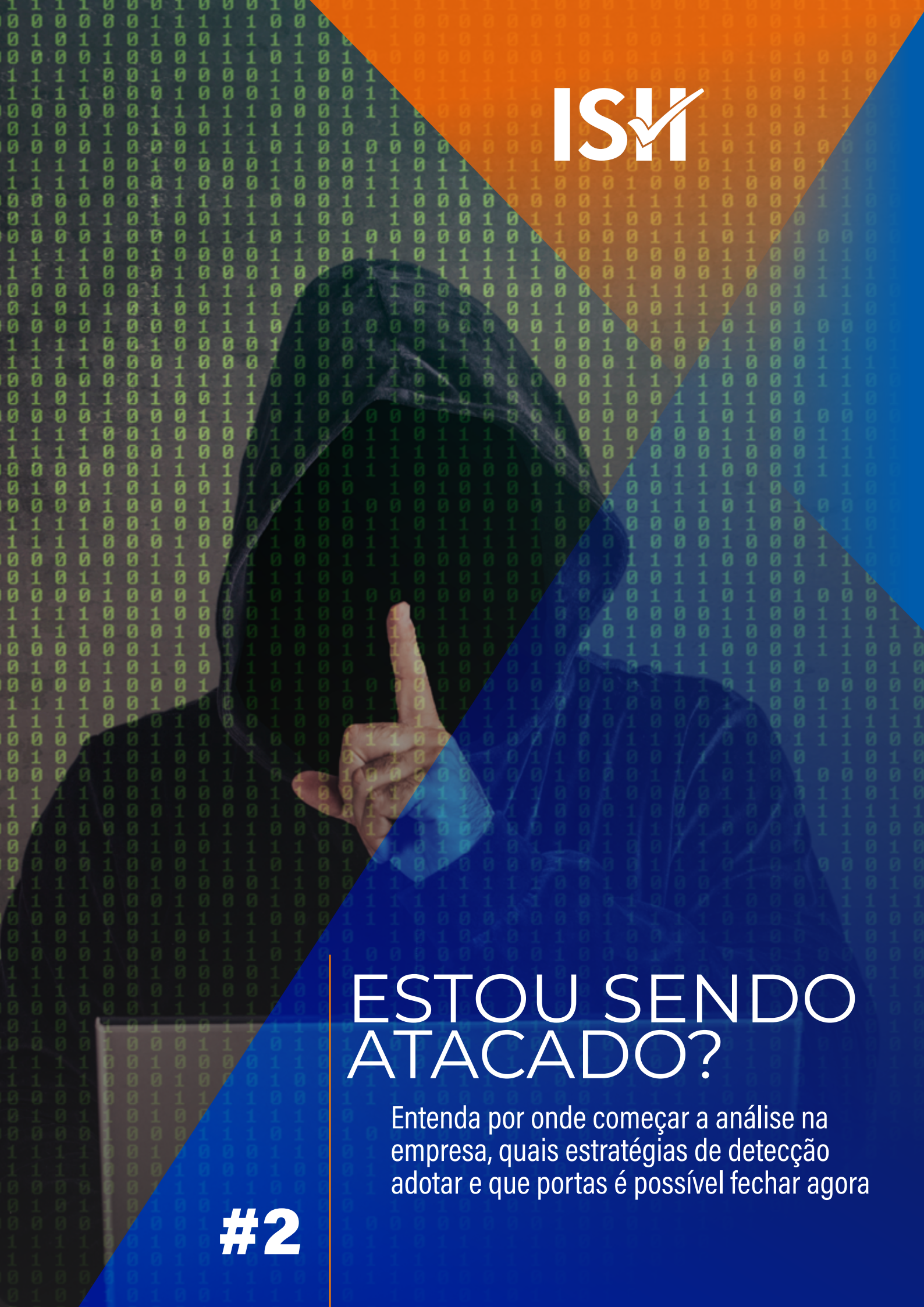

ISH

ESTOU SENDO ATACADO?

Entenda por onde começar a análise na empresa, quais estratégias de detecção adotar e que portas é possível fechar agora

#2

O que fazer para não ser infectado?

