Parecer de Segurança da Informação sobre:
Implicações de segurança da informação pela publicação de informações técnicas sobre a infraestrutura de TIC do TJPE

Este parecer pode ser utilizado para subsidiar a gestão do TJPE com informações técnicas sobre implicações de segurança da informação em qualquer caso onde pretenda-se publicar ou, por qualquer razão, já tenham sido publicadas informações sobre a infraestrutura de TIC do TJPE. A motivação para confecção deste parecer baseou-se na identificação pela SETIC/TJPE de informações sobre a infraestrutura de TIC do TJPE publicada no site do CNJ por meio do relatório Auto Circunstanciado de Inspeção no Tribunal de Pernambuco (Processo de Inspeção n. 0001794-22.2019.2.00.0000). O arquivo PDF com data de geração de 21/06/2019 está disponível publicamente no link abaixo:

- http://www.cnj.jus.br/corregedoriacnj/inspecoes-correicoes/relatorios/category/210-tribunal-de-justica-do-estado-do-pernambuco?download=3573:auto-circunstanciado-de-inspecao-no-tjpe-2019

Contexto

Todos os sistemas e informações mantidos pelo Tribunal de Justiça de Pernambuco que suportam, direta ou indiretamente, as prestações dos serviços jurisdicionais, funcionam sobre uma infraestrutura de Tecnologia da Informação e Comunicação (TIC), que é mantida pela Secretaria de Tecnologia da Informação e Comunicação (SETIC). Esta infraestrutura é composta por elementos de software e hardware. São elementos de software: sistemas operacionais, sistemas servidores de aplicações, aplicações, sistemas gerenciadores de bancos de dados. Roteadores, switches, computadores e impressoras são exemplos de elementos de hardware. É preciso esforço de planejamento, modelagem e de organização para que os mais variados elementos trabalhem em conjunto, entregando serviços de TIC com qualidade e segurança. Esta organização em inúmeras situações precisa ser documentada, de forma textual e/ou gráfica, para que o conhecimento não seja perdido e que a infraestrutura seja mantida e melhorada.

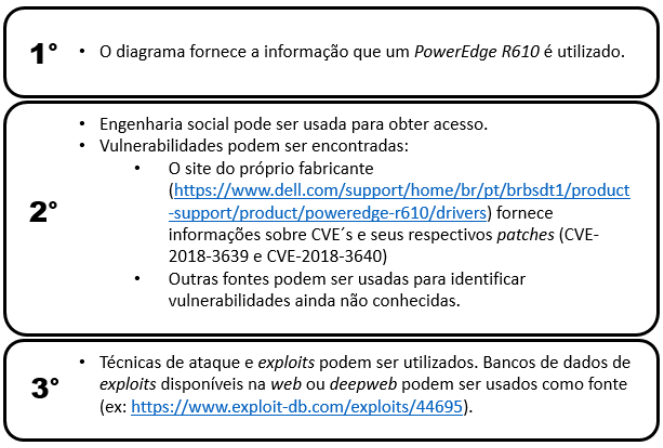
Sob a ótica da segurança da informação, a documentação da infraestrutura também é muito útil internamente, pois, por exemplo, pode possibilitar mais assertividade na implementação de camadas de segurança e reações mais precisas e rápidas em casos de incidente. Entretanto, a divulgação pública de detalhes da infraestrutura de TIC pode facilitar a ocorrência de incidentes de segurança, bastando que para isso caiam nas mãos de indivíduos mal intencionados. Por exemplo, com um diagrama da rede de uma infraestrutura contendo algumas características dos seus elementos é possível planejar e executar mais facilmente ataques de interrupção de serviços ou de outra natureza. Pode-se, por meio das informações divulgadas, tomar como base a capacidade de processamento, armazenamento e tráfego dos elementos envolvidos, características específicas de fornecedores, vulnerabilidades já conhecidas e desconhecidas pelo mercado e facilitar o uso de técnicas de engenharia social para obtenção de mais informações ou até mesmo acesso indevido. Portanto, algumas informações por si só não implicam automaticamente em uma invasão ou comprometimento de ambiente, mas servem muito bem para diminuir drasticamente os esforços de atacantes.

