Resiliência em tempos de **Ransomware** (I)

Por **Isabel María Gomez, Global CISO** do Atento

ATENTO

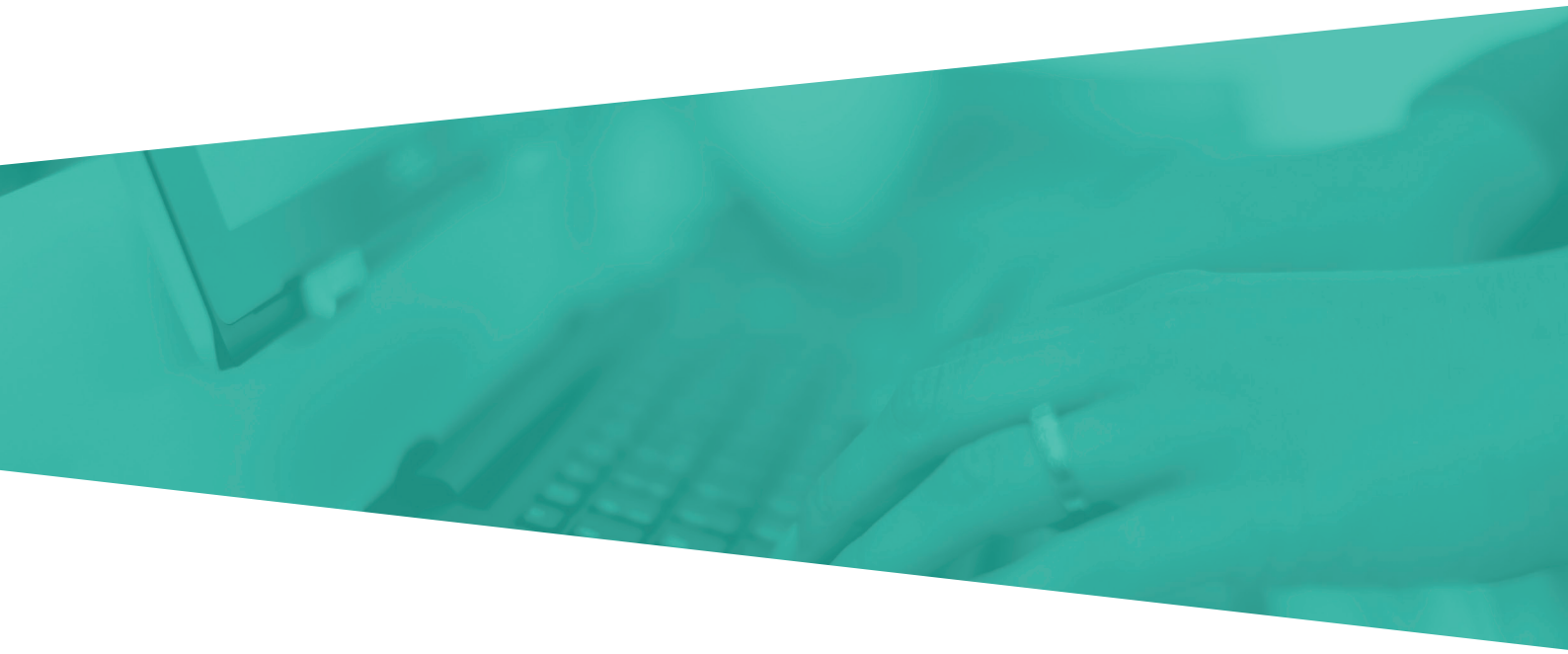
WHITE PAPER

CONTEÚDO

01 Resiliência em tempos de **Ransomware**

Um ataque de ransomware é um dos cenários mais difíceis que as empresas podem enfrentar na atualidade. Não apenas porque **testam os processos de continuidade de negócio da organização,** mas por gerar um cenário de estresse que vai além da cibersegurança e da tecnologia, produzindo linhas de atuação e tomadas de decisão que poucas vezes são testadas tão vigorosamente.