O CUSTO DE UMA INVASÃO DE DADOS AUMENTOU 12% NOS ÚLTIMOS CINCO ANOS. PASSOU PARA US$ 3,92 MILHÕES, EM MÉDIA. A VIOLAÇÃO DE DADOS TAMBÉM TRAZ IMPACTOS A LONGO PRAZO. ENQUANTO UMA MÉDIA DE 67% DOS CUSTOS DE ATAQUES SÃO PERCEBIDOS NO PRIMEIRO ANO, 22% ACUMULAM PARA O SEGUNDO E 11% VÃO ALÉM DE DOIS ANOS APÓS UMA INVASÃO.

O CUSTO DE UMA INVASÃO DE DADOS AUMENTOU 12% NOS ÚLTIMOS CINCO ANOS.

US$ 3,92 MILHÕES
EM MÉDIA

67% DE CUSTOS
PRIMEIRO ANO

22% DE CUSTOS
SEGUNDO ANO

11% DE CUSTOS
ACIMA DE DOIS ANOS

Ataques às empresas brasileiras representam o segundo maior crescimento do mundo. Nesse quesito, o Brasil perde apenas para a Índia. Portanto, há motivos para preocupação. Os hackers têm como alvo principal donos de empresas com proteção digital insuficiente. E não importa de que tamanho sejam, há casos de invasões em organizações multinacionais e também em pequenas empresas.

Por outro lado, segurança é como uma comunidade, em que ninguém consegue resolver todas as vulnerabilidades sozinho. Assim, um planejamento para evitar ransomware pode parecer um quebra-cabeças difícil de montar para um empresário que, talvez, não saiba por onde começar. Um especialista em cibersegurança pode dar os melhores caminhos. Mas, é possível dar algumas recomendações importantes para nortear o início de uma estratégia para prevenir, ou mitigar impactos.

1. Mentalidade de segurança

A mudança mais importante, antes da implantação de qualquer estrutura de proteção, é a de mentalidade. Muitas vezes, empresas se mantém em posturas reativas, limitadas a resposta a incidentes. Isso é o mesmo que apagar um incêndio e não investigar a causa para evitar que haja fogo novamente. Em vez de resposta a incidentes, a mentalidade deve ser de **resposta contínua**. Isso significa assumir a realidade de que sistemas exigem monitoramento e correção constantes.

2. Ajustes legais

Estabelecer um processo legal e de governança cibernética que envolva o CEO, o conselho e os principais executivos de operações deve preceder uma resposta técnica a um ataque de ransomware. Há muitos fatores jurídicos, financeiros, operacionais e de reputação a considerar que impactarão os planos da empresa de como lidar com ameaças.

3. Conscientização

Uma campanha interna de conscientização cibernética que envolva toda a organização é o que vai garantir o sucesso do planejamento de segurança. A ideia é orientar as pessoas a respeito de uma postura que deve ser mantida durante a utilização de recursos corporativos, evitando que, por comportamentos inadequados, elas acabem facilitando a ação de hackers.

4. Backup

Determine a criação de uma política de backup contínuo dos arquivos da área de trabalho e do servidor. Além disso, certifique-se, por meio de testes periódicos, de que eles podem ser recuperados.

Lembrando que os backups não são apenas para dados. Todos os aplicativos fora do padrão, como aqueles que não podem ser baixados novamente, e fora de toda a infraestrutura de TI, como o Active Directory, devem ser incluídos. A perda de aplicativos proprietários criados ao longo do tempo e dos principais sistemas de TI registrados, como o AD, são importantes para a restauração de serviços.

5. Contexto

Use formas de reconhecimento de contexto com plataformas de proteção de segurança de endpoints e aplicativos de fornecedores que integram recursos de previsão, prevenção, detecção e resposta.

6. As ferramentas certas

Trabalhe com a equipe de segurança interna, ou terceirizada, usando tecnologias e serviços especializados para detecção de ameaças avançadas e para resposta a incidentes de segurança cibernética. Arquitete o monitoramento abrangente e contínuo em todas as camadas da tecnologia: pacotes de rede, fluxos, atividades do Sistema Operacional, conteúdo, comportamentos do usuário e transações de aplicativos. Além disso, desenvolva um centro de operações de segurança que ofereça suporte ao monitoramento e seja responsável pelo processo contínuo de proteção contra ameaças.

Fui atacado, e agora?

