Os hackers não querem salvá-lo: eles querem apagá-lo.

Data: 2025-09-21 09:45:48

Autor: Inteligência Against Invaders

Redazione RHC**:21 Setembro 2025 11:37**

Os hackers estão cada vez mais visando backups – não sistemas ou servidores, mas os dados que as empresas retêm por um período limitado de tempo para que possam se recuperar de ataques.

Um novo estudo da Apricorn revela estatísticas alarmantes: uma em cinco violações de dados no Reino Unido é **diretamente vinculado a backups comprometidos** .

Isso indica que *Os invasores aprenderam a penetrar mais fundo e com mais precisão,* precisamente **onde as empresas esperam encontrar segurança no caso de um ataque cibernético.**

No passado, os dados de backup eram considerados um **tipo de seguro** , uma cópia fiável e segura das informações críticas que podem ser restauradas em caso de catástrofe. No entanto, a dinâmica está mudando. *Enquanto as empresas anteriormente se concentravam na proteção da infraestrutura de TI ativa (estações de trabalho, nuvens, roteadores), o armazenamento passivo agora também está sob ataque* . E isso não é apenas um efeito colateral: **Em alguns casos, os ataques visam exclusivamente os backups, comprometendo a própria possibilidade de recuperação.**

De acordo com a Apricorn, **18% das empresas citaram violações de backup como a principal causa de um incidente.** Isso não apenas causa danos diretos, mas também uma interrupção estratégica para **negócio continuidade** : a incapacidade de retornar ao trabalho sem uma reinstalação completa e negociação com chantagistas.

É particularmente digno de nota que **13% dos entrevistados admitiram que sua infraestrutura de recuperação não era robusta o suficiente para restaurar dados rapidamente.**

Quase um terço das empresas que experimentaram uma recuperação de backup eficaz não conseguiram restaurar tudo: algumas informações foram perdidas ou o processo foi ineficaz devido a **procedimentos mal elaborados** .

O exemplo da empresa dinamarquesa de nuvem CloudNordic, que foi atacada em 2023, é revelador. Os atacantes **não apenas desativou os servidores principais, mas também criptografou todos os backups.** Como resultado, **toda a base de clientes foi irremediavelmente perdida e as operações da empresa foram efetivamente paralisadas** . A CloudNordic tinha software antivírus, firewall e uma estratégia de backup em várias camadas. No entanto, os servidores vulneráveis e comprometidos anteriormente se tornaram o ponto de entrada.

Isso destaca um ponto importante: **O backup só é eficaz quando não apenas existe, mas**

também é testado regularmente, fisicamente isolado e projetado para ser "invisível" para a rede principal.

No entanto, o relatório da Apricorn também destaca algumas tendências positivas. **O número de empresas que restauram com sucesso toda a sua infraestrutura a partir de backups cresceu para 58%, acima dos 50% do ano anterior** .

Mais e mais organizações estão usando *Mecanismos de backup automatizados: 44% estão enviando dados para armazenamento central e privado, em comparação com apenas 30% no ano passado* . No geral, 85% das empresas já implementaram pelo menos um elemento de automação.

De acordo com John Fielding, diretor administrativo da EMEA da Apricorn, *O gerenciamento de incidentes deve incluir não apenas a preparação do ataque, mas também a preparação para a recuperação completa.* Fielding acredita que **Somente backups regularmente testados, completos e protegidos com segurança podem se tornar uma verdadeira ferramenta de defesa** , não apenas uma ilusão de segurança.

À medida que os ataques se tornam mais sofisticados, fica claro que simplesmente ter um backup não é suficiente. **Ele deve estar além do controle do invasor, duplicado, depurado e facilmente implantado isoladamente** . Caso contrário, as empresas correm o risco não apenas de perder dados, mas também de perder permanentemente a capacidade de recuperá-los.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli