Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.170-185, 2023.
DOI: 10.18762/1982-4920.20230011

PLANO DE CONTINGÊNCIA EM EMPRESAS DE TECNOLOGIA SOB UM ATAQUE *RANSOMWARE*

Bruno Otávio dos Santos, André Castro Rizo

RESUMO

Este artigo apresenta a preocupação das empresas de tecnologia em relação às ameaças de exploração de vulnerabilidades, com foco especial nos ataques *ransomware*, e descreve as medidas adotadas para mitigar o risco às operações. O texto apresenta uma contextualização do tema, incluindo definições e tipos de ataques mais frequentes ao longo dos anos, além de abordar as melhores práticas recomendadas pelo mercado e pelos frameworks e ferramentas disponíveis.

Palavras-chave: *ransomware*; ataques; vulnerabilidade; plano de contingência; recuperação do ambiente.

ABSTRACT

This article presents the concern of technology companies regarding the threats of vulnerability exploitation, with a special focus on *ransomware* attacks, and describes the measures adopted to mitigate the risk to operations. The text presents a contextualization of the theme, including definitions and types of attacks that have been most frequent over the years, as well as addressing best practices recommended by the market and by the frameworks and tools available.

Keywords: *ransomware*; attacks; vulnerability; contingency plan; environment recovery.

1 INTRODUÇÃO

Uma das preocupações mais urgentes das empresas de tecnologia, independente do porte e da segmentação do ramo de seus negócios, é a de acompanhar os avanços tecnológicos e se manter protegidas contra ameaças. Com a crescente disponibilização de serviços, soluções em nuvem e o tráfego de dados de clientes e de operações digitais; vimos aumentar, também, a exploração de vulnerabilidades por criminosos.

Entre os principais perigos expostos pelas organizações conectadas podemos citar o *ransomware*, que tem se mostrado uma ameaça persistente para as empresas em todo o mundo.

Um ataque *ransomware* consiste em sequestrar dados aplicando criptografia[1] e exigir o pagamento de um "resgate" para descriptografar as informações.

De acordo com os sites das empresas e ferramentas antivírus AVG e Kaspersky, esse tipo de ameaça não é novo, tendo sido relatado pela primeira vez em 1989, quando o trojan AIDS utilizou discos floppy para criptografar e extorquir suas vítimas. Tal ameaça limita-se a uma restrição física de acesso, já que a internet não era popular e disponível como veio a se tornar a partir do século XXI.

No início dos anos 2000, com a chegada de transações e contas bancárias online, as principais ações desse tipo de código eram mascaradas por falsos softwares de segurança e exibiam alertas de ameaças inexistentes e solicitavam pagamento para sua eliminação. Uma década depois, o Trojan.Winlock, ao infectar o dispositivo, solicitava uma chave de ativação do Windows e dizia que a mensagem seria removida após ligação para determinado número internacional e o pagamento de uma taxa; porém a ameaça podia ser facilmente detectada e removida.

Os formatos mais recentes desse tipo de ferramenta de sequestro digital datam de 2017 e consistem em infectar dispositivos conectados à internet; desde celulares e computadores, chegando às geladeiras domésticas ou smart TVs de aeroportos. Após o controle e/ou bloqueio dos dispositivos, costuma-se solicitar um pagamento – geralmente em criptomoeda – para "devolução" dos dispositivos ou de dados.

Embora esse assunto possa parecer relativamente isolado e alheio aos que não estão inseridos nesse contexto, os dados mostram que os ataques de extorsivos estão se tornando cada vez mais frequentes e sofisticados. No Brasil, por exemplo, a pesquisa anual "The State of *Ransomware*" (2021), divulgada em maio de 2022, revelou que 55% das organizações no país foram atingidas por algum tipo de *ransomware* em 2021. Esse número representa mais de 33 milhões de tentativas de invasão, indicando um aumento de 38% em relação a 2020. Diante desta realidade, empresas de tecnologia têm o desafio de manter a operação, garantir a segurança das informações e proteger seus clientes contra ameaças cibernéticas.

