SOPHOS
Cybersecurity evolved.

O Estado do Ransomware nos Serviços Financeiros 2021

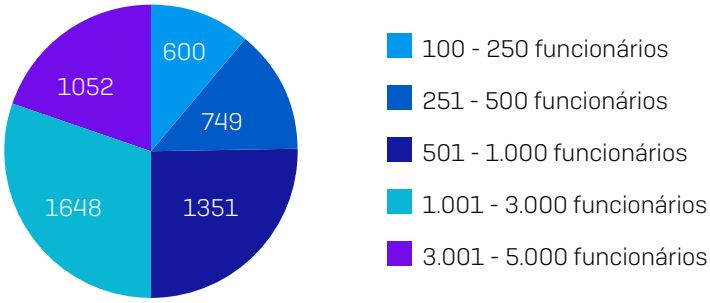
Com base em uma pesquisa independente com 550 tomadores de decisão de TI, este relatório compartilha novos insights do estado atual do ransomware no setor de serviços financeiros. Ele oferece um conhecimento aprofundado da predominância de ransomwares nos serviços financeiros, o impacto desses ataques nas vítimas, o custo de remediação do ransomware e como o setor se compara em termos de expectativas futuras e nível de preparo contra os ataques.

Documento técnico Sophos. Setembro, 2021

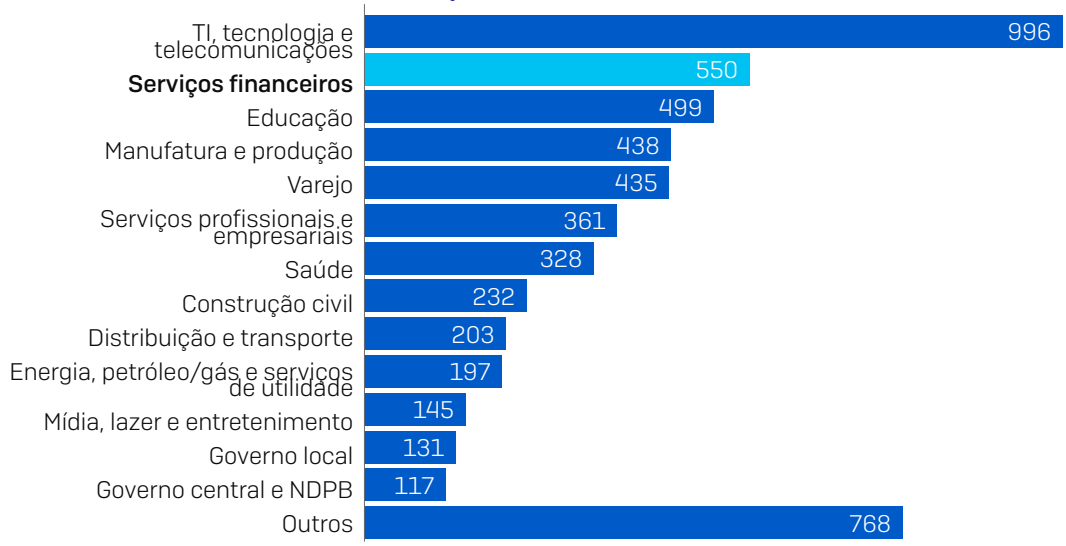
Sobre a pesquisa

A Sophos encarregou a firma de pesquisa de opinião independente Vanson Bourne de realizar uma pesquisa global com 5.400 gerentes de TI em 30 países. Os respondentes vieram de uma ampla gama de setores, incluindo 550 respondentes do setor de serviços financeiros. A pesquisa foi conduzida em janeiro e fevereiro de 2021.

Quantos funcionários a sua organização tem em âmbito global? [5.400]



Em que setor se encontra a sua organização? [5.400]



50% dos respondentes de cada país vieram de organizações com entre 100 e 1.000 funcionários e 50% vieram de organizações com entre 1.001 e 5.000 funcionários. Os 550 tomadores de decisão de TI da área de serviços financeiros vieram de todas as regiões geográficas pesquisadas: Américas, Europa, Oriente-Médio, África e Ásia-Pacífico.

Região	Nº de respondentes
Américas	146
Europa	197
Oriente Médio e África	78
Ásia-Pacífico	129

550 tomadores de decisão de TI em serviços financeiros

Principais descobertas nos serviços financeiros

- **34%** das organizações de serviços financeiros **foram atingidas por ransomware no último ano**
- **51%** das organizações atingidas por ransomware disseram que os **criminosos cibernéticos tiveram êxito na criptografia dos dados** no ataque mais significativo
- **25%** das que tiveram seus dados criptografados **pagaram o resgate para reaver seus dados** no ataque de ransomware mais significativo
- **62%** das que tiveram seus dados criptografados **usaram backups para restaurar os dados**
- **63% dos dados foram restaurados**, em média, após pagar o resgate, deixando mais de um terço dos dados inacessíveis
- **91%** das organizações de serviços financeiros **têm um plano de recuperação de incidente de malware**
- **A conta média para retificar um ataque de ransomware** no setor de serviços financeiros, considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago e outros fatores, foi de **US$ 2,10 milhões**

Ransomware é uma realidade dura para o setor de serviços financeiros. Aproximadamente um terço (34%) das organizações foram atingidas por ransomware no último ano – ainda que esteja abaixo da média global de 37%, não deixa de ser preocupante.

Um quarto (25%) das organizações de serviços financeiros cujos dados foram criptografados pagaram o resgate para reaver seus dados. Nesse caso também, o índice ficou abaixo da média entre setores de 32%, provavelmente devido à capacidade acima da média que o setor tem em restaurar dados de backups. Observamos que os serviços financeiros estão colhendo os benefícios de terem planos de continuidade de negócios e recuperação de desastres (BC-DR), que os prepara para situações como ataques de ransomware. Considerando-se que as organizações que pagaram o resgate recuperaram, em média, apenas 63% de seus dados, as instituições financeiras demonstram sensatez ao focar nos backups como o principal meio de recuperação de dados.

No geral, os serviços financeiros se sobressaem como o único setor em que todas as organizações que tiveram seus dados criptografados conseguiram reaver pelo menos parte deles. Mais uma vez, parece que o trabalho de recuperação de desastre das organizações financeiras as preparou bem para um ataque de ransomware.

Os serviços financeiros também estão abaixo da média quando se trata do real valor dos resgates pagos: um pagamento médio de US$ 69.369,00 comparado à média entre setores de US$ 170.404,00. Observação: o número de base de respondentes em serviços financeiros não foi suficiente para oferecer uma interpretação sólida.

Aqui acabam as boas notícias para o setor. O custo médio de recuperação de ransomware para os serviços financeiros fica em torno de um quarto de milhão de dólares acima da média global (US$ 2,10 milhões x US$ 1,85 milhão). Isso talvez se deva aos altos gastos com medidas de correção para manter suas transações em operação a qualquer custo, e aos altos custos de notificar a violação de dados, os danos à reputação e as penalidades regulamentares que causam impacto no setor.

Adicionalmente, dois terços (68%) das equipes de TI em serviços financeiros disseram que a carga de trabalho com a segurança cibernética aumentou em 2020, provavelmente devido à necessidade de apoiar a rápida mudança para o trabalho em casa gerada pela pandemia. Ainda que isso afete a capacidade das equipes de TI de encontrar e responder rapidamente às questões de segurança cibernética, o lado bom disso é que 70% das equipes de TI disseram que a capacidade de desenvolvimento de suas equipes em relação às suas habilidades e conhecimentos aumentou no decorrer do ano, dando-lhes uma boa base para enfrentar o futuro.

As organizações de serviços financeiros deveriam continuar a investir em backups e em seus esforços de recuperação de desastres para minimizar o impacto de um ataque. Deveriam também pensar em ampliar suas defesas anti-ransomware, combinando tecnologia com a caça a ameaças conduzida por humanos para neutralizar os ataques avançados atuais conduzidos por humanos.

