PODER JUDICIÁRIO DO ESTADO DO ESPÍRITO SANTO - PJES

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

FORMULÁRIO I - NP 09 - DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA PARA CONTRATAÇÃO DE TECNOLOGIA DA INFORMAÇÃO

Oficialização da Demanda para Contratação Nº 16/2024 - SECRETARIA DE TECNOLOGIA DA INFORMACAO

Em 16 de julho de 2024.

1 - DESCRIÇÃO DA SOLUÇÃO

Contratação de licença de subscrição de software de proteção contra ameaças avançadas (NGAV) baseada em agente com funcionalidade de EDR (“Endpoint Detection and Response”)

2 - IDENTIFICAÇÃO DA ÁREA DEMANDANTE DA SOLUÇÃO:

Secretaria/Coordenação/Seção:	Secretaria de Tecnologia da Informação / Coordenação de Suporte e Manutenção / Seção de Segurança da Informação		
Nome do Projeto:			
Responsável pela Demanda:	Havirdan das Rodor Araújo	Matrícula:	20974531
E-mail do responsável pela demanda:	hdaraujo@tjes.jus.br	Telefone:	(27) 3357-4511

3 - NECESSIDADE E MOTIVAÇÃO DA CONTRATAÇÃO:

Em novembro de 2020, os poderes executivo e judiciário brasileiro foram alvo de invasões hackers, conforme se observa:

Desde terça-feira, 5, importantes órgãos dos Poderes Executivo e Judiciário foram invadidos por cibercriminosos. Inicialmente, imaginava-se que somente o Superior Tribunal de Justiça (STJ) tivesse sido atacado e tido as informações roubadas. Contudo, outras bases de dados foram atacadas. Não se sabe ainda se o hackeamento foi orquestrado ou não. Porém, os sistemas do Datasus, do Ministério da Saúde, e do Governo do Distrito Federal (GDF) estão fora do ar e o motivo disso está sendo relacionado ao ciberataque. Alguns sistemas da Receita Federal também foram alvo da ação. Há risco de se perder as informações. Segundo especialistas em segurança cibernética consultados pelo Radar Econômico, este foi o maior ataque cibernético já sofrido pelo governo brasileiro em termos de impacto.
A Polícia Federal iniciou uma investigação e órgãos de tecnologia estão tentando resgatar os dados que estão criptografados. Contudo, não se sabe a possibilidade de reavê-los. “Existem técnicas para reverter criptografia. A depender da complexidade do algoritmo e do tamanho da chave da criptografia utilizada, podem colocar um computador por 200 anos calculando e não se consegue abrir. Mas, caso seja algo menos sofisticado, é possível reverter a situação”, afirma Marco Zanini, CEO da Dinamo Networks, que atua na segurança criptográfica do sistema PIX, do Banco Central.
Os supostos hackers fizeram um pedido de resgate pelas informações do STJ. O Tribunal, inclusive, suspendeu todos os prazos, de todos os processos, e está com uma página de emergência indicando que está apenas analisando pedidos urgentes. “É como se as bases de dados do STJ pudessem ser colocadas dentro de um incinerador”, diz Marta Schuh, diretora de seguro cibernético da corretora internacional Marsh.
Esse tipo de ataque não é incomum. Grandes empresas recebem às centenas diariamente. O que chama atenção é a forma orquestrada com que vários órgãos do federais foram atacados de uma só vez. Com exceção do STJ, os outros órgãos, Ministério da Saúde e GDF não confirmam que informações foram capturadas. E, diferentemente do que aconteceu com o Tribunal, não há ainda um pedido de resgate evidente. Os órgãos, ao que consta, segundo fontes da Polícia Federal, foram alvos de um ataque por meio de Ransomware. Esse tipo de crime é quando o hacker sequestra as informações que obteve acesso a partir da quebra da segurança virtual por meio de alguém hackeado — sendo esta pessoa, um alto executivo, servidor ou até mesmo um ministro de Estado. A partir disso, ele criptografa as informações e pede um resgate para liberá-las. “Como os hackers estão com acesso a dados do Tribunal, ninguém sabe o que pode ser feito com isso”, diz Marcos Camargo, presidente da Associação dos Peritos Criminais da Polícia Federal. “O que diminui um pouco a preocupação, é que, via de regra, fazem isso apenas com objetivo financeiro.”
Fonte:https://veja.abril.com.br/coluna/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia.

Em abril de 2021, o Tribunal de Justiça do Rio Grande do Sul foi alvo de ataque hacker, conforme se observa:

O Tribunal de Justiça do Rio Grande do Sul informou, nesta quinta-feira (29), que enfrenta instabilidade nos sistemas de informática por causa de um ataque cibernético. A Polícia Civil vai investigar o caso.

De acordo com o desembargador Antonio Vinicius Amaro da Silveira, do Conselho de Comunicação do TJ, o Tribunal percebeu que o sistema havia sido invadido na madrugada de quarta (28) quando o e-mail e o site saíram do ar.