AS CONSEQUÊNCIAS DE UM ATAQUE DE RANSOMWARE SÃO CATASTRÓFICAS E DIFÍCEIS DE SE REVERTER DEPOIS QUE UM SISTEMA FOI INFECTADO. NUNCA É DEMAIS REFORÇAR QUE PREVENIR UM ATAQUE AINDA É A ESTRATÉGIA MAIS EFICAZ. PORÉM, SE UMA EMPRESA TEVE OS DADOS SEQUESTRADOS, HÁ ALGUNS PASSOS QUE, SE FOREM SEGUIDOS, PODEM MINIMIZAR O DANO.

SE UMA INFECÇÃO FOR DESCOBERTA, PRIMEIRO, DESCONECTE E ISOLE OS SISTEMAS IMEDIATAMENTE. EM SEGUIDA, INICIE O PLANO DE RESPOSTA A INCIDENTES.

Caso possua seguro cibernético ou um especialista em resposta a ransomware, envolva essas pessoas em paralelo com as ações abaixo:

- **Determine o escopo da infecção.** Desinfete os sistemas, se possível. Esse processo deve ter como objetivo reverter o sistema para seu último estado conhecido ou instalar uma nova imagem;
- **Determine a variante do Ransomware.** É CryptoWall? WannaCry? Para isso, é fácil. Basta carregar as informações no ID Ransomware;
- **Antes de assumir que o pagamento é a única opção, envie seus arquivos criptografados ao Projeto No More Ransom.** Pesquise outras ferramentas gratuitas de descriptografia de ransomware e chaves adicionais de descriptografia disponíveis. Se houver chaves de descriptografia adequadas, restaure os sistemas e realize uma avaliação de risco completa. Em seguida, documente o procedimento de recuperação para evitar ataques futuros;
- **Depois, execute as seguintes etapas de recuperação:**
  a. Localize seus backups;
  b. Verifique se todos os arquivos e mídias estão disponíveis e não foram corrompidos ou criptografados. Também se certifique de que os backups estão íntegros;
  c. Veja se há snapshot de backup ou shadow copy (cópia oculta automática feita pelo próprio Sistema Operacional) de dados, se possível. Eles também podem ser afetados por ransomwares mais recentes;
  d. Olhe as versões anteriores dos arquivos que podem estar no armazenamento em nuvem, como DropBox, Google Drive e OneDrive.
- **Após remover o ransomware e restaurar os arquivos,** determine o vetor de infecção original e elimine as falhas de segurança relacionadas. Investigue todos os sistemas em contato com o recurso impactado, incluindo servidores de arquivos, servidores de aplicativos, sistemas de grupos de trabalho e backups do sistema.

Estamos em guerra

OS HACKERS NÃO TIRAM FÉRIAS, NEM DESISTEM DE APRIMORAR AS AMEAÇAS SOMENTE PORQUE ENCONTRARAM PORTAS FECHADAS AO TENTAR UMA INVASÃO. AS AMEAÇAS EVOLUEM NA MESMA VELOCIDADE QUE A INTERNET E AS FERRAMENTAS DE SEGURANÇA.

Apesar disso, algumas empresas, ao fazerem as contas sobre quanto custa implantar um bom serviço de proteção cibernética, acham tudo caro demais e adiam o planejamento. Mas, somente acreditam que a segurança pode ficar para depois, as companhias que insistem em se debruçar no cálculo mais fácil, naquele que envolve orçamentos de antivírus e ferramentas para a TI. Nesse cenário, o mais importante ficou de fora:

Precisamos, antes de tudo, colocar no papel quanto custa não proteger.

Faça exercícios de preparação para o gerenciamento de crises e mantenha estratégias e procedimentos atualizados pelo menos a cada seis meses. Crie testes regulares de cenários de resposta a incidentes, certificando-se de que a resposta a ataques não dependa de sistemas de TI, que podem ficar indisponíveis em um incidente. Em outras palavras, não descanse na vigília dos dados do seu negócio.

Por conhecer profundamente o mundo dos ciberataques é que a ISH Tecnologia, desde 1996, investe em pesquisa e em criação para desenvolver soluções voltadas às empresas, para que elas possam estar prontas para combater esse inimigo invisível e proteger o que os negócios têm de mais valioso.

Converse com um especialista do nosso time. É só acessar **www.ish.com.br** ou enviar um email para **contato@ish.com.br** .

ISH

www.ish.com.br