Este artigo aborda a problemática dos ataques ransomware e apresenta as melhores práticas e frameworks para a defesa e recuperação do ambiente, além da estrutura e base para

[1] Criptografia: é um conjunto de técnicas matemáticas e algoritmos que se destinam a transformar dados em uma forma incompreensível para quem não possui acesso aos meios necessários para realizar a decodificação. Essa transformação é feita por meio de uma chave que é utilizada tanto para a codificação quanto para a decodificação dos dados.

elaboração de um plano de contingência eficiente. Para isso, foi realizada uma revisão da literatura sobre o assunto, analisados casos famosos de ataques ransomware e identificadas as principais vulnerabilidades e falhas nas estratégias de defesa utilizadas pelas organizações afetadas. Também foram apresentados números de relatórios anuais que confirmam e comparam a adoção de práticas e técnicas de prevenção aos ataques de código maliciosos em determinados períodos, consolidando os resultados alcançados com a adoção dessas práticas.

2 REFERENCIAL TEÓRICO

Neste capítulo abordamos temas que são fundamentais para compreensão da exploração de vulnerabilidades, dos ataques *ransomware* e dos pilares da prevenção dos dados e informações sensíveis em meio aos ataques. Apresentamos a definição e a abrangência do tema Segurança da Informação, conforme proposto por Peixoto em 2006, bem como a explicação sobre os ataques *ransomware* elaborada por Neves em 2008. É importante destacar que a análise desses temas é relevante e necessária, tendo em vista a crescente utilização de tecnologias de informação nas empresas e na sociedade como um todo, o que torna essas questões ainda mais pertinentes.

2.1 Segurança da Informação

A Segurança da Informação é um tema crítico e fundamental para as empresas que buscam proteger seus ativos de informação contra acessos indevidos, modificações não autorizadas e garantir a disponibilidade dos recursos e dados. De acordo com Peixoto (2006), a Segurança da Informação é uma área do conhecimento que envolve a proteção dos princípios básicos:

• Integridade: garante que as informações serão precisas e completas, sem modificações não autorizadas por meio de técnicas como criptografia e assinaturas digitais.

• Disponibilidade: garante que as informações estarão sempre disponíveis para aqueles que precisam delas a partir de políticas como backups regulares e redundância de sistemas.

• Autenticidade: garante que as informações são autênticas e não foram falsificadas ou manipuladas por meio de técnicas como autenticação de usuários e certificados digitais.

• Confidencialidade: garante que as informações serão mantidas em sigilo e só serão acessadas por pessoas autorizadas por meio de como criptografia e controles de acesso.

2.2 Ataques *ransomware*

Neves (2008) descreve o *ransomware* como uma ameaça que funciona como um sequestro virtual, utilizando-se de código malicioso para encriptar as informações da vítima e exigir um resgate para liberá-las. O ataque pode ser instalado em dispositivos por meio de um e-mail com anexo ou direcionamento a um link malicioso, muitas vezes combinado com phishing.

Relatórios da Avast (2017) e da Cisco (2016) mostram que mais de 37% dos ataques bem-sucedidos em servidores entre 2015 e 2016 foram relacionados a *ransomware*. Já os dados da Veeam 2022 *Ransomware* Trend Report alertam que 76% das organizações mundiais e 91% das empresas brasileiras, em 2022, pagaram o resgate; porém 1/3 não obteve de volta os dados sequestrados.

2.3 Phishing

Olivo (2010) caracteriza phishing como técnica em que utiliza da Engenharia Social para persuadir vítimas a fim de se conseguir informações pessoais e assim, conseguir alguma vantagem financeira. É comum esse tipo de técnica chegar à vítima através de e-mails, mensagens nas redes sociais e pop-up de navegadores de internet. É comum que nessas mensagens sejam embutidos códigos HTML que direcionem a determinado endereço.

3 CASOS REPORTADOS

É importante enfatizar que, apesar dos números alarmantes de ataques, é possível que muitos casos não estejam divulgados por políticas internas de investigação ou que ganhem notoriedade e divulgação midiática. Empresas globais de serviços e de varejo podem encontrar mais dificuldade em “ocultar” um ataque, já que muitas vezes a operação e a interface com o usuário/cliente é afetada.

Segundo dados reportados pela Check Point Research (2023), divisão de Inteligência em Ameaças da Check Point Software Technologies Ltd., algumas marcas tiveram mais tentativas de roubo de informações pessoais ou de credenciais de pagamentos de cliente durante o primeiro trimestre de 2023, sendo a rede de supermercados Walmart a ocupante da primeira posição, seguida pela gigante de logística DHL e pela pioneira em computadores pessoais Microsoft, como consta no artigo da Security Report.

