I CONGRESSO NACIONAL DE SEGURANÇA E DEFESA

Por uma *Cibersegurança* mais eficaz das infra-estruturas e serviços críticos nacionais

José A. S. Alegria

PT Portugal

Lisboa, 25 de Junho de 2010

Disclaimer

Estas sugestões e ideias são do autor e não representam necessariamente a posição oficial da Portugal Telecom

Sumário

A ***CiberSegurança*** de qualquer nação depende, em grande parte, da capacidade, sofisticação, e interdisciplinaridade da sua rede de centros operacionais e/ou de competência em segurança da informação, redes de telecomunicações e de energia, sistemas distribuídos e de controlo, entre outros, e da eficácia da supervisão e coordenação operacional central dessa rede. Estes centros deverão ter responsabilidades operacionais claras, devendo estar associados às entidades directamente responsáveis pela gestão do risco cibernético das principais infra-estruturas e serviços críticos do país.

Centralmente, deverá ser garantido pelo governo um órgão único transversal de supervisão e coordenação operacional, com competências específicas na área, garantindo a acreditação técnica e "*security clearance*" dos elementos da rede, a existência e manutenção segura dos cadastros "lógicos" relevantes (*domínios e ranges de IP's públicos críticos, informação BGP relevante, informação sobre "core" routers e "peer" routers, …*) e ***CiberRiscos*** associados e, finalmente, a existência verificável de controlos adequados de gestão de risco para cada uma das situações críticas identificadas. Em situações de crise declarada este órgão deverá ter os meios necessários e suficientes para coordenar transversalmente e operacionalmente uma resposta a essa crise requisitando, se necessário, os serviços dos diferentes elementos da rede.

Finalmente, e como forma de estimular o desenvolvimento de conhecimento e competências avançadas em ***CiberSegurança***, é recomendável que um país garanta a existência de pelo menos um centro nacional de I&D na área, com fortes níveis de colaboração com centros universitários nacionais e internacionais e com centros de excelência congéneres em países aliados como o CyLab junto de CMU nos EUA.

Nesta intervenção apresentamos algumas ideias de como se poderão desenvolver os mecanismos atrás expostos em Portugal. *Estas sugestões e ideias são do autor e não representam necessariamente a posição oficial da Portugal Telecom.*

A **REDE** e

a **COORDENAÇÃO**

que ainda nos faltam…

A ***CiberSegurança*** de qualquer nação depende, em grande parte, da **capacidade**, **sofisticação**, e **interdisciplinaridade** da sua **rede de centros operacionais e de competência** em segurança da informação, redes de telecomunicações e de energia, sistemas distribuídos e de controlo, entre outros …

