Cyberwarfare no contexto de corporações públicas e privadas

Ilton Duccini

Setembro de 2019

Guerra Cibernética ou Cyberwarfare

Uso de tecnologia computacional para interromper as atividades de um estado ou organização, especialmente o ataque deliberado de sistemas de informação para fins estratégicos ou militares.

O CCDCOE

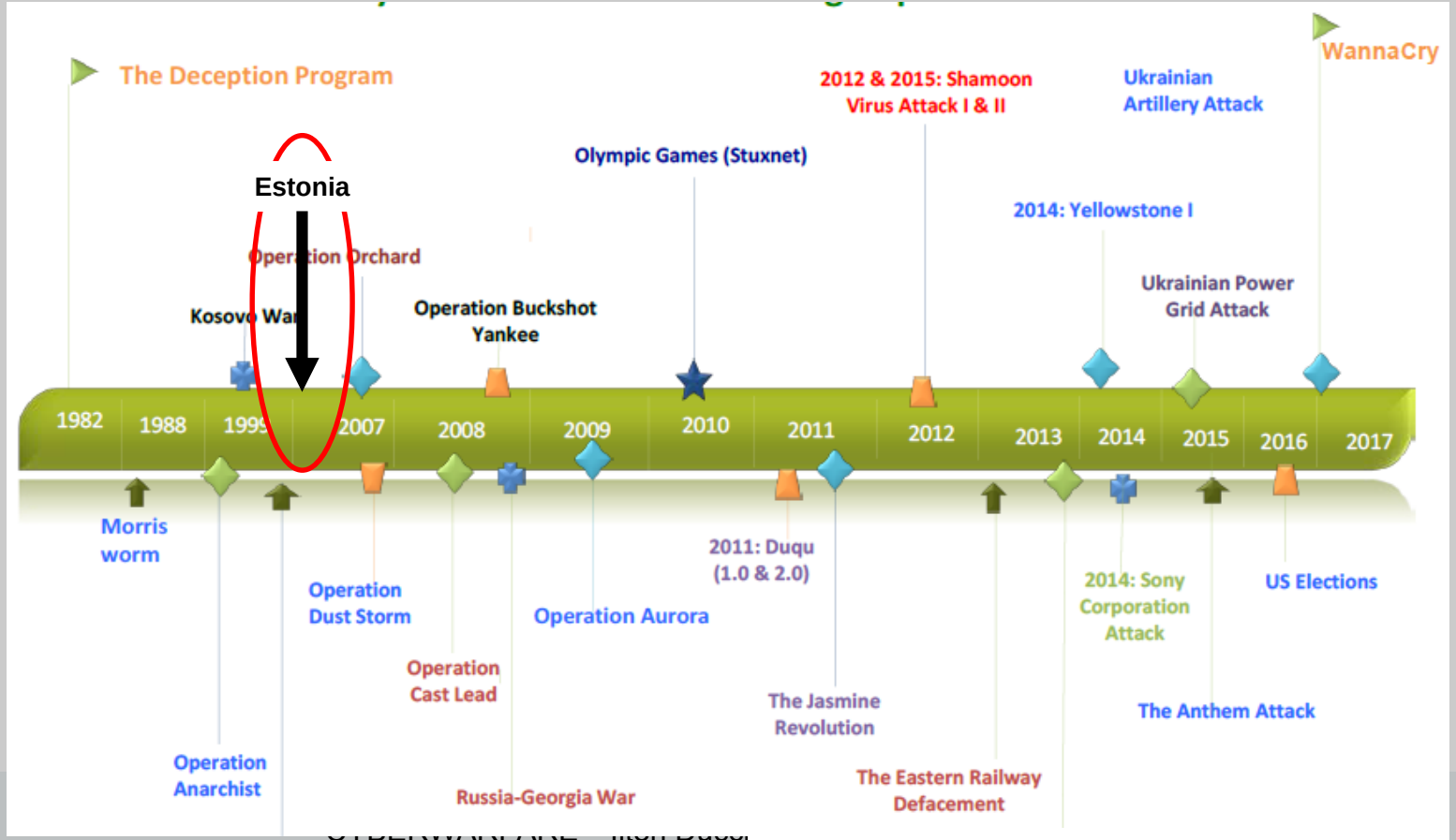
O Cooperative Cyber Defence Centre of Excellence ou Centro de Excelência de Defesa Cibernética Cooperativa é uma Organização Militar Internacional com a missão de melhorar a capacidade, cooperação e compartilhamento de informações entre a OTAN, seus países membros e parceiros na defesa cibernética através da educação, pesquisa e desenvolvimento, lições aprendidas e consultoria.

Foi criado em 2008 e está localizado em **Tallinn**, capital da Estônia.

