arcserve®

Proteja o que tem valor inestimável.

SEU GUIA PARA UM FUTURO SEM RANSOMWARE

UMA ABORDAGEM PROATIVA PARA ENFRENTAR A AMEAÇA DO RANSOMWARE

WHITE PAPER

O RANSOMWARE TORNOU-SE UM DOS MAIORES RISCOS PARA OS NEGÓCIOS E A AMEAÇA MAIS TEMIDA PELAS ORGANIZAÇÕES DE TI.

O ransomware tornou-se um dos maiores riscos para as empresas e a ameaça mais temida para os departamentos de TI. Já pode ser considerado uma epidemia mundial com custos estimados em US$ 20 bilhões para 2021[1].
Mas o cenário não precisa ser tão terrível assim para os profissionais de TI e tomadores de decisão das empresas. Embora os criminosos cibernéticos não deem sinais de que diminuirão o ritmo, os avanços na tecnologia de combate ao crime cibernético e de recuperação de desastres aliados às boas práticas de gerenciamento de TI permitem que as empresas revidem.
Este relatório analisa a ameaça crescente do ransomware, as tecnologias e práticas de gerenciamento de TI que estão sendo utilizadas como defesa, e apresenta uma abordagem para que se chegue a um futuro sem ransomware.

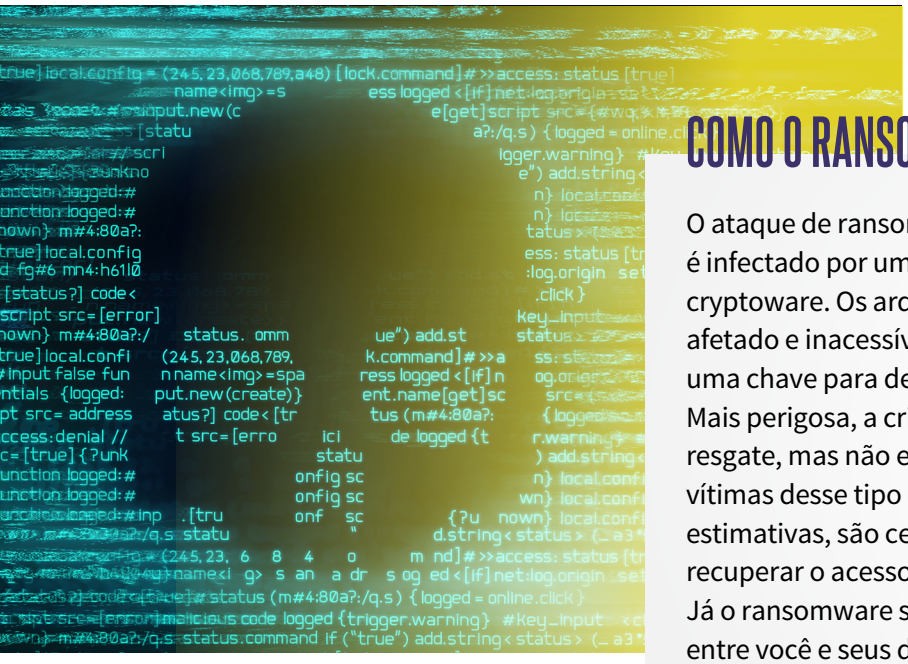
CONHEÇA SEU INIMIGO

O estrategista militar chinês Sun Tzu aconselhou sabiamente: "Conheça seu inimigo". Para desenvolver uma estratégia de proteção contra o ransomware para os sistemas de TI, é preciso conhecer bem essa ameaça. Então, vamos começar entendendo melhor o que é o ransomware.

Os dados são vitais para sua empresa. Eles revelam como a empresa trabalha em todos os departmentos. Eles mostram o que aconteceu no passado, revelam o estado atual dos negócios e apoiam as decisões. Sem eles, podemos dizer que não se faz negócios. O ransomware explora exatamente isso.

O ransomware é um software malicioso criado para impedir o acesso aos sistemas ou dados do seu computador até que um resgate seja pago. Ele pode interromper seus negócios e, se for do tipo leakware ou extortionware, vai além ameaçando extrair e divulgar seus dados.