…e da forma e **eficácia** como esses centros

cobrem os diferentes **riscos cibernéticos** do país

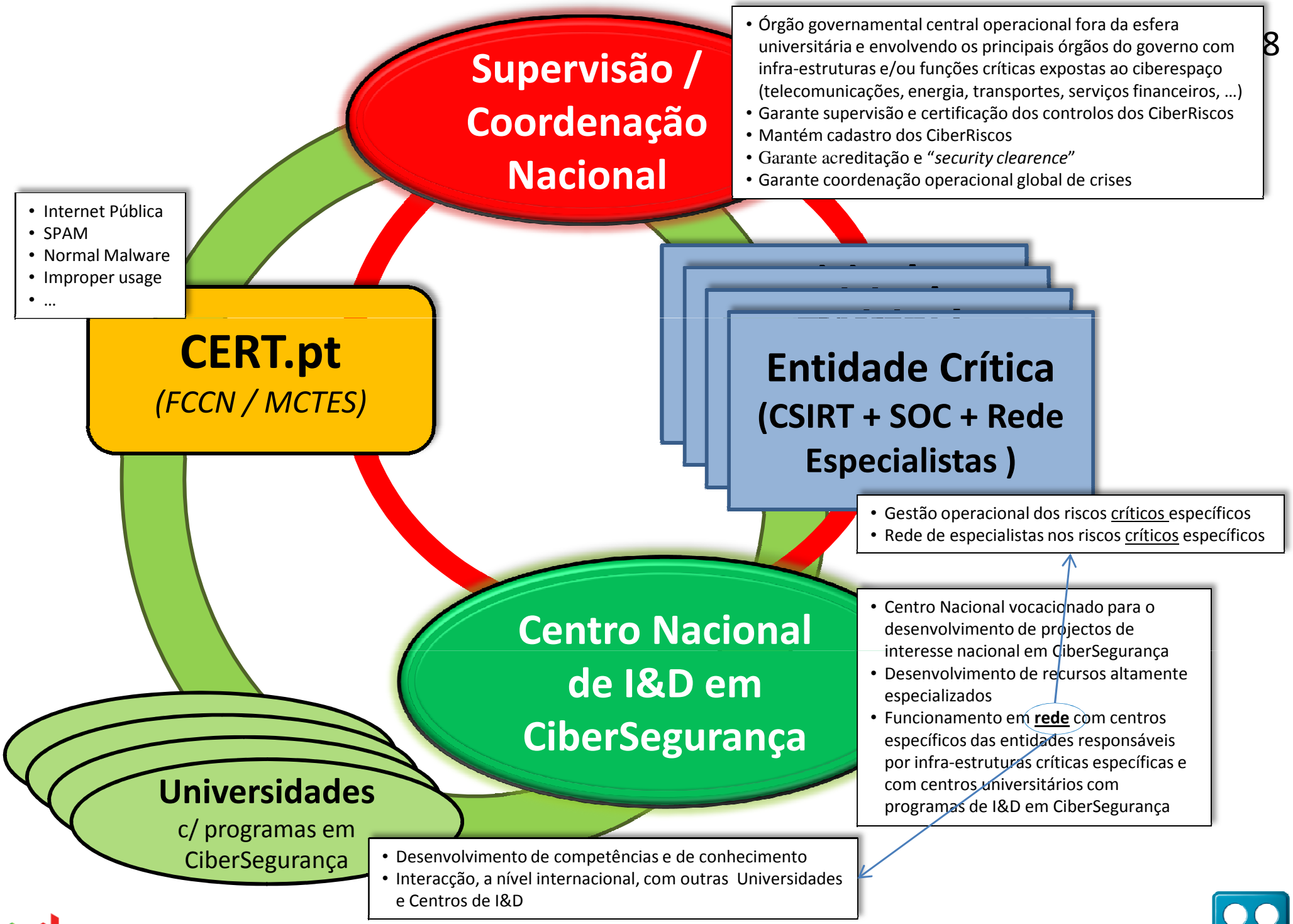
+

da **eficácia** da **supervisão preventiva** e

coordenação operacional central

dessa rede em caso de crise

Um **MODELO** possível…



CSIRT = Computer Security Incident Response Team
SOC = Security Operations Center

Com cada

ENTIDADE CRÍTICA

a assumir as suas

RESPONSABILIDADES …

Estes centros deverão pertencer a cada uma das entidades directamente **responsáveis** pelas infra-estruturas e serviços críticos nacionais onde deverão assegurar a **gestão dos riscos cibernéticos da sua responsabilidade** devendo também **colaborar** sempre que necessário com centros similares de outras entidades

Por outro lado, esta rede de centros só existirá se as entidades responsáveis pelas infra-estruturas e serviços críticos **assumirem** essa responsabilidade e se houver **mecanismos de supervisão** que garantam a sua eficácia mínima. Dados os investimentos envolvidos muitas dessas entidades deverão encontrar formas adequadas de **associação** criando, por exemplo, centros conjuntos com partilha de meios humanos

Exemplificando…

No caso dos operadores de telecomunicações IP é fundamental que cada um assegure, no mínimo, a segurança e resiliência do seu **backbone IP**, dos seus "***peering points***", dos servidores **NDS** primários da sua responsabilidade, e do seu **NOC/SOC** (*Network Operations Center/ Security Operations Center*) face a um eventual **ataque massivo de DDoS** (*Distributed Denial of Service*), eventualmente em simultâneo com ataques ao DNS, e que existam mecanismos de coordenação operacional de **todos** os operadores nacionais, incluindo os seus principais "*peers*" internacionais!

No caso da PT Portugal

CERT Network

Computer Emergency Response Team

CSIRT.telecom.pt
Computer Security Incident Response Team

Centro operacional da PT com ligação em rede a outros CERT's e CSIRT's

Política de Segurança da Informação

PtSecurityLab

CyLab
CMU
FCUL
IST
UP
...

