

RANSOMWARE: COMO UMA EMPRESA PODE PERDER OS SEUS DADOS

Relatório técnico | Prevenção, cópias de segurança, resposta e recuperação

O ransomware evoluiu de uma simples cifra de ficheiros para operações de extorsão que podem envolver roubo de informação, interrupção de serviços e pressão sobre fornecedores e clientes.

1. Como começa uma intrusão

Os vetores comuns incluem credenciais roubadas, serviços de acesso remoto mal protegidos, vulnerabilidades não corrigidas, phishing e exploração de fornecedores. O atacante pode permanecer na rede, elevar privilégios, identificar sistemas de backup e obter acesso aos servidores antes de executar a fase destrutiva.

2. Da intrusão à paralisação

A cadeia de ataque pode passar por reconhecimento, movimento lateral, persistência, exfiltração, desativação de controlos, eliminação de cópias acessíveis e encriptação de sistemas. Nem todos os incidentes têm as mesmas etapas nem envolvem cifragem: alguns focam-se na extração e ameaça de publicação dos dados.

3. Porque um backup não é automaticamente recuperável

Uma cópia no mesmo domínio, acessível com as mesmas credenciais administrativas e permanentemente ligada à rede, pode ser eliminada ou cifrada pelo atacante. Backups sem verificação podem estar incompletos ou conter dados já comprometidos. Snapshots e replicação imediata não substituem histórico independente, porque podem propagar alterações destrutivas.

4. A abordagem 3-2-1 e cópias protegidas

Uma estratégia útil é manter múltiplas cópias em suportes e localizações distintos, incluindo pelo menos uma cópia isolada, offline ou imutável, sempre de acordo com análise de risco e capacidade de recuperação. A retenção deve permitir regressar a um ponto anterior à intrusão e ser compatível com requisitos de privacidade e conservação.

5. O papel de RPO e RTO

RPO é a perda máxima de dados aceitável em função do intervalo entre pontos de recuperação; RTO é o tempo-alvo até restabelecer um serviço. Uma empresa pode ter um backup válido e ainda assim falhar o RTO por falta de hardware, ligações, credenciais, documentação ou dependências. Ambos devem ser acordados por serviço crítico.

6. Prevenção prioritária

Inventarie ativos, aplique MFA, reduza privilégios administrativos, proteja acessos remotos, segmente redes, corrija vulnerabilidades, monitorize eventos e separe credenciais de backup das de produção. A segurança inclui também processos de contratação, treino dos utilizadores e revisão da cadeia de fornecimento.

7. Resposta inicial

Em caso de suspeita, acione o procedimento de incidentes. Isole equipamentos afetados de forma coordenada, preserve evidências e evite desligar indiscriminadamente sistemas sem orientação técnica, pois pode perder dados voláteis necessários à análise. Avalie impacto, alcance e deveres legais de comunicação antes de recuperar.

8. Recuperar com segurança

Não repor sistemas diretamente numa rede ainda comprometida. Confirme a origem de confiança dos backups, elimine causas de intrusão, altere credenciais relevantes, valide integridade e priorize serviços essenciais. Teste autenticação, dependências, aplicações e acesso aos dados após a reposição.

9. Testes e evidências

Realize restauros regulares de ficheiros, máquinas virtuais e aplicações críticas. Registe duração, falhas, responsáveis e medidas corretivas. Os testes devem incluir cenários de perda do repositório principal, indisponibilidade do hipervisor e recuperação sem acesso às credenciais habituais.

10. Conclusão

A verdadeira capacidade de recuperação resulta de cópias independentes, procedimentos testados e decisões de negócio claras. O investimento deve ser orientado pela criticidade dos sistemas e não apenas pelo volume de dados armazenado.