WHITEPAPER

COMO PROTEGER SEUS DADOS CONTRA RANSOMWARE

The Register® | Lenovo

1. SUMÁRIO EXECUTIVO

A última década viu o ransomware deixar de ser um problema em grande parte teórico que afetou um número limitado de vítimas azaradas, para um problema generalizado para a maioria das organizações e uma ameaça existencial para uns poucos infelizes.

Isso aconteceu porque o volume de dados sendo gerado e retido pelas organizações explodiu, impulsionado em parte por novas cargas de trabalho como IA, Machine Learning e análises avançadas.

Enquanto isso, a pandemia deu uma chance aos maus atores elevarem seu jogo. À medida que as empresas mudaram para o trabalho remoto e híbrido, as equipes de segurança estendidas deixaram os trabalhadores e os seus dados mais expostos.

Este whitepaper define a escala da ameaça ransomware, incluindo como os invasores estão estendendo seus alvos além das grandes empresas e infraestrutura crítica, colocando médias e pequenas organizações cada vez mais na linha de fogo.

Também explica por que as organizações precisam adotar uma estratégia de defesa em profundidade, a fim de proteger seus ativos mais valiosos – seus dados e informações de infraestrutura – bem como seus negócios em geral. Isso significa não apenas focar na prevenção, mas na detecção e mitigação e, crucialmente, recuperação para garantir que eles possam voltar aos negócios rapidamente.

Também exploraremos como uma infraestrutura de armazenamento subjacente tem um papel cada vez mais importante a desempenhar, especialmente quando se trata de recuperação, para garantir que um ataque de ransomware seja uma irritação, em vez de um desastre completo.

2. INTRODUÇÃO

As raízes do ransomware remontam à década de 1980, quando um indivíduo sem escrúpulos se aliou pela primeira vez à ideia de um Trojan que criptografasse nomes de arquivos para um esquema de extorsão. Mas não foi até meados da década de 1990 que os pesquisadores conceberam a adição de uma chave pública criptográfica à mistura, aumentando a possibilidade de as vítimas perderem permanentemente seus dados se não pagassem.

Em 2010, o ransomware era uma ameaça viável, embora o impacto no mundo real talvez tenha sido ofuscado por manchetes hiperbólicas. No entanto, os últimos anos têm um aumento constante no impacto financeiro das gangues de ransomware, alimentadas em parte pela ascensão de Gangues Ransomware-as-a-Service (RaaS) e, em parte, porque as criptomoedas tornaram mais fácil recolher e transportar os resgates.

O ransomware é um problema para todos, não apenas grandes empresas ou operadores de infraestruturas críticas

O resultado é o aumento da atividade das gangues de ransomware e mais ataques de alto perfil, como os ataques contra a Colonial Pipeline e JBS USA, em 2021.

Tudo isso contribui para que o ransomware se torne não apenas uma preocupação técnica ou comercial, mas uma preocupação de segurança nacional.

A Casa Branca observa que as vítimas pagaram US $400 milhões em resgates de ataques de ransomware globalmente em 2020, com US$81 milhões no primeiro trimestre de 2021[1]. O custo médio do resgate em 2021 foi de US$170.404, de acordo com o relatório Sophos State of Ransomware 2021. Mas o custo total de remediar um ataque cresceu de uma média de US $761.106 em 2020 para US$1,85 milhão em 2021. Isso devido ao tempo de inatividade dos negócios, pedidos perdidos e custos operacionais.

Uma pesquisa da gigante de seguros AIG previu US$20 bilhões em custos de danos de ransomware em 2021, em comparação com US$325 milhões em 2015. Os custos de danos totais globais de crimes cibernéticos devem atingir US$10,5 trilhões até 2025, segundo a AIG. Nos casos em que os dados são extraídos por hackers, a AIG informou que os custos de pedidos de resgate e extorsão haviam dobrado[2].

