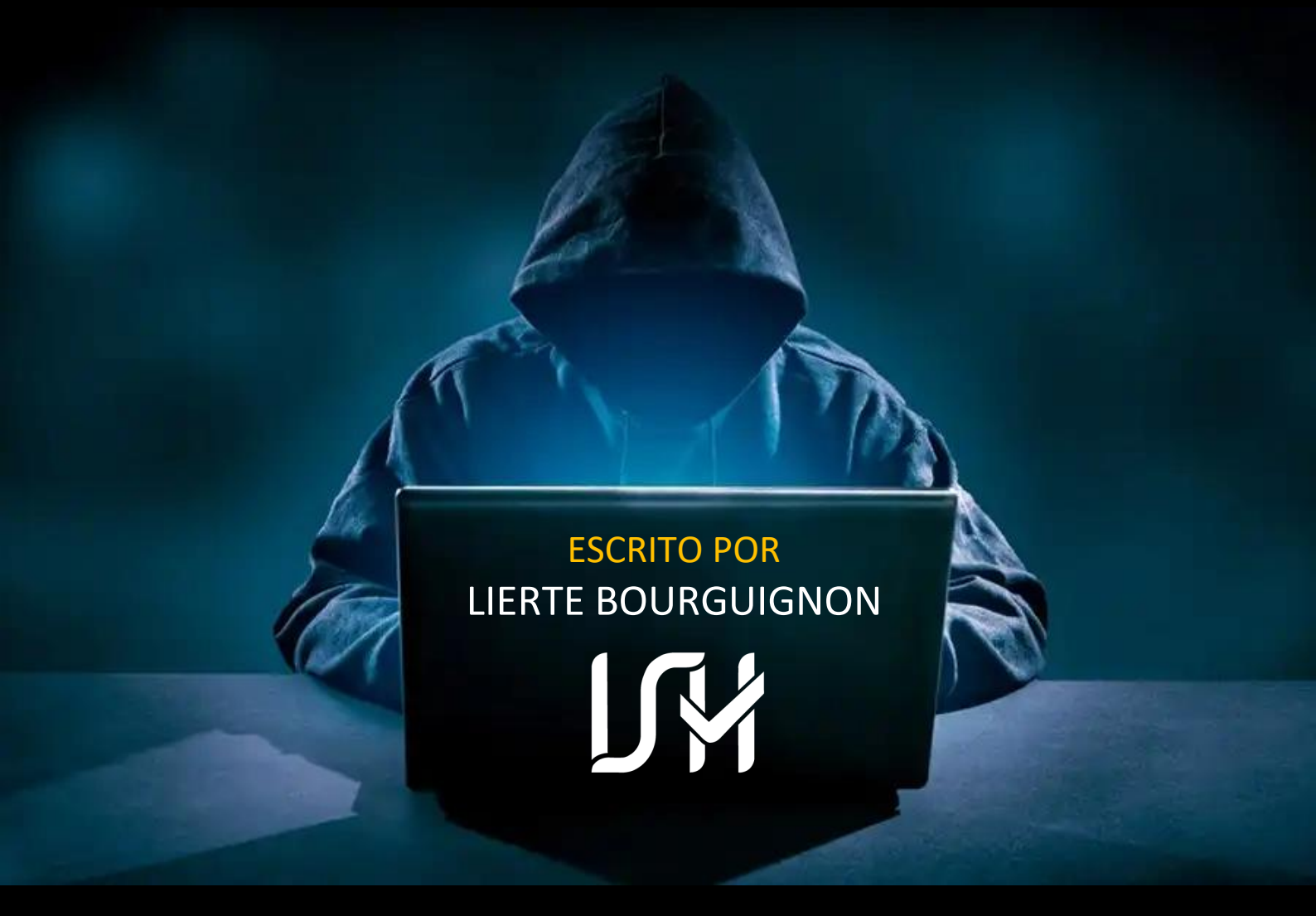
RANSOMWARE

O que fazer ANTES de um ataque



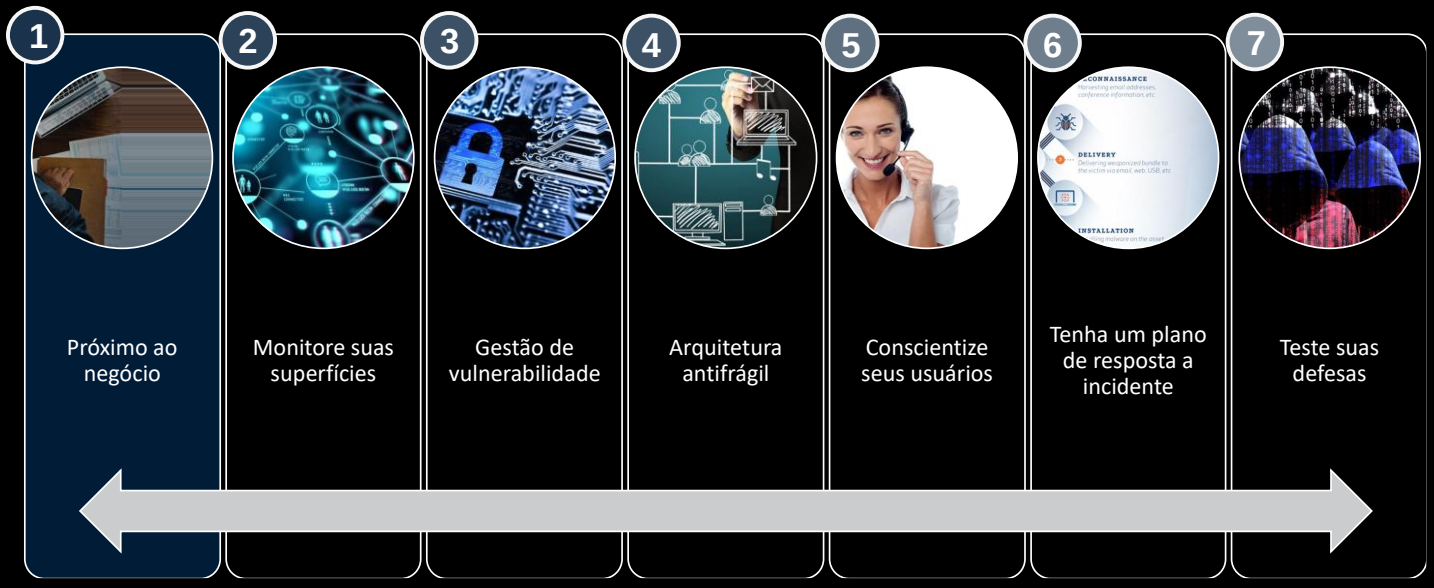
ESCRITO POR
LIERTE BOURGUIGNON

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



“Temos a tendência de não querer pensar em situações catastrófica.

Fazemos sempre um grande esforço para acreditar que isso nunca acontecerá conosco.”

Ransomware, uma palavra que faz nossos joelhos tremerem. A palavra que dá aquele nó no estômago só de pensar em acordar e ter a notícia que nosso ambiente foi totalmente criptografado; que os usuários não conseguem enviar e-mail; e até mesmo, que os clientes não conseguem acessar os principais canais de consumo ou comunicação da organização.

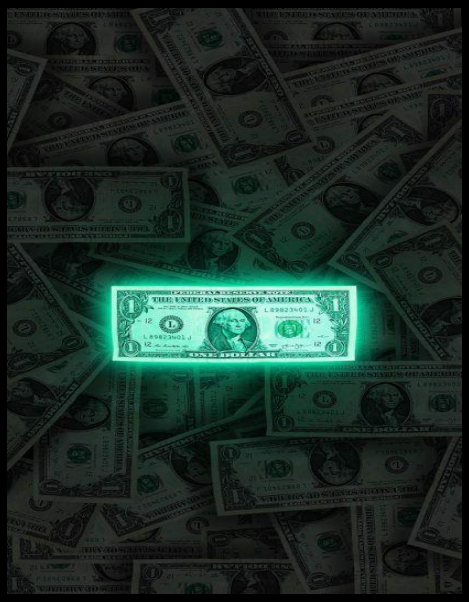
Imagine ver todas as telas da empresa, com uma mensagem amistosa do hacker pedindo **coins* para devolver seus dados.

Temos a tendência de não querer pensar em situações catastróficas como esta, e fazemos sempre um grande esforço para acreditar que isso nunca acontecerá conosco.

Vejo que é um trabalho psicológico e desejo de que nunca isso aconteça. Alguns mais supersticiosos batem até na madeira em pensar em eventos catastróficos. Porém, o melhor caminho é sempre nos perguntar: *“o por que não aconteceria comigo?”*. Sorte ou preparo? A melhor escolha é sempre desejar o melhor, mas, estar preparado para o pior.

Pensando nisso, quero compartilhar neste artigo 7 ações que podemos realizar para diminuir as probabilidades de um incidente com ransomware na sua organização.

1. PROXIMIDADE COM O NEGÓCIO



A proximidade com o negócio é uma das principais ações a serem tomadas. Em geral, o departamento de segurança das empresas quer distância dessa área, por eles, muitas vezes, não conhecerem técnicamente os problemas que estamos apresentando no dia a dia.

Entretanto, é justamente essa área que comanda a autorização de interrupção de uma aplicação para correção de uma vulnerabilidade, e que aprova uma janela para implantação de uma solução de segurança.

