TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

COMITÊ DE GOVERNANÇA DE TIC

REGISTRO SUMÁRIO DA 7ª REUNIÃO DE 2021

1. INFORMAÇÕES DA REUNIÃO

Data	**05/10/2021**	**Horário início**	**11h**	**Horário término**	**12:04h**
Tipo	Reunião do Comitê de Governança de TIC				
Local	SETIC				
Objetivo/Pauta	Relato acerca do ataque cibernético				

2. PARTICIPANTES

Nome	Cargo
Des. **CLÁUDIO ANTÔNIO CASSOU BARBOSA**	Presidente do Comitê de Governança de TIC, eleito pelo Tribunal Pleno
Desª. **DENISE PACHECO**	Eleita pelo Tribunal Pleno
Des. **MANUEL CID JARDON**	Eleito pelo Tribunal Pleno
Juiz **EDSON PECIS LERRER**	Juiz Diretor do Foro Porto Alegre
ADOLFO MARQUES PEREIRA	Representante da Secretaria-Geral da Presidência
Juiz **LEANDRO KREBS GONÇALVES**	Juiz Auxiliar da Corregedoria, representante da Secretaria da Corregedoria
BÁRBARA BURGARDT CASALETTI	Diretora-Geral
GERALDO CRUZ TEIXEIRA	Secretário-Geral Judiciário
NATACHA MORAES DE OLIVEIRA	Diretora da Secretaria de Tecnologia da Informação e Comunicações

3. PAUTA

3.1	Relato

A diretora da SETIC, Natacha, fez um breve relato sobre o incidente de segurança ocorrido no TRT e identificado em 30 de setembro de 2021, adiantando que o relatório contendo a análise detalhada dos eventos, bem como as ações tomadas para a contenção e reconstrução dos ambiente afetados está em elaboração pelas equipes da SETIC e da empresa especializada emergencialmente contratada para atuar no

evento.

Informou que a ferramenta de antivírus tradicional utilizada pelo TRT detectou possível atividade maliciosa por volta das 11h da manhã do dia 30/09/2021. Imediatamente após, iniciou-se a análise dos eventos apontados pelo sistema de segurança, bem como o trabalho para identificação e contenção do ataque que estava em curso.

A atuação das equipes da SETIC se deu de forma ininterrupta, tendo como principal preocupação garantir a integridade dos dados do Tribunal, especialmente aqueles vinculados aos processos judiciais. Após, a meta durante a contenção era manter os sistemas disponíveis para não trazer impacto à prestação jurisdicional e não acarretar problemas na realização da eleição para a nova Administração do TRT, que ocorreria na manhã do dia seguinte.

Na noite deste mesmo dia, quinta-feira, 30 de outubro, a situação demonstrou-se agravada na medida em que novos agentes maliciosos seguiam sendo identificados. Além disso, ficou evidente que as ferramentas que o Tribunal dispunha não estavam se mostrando suficientes para “enxergar” o que estava realmente ocorrendo e aplicar uma contenção efetiva. Como medida de emergência, a 1h do dia 01/11/2021, **Natacha** acionou empresa especializada em incidentes dessa natureza que, além de ter o conhecimento específico e a experiência com ataques cibernéticos, tivesse condições de aportar ferramentas mais apropriadas para análise e contenção do ataque. Destacou que a licitação para aquisição de antivírus de próxima geração estava em andamento, tendo sido remetida pela SETIC para a área competente no dia 25 de agosto de 2021. Infelizmente, o ataque ocorreu antes da aquisição e instalação do sistema mais moderno de antivírus.

O ataque foi totalmente contido às 6h da manhã de sexta-feira. Foi desligada parte da infraestrutura Microsoft, especificamente os servidores nos quais a ferramenta instalada pela empresa contratada identificou a presença de arquivos vinculados ao Ransomware. Por essa razão, a operação de sistemas como Espaço de Trabalho Remoto passou a se dar em contingência, o que acarretou lentidão no processo de autenticação nesse sistema. Considerando que o ambiente do ETR já tinha todos os usuários cadastrados e aplicações de sistemas legados disponíveis, optou-se pelo desligamento do serviço do Gabinete Virtual, que também apresentou comprometimento de segurança.

A equipe da SETIC reagiu a tempo de conter os comandos de criptografia que seriam executados na sequência da instalação dos agentes identificados e acionou os procedimentos definidos previamente para a continuidade operacional do Tribunal em caso de ataque cibernético.

