Especialistas em segurança da informação consideram o sistema do TRT ideal

Reportagem do Jornal Correio enfoca a segurança da informação nos órgãos do Poder Judiciário da Paraíba

O Jornal Correio da Paraíba publicou extensa reportagem na edição deste domingo, 28, enfocando a segurança da informação nos órgãos do Poder Judiciário da Paraíba, além de Ministério Público Estadual e do Tribunal de Contas. A reportagem, escrita pela jornalista Mislene Santos, ocupa três páginas e ouve especialistas em segurança da informação que consideram o sistema do Tribunal do Trabalho da Paraíba TRT como ideal.

As informações do TRT foram prestadas pelo diretor da Secretaria de Tecnologia da Informação e Comunicação Setic, Max Frederico Guedes Pereira.

Em resumo, o que diz a reportagem sobre o TRT-PB:

Em 2007, o Tribunal Regional do Trabalho da 13ª Região (TRT-PB) implantou, por meio da resolução administrativa 065, a política interna de segurança da informação do órgão. O objetivo da ação foi para preservar o ambiente tecnológico, assegurar o controle e a credibilidade das informações do tribunal.

O diretor da Secretaria de Tecnologia da Informação do órgão, Max Frederico Feitosa, informou que a segurança das informações online do tribunal é garantida através de softwares de segurança para proteção em servidores de rede, computadores e webmail como firewall, IPS, IronPort entre outros.

Ele destacou que, recentemente, o TRT investiu R$ 2,6 milhões em equipamentos de seguranças como compra de sala-cofre que custou R$ 1,6 milhão e mais R$ 1 milhão foi investido em Projeto de Alta Disponibilidade. O controle das informações é instantâneo a todo tempo, através dessas ferramentas, qualquer tentativa de invasão é detectada e medidas são tomadas imediatamente pelos servidores da área de segurança da Informação.

Os professores do IFET-PB destacaram que o sistema de segurança implantado no TRT dificulta as invasões e o acesso a informações importantes. Eles consideraram que essa é política de segurança ideal para proteger informações de instituições desse porte.

REPORTAGEM NA ÍNTEGRA:

Tribunal de Justiça e Tribunal de Contas são vulneráveis aos hackers

Recursos utilizados pelo TRT e TRE são mais eficazes e dificultam tentativa de invasões às redes de informações.

Os recursos usados pelo Tribunal de Justiça (TJ-PB) e pelo Tribunal de Contas (TCE-PB) para garantirem a segurança da informação dessas instituições são considerados frágeis e facilitam ataques externos de hackers. Já recursos utilizados pelo Tribunal Regional do Trabalho 13ª Região (TRT-PB) e Tribunal Regional Eleitoral (TRE-PB) são mais modernos, eficazes e conseguem dificultar - mas não eliminar - possíveis tentativas de invasões à rede de informações destes tribunais.

A avaliação da política de segurança da informação desses órgãos foi feita por professores especialistas do curso superior de Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia (IFET-PB), através das informações repassadas pelos órgãos, via e-mail, à reportagem do Correio. Para os especialistas na área, a realidade da política de segurança dos órgãos estaduais é bem diferente da dos federais.

O professor de Redes Márcio Emanuel de Araújo, que trabalha na área há dez anos, faz um alerta: quem entrar no sistema de um tribunal desses pode ter acesso a qualquer informação. Ele pode copiar processos e até modificar sentenças, dependendo de como esteja configurada a segurança e permissões da rede dos referidos órgãos.

Especialista vê perigo nas senhas

Também com dez anos trabalhando na área de tecnologia da informação, Thiago Moura, professor de Sistema de Internet, complementa: tudo que estiver disponível na rede o hacker terá acesso e se ele conseguir copiar as senhas de quem tem acesso as informações mais importantes da instituição poderá modificar todo o conteúdo dos processos dos tribunais.

Observamos que a política de segurança do TJ e do TCE é mais vulnerável a ataques de hackers do que as do TRT e TRE, disse Márcio Emanuel ao analisar as informações repassadas pelos setores competentes dos tribunais. Para o professor, o procedimento adotado pelo TRT, por exemplo, é correto e que lá, eles estão com um sistema bem mais seguro para ataques internos e externos.

Já o professor Thiago Moura enfatizou que, mais do que bons programas, é preciso ter profissionais bem preparados para manusear os softwares. Ele

frisou que o investimento em qualificação é muito mais importante do que nos próprios equipamentos, pois uma pessoa bem preparada consegue manter um órgão protegido com os programas que ele dispor, mas uma pessoa mal preparada não consegue manusear bons programas de segurança.

TRT investiu R$ 2,6 milhões

Em 2007, o Tribunal Regional do Trabalho da 13ª Região (TRT-PB) implantou, por meio da resolução administrativa 065, a política interna de segurança da informação do órgão. O objetivo da ação foi para preservar o ambiente tecnológico, assegurar o controle e a credibilidade das informações do tribunal.

O diretor da Secretaria de Tecnologia da Informação do órgão, Max Frederico Feitosa, informou que a segurança das informações online do tribunal é garantida através de softwares de segurança para proteção em servidores de rede, computadores e webmail como firewall, IPS, IronPort entre outros.

Ele destacou que, recentemente, o TRT investiu R$ 2,6 milhões em equipamentos de seguranças como compra de sala-cofre que custou R$ 1,6 milhão e mais R$ 1 milhão foi investido em Projeto de Alta Disponibilidade. O controle das informações é instantâneo a todo tempo, através dessas ferramentas, qualquer tentativa de invasão é detectada e medidas são tomadas imediatamente pelos servidores da área de segurança da Informação.

Os professores do IFET-PB destacaram que o sistema de segurança implantado no TRT dificulta as invasões e o acesso a informações importantes. Eles consideraram que essa é política de segurança ideal para proteger informações de instituições desse porte.

Segurança da informação

Para garantir a segurança da informação o Tribunal Regional Eleitoral da Paraíba (TRE-PB) conta com o apoio de Unidades da Justiça Eleitoral que detêm atribuições relacionadas à segurança de dados, além da X Comissão de Segurança da Informação cujas atividades são estabelecidas pela Resolução 22.780/08 do Tribunal Superior Eleitoral (TSE).

O documento estabelece normas para o uso de ambientes das redes de internet, intranet e correio eletrônico. Já a de nº 23.326/10 dispõe sobre as diretrizes para a tramitação de documentos e processos sigilosos no âmbito da Justiça Eleitoral.

O controle do acesso as informações é um das medidas que compõe a política de segurança da informação do TRE-PB, é o que afirma a assessoria

de comunicação do órgão. De acordo com a Assessoria de Comunicação do órgão, esse controle garante a confidencialidade processos que tramitam na Corte.

A assessoria não informou detalhes da forma e nem dos softwares que são usados pelo tribunal para não comprometer a segurança dos dados, mas afirma que não há vazamento de informações. Os responsáveis pela segurança dos dados são os servidores das unidades técnicas que controlam o acesso a rede do TRE-PB.

Segundo a Ascom, esses funcionários têm formação superior em informática e receberam treinamento em segurança da informação periodicamente.

Impedir invasão tem custo muito alto

O diretor de Tecnologia da Informação do TJ-PB, José Augusto de Oliveira Neto, disse que tornar uma invasão impossível tem um custo muito alto e não vale à pena implantá-los no tribunal.

Esses equipamentos são caríssimos, com valores muito superiores aos das informações que terão que proteger. Esse investimento só se justifica para proteger as informações da Nasa e das Forças Armadas, disse José Augusto.

Ele também afirmou que o TJ-PB só iniciou a implantação de uma política de segurança da informação depois que o Conselho Nacional de Justiça (CNJ) exigiu. O processo, que ainda está sendo implantado, tem o objetivo de proteger todo o conteúdo digital relativo aos processos judiciais.

Ele explicou que a política de segurança da informação do órgão é composta de um conjunto de normas e procedimentos que disciplinem o uso dos recursos de informática para que o sistema não corra risco de invasão, deteriorização e destruição de conteúdo.

Para conseguirmos um bom resultado foi necessário restringir o acesso a sites, para evitar a entrada em páginas maliciosas visando a defesa contra o ataque de vírus e execução de programas maliciosos acessados através destes sites, frisou.

Outra medida adotada para garantir a segurança das informações do tribunal é o controle do conteúdo instalado em todos os computadores existente no órgão e em todas as unidades ligadas ao TJ no Estado. Além disso, José Augusto ressaltou que dispõe de equipamentos e softwares que fazem varredura no sistema em busca de programas invasores, vírus e que também detectam intrusos no sistema.

106 técnicos

As ferramentas que garantem a segurança do tribunal são controladas internamente e ficam a cargo da diretoria de Tecnologia da Informação (TI), que é composta por 106 técnicos responsáveis pelo setor de informática.