Projectos de I&D aplicada em CiberSegurança em colaboração com o CyLab, CMU, e outras universidades portuguesas

Forte equipe interna de especialistas em Operational Information Intelligence e em CiberSecurity

ROI²
Real Time Operational Information Inteligence

Projectos de I&D aplicada em "*Realtime Operational Information Intelligence*" (ROI²), "*Sensor Networks*", "*Performance & Security Metrics*", com aplicação directa à plataforma de monitorização **Pulso** da PT

Security Operations Center (SOC)

International HoneyNet Project

Centro operacional da PT de supervisão da segurança, para uso interno e para serviços geridos para clientes empresariais

Mas onde estão os

ESPECIALISTAS

que o país precisa?

É evidente que só será possível criar e manter uma rede de centros operacionais e de competência em **CyberSecurity** se primeiro for possível **formar** e **desenvolver** em número e qualidade os necessários **especialistas**

Mas para isso são precisos grupos **Universitários** em número e qualidade com **programas** avançados de formação e com forte envolvimento em projectos de **I&D** de nível **internacional**.

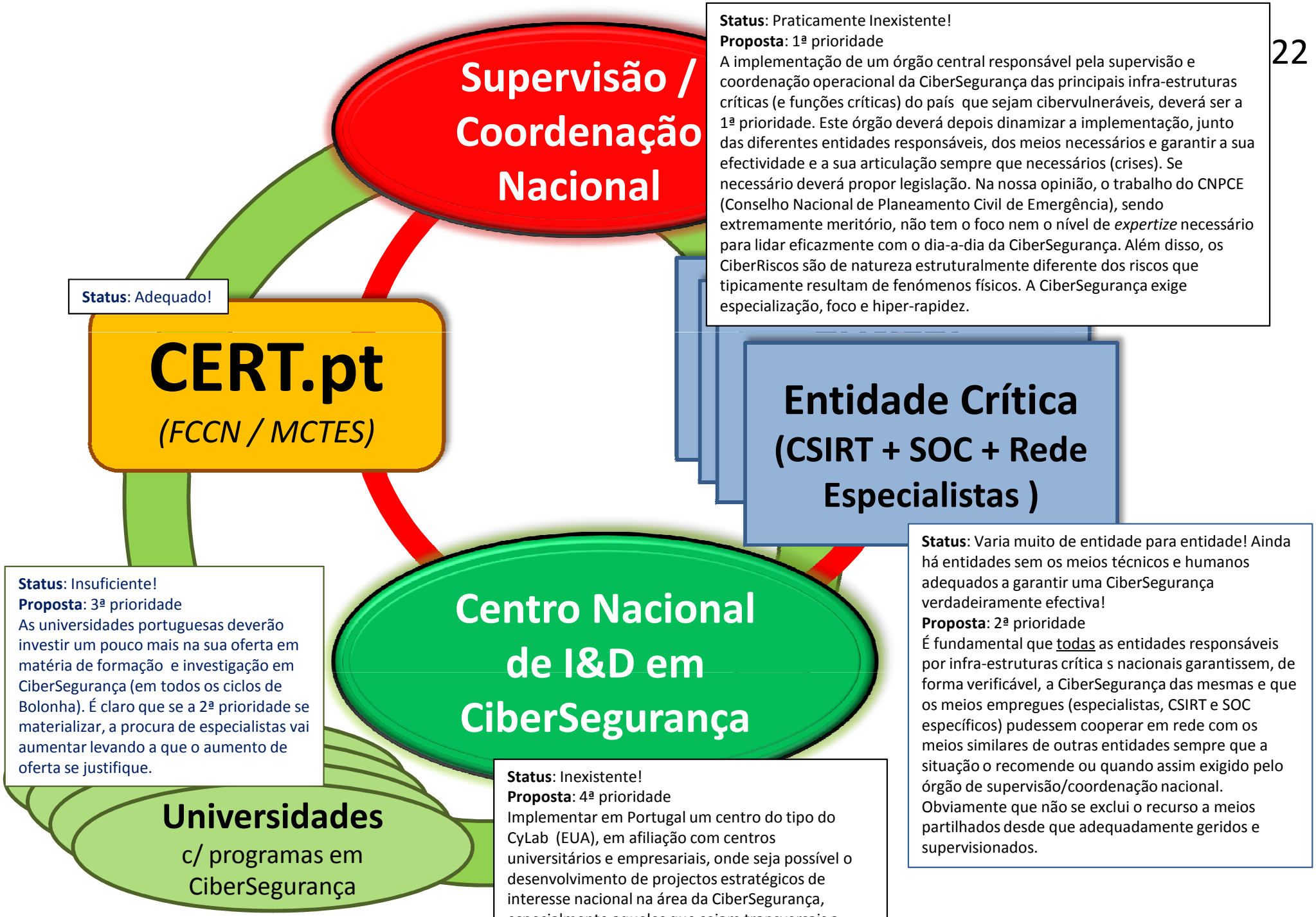
É preciso incentivar o desenvolvimento de mais e melhores grupos Universitários e estimular a sua **colaboração** com as entidades responsáveis pelas infra-estruturas e serviços críticos