A prevalência do ransomware nos serviços financeiros

Serviços financeiros atingidos por ransomware no último ano

De um total de 550 respondentes de serviços financeiros que foram pesquisados, 34% foram atingidos por ransomware no ano passado – definido como *vários computadores impactados por um ataque de ransomware, mas não necessariamente criptografados.*

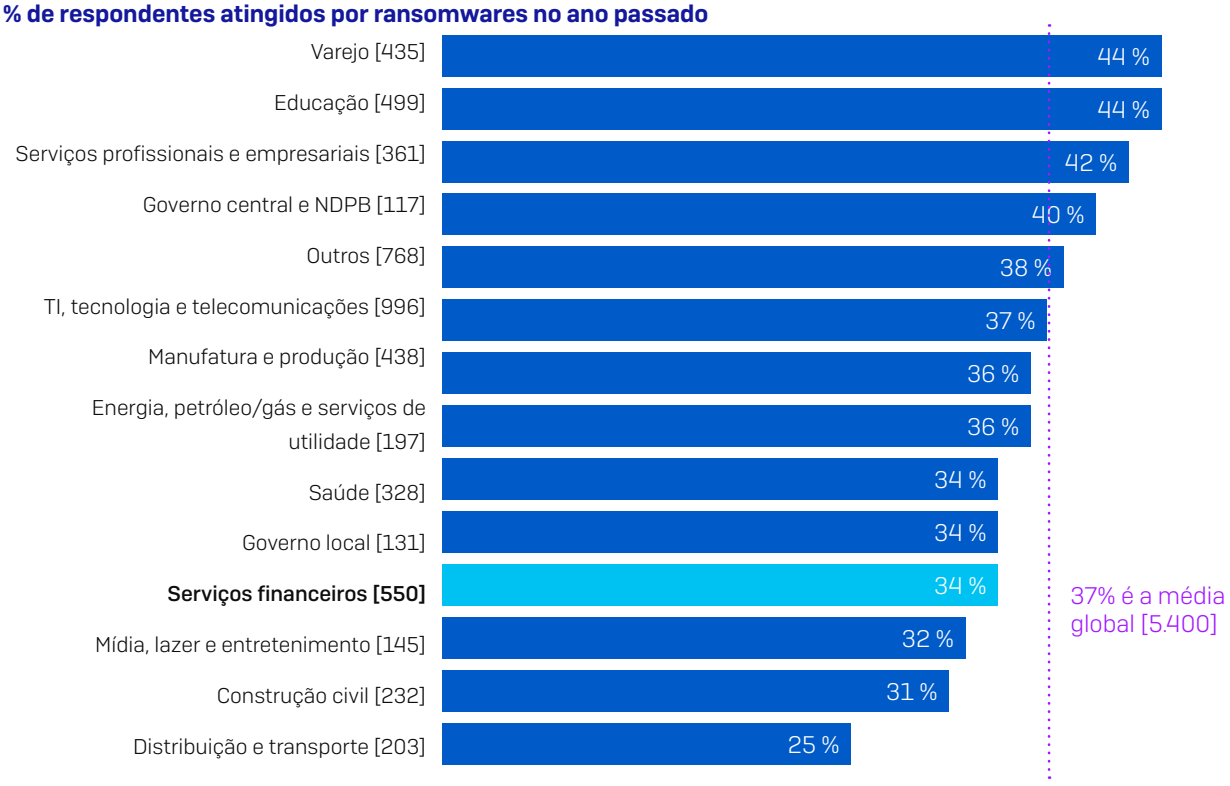
Sua organização foi atingida por ransomware neste último ano? [550 respondentes de serviços financeiros]

Entre as organizações que não foram atingidas no último ano, 42% disseram que esperam ser atingidas por ransomware no futuro, enquanto 22% se mostraram confiantes que estão protegidas contra futuros ataques. Iremos nos aprofundar mais nos motivos por trás da expectativa de serem atingidos no futuro e também falar sobre o que deixa os outros confiantes em face aos ataques futuros, mais adiante neste relatório.

Serviços financeiros abaixo da média global para ransomware

Quando comparamos os serviços financeiros com outros setores, notamos que realmente houve índices de ataque abaixo da média. Varejo e educação exibiram o mais alto índice de ataques de ransomware, com 44% dos respondentes nesses setores registrando que foram atingidos em comparação com a média global de 37%.

% de respondentes atingidos por ransomwares no ano passado



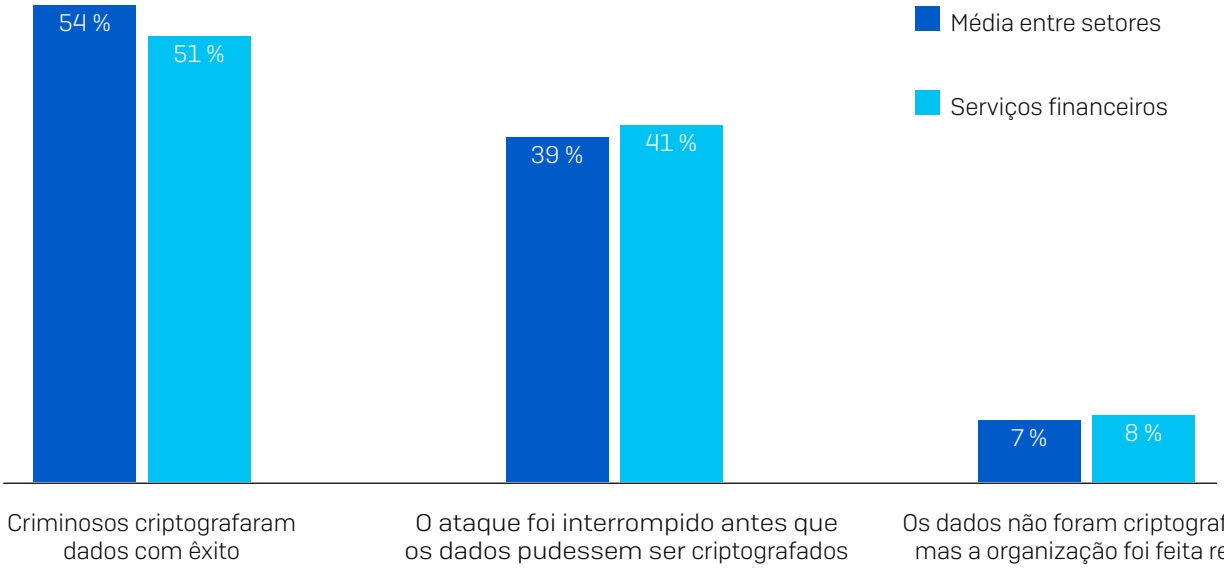
Sua organização foi atingida por ransomware neste último ano? Sim [números de base no gráfico], omitindo algumas opções de resposta, dividido por setor

Globalmente, entre todos os setores, a porcentagem de organizações atingidas por ransomware no ano passado caiu consideravelmente em relação ao ano anterior, quando 51% admitiram ter sido atingidas. Ainda que uma queda nos valores seja bem-vinda, provavelmente isso se dá, em parte, pelo comportamento evolutivo dos invasores observado pelo SophosLabs e pela equipe do Sophos Managed Threat Response. Por exemplo, muitos invasores mudaram dos ataques automatizados generalizados e em grande escala para ataques mais direcionados que incluem a manipulação fraudulenta realizada por humanos com as mãos no teclado. Enquanto o número de ataques em geral está menor, nossa experiência mostra que o potencial para danos desses ataques direcionados é muito maior.

O impacto dos ransomwares

Capacidade dos serviços financeiros de parar a criptografia de dados

Perguntamos aos respondentes cujas organizações foram atingidas por ransomware no ano passado se os criminosos cibernéticos obtiveram êxito na criptografia dos dados. 51% dos respondentes de serviços financeiros responderam que sim, um pouco abaixo da média global de 54%.



Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização nos ataques de ransomware mais significativos? [2006/185 das organizações de serviços financeiros que foram atingidas por ransomware no último ano]

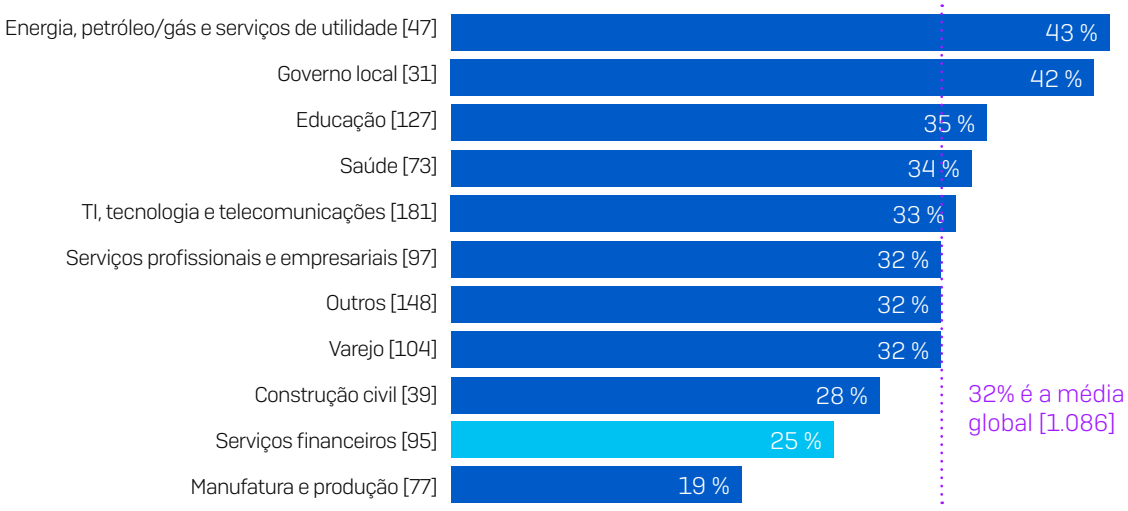
Ainda que o setor de serviços financeiros tenha obtido melhor êxito para interromper a criptografia do que a média global (41% dos ataques foram interrompidos em comparação com a média de 39%), esse também foi o setor mais vulnerável a uma nova tendência que está surgindo: ataques de extorsão apenas, quando os operadores do ransomware não criptografam os arquivos, mas ameaçam divulgar online as informações roubadas se o resgate não for pago. De fato, 8% das organizações de serviços financeiros que foram atingidas por ransomware passaram por um ataque de extorsão.

