From:
To: Departamento de Regulação Supervisão e Certificação
Cc:
Subject: Contributo ao Aviso 21606/2021
Date: 3 de dezembro de 2021 20:50:25
Attachments: image001.png
image002.png
image003.png
image004.png
image005.jpg

Boa tarde.

Relativamente ao Aviso e à regulamentação que este comporta, de utilidade reconhecida, percebe-se a utilização de standards como referência e, também a criação exacerbada quer do volume de dados quer da importância à centralização dessa mesma informação.
É uma descrição demasiado exaustiva, nomeadamente a relativa ao levantamento de riscos.

A realização dos relatórios poderia ser disposta numa página, a construir e disponibilizar para o efeito; as informações adicionais, registos de ataques, consequencias e a evolução dos ativos e dos riscos seriam parte das "versões" a existir. Desta forma seria muito mais eficaz a análise e a manutenção da informação: útil para a CNCS e útil para as entidades.

Seria importante, em minha opinião observar igualmente o seguinte:

- Considerar como ativos, o potencial humano, considerando-os também alvos de ataque ou instrumentos para a realização dos mesmos.
- Considerar como risco "muito elevado" a falta de profissionais em prevenção de 24 horas, nos serviços de risco e/ou superior interesse público ou de estado.
- Considerarem a responsabilidade pela cibersegurança exclusivamente aos profissionais das áreas técnicas relativas aos Sistemas de Informação com experiência na área.
- Definir o período de salvaguarda local dos logs nos vários domínios/servidores/serviços.
- Incluir na informação a prestar, a tipologia e hierarquia de rede, nomeadamente os critérios da sua segmentação.
- Perceber que os endereços dos equipamentos poderão ou ter tempos de vida curtos, ou utilizar os serviços de DHCP.
- Explicar como se organiza a informação relativa aos equipamento WiFi que tomam acessos das redes privadas ou públicas em locais privados e se ou que, salvaguarda de dados tem de ser feita e por quanto tempo, nomeadamente os dados relativos às comunicações.

A par desta problemática gostaria que fossem incluídos nesta análise situações como a seguinte:

Nos hospitais os equipamentos de laboratório (por exemplo) são disponibilizados, regra geral pelos fabricantes, contra consumo.
Ora esse equipamentos só serão disponibilizados se lhes for garantida ligação internet e/ou a abertura de um número específico de portos para comunicação. Outros já tem SIMs integrados para utilização do 4G para a comunicação.
Os dados que comunicam são, acreditamos nós, para alarmística de manutenção ou exclusivos à calibração relativa aos reagentes e dos equipamentos (cada gaveta de reagentes é validado pelo fabricante via web, dizem por questões de calibração ou para excluir contrafações).
Mas podem também não ser…

Os equipamentos tem também ligação à rede interna e trabalham dados dos utentes (mesmo sem serem dados nominais) e dados de produção; podem estes dados ser utilizados para condicionar negociações em procedimentos administrativos posteriores ou serem informados, nomeadamente para serem transacionados.
Este assunto já foi posto por várias vezes aos SPMS, EPE, sem qualquer resolução ou resposta.

Atenciosamente,