar ao time de MSS como mitigar a ameaça, que, por sua vez, vai aplicar a solução ao parque.

Agora imagine se você ignorar o time de MSS que já estava atuando e passar toda responsabilidade da resposta para o CISRT. Eles ficarão horas tentando buscar respostas para perguntas que mencionava a pouco.

7. RECUPERANDO O AMBIENTE

Neste tópico iremos abordar os itens 7 (Restaurando os sistemas afetados), 8 (Hardening do ambiente em quarentena) e 9 (Migrar o ambiente para produção), pois todas as ações estão diretamente relacionadas.

Mitigada a ameaça com a certeza de que o atacante não tem mais controle do nosso ambiente, podemos sim considerar em restaurar o ambiente impactado. Mas por onde começar? O que devo restaurar primeiro?

Espero que você tenha feito um bom trabalho nas fases anteriores principalmente no tópico - Identificando os sistemas afetados. Essa fase gera a entrada para o início da recuperação do ambiente. Após o extenso trabalho de identificar os sistemas afetados e as prioridades de retorno mediante a importância e esforço aplicado para obter resultados rápidos, o próximo passo é obter o resultado da fase de identificação e segui-lo como uma rota de GPS para recuperação do ambiente.

Assumindo que estamos utilizando o produto da fase de identificação, precisamos lidar com as expectativas. O atacante para ter encontrado sucesso provavelmente explorou um vetor e uma vulnerabilidade no seu ambiente.

Qual a probabilidade dessa vulnerabilidade também estar presente no backup dos servidores e/ou demais ativados? Diria que 100%.

Em geral, ransomwares exploram vulnerabilidades de sistemas operacionais. Vamos imaginar o seguinte cenário: por algum motivo a determinada vulnerabilidade está presente no seu parque a meses.
O backup destes ativos também está vulnerável.

Se retornarmos para o ambiente no mesmo formato, o atacante novamente terá o vetor disponível para um novo ataque. Neste caso, precisamos criar um ambiente antifrágil. Isso quer dizer que você não deve voltar o seu ambiente ao mesmo estado de antes, isso seria resiliência, e não queremos isso.

“Qual seria o caminho mais apropriado?”

Precisamos criar uma zona de quarentena totalmente apartada e isolada do ambiente de produção. O backup destes ativos deve ser restaurado nesta zona, e então, faremos um hardening nestes ativos antes deles irem para produção.

Em geral processos de hardening levam bastante tempo. Neste momento não é apropriado tentar encontrar e corrigir todas as vulnerabilidades presentes no ativo, o que queremos é corrigir principalmente a vulnerabilidade recém explorada pelo atacante e as classificadas como críticas.

Terminando o hardening no ambiente de quarentena, podemos movimentar os ativos para o ambiente de produção e iniciar a cadeia de testes afim de validar se o ambiente está funcionando como esperado. Vale lembrar que os responsáveis por realizar os determinados testes são os usuários dos sistemas.

8. LIÇÕES APRENDIDAS E CORREÇÕES EM DEFINITIVO

Essa é uma fase que também considero bastante relevante dentro do processo. O objetivo é entender o porquê o atacante conseguiu encontrar sucesso e definir um plano para aplicar as devidas correções no ambiente para que isso não ocorra novamente.

As respostas das lições aprendidas e correções virão da forense. Não é objetivo deste documento explorar todo o processo de forense, mesmo porque, na maioria das vezes, o board da organização contrata uma auditoria independente para realizar tal análise, orientados pelo eventual conflito de interesse que possa ter com o time de resposta a incidente realizar este tipo de trabalho.

Entretanto, gostaria aqui destacar que no tópico 3, do tema Identificar as ameaças e o ponto de entrada, ressaltei a importância de preservar a cadeia de custódia e a coleta das evidências. Ou seja, os primeiros passos da análise forense começaram no início da resposta a incidente. Se não conseguimos preservar essas ações, não seria possível dar andamento na análise forense e, por consequência, ficaremos no campo da hipótese do porquê fomos invadidos.

A conclusão da análise forense gera um extenso relatório, com muitos detalhes, mas que sua espinha dorsal será como qualquer análise de problema: quais foram os problemas encontrados, qual causa e diagnóstico, e por fim, as soluções.

Minha orientação aqui é sobre a comunicação destas informações. É preciso adaptar a linguagem para cada público que vai recebê-la, principalmente o board que em geral não tem conhecimento de bits e bytes. Essa será uma excelente oportunidade para aprovar os investimentos. O board neste momento sabe o real impacto de um ataque e o ROI preterido para o determinado investimento.

Em alguns tópicos deste documento pontuamos o quão perigoso pode ser durante a resposta a incidente inserir novas tecnologias no parque, porém o que menos queremos no pós incidente é que nossa arquitetura e ambiente fiquem como estavam.

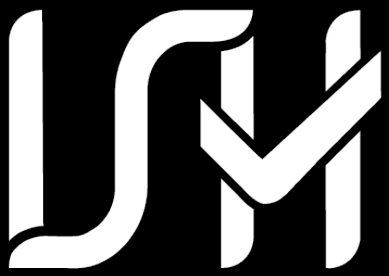
Precisamos aprender com as falhas e evoluir nossos ambientes. Depois de toda a análise, o recomendado é estudar e implantar novas tecnologias, entendendo como elas poderiam ter evitado o ataque ou contribuído para uma resposta a incidente mais eficiente.

Outro passo importante é avaliar quais serviços previamente poderiam ser contratados, um MSSP (Managed Security Services Providers) que poderiam também ter contribuído para monitorar, responder e detectar o ataque.

Para corrigir, não podemos receber o relatório do forense a qual terá inúmeras sugestões de evolução do ambiente e engavetar tais ações. Elas precisam virar projetos estratégicos de toda área de Segurança da Informação da companhia para que o mesmo problema não volte acontecer.

Cuidado ao criar um sentimento no patrocinador de que aplicando tais soluções nunca mais será invadido. Incluindo tais investimentos e ações a frequência com que os incidentes ocorrem serão bem menores, e se algo acontecer, a resposta será mais rápida, o que significa dizer que o impacto para a marca será menor.

O importante durante o incidente, é saber como se recuperar e ser capaz de restaurar com segurança os seus dados quando o malware tiver sido completamente removido do seu sistema.



www.ish.com.br