arcserve®

Não faça parte das estatísticas:

Antecipe-Se Aos Criminosos Cibernéticos Implementando Uma Estratégia Holística De Proteção Contra Ransomware

Nos ambientes corporativos de hoje, sempre ativos e baseados em dados, as ameaças cibernéticas são a maior preocupação das equipes de segurança de TI.

O ransomware, em particular, é a causa de muitas noites sem dormir. A frequência dos ataques está aumentando, e as últimas cepas e táticas estão cada vez mais direcionadas, destrutivas e difíceis de serem detectadas rapidamente.

Por exemplo, desde 2019, houve pelo menos 440 ataques de ransomware direcionados contra setores com infraestruturas essenciais, como da saúde, de serviços financeiros, do governo e da educação. E, em 2020, a COVID-19 deu início a uma tendência de golpes de phishing e ataques de ransomware com o tema da pandemia, cujo alvo eram funcionários distraídos em busca de respostas e conforto em um momento tão incerto.

O ransomware continua a evoluir, com novas táticas e tecnologias surgindo regularmente, entre elas:

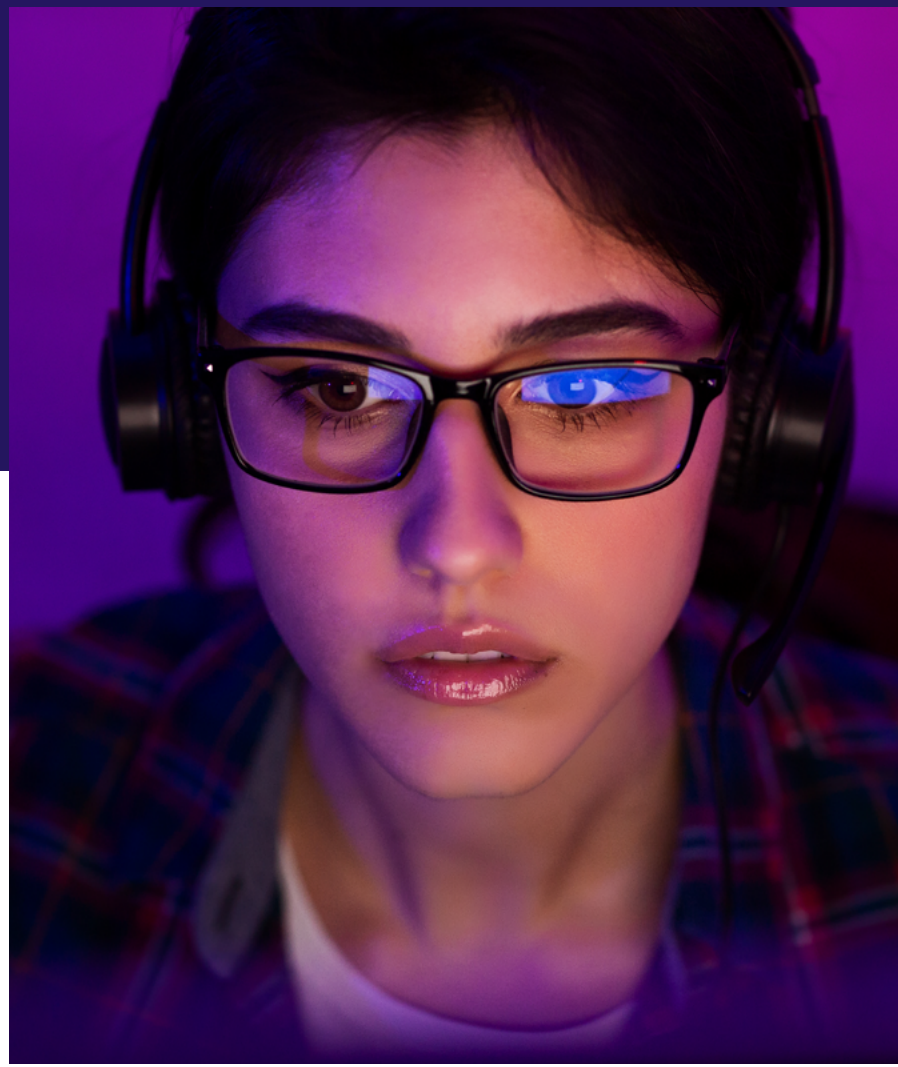
Dupla extorsão
Os criminosos criptografam e publicam os dados na internet.

