CIÊNCIA, TECNOLOGIA E INOVAÇÃO

AUDITORIA DOS CONTROLES DE SEGURANÇA DOS SERVIDORES WEB, E-MAIL E DNS

O QUE O TCU FISCALIZOU?

O TCU auditou milhares de sites de organizações públicas dos três poderes (Executivo, Legislativo e Judiciário), tanto do governo federal quanto de estados e municípios, para avaliar se a configuração de servidores de internet, e-mail e DNS (serviço que traduz endereços de sites) estava alinhada às boas práticas. Os testes foram feitos com a ferramenta "TOP", fornecida pelo NIC.BR **(http://top.nic.br)**.

O QUE O TCU ENCONTROU?

O Tribunal identificou sete riscos que podem ter como consequência manipulação de tráfego de rede; comprometimento de contas de usuários; roubo, vazamento ou perda de dados; falha ou paralisação dos sistemas de organizações públicas. As conclusões preliminares indicam que muitos serviços de hospedagem de sites, e-mail e DNS não seguem as melhores práticas de segurança. Isso deixa a maioria das organizações e seus usuários vulneráveis a ataques cibernéticos, principalmente por hackers, que podem realizar ações maliciosas, como as que seguem:

1.1 Interceptar o tráfego de um usuário conectado em uma rede sem fio insegura de um aeroporto com sua organização, observar as trocas de informações e alterar o conteúdo dos dados transitados (e.g., credenciais, conteúdos sensíveis), pois poucos domínios testados (2%) implementam conexão segura pela web;

1.2 Interceptar e-mails e informações contidas nas páginas web, geralmente sem o conhecimento dos usuários envolvidos, podendo ler, modificar e injetar informações na comunicação, na maioria das organizações, pois poucos domínios testados estão em nível baixo de risco, quanto à confidencialidade e à integridade que podem ser obtidas por meio da implementação de criptografia, no tráfego pela web e por e-mail (6% e 5%, respectivamente);

1.3 Sobrepor ou disfarçar elementos maliciosos em botões, links ou áreas vazias da página da web, induzindo o usuário a executar ações indesejadas, como permitir acesso a informações confidenciais, ativar permissões não autorizadas ou efetuar transações financeiras não intencionais, pois muitos domínios testados (84%) estão em nível alto de risco, para estes ataques, por não implementar nenhum dos quatro cabeçalhos web testados;

1.4 Redirecionar usuários para sites maliciosos, resultando em roubo de informações, ataques de *phishing* e outros tipos de exploração, pois seriam conectados a destinos incorretos e não autênticos, já que muitos domínios testados estão em nível alto de risco, para ataques ao serviço de resolução de nomes que apoiam tanto os serviços web quanto os serviços de e-mail (81% e 86%, respectivamente);

1.5 Realizar ataques de engenharia social por meio de *phishing*, pois poucos domínios avaliados (8%) implementam os três protocolos de segurança nos serviços de e-mail que reduzem alguns tipos de ataque dessa natureza.

O QUE O TCU DECIDIU?

O TCU decidiu dar conhecimento sobre a fiscalização a oito organizações que representam a multiplicidade das detentoras dos domínios testados, para que avaliem, se entenderem conveniente, a adoção de medidas e a elaboração de estratégias, para orientar as organizações a implementar os controles testados nesta auditoria. Caso as organizações não façam essas mudanças, manterão vulneráveis os serviços hospedados em seus servidores web, e-mail e DNS, que estão visíveis a todos os agentes de ameaça do planeta. O Tribunal também autorizou a Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI) a divulgar a Matriz de Riscos e Controles resultante da fiscalização, que é um guia de orientação para a tomada de decisão sobre

a implementação dos controles testados **(disponível em https://www.tcu.gov.br/dasi)**.

QUAIS OS BENEFÍCIOS ESPERADOS?

Caso as organizações adotem configurações seguras nestes serviços, haverá redução de riscos de ataques cibernéticos que exploram as falhas de configuração em serviços oferecidos na internet pela administração pública.

DADOS DA DELIBERAÇÃO

Acórdão: 523/2024-TCU-Plenário
Data da sessão: 27/03/2024
Relator: Ministro Aroldo Cedraz
TC: 017.413/2023-0
Unidade Técnica: Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI)