SOPHOS

O impacto dos backups comprometidos nos resultados do ransomware

Percepções de 2.974 organizações que foram vítimas de ransomware no ano passado

Um artigo da Sophos. Março de 2024

Introdução

Existem duas maneiras principais de recuperar dados criptografados em um ataque de ransomware: restaurar backups ou pagar o resgate. Comprometer os backups de uma organização permite que os agentes de ransomware restrinjam a capacidade da vítima de recuperar dados criptografados e, ao fazer isso, aumentar a pressão para pagar.

Este relatório fornece uma análise aprofundada do impacto que o comprometimento do backup tem nos resultados do ransomware. Ele também esclarece a frequência de comprometimento de backup em ataques de ransomware.

Visão geral da pesquisa

As descobertas são baseadas em uma pesquisa independente de fornecedor encomendada pela Sophos, com 2.974 profissionais de TI / segurança cibernética em 14 países cujas organizações foi atingido por ransomware no ano passado (2023). Conduzida pela agência de pesquisa independente Vanson Bourne em janeiro e fevereiro de 2024, a pesquisa reflete as experiências dos entrevistados nos 12 meses anteriores. Para mais detalhes sobre os entrevistados, consulte o apêndice no final do relatório.

Resumo Executivo

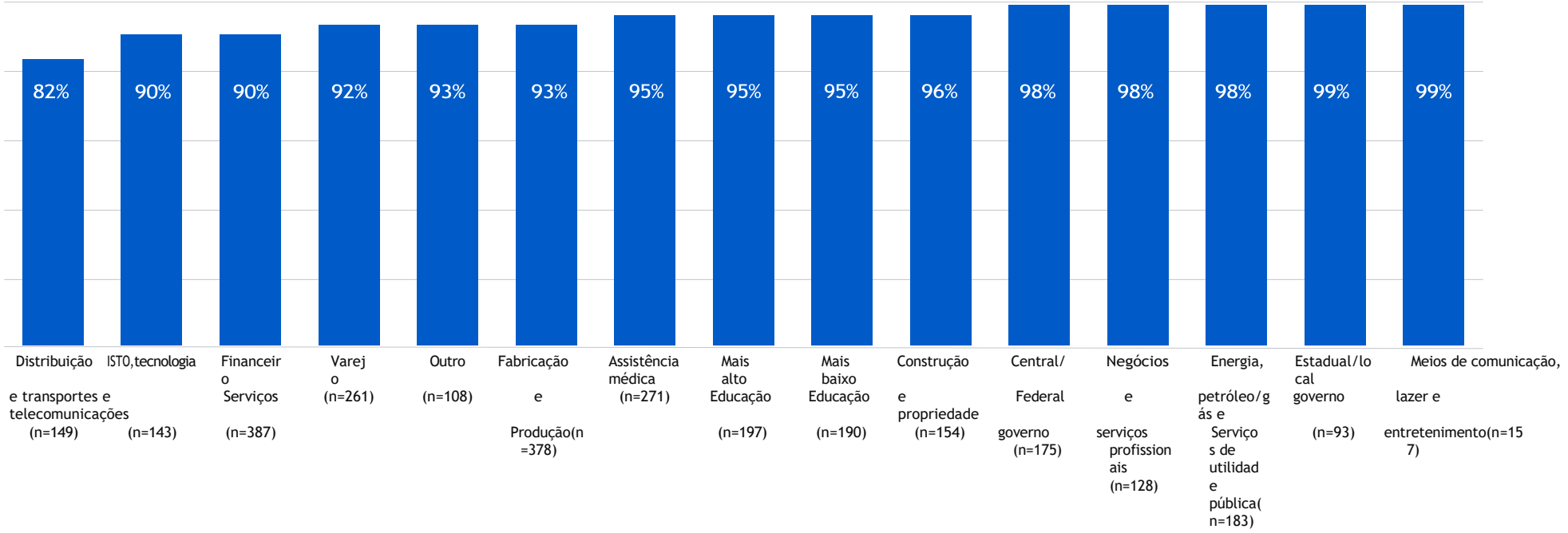
As implicações financeiras e operacionais de ter backups comprometidos num ataque de ransomware são imensas. Quando os invasores conseguem comprometer backups, uma organização tem quase duas vezes mais probabilidade de pagar o resgate e incorre em uma conta de recuperação geral oito vezes maior do que aquelas cujos backups não são afetados.