Todas as áreas da empresa, sem exceção, são envolvidas em um exercício que deixou de ser o teste teórico, monótono, e todos são envolvidos para garantir a recuperação no contexto de um cenário de desastre, sob controle e supervisão de tempo, que costumava finalizar nos prazos esperados sem maiores contratempos em função de sua cuidadosa planificação. **Um ataque de ransomware é uma situação real, que testará a resiliência real dos líderes de segurança e tecnologia,** responsáveis por oferecer suporte e direcionar o esforço excessivo de toda a equipe: ***Não existe vento favorável para quem não sabe aonde quer chegar.***



02 O momento que **muda tudo**

Como em todo cenário de desastre sempre há uma faísca, uma peça de dominó que cai e inevitavelmente arrasta outras que a acompanham: ***o começo da criptografia.*** É nesse momento que o **CISO (Chief Information Security Officer)** recebe a ligação que ativa o comitê de crise, que verdadeiramente aciona a resiliência da cibersegurança. Porque desse papel depende a tomada das primeiras decisões adequadas para conter e remediar, enquanto é oferecido suporte e o melhor conselho ao resto da empresa, para ajudar na priorização de cada linha de ação e dar mais vento às asas da tecnologia: ***o que for decidido nesses primeiros momentos será o que determinará o tempo de recuperação da empresa.***

Nesta altura, é mais do que conhecida a metodologia utilizada por um ransomware para funcionar. Contudo, é importante fazer um breve resumo, simplificando a sequência dos passos nos cenários que gerarão que um cibercriminoso tenha acesso à rede, aos sistemas e aos dispositivos conectados.

Há três etapas em um ataque de ransomware que podem ser simplificados em **3 grandes atividades:**

- O cibercriminoso consegue acessar sua rede, sistemas ou dispositivos.
- O cibercriminoso assume o controle e lança o ransomware.
- O cibercriminoso ativa a criptografia de dados, destrói as cópias de segurança e rouba os dados da organização e/ou de seus clientes, e depois exige o pagamento de um resgate.

03 A **origem**

Um cibercriminoso malicioso costuma encontrar **o ponto de entrada para sua rede** através de:

- Ataques de força bruta.
- Explorando vulnerabilidades não corrigidas.
- Mediante ataques de phishing, em que o cibercriminoso solicita informações confidenciais a um indivíduo, grupo ou organização imitando ou suplantando uma marca específica, em geral conhecida, para obter um lucro econômico. O cibercriminoso tentará enganar os usuários para revelarem dados pessoais, como números de cartões de crédito, dados bancários online e outras informações sensíveis, as quais depois poderá utilizar para cometer atos fraudulentos.

04 A implantação

Uma vez que o cibercriminoso **obtém acesso à rede:**

- Assumirá o controle de seus sistemas e dispositivos conectados ao escalar permissões, em caso de ainda não as ter conseguido.
- Implantará o malware e infectará seus sistemas e dispositivos conectados com ransomware.

05 A execução

Uma vez com **o controle total,** ele reduzirá as defesas talvez mediante o uso de políticas globais dentro do sistema ou do diretório ativo, criptografará seus dados, tudo ao mesmo tempo, e eliminará os arquivos de cópia de segurança disponíveis ou conectados. Além disso, também roubará todos os dados possíveis da organização.

Neste ponto, e se conseguiu extrair dados da empresa, é possível que ameace vazar esses dados em caso do não pagamento do resgate, garantindo que decifrará seus dados e restaurará seu acesso a eles, se você pagar o resgate. Isto, sem dúvida, é algo que ele realizará, pois é a chave de seu negócio.

06 Algumas **dicas técnicas** para melhorar a resiliência

Apesar de que apresentaremos os elementos organizacionais em uma segunda edição, é importante elencar **uma série de medidas técnicas que estão à altura de qualquer empresa** para ajudar a detectar de maneira precoce e facilitar a correlação de alertas e informações que permitem dificultar a execução deste tipo de ameaça.

Na lista das principais medidas de segurança contra ransomware, é aconselhável se distanciar e, enquanto se mantém no que já está estabelecido e amplamente conhecido, focar no que de forma simples e acessível possa incrementar o nível de resiliência e proteção contra ransomware, que ajude o CISO a protegê-los, não importa o tamanho de sua empresa.

1. **Instalação de LAPS (Local Administrator Password Solution)** em todas as workstations

   a. A Solução de senha de administrador local oferece gestão de senhas de contas locais de equipamentos ligados a um domínio. As senhas são armazenadas em um diretório ativo (AD) e são guardadas por uma lista de controle de acesso, assim apenas usuários elegíveis podem consultar ou restabelecer uma senha.

2. **Desativação do servidor SMB (Server Message Block)** nas workstations do domínio

   a. O SMB é um protocolo cliente/servidor que administra o acesso a arquivos e diretórios completos, bem como outros recursos da rede, como impressoras, roteadores ou interfaces abertas à rede.

   b. Link para leitura recomendada.

3. **Segmentação da rede**

   a. Talvez seja a medida mais importante de todas as mencionadas, pois seu principal objetivo é diminuir a abrangência do ataque aplicando regras que reduzam o risco de movimentos laterais, além de favorecer um modelo de segurança baseado na confiança zero. Isto permite que somente o tráfego autorizado possa ir de uma origem a um destino autorizado.

