Conforme postamos em " Os 5 principais riscos aos negócios em 2019 " o maior risco apontado na pesquisa do Fundo Econômico Mundial na América do Norte e Europa é o ataque cibernético. Após este post recebemos algumas consultas sobre "A Utilidade do Disaster Recovery num Ataque Cibernético".

Vamos tentar responder.
 Como é o seu ambiente de TI? Muito possivelmente, seguindo as tendências de mercado, o seu ambiente de TI deve ser multi-cloud, isto é, diferentes serviços em diferentes nuvens: Office 365 numa, SAP em outra, ERP em outra, ServiceNow, Salesforce etc. e também alguma parte de legado ainda no seu Data Center próprio ou terceirizado: full outsourcing, colocation etc.
 É possível que você também tenha alguma(s) conexão(ões) direta(s) com alguma(s) terceira(s) parte(s), cliente(s) ou fornecedor(es).

Agora vamos para a parte do ataque cibernético. Defina ataque cibernético.
 É um ataque DDoS – Distributed Denial of Service? É um ataque direto à sua rede ou a alguma das redes dos seus serviços na nuvem? Quem está no controle da situação?

A Utilidade do Disaster Recovery neste cenário é NENHUMA. O que você, ou o seu provedor de serviços, precisa ter são bons mecanismos de detecção e resposta a um ataque desta natureza.
 É um acesso indevido ou a divulgação não autorizada de dados que pode trazer implicações sérias para a GDPR e/ou LGPD? Quando o acesso indevido ou a divulgação não autorizada de dados ocorreu? No passado ou foi detectado enquanto estava ocorrendo?

A Utilidade do Disaster Recovery neste cenário também é NENHUMA. Se foi no passado o que deve ser feito é uma profunda análise de vulnerabilidades e aplicar todas as correções necessárias e/ou eventualmente alterações na arquitetura de defesa contra um novo acesso indevido ou divulgação não autorizada de dados.

Foi detectado enquanto estava ocorrendo? Neste caso a Utilidade do Disaster Recovery também é NENHUMA. O que deve ser feito é cortar todas as conexões entre o seu ambiente "invadido" e o "invasor". Estimar a quantidade de dados acessados indevidamente e executar as mesmas ações do passo acima.
 Foi um ransomware que criptografou alguns arquivos ou bases de dados importantes? Como é o seu mecanismo de replicação dos dados de produção para o DR? Praticamente em tempo real, isto é, enche as logs ou archives, envia e aplica no DR? Então é bastante provável que os mesmos arquivos ou bases de dados criptografadas na produção também foram criptografadas no DR.

A Utilidade do Disaster Recovery neste cenário também é NENHUMA. A recuperação dos seus dados dependerá, fundamentalmente, dos seus backups em meio removível pois, num cenário de pior caso, é possível que os seus backups em disco (caso você os faça, é claro) também tenham sido comprometidos.

 Foi um ataque em massa de vírus que comprometeu toda ou uma boa parte das suas estações?

Já estamos nos tornando repetitivos, a Utilidade do Disaster Recovery neste cenário também é NENHUMA. A sua recuperação dependerá de alguma ferramenta de remoção deste vírus, se houver, ou de reinstalar as imagens de todas as estações de trabalho infectadas. Depois, poderá ser necessário um scan full em toda rede, com os detectores de antivírus devidamente atualizados e capazes de identificar o invasor antes de liberar as estações aos usuários.

Bem, não vamos nos estender. Pode ser que em alguma situação particular o Disaster Recovery (DR) tenha alguma utilidade na ocorrência de um ataque cibernético específico mas, geralmente, a Utilidade do Disaster Recovery num Ataque Cibernético é, lamentamos dizer, NENHUMA.

Você, responsável pela Continuidade de Negócios da sua organização, deve se assegurar que a sua área de Segurança da Informação tenha todos os mecanismos necessários para identificar e responder a um ataque cibernético, não esquecendo que:
 O seu ambiente está cheio de vulnerabilidades, falhas nos sistemas operacionais, nas aplicações “in house” ou terceirizadas, correções não aplicadas, regras de firewall com vulnerabilidades etc. que os invasores determinados conhecem muito melhor do que a sua estrutura de segurança;
 Que os invasores, como qualquer criminoso, estão sempre, pelo menos, um passo à frente da lei, no nosso caso das correções necessárias;
 Quem determina se a sua organização é “target” ou não é o invasor e não, como certa vez um CSO nos disse, que a empresa é alvo ou não;
 Que a NASA, FBI, NSA, Microsoft… já foram invadidas;
 Não existe, NUNCA, segurança 100%;
 Você terá sérios problemas para tentar explicar para os seus executivos que a Utilidade do Disaster Recovery (DR) num Ataque Cibernético é NENHUMA.

Autor: Sidney Modenesi
Fonte: https://strohlbrasil.com.br/o-disaster-recovery-num-ataque-cibernetico