O grande "X" da questão é a comunicação. Temos a tendência de querer falar de *bits e bytes*, de forma técnica. Neste sentido, precisamos nos comunicar no idioma da área de negócio e na missão deste time, que se resume em obter mais clientes e lucros para as organizações.

Imagine que você identifique uma vulnerabilidade crítica no principal sistema de obtenção de receita da organização, e que será necessário um bloqueio temporário nesta aplicação para correção do problema. Dito isso, será preciso a autorização da área de negócio. Qual comunicação funcionaria melhor?

Opção 1: *"Olá! seu sistema está com uma vulnerabilidade de SQL Injection, classificada pelo MITRE como TTP de exfiltração de dados, com código CVE 1234. Isso é bastante crítico, precisamos corrigir o mais rápido possível, e para isso precisamos parar o sistema."*

Opção 2: *"Olá! encontramos uma vulnerabilidade no nosso principal sistema. Através desta vulnerabilidade, um hacker pode invadir nosso ambiente e provocar uma parada de 3 a 4 semanas, gerando perdas financeiras na ordem de 1M dólares. Para que isso não aconteça, precisamos parar a aplicação por poucas horas, mas vamos te dar o privilégio de escolher o momento, que certamente será um investimento para nós.".*

A opção dois soaria muito melhor, já que na primeira opção, a área de negócio escutaria apenas duas palavras *"parar o sistema"*.

É importante esclarecer qual seria o prejuízo para a empresa, tanto financeiro, quanto em imagem e reputação, no relacionamento com os clientes e com o mercado.

2. MONITORE SUAS SUPERFÍCIES

Todo produto a ser criado sempre nasce para resolver algum problema de maneira rápida e fácil. Nada pode ser demorado ou lento, já que o mundo em que vivemos muda a todo instante, principalmente com as transformações tecnológicas.

A maioria das soluções consumidas hoje são facilmente instaladas e usadas de maneira muito simples, seja um usuário final ou um usuário mais avançado como um desenvolvedor. O problema é que a segurança desse produto, muitas vezes, não combina muito bem com agilidade.