O SophosLabs registrou um aumento nesse estilo de ataque durante o último ano. Esse ataque requer menos esforços da parte dos invasores, já que eles não precisam criptografar nem descriptografar dados, e os adversários geralmente equiparam o valor das multas por violação de dados em suas demandas, em uma tentativa a mais de forçar suas vítimas a pagar.

Propensão a pagar o resgate

A pesquisa revelou que os serviços financeiros têm uma propensão bem menor a pagar um resgate do que a maioria dos outros setores. Uma em cada quatro organizações de serviços financeiros (25%) cujos dados foram criptografados se submeteu às demandas de resgate, comparado com a média entre setores de 32%. Um provável motivo para isso, como discutimos acima, é a incrível capacidade que o setor tem para restaurar dados usando backups.

% que pagou resgate para reaver os dados



Sua organização conseguiu reaver os dados capturados no ataque de ransomware mais significativo? Sim, pagamos o resgate [números de base no gráfico] organizações em que os criminosos cibernéticos tiveram êxito na criptografia dos dados no ataque de ransomware mais significativo, omitindo algumas opções de resposta, dividido por setor

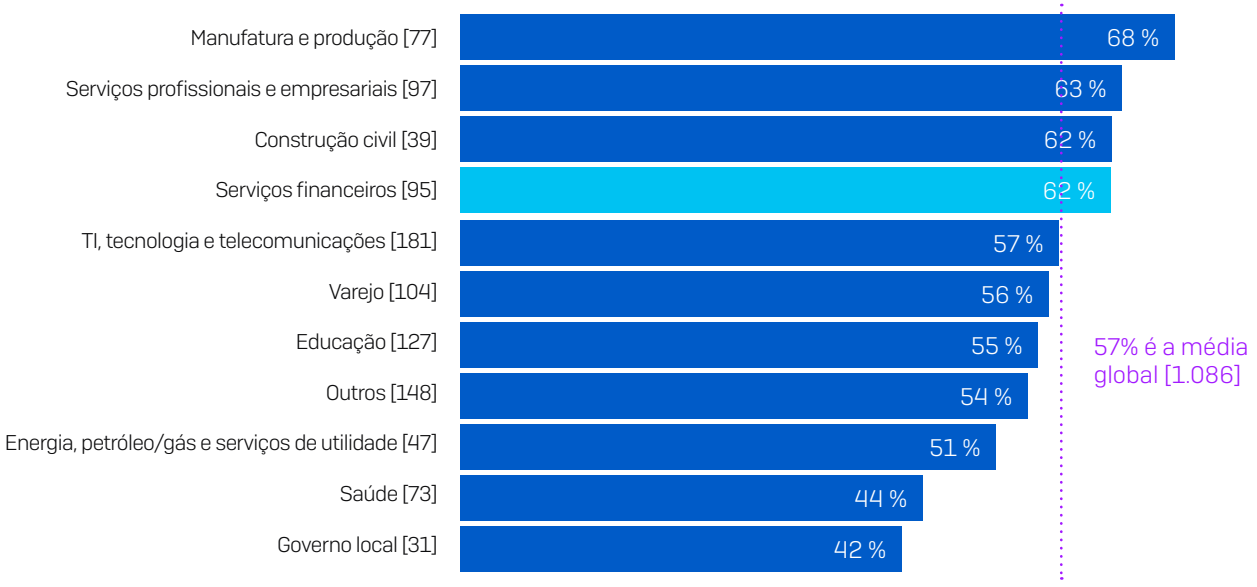
Entre os setores, **energia, petróleo/gás e serviços de utilidade** é o mais propenso a pagar o resgate, com 43% aceitando a demanda de resgate. Esse setor normalmente tem um legado estrutural intenso que não pode ser facilmente atualizado, assim as vítimas se sentem coagidas a pagar o resgate para possibilitar a continuidade dos serviços.

Governo local registra o segundo mais alto índice de pagamento de resgate (42%). Esse também é o setor mais propenso a ter seus dados criptografados. Pode ser também que a propensão de as organizações de governo local pagarem leve os invasores a focar seus ataques mais complexos e eficazes nesse público.

Capacidade de restaurar dados usando backups

Quando comparamos esta seção com a anterior, a correlação entre capacidade de restaurar dados de backups e propensão a pagar ransomware fica claramente visível, com esses setores se mostrando os mais preparados para usar backups e também os menos propensos a pagar resgates.

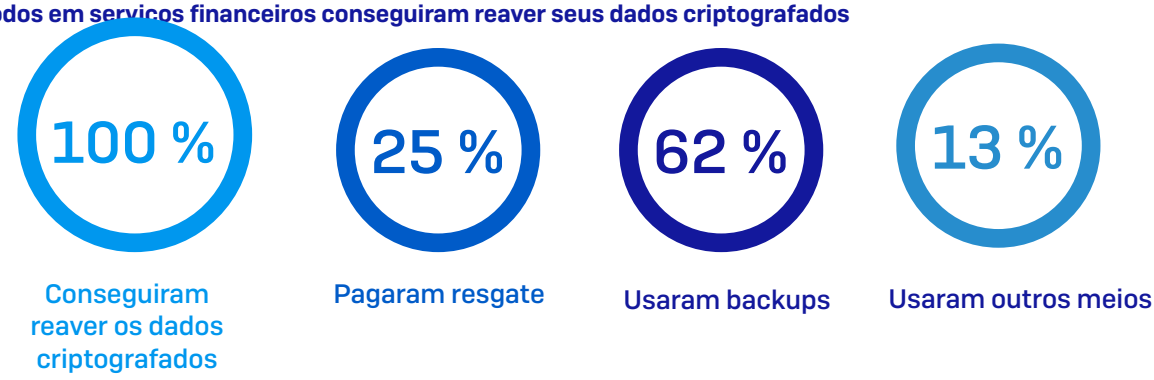
% que usou backups para restaurar dados criptografados



Sua organização conseguiu reaver os dados capturados no ataque de ransomware mais significativo? Sim, usamos backups para restaurar os dados [números de base no gráfico] organizações em que os criminosos cibernéticos tiveram êxito na criptografia dos dados no ataque de ransomware mais significativo, omitindo algumas opções de resposta, dividido por setor

Os respondentes de serviços financeiros (62%) estavam entre os mais capacitados para restaurar dados criptografados usando backups. Provavelmente, isso ocorre porque os bancos e muitas outras organizações de serviços financeiros sejam obrigados a ter planos de continuidade dos negócios e recuperação de desastres (BC-DR) a fim de evitar grandes perdas na eventualidade de um desastre ou uma violação de dados. A falta de um plano pode resultar em multas e/ou penalidades no FDIC. Criar backups e praticar a restauração de dados usando esses backups seria parte integral de qualquer bom plano.

Todos em serviços financeiros conseguiram reaver seus dados criptografados

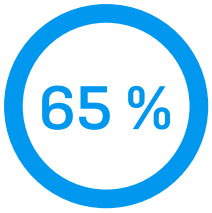


Sua organização conseguiu reaver os dados capturados no ataque de ransomware mais significativo? [95] organizações de serviços financeiros em que os criminosos cibernéticos tiveram sucesso na criptografia de dados no ataque de ransomware mais significativo.

A boa notícia para os serviços financeiros é que eles foram o único setor em que todas as organizações cujos dados foram criptografados puderam recuperá-los. Como observamos, 25% pagaram o resgate, 62% usaram backups e 13% usaram outros meios para reaver seus dados.

Pagar o resgate recupera apenas parte dos seus dados

Aqueles que pagaram o resgate, contudo, não conseguiram reaver todos os dados. O que os invasores deixam de dizer quando fazem suas demandas de regaste é que, mesmo que você pague, as chances de reaver todos os seus dados são ínfimas.

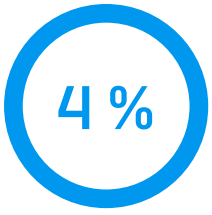


Porcentagem de dados recuperados após pagar o resgate
MÉDIA ENTRE SETORES

Porcentagem de dados recuperados após pagar o resgate
MÉDIA EM SERVIÇOS FINANCEIROS

Quantidade média de dados que as organizações conseguiram reaver no ataque de ransomware mais significativo. [344/24] organizações que pagaram o resgate para reaver seus dados

O número de base de respondentes em serviços financeiros não foi suficiente para oferecer uma interpretação sólida. Porém, como demonstrativo, os respondentes de serviços financeiros registraram reaver uma média de 63% de seus dados após pagar o resgate, deixando mais de um terço dos dados inacessíveis, um pouco abaixo da média global (65%). Não que isso seja uma manobra deliberada dos hackers, porém uma reflexão: os adversários dedicam mais tempo e esforços no desenvolvimento de ferramentas de criptografia fortes do que em ferramentas de descriptografia.



