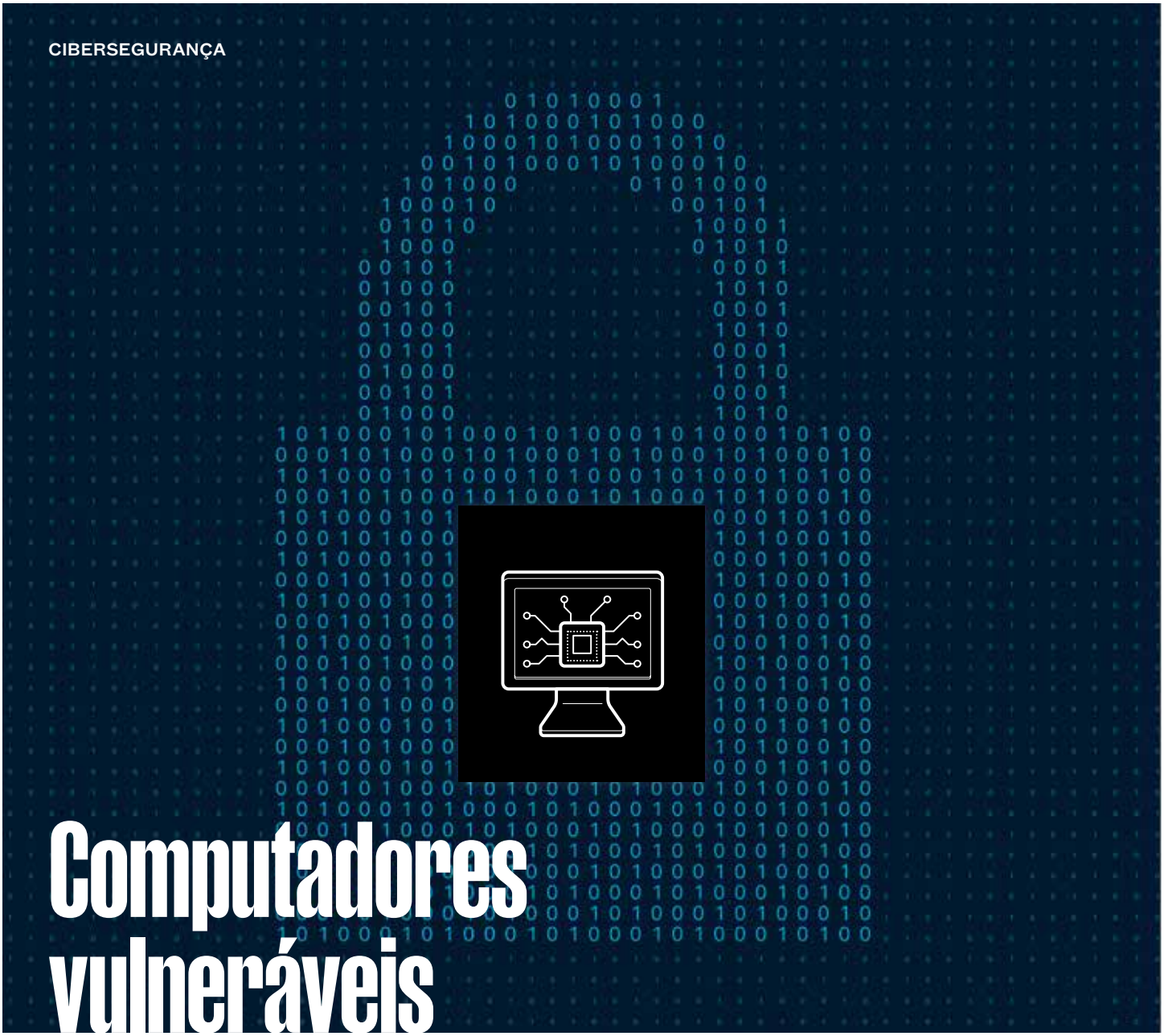


Computadores vulneráveis

Ataques cibernéticos a instituições de ensino e pesquisa crescem nos últimos anos e trazem alerta para reforço em segurança da informação

