DELL Technologies

Lições de um ataque de ransomware

na Universitat Autònoma de Barcelona

Gonçal Badenes
CIO, Universitat Autònoma de Barcelona.
Entrevista resumida e editada para maior clareza.

Ação rápida, transparência e um compromisso renovado com a atualização da segurança cibernética definiram a resposta da Universidade a um ataque de ransomware.

Sameer Shah, da área de marketing de segurança cibernética da Dell Technologies, conversou com o CIO Gonçal Badenes sobre o incidente.

Shah: Temos falado sobre a necessidade de ajudar as organizações a melhorar incrementalmente a maturidade de segurança cibernética. Vocês sofreram um ataque cibernético há algum tempo. Antes de detalharmos melhor o ataque, conte-nos um pouco sobre a Universidade e o ambiente de TI dela.

Badenes: A Universitat Autònoma de Barcelona é uma das principais universidades da Espanha. A TI supervisiona todos os serviços necessários para o funcionamento da universidade.

Logo antes do ataque, tínhamos um plano completo para melhorar nossa postura de segurança cibernética. Tínhamos implementado a autenticação baseada em vários fatores (MFA), mas não em todos os serviços e usuários. Os alunos e toda a equipe de TI já tinham MFA, mas apenas na plataforma Microsoft 365. Outros serviços não estavam protegidos. Implementar a MFA em tudo era importante, como veremos mais adiante.

Qual o tipo de ataque e quando ele ocorreu?

Foi um ataque de ransomware que aconteceu em um fim de semana prolongado, como geralmente acontece. Por volta das quatro horas da manhã, recebi uma ligação da minha equipe informando que os serviços estavam caindo como dominó. Eles deram o alarme e imediatamente montamos a equipe de resposta que havíamos previsto para esses casos.

Como vocês sabiam que era um ataque de ransomware? Havia um aviso de resgate?

Havia avisos de resgate nos sistemas afetados. Mas eles também realizaram um pequeno ataque executando um script para criptografar computadores que estavam on-line no fim de semana. O impacto disso foi limitado, e o objetivo principal provavelmente era garantir que a equipe e os alunos soubessem do ataque, não apenas a equipe de TI.

Em algum momento sua organização considerou pagar o resgate?

Não.

Por que não?

Do ponto de vista ético, não podíamos fazer isso. Felizmente, tínhamos backups em vigor, duas cópias em dois data centers diferentes no campus e uma terceira em fita fora do perímetro da organização.

E, para ficar claro, esses backups não eram um cofre de dados, certo?

Não, naquele momento não tínhamos um cofre. Era uma prioridade futura que estava no roteiro, e foi priorizada [após o ataque].

As comunicações podem ser essenciais nessas situações. Parece que você assumiu o controle no ataque se comunicando de maneira clara e transparente, inclusive com a mídia?

Sim, desde o primeiro dia. Tínhamos de ser totalmente transparentes e o mais abertos possível, explicando o que tinha acontecido. Queríamos garantir que outras pessoas pudessem se preparar e aprender com nossa experiência. Meu palpite é que parte da imprensa realmente leu o aviso de resgate e entrou em contato com os atacantes, porque nunca o fizemos. O grupo invasor se identificou como PISA (Protect Your System, Amigo, Proteja seu sistema, amigo).

Muitas vezes, as organizações preferem o sigilo para evitar expor os pontos fracos ou táticas de correção. Isso era uma preocupação?

Essas são preocupações muito válidas. Mas tenho certeza de que todos sabemos que somos vulneráveis. Quando tentamos proteger nossa casa, sabemos que, mesmo com a melhor porta do mundo, os ladrões encontrarão uma maneira de quebrá-la ou achar outra forma de entrar, se realmente quiserem. É exatamente a mesma coisa.

Fomos atacados e tínhamos vulnerabilidades, e não há vergonha nisso. É importante compartilhar com as pessoas que fomos atingidos mesmo tendo um roteiro de proteção muito claro. Mesmo que tivéssemos uma proteção muito boa, ainda tínhamos vulnerabilidades que poderiam ser atacadas. Ao implementar etapas adicionais, é possível ficar em uma posição muito mais protegida.

Conte-nos quais foram suas ações imediatas para começar a lidar com o problema.

Desligamos a rede, todos os sistemas. Entramos em contato com a polícia e com a agência regional de proteção de dados, que são obrigações legais. Então, imediatamente montamos duas equipes: perícia e recuperação. Ligamos para a Dell, nosso problema recebeu prioridade máxima e uma equipe incrível começou a trabalhar nele sem parar. Eles conseguiram recuperar completamente todos os dados no segundo domínio de dados.

A perícia começou durante o processo de recuperação?

Para alguns dos processos de recuperação, tivemos que esperar um pouco. É por isso que digo que a perícia começou primeiro. Tudo foi colocado em quarentena porque é preciso entender o que aconteceu. Tivemos que montar um outro sistema para começar a colocar as coisas de volta. Decidimos que, mesmo que demorasse um pouco mais, todos os sistemas que fossem colocados operação teriam que ter os melhores padrões de segurança.

"Acredito que o mais importante a considerar é que é muito provável que, mais cedo ou mais tarde, todos vamos sofrer um ataque cibernético. Portanto, precisamos ter em vigor um plano detalhado de redução e recuperação."

Você mencionou que a MFA estava apenas no Microsoft 365, o que em parte permitiu o ataque. Agora a MFA está implementada em tudo?

O vetor de ataque foi um usuário com credenciais comprometidas que estava em uma equipe que já tinha MFA na Microsoft. Mas, quando os invasores tentaram acessar o e-mail e perceberam que não seria possível por causa da MFA, continuaram procurando. E descobriram que temos uma VPN, que não estava protegida pela MFA. Assim que conseguiram acesso pela VPN, eles começaram a pesquisar a rede.

Em uma rede muito grande como a nossa, encontraram um sistema vulnerável e iniciaram movimentos laterais. Então, quando começamos a recuperar os sistemas, decidimos que nada ficaria on-line até que fosse protegido com a MFA.

Se tivesse que oferecer aos seus colegas apenas UMA recomendação importante ou conselho para evitar um ataque de ransomware, qual seria?

É muito difícil dar um único conselho, mas acredito que o mais importante a considerar é que é muito provável que, mais cedo ou mais tarde, todos vamos sofrer um ataque cibernético. Portanto, precisamos ter em vigor um plano detalhado de redução e recuperação.

Por exemplo, é muito importante ter em mãos os contatos dos principais parceiros de perícia e recuperação, ter um mapa detalhado e priorizado de serviços com um cronograma de recuperação e uma estratégia bem alinhada com as principais unidades de negócios, incluindo comunicação (interna e externa). E, claro, é muito importante manter os usuários alertas e treinados sobre as técnicas usadas pelos invasores.

Você sente que o fortalecimento dos recursos de segurança cibernética na universidade aumentou a confiança para continuar a missão e fazer todas as coisas importantes que você está fazendo?

Com certeza. Antes do ataque, uma das percepções era que todas as novas medidas para proteger o sistema eram muito questionadas e as pessoas se perguntavam se realmente precisávamos delas. O fato é que a proteção é absolutamente necessária para não colocar todo o empreendimento em perigo. E é claro que algumas pessoas ainda acreditam que essas medidas estão atrapalhando o trabalho. Mas a maioria acha que os sistemas estão muito mais protegidos.

Obrigado. Sua franqueza e transparência são benéficas para todos que trabalham para melhorar a maturidade da segurança cibernética.