4. **Desativação de Macros** em Words

   a. Uma macro é uma série de comandos e instruções agrupados de forma conjunta, como um mesmo comando, para completar uma tarefa automaticamente.

5. **Definição de políticas de segurança via GPO (Objeto de Política de Grupo)** dos Navegadores

   a. Configurações como o filtro de phishing, gestão de senhas e verificação de certificados podem proteger a organização contra ataques baseados em web, quando

são configurados centralmente e implementados nos equipamentos da organização. Isto pode ser conseguido utilizando o GPO fornecido por Microsoft para Edge e Internet Explorer, e os modelos ADMX para Chrome e Firefox, proporcionados pelos respectivos provedores dos navegadores.

6. **Proteção do LSASS (Local Security Authority Subsystem Service)** para evitar a obtenção de credenciais

a. O Serviço de Subsistema de Autoridade de Segurança Local (Local Security Authority Subsystem Service, LSASS) é o processo responsável pelo cumprimento da política de segurança nos sistemas operacionais Microsoft Windows. Verifica se os usuários se logaram em um equipamento ou servidor Windows, gerencia as mudanças de senhas, cria tokens de acesso e escreve no registro de segurança de Windows. *(Wikipédia)*

b. Como lsass.exe é um arquivo de sistema chave, o seu nome é com frequência falsificado por malware. O arquivo lsass.exe utilizado por Windows é encontrado no diretório Windows\System32. Ao ser executado a partir de qualquer outra localização, é provável que lsass.exe seja um vírus, spyware, cavalo de tróia ou worm. Devido à forma em que alguns sistemas exibem as fontes, os desenvolvedores mal-intencionados podem nomear o arquivo como lsass.exe ("i" maiúsculo ao invés de um "L" minúsculo) para enganar os usuários e instalar ou executar um arquivo malicioso e não o sistema confiável.

c. Link para leitura recomendada.

7. **Geração de políticas de Firewall local** por servidor e sua ativação

a. Depois de identificar os requisitos e contar com as informações sobre o desenho da rede e dos dispositivos, pode começar a projetar as regras e a configuração de GPO que permitirão aplicar seus requisitos nos dispositivos.

b. Link para leitura recomendada.

8. **Implementação de AppLocker** em todas as workstations

a. A ferramenta denominada AppLocker permite bloquear certos aplicativos sempre que você possua permissões de administrador. Desta forma, pode decidir quais programas são executados no PC, impedindo que os usuários ponham em funcionamento aplicativos considerados perigosos ou inadequados. Trata-se de uma importante funcionalidade que permitirá incrementar a segurança dos computadores contra ameaças externas.

b. Link para leitura recomendada.

9. Migração de sistemas operacionais fora de suporte

a. Muitas vezes, acredita-se que é melhor tratar a infraestrutura de TI em forma conjunta, mas isso pode adiantar a obsolescência. De fato, o hardware, o software e as redes costumam ser tratados de forma conjunta. Este erro comum origina que os efeitos da obsolescência não sejam considerados em cada equipamento individual. Nem todos os equipamentos precisam do mesmo tipo de programas e nem todos são usados para o mesmo tipo de trabalho. O mais recomendável é realizar uma análise de cada dispositivo de forma individual, para antecipar o aparecimento de alterações em sua funcionalidade.

10. Estabelecimento de assinatura SMB e SMB3 em toda a empresa

a. O protocolo de autenticação SMB assina essencialmente cada pacote com uma assinatura digital, para que cliente e servidor confirmem sua origem, assim como a autenticidade da chamada. Quando a assinatura SMB está ativada, se um atacante tentar roubar uma sessão SMB, não poderá modificar os pacotes.

b. Link para leitura recomendada.

07 Mas não é apenas uma questão de tecnologia. **Há também a diligência prévia.**

Se diversas medidas técnicas forem aplicadas e houver relativa segurança e resiliência em relação à tecnologia, é preciso focar em outro tipo de resiliência que também será necessária durante ataques deste tipo: **a diligência prévia.** Fornecer à empresa um adequado modelo de cibersegurança não é o suficiente: os valores da organização e das pessoas é que irão encorajar todo o time a se esforçar para colocar a empresa no eixo novamente e de forma rápida.

Entre alguns dos conceitos que serão elaborados na segunda edição, estão a adaptabilidade, a reação organizacional ou mesmo os impactos legais e comerciais do controle das informações ao incidente.

ATENTO

www.atento.com