A indústria de segurança de TI e a segurança da indústria de TI

Joseph S. Nye Jr., Professor da Kennedy School of Government, da Harvard University nos EUA, autor de livros famosos tais como "*The Paradox o f American Power: Why the World´s only superpower can´t go it alone"* (de 2002, traduzido para português como "*O Paradoxo do Poder Americano: por que a única superpotência mundial não pode continuar sozinha"*); "*Soft Power: the means to success in world politics*" (de 2004, traduzido como "*Poder Brando: os meios para ter sucesso na política mundial*"), e mais recentemente "*The Future of Power*" (de 2011, traduzido como "*O Futuro do Poder*"), defende, entre diversas coisas, que dois grandes ***deslocamentos*** de poder estão ocorrendo neste século: uma ***transição*** de poder entre os estados e uma ***difusão*** de poder espalhando-se de todos os estados para os atores não estatais.

Nesta difusão de poder ele dá destaque (junto do Poder Militar, do Poder Econômico, e do Poder Brando) ao Poder Cibernético. Segundo ele, o poder baseado em recursos de informação não é novo, mas o ***poder cibernético é***! Ele conceitua o poder cibernético como um conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas e baseadas em computador – infraestrutura, redes, software, habilidades humanas. Isso inclui não somente a internet dos computadores ligados à rede, mas também intranets, tecnologias de telefonia celular e comunicações via satélite. Definido do ponto de vista comportamental, o poder cibernético é a *capacidade para obter resultados preferidos* mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético (estes resultados preferidos podem ser obtidos *dentro* do espaço cibernético, ou podem ser obtidos em outros domínios *fora* do espaço cibernético).

Tendo esta noção de poder cibernético em mente, gostaríamos de destacar duas dimensões do universo de TI- tecnologias de informação - em matéria de segurança: a) a indústria de segurança de TI, e b) a segurança da indústria de TI. Nesta newsletter vamos tecer breves comentários somente sobre a primeira dimensão.

O que é a indústria de segurança de TI? Se formos seguir as definições da empresa Gartner (www.gartner.com), e mais detalhadamente seus relatórios denominados *Magic Quadrants* (*Quadrantes Mágicos*, que já tratamos nesta newsletter: ver http://bit.ly/I91GBl; http://bit.ly/IfVMcy; http://bit.ly/IlRxv6; http://bit.ly/IaxYtP), veremos que esta é uma indústria em crescente desenvolvimento, compreendendo mercados como o de *Static Application Security Testing (SAST)*; o mercado de *Mobile Data Protection (MDP)*; o mercado de *Enterprise Endpoint Protection Platforms (EPP)*; e o mercado de *Unified Thread Management (UTM)*, para citar os mais facilmente visíveis.

O mercado de SAST é um mercado de tecnologia voltado para aplicações de segurança. À medida que ataques à segurança tem se tornado mais financeiramente motivados, e à medida que as organizações melhoraram a segurança de suas infraestruturas de redes, desktops e servidores, tem havido uma mudança para ataques ao nível das aplicações; dai o crescente mercado de SAST. O mercado de MDP é aquele de sistemas e procedimentos necessários para proteger a privacidade de dados de negócios, para fazer face aos requisitos regulatórios e contratuais, e cumprir com auditorias. O mercado de EPP é composto primariamente de uma coleção de produtos, tais como: anti-malware, anti-spyware, personal firewalls, host-based intrusion prevention; port and device control; full-disk and file encryption; endpoint data loss prevention (DLP), e application vulnerability management control. O mercado de artefatos UTM oferece pequenos e médios negócios com múltiplas funções de redes de segurança em uma simples appliance (eletrodoméstico).

Ainda segundo o Gartner, 44% dos US $ 16,5 bilhões do mercado mundial de software de segurança em 2010 pertenciam a cinco empresas: Symantec (18,9%), MacAfee (10,4%), Trend Micro (6,3%), IBM (4,9%) e EMC (3,8%). Este percentual combinado de fatia de mercado destes cinco vendedores caiu de um percentual de 60% em 2006, o que sinaliza para o surgimento de novos players neste crescente mercado (tais como Sophos, Kaspersky, Check Point, dentre outras).

E o que tem acontecido com esta indústria? Um número de ***cyberattacks*** (*ataques cibernéticos* são atividades da ***cyberwarfare***, que são ações de um estado-nação para penetrar os computadores e redes de outra nação com a intenção de causar danos ou interrupções através de sabotagem e espionagem; os ataques podem vir também de entidades não-estado, mas com os mesmos propósitos) altamente visíveis tem aparecido nas manchetes ao redor do mundo, mas os problemas subjacentes afetam todos nós. Parece que os ***cybercriminals*** (criminosos do espaço cibernético) estão ficando mais ousados em seus ataques à medida que a disponibilidade de ferramentas comerciais torna a geração em massa de novas campanhas maliciosas de códigos (ataques aos códigos dos software) e *exploits* (vírus e *DOS- denials of services*, negações de serviços) mais fáceis. O resultado líquido, como nos aponta Gerhard Eschelbeck, CTO-Chief Technology Officer da empresa SOPHOS (www.sophos.com), especializada em segurança de TI, tem sido um significativo crescimento em volume de ***malware*** (software malicioso projetado para interromper operações computacionais) e infecções.

A web continua a ser, sem dúvidas, o mais proeminente vetor de ataques. Os cybercriminals tendem a focar onde estão os pontos fracos e usam uma técnica até que se torne menos efetivo. Mas o rápido influxo de ***smartphones*** e ***tablets*** está causando significativos desafios de segurança para muitas organizações. Departamentos de TI estão sendo chamados a conectar seus dispositivos às redes corporativas e a segurar dados nestes dispositivos, os quais eles têm pouco controle. A natureza única na forma moderna de fatores (em termos de poder de processamento, memória, vida das baterias) requer um repensar os mecanismos de segurança e de defesa.

E como está a segurança da indústria de TI? Este é o tema da próxima newsletter!

Se sua empresa, organização ou instituição deseja saber mais sobre as indústrias de TI em matéria de segurança, fique a vontade para nos contatar!