A AIG também observou que as interrupções de rede devido a ataques de ransomware estão ficando mais longas, com sete a dez dias sendo um prazo típico. E enquanto os pedidos perdidos em curto prazo são uma dor de cabeça óbvia, como você leva em conta o impacto de longo prazo sobre a confiança do cliente? Da mesma forma, qual o impacto sobre fornecedores, investidores e outras partes interessadas?

O ransomware é um problema para todos, não apenas grandes empresas ou operadores de infraestruturas críticas. A AIG disse que viu um aumento de 150% na frequência de reclamações de ransomware e extorsão desde 2018, e estas vinham de “empresas de todos os tamanhos... em todos os tipos de indústria.”

Um conselho conjunto das autoridades dos EUA e Centro Nacional de Segurança Cibernética do Reino Unido no início deste ano, disse que os atacantes estavam "se afastando do 'grande jogo' nos Estados Unidos”, e partindo para médias organizações. Entretanto, a Agência Europeia para o cenário de ameaças de cibersegurança mais recente classificou o ransomware “como a principal ameaça” para o período.

NOTAS DE RODAPÉ

1. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

2. https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-ransomware-global.pdf

Por isso, é importante entender a ameaça, reconhecer que qualquer pessoa pode ser vítima, e garantir que os sistemas estejam preparados para detectar o ransomware e implementar uma estratégia para responder se o ransomware violar suas defesas.

3. VOCÊ FOI ATINGIDO POR UM ATAQUE RANSOMWARE? QUAL O MELHOR RESULTADO QUE VOCÊ PODE ESPERAR?

O ransomware é uma ameaça generalizada e contínua e pode parecer tentador usar como padrão uma mentalidade de bunker em resposta, apostando em um perímetro de fortaleza e vigilância constante para manter os maus atores fora de seus sistemas.

Mas isso é difícil de sustentar no ambiente de tecnologia de hoje. Poucos especialistas acham que a tradicional abordagem perimetral é suficiente, porque a natureza dos invasores de ransomware é entrar silenciosamente em seus sistemas e deslocar-se, lateralmente, até encontrarem as mercadorias que eles estão procurando.

As equipes de tecnologia precisam de detecção e escaneamento automatizados, de modo que se os intrusos passarem pelas defesas externas, eles podem ser desmascarados e parados antes de danificar ou exfiltrar dados

Uma abordagem melhor é adotar a defesa em profundidade, como recomendado por agências governamentais como o NCSC3 do Reino Unido e a Agência de Infraestrutura de Segurança e Cibersegurança dos Estados Unidos.

Isso significa que as organizações devem praticar uma "higiene" de segurança básica, para evitar ataques em primeiro lugar. Isso inclui correção e atualização de sistemas e aplicativos para minimizar vulnerabilidades; educar usuários sobre phishing e outras ameaças; e exigir outros tipos de defesas, como autenticação multifator, senhas fortes, etc.

Mas o combate ao ransomware não para por aí. Alguns ataques vão passar, e é aqui que a detecção e mitigação entram em jogo. Equipes de tecnologia precisam de varredura e detecção automatizadas, de modo que, se intrusos passarem pelas defesas externas, eles podem ser desmascarados e parados antes de danificar ou exfiltrar dados. E eles devem considerar ações no nível de rede, como segmentação, criptografia de ponta a ponta e privilégio mínimo.

E é claro que eles precisam aumentar seu foco sobre remediação e recuperação. A detecção contará pouco se a empresa estiver offline e incapaz de fazer negócios por horas, dias ou mais. Estratégias de recuperação devem estar em vigor e testadas bem antes de qualquer ataque, com a equipe treinada exatamente no que eles têm de fazer.

QUAIS DADOS CORREM MAIS RISCO?

O primeiro passo é analisar as principais fontes de dados e seus riscos associados. Que impacto perder o acesso a um determinado armazenamento de dados teria na capacidade da organização para fazer negócios?

Grandes conjuntos de histórico de dados podem ser essenciais para treinar algoritmos de Machine Learning, mas pode não ser imediatamente necessário fazer backup desses dados e correr logo após um ataque.