Qualquer empresa com dados importantes armazenados em computadores ou redes corre risco, ou seja, hoje em dia, praticamente todas. Os alvos preferenciais são os órgãos públicos locais, órgãos de segurança pública, instituições de saúde, bancos e operadoras de cartão de crédito. O roubo de identidade causou um prejuízo de US$ 14,7 bilhões para os consumidores em 2018[2]. As vítimas não são só as grandes organizações. Os ataques de ransomware atingiram tanto consumidores como pequenas e grandes empresas.



COMO O RANSOMWARE FUNCIONA?

O ataque de ransomware acontece quando um computador é infectado por um vírus. A maioria dos ransomwares é um cryptoware. Os arquivos ficam criptografados no computador afetado e inacessíveis até que seja pago um resgate em troca de uma chave para decodificá-los. Mas cuidado com o que você paga. Mais perigosa, a criptografia falsa criptografa os arquivos e exige resgate, mas não envia uma chave de decodificação válida. As vítimas desse tipo de ransomware, que, segundo algumas estimativas, são cerca de 50% dos casos de ataque, podem nunca recuperar o acesso aos arquivos, mesmo depois de pagar o resgate. Já o ransomware sem criptografia coloca uma tela de bloqueio entre você e seus dados, sem criptografar nada diretamente.

O ransomware pode atacar arquivos específicos ou todo o sistema pelo MBR (Master Boot Record) de um drive ou o NTFS da Microsoft, impedindo a inicialização do sistema operacional. Para evitar ser detectado, ele usa uma rede de tráfego criptografado como HTTPS ou Tor. Diferente de outros tipos de malware que podem operar em segundo plano, assim que se infiltra no host azarado, o ransomware aparece exigindo criptomoedas não rastreáveis para pagamento do resgate.

Basta uma ação insignificante e involuntária de um usuário inocente, como clicar em um link malicioso, por exemplo, para que um computador seja infectado. O ransomware geralmente se espalha por e-mails de phishing, mas os criminosos cibernéticos usam inúmeras técnicas para infectar as vítimas com ransomware. Normalmente, a infecção ocorre ao abrir um anexo de e-mail ou clicar em um link falso. Os vetores mais comuns para disseminar malware são:

- **E-mails e mensagens de texto** contendo links que baixam um malware ou um anexo com malware.
- **Sites** cujo único objetivo é atrair usuários e fazê-los clicar em um link ou download malicioso.
- **Malvertising** ou anúncios maliciosos que são truques que levam a clicar e fazer downloads indesejados
- **Mídias sociais**, que aparentemente estão ligadas a fontes confiáveis, mas que levam a um criminoso cibernético desonesto. As vítimas involuntárias são infectadas diretamente por um aplicativo da mídia social ou são atraídas para um link ou anúncio enganoso.
- **Usuários de aplicativos móveis** que fazem o download voluntariamente para o dispositivo, sem perceber que são realmente falsos e projetados para transferir um vírus na próxima vez que o dispositivo móvel for conectado a um computador.

Os hackers estão cada vez mais sofisticados. Eles enviam anexos infectados em um e-mail que parece ser de alguém da lista de contatos do usuário. Embora as políticas de uso e o treinamento sejam úteis para reduzir o comportamento de risco dos usuários, é impossível eliminar por completo essa vulnerabilidade porque os pontos de entrada nem sempre são tão óbvios. O conteúdo malicioso pode explorar vulnerabilidades no navegador ou nos plugins e executar código malicioso sem o conhecimento do usuário. Assim que penetra em um host, a infecção pode se espalhar com facilidade para outros computadores da mesma rede. Além de atrair os usuários a baixar o ransomware sem saber, os criminosos cibernéticos obtêm acesso aos sistemas pela Internet quando ninguém está vendo. Eles usam métodos de ataque por "força bruta" e credenciais compradas na "dark web" para obter acesso a recursos e dados, usando o protocolo RDP (Remote Desktop Protocol) e vulnerabilidades de software.