"A questão é muito grave. Nós nunca enfrentamos esse tipo de problema, nessa dimensão. Os sistemas foram invadidos e arquivos corrompidos e nós estamos ainda sob ataque, permanecemos sob ataque. Não temos segurança ainda para dizer quando podemos retomar a operação dos sistemas de forma normal".

No início da noite desta quinta, apenas o sistema Eproc, para consulta de processos, estava funcionando pela rede externa do Tribunal.

O desembargador confirmou que se trata de um ataque de ransomware, um programa que se infiltra no computador de forma ilícita.

"O ransomware é um malware de extorsão que pode bloquear o sistema operacional ou criptografar arquivos e exigir um resgate para desbloquear os arquivos. A prevenção é feita com um bom antimalware, backups, e conscientização", explica o especialista em crimes cibernéticos José Milagre, presidente do Instituto de Defesa do Cidadão na Internet.

Para Milagre, o software percorre o sistema e criptografa [codifica] os arquivos. Caso existam serviços disponíveis no equipamento, eles são paralisados e, em algumas vezes, o programa pode renomear os arquivos com uma extensão codificada.

Fonte:https://g1.globo.com/rs/rio-grande-do-sul/noticia/2021/04/29/tj-rs-diz-que-sistema-de-informatica-do-tribunal-foi-alvo-de-ataque-hacker-e-muito-grave.ghtml

Em notícia, a Watch Guard, conforme estudo da Cybersecurity Ventures, relata que “houve um ataque cibernético a cada 39 segundos em 2023”, conforme se observa:

Os ataques cibernéticos continuam a ser motivo de preocupação para as empresas. Embora tenham sido feitos grandes progressos para combater este problema, a capacidade de adaptação dos agentes da ameaça, combinada com outros fatores, como o aumento do trabalho remoto ou o aumento do número de dispositivos com acesso à Internet, significa que o cibercrime persiste. De acordo com um estudo da Cybersecurity Ventures, um ataque cibernético ocorreu a cada 39 segundos em 2023, o que se traduz em mais de 2.200 casos por dia. Isto contrasta com os dados de 2022, quando ocorreu um incidente a cada 44 segundos. Esta taxa de ataque mais rápida preocupa os profissionais da indústria, que enfrentam ameaças cada vez mais

sofisticadas, concebidas para contornar os protocolos de segurança cibernética. É importante que as organizações estejam cientes dos tipos de ataques cibernéticos atualmente no radar dos profissionais de segurança cibernética para que possam adaptar os seus protocolos para lidar com essas ameaças de forma mais eficaz.

O ano de 2023 foi marcado por três modalidades de ataque que se tornaram prioridade para as equipes de segurança cibernética. Avaliamos abaixo sua evolução nos últimos meses.

Ataques de malware: Este é o termo usado para se referir a software malicioso. Os agentes de ameaças usam malware para invadir, danificar ou desabilitar computadores, sistemas de computador, redes e dispositivos, muitas vezes assumindo o controle de algumas das operações do sistema. Dentro da família dos malwares, existem diferentes tipos de ataques que comprometem a segurança e os sistemas internos das empresas. Foi uma das maiores ameaças em 2023 e há 1 bilhão de malwares ativos atualmente.

Ataques de ransomware: Esta é uma forma de software malicioso usado para criptografar arquivos ou bloquear o acesso a um sistema ou dispositivo. O ransomware geralmente afeta todos os tipos de organizações, independentemente do tamanho, mas, principalmente, aquelas que usam e armazenam informações críticas. Depois que seu software malicioso é instalado, os cibercriminosos exigem um resgate de suas vítimas em troca do desbloqueio do acesso ao sistema. De acordo com nosso e-book Escape the ransomware maze, os ataques de ransomware foram a principal ameaça em 2023, mostrando um aumento de 95% ano a ano em termos de frequência.

Ataques de phishing: Esta é a forma de ataque mais conhecida, pois afeta o usuário final e tende a impactar nossas atividades diárias. Apesar da maior consciência desta ameaça, surgiram novas modalidades nos últimos meses que continuam a fazer do phishing um dos problemas mais comuns. Graças às tecnologias recentes e ao uso da inteligência artificial, os cibercriminosos conseguiram aperfeiçoar suas técnicas simulando a voz de conhecidos por meio de vishing ou lançando ataques smishing realizados por SMS ou WhatsApp.

Fonte:https://www.watchguard.com/wgrd-news/blog/there-was-cyberattack-every-39-seconds-2023

Como pode-se verificar, os ataques hackers são recorrentes. As formas utilizadas pelos hackers vão evoluindo para conseguir transpassar as barreiras e com isso é necessário o desenvolvimento de novas técnicas de prevenção e combate.

Atualmente, as estações de trabalho do PJES são protegidas por soluções da Symantec, cuja aquisição ocorrera por meio do Processo nº 2010.00.276.988, e tem o Contrato nº CF007/2019 - Processo 7001192-83.2019.8.08.0000, cuja validade se encerrou em 08-02-2023, tendo sido realizada uma renovação emergencial pelo período de 1 ano, com validade até 08-02-2024.