3. https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware

4. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

Por outro lado, voltar aos negócios pode requerer uma quantidade relativamente pequena de dados no primeiro exemplo – os líderes precisam saber exatamente o que isto é. Por exemplo, o primeiro pensamento de uma empresa financeira pode ser garantir que seus registros de transações estejam seguros. Já uma empresa de manufatura pode querer seus dados de PLM (Product Lifecycle Management) como prioridade em qualquer restauração.

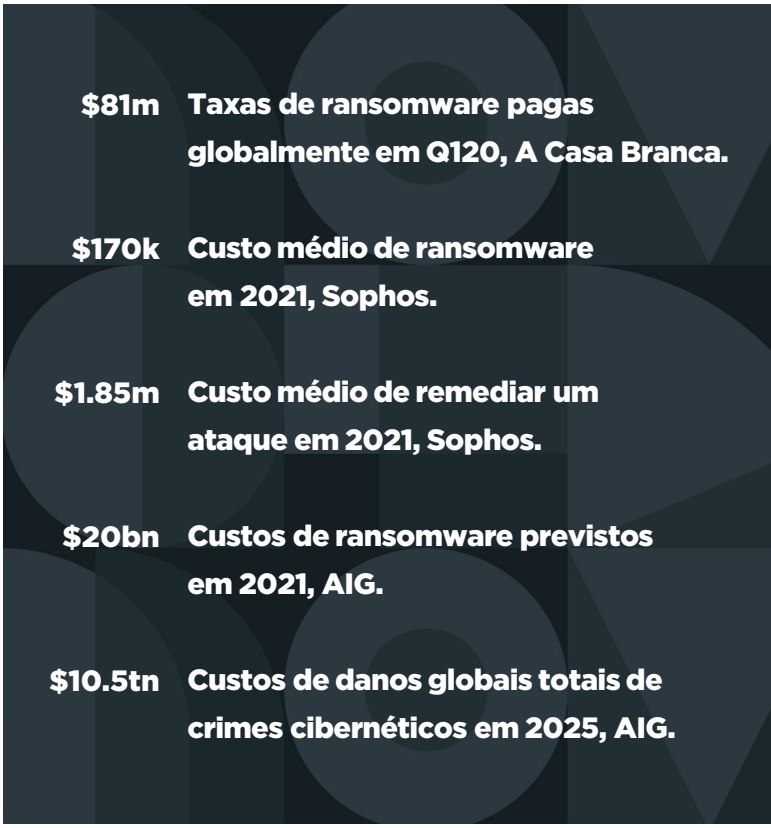
E um ataque pode ter impacto limitado se for detectado antes. As empresas precisam de ferramentas que permitam identificar o raio da explosão rapidamente, restaurando apenas os arquivos que realmente são necessários.

COMO ISSO AFETA A SUA RECUPERAÇÃO?

Abordagens tradicionais de backup, normalmente com fita como destino final, estavam focadas em produzir um registro completo de todos os dados da empresa, que seria realizado fora do local. Embora abrangente, esta abordagem pode ser difícil de manejar para uma rápida restauração de negócios.

A criação desses backups é uma tarefa demorada que pode interferir nas cargas de trabalho. Pior, pode levar dias ou semanas para realizar uma restauração.

Compreender a importância das fontes de dados específicos significa que a organização pode pensar sobre com que rapidez ela deseja restaurar seus dados e quais dados – se houver – ela pode se dar ao luxo de perder. Pode não ser necessário ter esses históricos de dados para funcionar imediatamente. Para históricos de dados para fins de conformidade, abordagens tradicionais de backup podem ser aceitáveis, mesmo que a recuperação seja medida em semanas.



Mas se os dados de produção forem perdidos, isso afetará a capacidade da organização de fazer negócios, agora. A vítima vai querer recuperar seu dados minutos, ou mesmo segundos antes da interrupção.