Detectar e impedir agentes mal-intencionados antes que seus backups sejam comprometidos permite reduzir consideravelmente o impacto de um ataque de ransomware em sua organização. Investir na prevenção do comprometimento do backup aumenta a resiliência do ransomware e, ao mesmo tempo, reduz o custo total de propriedade (TCO) geral da segurança cibernética.

Aprendizado 1: Os agentes de ransomware quase sempre tentam comprometer seus backups

94% das organizações atingidas por ransomware no ano passado afirmaram que os cibercriminosos tentaram comprometer os seus backups durante o ataque. Este número aumentou para 99%, tanto no governo estadual como local, e no setor de mídia, lazer e entretenimento. A taxa mais baixa de tentativas de comprometimento foi relatada pela distribuição e transporte, no entanto, mesmo aqui, mais de oito em cada dez (82%) organizações atingidas por ransomware disseram que os invasores tentaram acessar seus backups.

Porcentagem de ataques de ransomware em que os invasores tentaram comprometer backups



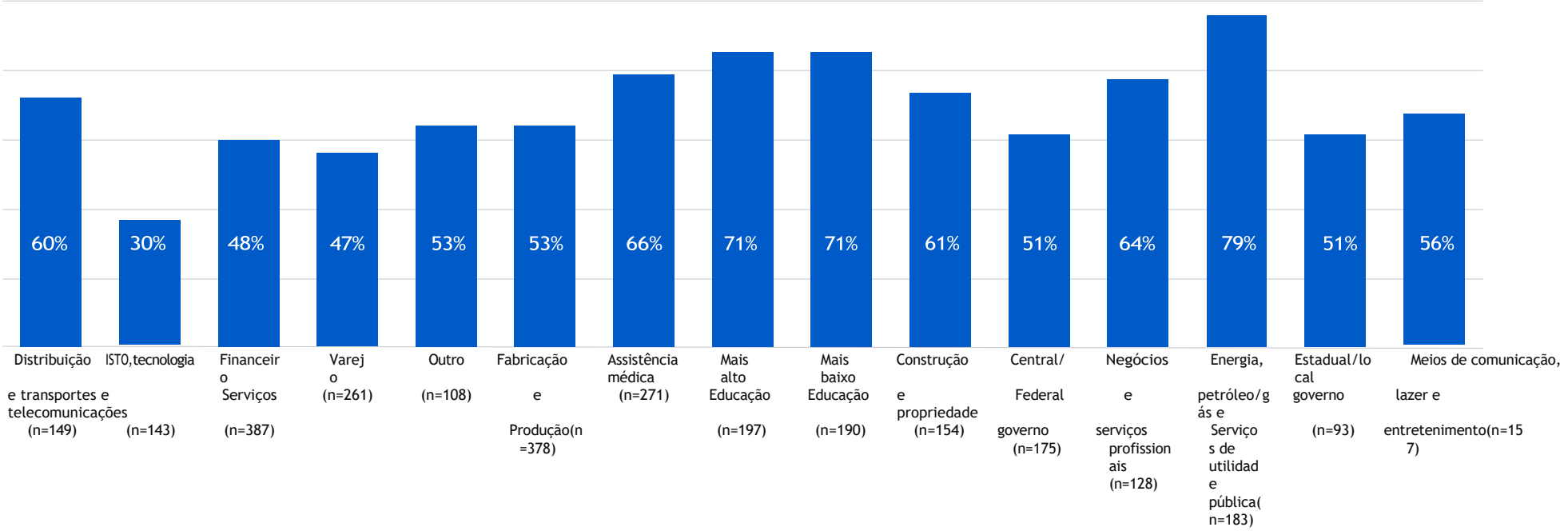
Aprendizado2:
A taxa de sucesso do comprometimento varia muito pela indústria