Recuperaram TODOS os dados

Recuperaram metade dos dados ou menos

Quantidade de dados que as organizações conseguiram reaver no ataque de ransomware mais significativo. [24] organizações de serviços financeiros que pagaram o resgate para reaver seus dados

Para enfatizar esse ponto, apenas 4% das organizações de serviços financeiros que pagaram resgate recuperaram **todos** os seus dados, e 33% recuperaram **metade ou menos** dos dados. Claramente, pagar o resgate não ajuda. De novo, o número de base dos serviços financeiros é um pouco baixo, devendo ser considerado meramente indicativo.

O custo do ransomware

Revelado o pagamento dos resgates

Dos 357 respondentes entre os setores que relataram que suas organizações pagaram o resgate, 282 também mencionaram a quantia exata que foi paga.

US$ 170.404,00

Pagamento médio GLOBAL de resgate

Qual foi o resgate que a sua organização pagou no ataque de ransomware mais significativo? [282] organizações que pagaram o resgate para reaver seus dados

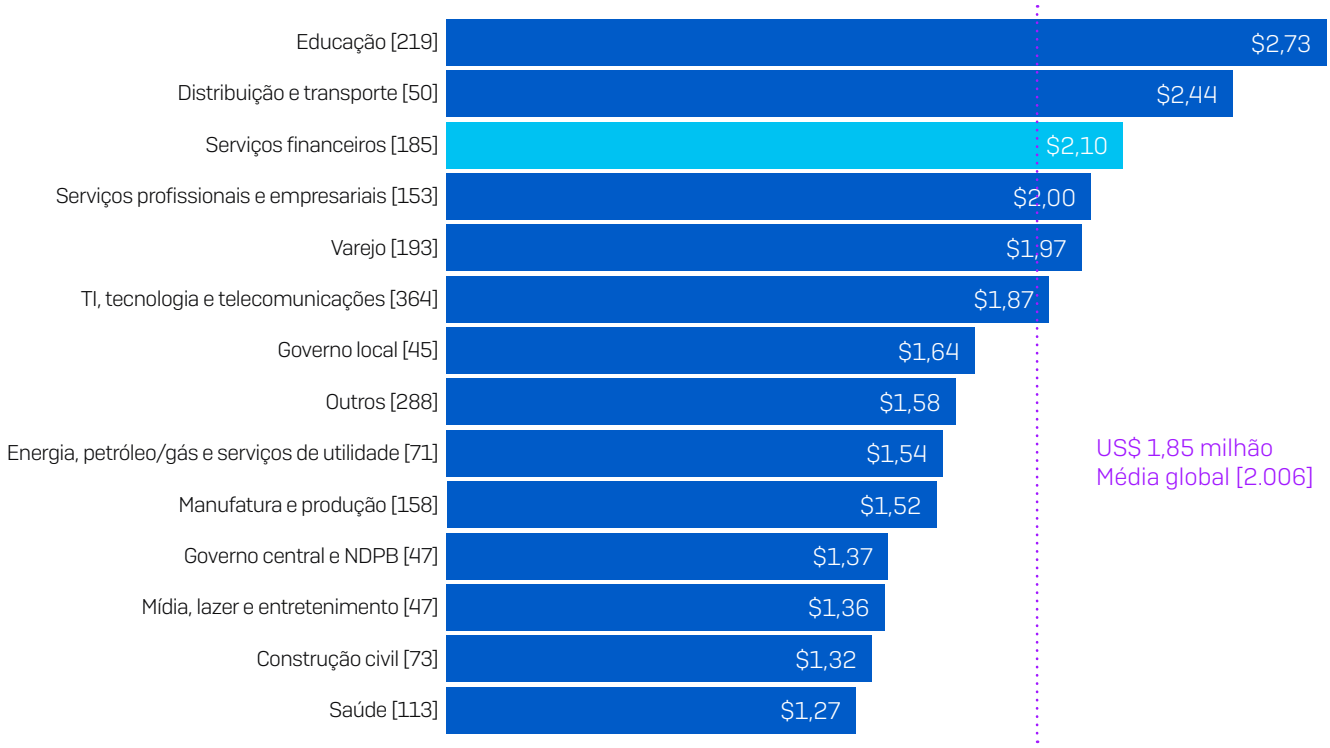
Globalmente, **entre todos os setores**, o pagamento médio de resgate foi de US$ 170.404,00. 13 respondentes em organizações de **serviços financeiros** compartilharam os pagamentos reais de resgaste, com um pagamento médio de resgate chegando a US$ 69.369,00, mais de US$ 100.000,00 abaixo da média global. O baixo índice de pagamento pode ser devido, em parte, à grande aptidão desse setor em restaurar dados usando backups. Além disso, pagar o resgate pode expor as organizações de serviços financeiros a um aumento em riscos legais e de conformidade, incluindo contravenções às leis de prevenção à lavagem de dinheiro (AMC) e de combate ao financiamento de terrorismo (CFT).

Esses números variam bastante dos valores em dólar de oito casas que dominaram as manchetes por diferentes motivos.

1. **Tamanho da organização**. Nossos respondentes são organizações de médio porte, com entre 100 e 5.000 usuários que, em geral, têm menos recursos financeiros do que as grandes organizações. Os agentes de ransomware ajustam suas demandas de resgate de modo a refletir a capacidade de pagamento de suas vítimas, e normalmente aceitam pagamentos mais baixos das empresas menores. Os dados confirmam: a média de pagamento de resgate por organizações com 100 a 1.000 funcionários atingiu a marca de US$ 107.694,00, enquanto o resgate médio pago por organizações com 1.001 a 5.000 funcionários é de US$ 225.588,00.
2. **A natureza do ataque**. Existem muitos agentes de ransomware e muitos tipos de ataques de ransomware, variando entre invasores mais bem equipados, que utilizam táticas, técnicas e procedimentos (TTPs) sofisticados que focam em alvos individuais, e operadores com poucas habilidades, que usam ransomwares "pré-prontos" e uma abordagem geral do tipo "spray and pray". Os invasores que investem pesado em um ataque direcionado buscarão altos resgates em pagamento por seus esforços, enquanto os operadores por trás dos ataques mais comuns geralmente aceitam menores retornos sobre seus investimentos (ROI).
3. **Localização**. Como vimos no início, essa pesquisa cobriu 30 países mundialmente, com índices variados de PIB. Os invasores visam suas mais altas demandas de resgate às economias ocidentais desenvolvidas, motivados pelo entendimento de que podem pagar altas somas. Os dois resgates mais altos pagos foram relatados por respondentes na Itália. De modo recíproco, na Índia, o pagamento médio de resgate foi de US$ 76.619,00, menos da metade do número global (base: 86 respondentes).

Custo de recuperação de ransomware nos serviços financeiros

O resgate é apenas uma pequena parte do custo geral para se recuperar de um ataque de ransomware. As vítimas enfrentam uma extensa lista de custos adicionais, incluindo despesas com a reconstrução e proteção de seus sistemas de TI, relações públicas e análises forenses.



Média aproximada do custo para as organizações retificarem o impacto do mais recente ataque de ransomware [considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago etc.] [números de base no gráfico] respondentes cuja organização foi atingida por ransomware no último ano, dividido por setor

A pesquisa revelou que o setor de serviços financeiros apresentou um custo médio de remediação de ransomware de US$ 2,10 milhões (considerando-se período de inatividade, horas perdidas, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago, multas e penalidades regulamentares etc.), consideravelmente mais alto do que a média global de US$ 1,85 milhão.

Há uma variedade de fatores prováveis por trás disso. Primeiramente, as organizações de serviços financeiros detêm uma grande quantidade de dados altamente sigilosos sobre pessoas físicas, empresas e entidades públicas, o que incorre em altos custos de notificação de violação de dados como parte do trabalho de remediação. Em segundo lugar, a interrupção nas operações das organizações de serviços financeiros pode causar uma desordem global. Isso coloca uma imensa pressão nas empresas para voltarem a operar o mais rapidamente possível, a qualquer custo.

Além disso, o setor de serviços financeiros é um dos mais regulamentados do mundo. As organizações devem aderir a uma infinidade de regulamentações, incluindo SOX, GDPR e PCI DSS, as quais aplicam altas penalidades por não conformidade. Multas punitivas por violações de dados incorrem como parte de um ataque de ransomware, adicionando aos custos gerais de recuperação.

Por último, com a facilidade que os clientes costumam ter de mudar de provedores, as organizações de serviços financeiros estão totalmente expostas ao impacto dos danos à reputação, incluindo perda de clientes e cancelamento de contas.