SNAPSHOTTING

A resposta para o dilema de backup/restauração é o snapshotting. Um snapshotting captura o estado do sistema de arquivos no momento em que é obtido, criando um volume de imagem somente como leitura. O registro de snapshots subsequentes muda apenas os snapshots anteriores.

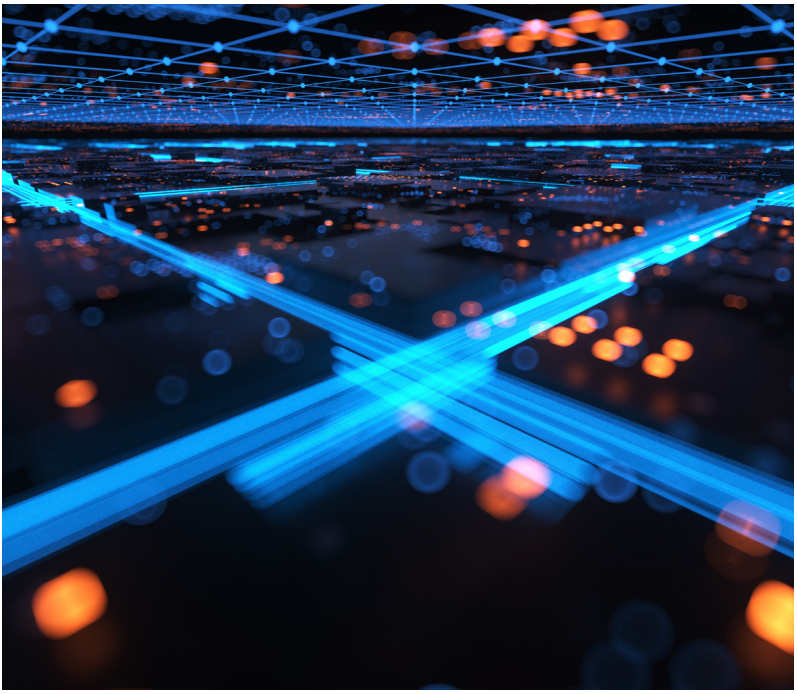
Isso fornece a base para um registro imutável de dados em vários momentos, permitindo que os administradores guardem versões anteriores no cofre antes de um incidente, como um ransomware. Também permite a recuperação não apenas de volumes inteiros, mas “LUNS” ou arquivos individuais.

É importante entender que nem todos os snapshots são criados iguais. O snapshot em si pode constituir um desafio de gestão de dados, com organizações potencialmente procurando fazer centenas ou milhares de snapshots por dia. Em alguns sistemas, o snapshot é efetivamente uma integração, adicionado ao topo de uma estrutura de bloco subjacente. É improvável que seja eficiente em relação ao tempo ou espaço com snapshots integrados ao sistema operacional.

Da mesma forma, os clientes devem considerar como a capacidade de snapshotting e sua infraestrutura de dados se integram com outras partes de sua pilha de backup e recuperação, como Veeam, Veritas ou Commvault. Isso poderia implicar em reexaminar as opções de backup e recuperação diante do aumento do ransomware, mas isso não significa necessariamente que investimentos existentes e parcerias devem ser desperdiçadas.

E O AIR GAPPING?

O Air Gapping (abertura de ar) tem sido uma parte essencial das estratégias de backup e recuperação. A regra tradicional foi 3-2-1, significando três cópias dos dados, em duas mídias diferentes, com uma cópia sendo mantida fora do local.



Mas o que isso significa no mundo moderno? Mídia fisicamente separada e sem rede mantida fora do local, obviamente, será inacessível aos invasores. Mas, não monitorável, também se torna inacessível para os profissionais de dados garantirem que os sistemas de uma organização de interesse sejam instalados de volta e funcionem em poucos minutos.

Então, eles vão querer considerar o que constitui um “air gap virtual”. As cópias no local imutáveis serão parte disso - se um invasor alcançar os dados eles são incapazes de alterá-lo, preservando a capacidade de restaurar instantaneamente.