Um exemplo: se retirar a fechadura da porta da sua casa, você poderá entrar de forma mais rápida. Consequentemente, estará inseguro e suscetível a uma invasão ou roubo, já que qualquer pessoa tem acesso, uma vez que você não tem o equipamento de segurança. Isso traz mais vulnerabilidade para o seu ambiente.

Mas o que esse exemplo tem a ver com superfície de ataque?

“Diariamente, nossos usuários estão pesquisando inúmeras formas de deixar sua rotina mais ágil. Desde uma simples instalação de um aplicativo que vai salvar suas anotações na nuvem, até um desenvolvedor avançado que está usando um *github*, e compartilha o código do principal sistema da empresa com toda a internet. Desta forma, vão surgindo inúmeras superfícies no seu ambiente, a qual o atacante malicioso pode usar como vetor para invasões criminosas.”

Recentemente acompanhei um caso interessante. A empresa investiu em larga escala para proteger seu serviço de diretório, com PAM, IAM e outras tecnologias para monitorar seus acessos. Porém, o time de desenvolvimento criou uma aplicação na AWS que tinha acesso privilegiado ao serviço de diretório. Certa vez, o desenvolvedor resolveu usar o *github* para evoluir com seu código fora do escritório. O resultado? Um cibercriminoso obteve acesso ao código, e através da aplicação conseguiu acesso a todos os usuários presentes no serviço de diretório. Nesta hora, o patrocinador do projeto vai perguntar:

“*Por que o investimento não funcionou? Por que fomos invadidos?*”

A resposta é simples: **uma nova superfície de ataque** nasceu e ninguém sabia que ela existia. Não sabendo, nada foi feito para protegê-la. Você não pode proteger o que não pode encontrar no sistema.

Em geral, nos acostumamos a pensar em empresas como castelos, onde teríamos o domínio de todas as nossas superfícies (endpoint, aplicações, network etc.), dando a sensação de que subimos muros para proteção. Acontece que empresas não são mais castelos. Os usuários pularam os muros e estão trabalhando fora desse ambiente. E agora? *"Se eu não consigo encontrar estas superfícies como vou protegê-las?"*.

De fato, é uma tarefa bastante árdua, já que os principais incidentes que pude acompanhar nos últimos meses, vem de superfícies não monitoradas. Por isso, segue os três caminhos possíveis para evitar um ataque.

Processo: Secure by design
Significa pensar em segurança desde o escopo de desenvolvimento de um novo software, prevendo toda possibilidade de riscos aos quais aquela aplicação pode estar sujeita. Leia mais sobre Secure Software Development Lifecycle (S-SDLC).

Ferramenta: Cyber Asset Attack Surface Management (CAASM)
É uma tecnologia emergente que dá capacidade as equipes de segurança para resolver os desafios de visibilidade e vulnerabilidade de ativos de segurança cibernética (Gartner).

Essa tecnologia permite que suas equipes monitorem todas as suas principais soluções e dados existentes, em uma visão unificada de todo o seu universo de ativos cibernéticos.

Ferramenta: External Attack Surface Management (EASM)
São soluções focadas em descobrir e documentar ativos externos que podem ser possíveis pontos de violação na rede de uma organização.

O EASM ajuda a obter mais visibilidade dos aplicativos, serviços em nuvem e sistemas que são visíveis no domínio público – que, portanto, também podem ser visíveis para um invasor. A partir daí, as equipes de segurança podem reduzir configurações incorretas, melhorar a configuração de seus sistemas e reduzir a exposição.

3. GESTÃO DE VULNERABILIDADES

A Gestão de Vulnerabilidades talvez seja um dos processos mais antigos no universo de serviços de cibersegurança. No passado, eram feitas análises com imensos relatórios que eram impressos e armazenados na gaveta do CISO. Ao longo do tempo, notamos que isso não funcionava, pois não dependia do CISO a correção daquelas vulnerabilidades.

Desta forma, notamos a importância de saber para quem a área de segurança escalou a solução daquelas correções, o tempo de vida daquela vulnerabilidade, quais aplicações estavam vulneráveis, englobando assim, todos os conceitos de um processo de gerenciamento. Pensando nisso, é que surgiram os novos processos e tecnologias para realizar esse processo.

Acompanhar e trabalhar em um provedor de serviço de segurança me dá o benefício de ter visibilidade e acompanhar várias empresas. O que observo no dia a dia é a dificuldade de as organizações conseguirem corrigir suas vulnerabilidades e, ao mesmo tempo, ter indicadores saudáveis. Em geral, as vulnerabilidades nas companhias só crescem, e a pergunta que surge e nos intriga sempre é:

> *“Por que alguém não corrige isso? Essa vulnerabilidade oferece risco ao negócio e ninguém está vendo!”*

A pergunta gera a resposta: risco e negócio. Essas duas palavras, muitas vezes, são ignoradas das plataformas de gerenciamento de vulnerabilidade. Em geral, estas plataformas não geram risco, e sim, geram severidade da vulnerabilidade, que sempre possuem apenas uma definição técnica.

Por exemplo, a vulnerabilidade com o código CVE-2017-0143 a qual está associada ao *ransomware* mais famoso da história, Wannacry. Ela vai receber a mesma classificação de severidade quando encontrada na máquina da recepcionista ou quando for encontrada no servidor de SAP da organização, porque estas principais plataformas de SAST e DAST, não olham o fator risco ao negócio.