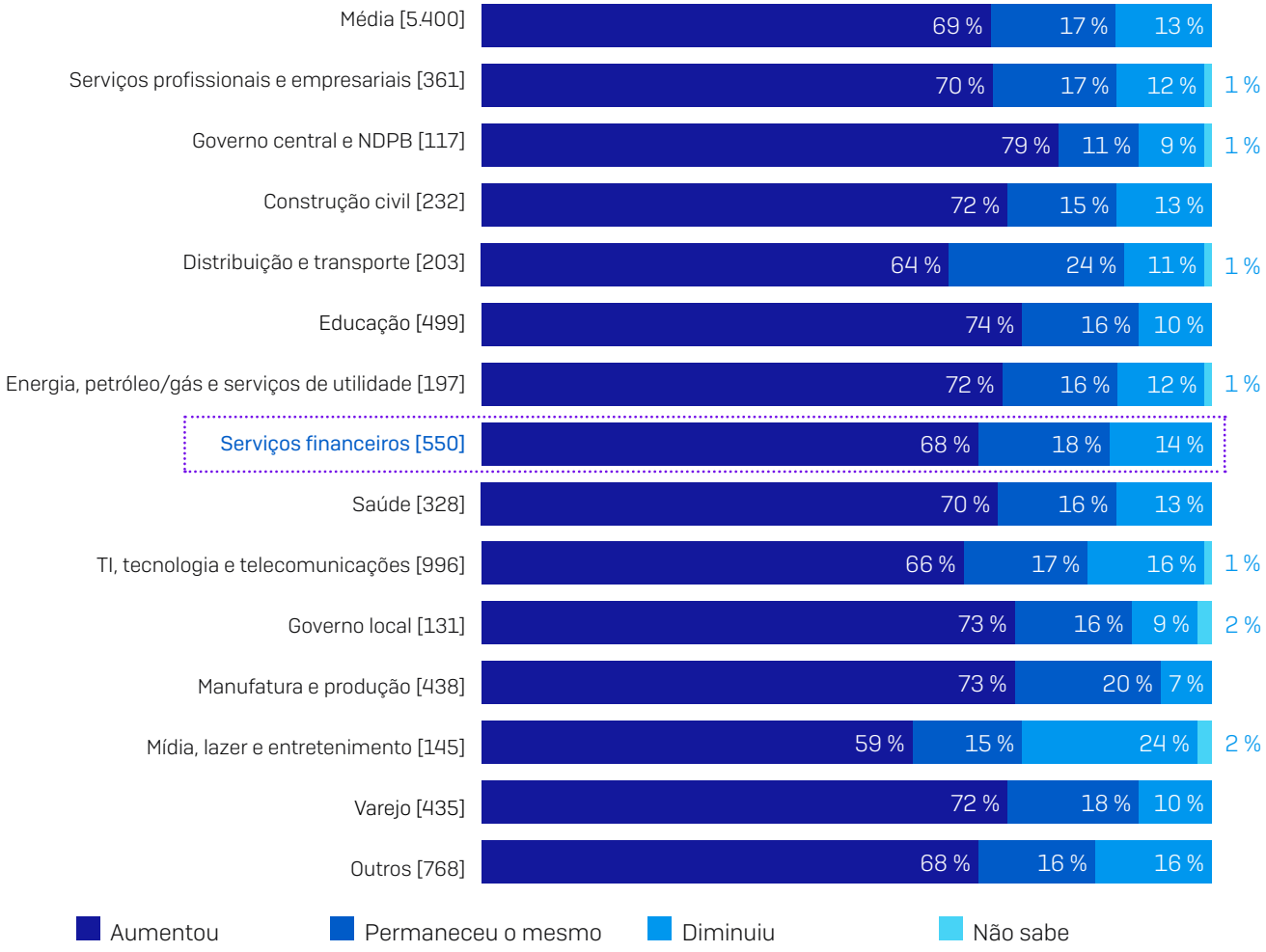
Ransomware é apenas uma parte do desafio da segurança cibernética

Ransomware é um problema importante de segurança cibernética para as organizações de serviços financeiros, mas não é o único. As equipes de TI já lidam com altas demandas em segurança cibernética, e o desafio que enfrentam foi exacerbado pela pandemia.

A carga de trabalho de segurança cibernética aumentou em 2020

As equipes de TI no setor de serviços financeiros foram duramente afetadas pela pandemia, com 68% sentindo um aumento na carga de trabalho de segurança cibernética no decorrer de 2020. Enquanto a maioria dos respondentes em todos os setores relatou um aumento, o governo central sentiu o maior aumento na carga de trabalho.

Como a carga de trabalho de segurança cibernética mudou no decorrer de 2020



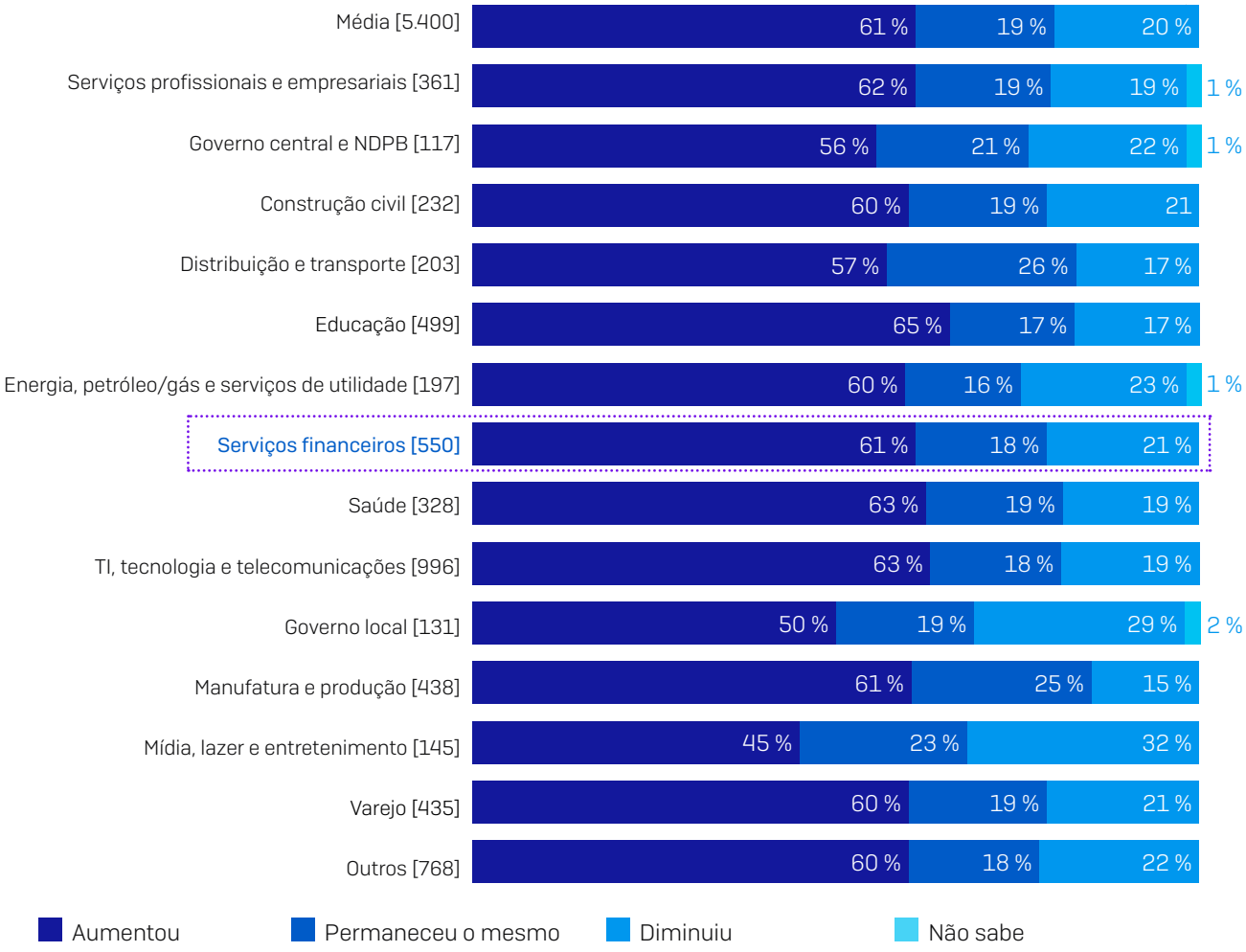
Durante o ano de 2020, nossa carga de trabalho de segurança cibernética diminuiu/aumentou/permaneceu a mesma [tamanhos de base no gráfico], dividido por setor

A rápida mudança para o trabalho remoto e a necessidade de lançar serviços e soluções adicionais para os funcionários, bem como para os clientes, no ímpeto de manterem suas operações, foi provavelmente um fator principal por trás do aumento da carga de trabalho para as equipes de TI. Esse foco intenso na proteção das novas plataformas online muito provavelmente reduziu a capacidade das equipes de TI de monitorar e responder a ameaças de ransomware.