Criptografia dormente
O ransomware permanece inativo por um período antes de criptografar seus dados, esperando pelos backups.

O alvo é o backup
Algumas cepas de ransomware buscam e criptografam os arquivos de backup, tornando a recuperação de desastres um pesadelo.

Como os ambientes de TI de hoje facilitam a entrada de ransomware

A natureza e a estrutura dos ambientes de TI modernos criaram um ecossistema com muitas partes móveis e sistemas diferentes.



Essa dispersão, invariavelmente, amplia a superfície de ataque da empresa e torna mais difícil se defender do ransomware. As vulnerabilidades mais exploradas têm origens comuns.

Altos níveis de complexidade

As infraestruturas de TI de hoje são bem mais complexas. Muitas empresas têm dificuldade para dar suporte e proteger sua ampla variedade de plataformas e aplicativos. As equipes de TI, muitas vezes, têm que fazer malabarismo para atender aos inúmeros elementos da infraestrutura, como:

- Infraestrutura on premises e de nuvem pública, privada e híbrida
- Dispositivos e computadores móveis
- Soluções como SaaS (software como serviço), PaaS (plataforma como serviço) e IaaS (infraestrutura como serviço)
- E muito mais

Risco do provedor terceirizado

Quando você trabalha com terceiros, é muito importante verificar se eles levam a segurança cibernética tão a sério quanto você. Cada ponto de acesso, rede e banco de dados compartilhado é uma oportunidade para os operadores de ransomware, daí a importância de uma auditoria prévia e uma avaliação da segurança dos terceiros.

Equipes distribuídas

A COVID-19 transformou quase todas as equipes em equipes distribuídas. Mas, com pouco tempo para se preparar para a transição, as empresas tiveram que providenciar um suporte e uma infraestrutura de segurança que fossem “bons o suficiente”. Em muitos casos, na verdade, eles não eram “bons o suficiente”, o que tornou os funcionários remotos alvos fáceis de pessoas mal-intencionadas.

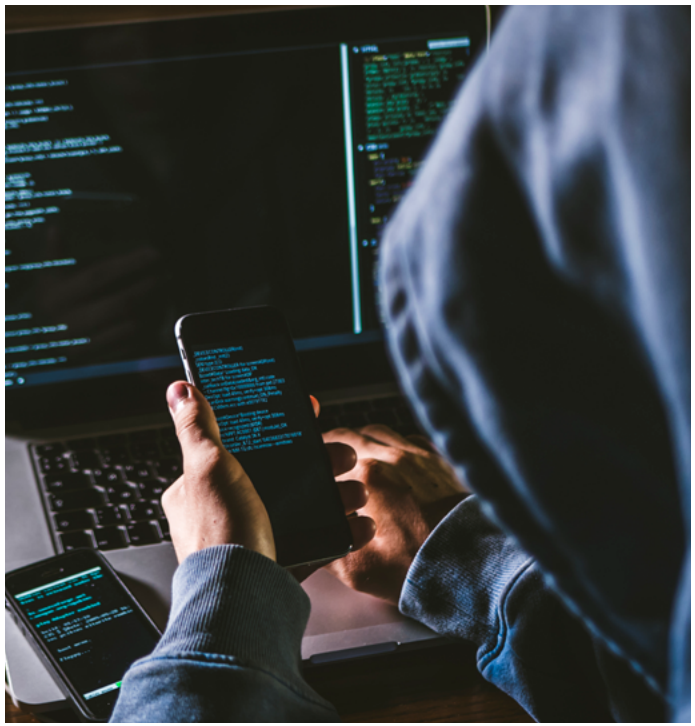
Patches e atualizações não aplicadas

As atualizações de segurança e patches são demorados e cansativos, mas também são as melhores formas de prevenir o ransomware. Estudos mostram que uma em cada três violações de segurança poderia ser evitada se o patch fosse atualizado. A realidade é que está sendo liberada uma quantidade enorme de patches, e as equipes de TI são enxutas demais para dar conta.