Essas ferramentas registram o endereço do IP de todos os computadores que acessarem o site o TJ. Nenhum sistema é 100% seguro, mas nós fazemos o monitoramento constante do servidor para garante a privacidade das informações do tribunal.

Monitoramento criptografado

A chefe do Centro de Processamento de Dados (CPD) - responsável pela segurança dos dados do Tribunal de Contas do Estado (TCE-PB) - Gerluce Baracho, Informou que o órgão dispõe de um sistema de monitoramento criptografado, que identifica qualquer entrada no sistema de dados do Tribunal. Isso significa que: se uma pessoa acessar o site do TCE o login dela é identificado e se alguém tentar penetrar em locais que não são acessíveis ao público o TCE terá sua emissão identificada.

Gerluce Baracho disse que cada funcionário possui uma senha de entrada no sistema e ao acionar seu computador é imediatamente detectado pela central. Ela explicou que para entrar em setores mais delicados o servidor depende de outra senha, do Sistema Tramita que só é dada conforme o grau de necessidade de cada funcionário para acessar essa informação.

Ela garantiu que as decisões do TCE não vazam, pois elas são públicas e transmitidas online pela internet. Somente durante a fase de apuração e julgamento os processos são protegidos pelo sistema de cifras que impede a entrada no nosso sistema de informática, frisou Gerluce Baracho. Segundo ela, esse tipo de vazamento nunca aconteceu no TCE.

AL tenta se proteger de invasões

Assim como os tribunais, a Assembleia Legislativa do Estado (AL-PB) também tenta se proteger contra invasões, embora o diretor de redes e conectividades da instituição, Bruno Hugolino de Araújo, reconheça que nenhum.

O cuidado foi redobrado já que em maio deste ano a Polícia Federal, em uma varredura, descobriu um grampo telefônico e ambiental no gabinete do deputado estadual Ricardo Marcelo (PSDB), presidente do Poder Legislativo paraibano. A varredura foi solicitada pelo próprio presidente, que encaminhou um pedido de investigação ao Ministério Público da Paraíba e, agora, aguarda o resultado.

Ele disse que usa vários programas para proteger o sistema que hospeda os Processos Legislativos e o sistema que acompanha esses processos. Ele

disse também que o site da AL é de responsabilidade da Companhia de Processamento de Dados da Paraíba (Codata). A gente tem vários firewall, programas de detecção de intrusos e antivírus para tentar nos proteger, enfatizou Bruno. Além desses programas ele disse que têm outros que não pode revelar por questões de segurança.

Bruno Hugolino explicou que também faz parte do pacote de proteção das informações da AL sistemas de linguagens e serviços que acompanham o domínio da Casa. Ele informou que esses procedimentos protegem o sistema contra ataques internos e externos. Internamente usamos domínios que controla tudo que é feitos nos computadores da instituição, frisou Bruno.

Ele considera que em termos de proteção de dados a Assembleia está bem protegida e os profissionais estão preparados para, em casos de invasão, resolver o problema rápido. Agente tem que estar preparado para controlar o problema, porque quando o hacker quer não tem jeito de impedir a invasão, finalizou.

O presidente Ricardo Marcelo espera que o MPE apure os fatos e puna os responsáveis pelas escutas telefônicas. Ele disse ter consciência plena da responsabilidade do Ministério Público e na capacidade do órgão para descobrir os culpados pelo crime. Estamos aguardando a conclusão do caso e creio que o órgão está à altura de resolver o problema. Os grampos foram encontrados no dia nove de maio, depois que o presidente da casa solicitou que a PF realizasse uma varredura na Assembleia.

Restrição de acesso a sites

Para o professor de Redes, Márcio Emanuel de Araújo, a restrição de acesso a sites considerados maliciosos e o controle na instalação de conteúdo nos computadores feito pelo TJ, por exemplo, é uma forma de impedir que o sistema seja atingido por vírus e venha a ser danificado.

No entanto, ele alerta que esse procedimento não protege a rede de nenhum ataque externo que na maioria das vezes ocorre de computadores que estão fora do órgão. Araújo considerou que a varredura realizada no sistema do tribunal, dependendo do programa utilizado, pode identificar invasões e também dificultá-las.

O professor de Sistema de Internet, Thiago Moura, considerou o sistema de monitoramento criptografado utilizado pelo TCE bastante vulnerável a invasões. Este tipo de monitoramento a melhor solução para proteção das senhas e logins de usuários externos ao site do TCE. Para ele, o modo mais eficiente para se proteger informações importantes é através de investimentos

em bons equipamentos e na qualificação profissional. Segundo o professor a proteção seria mais eficiente.