Desta forma, para manter o parque tecnológico do PJES atualizado e protegido contra novas ameaças provocadas pelos milhares de vírus já existentes, e pelos que surgem todos os meses, assim como combater as ameaças com novas estratégias de segurança, garantir sua perfeita operacionalização, assegurar a continuidade dos serviços prestados pela STI, a rápida resolução de eventuais problemas e a maximização da segurança do ambiente computacional do PJES, é necessária a realização de novo procedimento licitatório, visando a contratação de solução de proteção de endpoint que inclua novas técnicas e ferramentas de combate a ameaças pois o contrato atual encerra sua vigência em 08/02/2024.

4 - RESULTADOS A SEREM ALCANÇADOS COM A SOLUÇÃO:

Além da segurança de toda a rede do PJES, a contratação do serviço de suporte proporcionará:

- **Minimizar os riscos causados por desatualização de programas de computador e/ou não evolução desses e pela ausência de canal de suporte para solução de problemas.**
- **Proteção das estações de trabalho e da infraestrutura tecnológica do PJES;**
- **Proteção contra vazamento de informações, sigilosas ou não;**
- **Redução dos riscos de ataques aos sistemas;**
- **Resolução de problemas de gerência ou configuração.**

5 - PROJETOS RELACIONADOS:

Existe algum projeto em andamento relacionado a esta contratação?

[X] Não.

[ ] Sim. Qual?

6 - ALINHAMENTO ESTRATÉGICO:

A contratação está alinhada a qual objetivo do planejamento estratégico institucional/ tecnologia da informação e a qual indicador?

[ ] Elevar a produtividade do Poder Judiciário

[ ] Gerenciar as demandas repetitivas de grandes litigantes

[ ] Implantar a governança de TI

[ ] Implantar a gestão de custos

[ ] Otimizar e incrementar as possibilidades de acesso à justiça

[x] Assegurar sistemas e infraestrutura de TI adequados

[ ] Gerenciar e adequar recursos tecnológicos de forma a maximizar sua utilização para uma melhor produtividade

[ ] Implantar o Gerenciamento de Processos
[ ] Implantar o Gerenciamento de Projetos
[ ] Implantar o Gerenciamento de Serviços de TI
[ ] Contratar o serviço de suporte técnico – Service Desk
[ ] Implantar o Gerenciamento de Segurança da Informação
[ ] Reestruturar a STI – Recursos humanos e Estrutura organizacional
[ ] Implantar um sistema informatizado de Gestão de Custos
[ ] Estruturar e unificar o sistema virtual de acesso à justiça
[x] Atualizar o parque tecnológico
[ ] Implantar projeto Datacenter backup visando a Gestão de Continuidade de Negócio
[ ] Adquirir e Implantar um Sistema Integrado de Gestão Administrativa
[ ] Convergir e integrar os sistemas legados
[ ] Implantar o Processo Judicial Eletrônico
[ ] Implantar sistema de diárias e suprimento de fundos
[ ] Integração dos sistemas de folha de pagamento, almoxarifado, patrimônio e contábil
[ ] Melhoria do sistema de controle de contratos e inclusão do controle de convênios e termos congêneres

7 – FONTE DE RECURSOS

Fonte de Recursos	Elemento(s) de Despesa
[x] FUNEPJ – Fundo Especial do Poder Judiciário	

[ ] TJES	3.3.90.40.08

8 - EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Integrante Demandante:	Havirdan das Rodor Araújo	**Matrícula:**	209.745-31
E-mail do Integrante Demandante:	hdaraujo@tjes.jus.br	**Telefone:**	(27) 3357-4511
Integrante Técnico:	Pedro Luiz Chacur Seixas	**Matrícula:**	209.932-24
E-mail do Integrante Técnico:	plseixas@tjes.jus.br	**Telefone:**	(27) 3357-4038
Integrante Administrativo	Vinícius Milere Moreira	**Matrícula:**	209.614-44
E-mail do Integrante Administrativo:	vmmoreira@tjes.jus.br	**Telefone:**	(27) 3357-4513

ENCAMINHAMENTO

Diante de tais informações, **encaminhem-se os autos à Secretaria Geral,** a fim de que seja instituída a Equipe de Planejamento da Contratação, conforme indicação no item anterior.

Respeitosamente,

Secretário(a) da área demandante.

Assina neste documento o Secretário da área demandante, conforme descrito no FORMULÁRIO I da NP 09.

Documento assinado eletronicamente por **MARCIANNE RIBEIRO ANTUNES LIMA**, **SECRETARIO DE TECNOLOGIA DA INFORMACAO**, em 19/07/2024, às 18:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sistemas.tjes.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2185951** e o código CRC **A83F7FED**.

7006039-55.2024.8.08.0000 2185951v11