SARAH SCHMIDT

O primeiro alerta veio na noite de uma sexta-feira, 28 de março, por meio de um software de segurança cibernética: havia um ataque hacker em curso na rede de computadores e servidores do Instituto de Pesquisas Energéticas e Nucleares (Ipen), em São Paulo. Acionada, a equipe de tecnologia da informação percebeu que, para conter o avanço, que se espalhava para outras máquinas do instituto, toda a comunicação com o Ipen deveria ser cortada: o acesso à internet, ao telefone e à própria rede interna, interrompendo o fluxo de dados de seus computadores. Em consequência, o instituto paralisou todas as suas atividades, tanto as de pesquisa quanto a de produção de radiofármacos, essenciais ao tratamento de pessoas com câncer, por 10 dias. O rescaldo

FOTO CALVINDEXTER/GETTY IMAGES

dos danos ainda continua. "Vamos levar cerca três meses para avaliar tudo o que pode ter sido afetado e retornar às atividades de forma plena", comenta Pedro Maffia, diretor de gestão institucional da Comissão Nacional de Energia Nuclear (CNEN), da qual o Ipen faz parte.

Ainda não foi possível estimar todo o prejuízo causado pelo incidente, mas R$ 2,5 milhões deixaram de ser arrecadados com a venda dos insumos. O ataque desferido foi do tipo *ransomware*, que por meio de software malicioso controla e bloqueia arquivos computacionais da instituição, usando criptografia, e exige dinheiro para restabelecer o acesso. "Deixaram uma mensagem pedindo um resgate para ser pago em bitcoin. Em nenhum momento pensamos em negociar com os criminosos", conta. Os pesquisadores cujas atividades podiam ser realizadas remotamente seguiram trabalhando, mas de forma parcial e com produtividade reduzida. "Todas as atividades que dependiam de sistemas conectados à rede do Ipen foram afetadas", observa o físico Niklaus Wetter, coordenador de Pesquisa e Desenvolvimento do instituto.

Tentativas de ataques como a enfrentada pelo Ipen são comuns em instituições de ensino e de pesquisa do país. A rede acadêmica Ipê, que conecta aproximadamente 1,8 mil instituições de pesquisa, inovação e ensino superior brasileiras e 4 milhões de usuários, lida com cerca de 20 mil tentativas de ataques por mês. A maioria é bloqueada de forma automática pela Rede Nacional de Ensino e Pesquisa (RNP), organização social vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI), que administra a rede. Alguns desses ataques, por serem mais elaborados, exigem intervenção direta dos profissionais da equipe de cibersegurança.

"As instituições de ensino e pesquisa vêm ampliando a oferta de serviços digitais e isso naturalmente abre mais portas para ataques", explica João Eduardo Ferreira, pesquisador do Instituto de Matemática e Estatística da Universidade de São Paulo (IME-USP) e superintendente de Tecnologia de Informação da universidade. Segundo ele, a USP sofre e monitora continuamente tentativas de ataques cibernéticos, cujo perfil mudou nos últimos dois anos. "O que observamos é que os hackers não precisam mais dispor de equipamentos para atacar, pois muitos alugam máquinas de boa capacidade computacional na *deep web*. Outra mudança é que, na maioria das vezes, não se trata de um indivíduo, mas de grupos que se articulam em locais diferentes. E, por fim, eles exibem um conhecimento técnico cada vez mais sofisticado." Para lidar com os ataques, a USP investe em várias estratégias, desde a construção e aperfeiçoamento de barreiras de conectividade (firewall) até a criptografia de dados sensíveis e a adoção de uma arquitetura de software em quatro camadas, que permite o desenvolvimento de novas funcionalidades e a correção de problemas sem afetar outras partes do sistema. A pandemia também abriu flancos: as instituições passaram a receber centenas de acessos remotos de colaboradores trabalhando em casa.

É comum que criminosos tentem instalar softwares maliciosos em máquinas de instituições de pesquisa para minerar criptomoedas, processo que exige o uso de sistemas computacionais potentes para resolver problemas matemáticos – como recompensa, os hackers recebem moedas digitais. "Centros de pesquisa e universidades são alvo porque costumam ter computadores com alto poder de processamento. Além disso, podem guardar informações de valor, como segredos de patentes", observa Dennis Campos, gerente de tecnologia da informação do Centro Nacional de Pesquisa em Energia e Materiais (CNPEM), em Campinas.

O CNPEM teve um caso desse tipo, há alguns anos: seu sistema de monitoramento detectou um consumo de memória acima do normal e havia um software em um de seus computadores minerando criptomoedas. O centro reforçou sua equipe de segurança da informação após sofrer um outro ataque cibernético, em um final de semana em fevereiro de 2022. Assim como no caso do Ipen, foi um ataque do tipo *ransomware*. "Os criminosos já tinham conseguido criptografar algumas informações do nosso sistema, como dados administrativos e de pesquisa", recorda-se. Como havia um backup, a maioria deles pôde ser recuperada.