O aumento na carga de trabalho desacelerou o tempo de resposta

Uma das consequências do aumento na carga de trabalho de segurança cibernética no decorrer de 2020 foi a lentidão no tempo de resposta a questões pertinentes à TI. O setor de serviços financeiros foi consideravelmente afetado, com 61% dos respondentes registrando que o tempo de resposta aumentou no último ano.

Mudanças no tempo de resposta aos casos de TI no decorrer de 2020



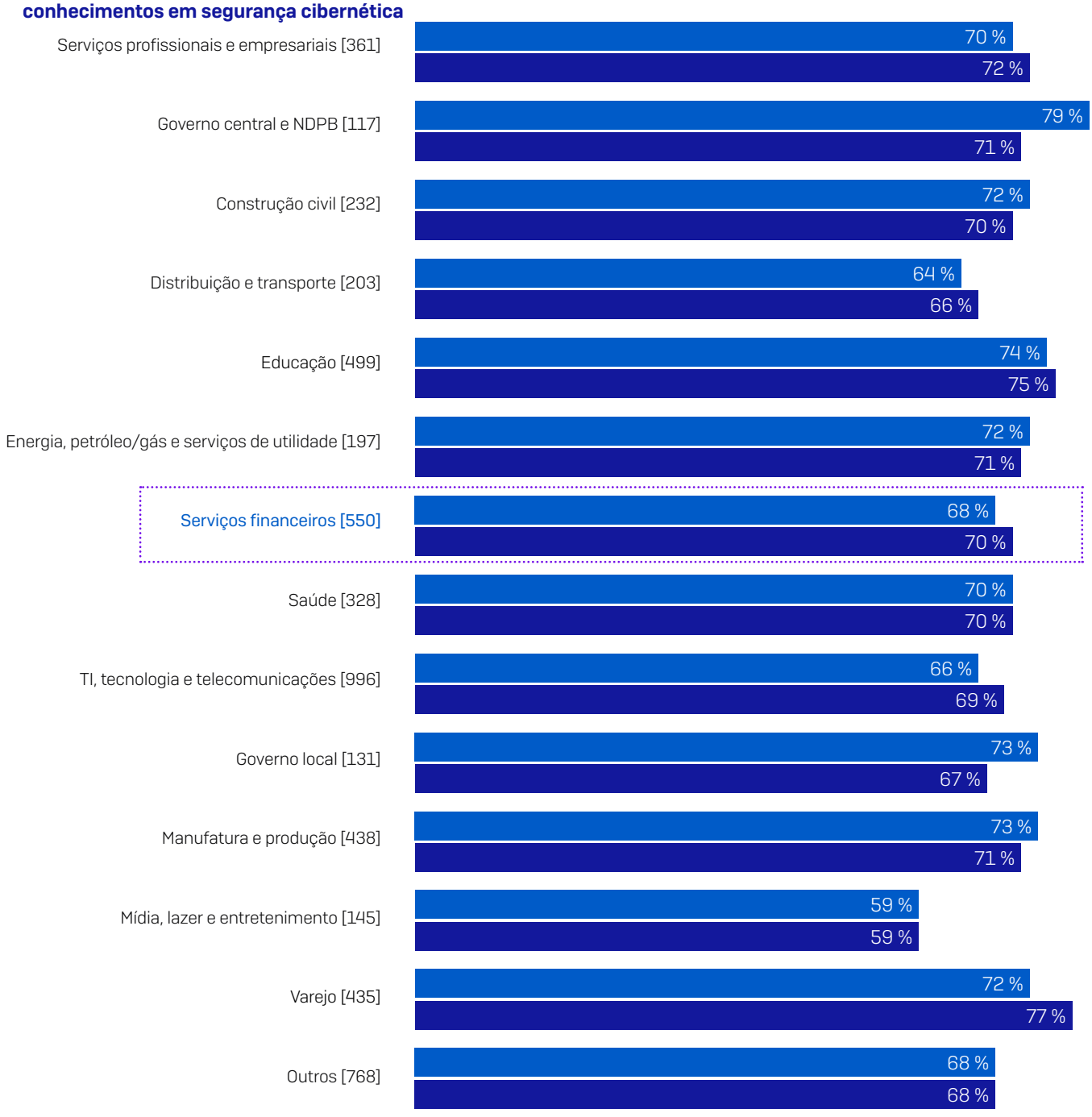
Durante o ano de 2020, nosso tempo de resposta aos casos de TI diminuiu/aumentou/permaneceu o mesmo. [tamanhos de base no gráfico], dividido por setor

Quando um adversário se aloja no seu ambiente, é imperativo bloqueá-lo o mais rápido possível. Quanto mais tempo ele tiver para explorar a sua rede e acessar os seus dados, maior será o impacto financeiro e operacional do ataque. A lentidão no tempo de resposta é, portanto, motivo para alarme.

Aumento na carga de trabalho aumentou habilidades e conhecimentos

Por trás de toda nuvem sempre há um raio de sol. Também existe uma clara correlação entre o aumento na carga de trabalho de segurança cibernética e o aumento na capacidade de desenvolver habilidades e conhecimentos em segurança cibernética.

Aumento na carga de trabalho de segurança cibernética e aumento na capacidade de desenvolver habilidades e conhecimentos em segurança cibernética



Durante o ano de 2020, nossa carga de trabalho de segurança cibernética/nossa capacidade de desenvolver nossas habilidades e conhecimentos em segurança cibernética aumentou [tamanhos de base no gráfico], dividido por setor

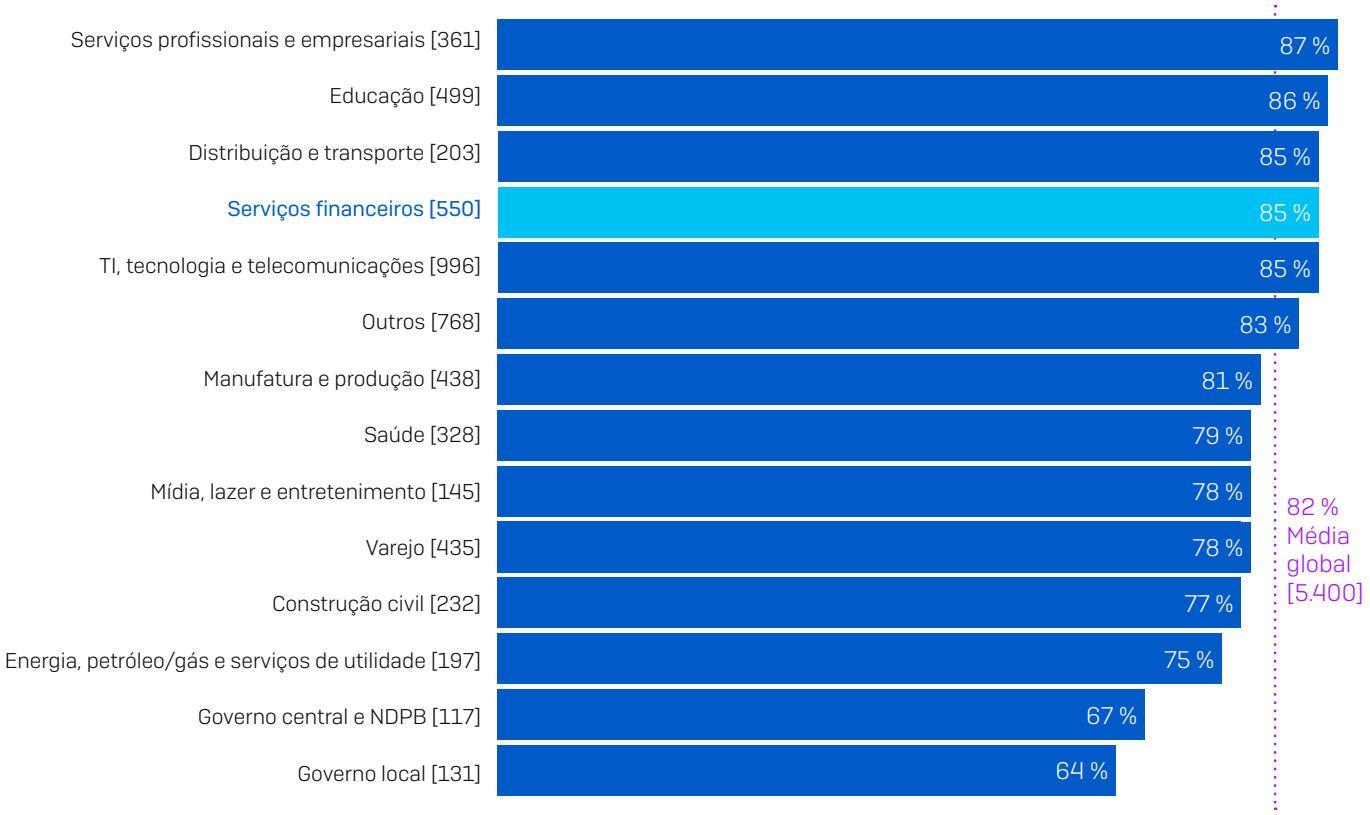
70% das equipes de TI na área de serviços financeiros disseram que a capacidade de desenvolvimento das suas habilidades e conhecimentos aumentou no decorrer de 2020.

