TECNOLOGIA

Segurança digital do governo em xeque

Invasores do Siafi conseguiram mascarar desvios, enganar gestores do sistema e roubar credenciais de acesso que foram usadas para desviar milhões de reais, evidenciando falhas nos mecanismos de proteção das redes governamentais

» RENATO SOUZA

Ao longo deste mês, criminosos que agem na internet fizeram pelo menos três investidas contra o Sistema Integrado de Administração Financeiro (Siafi), usado pelo governo federal para executar ordens de pagamento. As tentativas realizadas pelos invasores não foram bloqueadas e, pelo menos, R$ 14 milhões foram desviados para contas particulares em várias partes do país. O ataque, exitoso em subtrair recursos públicos, coloca em dúvida a segurança cibernética do Executivo e dos sistemas usados pelo poder público — que envolvem também os poderes Legislativo e Judiciário.

De acordo com as investigações feitas até agora, o ataque contra o Siafi se deu por um método conhecido como "fishing", palavra em inglês que, na tradução literal, significa "pescaria". Nesse tipo de cibercrime, pessoas mal-intencionadas enviam iscas, como links de páginas falsas, para coletar os dados dos alvos. Acreditando estar em uma página oficial — do governo ou de bancos, por exemplo —, a vítima insere informações que são usadas em golpes e fraudes. Além disso, segundo fontes da Polícia Federal (PF) consultadas pelo **Correio**, os criminosos também usaram de engenharia social. Um inquérito foi aberto para investigar o caso.

O sistema foi invadido por crackers, como são conhecidas as pessoas com amplo conhecimento de informática para gerar danos e prejudicar pessoas, empresas e instituições. É comum que as pessoas usem o termo hacker para se referir a autores de crimes cibernéticos. Porém, tecnicamente, os hackers são profissionais de tecnologia da informação que atuam para proteger sistemas, encontrando vulnerabilidades para resolver as falhas. Estão nesse grupo investigadores e agentes da Polícia Federal que atuam na área de defesa cibernética, militares do Exército especializados e integrantes de equipes de segurança da informação de empresas privadas e profissionais independentes que atuam com soluções de TI.

A engenharia social ocorre quando funcionários de empresas ou entes públicos são convencidos, por meio de técnicas de enganação, a repassar informações sensíveis, como senhas de sistemas, números de matrícula e de login ou, ainda, liberar acesso físico a salas de segurança ou a redes internas. Esse tipo de situação pode ser amenizada com uma "boa cultura corporativa", ou seja, com cursos, metodologias, orientações e criação de normas internas para evitar que os atacantes tenham sucesso em seus objetivos.

Fragilidade

O Siafi é utilizado para realizar a gestão financeira e executar ordens de pagamento do governo, do Legislativo (Câmara e Senado) e do Judiciário, que inclui o Supremo Tribunal Federal (STF) e o Tribunal Superior Eleitoral (TSE). A invasão, que se deu de maneira silenciosa por semanas, demonstra fragilidades nas camadas de segurança do sistema responsável pelo gerenciamento de bilhões de reais do Orçamento, destinados ao pagamento de servidores públicos e de serviços.

Bruno Fraga, especialista em segurança da informação e investigador digital, explica que o ataque ao Siafi pode ser explicado, em parte, pela educação dos usuários que têm acesso ao sistema. "O suposto ataque ao Siafi demonstrou uma combinação de vulnerabilidades que podem ser entendidas sob vários aspectos técnicos e operacionais relevantes na área de segurança cibernética. O incidente foi caracterizado pelo uso de técnicas de phishing para coletar credenciais de administradores financeiros do sistema. Isso sugere uma falha significativa na segurança das informações e na educação dos usuários quanto a ameaças cibernéticas, permitindo que atacantes obtivessem acesso não autorizado a operações financeiras críticas. Uma vez que os atacantes conseguiram acesso mediante credenciais válidas, exploraram deficiências no sistema de autenticação do Siafi", afirmou.

O especialista destaca que os invasores conseguiram "mascarar" suas ações ilegais como se fossem lícitas e corriqueiras. "A autenticação insuficientemente robusta permitiu que eles mascarassem suas atividades ilícitas como se fossem transações legítimas, dificultando a detecção imediata. Após a detecção do suposto ataque, foram implementadas medidas adicionais de segurança. No entanto, a reação pós-ataque sugere que o sistema não estava adequadamente preparado para responder a uma intrusão dessa magnitude", completa.