Um relatório de 2019 revelou que, entre as empresas públicas e privadas, os alvos mais comuns dos ataques de ransomware são os ativos de maior valor, como os servidores, a infraestrutura de aplicativos e as ferramentas de colaboração. Embora os departamentos de TI deem prioridade às tendências e vulnerabilidades mais críticas, as mais antigas ou menos críticas não podem ser ignoradas. No relatório, as vulnerabilidades mais antigas (com três anos ou mais) foram vítimas de mais de um terço dos ataques, sendo que mais da metade visava as vulnerabilidades menos críticas[3].

EM MÉDIA, OS ATAQUES DE RANSOMWARE CAUSAM CERCA DE 10 DIAS DE INATIVIDADE[4].

Quais são os impactos de uma infecção de ransomware?

A avalanche de notícias sobre ataques de ransomware e as estatísticas assustadoras já deixaram as empresas cientes e as levaram a procurar soluções de segurança ou de proteção de dados eficazes. O efeito imediato de um ataque de ransomware é uma grande interrupção nas operações da empresa, quando os dispositivos e sistemas ficam inativos para a desinfecção e, se tudo der certo, a restauração total dos dados limpos, que é possível graças a uma estratégia bem planejada de backup e recuperação de desastres. Em média, os ataques de ransomware causam cerca de 10 dias de inatividade[4].

Embora a recomendação seja não pagar o resgate, segundo o FBI, foram pagos mais de US$ 2,57 milhões em 2018[5]. Em média, uma empresa pode esperar um custo médio de US$ 133.000 por ataque para recuperar o acesso aos seus próprios dados . Infelizmente, algumas vítimas pagam, sem garantia de que vão recuperar seus arquivos e dados[6]. Estudos revelam que os autores dos ataques de ransomware geralmente ganham mais do que o dobro do salário médio dos desenvolvedores que trabalham em projetos legítimos[7]. Obviamente, o que é bom para os invasores, não é bom para as empresas nem para e sua equipe de profissionais de TI.

USD 2,57
MILHÕES PAGOS EM RESGATE[5]

USD 133,000
CUSTO MÉDIO POR ATAQUE[6]

As empresas torcem muito para que suas defesas contra o ransomware funcionem. Mas, mesmo que consigam impedir o pior, ou pelo menos parcialmente, elas ainda têm que enfrentar a perda de dados resultante do ataque. A média de perdas no caso de um ataque é de cerca de 8% dos dados[8]. Além de tentar receber um resgate, os criminosos podem extrair dados de um computador ou servidor comprometido, expondo informações confidenciais, como nomes de usuário e senhas, dados de pagamento e e-mails de contatos. O ransomware moderno ataca arquivos de backup compartilhados na rede e pode até excluir cópias sombra da estação de trabalho para impedir a restauração. O ataque e a consequente perda de dados são um golpe duplo poderoso, e os riscos à reputação da marca podem ter um impacto devastador de longo prazo que afeta seriamente a credibilidade.

> *"Os criminosos cibernéticos estão cada dia mais sofisticados em suas táticas e, aparentemente, nenhum setor está imune aos ataques de ransomware. Usando como alvo os sistemas de backup, os hackers têm mais chances de fazer as empresas comprometidas pagarem os resgates por causa das graves consequências relacionadas à perda de dados e ao tempo de inatividade, que costumam causar sérias consequências além do prejuízo financeiro. Os responsáveis pela TI e pela área administrativa também precisam considerar o impacto negativo na produtividade dos funcionários, na confiança dos clientes, na reputação da marca e na conformidade regulamentar quando os sistemas e dados ficam comprometidos."*
>
> *- Oussama El-Hilali, diretor de tecnologia da Arcserve*

Como os profissionais de TI estão protegendo suas empresas contra o ransomware?

Vários métodos são usados para detectar ransomware e proteger sistemas e dados valiosos, entre eles:

- **Software de proteção contra ransomware** para identificar possíveis ataques, detectando e evitando invasões prontamente.
- **Firewall** para bloquear o acesso não autorizado a um computador ou rede.
- **Filtros de arquivo e filtros de spam** que bloqueiam sites suspeitos de malware e impedem que anexos indesejados entrem na caixa de entrada de e-mail do usuário.
- **Software para definição de políticas para grupos** que bloqueia a execução de arquivos em pastas locais que podem infectar o sistema.
- **Pacotes de gerenciamento de informações e eventos de segurança** (SIEM) que fornecem informações sobre o tráfego de rede para detectar anomalias que indicam uma violação.
- **Software de backup** para proteger dados comerciais, copiando dados de servidores, bancos de dados, desktops, laptops e outros dispositivos.
- **Monitoramento da integridade do arquivo** para verificar a consistência entre o arquivo atual e um arquivo validado.
- **Software antivírus e antimalware** para evitar, detectar e remover malware.
- **Soluções de gerenciamento unificado de ameaças (UTM)** para lidar com diversas ameaças com um único ponto de defesa e console.