Enquanto o aumento na carga de trabalho aumenta a pressão, ele também proporciona mais oportunidades para aprender coisas novas. É provável que as circunstâncias únicas da pandemia tenham exigido das equipes de TI posicionamentos e decisões nunca antes solicitados.

Preparo para enfrentar desafios futuros

85% dos respondentes em serviços financeiros concordam que, se detectarem atividades suspeitas em suas organizações, terão as ferramentas e os conhecimentos necessários para investigá-las completamente – mais alto que a média global (82%). A notícia é muito boa para o setor, considerando-se o aumento na carga de trabalho em segurança cibernética que sofreram. Ter o conhecimento e as ferramentas certas é a chave para investigar e tratar de ameaças cibernéticas.

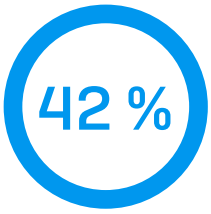
Têm as ferramentas e conhecimentos para investigar a atividade suspeita



Se eu detectar atividades suspeitas na minha organização, terei as ferramentas e os conhecimentos necessários para investigá-las completamente: Concordo totalmente, Concordo. Omitindo algumas opções de resposta [tamanhos de base no gráfico], dividido por setor

O futuro

Expectativas dos serviços financeiros sobre ataques futuros



Esperam ser atingidos por ransomware no futuro

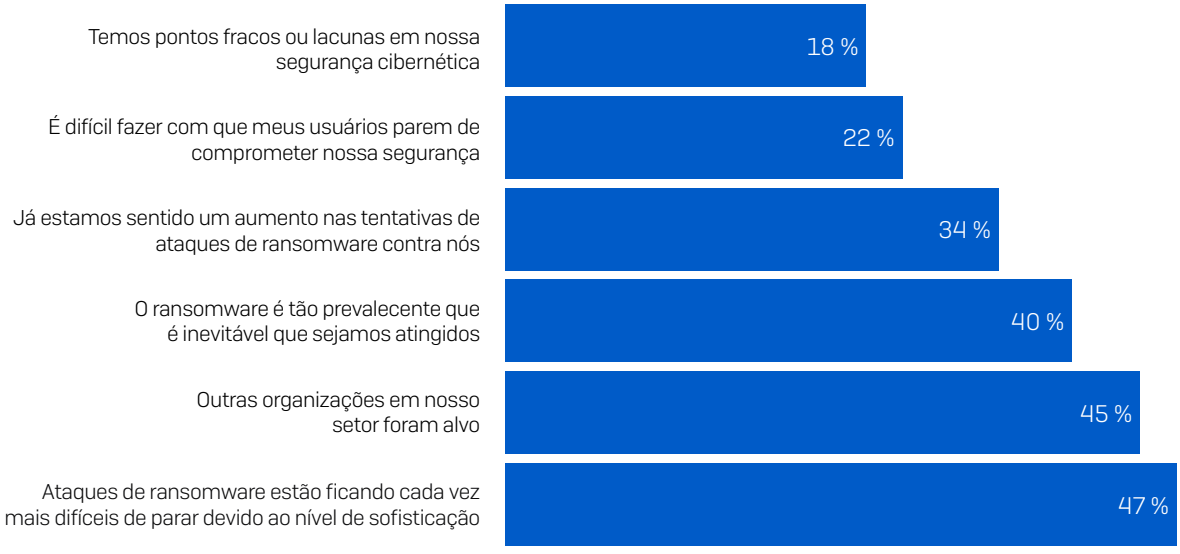
Não esperam ser atingidos por ransomware no futuro

[550] Respondentes dos serviços financeiros que responderam "Não" à pergunta "Sua organização foi atingida por ransomware neste último ano?"

Vimos anteriormente neste documento que 63% dos respondentes do setor de serviços financeiros não foram atingidos por ransomware no último ano. 42% esperam ser atingidos por ransomware no futuro. De modo recíproco, 22% não preveem um ataque.

Por que o setor de serviços financeiros espera ser atingido

Entre as organizações de serviços financeiros que não foram atingidas por ransomware, mas que esperam ser atingidas no futuro, o motivo mais comum (47%) é que os ataques de ransomware estão ficando cada vez mais difíceis de parar devido ao nível de sofisticação. Ainda que esse seja um número alto, o fato de que essas organizações estão atentas ao detalhe de o ransomware estar ficando cada vez mais avançado é positivo e pode ter sido um fator contribuinte de terem sido capazes de bloquear possíveis ataques de ransomware no ano passado com sucesso.



Por que você espera que a sua organização seja atingida por ransomware no futuro? [229 organizações de serviços financeiros que não foram atingidas por ransomware no ano passado, mas que esperam ser atingidas no futuro, omitindo algumas opções de resposta]

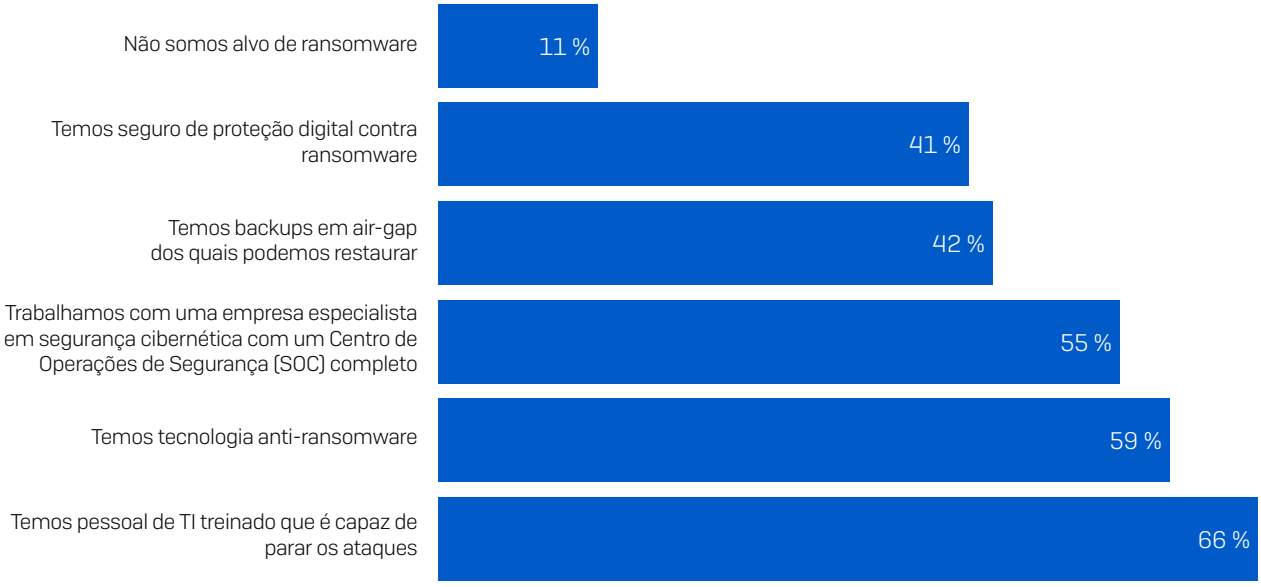
Além disso, 45% dos respondentes disseram que outras organizações do mesmao setor que eles foram visadas, aumentando a probabilidade de serem atingidos.

Dos respondentes, 22% consideram o comprometimento da segurança pelos usuários um fator principal por trás do motivo da probabilidade de serem atingidos por ransomware no futuro. É animador notar que, em vista a invasores sofisticados, a maioria das equipes de TI não está mais saindo pela tangente e culpando seus usuários.

De modo similar, 18% dos respondentes de serviços financeiros admitem ter fraquezas ou lacunas na segurança cibernética. Ainda que claramente não seja nada bom ter deficiências na segurança, reconhecer que elas existem é um importante passo para fortalecer as suas defesas.

Por que o setor de serviços financeiros não espera ser atingido por ransomware

119 respondentes da área de serviços financeiros disseram que suas organizações não foram atingidas por ransomware no ano passado e que não esperam ser atingidas no futuro.



Por que você não espera que a sua organização seja atingida por ransomware no futuro? [119] estabelecimentos de serviços financeiros que não foram atingidos por ransomware no ano passado e que não esperam ser atingidos no futuro, omitindo algumas opções de resposta

O principal motivo por trás dessa confiança é ter pessoal de TI treinado que está apto a parar os ataques (66%), seguido pelo uso de tecnologia anti-ransomware (59%). Enquanto as tecnologias avançadas e automatizadas são elementos essenciais de uma defesa anti-ransomware eficaz, interromper os invasores que trabalham ativamente também exige monitoramento e intervenção humana por profissionais capacitados. Seja seu pessoal interno ou profissionais contratados, os peritos humanos são únicos em sua capacidade de identificar alguns dos indicativos de que invasores de ransomware têm você na mira. Recomendamos que todas as organizações fortaleçam sua expertise humana em face às ameaças contínuas de ransomware.