Prevenção

Lucas Bonfim, especialista em engenharia e gestão de infraestruturas tecnológicas complexas, ressalta que é fundamental prevenir esse tipo de invasão, mas, agora que o problema já aconteceu, faz-se necessário rever os procedimentos, promover treinamentos dos usuários e fechar as portas do sistema para acessos não autorizados. "O ataque ao Siafi revelou várias vulnerabilidades no sistema, tanto em termos de segurança da informação quanto na educação dos usuários sobre ameaças cibernéticas. A invasão bem-sucedida destacou falhas na autenticação dos usuários, permitindo que os invasores utilizassem credenciais legítimas para realizar atividades maliciosas. Isso evidencia a necessidade de melhorar as medidas de segurança e implementar processos de conscientização e treinamento mais eficazes para os usuários do sistema", afirma.

Segurança em jogo

Ataque ao sistema de pagamentos do governo gera alerta sobre importância de se proteger de criminosos virtuais e temor de prejuízos financeiros

CASO SIAFI

O que é: invasão ao Sistema Integrado de Administração Financeiro
Quando: abril de 2024
Quem: crackers, que seriam de uma organização criminosa
Porque: objetivo era desviar milhões dos cofres públicos
Como: phishing, roubo de dados
Prejuízo: R$ 14 milhões e necessidade de atualização dos sistemas

PRINCIPAIS ATAQUES

Ransomware
Definição: um tipo de malware que criptografa os arquivos do sistema da vítima e exige o pagamento de um resgate para restaurar o acesso aos dados.
Funcionamento: O ransomware geralmente é distribuído por e-mail ou através de sites comprometidos.

Phishing
Definição: Um método de fraude on-line que utiliza e-mails falsos, mensagens de texto ou sites fraudulentos para enganar as pessoas e obter informações confidenciais, como senhas e números de cartão de crédito.
Funcionamento: os criminosos enviam mensagens ou criam páginas da web que se assemelham a comunicações legítimas de empresas conhecidas ou instituições financeiras.

Ataques de Engenharia Social
Definição: nestes casos, os criminosos usam artimanhas para enganar e convencer os funcionários humanos a entregarem informações sensíveis, como senhas.
Funcionamento: os crackers se passam por diretores das empresas, equipes de suporte técnico e até autoridades para obterem dados importantes e de segurança.

Ataques de Negação de Serviço (DDoS)
Definição: visam sobrecarregar os servidores de uma organização, tornando seus serviços indisponíveis para usuários legítimos.
Funcionamento: os criminosos utilizam uma grande rede de computadores comprometidos (botnets) para enviar um grande volume de tráfego de internet, ao mesmo tempo, para o servidor-alvo, congestionando sua capacidade de resposta e tornando-o inacessível.

Ataques de Injeção de Código (SQL Injection)
Definição: ataques que exploram falhas de segurança em sites e aplicativos da web para inserir código malicioso em bancos de dados, permitindo acesso não autorizado ou exfiltração de dados.
Funcionamento: os criminosos exploram vulnerabilidades em formulários da web ou parâmetros de URL para injetar comandos SQL maliciosos, que podem ser usados para extrair informações sensíveis do banco de dados ou comprometer o sistema.

COMO PREVENIR

- Certifique-se de que o acesso a todos os recursos seja seguro: independentemente se os recursos estejam na nuvem, ou sejam itens locais ou qualquer lugar que os usuário estejam localizados;
- Foque no controle de acesso: quanto menos privilégio, melhor. Qualquer pessoa tem acesso à rede, desde o CEO da empresa até quem está fazendo seu estágio profissional, o que permite passar de um elemento a outro.
- Empregue energias no gerenciamento de acesso.
- Visibilidade dos dados: é fundamental saber o que está acontecendo na rede e armazenar isso para alimentar outras ferramentas, gerar relatórios, ver como os usuários estão se comportando e quem está acessando quais recursos.
- Faça cópias (backups) dos arquivos, para o caso de perdas.

PARA PESSOAS

- Não clique em links suspeitos.
- Não repasse seus dados para contas suspeitas no WhatsApp.
- Ative autenticação em dois fatores nas redes sociais.
- Evite pagar boletos que chegam por e-mail.
- Evite conectar o celular em redes de internet públicas.
- Desconfie de pedidos de dinheiro nas rede sociais.
- Desconfie de itens à venda nas redes por preços baixos demais.
- Confirme que está falando com amigos ou parentes (podem ser contas falsas).

Fonte: One Identity, Correio Braziliense