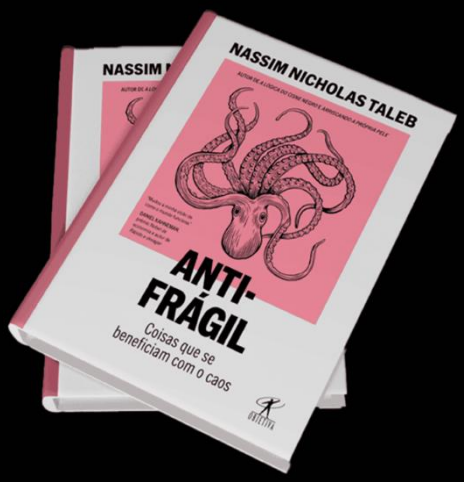
Para resolver esta questão, precisamos associar o gerenciamento de vulnerabilidade a um novo conceito que surge chamado: *Integrated Risk Management (IRM)*. Como o próprio nome do conceito sugere, a ideia é integrar e correlacionar todos os riscos de uma empresa em um único ponto. Desta forma, os riscos relacionados a *Cyber Security* da organização passam a fazer parte deste gerenciamento.

Aplicando esse movimento, é possível mudar a forma com lidamos com as vulnerabilidades da organização. Primeiramente vamos passar a ter contexto de negócio, ou seja, esses incidentes não mais recebem apenas o carimbo de severidade técnica, mas também passam a receber o termo de risco para o negócio. Neste caminho, a vulnerabilidade da máquina da recepção pode até ser a mesma do servidor de SAP, porém, o fator risco será totalmente diferente.

O segundo ponto é que geralmente inciativas de IRM são de responsabilidade da governança das corporações. Eles estão conectados diretamente ao conselho administrativo ou presidência, ganhando assim, um fórum estratégico e de autoridade que certamente estará mais sensível para resolver o quanto antes um possível problema que oferece risco ao negócio.

Mas atenção! Este movimento só vai funcionar se houver combinação com o primeiro item. O board vai ter pouco interesse em falar sobre bit e bytes. É preciso lembrar de apresentar os riscos considerando a forma como eles pensam: sem termos muito técnicos e visando a segurança da empresa.

4. ARQUITETURA ANTIFRÁGIL



Nassim Nicholas Taleb um libanês matemático e analista de risco criou o conceito de ser antifrágil. Uma leitura que recomendo (Antifrágil: coisas que se beneficiam com o caos). O antifrágil está além do resiliente e do robusto. Estes resistem a choques e permanecem os mesmos. O antifrágil, por sua vez, se torna cada vez melhor. Além disso, ele é imune a erros de previsão e está protegido de eventos adversos.

Extremamente ambicioso e multidisciplinar, antifrágil é sobre como se comportar, e prosperar, em um mundo cheio de imprevistos. Erudita e espirituosa, a mensagem de Taleb é revolucionária: o que não é antifrágil certamente sucumbirá.

“Mas o que isso tem a ver com cibersegurança?”

Tudo! Veja abaixo os três problemas que sempre vamos encontrar em arquiteturas de defesa:

a) **“Adoramos o que fazemos e temos inclinação sempre a sermos entusiastas por um fabricante A ou B que mais gostamos.”.**

Neste caminho criamos arquiteturas que nem sempre foram criadas pensando no ataque (*TTP - Tactics, Techniques, and Procedures*), mas sim no desenho sugerido pelo fabricante. Em alguns momentos, pode resolver parte do problema. Mas é preciso ficar atento. A cada dia, os ataques se tornam cada vez mais específicos, complexos e inteligentes.

Onde está o “pote de mel” da minha organização? Onde estão os dados mais importantes que o atacante tentará capturá-lo? Que técnicas e táticas o atacante usará para alcançar este pote? Com isso em mãos, é possível pensar em uma arquitetura mais robusta e eficaz.

É preciso alinhar pela ótica de defesa dos dados da sua organização. Não existe arquitetura de segurança sem as tecnologias dos fabricantes, mas é preciso ser crítico e construir pensando em solucionar problemas específicos do seu negócio.

b) **Costumo dizer que um incidente de segurança é como sangue no mar. Uma simples gota, atrai tubarões de todos os lados.**

Se você já passou por um incidente grave de segurança vai lembrar que recebeu inúmeras ligações para te dizerem que encontraram a solução para seu problema. "É só colocar para funcionar do dia para noite a tecnologia X que o ataque vai parar". neste caminho, paramos para implantar tal tecnologia no ambiente na expectativa de que o problema será resolvido, e o que na maioria das vezes acontece? *Shazam*, criamos mais problemas do que soluções. Em geral os ambientes das organizações são complexos o suficiente para não ser possível algo do dia para noite entrar em produção sem gerar um grande impacto.

Outro fator é que organizações vão ter 4, ou talvez 5 profissionais focados em segurança. Na hora de um ataque, estes profissionais estarão 100% focados em responder ao incidente. Acontece que, quando há a necessidade de instalar uma nova tecnologia no ambiente, mesmo com a intenção de que ela resolva o incidente, o foco deixa de ser a resposta para implantar uma nova solução.

Sugestão: tente primeiro defender com o que você já tem instalado no parque. Na maioria das vezes, isso é possível de ser feito. Nesta hora você pensa "se existe algo instalado no meu ambiente que poderia ter bloqueado o ataque, por que o hacker encontrou sucesso?". As causas de incidente têm mais a ver com visibilidade, monitoramento e detecção do que com tecnologia.

A segunda pergunta seria "se o ataque ainda estiver em curso, e eu não tenho nada para monitorar as movimentações laterais, não seria necessário instalar algo para entender o que está acontecendo?". Eu diria que sim, porém, soluções de monitoramento e detecção como um SIEM, em geral, não provocam mudanças de arquitetura no seu ambiente.

