ANEEL
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA

Documento de Oficialização da Demanda (DOD) nº 019/2020-SGI/ANEEL.

1. Identificação da Área Requisitante da solução

Unidade/Setor: SGI/Núcleo de Segurança da Informação	Data: 10/08/2020
Responsável pela Demanda: Igo Rodrigues de Castro	SIAPE do Responsável: 1912777
E-mail do Responsável: igocastro@aneel.gov.br	Telefone do Responsável: 2192-8671
Integrante Requisitante: Issao Hirata	
E-mail do Integrante Requisitante: issaohirata@aneel.gov.br	Telefone do Integrante Requisitante: 2192-8008

2. Identificação da Demanda

Contratação de solução de contingência isolada de cópias de segurança contra ataques cibernéticos (ransomwares)

3. Alinhamento Estratégico

Id	Objetivo Estratégico (PEI/PETI - ANEEL e EGD)	Id	Alinhamento com o PDTI/PTD - ANEEL
OE15	Modernizar a infraestrutura e soluções de tecnologia da informação	OETI11	Desenvolver a segurança da informação em nível corporativo (PDTI/PTD - 2018/2021)
OETI10	Avançar na modernização da infraestrutura de TI		
OE11	Garantia da segurança das plataformas de governo digital e de missão crítica (EGD 2020/2022)	IETI11.1	Estabelecer diretrizes institucionais para a segurança da informação (PDTI/PTD-2018/2021)

4. Fontes de Recurso

Programa: Gestão e Manutenção do Ministério de Minas e Energia
Ação: Administração da Unidade
Item: Contratação de solução de contingência isolada de cópias de segurança

5. Motivação/Justificativa

ANEEL
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA

A ocorrência de ataques cibernéticos contra diversas organizações públicas e privadas nacionais e internacionais vem se intensificando nos últimos anos. A alta rentabilidade do crime cibernético acompanhada pela dificuldade da identificação de seus autores e a digitalização das operações torna o risco cibernético cada vez mais relevante para as organizações.

Nesse sentido, o panorama atual de ameaças cibernéticas apresentou um expressivo aumento do número de ataques cibernéticos a organizações tendo como uma das principais causas o teletrabalho adotado em larga escala como medida rápida e emergencial de proteção à vida de seus colaboradores e em resposta às restrições de isolamento social estabelecidas pelos governantes como estratégia de combate à pandemia de COVID19.

Uma vez que as organizações não se encontravam preparadas para a utilização em massa dessa modalidade de trabalho, que se caracteriza por sua realização fora das dependências da organização e, com isso, altamente dependente de tecnologia, os riscos de segurança cibernética à ela associados que eram até então controlados foram, desse modo, alavancados, uma vez que os sistemas de acesso remoto das organizações não possuem todos os recursos de segurança e os acessos remotos dos colaboradores aos sistemas corporativos são em sua maioria realizados por meio de computadores, redes wi-fi, modems de internet e dispositivos móveis pessoais que, além de estarem fora do alcance das soluções de segurança da informação corporativas, também não possuem um nível de proteção adequado (inexistência de antivírus, uso de credenciais administrativas com privilégios de instalação, aplicativos inseguros instalados, navegação na web insegura, uso de senhas padrão, entre outros).

Com isso, criou-se um ecossistema farto de vulnerabilidades às redes corporativas que podem ser facilmente exploradas por criminosos cibernéticos visando desde o furto de informações e vazamento de dados ao sequestro digital de dados corporativos, esta última merecendo, pois é atualmente considerada a ameaça de maior risco e impacto à continuidade e sobrevivência dos negócios das organizações, mais conhecido como “ransomware”.

Os “ransomwares” são uma categoria de software malicioso (malwares) que ao serem inseridos e instalados por criminosos virtuais no ambiente computacional das organizações se proliferam pela sua rede corporativa e criptografam todos os arquivos de dados contidos nos discos das estações de trabalho e equipamentos servidores físicos e virtuais (hard disks), sistemas de armazenamento de arquivos corporativos (servidores de arquivos), sistemas de bancos de dados, sistemas de backup e demais repositórios de arquivos existentes na infraestrutura computacional, inclusive aqueles que estejam eventualmente sincronizados em nuvem com a rede corporativa da organização.

Os arquivos corporativos, ao serem criptografados pelo “ransomware”, são impossibilitados de serem abertos ou lidos pelos colaboradores e pelos demais sistemas internos da organização comprometendo-se imediatamente a disponibilidade dos recursos computacionais e das informações necessárias ao trabalho dos colaboradores. Ao final do processo de criptografia dos dados, o malware disponibiliza um comunicado na tela das estações e dos sistemas atingidos informando a necessidade de pagamento de um resgate ao atacante, em criptomoedas, para obtenção da chave de descriptografia que reverte todo o processo.