Sistemas legados

Os sistemas e softwares legados são um convite para os operadores de ransomware. Os sistemas mais antigos não têm uma boa integração com as soluções de segurança cibernética mais recentes, ou seja, não ficam protegidos como deveriam.

A COVID-19 transformou quase todas as equipes em equipes distribuídas. Mas, com pouco tempo para se preparar para a transição, as empresas tiveram que providenciar um suporte e uma infraestrutura de segurança que fossem “bons o suficiente”.



Somando os custos diretos e indiretos do ransomware

O impacto de um ataque de ransomware bem-sucedido varia bastante de uma empresa para outra, dependendo do setor, nível de risco e gravidade. No entanto, as empresas não podem se esquecer de uma verdade universal: o dano causado pelo ransomware vai muito além do ataque inicial.

Os impactos mais óbvios e imediatos do ransomware são inúmeros e incluem:

- Tempo de inatividade e perda de produtividade causados pela criptografia dos dados
- Perda de receita como resultado do tempo de inatividade
- Possível perda de dados quando os backups estão incompletos ou desprotegidos
- Custos diretos associados à tarefa de limpeza e pagamento de resgate (se você decidir ir nessa direção, o que não recomendamos)

No entanto, há vários impactos menos tangíveis, mas igualmente prejudiciais. São impactos de longo prazo sobre os quais você precisa estar ciente. Por exemplo, é difícil quantificar os danos causados à reputação da sua empresa. As violações de segurança afetam a confiança dos clientes e das partes interessadas da sua empresa. Pode ser que você note uma diminuição de novos clientes, uma migração repentina de clientes para outro provedor de soluções ou perda da vantagem competitiva.

Dependendo do seu setor e da gravidade da violação, sua empresa também pode ter que resolver problemas de normas e conformidade ou enfrentar processos judiciais que resultam em multas e penalidades pesadas.

As violações de segurança afetam a confiança dos clientes e das partes interessadas da sua empresa. Pode ser que você note uma diminuição de novos clientes, uma migração repentina de clientes para outro provedor de soluções ou perda da vantagem competitiva.

Adotando uma abordagem holística de proteção contra ransomware

Diante de tantos tipos novos de ameaças de ransomware, muitas empresas acham que suas antigas estratégias de segurança e mitigação não são mais suficientes. Por isso, as equipes de segurança de TI estão adotando soluções holísticas e proativas para combater o ransomware.

A abordagem holística de proteção contra ransomware é como colocar um campo de força ao redor da sua empresa. Ela combina uma estratégia de segurança abrangente que bloqueia o acesso e minimiza os danos à sua infraestrutura de TI, tomando medidas ofensivas e defensivas.

A proteção total contra ransomware envolve uma mistura de:

- **Ferramentas e tecnologias de segurança cibernética**
- **Recursos de recuperação orquestrados**
- **Planos práticos para gerenciar pessoas, políticas e processos**

Ferramentas e tecnologias de segurança cibernética

O objetivo principal das equipes de segurança de TI é proteger a infraestrutura multigeracional e os dados essenciais para os negócios. Como parte da estratégia holística de proteção contra ransomware, a segurança cibernética abrange desde a proteção de endpoints e firewalls até o gerenciamento de identidade e acesso, e prevenção da perda de dados.

Para responder aos desafios atuais do ransomware, sua solução de segurança cibernética precisa ter uma tecnologia de detecção e prevenção, que inclua:

- Detecção de malware baseada em assinatura e sem assinatura
- Uma rede neural de deep learning
- Tecnologia anti-exploit, como o Sophos Intercept X Advanced

Recursos orquestrados de recuperação

O cenário ideal seria poder evitar 100% dos ataques de ransomware, 100% do tempo, mas a verdade é que, em algum momento, é bem provável que a sua empresa seja um alvo. A recuperação rápida após uma crise depende do seu nível de preparo e recursos de orquestração, o que deve ser contemplado na sua estratégia de proteção holística.

Empresas com mais flexibilidade contam com um plano de recuperação de desastres (DR) testado e pronto para ser colocado em prática antes de ser necessário. Um dos principais componentes de um plano DR sólido é um backup seguro, completo e atualizado, mas isso por si só não é suficiente.