Apenas em 2024, os sistemas de segurança do CNPEM bloquearam cerca de 1.800 ataques e 116 milhões de tentativas. "Caso haja um ataque forte bem-sucedido, o maior risco é precisar parar o funcionamento da infraestrutura da instituição e suspender a operação da fonte de luz síncrotron Sirius", avalia.

A equipe do CNPEM descobriu que a invasão ocorreu devido à vulnerabilidade de um software. Após o incidente, definiu-se que atualizações de programas críticos devem ser feitas no mesmo dia em que forem liberadas. Outro procedimento que o centro está implementando é a instalação de um sistema de autenticação multifator, ou seja, o usuário da rede – colaborador ou visitante – deve fornecer mais de um tipo de verificação de identidade, em vez de apenas colocar sua senha. "É uma primeira barreira, permite que a gente identifique o horário, a localização e o que foi baixado. Isso ajuda no rastreamento da origem de eventuais incidentes", diz Rogger de Lima, gerente de segurança da informação do CNPEM, contratado após o ataque de 2022.

A Universidade Estadual de Campinas (Unicamp) sofreu uma tentativa de ataque em março passado. A investida hacker foi barrada, mas deixou a rede de computadores do *campus* mais lenta por quatro dias. Segundo Ricardo Dahab, diretor de Tecnologia da Informação e Comunicação (TIC) da Unicamp, os computadores da universidade são sondados diariamente por softwares maliciosos em busca de brechas para invasões. "O pior cenário seria ocorrer vazamentos de informações de pesquisas feitas em parceria com empresas, protegidas com contratos de sigilo. Ou, ainda, de dados sensíveis de pacientes do hospital da universidade", afirma.

No início de 2020 e em 2024, a universidade sofreu grandes vazamentos de dados de funcionários, de alunos e de usuários de um sistema de avaliação a distância, resultantes de ataques cibernéticos. No primeiro, dados de 200 mil usuários foram vazados e, no segundo, 140 mil. Segundo Dahab, o ataque de 2020 foi o maior incidente da instituição até o momento. "Descobrimos que houve uma configuração errada de um software. Depois disso, analisamos as vulnerabilidades e fechamos várias portas", conta. Outra medida foi investir em infraestrutura na instituição. "Além de usar o serviço em nuvem da Amazon, temos a nossa nuvem própria, da Unicamp, que armazena nossas bases de dados principais protegidas com backup."

Um problema comum em universidades é que seus laboratórios têm autonomia para criar sites e páginas, abrigando-as nos servidores centrais. "Criam-se sites à vontade. É comum que sejam administrados por bolsistas e fiquem sem manutenção depois que a bolsa termina e eles vão embora. A desatualização abre flancos de segurança", observa Dahab. Ele destaca que, caso não haja manutenção e ocorra alguma invasão, o departamento de TIC tem a liberdade de derrubar o site.

Para encontrar vulnerabilidades e ampliar a capacidade de se antecipar a ataques, a USP criou o programa Hackers do Bem, que oferece bolsas para cinco alunos do bacharelado de ciência da computação do IME-USP. O trabalho dos estudantes é atacar os sistemas da USP e encontrar flancos, a fim de que sejam corrigidos pela Superintendência de TI. "É um programa muito interessante, porque gera conhecimento novo, treina os alunos e ajuda a universidade a aperfeiçoar sua segurança", explica Ferreira. "Os bolsistas não têm contato com os técnicos que monitoram os sistemas computacionais da USP. O trabalho deles é independente."

Para ajudar a evitar perdas de dados sobre pesquisas em andamento ou de infraestrutura de ensino, a RNP criou em 2023 um Centro de Operações de Segurança (SOC), para acompanhar e neutralizar ataques. Por enquanto, o SOC contempla diversas camadas de proteção, e uma

Segurança da informação

Confira as medidas que podem melhorar a cibersegurança

Defesa em profundidade

Adote múltiplas camadas de proteção para dificultar a ação de invasores e detectar incidentes precocemente

Backup

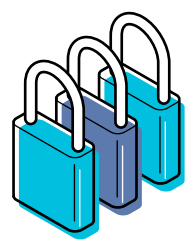
Faça cópias de segurança regularmente para garantir a disponibilidade dos dados e recuperar sistemas após falhas ou ataques