Há ainda outros tipos de informação que não servem para facilitar um ataque, mas podem servir para instigar ataques. Por exemplo, a confirmação da existência um determinado dado ou informação cujo valor é relevante para um atacante, ou ainda informações sobre disponibilidade de recursos na infraestrutura (espaço para armazenamento ou capacidade de processamento e memória disponíveis).

Posicionamento Técnico

A exploração de aspectos técnicos, eventualmente tornados públicos, pode ocorrer de muitas formas. Tomando como exemplo a divulgação de informações sobre disponibilidade de recursos de processamento e armazenamento e ainda um diagrama de redes de um *datacenter* com informações sobre a distribuição e comunicação entre os elementos, bem como seus respectivos fornecedores e/ou modelos:

- Instiga atacantes pelas informações de disponibilidade de recursos, como capacidade de processamento e armazenamento, que podem servir de atrativo para indivíduos com propósitos específicos. Nos casos de atacantes que buscam espaço de armazenamento em infraestruturas de terceiros os propósitos mais comuns são para a hospedagem de conteúdo pirata e/ou adulto e para distribuição de imagens de pedofilia. No caso de roubo de processamento, atualmente uma finalidade muito comum é a utilização dos processadores "tomados" para mineração de criptomoedas. Saber que existe processamento ocioso disponível no ambiente da vítima torna o cenário ainda mais atraente, pois pode indicar menor chance de detecção do processamento adicional.
- Permite inferir com maior facilidade e precisão onde podem estar os alvos (servidores, dados, serviços, etc.) que se quer obter acesso ou tornar indisponível. Com o desenho da rede, o número de possibilidades torna-se menor, portanto, mais fácil de testar e identificar.
- Facilita o entendimento sobre os caminhos que se deve tentar percorrer e os que se deve evitar para atingir determinados alvos. Identificando onde podem estar as ferramentas de segurança (IPS, firewall, etc.) e as conexões entre os elementos é possível tentar formas de evitar determinados elementos ou testar a existência de possíveis camadas adicionais de proteção (inspeção TLS, IPS, etc.)
- Depois de traçada uma estratégia, conhecendo o fornecedor e/ou modelo de um ou mais elementos, é possível tentar descobrir vulnerabilidades, conhecidas ou desconhecidas pelos fabricantes do equipamento e fornecedores de soluções de segurança. Uma vulnerabilidade conhecida é catalogada como uma CVE - *Common Vulnerabilities and Exposures* e pode ser encontrada em sítios de fácil acesso na Internet (ex.: https://cve.mitre.org/). Depois de identificar uma vulnerabilidade é possível recorrer aos *exploits* (kits de invasão) disponíveis na *web* ou *deepweb*, desenvolver um *exploit* ou ainda aplicar técnicas de invasão para tentar explorar a vulnerabilidade. Considerando que existem vulnerabilidades ainda desconhecidas pelos próprios fabricantes e que na prática é inviável manter um ambiente amplo e complexo de TIC completamente atualizado com todos os últimos patches de segurança lançados (para *softwares* e *firmwares*), existirão janelas abertas. A figura abaixo apenas ilustra com um exemplo hipotético passos comumente seguidos por indivíduos que buscam explorar vulnerabilidades em um ambiente de TIC usando informações para as quais tiveram o acesso facilitado:



Conclusão

Considerado o exposto, o Núcleo de Gestão de Segurança da Informação entende que antes de tornarem-se públicos detalhes técnicos sobre a infraestrutura de TIC do Tribunal de Justiça de Pernambuco, é imprescindível analisar as informações sob a ótica da segurança da informação. Deve-se sempre buscar o caminho da publicidade, mas preservando a sensibilidade e o sigilo de informações que, se divulgadas, podem inclusive implicar em danos a prestação dos serviços jurisdicionais. A publicação de informações cuja natureza seja a mesma das ilustradas neste parecer claramente implica em riscos razoáveis de segurança da informação.

Recife - 12/07/2019

Poder Judiciário de Pernambuco
NGSI/AGTIC/SETIC/TJPE