Durante a última década, cabe trazer alguns dos casos de ataques que foram amplamente divulgados pela mídia e tem suas definições nos sites da AVG e Kaspersky, presentes na bibliografia:

• **CryptoLocker:** o ataque ocorrido em 2013 utilizou um malware com chave de criptografia fora do padrão, o que desafiou especialistas. O ataque causou perdas de mais de 3 milhões de dólares, infectando mais de 200 mil computadores com sistema Windows. A infecção se deu por inclusão e distribuição de arquivos maliciosos via e-mail.

• **WannaCry:** foi um ataque global que ocorreu em maio de 2017, afetando mais de 250 mil computadores em mais de 150 países. O vírus se espalhou rapidamente por e-mail de phishing e explorava uma vulnerabilidade do sistema operacional Windows, bloqueando arquivos e exigindo um resgate em bitcoins para que as vítimas pudessem recuperar seus dados. O resgate estimado estava em 300 dólares por equipamento e as perdas foram estimadas em 4 bilhões de dólares. A recuperação envolveu a aplicação de um patch de segurança no sistema operacional e o uso de ferramentas de descriptografia disponibilizadas por empresas de segurança. Algumas empresas que foram afetadas neste ataque foram Telefônica, Nissan, FedEx e Renault.

• **Petya/NotPetya:** Em junho de 2017, o *ransomware* Petya afetou empresas em todo o mundo, incluindo a gigante de logística Maersk, que teve que interromper suas operações em vários portos. O Petya se espalhou por meio de uma vulnerabilidade do Windows, mas também utilizou outras técnicas de propagação. O malware infectou o registro de inicialização do sistema operacional, afetando toda a execução do Windows. Estima-se que o impacto foi de mais de 10 bilhões de dólares de prejuízo e até mesmo o Banco Nacional da Ucrânia foi afetado. A recuperação envolveu a aplicação de um patch de segurança, a restauração de backups e, em alguns casos, a reconstrução completa de sistemas afetados.

• **GandCrab:** apareceu pela primeira vez em janeiro de 2018 e rapidamente se tornou um dos mais difundidos. Ele foi distribuído por meio de campanhas de spam e kits de exploração de vulnerabilidades e exigia o pagamento de um resgate em criptomoedas para a recuperação de arquivos. A recuperação envolveu o uso de ferramentas de descriptografia disponibilizadas por empresas de segurança, bem como a restauração de backups.

Segundo informações reunidas na página do Security Report (2021), o Brasil é o principal alvo desse tipo de ataques na América Latina e ocupa a 4ª posição mundial, ficando atrás dos EUA, Japão e Taiwan. Mas não só empresas multinacionais que devem se preocupar com esses ataques; setores do Governo, Industria, Saúde e Educação despontam como alvos favoritos de ataques e extorsões.

Veja alguns casos que ganharam notoriedade no Brasil e que estão disponíveis nos sites Núcleo do Conhecimento e, também, na Kaspersky:

• **Universidade Presbiteriana Mackenzie:** no caso do ataque sofrido pela universidade, em agosto de 2020, o *ransomware* bloqueou o acesso a arquivos do sistema da universidade e os hackers exigiram o pagamento de um resgate para liberar as informações. A universidade se recusou a pagar o resgate e optou por restaurar os dados por meio de backups.

• **Jamef:** A empresa de logística Jamef também sofreu um ataque em setembro de 2018. O *ransomware* afetou os sistemas de gestão da empresa, deixando os serviços de transporte de mercadorias paralisados. A Jamef conseguiu recuperar as informações por meio do uso de backups e do trabalho em conjunto com empresas de segurança.

• **Record TV:** Em outubro 2022, a emissora de TV acionou especialistas em tecnologia e autoridades para investigar um ataque sofrido. O sistema central da emissora foi invadido e o acervo da emissora foi sequestrado por inserção de criptografia. O departamento de T.I possuía cópias do acervo, permitindo a restauração completa dos dados. Este foi, provavelmente, o maior ataque hacker sofrido por uma empresa de mídia em todo o mundo.