Proteção contra vulnerabilidade

Monitore sistemas, aplique atualizações e acompanhe canais técnicos para prevenir falhas

Segmentação e controle de acesso

Use autenticação multifator e o modelo de confiança zero (nenhum usuário ou sistema é confiável e todos devem ser verificados continuamente, mesmo dentro da rede) para limitar acessos e isolar incidentes



Conscientização

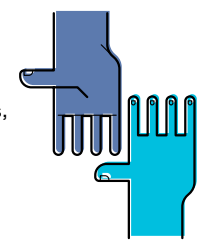
Realize treinamentos para tornar os colaboradores agentes ativos na segurança da informação

Continuidade de negócios

Elabore planos para manter as operações mesmo diante de incidentes cibernéticos

Resposta e cooperação

Integre especialistas externos (como consultores, equipes de segurança ou órgãos especializados) aos processos de resposta a incidentes para agir com eficiência



FONTE "RELATÓRIO ANUAL DE SEGURANÇA 2023" (CAIS-RNP)

FOTO LÉO RAMOS CHAVES/REVISTA PESQUISA FAPESP **INFOGRÁFICO** ALEXANDRE AFFONSO/REVISTA PESQUISA FAPESP

Profissionais de cibersegurança monitoram tentativas de ataques ao CNPEM, em Campinas

delas monitora ataques de negação de serviço, em que é enviado um grande volume de solicitações de acesso, sobrecarregando e derrubando sistemas. O monitoramento é feito 24 horas por dia nas 97 instituições que até o momento passaram pelo processo de adesão ao centro, e na própria infraestrutura principal da rede, o *backbone*. Se bem-sucedido, esse tipo de ataque pode prejudicar a rotina de trabalho e de pesquisa das instituições. "Não se trata de uma possibilidade. Incidentes cibernéticos vão acontecer", destaca o especialista em cibersegurança Ivan Tasso Benevides, gerente de Operações de Segurança da RNP. Entre 2023 e 2024, o número de ataques à rede aumentou 56%.

O centro montado pela RNP fica em uma sala na sede da instituição em Brasília, com analistas que acompanham a rede e a *deep web*, para onde geralmente vão os dados vazados. "Isso permite uma resposta mais rápida e mais efetiva nesses casos", conta Benevides. "Lançamos um edital para montar mais três centros pelo Brasil até o final deste ano. Um deles será na cidade de São Paulo", complementa.

Antes de o centro entrar em operação, as instituições que sofriam ataques costumavam procurar o Centro de Atendimento a Incidentes de Segurança (Cais), ao qual o SOC está vinculado, para pedir orientações sobre como proceder. "Aguardávamos os chamados de apoio das instituições para suportá-los. Agora, adotamos uma postura ativa e conseguimos deter os ataques antes que aconteçam nas instituições associadas à Rede", observa Benevides. Elas podem optar por aderir ao sistema do SOC. Para isso, há pacotes – o primeiro, mais básico, é gratuito. Depois há o intermediário e o avançado, pagos.

Ele conta que, em um caso atendido recentemente pela RNP, uma instituição de ensino por pouco não teve sua rede invadida depois que um funcionário usou as credenciais da instituição – e-mail e senhas corporativos – para fazer cadastro em um outro site. Houve um vazamento e suas informações foram parar na *deep web*. Em outro caso, uma universidade da região Norte foi alvo de um ataque em que o hacker apagou dados e o backup estava desatualizado há dois meses. "Eles perderam tudo o que foi feito nesse intervalo."

Os ataques de negação de serviço são os mais recorrentes que as instituições associadas à RNP sofrem, segundo Benevides. O segundo mais frequente é o *phishing*, golpe que tenta levar o usuário a clicar em formulários falsos e fornecer dados e senhas. O terceiro tipo mais comum é o *ransomware*, o que atingiu o Ipen.

O CNPEM foi uma das instituições que aderiu ao SOC da RNP como um serviço complementar às medidas internas de segurança. Campos, do CNPEM, destaca que a equipe tem buscado informações com outros centros de pesquisa internacionais para garantir a cibersegurança do projeto Orion, complexo laboratorial para pesquisas avançadas em vírus e bactérias, com instalações de máxima contenção biológica (NB4), que devem ser as primeiras do mundo conectadas a uma fonte de luz síncrotron (*ver entrevista na página 56*). Seus sistemas críticos, como o ar-condicionado, serão automatizados, e a proteção contra falhas e interferências vai ser essencial para preservar o material biológico. ●