MATERIAL GRATUITO - PROTEÇÃO DE DADOS

Checklist anti-ransomware em 10 itens

Dez perguntas que você mesmo consegue verificar em uma tarde, para saber se a sua empresa estaria preparada para se recuperar de um ataque hoje.

DLL Tecnologia - Inteligência em TI

TI para empresas e escritórios de contabilidade que não podem parar.

(31) 3040-4321 | dlltecnologia.com.br

Este checklist não usa jargão técnico. Cada item é uma pergunta que você faz para quem cuida da sua TI - e que tem uma resposta verificável. Ao lado dela estão a resposta aceitável e o sinal de alerta.

Se a resposta vier em forma de promessa (“está tudo certo”, “o sistema faz sozinho”) e não em forma de registro, marque como alerta. O que não pode ser mostrado não existe no dia do incidente.

Regra do exercício: só vale o item que alguém consegue PROVAR na sua frente.

Os 10 itens

1. Onde estão as cópias do meu backup - e alguma delas está fora do prédio?

Aceitável: pelo menos duas cópias em mídias diferentes e uma delas fora da empresa (nuvem ou local físico distinto). É o princípio 3-2-1: três cópias, dois tipos de mídia, uma fora.

Alerta: a única cópia está no mesmo servidor, no mesmo HD externo do armário da sala ou no mesmo prédio. Incêndio, furto e ransomware levam as duas no mesmo movimento.

2. Existe cópia imutável?

Aceitável: existe uma cópia que não pode ser alterada nem apagada durante um período definido - nem por quem tem a senha de administrador.

Alerta: todo o backup pode ser apagado por quem tem acesso administrativo. O ransomware moderno procura o backup antes de criptografar os arquivos, exatamente para reduzir a sua margem de escolha.

3. Qual foi a data do último teste de restauração? Pode me mostrar o registro?

Aceitável: uma data recente, com registro escrito de qual arquivo foi restaurado, quanto tempo levou e se abriu corretamente.

Alerta: “o backup roda todo dia”. Backup que roda não é backup que volta. Rodar é o meio; restaurar é o fim. Sem teste, você tem um arquivo, não uma garantia.

4. Quem ainda tem acesso de administrador ao meu ambiente?

Aceitável: uma lista nominal, curta, revisada, sem ex-funcionário, sem ex-técnico e sem usuário genérico compartilhado.

Alerta: ninguém sabe responder de cabeça, existe um usuário “admin” que várias pessoas usam, ou o técnico que saiu há dois anos nunca teve o acesso removido.

5. O meu Microsoft 365 tem backup próprio?

Aceitável: existe uma ferramenta de backup do e-mail, do OneDrive/SharePoint e do Teams, com retenção definida e independente da Microsoft.

Alerta: “está na nuvem, então está salvo”. A nuvem garante disponibilidade do serviço, não o retorno do arquivo que um usuário apagou há quatro meses nem a caixa de quem saiu da empresa.

6. O MFA (segundo fator) está ativo para todo mundo - inclusive para a diretoria?

Aceitável: segundo fator obrigatório para todos os acessos de e-mail, VPN, acesso remoto e sistemas críticos, sem exceção por cargo.

Alerta: está ativo “para quase todos”. A conta sem MFA costuma ser justamente a que tem mais acesso - e é por ela que o golpe de e-mail entra.

7. Quanto tempo a minha operação aguenta parada? E quanto de trabalho eu posso perder?

Aceitável: os dois números existem, estão escritos e foram acordados com você - quanto tempo até voltar e até quantas horas de trabalho podem se perder.

Alerta: ninguém nunca fez essa conta. Sem ela, o desenho do backup foi feito no chute e você só vai descobrir o tamanho do prejuízo no dia.

8. As estações e os servidores recebem atualização de segurança? Qual foi a última?

Aceitável: existe uma rotina de atualização com registro de quando foi aplicada e em quais máquinas, e uma lista do que já saiu de suporte do fabricante.

Alerta: “atualiza sozinho”. Máquina fora de suporte não recebe correção nenhuma - e ela costuma ser a que roda o sistema mais importante.

9. Quem consegue acessar a minha rede de fora, e como?

Aceitável: acesso remoto por canal controlado, com usuário nominal, segundo fator e registro de quem entrou e quando.

Alerta: a porta do acesso remoto está publicada direto na internet, com senha e mais nada. É o caminho de entrada mais explorado que existe.

10. Existe um plano escrito para a primeira hora do incidente?

Aceitável: uma página que diz quem desliga o quê, quem avisa quem, de onde a restauração começa e qual é o telefone de quem resolve - guardada também fora dos sistemas da empresa.

Alerta: o plano é ligar para o técnico e esperar. Se o ataque derrubou o servidor de arquivos, o plano provavelmente estava dentro dele.

Como ler o seu resultado

Conte quantos itens você conseguiu marcar como aceitáveis - com prova, não com promessa.

8 a 10 aceitáveis: o seu ambiente tem processo. Vale manter o teste de restauração com data e o inventário em dia.

5 a 7 aceitáveis: as peças existem, o processo não. Costuma faltar exatamente o registro - teste de restauração, lista de acessos, data de atualização.

4 ou menos: o ambiente depende de sorte e da memória de uma pessoa só. Priorize os itens 1, 2, 3 e 6, nessa ordem.

O item mais importante da lista é o 3.

Todos os outros nove podem estar perfeitos e não valer nada se o backup nunca foi restaurado. O único backup que existe de verdade é o que já voltou pelo menos uma vez, com data registrada. Se você só puder cobrar uma coisa depois de ler este material, cobre o registro do último teste de restauração.

Quer conferir esses 10 itens no seu ambiente?

A DLL Tecnologia faz o Raio-X de TI: compara o cenário atual da sua infraestrutura com o que os seus sistemas críticos (como o ERP) exigem, mapeia rede e equipamentos e lista o que está fora de suporte. Testes de restauração podem ser incluídos quando previstos no escopo e autorizados. Você fica com o relatório priorizado, independentemente de contratar qualquer coisa.

1. Você fala com a gente pelo WhatsApp ou pelo telefone.
2. Agendamos uma visita ou uma sessão remota para levantar o ambiente e combinar o escopo.
3. Testes de restauração podem ser incluídos quando previstos no escopo e autorizados.
4. Você recebe o relatório priorizado. Sem custo, sem contrato e sem insistência depois.

Fale com a DLL Tecnologia

Telefone e WhatsApp: (31) 3040-4321

Site: dlltecnologia.com.br