O pior cenário de ataque cibernético para os EUA

[Cyber Command and National Security Agency chief Adm. Michael S. Rogers]
Maio/2017

Panorama histórico dos casos de guerra cibernética



http://web.mit.edu/smadnick/www/wp/2017-10.pdf

Como devemos nos preparar

Se preocupar não é ação tática

Ação tática é Atacar, Defender, Retardar, Reforçar, Preparar, Capacitar, Destruir, Evadir e outros.

Desta forma, preparar uma Estratégia de Segurança Cibernética é o primeiro passo que deve ser adotado pelas empresas.

Uma Estratégia de Segurança Cibernética deve:

• Ser uma expressão da visão, objetivos de alto nível, princípios e prioridades que orientarão a empresa na abordagem da segurança cibernética;

• Ser uma visão geral das partes interessadas “stakeholders” encarregadas de melhorar a segurança cibernética da empresa e seus respectivos papéis e responsabilidades; e

• Ser uma descrição das etapas, programas e iniciativas que a empresa irá comprometer-se para proteger sua infraestrutura cibernética e aumentar sua segurança e resiliência.

Os benefícios da Estratégia de Segurança Cibernética

É fundamental identificar quais são as nossas prioridades e subsequentemente priorizar investimentos e recursos para gerenciar com sucesso os riscos em uma área tão abrangente quanto a segurança cibernética.

Os benefícios da Estratégia de Segurança Cibernética

Uma Estratégia de Segurança Cibernética também oferece a oportunidade de alinhar as prioridades de cibersegurança com os objetivos relacionados ao negócio da empresa.

A segurança cibernética tornou-se peça central para alcançar os objetivos sócioeconômicos das empresas modernas e a Estratégia deve refletir como estes objetivos serão suportados.

Isso pode ser feito referenciando os projetos que buscam implementar agendas digitais com as iniciativas de segurança cibernética incorporada aos mesmos.

Os benefícios da Estratégia de Segurança Cibernética

Finalmente, um processo de desenvolvimento da Estratégia de Segurança Cibernética deve traduzir a visão de riscos de segurança em projetos coerentes e implementáveis que ajudarão a empresa a alcançar seus objetivos.

Isso inclui não apenas as etapas, programas e iniciativas que devem ser postos em prática, mas também os recursos alocados para esses esforços e como esses recursos devem ser usados.

Da mesma forma, o processo deve identificar as métricas que serão usadas para ajudar a garantir que os resultados desejados sejam atingidos dentro dos orçamentos e cronogramas definidos.

Principais tópicos da Estratégia

Governança

Gestão de Riscos

Resposta a Incidentes e Resiliência

Equipar, Capacitar e Conscientizar

Legislação e regulamentação

Ecossistema de colaboração e cooperação

Governança

Pontos chaves:

- A estratégia deve identificar e capacitar o responsável pela execução da Estratégia;
- Estabelecer um mecanismo para identificar e incluir as entidades afetadas ou responsáveis pela a implementação da Estratégia;
- Comprometer-se a incluir dados específicos, mensuráveis, objetivos alcançáveis, baseados em resultados e baseados em tempo, no plano de implementação para a Estratégia;
- Reconhecer a necessidade de comprometer recursos (por exemplo, vontade política, financiamento, tempo e pessoas) para alcançar os resultados desejados;
- E principalmente ter um Plano de Implementação.

Gestão de Risco

Pontos chaves:

- Definir uma abordagem de gerenciamento de risco;
- Identificar uma metodologia comum para gerenciar o risco de segurança cibernética;
- Desenvolver perfis setoriais de risco de segurança cibernética;
- Estabelecimento de políticas de segurança cibernética

Resposta a Incidentes e Resiliência

Pontos chaves:

- Estabelecer recursos de resposta a incidentes cibernéticos;
- Estabelecer planos de contingência para gerenciamento de crises de segurança cibernética;
- Promover o compartilhamento de informações;
- Realizar exercícios de segurança cibernética.

Equipar, Capacitar e Conscientizar

Pontos chaves:

- Desenvolver currículos de segurança cibernética;
- Estimular o desenvolvimento de habilidades e treinamento da força de trabalho (Cybersecurity Workforce);
- Implementar um programa coordenado de conscientização sobre segurança cibernética;
- Promover inovação em cibersegurança e pesquisa e desenvolvimento.

Legislação e regulamentação

Pontos chaves:

- Adoção de legislação que defina o que constitui a atividade cibernética ilegal;
- Reconhecimento legal de direitos individuais e liberdades civis;
- Estabelecimento de mecanismos de conformidade;
- Promover o fortalecimento institucional para a aplicação da lei;
- Institucionalização de entidades críticas; e
- Cooperação internacional e interorganizacional para combater o crime cibernético.

Ecossistema de colaboração e cooperação

Pontos chaves:

- Reconhecer a importância da segurança cibernética como prioridade dentro da empresa, do setor e do país;
- Envolver-se em discussões internacionais;
- Promover a cooperação formal e informal no ciberespaço;
- Alinhar os esforços nacionais e internacionais de segurança cibernética.

Obrigado!