Existem exceções onde tecnologias resolvem problemas. Inclusive, já participei de respostas a incidentes onde tínhamos a certeza, de que o EDR resolveria o problema. Mas sempre se pergunte: Tenho evidências claras que a tecnologia resolve meu problema? Tenho gente com conhecimento e tempo suficiente para colocar em produção? A implantação gera menos impacto do que o incidente?
Se a resposta for sim para todas as questões, aposte na ideia.

c) **O pós incidente é o passo mais importante das grandes fases de resposta.**

Nessa linha, precisamos ter respostas para perguntas como: O que aconteceu? Por quê? Qual a solução para que não aconteça mais?

Em geral, geramos extensos relatórios com análises *forenses*, muitas apresentações para vários públicos sobre o ocorrido, já outros, procuram culpados. Porém, a pergunta que ninguém consegue responder é: quando começar a aplicar as lições aprendidas?

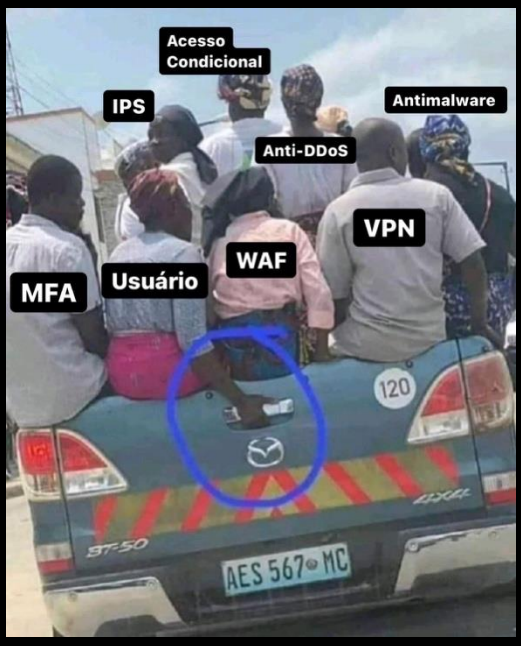
E aqui reside o problema. A recuperação do ambiente tem por objetivo retornar para o status idêntico ao dia anterior ao ataque. Esse processo se chama resiliência, quando retorna a forma original, após terem sido submetidos a uma deformação. Mas, é provável que este ambiente, se for atacado utilizando as mesmas técnicas e táticas, seja novamente comprometido.

Este não é o melhor caminho, é o pior deles. E por que isso acontece? Porque envolve novos investimentos, gerando novos custos à organização. Neste momento, a área de negócio da empresa está sensível a ser seu principal parceiro para aprovar todos os projetos possíveis com o foco em defender seu ambiente, já que eles possuem a dimensão do impacto e prejuízo que tal incidente gerou.

É hora de calcular um ROI dos investimentos necessários para que este problema não aconteça novamente. A resposta do incidente só termina quando o ambiente se tornar antifrágil, ou seja, se beneficie com o caos e se torne mais robusto e eficiente.

5. CONSCIENTIZAÇÃO DOS USUÁRIOS

Chegamos no grande vilão por trás de muitos ataques atuais. E para mudar essa realidade, é preciso transformar o olhar. É necessário compreender os usuários como nossos clientes.



A nossa missão é protegê-los, e não existe maneira mais proativa e/ou preventiva de proteger seus usuários do que com capacitação em simples conceitos de *cyber sec*.

Investir em conhecimento é uma maneira para desenvolver o colaborador, reforçar o alinhamento de informações entre as equipes e ter tarefas executadas com muito mais precisão.

É preciso lembrar que comunicação é quando os dois lados compreendem o que está sendo transmitido, e como *Three-Way HandShake* do TCP, nenhum pacote pode ser perdido na comunicação. O ideal, seria adaptar o conteúdo a cada geração, por interesse e por níveis de conhecimento.

Vejo as empresas criando espaço de conscientização de usuários, com softwares que de tempos em tempos, disparam spans internos controlados para validar quem clicaria em link ou quem colocaria uma senha em site falso. Sim, isso é uma ferramenta de conscientização importante, porém não basta apenas esse protocolo.

Aproxime-se da sua área com o endomarketing, formule campanhas, palestras ao longo do ano e crie uma gamificação do conteúdo.

Agora, será que conscientização se limita ao usuário final?

Ao longo do tempo, lemos e vemos que a maioria dos ataques tiveram como vetores iniciais os usuários finais. Entretanto, queria te contar uma novidade: nem sempre é assim. As últimas respostas que participei não foram causados por usuários finais. Eles foram causados por usuários avançados de TI.

Dito isso, queria chamar sua atenção para dois pontos com relação a usuários avançados:

- **Gerenciamento de credenciais** – participei de uma resposta no qual um analista de suporte tinha uma credencial com privilégio de *domain admin.* Ele usava para

administrar o serviço de diretório, mas também usava a mesma credencial para acessar remotamente as máquinas dos usuários que demandavam atendimentos.

Em um destes atendimentos, ele deixou sua sessão aberta no computador de um usuário que não tinha todos os patchs do Windows aplicado. O atacante conseguiu explorar uma vulnerabilidade que lhe permitia tomar as sessões ativas, e dentre elas, lá estava a sessão do *domain admin*.

O hacker se aproveitou e escalou privilégio até tomar todas as principais contas do domínio, chegando até o serviço de diretório. Rapidamente, ele criou uma política que distribuía um *ransomware* para todos os computadores do domínio.

Garantir a segurança das credenciais privilegiadas da sua empresa, tornou-se uma prática fundamental para se proteger de ameaças internas, vazamentos de dados e perdas financeiras imensuráveis.

Area de desenvolvimento – Tudo no mundo evoluiu para ser simples, rápido e de fácil acesso/uso. E como já disse, todas estas evoluções tornaram o mundo um lugar mais inseguro.

