INCA dá resposta rápida a invasão cibernética

O ataque na rede de computadores sofrido pelo INCA provocou a suspensão temporária das sessões de radioterapia (interrompidas por três dias) e exigiu que prontuários e pedidos de exames fossem escritos à mão. As compras e aquisições também foram afetadas. Esse cenário se manteve por quatro dias, quando, gradativamente, a situação foi se normalizando. O diretor-geral, Roberto Gil, afirmou que o gabinete de crise criado exclusivamente para encontrar soluções rápidas para esse problema deu prioridade para que as atividades retornassem o quanto antes na Assistência e no abastecimento das unidades hospitalares.

"A instituição sempre se preocupou com sua segurança cibernética, porém os grupos criminosos estão se aperfeiçoando cada vez mais nesse tipo de invasão. O ataque aconteceu durante a madrugada do dia 27 de janeiro, mas rapidamente foi percebido. Prontamente, a maioria das estações de trabalho que funcionavam no período noturno, um número naturalmente reduzido, foi desligada", conta o diretor.

A recomendação de não manter as estações operando após o final do expediente ajudou a diminuir o impacto. "Não perdemos nenhum dos servidores [máquinas que armazenam informações disponíveis na rede] e conseguimos preservar boa parte dos dados, mas o transtorno foi enorme. Imagina o que é, em pleno século 21, ter que desligar todo seu sistema interligado e sua rede de assistência?", pondera Roberto Gil.

O responsável pela Área de Governança e Inovação em Tecnologia da Informação e Comunicação, Carlos Henrique Martins, explica que um software malicioso, que criptografa alguns ou todos os arquivos de um computador e pede um resgate para sua liberação, afetou aproximadamente 40% das estações de trabalho. "O Serviço de Tecnologia da Informação [SETI] adotou medidas imediatas, isolando a rede de computadores e interrompendo as comunicações internas e externas. Todas as estações foram desligadas e retiradas da rede."

Os Centros Cirúrgicos não pararam de funcionar, e os mapas de cirurgia não foram alterados. Apenas dois procedimentos que dependiam de alta tecnologia foram adiados para o dia seguinte. A Patologia, em menos de uma semana, conseguiu ter acesso aos laudos. "Ficamos preocupados com a perda de dados, mas felizmente tínhamos backup. Também verificamos que nenhuma informação foi vazada", relata Roberto Gil.

Chantagem financeira

O Ministério da Saúde e a Polícia Federal foram imediatamente notificados sobre o ocorrido. Os autores da investida exigiram dinheiro do INCA. "Não houve negociação. Não cedemos em absolutamente nada."

Roberto Gil agradece os esforços da força de trabalho, especialmente do SETI, que se empenhou incansavelmente para dar respostas ao episódio. "Todos do INCA se solidarizaram, entendendo que aquele não era um problema da Direção ou de chefias, mas da instituição inteira."

Lições aprendidas

O SETI aumentou os cuidados com as portas de entrada de possíveis acessos não autorizados, como impressoras, por exemplo, e terá como foco a atualização constante de antivírus e a reconfiguração e atualização de sistemas e *firewalls*. Após a contenção inicial, o serviço fez uma revisão em toda a segurança da informação, com apoio de especialistas e de algumas ferramentas. "A equipe de TI começou a recuperação do ambiente colocando todos os servidores em funcionamento no dia seguinte ao ataque e, posteriormente, iniciou a restauração gradativa das estações de trabalho. Do parque de 3 mil máquinas, em média, cerca de 1.160 tiveram que ser reformatadas por profissionais que trabalharam 24 horas ininterruptas, durante aproximadamente duas semanas, inclusive aos sábados e domingos", revela Carlos Henrique.

"Não podemos economizar em custos na segurança cibernética. Precisamos buscar inovações e contatos com outras instituições. A solução de uma pode ser a de outra. Isso reforça a importância da construção de redes para troca de experiências", enfatiza Roberto Gil, que garante que o Instituto sai fortalecido do atentado.

De acordo com ele, os pacientes foram tranquilizados, ao serem avisados de que nenhum tratamento seria afetado. "Ao mesmo tempo que ficamos tristes com o ser humano, por existirem pessoas que dedicam sua capacidade ao mal, para prejudicar quem já está em situação de vulnerabilidade [tratando câncer], a gente recupera um certo otimismo quando constata a solidariedade que o Instituto recebeu, tanto de sua força de trabalho quanto da população, e a pronta colaboração do Ministério da Saúde e dos outros institutos federais."

Carlos Henrique destaca que é essencial refletir sobre as lições aprendidas e fortalecer as práticas de segurança da informação. "Temos que conscientizar nossos colaboradores sobre a responsabilidade de cada um em proteger informações sensíveis. Ações simples podem ser adotadas, como colocar uma senha forte, revisar e restringir acesso a dados confidenciais e ter cuidado ao clicar em links recebidos em e-mails ou mesmo por celular. O SETI pretende, em conjunto com o Serviço de Comunicação Social, fazer campanhas sobre ameaças cibernéticas para fortalecer a cultura em segurança da informação."