O trabalho das equipes de infraestrutura tecnológica e de segurança da informação seguiram ininterruptamente até o final do dia 01/11/2021. A partir do dia 02/11, o trabalho de reconstrução da infraestrutura afetada passou a ser realizado entre 8h e 22h, de modo a garantir que a equipe tivesse seus momentos de descanso e pudesse contribuir da melhor forma nas tarefas que precisavam ser realizadas.

Natacha ressaltou que a equipe de monitoração de infraestrutura e segurança da informação precisa ser urgentemente incrementada, conforme já informado em diversas reuniões e em processos administrativos que tramitam no TRT há mais tempo. O ambiente computacional atual é grande, altamente complexo e em constante mutação em decorrência da instalação contínua de novos sistemas definidos pelo CNJ, CSJT e mesmo pelo TRT. Com um número grande de serviços baseados em TI, muitos servidores e aplicações precisam ser monitorados e atualizados praticamente todos os dias, o que é inviável com o número de

servidores disponíveis atualmente e com a alta rotatividade presente na SETIC.

A reação ao incidente foi considerada um sucesso e demonstrou que a SETIC tinha processos definidos para a continuidade dos serviços de TI considerados críticos. Inclusive as ferramentas que estavam em processo de contratação são da mesma família daquelas utilizadas pela empresa que atuou na contenção, o que indica a decisão acertada em realizar tal contratação, que diferiu da decisão tomada pelos demais TRTs, que estão em processo de aquisição de antivírus tradicional. Natacha fez um agradecimento ao Diretor da SLC, João Henrique Ribas, que de imediato agilizou o processo de contratação.

O público em geral não foi afetado, de forma que a imagem do Tribunal perante a sociedade ficou preservada. Salientou que recebeu inúmeras mensagens de advogados representantes da OAB, parabenizando pela transparência com que o TRT tratou o assunto na medida em que os serviços não foram afetados.

O trabalho segue nas salas de guerra, reagindo ao incidente, assim como as demais atividades rotineiras da SETIC de forma a manter o TRT atuando em todas as suas áreas. Reitera que o sigilo com que o assunto foi tratado nas primeiras 24h foi fundamental para que as equipes e gestores se mantivessem concentrados e sem interrupções, tendo sido acionado apenas o Comitê Permanente de Crises Cibernéticas do TRT

Agradecimentos feitos também ao coordenador de segurança institucional do TRT, João Peixoto, que atuou na logística de transporte dos equipamentos envolvidos. Relatou, ainda, que foi necessário acionar o Diretor a VT de Santo Ângelo, local onde foi identificada máquina suspeita, o qual prontamente fez o encaminhamento do equipamento no domingo à noite.

No momento, a área que está sofrendo com os efeitos do ataque é a infraestrutura da SETIC, que segue atuando na reconstrução do ambiente até que se tenha certeza de estar livre de qualquer malware.

Des. Cassou declarou que as informações prestadas confirmam que o TRT4 estava preparado para reagir ao ataque, tratado com muita competência por todos os envolvidos. Parabenizou toda a equipe da SETIC e entende como prioridade fazer as contratações necessárias para aumentar a segurança do ambiente tecnológico.

A Diretora Geral Bárbara parabenizou a Setic por ter sido incansável na atuação relacionada ao incidente e colocou a área administrativa à disposição no que for necessário, ressaltando que as contratações envolvidas estão sendo tratadas com prioridade total pelo Diretor da SLC. Ressaltou que o trabalho de migração da folha de pagamento para o SIGEP foi impactado no sentido de ter ficado mais lento mas que porém o pagamento da folha está garantido, ainda que seja pelo sistema legado, caso necessário.

Desa. Denise solidarizou-se ao Des. Cassou nos cumprimentos à equipe pela dedicação e comprometimento no tratamento do incidente e relembrou que muitas das reuniões do comitê ao longo desta gestão, foram dedicadas a questões de cuidados com a rede e aumento de segurança da informação, o que dá a ela muita satisfação por estar em um Tribunal que tem essa preocupação e compreensão de todas as áreas envolvidas com os cuidados para com a área de Tecnologia, que cada vez mais vem se tornando área fim.

Natacha informou ainda, que o TST sinalizou que irá custear o serviço de aumento de segurança, que está sendo licitado no TRT4, para todos os TRTs.

O Diretor da Segjud, Geraldo ressaltou que o TRT está trabalhando em um plano para atendimento de medidas urgentes em caso de necessidade de desconexão total dos serviços.

Des. Jardon enalteceu também a atuação da SETIC, seguido pelo Juiz Edson, que transmitiu os

cumprimentos a toda a equipe e agradavelmente comparou o relato da diretora da SETIC ao enredo de um filme, tamanha a complexidade, agilidade e seriedade com que foi tratado.

Reunião encerrada às 12:04h