Ataque cibernético alerta para cuidados no uso dos sistemas

Ação criminosa afetou trabalho na Justiça Federal da 3ª Região

O crescente número de ações criminosas de hackers no Brasil, ao longo dos últimos anos, tem afetado a prestação de serviços de órgãos públicos e provocado prejuízos significativos a empresas privadas e a pessoas físicas. A prevenção aos ataques se tornou especialmente mais desafiadora com a expansão do home office, em razão da pandemia.

No TRF3, desde 2020, com o aumento do teletrabalho e dos riscos de ataques, houve aumento nos investimentos na área. Planos de Contratação de Tecnologia da Informação (TI) tiveram um incremento, com verbas destinadas à internet, compra de equipamentos de servidores de rede mais seguros e potentes, além de atualizações de softwares.

Essas ações foram fundamentais para que a Secretaria de Tecnologia da Informação (SETI) agisse rapidamente para conter ataques hackers aos sistemas de informação da Justiça Federal da 3ª Região (JF3R), em 2021, e para resolução e restabelecimento dos sistemas digitais devido à invasão cibernética ocorrida em 30 de março.

No ano passado, os ataques foram do tipo Dynamic Deny of Service (DDoS), também conhecido como negação distribuída de serviço. Trata-se de uma sobrecarga produzida por meio do excesso de demanda, que tem como resultado a indisponibilidade de websites. O caso deste ano foi do tipo ransomware, considerado mais grave.

“Esse tipo de ataque é mais danoso do que outros tipos e provoca uma interrupção maior dos serviços de TI. Muitas vezes, são necessários meses para sua total restauração. A SETI teve que refazer praticamente toda a infraestrutura de TI em tempo recorde, 15 dias corridos”, explica o diretor da SETI, Daniel Guimarães.

O ransomware é um tipo de código malicioso (malware) que criptografa arquivos no armazenamento local e de rede, além de máquinas virtuais e banco de dados. Em geral, criminosos exigem um resgate (ransom) para descriptografar os documentos e restabelecer o acesso

ao usuário. Os hackers desenvolvem esse malware para ganhar dinheiro com extorsão digital. O código pode ser instalado por meio de links enganosos em e-mails, mensagens instantâneas ou sites.

O ataque ocorreu na madrugada do dia 30 de março e foi interrompido com o desligamento total de equipamentos de datacenter. O tribunal acionou a Polícia Federal, que no mesmo dia coletou informações para o Inquérito Policial. A investigação corre em segredo de Justiça.

Daniel Guimarães, diretor da SETI, explica que a área de tecnologia seguiu o Plano de Continuidade de Serviços de TI, reconstruindo e restaurando toda infraestrutura e sistemas da JF3R. Os protocolos de segurança visaram garantir o retorno da prestação jurisdicional o mais rapidamente possível.

“No período de 15 dias, os principais serviços, como PJe, SEI e Precatórios, foram restabelecidos. Em seguida, iniciamos a higienização de 8.200 computadores e notebooks. Os bancos de dados e sistema judiciais e administrativos de produção não foram prejudicados e retornaram de forma íntegra, sem perda de informação. Apenas os ambientes de homologação, desenvolvimento e arquivos pessoais dos computadores e notebooks foram perdidos”, conclui.

Os prazos dos processos eletrônicos voltaram a fluir no dia 18 de abril. Para que o retorno das atividades ocorresse de maneira segura, os prazos de processos físicos e o atendimento presencial ao público permaneceram suspensos durante todo o mês de abril, no TRF3 e nas Seções Judiciárias de São Paulo (SJSP) e Mato Grosso do Sul (SJMS). O teletrabalho extraordinário de servidores e magistrados foi prorrogado. Durante as duas primeiras semanas do mês, a JF3R funcionou exclusivamente em regime de plantão judiciário.

Outros ataques

Outros órgãos públicos também sofreram “invasões” do mesmo tipo. O Poder Judiciário tem sido alvo frequente dos criminosos.

Em 6 de março, a Justiça Federal de Pernambuco foi vítima de um ataque que deixou o site e os sistemas fora do ar. Em fevereiro, hackers invadiram sistemas do Tribunal Regional do Trabalho do Espírito Santo. Em 2020, o Superior Tribunal de Justiça informou que um vírus invadira suas redes de telefonia e internet. O Tribunal Regional Federal da 1ª Região, o Tribunal Superior Eleitoral e o Supremo Tribunal Federal também já foram vítimas de ações criminosas.