Mais segurança e tranquilidade virão com capacidade off-premises na forma de cópias imutáveis mantidas em uma nuvem privada ou pública, ou híbrida. Novamente, a capacidade de uma plataforma de integração com outros serviços entra em jogo aqui.

OS ATACANTES SE PREOCUPARAM COM SEUS DADOS SEUS SISTEMAS DE PROTEÇÃO TAMBÉM

Ao longo deste processo, as equipes de tecnologia devem ter em mente qual é o seu objetivo final. Na grande maioria dos casos, isso será para voltar a funcionar em minutos, sem perder negócios, sem perder dados, e sem pagar o resgate.

Os atacantes também sabem disso. Eles são conhecidos por analisar a infraestrutura de dados de suas vítimas, identificar potenciais deficiências nos procedimentos de recuperação e definir as suas exigências de resgate em conformidade.

Se uma gangue de ransomware puder ter certeza de que um organização está contando com uma fita de backup fisicamente separada, ela sabe que a perspectiva de pagar um alto resgate pode ser mais palpável do que iniciar um processo de restauração de dados que levará dias ou semanas, e que a gangue pode não ser bem-sucedida. E se eles encontrarem o caminho para um backup conectado, você pode ter certeza que eles irão excluir antes de você ter a chance de detectar, bloqueando os dados de produção virtualmente, garantindo um pagamento ainda maior.

4. O PAPEL DO ARMAZENAMENTO PRIMÁRIO DEVE JOGAR EM SUA DEFESA EM UMA ESTRATÉGIA DE PROFUNDIDADE

O destino final de um invasor de ransomware é a infraestrutura de armazenamento local da organização. Se isso não oferecer o desempenho ou recursos necessários para sustentar sua estratégia de defesa em profundidade, incluindo o snapshot e as ferramentas de backup apropriadas e a capacidade de restaurar rapidamente, todas as suas outras precauções podem não valer nada.

A série DM de matrizes all-flash da Lenovo abrange o nível básico para soluções NVMe de ponta. O premiado CRN O DM5100F All-Flash Array, em particular, é semelhante aos blocos de construção de plástico na medida em que oferece flexibilidade para que as empresas comecem pequenas e construam capacidade de atender a maioria das necessidades. Ele fornece um caminho de uma única solução SAN para escalar até uma borda unificada para a plataforma em nuvem com recursos de classe empresarial. Um único dispositivo é dimensionado para até 88PB de capacidade bruta, com até 12 dispositivos em um único cluster[5].

A série DM oferece para organizações de todos tamanhos acesso à ordenação de resiliência de dados e gestão que foram anteriormente a preservação de alta qualidade de sistemas empresariais.

SNAPSHOTTING NO SEU CORAÇÃO

A série DM é alimentada pelo sistema operacional ONTAP, que tem a capacidade de snapshotting em seu coração. Como vimos, alguns sistemas fornecem capacidade de snapshotting como um bolt-on, que tem implicações para a eficiência do espaço, facilidade de gerenciamento e integração com outros sistemas de backup e tecnologias e serviços de recuperação.

A capacidade de snapshotting da série DM suporta até 1.023 snapshots por volume. Os snapshots são lidos apenas, fornecendo proteção contra a corrupção por um ataque de ransomware. Um snapshot leva menos de um segundo para criar e fornecer a base para restaurações instantâneas com arrays baseados em flash, se o gatilho é a exclusão acidental, ou no caso de um ataque de ransomware completo. As restaurações podem ser em arquivo, LUN ou nível de volume total. Esta é, obviamente, uma opção mais rápida do que uma restauração ou backup completo usando uma arquitetura tradicional.

Os snapshots podem ser agendados, mas também podem ser acionados pelo próprio sistema host integrado aos recursos de segurança.

A série DM oferece a organizações de todos os tamanhos acesso ao tipo de resiliência e gerenciamento de dados que anteriormente eram a preservação de high-end, sistemas empresariais.