Embora cada um dos métodos seja importante e útil para detectar ransomware e proteger dados e sistemas valiosos, as empresas estão correndo um grande risco. Os invasores estão cada vez mais sofisticados e engenhosos. As estratégias de ataque geralmente combinam várias técnicas simultaneamente, visando partes separadas da rede de TI ao mesmo tempo. Os ataques de ransomware usam novas variantes de malware para driblar os programas antivírus. Quais são os pontos fracos das estratégias tradicionais de proteção contra ransomware?

Muitos sistemas não têm funcionalidades importantes

Era mais fácil resolver o problema do malware quando as explorações podiam ser combatidas com tecnologia antivírus por assinatura. Com a evolução das ameaças, fazendo ataques distintos contra vulnerabilidades comuns, ficou bem mais difícil detectá-las usando a tecnologia por assinatura.

Além disso, muitos fornecedores de proteção de dados resolveram pensar só no ransomware, enfatizando "recursos" de segurança cibernética que, na realidade, só detectam as anomalias nos dados que podem ou não estar relacionadas a ransomware. E, quando a anomalia é detectada, geralmente as soluções emitem só um alerta, em vez de fazer alguma coisa para resolver o problema.

É difícil gerenciar várias ferramentas diferentes, o que aumenta a vulnerabilidade

Muitas empresas trabalham com diferentes ferramentas e fornecedores para várias funções de segurança de combate ao ransomware. Por exemplo, pode ser que elas usem dois provedores de firewall, um de DLP ou filtros da internet, um de solução de backup e recuperação de desastres, um de backup em nuvem, um de datacenter e outro de backup de dispositivos móveis.

O uso de dispositivos e provedores diferentes para as diversas tarefas de segurança torna ainda mais difícil rastrear e impedir os ataques. Ferramentas e softwares exigem gerenciamento e atualização. Fica difícil manter tudo atualizado com os tipos mais recentes de malware quando se combinam várias soluções. Administrar vários fornecedores e soluções aumenta o risco, a vulnerabilidade e o erro. A produtividade é afetada e os custos crescem.

Hoje, você pode transformar uma combinação de ferramentas complexas de ransomware antigas e de diferentes fornecedores usando uma única solução de defesa poderosa que oferece backup e recuperação de dados abrangentes, rede neural e proteção de pontos de extremidade contra malwares desconhecidos, exploits e ransomware.

Os profissionais de TI também precisam de práticas de gerenciamento de TI

As soluções tecnológicas são vitais para a segurança cibernética e a proteção contra ransomware, como firewall, sistema de detecção e prevenção de invasão e segurança de e-mail. As soluções avançadas e integradas de segurança e proteção de dados contribuem muito para proteger a empresa, mas boas práticas de gerenciamento de TI também são fundamentais.

É importante reconhecer que o comportamento do usuário final é a maior ameaça. As empresas precisam implementar controles de gerenciamento de TI que detectem quando os funcionários estão ignorando uma política ou procedimento. As práticas de gerenciamento devem incluir o envolvimento ativo do usuário, informando que eles devem mudar de comportamento para maior segurança.

Os profissionais de TI também devem observar o portfólio geral de TI e avaliar os riscos. Embora qualquer sistema seja suscetível a ataques, os criminosos estão mais interessados nas informações de valor que não estão devidamente protegidas. As empresas precisam priorizar a proteção dos recursos e fazer um gerenciamento proativo da TI, incluindo RPOs (objetivos de pontos de recuperação) para considerar o volume da perda de dados aceitável no caso de um problema e reforçar as defesas. Elas precisam saber quais recursos estão disponíveis, como eles estão configurados e controlar de perto qualquer alteração.