Seu plano de recuperação deve, sem dúvida, incluir backup na nuvem, mas você também precisa de proteção contra as novas cepas de ransomware que visam os arquivos de backup. A estratégia tradicional de backup 3-2-1 já não basta. Para garantir recuperação total, agora é preciso incluir backups fora das instalações, tornando-se um plano de backup 3-2-1-1.

Como mais empresas estão respaldando os funcionários remotos que usam soluções baseadas na nuvem, como o Microsoft Office 365, é fundamental ter um plano para proteger os aplicativos SaaS contra a perda de dados. Muitas soluções SaaS usam um modelo de responsabilidade compartilhada, e isso significa que, se você não está fazendo backup dos dados, você está procurando problema.

Medidas práticas para pessoas, políticas e processos

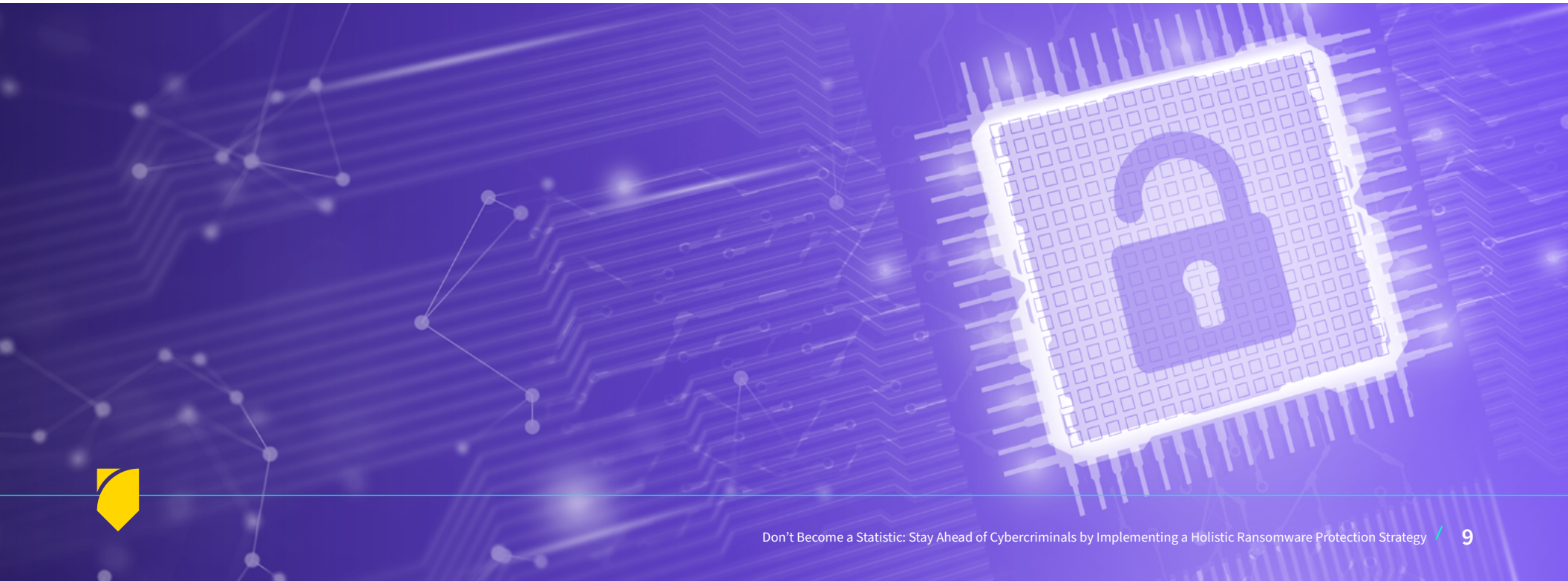
A parte humana, em geral, é o elo mais fraco das iniciativas de proteção contra ransomware. E se você pudesse transformar todos os funcionários em uma extensão da TI, para que eles se tornassem a primeira linha de defesa da sua empresa?