4 FRAMEWORKS E MELHORES PRÁTICAS

O blog Cronapp, especializado em tecnologia e Low-Code, define frameworks como conjuntos de diretrizes, práticas e instruções para implementar, suportar, gerenciar ou fazer a manutenção no setor de T.I. Ao que tange à Segurança da Informação, os frameworks ajudam a garantir a segurança cibernética de uma organização, fornecendo orientações sobre como avaliar e mitigar riscos em relação às ameaças virtuais. Essas práticas incluem medidas preventivas para minimizar as chances de ataques, como treinamento de conscientização em segurança, backups de dados e atualizações regulares de sistemas e softwares, além de preparação para possíveis incidentes relacionados à segurança cibernética, como ataques *ransomware*. Neste contexto, é importante destacar alguns dos principais frameworks e práticas disponíveis para proteger organizações:

4.1 ITIL e COBIT

ITIL e COBIT são frameworks de boas práticas em gestão de TI que ajudam as empresas a alcançarem seus objetivos de negócios por meio de processos e procedimentos bem definidos. Embora não tratem especificamente do tema de ataques *ransomware*, ambos destacam a importância de ter planos de contingência atualizados e medidas de segurança robustas para proteger os sistemas e dados contra ameaças de segurança.

Segundo Almeida (2020), o ITIL (Information Technology Infrastructure Library) é uma referência das melhores práticas para a gestão de serviços de TI, fornecendo um conjunto de processos e procedimentos que permitem que as empresas gerenciem seus serviços de TI de forma eficaz e eficiente. O ITIL enfatiza a importância de ter um plano de continuidade de negócios bem definido e atualizado, que inclui a recuperação de sistemas e dados em caso de interrupções nas operações de negócios. Isso é especialmente importante no caso de ataques *ransomware*, pois a recuperação de sistemas e dados é crucial para minimizar os danos causados pelo ataque. Também apresenta a importância de ter medidas de segurança robustas em vigor para proteger os sistemas e dados contra ameaças de segurança, incluindo a implementação de firewalls e antivírus, a limitação do acesso aos dados mais críticos do negócio e a realização de backups regulares dos dados.

Almeida (2020) apresenta também o COBIT (Control Objectives for Information and Related Technologies), que fornece estruturas, processos e modelos para ajudar as empresas a garantir que seus sistemas de TI sejam gerenciados de forma eficiente e eficaz, atendendo aos objetivos de negócios e regulamentações. Com o COBIT, as empresas podem estabelecer controles claros e métricas de desempenho para avaliar e melhorar continuamente os processos de TI, garantindo que eles estejam alinhados com as metas organizacionais e os requisitos regulatórios.

4.2 CIS Controls

Segundo Netto (2022), o CIS Controls consiste em um conjunto de controles de segurança de TI desenvolvido pelo Center for Internet Security. Esses controles abrangem diversas medidas de segurança, como a gestão de ativos de TI, controle de acesso, proteção contra malware, monitoramento de uso de redes e sistemas, proteção de dados, controle de acesso a

dispositivos móveis e implementação de planos de gerenciamento de incidentes e resposta a incidentes, entre outros.

O principal objetivo do CIS Controls é auxiliar as empresas na proteção de seus sistemas e dados contra ameaças cibernéticas, incluindo o ransomware, que tem se destacado como uma das principais preocupações nessa área. Com a crescente sofisticação e frequência dessas ameaças, torna-se cada vez mais importante adotar medidas de segurança robustas para garantir a integridade das informações e processos críticos das organizações. Por isso, o CIS Controls tem sido amplamente utilizado como estratégia de segurança por diversas empresas.

4.3 SANS Institute

Segundo Ribeiro (2016), o Sans Institute é uma organização de treinamento em segurança da informação que oferece uma variedade de cursos e certificações em segurança da informação. Entre os tópicos abordados nos cursos estão a prevenção de ataques de programa malicioso de criptografia.

Os cursos do SANS Institute são reconhecidos mundialmente por sua excelência e abrangência e são ministrados por especialistas em segurança da informação. Eles oferecem não só conhecimento teórico, mas também prática e experiência real para lidar com os desafios da segurança da informação na atualidade. Entre as trilhas oferecidas, destacam-se os de prevenção de ataques *ransomware* e resposta a incidentes de segurança; que são fundamentais para quem quer entender melhor como se proteger desses tipos de ataques e como lidar com incidentes de segurança quando eles ocorrem.

4.4 NIST Cybersecurity Framework

O NIST Cybersecurity Framework é um conjunto de diretrizes destinadas a ajudar as empresas a gerenciar e reduzir o risco de ciberataques. Netto (2022) reforça que o framework inclui uma série de controles de segurança que as empresas podem implementar para proteger seus sistemas e dados contra ameaças de segurança. O NIST é referenciado pela própria IBM como uma das ferramentas de padrão, diretrizes e práticas adotadas pela companhia.