Segundo o diretor da SETI, questões relativas à segurança da informação são debatidas diariamente pela Secretaria e pela Equipe de Tratamento de Resposta a Incidentes de Segurança Cibernética (ETIR). São, também, realizadas reuniões mensais da Comissão Local de Respostas

“O elo mais fraco da Segurança da Informação são as pessoas. De nada adianta implementar as melhores ferramentas de proteção no seu ambiente se não houver um treinamento básico para as pessoas que o utilizam diariamente. Cursos, treinamentos e orientações são fundamentais”

Daniel Guimarães, diretor da SETI

a Incidentes de Segurança (CLRI) e da Comissão Local de Segurança da Informação (CLSI).

“Após este ataque ransomware, foi contratado o serviço de Security Operations Center, Centro de Operações de Segurança (SOC). Trata-se de uma forma de denominar a plataforma que registra qualquer problema de segurança digital. Com muita agilidade, o sistema também recolhe, armazena e analisa relatórios para corrigir qualquer vulnerabilidade ou ameaça cibernética”, salientou Daniel Guimarães.

Cuidados

Vazamentos e invasões nos computadores podem ser mais frequentes com as pessoas trabalhando virtualmente. O problema ocorrido dentro de casa pode ser levado para o local de trabalho, mesmo em uma conexão VPN (rede virtual privada) e com utilização de usuário e senha pessoais.

Na 3ª Região, a conexão VPN foi descontinuada por questões de segurança. O acesso aos sistemas e serviços de TI remotamente fica condicionado à extranet, pelo portal Trabalho Remoto (https://trf3virtual.trf3.jus.br/), que possui as principais ferramentas de trabalho, sem afetar a segurança da informação.

Como se proteger

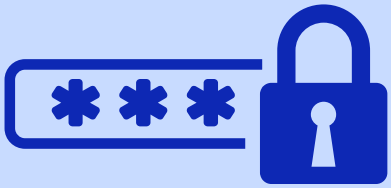
Uma dica importante é instalar um antivírus. Segundo Eduardo Carvalho Pereira, analista da Equipe de Tratamento de Resposta a Incidentes de Segurança Cibernética (ETIR) do TRF3, a utilização do programa, seja pago ou gratuito, continua sendo uma das dicas mais eficazes para a proteção de dispositivos, ainda mais em tempos de teletrabalho. “Ele elimina o trabalho duro, oferecendo segurança automática de trabalho remoto contra uma série de ameaças, como ataques de dia zero, malwares, phishing, etc”.

Marlon Borba, servidor aposentado especialista em TI ouvido pela 3R, diz que é preciso educar e conscientizar colaboradores. Para ele, a saída é “a educação dos usuários por meio de campanhas promovidas pela área de segurança da informação”. Com funcionários treinados, é mais fácil para a empresa estabelecer planos de contingência caso algo inesperado aconteça.

Na dúvida, não hesite em procurar as áreas técnicas. “Diante de qualquer suspeita de ação maliciosa, seja nos sistemas ou equipamentos, servidores e magistrados devem fazer contato diretamente com a SETI e ETIR pelos meios de comunicação existentes (callcenter, telefone, Teams), para posterior análise e verificação. Por e-mail, a mensagem deve ser enviada para SECURITY@trf3.jus.br”, esclarece o diretor da SETI, Daniel Guimarães.

Mais dicas de como se proteger no ciberespaço

Utilize senhas longas, fortes e exclusivas para cada dispositivo e aplicativo, com pelo menos 12 caracteres (símbolos, números, letras maiúsculas e minúsculas). Recomenda-se o uso de um gerenciador de senhas.



Ative a autenticação de dois fatores, fornecendo duas informações ao fazer login em um site.

Cuidado ao acessar redes sem fio em locais públicos, somente o faça quando estritamente necessário.

Mantenha o trabalho separado de suas atividades pessoais. Por exemplo: pendrives e HDs externos pessoais devem ser diferentes daqueles de uso profissional.

Abuse dos backups. Use a estratégia de backup 3-2-1: três cópias dos dados em pelo menos duas soluções de armazenamento, uma das quais de modo remoto.

Use apenas software licenciado e instale as atualizações assim que estiverem disponíveis.

Desconfie de e-mails por mais confiável que pareça o remetente. Não abra arquivos anexos principalmente se você não estiver esperando pela mensagem.

Bloqueie a tela quando estiver longe da mesa. Não deixe documentos ou notebooks sem vigilância.

Evite compartilhar informações pessoais ou corporativas. Não faça cadastro em sites desconhecidos;

Criptografe o dispositivo móvel e o disco rígido. Essa medida protege os arquivos locais, caso ocorra perda, roubo ou o aparelho seja submetido a acesso não autorizado. Implemente a criptografia na nuvem.

Durante o expediente, não acesse sítios eletrônicos que não fazem parte do cotidiano de trabalho.

A SETI mantém a página
Dicas da Segurança da Informação,
com cartilhas e recomendações sobre o tema.