Neste movimento, surgiu os *githubs* e novas plataformas de desenvolvimento, criando superfícies que os grandes players de *cyber sec* e startups ainda estão tentando criar soluções para protegê-las.

Security by design está longe de ser uma realidade cultural nas organizações. Estamos desenvolvendo com o foco em colocar em produção rápida, com metodologias ágeis, utilizando plataformas de fácil acesso que não foram pensadas para serem seguradas, e em superfícies novas que se quer temos tecnologias de fato prontas para poder proteger.

Acompanhei um outro incidente de Ransomware. Logo que chegamos, executamos o primeiro passo de uma resposta a incidente como está, *lockdown*. Ou seja, isolamos todos os perímetros possíveis e imaginários que foram afetados. Logo pensamos: “temos o controle total da situação, agora vamos para a próxima fase de resposta”.

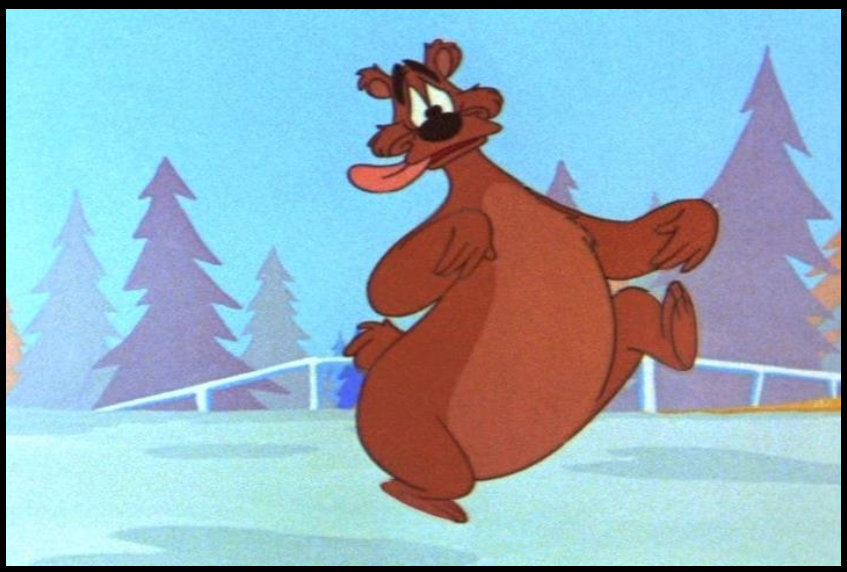
Horas depois de termos executado o *lockdown*, vimos o atacante fazendo uma transmissão ao vivo do código da principal aplicação do cliente. De imediato imaginamos que deixamos passar algum perímetro, e que ele ainda tinha o controle sobre parte do ambiente. No caminho de investigar o que faltava, descobrimos um github em modo público, recém criado com todo o código da principal aplicação.

Surgiu a pergunta: quem criou isso? Foi quando recebemos a informação de que um DEV colocou um código git para trabalhar de casa, mesmo quando isolamos a operação. A aplicação inclusive, fazia uma consulta via LDAP no principal domínio do cliente e claro o código mostrava uma credencial válida para fazer tal consulta.

Estamos muito preocupados em falar do usuário final, mas precisamos também ficar alertas com o nosso time avançado. É preciso implementar políticas, procedimentos, regulações e boas práticas. No final do dia, tudo se resume a ter uma boa governança sobre os indivíduos. Precisamos reforçar, principalmente, a cultura de security by design, no qual o primeiro passo é pensar de forma segura.

Leia mais sobre *Secure Software Development Lifecycle (S-SDLC)* e *DevSecOps,* este é o caminho.

6. TENHA UM PLANO DE RESPOSTA A INCIDENTE



Quando vejo uma empresa sem Plano de Resposta a Incidente, me vem a memória o episódio do Urso Fatso do pica pau. Ele corre de um lado para o outro, tentando fazer várias coisas ao mesmo tempo, mas não faz nada. E é exatamente isso que acontece com organizações que não possuem um plano eficiente.

Muitas das vezes, a empresa investiu em tecnologias para o ambiente, mas não investiu em um plano bem estruturado.

A diferença entre voltar o ambiente em produção em 8 horas ou 8 semanas, está ligado a um plano de resposta. Muitas organizações quando questiono este ponto, me responde com um: “temos o NIST 800-61 implantado, somos certificados ISO 27001, então não há com o que se preocupar, fique tranquilo.”.

Duas verdades precisam ser ditas. A primeira, é que podemos fazer de tudo para tornar nosso ambiente seguro, mas nunca um profissional de segurança dormirá tranquilo. A segunda, é que todos estes frameworks de segurança são fantásticos, e de fato, precisam ser utilizados. Eles encurtam o caminho do processo de criação de um plano de resposta a incidente. Porém, em sua maioria, são um conjunto de boas práticas.

Muitos explicam que você precisa pensar e adaptar tais processos, procedimentos ou itens de controle a sua organização. Adaptar significa trazer as características da cultura da sua organização e seu modelo de negócio para o processo de resposta a incidente.

Um bom plano precisa falar com o seu *business Impact Analysis (BIA)*. Caso não tenha ainda um BIA, não comece criando um processo de resposta a incidente, porque você não saberá no momento de uma resposta o que é mais importante para o seu negócio, deixando o seu plano sem foco e sem eficiência. Por onde devo começar? Sua área de negócio tem esta resposta, e você vai conseguir esta resposta quando for criar o BIA.

Como mencionei antes, pensar na cultura, no momento de desenvolver este plano também é importante. No incidente você não responderá a ele sozinho. Praticamente todas as áreas da organização de alguma forma estarão envolvidas. Mais uma vez, a comunicação é uma das partes mais importantes.