O site do NIST apresenta sua composição por cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar. Cada uma dessas funções é composta por uma série de categorias e subcategorias que descrevem as atividades a serem realizadas para proteger os sistemas e dados contra ameaças de segurança.

4.5 ISO/IEC 27001

Segundo Hintzbergen (2018), no livro Fundamentos de Segurança da Informação, a ISO/IEC 27001 é apresentada como um padrão internacional que estabelece requisitos para um SGSI - Sistema de Gestão de Segurança da Informação). O SGSI inclui políticas, procedimentos, processos e controles de segurança que ajudam as empresas a gerenciar e reduzir o risco de ciberataques, incluindo o *ransomware*.

Ao implementar os requisitos da ISO/IEC 27001, as empresas podem melhorar sua segurança cibernética e reduzir o risco de ataques. Existem vários pontos a serem considerados em relação a um ataque *ransomware* na implementação:

Garantir que o SGSI inclua controles de segurança adequados para prevenir e detectar ataques *ransomware*: Isso pode incluir a implementação de firewalls, antivírus e outras ferramentas de segurança para proteger a rede da organização contra ameaças cibernéticas.

Realizar avaliações regulares de risco e vulnerabilidades para identificar e mitigar quaisquer riscos de *ransomware*: A avaliação de vulnerabilidades pode ajudar a identificar possíveis pontos fracos na segurança da organização e permitir que medidas preventivas sejam tomadas antes de um ataque acontecer.

Garantir que a equipe de segurança da informação esteja preparada para lidar com incidentes de *ransomware,* incluindo planos de resposta a incidentes e treinamento adequado: Ter um plano de resposta a incidentes em vigor e uma equipe de segurança treinada pode ajudar a minimizar os danos em caso de um ataque de *ransomware*.

Implementar controles de backup e recuperação de dados adequados para garantir que, se ocorrer um ataque *ransomware*, os dados possam ser recuperados sem ter que pagar o resgate.

Ao seguir essas práticas recomendadas, as empresas podem melhorar sua segurança cibernética e reduzir o risco de ataques de *ransomware*, além de estar em conformidade com os requisitos da ISO/IEC 27001.

5 PLANO DE CONTINGÊNCIA

Miller (2017) ressalta que existe uma série de práticas recomendadas que as organizações podem implementar de forma proativa para evitar ou tornar mais difícil a vida de um cibercriminoso. O autor aborda que o intuito desses ataques é o de conseguir algum ganho, em

contrapartida, o esforço e o risco pretendem ser mínimos. Dessa forma, as empresas devem partir para uma sequência de ações que tornam esse esforço maior e a certeza de ataques bem-sucedidos menor.

As organizações devem fornecer treinamentos aos usuários e verificar vulnerabilidades e riscos. Em casos de ataques, as medidas propostas devem ser praticadas no menor tempo possível a fim de se evitar maiores danos.

Baseada na obra de Miller (2017), dividimos o Plano de Contingência em 3 etapas:

5.1.1 Prevenção

O autor aborda a prevenção como a melhor maneira de combater os ataques *ransomware* e, para alcançar esse objetivo, é necessário investir em ações rotineiras que incluem atualizações do sistema operacional e dos softwares utilizados. As atualizações frequentes podem incluir correções de segurança que impedem os hackers de explorar as vulnerabilidades do sistema. Além disso, o uso de ferramentas de segurança como antivírus e firewalls é fundamental para proteger os sistemas contra os ataques.

Outras medidas preventivas importantes incluem fazer backups regulares de dados para permitir a recuperação dos dados após um ataque e instruir a equipe a não clicar em links ou baixar arquivos de fontes não confiáveis. É comum que os hackers usem e-mails maliciosos para disseminar o *ransomware*, logo, estar atento a e-mails suspeitos e não fornecer informações pessoais ou de login em sites não confiáveis também é crucial para prevenir esses ataques. Ao seguir essas medidas preventivas, empresas e indivíduos podem reduzir significativamente o risco de sofrerem ataques de *ransomware*.

5.1.2 Resposta

No caso de um ataque *ransomware*, Miller (2022) reforça que é fundamental seguir o plano de resposta definido para minimizar os danos. Isso inclui identificar precocemente a origem do ataque, isolando os sistemas afetados e acionar imediatamente a equipe de segurança da informação. Identificar a origem do ataque *ransomware* o mais cedo possível é crucial para evitar a propagação do malware e minimizar o impacto. A equipe de segurança da informação deve ser acionada para auxiliar na identificação da origem do ataque e recuperar os arquivos afetados.

