Protocolos ampliam mecanismos de segurança cibernética no Judiciário

12/01/2021

Prevenir, gerenciar e investigar. Essas são as diretrizes de protocolos instituídos pelo Conselho Nacional de Justiça para garantir a segurança do ecossistema digital dos tribunais e demais órgãos jurisdicionais do país. As normas são decorrentes do trabalho do Comitê de Segurança Cibernética do Poder Judiciário.

123RF

123RFProtocolos ampliam mecanismos de segurança cibernética no Poder Judiciário

Segundo o coordenador do Comitê, o juiz auxiliar da presidência do CNJ Alexandre Libonati, a ideia é que os protocolos de prevenção, gerenciamento e investigação de incidentes cibernéticos uniformizem e permitam maior proteção de dados e informações virtuais dos órgãos do Poder Judiciário.

"As situações são as mais diversas em razão do porte do órgão, do quantitativo de servidores na área de segurança, dos sistemas envolvidos, do tipo de autenticação e acesso empregados e da própria atenção que dão ao tema. O que se pretende com os protocolos é estabelecer padrões mínimos de segurança que sejam uniformes", disse.

Para o representante do Gabinete de Segurança Institucional da Presidência da República no Comitê de Segurança Cibernética, Marcelo Fontenelle, os protocolos constituem um primeiro conjunto normativo de segurança cibernética a serem observados pelos órgãos do Poder Judiciário.

"Acredito que as maiores contribuições sejam uma crescente sensibilização dos órgãos do Poder Judiciário quanto à relevância do tema segurança cibernética, a possibilidade de trabalhar de forma colaborativa com órgãos de outros Poderes e abrir caminho para um posicionamento convergente do Brasil em termos de segurança cibernética", afirmou.

Fontenelle, que atua como diretor do Departamento de Segurança da Informação da Presidência da República, destacou a importância da contribuição de diferentes órgãos na construção dos protocolos de segurança cibernética do Judiciário.

"É importante o trabalho colaborativo. Isso é notório, por exemplo, na administração pública, onde o Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo atua na coordenação de uma rede de equipes de prevenção, tratamento e resposta a incidentes cibernéticos. E não existe uma relação de subordinação nesse caso, posto que cada órgão é responsável pela sua própria segurança", completou.

Prevenção
O Protocolo de Prevenção a Incidentes Cibernéticos (PPICiber/PJ) foi instituído pela Resolução CNJ 361/2020. Ele traz diretrizes para a gestão do risco organizacional e permite decisões adequadas para o enfrentamento de ameaças e a implementação de melhores práticas e metodologias levando em consideração a realidade de cada órgão do Judiciário.

As funções básicas do PPICiber contemplam aspectos de identificação, proteção, detecção, resposta e recuperação em casos de incidentes cibernéticos. Cada órgão deve instituir Equipes de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), que poderão solicitar apoio multidisciplinar abrangendo as áreas de tecnologia da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, dentre outras necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva.

"Temos a previsão de apresentar, em março, um procedimento de *compliance* mediante o preenchimento de *check lists*, sem prejuízo de vistorias e inspeções locais", explica Libonati.

Para dar um tratamento mais adequado aos ataques cibernéticos bem como para minimizar eventuais impactos na operação, o Protocolo de Prevenção a Incidentes Cibernéticos prevê que os órgãos possuam mecanismos de respostas e prevenção, com parâmetros de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.

Gerenciamento
Complementar ao PPICiber, o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC/PJ) é regulamentado pela Resolução CNJ 360/2020. Ele apoia a implementação de ações responsivas quando ficar evidente que uma ocorrência de segurança cibernética não será mitigada rapidamente e poderá durar dias, semanas ou meses.

O PGCC é iniciado quando ficar caracterizado grave dano material ou de imagem e o incidente impactar alguma atividade finalística ou serviço crítico, por longo período, com impacto no atendimento à população. O protocolo estabelece medidas a serem tomadas antes, durante e depois da crise.

Na chamada fase pré-crise, o Protocolo prevê que os órgãos do Judiciário estabeleçam um Programa de Gestão da Continuidade de Negócios, definindo atividades críticas cruciais, identificando os ativos de informação, avaliando continuamente os riscos, categorizando os incidentes e estabelecendo procedimentos de resposta específicos. Isso implica em priorizar o monitoramento, acompanhamento e tratamento dos riscos, com a realização de testes para validação dos planos e procedimentos.

Cada órgão deve criar uma sala de situação e um Comitê de Crises Cibernéticas. Assim, quando a ETIR identifica uma crise cibernética, o Comitê de Crises é acionado imediatamente e efetiva os planos de contingência para a continuidade dos serviços prestados. Cabe também ao Comitê entender o incidente, levantar as informações e soluções, avaliar suspensão de serviços ou sistemas, aplicar protocolo de investigação, organizar a comunicação e elaborar plano de retorno à normalidade.

Quando as operações retornam à normalidade, o Comitê de Crises Cibernéticas realiza a análise criteriosa das ações tomadas, observando as bem-sucedidas e as que ocorreram de forma inadequada, levando em consideração aspectos como causa-raiz do incidente, impacto nos dados, sistemas e operações, processos de detecção e proteção e estratégias de recuperação.

Ao final, é elaborado relatório contendo a descrição e detalhamento do incidente bem como o plano de ação tomado. O objetivo é documentar o processo para evitar que novos incidentes similares ocorram ou para que, em caso de ocorrência, se reduzam os danos causados.

Investigação
Para estabelecer os procedimentos básicos para coleta e preservação de evidências, bem como para comunicação dos fatos relevantes ao órgão policial, o CNJ instituiu, por meio da Resolução CNJ 362/2020, o Protocolo de Investigação para Ilícitos Cibernéticos. Ele apresenta as ações que devem ser realizadas pela ETIR para organizar as informações necessárias para apuração policial.

Durante o processo de tratamento do incidente penalmente relevante, a Equipe deverá coletar e preservar, entre outros, as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses, os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM), bem como a adequação dos ativos de informação.

Se não for possível preservar as mídias de armazenamento, a ETIR deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: *logs*, configurações do sistema operacional, arquivos do sistema de informação e outros julgados necessários, mantendo-se a estrutura de diretórios original e os metadados desses arquivos, como data, hora de criação e permissões.

Após a conclusão do processo de coleta e preservação das evidências da ocorrência penalmente relevante, a ETIR elabora Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, descrevendo detalhadamente os eventos verificados, que será encaminhado ao órgão de polícia judiciária com atribuição para apurar os fatos.

Gestão
Relator dos atos normativos que definiram os protocolos de segurança cibernética, o presidente do CNJ, ministro Luiz Fux, afirmou que "ao caminharmos a passos largos para o Judiciário 100% digital, torna-se imprescindível garantir a segurança cibernética do ecossistema digital do Poder Judiciário brasileiro, estabelecendo processos de trabalho orientados para a boa gestão da segurança da informação, o que abrange o estabelecimento de protocolos de prevenção, de atuação em eventuais momentos de crise e, finalmente, de constante atualização e acompanhamento das regras de *compliance* às melhores práticas".

Assim, assegura-se, ao mesmo tempo, o cumprimento da Lei de Acesso à Informação, bem como do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais (LGPD). *Com informações da assessoria de imprensa do CNJ.*

Fonte: https://conjur.jumps.com.br/2021-jan-12/protocolos-ampliam-mecanismos-seguranca-cibernetica-judiciario/