Em todos os setores, 57% das tentativas de comprometimento de backup foram bem-sucedidas, o que significa que os adversários conseguiram impactar as operações de recuperação de ransomware de mais da metade das suas vítimas. Curiosamente, a análise revelou uma variação considerável na taxa de sucesso do adversário por setor:

- Os invasores tinham maior probabilidade de comprometer com êxito os backups de suas vítimas nos setores de energia, petróleo / gás e serviços públicos (taxa de sucesso de 79%) e educação (taxa de sucesso de 71%).
- Por outro lado, TI, tecnologia e telecomunicações (taxa de sucesso de 30%) e varejo (taxa de sucesso de 47%) relataram as taxas mais baixas de comprometimento de backup bem-sucedido.

Existem várias razões possíveis por trás das diferentes taxas de sucesso. Pode ser que a TI, as telecomunicações e a tecnologia tivessem uma proteção de backup mais forte, para começar, por isso estavam mais capazes de resistir ao ataque. Eles também podem ser mais eficazes na detecção e interrupção de tentativas de comprometimento antes que os invasores tenham sucesso. Por outro lado, o setor de energia, petróleo / gás e serviços públicos pode ter sofrido uma percentagem mais elevada de ataques muito avançados. Qualquer que seja a causa, o impacto pode ser considerável.

Taxa de sucesso de tentativas de comprometimento de backup



Aprendizado3: Exigências de resgate e pagamentos dobram quando os backups são comprometidos

Dados criptografados
As organizações cujos backups foram comprometidos tinham 63% mais probabilidade de ter dados criptografados do que aquelas que não os tinham: 85% das organizações com backups comprometidos disseram que os invasores conseguiram criptografar seus dados, em comparação com 52% daquelas cujos backups não foram afetados. A taxa de encriptação mais elevada pode ser indicativa de uma resiliência cibernética global mais fraca, o que deixa as organizações menos capazes de se defenderem contra todas as fases do ataque de ransomware.

Pedido de resgate
As vítimas cujos backups foram comprometidos receberam pedidos de resgate que foram, em média, mais que o dobro daqueles cujos backups não foram afetados, com a demanda média de resgate chegando a US$ 2,3 milhões (backups comprometidos) e US$ 1 milhão (backups não comprometidos), respectivamente. É provável que os adversários sintam que estão numa posição mais forte se comprometerem os backups e, portanto, puderam exigir um pagamento mais elevado.

Taxa de pagamento do Resgate
As organizações cujos backups foram comprometidos tinham quase duas vezes mais probabilidade de pagar o resgate para recuperar dados criptografados do que aquelas cujos backups não foram afetados (67% vs. 36%).

Montante de pagamento de Resgate
O pagamento médio de resgate por organizações cujos backups foram comprometidos foi de US$ 2 milhões, quase o dobro daquelas cujos backups permaneceram intactos (US$ 1.062 milhões). Também foram menos capazes de negociar o pagamento do resgate, com aqueles cujos backups foram comprometidos pagando, em média, 98% da quantia exigida. Aqueles cujos backups não foram comprometidos conseguiram reduzir o pagamento para 82% da demanda.

Taxa de criptografia de dados

89%
quando os backups são comprometidos

52%
quando os backups não estão comprometidos

Demanda de resgate (mediana)

US$ 2,3 milhões quando os backups são comprometidos

US$ 1 milhão quando os backups não estão comprometidos

Resgate pago para recuperar dados

67%
quando os backups são comprometidos

36%
quando os backups não estão comprometidos

Pagamento de resgate (mediana)

US$ 2,3 milhões quando os backups são comprometidos

US$ 1,062 milhão quando os backups não estão comprometidos

Aprendizado 4:
Os custos gerais de recuperação de ransomware são 8 vezes maiores quando os backups são comprometidos

Nem todos os ataques de ransomware resultam no pagamento de um resgate. Mesmo quando isso acontece, os pagamentos de resgate são apenas parte dos custos gerais de recuperação ao lidar com um ataque de ransomware. As interrupções causadas por ransomware frequentemente têm um impacto considerável nas transações comerciais diárias, enquanto a tarefa de restaurar sistemas de TI é muitas vezes complexa e cara.

O custo médio geral de recuperação de ransomware para organizações cujos backups foram comprometidos (US$ 3 milhões) foi oito vezes maior do que o de organizações cujos backups não foram afetados (US$ 375 mil). Provavelmente há vários motivos por trás dessa diferença, entre eles o trabalho adicional que normalmente é necessário para restaurar dados descriptografados, em vez de backups bem preparados. Também pode ser que uma proteção de backup mais fraca seja indicativa de defesas menos robustas e de maior necessidade de trabalho de reconstrução resultante.

Aqueles cujos backups foram comprometidos também tiveram um tempo de recuperação consideravelmente mais longo, com apenas 26% totalmente recuperados em uma semana, em comparação com 46% daqueles cujos backups não foram afetados.

Custos gerais de recuperação de ransomware (Média)

US$ 3 milhões	quando os backups são comprometidos
US$ 0,375 milhões	quando os backups não estão comprometidos

Recomendações

Os backups são uma parte fundamental de uma estratégia holística de redução de riscos cibernéticos. Se seus backups estiverem acessíveis on-line, você deverá presumir que os adversários os encontrarão. As organizações seriam sábias se:

- Fizerem backups regulares e armazenar em vários locais. Certifique-se de adicionar MFA (autenticação multifator) às suas contas de backup na nuvem para ajudar a impedir que invasores obtenham acesso.
- Pratique a recuperação de backups. Quanto mais fluente você for no processo de restauração, mais rápido e fácil será a recuperação de um ataque.
- Proteja seus backups. Monitore e responda a atividades suspeitas em torno de seus backups, pois isso pode ser um indicador de que adversários estão tentando comprometê-los.

Como a Sophos pode ajudar

Sophos MDR: Nossos especialistas defendem seus backups

O Sophos MDR é um serviço gerenciado de detecção e resposta 24 horas por dia, 7 dias por semana, liderado por especialistas, especializado em impedir ataques avançados que a tecnologia por si só não pode evitar. O serviço amplia sua equipe de TI / segurança com mais de 500 especialistas que monitoram seu ambiente, detectando, investigando e respondendo a atividades e alertas suspeitos.

Os analistas de MDR da Sophos aproveitam a telemetria de sua solução de backup e recuperação para detectar e interromper tentativas de comprometimento de backup, neutralizando os agentes de ransomware antes que grandes danos sejam causados. Eles também recebem sinais das ferramentas de segurança que você já usa, incluindo soluções de endpoint, email e firewall, para detectar ransomware e violações. Com um tempo médio de resposta a ameaças de apenas 38 minutos, o Sophos MDR funciona mais rápido que sua próxima ameaça.

Sophos XDR: Dando às equipes de TI visibilidade e ferramentas para impedir invasores

As equipes internas podem usar o Sophos XDR para obter a visibilidade, os insights e as ferramentas necessárias para detectar, investigar e responder a ameaças em vários estágios, em todos os principais vetores de ataque, no menor tempo possível. Com o Sophos XDR você pode aproveitar a telemetria de sua solução de backup e recuperação, bem como de sua pilha de segurança mais ampla, para ver e responder rapidamente a ataques.

Apêndice

A pesquisa foi realizada em organizações de pequeno e médio porte com 100 a 5.000 funcionários em 14 países: Austrália, Áustria, Brasil, França, Alemanha, Índia, Itália, Japão, Cingapura, África do Sul, Espanha, Suíça, Reino Unido, Estados Unidos.

Revenda Autorizada
Tel: +55 21 2215 7892
sninformatica@sninformatica.com.br

SN Informatica Ltda
Tel: +55 21 2215 9681
https://www.sninformatica.rio/

Rio de Janeiro
Tel: +55 11 4950 8764
linktr.ee/sninformatica

Brazil
-
-

18/03/2024 (WP-NP)

SOPHOS