Outras ações importantes incluem não realizar o pagamento do resgate, pois isso não garante a recuperação dos dados e pode incentivar ainda mais esse tipo de crime. Informar a polícia e outras autoridades competentes também é importante para ajudar a investigar o ataque e identificar os responsáveis pelo crime para que ações jurídicas possam ser tomadas. Ao seguir essas ações, as empresas podem minimizar significativamente os danos causados por ataques *ransomware* e aumentar suas chances de recuperar seus dados com sucesso.

5.1.3 Recuperação

Após um ataque *ransomware*, é fundamental que a empresa tenha um plano de recuperação bem definido para minimizar os danos e restaurar os sistemas afetados. Essa etapa é complexa e demorada, mas pode ser facilitada por meio da implementação de um plano de backup eficiente e do armazenamento seguro dos dados. A obra de Miller (2022) embasa que as medidas mais comuns incluem: restaurar os dados a partir dos backups, reinstalar os sistemas operacionais e softwares afetados, realizar uma análise de vulnerabilidades, avaliar o impacto do ataque e promover treinamentos para conscientização dos funcionários.

Todas as ações do Plano de Contingência elaborado pela empresa devem estar documentadas e compreendidas para uma boa coordenação dos passos necessários à recuperação dos sistemas. Após a solução do problema, é importante avaliar os danos causados e identificar as vulnerabilidades que permitiram a invasão, a fim de reconstruir o cenário que tornou propícia a intrusão e identificar pontos de melhoria e correções necessárias.

Por fim, é fundamental aplicar as lições aprendidas em casos futuros, promovendo um ambiente mais seguro e consciente da importância da segurança da informação. Treinar os funcionários para prevenção de ataques *ransomware* também é crucial para aumentar a conscientização e evitar futuros incidentes.

5.1.4 Políticas de Backups

Um plano de backup eficaz é fundamental para garantir a disponibilidade e integridade dos dados em caso de um ataque *ransomware*. De acordo com Cardoso Neto e outros autores (2014) seguem alguns pontos que devem ser levados em conta incluem:

- Identificação dos dados críticos a fim de identificar quais dados são críticos para o negócio e precisam ser protegidos por meio de backups.

- Definição da frequência dos backups e dos métodos, como backup completo, incremental e diferencial com base na criticidade dos dados e na capacidade de armazenamento disponível.
- Definição do local de armazenamento dos backups, como discos rígidos externos, nuvem e locais offsite de forma segura à acessos não autorizados e definição da política de retenção dos backups prevendo por quanto tempo os backups serão mantidos e quando eles serão descartados
- Definição da política de acesso aos backups levando em consideração o nível de criticidade dos dados e a necessidade de proteger os backups contra acessos não autorizados.
- Monitoramento e testes regulares dos backups para garantir que eles estejam funcionando corretamente e que os dados possam ser recuperados em caso de ataque *ransomware*. O monitoramento regular também ajuda a identificar problemas antes que eles se tornem críticos.
- Revisão e atualização do plano de backup para garantir que ele esteja atualizado e que leve em consideração as mudanças na infraestrutura de TI e no ambiente regulatório.
- Além disso, é importante que as empresas implementem medidas adicionais para proteger os backups contra ameaças de segurança. Isso pode incluir a criptografia dos backups, a implementação de firewalls e antivírus nos sistemas de backup.