E quanto à **SUPERVISÃO** e **COORDENAÇÃO** central ?

Centralmente, deverá ser garantido pelo governo um órgão único transversal de supervisão e **coordenação operacional** garantindo a **acreditação técnica** e "***security clearance***" dos elementos da rede, a existência e manutenção segura dos **cadastros lógicos** relevantes e ***CiberRiscos*** associados e, finalmente, a existência verificável de **controlos** adequados de gestão de risco para cada uma das situações críticas identificadas

Em situações de crise declarada este órgão deverá ter os meios necessários e suficientes para **coordenar** transversalmente uma **resposta** a essa **crise** requisitando, se necessário, os serviços dos diferentes elementos da rede

Em que ponto estamos ?


Supervisão / Coordenação Nacional
Status: Praticamente Inexistente!
Proposta: 1ª prioridade
A implementação de um órgão central responsável pela supervisão e coordenação operacional da CiberSegurança das principais infra-estruturas críticas (e funções críticas) do país que sejam cibervulneráveis, deverá ser a 1ª prioridade. Este órgão deverá depois dinamizar a implementação, junto das diferentes entidades responsáveis, dos meios necessários e garantir a sua efectividade e a sua articulação sempre que necessários (crises). Se necessário deverá propor legislação. Na nossa opinião, o trabalho do CNPCE (Conselho Nacional de Planeamento Civil de Emergência), sendo extremamente meritório, não tem o foco nem o nível de expertize necessário para lidar eficazmente com o dia-a-dia da CiberSegurança. Além disso, os CiberRiscos são de natureza estruturalmente diferente dos riscos que tipicamente resultam de fenómenos físicos. A CiberSegurança exige especialização, foco e hiper-rapidez.
Status: Adequado!
CERT.pt
(FCCN / MCTES)
Entidade Crítica
(CSIRT + SOC + Rede Especialistas)
Status: Varia muito de entidade para entidade! Ainda há entidades sem os meios técnicos e humanos adequados a garantir uma CiberSegurança verdadeiramente efectiva!
Proposta: 2ª prioridade
É fundamental que todas as entidades responsáveis por infra-estruturas crítica s nacionais garantissem, de forma verificável, a CiberSegurança das mesmas e que os meios empregues (especialistas, CSIRT e SOC específicos) pudessem cooperar em rede com os meios similares de outras entidades sempre que a situação o recomende ou quando assim exigido pelo órgão de supervisão/coordenação nacional. Obviamente que não se exclui o recurso a meios partilhados desde que adequadamente geridos e supervisionados.
Status: Insuficiente!
Proposta: 3ª prioridade
As universidades portuguesas deverão investir um pouco mais na sua oferta em matéria de formação e investigação em CiberSegurança (em todos os ciclos de Bolonha). É claro que se a 2ª prioridade se materializar, a procura de especialistas vai aumentar levando a que o aumento de oferta se justifique.
Centro Nacional de I&D em CiberSegurança
Status: Inexistente!
Proposta: 4ª prioridade
Implementar em Portugal um centro do tipo do CyLab (EUA), em afiliação com centros universitários e empresariais, onde seja possível o desenvolvimento de projectos estratégicos de interesse nacional na área da CiberSegurança, especialmente aqueles que sejam transversais a mais do que um tipo de infra-estrutura crítica.
Universidades
c/ programas em CiberSegurança

Obrigado !