Outros dois planos precisam ser criados. Ambos estão relacionados à Continuidade de Negócio (PCN) e conversam diretamente com a fase de recuperação do processo de resposta a incidente:

a) **Disaster recovery plan (DRP):** como o próprio nome sugere, basicamente é plano criado para retornar seu ambiente vivo o mais rápido possível em uma situação de catástrofe.

   Pensar nele é importante porque, em geral, tal plano dispara gatilhos de novos investimentos, como por exemplo, a criação ou contratação de um site de DR para as principais aplicações da organização. Vocês serão provocados no processo de criação sobre qual seria o melhor RTO (*Recovery Time Objective*) para sua organização. Tal tempo vai influenciar diretamente no principal indicador do processo de resposta a incidente, que é o *Incident Time to Response (TTR)*, ou no *Time to Recover (TTV)*.

b) **Communications and Operation Management (COM**): é um conjunto de processos e procedimentos operacionais para proteger as informações. São cerca de 17 grandes processos, que listo abaixo:

   1. *Change Management*
   2. *Segregation of Duties*
   3. *Separation of Development, Test, and Operational Facilities*
   4. *Monitoring and Review of Third Party Services*
   5. *Capacity Management*
   6. *Controls Against Malicious Code*
   7. *Controls Against Mobile Code*
   8. *Information Backup*

9. *Network Controls*
10. *Security of Network Services*
11. *Electronic Messaging*
12. *Audit Logging*
13. *Monitoring System Use*
14. *Protection of Log Information*
15. *Administrative and Operator Logs*
16. *Fault Logging*
17. *Clock Synchronization*

> *“Devemos dar atenção a isso antes de criarmos o nosso processo de Resposta a Incidente”*

Vamos pensar que respondemos a um ataque e que avançamos para a fase de recuperação do ambiente. Acredito que você vai querer um backup íntegro e funcional, e para que este desejo seja atendido, precisamos pensar em políticas de backup, como no item 8 da lista (*Information Backup*).

Também não queremos durante o ataque descobrir que, apesar do EDR resolver o problema, talvez não teríamos licença para todos os dispositivos do ambiente, como no item 5 (*Capacity Management*).

E se nas fases de investigação descobrirmos que uma mudança legítima no ambiente foi feita, e tal mudança gerou uma vulnerabilidade a qual foi utilizada como vetor de ataque? Vamos querer saber quando esta mudança foi feita, o motivo e por quem foi feita. Tais perguntas são respondidas pelo item 1 da lista (*Change Management*).

Quem já ouviu a expressão “sem log, sem crime”? Então eis o grupo de itens que considero mais importante desta lista: os itens de 12 a 17. Todos estão relacionados ao gerenciamento de logs do seu ambiente, e será impossível avançar para a última fase de uma resposta a incidente (pós incidente). Sem o pós incidente, será gerado um relatório de hipóteses prováveis do ataque. Com este grupo de processos, você terá um verdadeiro relatório de *forense* com fatos, que poderá salvar sua carreira e a continuidade do negócio.

Agora sim, tendo um BIA, um DRP, e um COM para chamar de meu, podemos avançar para o desenvolvimento de um processo de resposta a incidente.

Qual que eu devo usar como base? Qual o melhor deles? O melhor é aquele que está mais adaptado à sua organização. Se você me perguntar o que eu mais gosto, eu responderia o NIST 800-61, aplicando o CARTA (Continuous Adaptative Risk and Trust Assessment) do Gartner.

7. TESTE SUAS DEFESAS

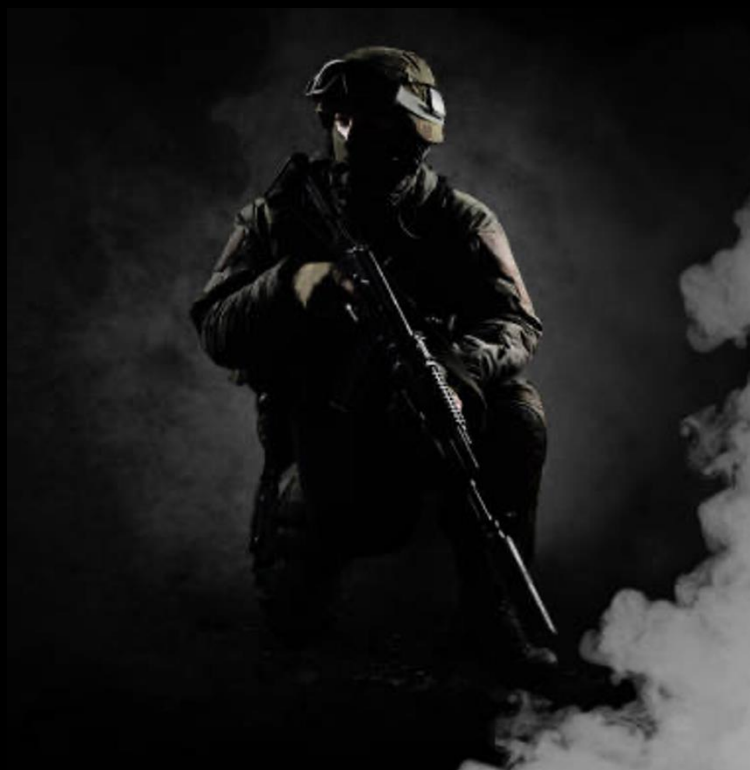
O que será que acontece se estou preparado para a guerra, porém ela nunca acontece? Os SEALs, principal divisão de elite da marinha dos Estados Unidos já percebeu isso. Não basta apenas se planejar e treinar, precisamos nos testar. Ou seja, colocar nosso plano em prática.