6 RESULTADOS OBTIDOS

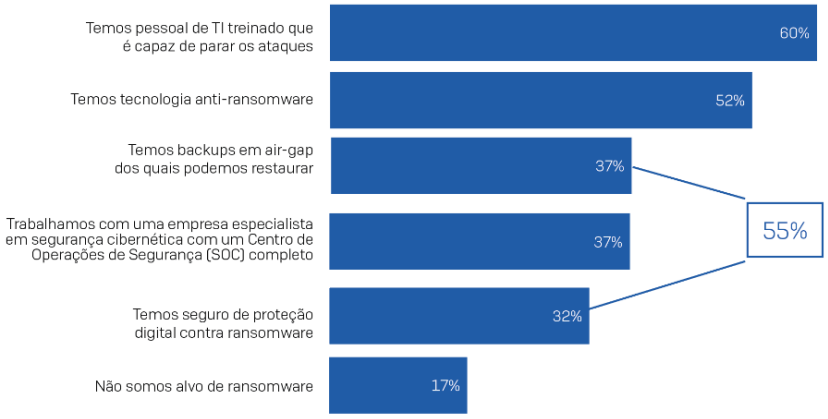
De acordo com o relatório anual da Sophos, publicado em 2021, o número de empresas que sofreram ataques *ransomware* sofreu uma redução; saindo de 3 mil casos em 2017 e passando para cerca de 2 mil em 2021. A pesquisa foi realizada entre janeiro e fevereiro de 2021 com mais de 5 mil entrevistados de 30 países. Dentre os motivos analisados pela Sophos estão as tratativas das empresas como política de backups e treinamento de funcionários, tornando o uso de automatizações para ataques menos viáveis e forçando ataques mais direcionados e planejados.

Figura 1 – Dados de empresas que sofreram ataques entre 2017 e 2021.

Fonte: https://www.addvalue.com.br/*ransomware*-2021/.

Outro dado importante do estudo é que mais de 1/5 dos entrevistados declaram que ter uma equipe treinada, tecnologia anti-*ransomware* e política de backup estão entre os principais meios que utilizados pela organização e consideram estar na eficácia da redução de ataques. Ter uma equipe treinada é também essencial, já que uma das técnicas mais utilizadas pelos atacantes é a de engenharia social através do phishing. Abaixo apresentamos as ações mais efetivas para combater os ataques hackers nas organizações, segundo a visão dos entrevistados:

Figura 2 – Ações utilizadas pelas empresas para redução de ataques.



Fonte: https://www.addvalue.com.br/*ransomware*-2021/.

7 CONCLUSÃO

Os ataques cibernéticos, em especial os *ransomware*, representam uma ameaça crescente para as empresas e as organizações. Para cuidar do ambiente a fim de minimizar os impactos causados por esses ataques, é fundamental adotar medidas preventivas, elaborar um plano de contingência e continuidade, e estar preparado para lidar com a situação caso ocorra um ataque.

A implementação de medidas de segurança robustas, como firewalls, antivírus e sistemas de detecção de invasão, aliada a treinamentos para os funcionários, pode ajudar a evitar ataques cibernéticos. Caso ocorra um ataque, é importante seguir o plano de contingência elaborado pela empresa e agir de forma coordenada para minimizar os danos.

Como apresentado no capítulo anterior, a adoção de rotinas e atividades sistemáticas têm se mostrado eficiente para redução da efetividade de ataques *ransomware* ou auxiliado empresas a recuperarem seus sistemas e dados com o menor impacto.

As empresas podem garantir a segurança das informações e a continuidade das atividades mesmo em caso de ataques cibernéticos; para isso, é importante estar atento às tendências e mudanças no cenário de Segurança da Informação e revisitar os frameworks e as melhores práticas adotadas pelas empresas do segmento.

REFERÊNCIAS

ADD VALUE. **Sophos – O Estado do *Ranso*mware 2021**. *[S.l.]*. In Artigos, 2021. Disponível em: https://www.addvalue.com.br/*ransomware*-2021/. Acesso em: 26 mai. 2023.

AVG. **Uma breve história dos vírus de computador.** Disponível em: <https://www.avg.com/pt/signal/history-of-viruses>. Acesso em: 16 mar. 2023

ALMEIDA, A. **ITIL e COBIT: qual é a melhor metodologia de governança de TI?** Blog Hosts Green. [*S. l.*], 5 ago. 2020. Disponível em: https://blog.hosts.green/itil-e-cobit/. Acesso em: 22 abr. 2023.

AVAST. **GUIA básico sobre *ransomware***. *[S.l.]*. *Ransomware*, 2022. Disponível em: https://www.avast.com/pt-br/c-topic-*ransomware*. Acesso em: 10 nov. 2022.

CARDOSO NETO, Celso et al. **Backup.** Revista de Trabalhos Acadêmicos-Campus Niterói. Niterói-RJ, 2014

CENTER FOR INTERNET SECURITY. **The 18 CIS Critical Security Controls.** *[S.l.]*. Center for Internet Security, 2023. Disponível em: https://www.cisecurity.org/controls/cis-controls-list. Acesso em: 22 abr. 2023.