Uma estrutura como a ITIL (Information Technology Infrastructure Library) pode ajudar as empresas a implementar as práticas recomendadas de gerenciamento da TI. A ITIL fornece práticas para gerenciamento de configuração, alteração e versão para que as principais organizações de processos reforcem a segurança cibernética e a proteção contra a ameaça do ransomware.

FICAR TOTALMENTE PROTEGIDO CONTRA O RANSOMWARE É UM OBJETIVO REALISTA?

Evitar um ataque de ransomware multifacetado exige uma defesa coordenada que combine a tecnologia certa com boas práticas de gerenciamento de TI. O ideal é uma solução de segurança e proteção multicamada, de ponta a ponta.
Implantando a primeira e a última linha de defesa contra o ransomware, os departamentos de TI poderão acabar com a ameaça do ransomware e transformar a maneira como protegem e defendem os dados das empresas contra chantagistas, hackers e ladrões

Uma pesquisa global recente com profissionais de TI revelou que dois em cada três entrevistados acreditam ser muito importante encontrar soluções que combinem segurança e proteção de dados[9]. Os entrevistados consideram isso ainda mais importante do que contar com soluções que agregam IA à prevenção de desastres ou que automatizam a conformidade[10].

ESTRATÉGIAS DE PROTEÇÃO CONTRA O RANSOMWARE

Apresentamos **cinco estratégias de proteção contra ransomware** que podem ajudar sua empresa a ir além das abordagens de segurança reativas e integrar tecnologias contra ransomware e outras de prevenção de ameaças aos recursos de recuperação de desastres e alta disponibilidade para neutralizar os ataques cibernéticos

1 Gerencie ativamente o acesso

Defina os controles e procedimentos necessários para proteger os aplicativos e sistemas de usuários não autorizados.

- Restrinja o acesso a pontos de entrada comuns de ransomware, como contas de e-mail pessoais e sites de redes sociais. Use filtros da internet no gateway e no ponto de extremidade para bloquear as tentativas de phishing que induzem os usuários a clicar em um link.
- Use autenticação multifatorial e padrões avançados de senha. Inclua requisitos de senha quando os usuários se comunicarem com sites não categorizados pelo proxy ou firewall.
- Use servidores proxy e software de bloqueio de anúncios e restrinja as permissões para instalar e executar aplicativos de software.
- Controle e monitore terceiros que tenham acesso remoto à rede da empresa e suas conexões com terceiros para garantir que sigam as práticas recomendadas de segurança cibernética.
- Use a lista de permissões de aplicativos para permitir que apenas os programas aprovados sejam executados na rede.

2 Gerencie a configuração dos sistemas nos vetores de ataque

Implemente sistemas e procedimentos de gerenciamento centralizado que incluam todo o espectro de ameaças de ransomware.

- Avalie e categorize dados confidenciais da empresa e faça uma separação física e lógica dos servidores, redes e repositórios de dados.
- Verifique se as soluções antivírus e contra malware estão habilitadas para serem atualizadas automaticamente. Faça uma varredura nos e-mails recebidos e enviados para detectar phishing, impedir spoofing de e-mails e filtrar arquivos executáveis.
- Use um sistema centralizado de gerenciamento de patches para corrigir todos os pontos de extremidade no caso de descoberta de vulnerabilidades, inclusive em dispositivos móveis, sistemas operacionais, softwares, aplicativos, locais na nuvem e IoT.
- Implemente tecnologias de deep learning, contra exploração e ransomware sem assinatura que detectem malwares conhecidos e desconhecidos.
- Implemente tecnologias integradas de proteção de pontos de extremidade e de continuidade dos negócios para acelerar a prevenção de ameaças e possibilitar a restauração imediata dos dados.
- Proteja aplicativos e servidores da Web usando firewalls de aplicativos webb.
- Desabilite scripts de arquivos do Microsoft Office enviados por e-mail e considere o uso do software Office Viewer para abrir arquivos do Office.