O treinamento é o primeiro passo para mitigar o erro humano. Entre as áreas que merecem atenção estão:

- Exercícios de recuperação de desastres de dados
- Treinamento em segurança cibernética, para que os funcionários saibam quais ameaças procurar
- Treinamento em conscientização de segurança para ensinar a eles o que fazer (ou não fazer) para evitar a violação de segurança e infecção de malware

Outras maneiras de minimizar o aspecto do erro humano das ameaças de ransomware é implementar políticas de acesso seguro, como autenticação de vários fatores e auditoria, incluindo verificação de antecedentes dos funcionários, avaliação de risco de terceiros e a boa e velha segurança física.

> **A parte humana, em geral, é o elo mais fraco das iniciativas de proteção contra ransomware.**



Como chegar a um futuro sem ransomware com o parceiro certo

Quando você estiver pronto para implementar uma estratégia holística de proteção contra ransomware, é importante trabalhar com um provedor de soluções com experiência nessa área.

Além de experiência, você precisa de alguém que compartilhe os mesmos valores da sua empresa e entenda o seu negócio.

Se você e seu parceiro falarem a mesma língua e compartilharem os mesmos objetivos, será muito mais fácil trabalhar em equipe para alcançar seus objetivos de negócios. O provedor de soluções certo pode ajudar você a implementar uma estratégia holística de ransomware ajudando a descobrir os principais componentes de um plano consistente de segurança de dados e sistemas.

Se você e seu parceiro falarem a mesma língua e compartilharem os mesmos objetivos, será muito mais fácil trabalhar em equipe para alcançar seus objetivos de negócios.

Integração e segurança

Integrar a segurança cibernética e a proteção de dados é a única forma de se proteger totalmente contra o ransomware. Adotando uma estratégia de proteção contra ransomware em uma solução que combina forças, como o Sophos Intercept X, Nutanix HCI and Arcserve Unified Data Protection, você consegue:

- Reduzir a complexidade da infraestrutura
- Melhorar os contratos de nível de serviço (SLAs)
- Integrar perfeitamente a proteção cibernética e de dados em cargas de trabalho on premises, na nuvem, em infraestrutura hiperconvergente (HCI) e baseadas em SaaS

Backup e recuperação

Vale ressaltar a importância de ter um backup seguro, testado e atualizado para fazer uma recuperação bem-sucedida após um ataque de ransomware ou outra interrupção não planejada. O parceiro certo pode ajudar sua empresa a encontrar soluções de backup e recuperação adequadas que atendam às suas necessidades atuais de armazenamento e proteção de dados e que possam ser dimensionadas conforme necessário no futuro.

Proteção de dados baseada em assinatura

É importante encontrar um parceiro que mantenha os objetivos e metas da sua empresa no centro de cada transação, principalmente na hora de planejar a verba da solução de proteção contra ransomware.

Quando você trabalha com um provedor de soluções que oferece licença universal, sente mais confiança de que todos os seus dados estarão protegidos e sabe exatamente pelo que está pagando. Não há nenhum custo oculto. Você paga só pelo que precisa e fica à vontade para ampliar ou reduzir a estrutura, se necessário.

Defender, evoluir e adaptar

O ransomware e outras ameaças cibernéticas vieram para ficar, portanto, nossa única opção é aprender a defender nossos sistemas, aplicativos e dados contra eles.

Essas ameaças estão sempre evoluindo e se adaptando, o que significa que temos que evoluir e adaptar nossas estratégias de segurança também.

A segurança total dos dados começa com uma abordagem gerenciada para proteger as infraestruturas de TI e os dados de backup de ataques cibernéticos, mas não termina aí.

O caminho para um futuro sem ransomware deve combinar tecnologia de segurança cibernética, backup e recuperação orquestrados, além de políticas, processos e treinamentos abrangentes para cobrir o lado humano da prevenção de ransomware. As equipes de segurança de TI precisam responder às ameaças de ransomware, de forma proativa e constante, com uma estratégia de proteção holística que muda de acordo com o cenário das ameaças.

O caminho para um futuro sem ransomware deve combinar tecnologia de segurança cibernética, backup e recuperação orquestrados, além de políticas, processos e treinamentos abrangentes para cobrir o lado humano da prevenção de ransomware.

arcserve®

Para saber como a Arcserve pode ajudá-lo a ficar à frente dos cibercriminosos, entre em contato abaixo.

SABER MAIS