CRONAPP. **Fique por dentro dos principais frameworks para gestão de projetos em TI**. Cronapp Blog. [S.l.]. 2 jun. 2022. Disponível em: https://blog.cronapp.io/frameworks-para-gestao-de-projetos-em-ti/. Acesso em: 3 jun. 2023.

GRUSTNIY, L. **Pesquisa: 66% das organizações foram atingidas por *ransomware* em 2021.** [S.l.]. Kaspersky Daily, 2021. Disponível em: https://www.kaspersky.com.br/blog/history-of-*ransomware*/17280/. Acesso em: 25 nov. 2022.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018.

INFOR CHANNEL. **Check Point divulga ranking de ameaças mais ativas em março.** 13 abr. 2022. Disponível em: https://inforchannel.com.br/2023/04/13/check-point-divulga-ranking-de-ameacas-mais-ativas-em-marco/. Acesso em: 21 abr. 2023.

KASPERSKY. **Um breve histórico dos vírus de computador e qual será o seu futuro**. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>. Acesso em: 15 mar. 2023.

KASPERSKY. **Principais ataques de *Ransomware***. Disponível em: < https://www.kaspersky.com.br/resource-center/threats/top-ransomware-2020>. Acesso em: 22 mar. 2023.

LEVI ALVES DOS SANTOS. **Os ataques *ransomware* e a camada de proteção de sistemas governamentais**. [S.l.]. Núcleo do Conhecimento, 2022. Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/ataques-ransomware. Acesso em: 25 mar. 2023.

MANAGE ENGINE. **O que são os Controles CIS?** [S.l.]. Manage Engine, 2022. Disponível em: https://www.manageengine.com/br/cis-critical-security-controls. Acesso em: 23 abr. 2023.

MILLER**,** L. **Defesa contra *ransomware*.** Hoboken: NJ: John Wiley & Sons, 2017. Edição especial da Cisco.

NEVES, A. **Como evitar se tornar uma vítima de *ransomware*?** Canaltech, [*S. l.*], 14 jun. 2017. Disponível em: https://canaltech.com.br/seguranca/como-evitar-se-tornar-umavitima-de-*ransomware*-confira-nossas-dicas/ Acesso em: 11 nov. 2022.

NIST. **Secure Software Development Framework (SSDF): Recommendations for Mitigating the Risk of Software Vulnerabilities**, v1.1, 2021, Gaithersburg, MD. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-218/archive/2021-09-30. Acesso em: 19 de abr.2023

NETTO, Vinicius Valle Uchoa. **Metodologia para aplicação conjunta de frameworks de segurança.** 2022.

OLIVO, CK. **Avaliação de características para detecção de phishing de e-mail**. Dissertação(mestrado), Pontifícia Universidade Católica do Paraná, Curitiba, 2010.

PEREIRA, C. G. ***Phishing*: Conceitos e ações preventivas aplicadas à empresa**. Brasília, 2012. Centro Universitário de Brasília, Brasília, 2012. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/235/8136/1/50910909.pdf. Acesso em: 30 abr. 2022.

PEIXOTO, M. C. P. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

RIBEIRO, M. **Conheça um pouco sobre o SANS Institute**. Linkedin, [*S. l.*], 12 jan. 2016. Disponível em: https://www.linkedin.com/pulse/conhe%C3%A7a-um-pouco-sobre-o-sans-institute-marcelo-ribeiro/?originalSubdomain=pt. Acesso em: 29 abr. 2023.

SECURITY REPORT. **76% das organizações admitem pagar criminosos de *ransomware*, mas 13% delas não recupera os dados.** Security Report, 2021. Disponível em: https://www.securityreport.com.br/overview/76-das-organizacoes-admitem-pagar-criminosos-de-*ransomware*-mas-13-delas-nao-recupera-os-dados/#.ZD80gnbMIok. Acesso em: 20 abr. 2023.

SECURITY REPORT. **Walmart lidera a lista de marcas mais imitadas em ataques de phishing.** [S.l.]. Redação, 2021. Disponível em: https://www.securityreport.com.br/overview/walmart-lidera-a-lista-de-marcas-mais-imitadas-em-ataques-de-phishing/. Acesso em: 22 abr. 2023.

TI INSIDE. **Pesquisa: 66% das organizações foram atingidas por *ransomware* em 2021**. [S.l.]. Redação, 2022. Disponível em: https://tiinside.com.br/09/05/2022/66-das-organizacoes-foram-atingidas-por-*ransomware*-em-2021-diz-relatorio/. Acesso em: 14 jan. 2023.