- Audite sua rede em busca de sistemas que usem o Remote Desktop Protocol, feche as portas não utilizadas e use autenticação de dois fatores.
- Detecte, diagnostique como malicioso e bloqueie comportamentos como a criptografia de arquivos em massa.
- Coloque um banner de aviso nos e-mails de fontes externas, lembrando os usuários do perigo de clicar em links e abrir anexos.
- Use os dispositivos de Gerenciamento Unificado de Ameaças (UTM) que combinam firewall, antivírus no gateway e recursos de detecção e prevenção de invasão para bloquear o acesso a endereços IP maliciosos conhecidos.

3 Combine soluções de segurança e proteção de dados

Integre, teste e mantenha uma segurança cibernética e proteção de dados abrangente, de ponta a ponta.

- Proteja os repositórios de backup contra malware, ransomware e ataques de dia zero.
- Interrompa e remova ameaças como malware e ransomware dos backups.
- Mantenha o backup dos dados em dispositivos separados e use armazenamento offline para que eles não possam ser acessados diretamente por dispositivos infectados.
- Faça backup de máquinas virtuais, armazenamento em nuvem e sistemas operacionais baseados em RPO, considerando um volume de perda de dados aceitável no caso de um problema.
- Use um sistema que permita que várias iterações de backups sejam salvas, caso uma cópia dos backups contenha arquivos criptografados ou infectados.
- Integre dispositivos para recuperação de desastres e disponibilidade de aplicativos e use inteligência artificial na proteção de pontos de extremidade.
- Verifique as vulnerabilidades e use criptografia SSL e outros controles técnicos para confirmar se os backups estão sendo feitos.
- Use a regra 3-2-1 criando três cópias dos dados, armazenando tudo em duas mídias diferentes, sendo uma delas fora da empresa.
- Teste regularmente os backups quanto à integridade dos dados e para garantir que estejam operacionais
- Teste regularmente os dados e os processos de recuperação de desastres para garantir a prontidão.

4 Dê treinamento e muita informação para os usuários

Capacite os usuários com treinamento e as práticas necessárias para que eles se protejam contra as ameaças de ransomware.

- Forneça treinamento e informação regularmente para que todos na sua empresa fiquem cientes da ameaça do ransomware e conheçam as técnicas de segurança.
- Defina políticas e procedimentos de segurança e prevenção de ransomware para o usuário final.
- Oriente os usuários a não abrir e-mails suspeitos, clicar em links, abrir anexos, a ter cuidado ao entrar em sites desconhecidos e a fechar o navegador quando não estiver em uso.
- Garanta que os funcionários saibam onde e como denunciar atividades suspeitas.

5 Mantenha e teste um plano de continuidade dos negócios e recuperação de desastres

Defina, teste e mantenha as práticas, procedimentos e ferramentas de tecnologia para garantir que os aplicativos e dados sejam totalmente recuperados no caso de um desastre.

- Defina planos de contingência e correção. Eles são essenciais para a recuperação e continuidade dos negócios, seja qual for o motivo da interrupção.
- Faça uma avaliação de risco que classifique os tipos de desastre que podem acontecer e estabeleça prioridades para a recuperação e continuidade dos negócios.
- Implante soluções de recuperação de desastres, backup e alta disponibilidade dentro e fora da empresa.
- Tenha um plano de resposta a incidentes que indique o que fazer durante um evento de ransomware, inclusive como desconectar o sistema infectado da rede para impedir que a infeção se propague, de acordo com o nível de confidencialidade dos dados.
- Teste o plano, sistemas e dispositivos de tecnologia para garantir a proteção completa.
- Relate qualquer infecção aos órgãos apropriados.

VOCÊ ESTÁ PREPARADO PARA ENFRENTAR O RANSOMWARE?

Baixe a ferramenta de **Avaliação de prontidão para enfrentar o ransomware** para avaliar seus recursos e traçar um plano para um futuro sem ransomware.

NOVA TECNOLOGIA PROMETE UM FUTURO SEM RANSOMWARE

Há anos, os profissionais de TI procuram, sem sucesso, uma solução de segurança e proteção de dados multicamada, de ponta a ponta, que dê resiliência à TI e previna contra o ransomware. A boa notícia é que ela já existe e oferece a primeira e última linha de defesa contra a ameaça do ransomware.