Pensando nisso, esta divisão desenvolveu um método simples que posteriormente foi adotada por todos os exércitos militares pelo mundo. Basicamente consiste em simular uma guerra. Essa simulação divide o exército em dois grupos: um chamado de ataque, os Red Team, que simulam o inimigo, e outro time de defesa, o Blue Team, em que coloca em prática todo o plano criado.

Tal método gera muitos ganhos, já que vai entender de fato, como o inimigo pensa, como os soldados funcionam sobre estresse e/ou existe alguma vulnerabilidade grave no exército.

A história não conta, mas imagino que um bom soldado de cyber olhando para este método um dia pensou: por que não aplicar este conceito em cibersegurança? Nascendo assim, o Cyber Security War Game.

Esse War Game são simulações criadas para testar todo o seu ecossistema de segurança. Quando digo todo ecossistema, isso não inclui apenas as tecnologias adquiridas, mas também todos os processos criados e as pessoas, usando metodologias de PDCA (Plan, Do, Check, Action).



Veja o acontece em cada fase:

a) **Planejamento:** O objetivo principal desta fase é criar o teatro de guerra, ou seja, quais são os principais cenários possíveis de invasão do ambiente, e como minha organização pode ser impactada por tal ataque.

A construção deste teatro de guerra é feita por um time de arquitetos ou designers, que em geral, são formados por profissionais com conhecimentos de inteligências de ameaças (Threat Intel), risco e arquitetura.

b) **Execução:** Nesta fase, os cenários criados são executados por dois times, que não conhecem toda a história do teatro. Eles vão ser inseridos dentro do contexto para serem surpreendidos pelos eventos e ações planejadas, afinal, na realidade, não sabemos como e nem quando um ataque irá acontecer. A ideia é provocar um efeito surpresa em todos envolvidos.

   Todas as pessoas envolvidas em processo de resposta a incidente na organização devem participar da simulação. Essas pessoas são organizadas em dois grandes times, um que defende (Blue Team) e outro que ataca (Red Team). O time de ataque recebe o script proposto para executar o ataque, e a ideia é que o time de defesa use todo o processo de resposta a incidente, bem como as ferramentas instaladas no parque para mitigar o ataque.

c) **Verificações:** Durante e depois da conclusão da simulação, um time acompanha e avalia se os participantes estão seguindo todo o plano de resposta criado e se tais ações foram efetivas para bloquear o ataque, além das lições aprendidas que serão compartilhadas com todos os envolvidos para melhoria contínua das defesas. Chamamos este time de Purple Team, que basicamente é a mistura do Red com o Blue. Ou seja, um time mediador do conflito simulando apenas para observar e gerar novos aprendizados.

d) **Ação:** As lições aprendidas geram ações de melhoria do ecossistema de cyber, que devem ser aplicadas, e novamente, voltamos ao primeiro passo que é repetir a simulação com as ações correção aplicadas no ambiente.

Geralmente War Games são feitos duas ou três vezes por ano. Não é algo que seja praticável de forma recorrente, porque exige tempo de todos os envolvidos, um planejamento bem elaborado. Como vamos testar nossas defesas ao longo do tempo?

O caminho mais comum são os velhos conhecidos como o Pentest. Aliás cabe uma consideração importante. No passado a gente romantizava os Pentests blackbox (*pentest* a qual é concedida pouquíssima informação para o hacker ético). Entretanto, isso não cabe mais nas organizações atuais. Se já sabemos através dos processos de gestão de vulnerabilidade onde estão os nossos problemas, porque vamos esconder isso de quem vai testar o ambiente? O melhor caminho é informar e realizar a prova de conceito se tal vulnerabilidade é passiva de exploração ou não.

Ainda sobre os Pentests, também entramos em outra encruzilhada. Apesar de ser viável realizar mais de uma vezes ao longo do ano, ainda é algo sobre demanda, e não é o tipo de execução que é possível de ser feita diariamente.

Neste sentido surgiu uma nova tecnologia chamada Breach and Attack Simulation (BAS). Este nicho de tecnologia é uma plataforma projetada para executar ações que imitam ações de ameaças reais para determinar se elas são detectadas por seus controles de segurança.

O BAS usa um conjunto de cenários de ataque complexos que tentam contornar esses sistemas de controle para atingir um objetivo específico. Se esse objetivo puder ser alcançado, como tráfego passando por um firewall ou um e-mail sendo entregue a um destinatário final, a plataforma BAS ajuda a descobrir uma falha nesse controle que precisa ser corrigida.

Os testes são projetados para não interferir nas operações de produção, trabalhando silenciosamente nos bastidores para que os usuários não percebam que estão sendo executados, a menos que o vetor seja algo como *Phishing Awareness*, que testa a vigilância dos funcionários.

Então qual a melhor escolha? War Game? Pentests? ou BAS? A resposta é a combinação de todos. Cada um deles possui um propósito e seus benefícios.O War Game vai estar mais focado em validar se o processo de resposta está funcionando corretamente, e como todos funcionam sobre pressão. O Pentest, executará a prova de conceito das vulnerabilidades que são descobertas pelo processo de gestão de vulnerabilidade, e o BAS vai de forma contínua validar se seus controles de segurança estão sendo eficientes.

Avaliando todos os tópicos aqui apresentados, é imprescindível estar preparado. Lidar com um momento de crise é tão importante quanto investir em tecnologia e no desenvolvimento dos negócios. Organizações de todo o mundo estão expostas a diversos tipos de incidente, que podem ocorrer a qualquer momento.

A ausência de uma cultura de gestão de riscos e crises, como PCN, pode promover consequências irreversíveis aos negócios, já que algumas situações são de difícil previsão e podem se tornar frequentes. Para que seja efetivo, é preciso pensar no que fazer antes de um ataque. Realizar uma análise aprimorada dos riscos e criar um plano estratégico.

www.ish.com.br