SOPHOS
Cybersecurity delivered.

O Estado do Ransomware no Brazil em 2022

Resultados de uma pesquisa independente de fornecedores com 200 profissionais de TI em organizações de médio porte no Brasil.

Um WhitePaper Sophos / Abril 2022

Sobre a pesquisa

A Sophos contratou a agência de pesquisa Vanson Bourne para realizar uma pesquisa independente de fornecedores com 5.600 profissionais de TI em organizações de médio porte (100-5.000 funcionários) em 31 países, incluindo 200 no Brasil. A pesquisa foi realizada durante janeiro e fevereiro de 2022, e os entrevistados foram solicitados a responder com base em suas experiências no ano anterior.

Principais conclusões

- 55% dos entrevistados no Brasil dizem que sua organização foi atingida por ransomware no ano passado, um aumento considerável em relação aos 38% que relataram um ataque em 2020. Em comparação, globalmente, 66% dos entrevistados sofreram um ataque de ransomware em 2021.
- 56% dos ataques resultaram em dados criptografados. Isso é inferior à média global de 65%, mas um aumento considerável em relação aos 36% que os entrevistados no Brasil relataram em 2020.
- 97% daqueles cujos dados foram criptografados receberam alguns dados de volta. Isso está alinhado com os resultados globais em que 99% relataram obter pelo menos alguns de seus dados.
- Os backups foram o método número 1 usado para restaurar dados, com 73% dos entrevistados brasileiros cujos dados foram criptografados usando essa abordagem. 40% pagaram o resgate. Está claro que usar vários métodos de recuperação em paralelo agora é comum. Em comparação, globalmente 73% dos entrevistados usaram backups e 46% pagaram o resgate para restaurar os dados.
- As organizações brasileiras que pagaram o resgate recuperaram em média 55% de seus dados. Nota: este achado é baseado em uma base relativamente baixa de 25 respostas. Globalmente, 61% dos dados foram restaurados por aqueles que pagaram o resgate, uma ligeira redução em relação aos 65% de 2020.
- 25 entrevistados do Brasil que pagaram o resgate compartilharam o valor exato, com o pagamento médio chegando a US$ 211.790. 39% pagaram menos de US$ 10.000, enquanto 9% pagaram US$ 500.000 ou mais. Globalmente, o pagamento médio de resgate foi de US$ 812.360 e houve um aumento de quase três vezes na porcentagem pagando US$ 1 milhão ou mais (de 4% em 2020 para 11% em 2021).
- A fatura média brasileira para se recuperar de um ataque de ransomware em 2021 foi de US$ 0,69 milhão. Esta é uma ligeira queda em relação aos US$ 0,82 milhão relatados em 2020.
- 92% dos entrevistados no Brasil disseram que o ataque de ransomware afetou sua capacidade de operação. Isso está em linha com o valor global de 90%.
- 83% relataram que o ataque de ransomware fez com que sua organização perdessem negócios/receitas. Novamente, isso está de acordo com o valor global de 86%.
- As organizações brasileiras levaram em média um mês para se recuperar do ataque.
- 85% dos entrevistados brasileiros disseram que sua organização tem seguro cibernético que os cobre se forem atingidos por ransomware. Globalmente, esse número é de 83%.
- 95% relataram que a experiência de sua organização em proteger com o seguro cibernético mudou no último ano. 59% disseram que o nível de segurança cibernética necessário para se qualificar para o seguro é maior, 49% disseram que as políticas de segurança cibernética agora são mais complexas, 22% disseram que o processo leva mais tempo e 44% relataram que é mais caro. Dado que o grande aumento de preço do seguro cibernético começou no segundo e terceiro trimestres de 2021, é provável que muitas organizações experimentem um aumento de preço considerável na próxima renovação.

- 99% fizeram alterações em suas defesas cibernéticas no último ano para melhorar sua posição de seguro. Globalmente, 97% fizeram mudanças com 64% implementando novas tecnologias / serviços, 56% aumentando as atividades de treinamento e educação da equipe e 52% mudando seus processos e comportamentos.
- O seguro cibernético pagou em 97% dos sinistros de ransomware brasileiros. Daqueles atingidos por ransomware e que tinham cobertura de seguro cibernético contra ransomware, 73% relataram que o seguro pagou os custos para colocá-los em funcionamento novamente, 36% disseram que pagou o resgate e 33% disseram que pagou outros custos.

Conclusão

O desafio do ransomware enfrentado pelas organizações brasileiras continua crescendo. Otimizar sua segurança cibernética é um imperativo para todas as organizações. Nossas cinco principais dicas são:

- Garanta defesas de alta qualidade em todos os pontos do seu ambiente. Revise seus controles de segurança e verifique se eles atendem às suas necessidades.
- Procure ameaças proativamente para que você possa neutralizar os invasores antes que eles possam executar seu ataque – se você não tiver tempo ou habilidades em casa, terceirize com um especialista em MDR
- Proteja seu ambiente procurando e eliminando lacunas de segurança: dispositivos sem patches, máquinas desprotegidas, portas RDP abertas. O XDR é ideal para esta finalidade.
- Prepare-se para o pior. Saiba o que você fará se ocorrer um incidente cibernético e pratique as etapas com antecedência.
- Faça backups e pratique a restauração a partir deles. Seu objetivo é ser capaz de voltar a funcionar rapidamente.

Outras informações

Leia o relatório O Estado do Ransomware 2022 para obter as descobertas globais completas e dados por setor.

Para obter informações detalhadas sobre grupos de ransomware individuais, consulte o Sophos Ransomware Threat Intelligence Center.

Saiba mais sobre ransomware e como a Sophos pode ajudá-lo a defender sua organização.

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 21 3500-0312
-

Brazil
Tel: +55 11 4950 8764-
-

2022-04-07 (WP-NP)