Tal cenário caótico foi vivido recentemente por várias empresas internacionais (HONDA, HYDRO, GARMIN, CANON, JOHANNESBURG CITY POWER, TELECOM ARGENTINA) e sobretudo por algumas grandes empresas brasileiras do Setor Elétrico, públicas e privadas, onde o valor monetário do resgate estabelecido pelos criminosos foi da ordem inicial de sete a oito milhões de dólares. Em alguns casos, o valor do resgate era aumentado exponencialmente em menos de vinte e quatro horas. Essas empresas, ao optarem pela sensata decisão de não pagarem o resgate, pois o pagamento não garante que os criminosos disponibilizarão a chave de

descriptografia nem tampouco se deve alimentar tais crimes, várias dessas empresas brasileiras sofreram paralização de atividades administrativas por vários dias enquanto recuperavam seus dados e sistemas por meio da restauração de cópias de segurança realizadas em mídias externas (fitas) num processo manual, iterativo, demorado, custoso financeiramente e extremamente laborioso, uma vez que os dados guardados nos sistemas de armazenamento do backup corporativo também foram atingidos. Durante esse processo, dados críticos recentes normalmente são perdidos em definitivo por não estarem ainda armazenados em fitas mas depositados nesses sistemas de backup padrão que não possuem recursos de segurança contra este tipo de ataque.

Não obstante à existência de diversas soluções de segurança cibernética empregadas na proteção do ambiente computacional das organizações, os ataques de "ransomwares" são normalmente efetuados por criminosos virtuais ou grupos organizados especializados que empregam modernas técnicas, táticas e procedimentos de ataques planejados que não são, em virtude disso, facilmente detectados e alertados pelos mecanismos de proteções dessas soluções, tais como firewalls, antispam e antivírus.

Em função disso, na 3ª Reunião Ordinária do Comitê de Gestão da Informação da ANEEL ocorrida no dia 15 de julho de 2020, foi apresentado o panorama de ameaças em questão e as ações de segurança cibernética em andamento para reforço da proteção do ambiente computacional da Agência, entre elas, a proposição de contratação de solução de backup seguro contra ataques de "ransomwares" (cyberrecovery).

Portanto, diante desse contexto de aumento de ataques cibernéticos ao Setor Elétrico pelo qual a ANEEL está inserida e as graves consequências que eles podem trazer à integridade e disponibilidade de suas informações verificou-se a necessidade de contratação de solução de TI específica para proteção de cópias de segurança dos dados mais críticos da Agência, sobretudo contra ataques virtuais do tipo "ransomwares", visando evitar em caso de concretização, a perda definitiva desses dados e permitir a recuperação dos mesmos em menor custo, tempo e esforço, garantindo-se a continuidade das atividades e o cumprimento da Missão da Agência.

6. Resultados a serem alcançados com a contratação

- Prevenir contra a perda definitiva de dados críticos da ANEEL mediante a ocorrência de ataques cibernéticos complexos do tipo "ransomwares" e que podem causar a disrupção de suas operações;
- Prover a recuperação dos dados críticos da Agência em caso de ataque cibernético que cause indisponibilidade de dados dispostos na solução de backup corporativa menor tempo e custo, minimizando prejuízos nas suas atividades;
- Melhorar a qualidade dos backups de dados críticos da ANEEL minimizando a possibilidade da realização de cópias de segurança corrompidas ou criptografadas;
- Possibilitar a identificação mais rápida de eventuais ataques cibernéticos nos dados críticos da Agência (em alguns casos de ataques de "ransomware" ocorridos no Setor Elétrico a detecção do incidente levou alguns dias, aumentando os impactos);
- Prover garantia de integridade e disponibilidade das informações críticas da Agência em caso de ataque cibernético onde os dados dispostos na solução de backup atual tenham sido bloqueados ou criptografados;
- Prover resiliência cibernética às operações críticas da ANEEL mediante a ocorrência de ataques

ANEEL
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA

virtuais que podem paralisar as atividades e acesso aos dados da Agência;

- Minimizar os riscos operacionais de segurança da informação que possuem elevada motricidade com operações estratégias da Agência (risco cibernético);

- Contribuir para o cumprimento da Política de Segurança da Informação da Agência (Norma de Organização da ANEEL nº 012), sobretudo no que diz respeito à garantia de disponibilidade das informações da Agência.

Em conformidade com o art. 10°, § 2º da Instrução Normativa n°1, de 4 de abril de 2019, emitida pela Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo, encaminha-se ao Superintendente de Gestão Técnica da Informação, Issao Hirata, para providências.

Issao Hirata
Secretário-Geral do Comitê de Gestão da Informação da ANEEL
Integrante Requisitante

Brasília, 10 de agosto de 2020.