A solução combina Arcserve Appliance Series com o Sophos Intercept X Advanced for Server em uma abordagem multicamada que fornece proteção e segurança de dados completas, tudo em uma plataforma unificada.

Os usuários têm acesso a recursos abrangentes de sistemas independentes que acabam com a necessidade de usar uma solução inteira só por causa de alguns componentes. Uma interface centralizada administra os processos, ferramentas e a infraestrutura de backup. Os Arcserve Appliances combinam armazenamento desduplicado acelerado por flash, o processamento poderoso do servidor e rede de alta velocidade com redundância de hardware e serviços em nuvem.

Adicione a proteção de ponto de extremidade do Sophos Intercept X Advanced for Server para ter uma solução de ponta a ponta que inclui detecção de malware por assinatura e sem assinatura, inteligência artificial avançada/rede neural (deep learning), tecnologia contra exploits e ransomware para proteger contra a mais ampla gama de ameaças aos pontos de extremidade.

O resultado é uma combinação incomparável de “tudo em um”, ou seja, segurança cibernética do começo ao fim, backup de dados, recuperação de desastres e alta disponibilidade, tudo em uma única solução que atende a todas as necessidades da infraestrutura.

RESUMO

Embora o ransomware represente um risco comercial significativo e uma grande ameaça, o futuro é promissor. Hoje as empresas podem:

- **Implementar soluções integradas e abrangentes de proteção** com recursos avançados de backup, recuperação de desastres, alta disponibilidade e segurança cibernética;
- **Adotar práticas de TI** com envolvimento real do usuário, gerenciamento de dados e práticas de recuperação de desastres com ótimo retorno do investimento (ROI); e
- **Contar com a primeira e a última linha de defesa** para acelerar a detecção de ameaças e possibilitar a restauração imediata dos dados de backup.

Então, por que aceitar o status quo? Por que se sujeitar a um mundo em que chantagistas cibernéticos, hackers e ladrões usam o ransomware para obter ganhos ilícitos de empresas que só estão tentando trabalhar? Contra-ataque. Mantenha seus dados seguros. Use uma tecnologia de proteção de ponta a ponta atual e boas práticas de gerenciamento de TI para garantir que você e sua empresa, finalmente, tenham um futuro sem ransomware.

SOBRE A ARCSERVE

A Arcserve fornece soluções excepcionais para proteger os ativos digitais inestimáveis de empresas que precisam de proteção abrangente e em larga escala dos dados. Fundada em 1983, a Arcserve é o nome mais experiente do mundo em soluções para a continuidade de negócios, protegendo infraestruturas de TI de diferentes gerações com aplicações e sistemas em qualquer local, dentro da empresa e na nuvem. Organizações em mais de 150 países confiam na experiência, no conhecimento e nas tecnologias integradas e altamente eficientes da Arcserve para eliminar os riscos de perda de dados e de inatividade prolongada, reduzindo em até 50% os custos e a complexidade da realização de backup e recuperação de dados.

SOBRE A SOPHOS

Mais de 100 milhões de usuários em 150 países confiam no Sophos como a melhor proteção contra ameaças complexas e perda de dados.

O compromisso da Sophos é fornecer soluções de segurança completas, fáceis de implementar, gerenciar e usar, que proporcionam o menor custo total de propriedade do setor. A Sophos oferece criptografia premiada, segurança para pontos de extremidade, web, e-mail, celular, servidor e segurança de rede com o suporte do SophosLabs, uma rede global de centros de inteligência de ameaças.

RECURSOS

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[2] https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt https://www.aarp.org/money/scams-fraud/info-2019/survey-identity-fraud-decline.html

[3] https://risksense.com/press_release/risksense-spotlight-report-exposes-top-vulnerabilities-used-in-enterprise-ransomwareattacks/

[4] https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

[5] https://pdf.ic3.gov/2018_IC3Report.pdf

[6] https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacksaccording-to-sophos-global-survey.aspx

[7] https://twitter.com/CarbonBlack_Inc/status/925348051782373382

[8] https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

[9] Encuesta de Arcserve EMEA, 31 de julio de 2019

[10] Encuesta de Arcserve EMEA, 31 de julio de 2019

Para mais informações sobre a Arcserve, **acesse** **www.arcserve.com/br**