Dos respondentes de serviços financeiros, 55% deles que não esperam ser atingidos por ransomware trabalham com uma empresa especialista em segurança cibernética que tem um Centro de Operações de Segurança (SOC). É animador observar que as organizações estão terceirizando segurança cibernética especializada quando necessário, ampliando sua proteção.

Mas não são só boas notícias. Alguns resultados são motivo de preocupação:

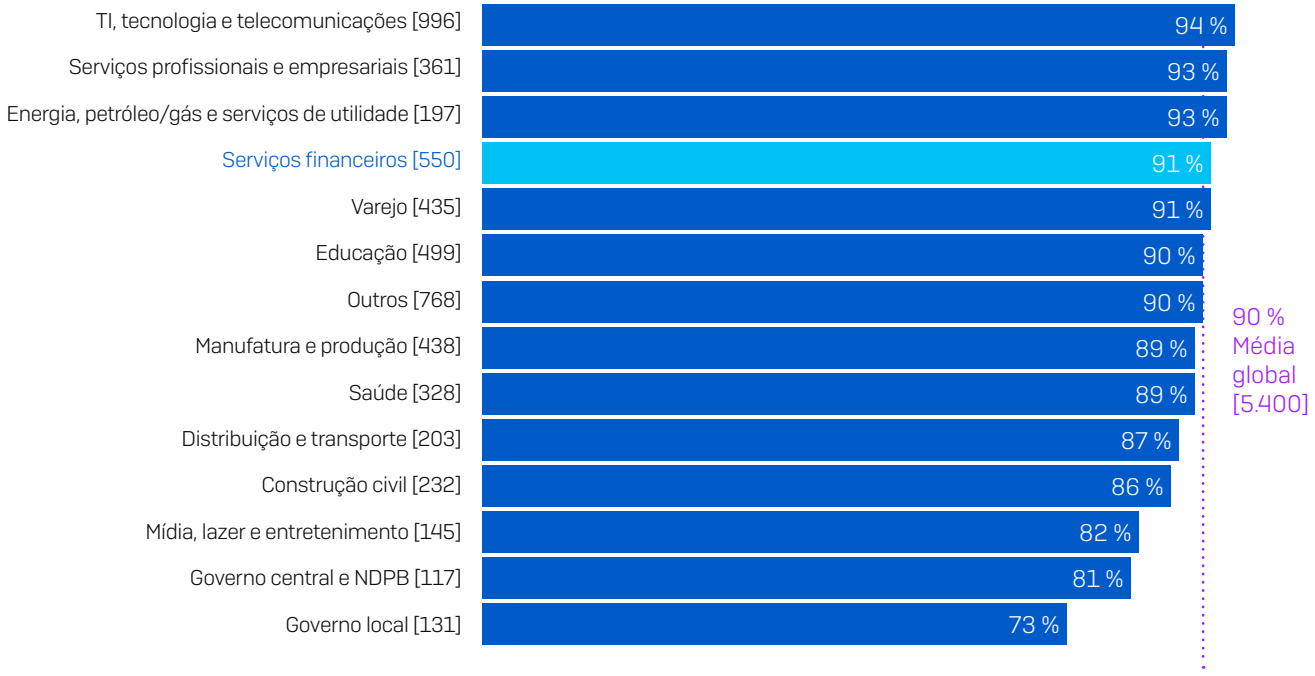
- 61% dos respondentes de serviços financeiros que não esperam ser atingidos estão acreditando em abordagens que não oferecem nenhuma proteção contra ransomware.
  - 41% mencionaram ter seguro de proteção digital contra ransomware. O seguro ajuda a cobrir os gastos gerados pelo ataque, mas não previne o ataque em si.
  - 42% mencionaram os backups air-gap em sistemas físicos isolados. Ainda que backups sejam ferramentas valiosas para restaurar dados pós-ataque, eles não impedem que você seja atingido.

  N.B. Alguns respondentes selecionaram as duas opções acima, com 61% selecionando pelo menos uma dessas duas opções.
- 11% acreditam não ser alvo de ransomware. Mas isso não é verdade. Nenhuma organização está segura.

Organizações de serviços financeiros estão bem-preparadas

Responder a incidentes ou ataques cibernéticos críticos pode ser incrivelmente estressante. Enquanto nada pode aliviar por completo a tensão de encarar um ataque, ter um plano de resposta a incidentes eficiente em vigor é um modo infalível de minimizar o impacto.

% que tem um plano para se recuperar de um incidente de malware significativo



O Plano de continuidade dos negócios (BCP, Business Continuity Plan) ou Plano de recuperação de desastres (DRP, Disaster Recovery Plan) da sua organização inclui planos para a recuperação de um incidente de malware significativo? Sim, temos um plano completo e detalhado de recuperação de incidentes de malware e Sim, temos um plano desenvolvido parcialmente de recuperação de incidentes de malware [números de base no gráfico], omitindo algumas opções de resposta, dividido por setor

Por isso é animador descobrir que 91% das organizações de serviços financeiros têm um plano de recuperação de incidente de malware, com um pouco mais da metade (51%) que afirmam ter um plano completo e detalhado e 40% que afirmam ter um plano parcialmente desenvolvido. Essas estatísticas estão alinhadas aos números médios entre setores (90%).

Recomendações

Com base nos resultados da pesquisa, os especialistas da Sophos recomendam as seguintes práticas para todas as organizações em todos os setores:

1. **Admita que você será atingido**. Ransomware continua a marcar forte presença. Não há setor, país ou organização de nenhum tamanho que esteja imune ao risco. É melhor se preparar e não ser atingido do que o contrário.
2. **Faça backups**. Backups são o método número 1 utilizado pelas organizações para recuperar dados após um ataque. E como temos notado, mesmo que pague o resgate, você raramente irá reaver seus dados, ou seja, você terá que contar com backups de um jeito ou de outro.

   Uma regra simples de backups: "3-2-1". Você deve ter pelo menos **três** cópias diferentes (a que está usando agora, além de duas ou mais sobressalentes), usar pelo menos **dois** sistemas de backup diferentes (no caso de um deles não funcionar) e ter pelo menos **uma** cópia armazenada offline e de preferência em outra localidade física (onde os impostores não possam adulterá-la durante um ataque).
3. **Implemente uma proteção em camadas**. Em face ao aumento considerável nos ataques de extorsão, manter os adversários fora do seu ambiente é o fator mais importante no momento. Use proteção em camadas para bloquear o máximo possível de pontos de ataque em todo o seu ambiente.
4. **Combine perícia humana e tecnologia anti-ransomware**. O fundamental para deter um ransomware é uma defesa profunda que combine tecnologia anti-ransomware dedicada e caça a ameaças conduzida por humanos. A tecnologia oferece a escala e automação que você precisa, enquanto os peritos humanos são mais bem capacitados a detectar os indicativos de táticas, técnicas e procedimentos quando um invasor habilidoso está tentando entrar no seu ambiente. Se você não tem pessoal interno habilitado, pondere contratar os serviços de uma empresa especialista em segurança cibernética. As SOCs agora são opções realistas para organizações de todos os tamanhos.
5. **Não pague o resgate**. Sabemos que falar é fácil – e que difícil mesmo é fazer, quando a sua organização se vê paralisada devido a um ataque de ransomware. Independentemente das considerações éticas, pagar o resgate é um modo ineficaz de reaver seus dados. Se decidir pagar, não deixe de incluir na sua análise de custos/benefícios a perspectiva de que seus adversários irão restaurar, em média, apenas dois terços dos seus arquivos.
6. **Tenha um plano de recuperação de malware**. A melhor forma de parar um ataque virtual antes que se torne uma violação total é se preparar com antecedência. As organizações que são vítimas de um ataque frequentemente se dão conta de que poderiam ter evitado boa parte do custo, estresse e interrupção se tivessem um plano de resposta a incidentes em vigor.

Recursos extras

O Guia de Resposta a Incidentes da Sophos ajuda as organizações a definir a estrutura do seu plano de resposta a incidentes contra a segurança cibernética e explora as 10 etapas principais que o seu plano deve incluir.

O pessoal da defesa também achará útil as Quatro grandes dicas de peritos em resposta a incidentes, destacando os principais aprendizados que todos deveriam ter quando se trata de responder a incidentes de segurança cibernética.

Esses dois recursos se baseiam em experiências reais do mundo real das equipes da Sophos Managed Threat Response e Sophos Rapid Response, que coletivamente já responderam a milhares de incidentes de segurança cibernética.

Saiba mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização.

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2021-09-1 (PTBR-MP)

SOPHOS