Para os professores, não há regra para invadir o sistema de informações e a melhor forma de evitá-la é através de capacitação profissional e monitoramento da rede de informação. Segundo eles, a única forma de identificar os invasores é por meio do registro do IP ((Internet Protocol) do computador que foi usado no ataque, mas Márcio Emanuel destacou que quem vai invadir grandes sites não faz isso de casa.

Ele explicou que, geralmente, quem faz esses ataques utiliza uma máquina Zumbi .O professor disse que esta máquina instala um programa em vários computadores de usuários comuns da internet e com um comando disparado ou uma hora pré-programada todas as máquinas fazem um ataque simultâneo tentando desativar algum serviço disponível na internet. De acordo com o Márcio Araújo, isso dificulta a identificação de quem cometeu a invasão.

Tribunais não têm equipamentos que possam identificar grampos

Nos Tribunais de Justiça e de Contas não há nenhum equipamento que identifique grampos telefônicos e também não são realizadas varreduras periódicas para verificar a existência deles. A professora de Arquitetura de Sistema da Informação do IFPB, Rafaelle Feliciano, trabalha com telefonia há 11 anos, considera a falta de varredura na rede telefona desses órgãos um erro que faz com que informações sigilosas discutidas por telefone fiquem desprotegidas e podem ser gravadas sem que se descubra o grampo a curto prazo.

A gerente de apoio operacional do TJPB, Valquíria Uchoa, disse que o órgão não dispõe de nenhum mecanismo para inibir e identificar grampos telefônicos nas dependências do tribunal. Ela revelou que este ano não foi realizada nenhuma varredura na central telefônica para identificar a existência de grampos.

Já a chefe do Centro de Processamento de Dados (CPD) do TCE, Gerluce Baracho, explicou que o Tribunal de Contas não costuma solicitar varreduras no sistema telefônico. Como nunca houve suspeita de escutas, o TCE nunca se preocupou com essa área. Segundo e ela, apenas, a empresa de telefonia realiza a manutenção regular.

Para Rafaelle Feliciano, o maior vilão dos grampos telefônicos são os próprios funcionários das operadoras de telefonia que tem acesso a muitas informações importantes. Ela explicou que os grampos podem ser feitos nos

telefones fixos e móveis, sendo que para conseguir fazer escutas telefônicas na rede móvel é necessário corromper alguém da operadora.

A professora destacou que a rede de telefonia fixa não oferece a mesma dificuldade e basta alguém ter acesso aos armários onde estão instaladas as centrais ou, no caso dos tribunais, ao PABX, tipo de central privada que controla vários ramais telefônicos. Eu não conheço nenhum mecanismo antigrampo, enfatizou a professora. Segundo ela, a melhor forma de se precaver é solicitar varreduras periódicas na central telefônica.

Acesso indevido à informação é crime

Qualquer acesso indevido a determinada informação é crime e o Ministério Público visa responsabilizar os autores desse crime. Quem garante é o promotor Octávio Paulo Neto. Ele explicou que qualquer investigação realizada por órgãos oficiais terá as conclusões encaminhadas ao MP, que poderá denunciar, arquivar ou solicitar novas diligências.

Segundo ele, o órgão pode acompanhar as investigações, bem como realizá-las e achando necessário, o Ministério Público pode até conduzir a investigação.

O promotor disse que todo órgão tem que ter na estrutura interna uma política de segurança. Ressaltou ainda que o grampo mostra a fragilidade da segurança da instituição que for vítima dele.

Otacílio Paulo Neto frisou que, com a evolução tecnológica, a questão da privacidade está cada vez mais comprometida. Para ele, a melhor forma de se proteger desse tipo de crime é por meio da conscientização da importância da prevenção da proteção de si e dos outros, mas as pessoas e os órgão não tem uma política de prevenção e só protegem depois que as coisas acontecem.

Ele destacou que o MPE é um dos poucos órgãos no país que tem um laboratório com equipamentos para investigar crimes virtuais. A internet como qualquer sistema deixa rastros e os equipamentos que temos ajuda a seguir esses rastros facilitando a localização do criminoso, destacou Otávio Paulo Neto.

O crime

Realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei é crime previsto na 9.296/69 que regulamenta o inciso XII do artigo 5º da Constituição Federal. A pena para

esse tipo de crime de dois a quatro anos de reclusa e multa.

Jornal Correio da Paraíba

Edição de domingo 28 de agosto de 2011

Reportagem Mislene Santos