INTEGRAÇÃO

A série DM da Lenovo oferece integração com a Veeam, Veritas, Commvault e outros provedores, que fornecem snapshotting e backup para VMs. Assim, os administradores são capazes de gerenciar sua proteção de dados e backup para vários tipos de dados e aplicativos em uma única plataforma. A série DM tem soluções baseadas em parceiros para detecção de ransomware integrada adicional e

5. https://www.lenovoxperience.com/newsDetail/283yi044hzgcdv7snkrmmx9okesnwqxuzayrlke1e8sv4ubs

proteção, como o CryptoSpike da ProLion, que usa IA para monitorar o comportamento do sistema de arquivos e bloquear assinaturas de ransomware e tipos de arquivo conhecidos. Este dá aos administradores a capacidade de rastrear o arquivo "entropia" e alterações, alertando-os para atividades suspeitas que podem ser um precursor de uma tentativa de ransomware.

Poucas organizações existem como uma ilha. A série DM tem integrações com provedores de nuvem empresarial-chaves, incluindo AWS, Microsoft, Google e IBM, permitindo que os clientes migrem e repliquem camadas de dados para várias nuvens e fornecendo o Air gapping necessário para garantir proteção completa contra invasores cibernéticos.

SEMPRE ATUALIZADO

A série DM está disponível sob a licença do programa Lenovo's TruScale Infinite Storage. Isso significa que a infraestrutura pode ser adquirida em uma base OPEX, proporcionando assim um custo-benefício maior e imediato benefício para a segurança operacional.

O programa inclui exames de saúde regulares e garante que atualizações e patches sejam automaticamente aplicados, para garantir que o armazenamento tenha a segurança mais recente e atualizações para fornecer a proteção mais atualizada.

Com TruScale Infinite Storage, a infraestrutura de armazenamento no local é implantada com a garantia de atualizações de tecnologia que são transparentes para as operações dos clientes e eliminam migrações de dados demoradas. Dessa forma, as organizações podem se concentrar em gerenciar seus dados com a mais recente tecnologia e evitar as limitações do hardware antigo e os riscos de segurança associados.

5. CONCLUSÃO

O ransomware é um perigo claro e presente, e a maioria das organizações estão cientes das ramificações de um invasor se apoderando com sucesso do controle de seus dados.

Com os atacantes indo além da "caça ao grande jogo", organizações de médio porte devem entender que também estão na linha de fogo.

Eles podem pensar que as empresas e organizações de nível superior lutam para conter a maré de ransomware e se recuperar enquanto os invasores avançam: neste sentido, que esperança há para eles? Eles podem imaginar que elas simplesmente não têm os recursos para detectar e mitigar as ameaças.

Mas eles estariam errados. Eles podem garantir seguir as melhores práticas de prevenção, detecção e mitigação e recuperação. Eles podem ter olhos claros sobre quais dados são mais críticos para eles e certeza de que eles entendem as funções específicas de seus dados e como as infraestruturas desempenham para protegê-los dos ataques.

Ao combinar as práticas corretas e a infraestrutura de armazenamento e ferramentas apropriadas, eles podem minimizar as chances de serem atingidos em primeiro lugar, maximizar as chances de voltar a operar rapidamente, e erradicar a necessidade de colocar "resgate" para baixo como um custo de fazer negócios.

6. SOBRE A LENOVO

A Lenovo Infrastructure Solutions Group (ISG) é um fornecedor de soluções de infraestrutura mais inteligentes para organizações de todos os tamanhos. Nossa tecnologia e insights fortalecem o coração dos Data-Centered do varejo mais inteligente, da fabricação mais inteligente, das cidades mais inteligentes, da saúde mais inteligente, das finanças mais inteligentes e muito mais. Pela computação de borda e nuvem, analytics, inteligência artificial e Infraestrutura como Serviço via TruScale, oferecemos tecnologias mais inteligentes para todos. Somos o único provedor de data center com produção de ponta a ponta . Possuímos toda a nossa cadeia de suprimentos para tudo o que construímos, para oferecer um nível de segurança e perfeição que ninguém mais pode, em qualquer lugar do mundo.