Consulta Pública 001/2020.

Qui, 02/07/2020 09:49

Para: NULIT-TRF1-Núcleo de Licitações <nulit@trf1.jus.br>

Prezada Elizete, bom dia.

Gostaria de saber se ainda posso contribuir com mais uma sugestão para esta Consulta Pública. Percebi um item que para ser aceito, depende do entendimento da equipe técnica, portanto, poderia ser mais abrangente para se evitar possíveis impugnações e questionamentos.

Caso possível, segue nossa sugestão abaixo, caso não seja mais possível, peço desculpas pelo incoveniente.

Item 2.51
Item 4.53
Ambos os Itens mencionam a funcionalidade WIPS (Wireless Intrusion Prevention System) ou Sistema de Prevenção de Instrusão. Esta não é uma funcionalidade específica padrão para todos os fabricantes, e depende de entendimento para seu aceite, por isso acreditamos que os textos de tais Itens possam ser mais abrangentes. Na verdade, o WIPS é a nomenclatura dada para um conjunto de recursos que tem a capacidade de tomar algum tipo de ação, como, por exemplo, bloquear ataques de IP Spoofing, ataque SMURF e de ataque por IPs fragmentados, bloqueios de dispositivos por Mac Address ou IP, bloqueios por listas de acesso, etc. Não são todos os fabricantes que dedicam um capítulo para o tema WIPS em suas documentações, mas possuem descrições sobre as funcionalidades de WIPS disponíveis em seus equipamentos. Podemos entender que o equipamento pode sim possuir uma tela que concentre os recursos de WIPS mas que, também, outros equipamentos possuem tais recursos em telas separadas. É o caso do Firewall L2 e L3 por exemplo. Ele pode realizar recursos de WIPS que realizam os bloqueios de proteções mencionados acima.

Outra conclusão que tiramos sobre o WIPS é que, normalmente, as redes de WIFI já possuem uma segmentação vinda diretamente do Firewall Core do ambiente, onde são filtrados os tráfegos e implementadas políticas de segurança, ou seja, saindo do Firewall, a rede WIFI já possui um considerável nível de segurança, o que dispensa recursos idênticos nos dispositivos que proveem a rede WIFI. É como uma redundância, muitas vezes, desnecessária. Cabe a avaliação da manutenção sobre a exigência de módulos WIPS na solução WIFI uma vez que a sua exclusão reduz o custo de contratação.

Por fim, nossas sugestões são a de retirar o termo “WIPS” mas manter as exigências das funções que o compõem, como o Firewall embarcado nos APs por exemplo, ou sua completa remoção uma vez que já há um nível de segurança no Firewall Core da organização, e o aceite de ferramentas externas para a realização dos recursos de WIPS, ou seja, a composição da solução por produtos de outros fabricantes especificamente para este caso.

Agradeço pela atenção e me coloco á disposição para o que mais se fizer necessário.

Obrigado.