A Importância de uma abordagem multissetorial para a segurança cibernética efetiva

Texto baseado em artigo de Cristine Hoepers, Klaus Steding-Jessen e Henrique Faulhaber para o Encontro NETmundial de 2014, adaptado e atualizado para esta edição da poliTICs.

Data da publicação:

Março 2022

1. Introdução

Muitas das ameaças de segurança da Internet são cada vez mais complexas, afetando vários setores ao mesmo tempo e exigindo esforços coordenados para ser detectadas e efetivamente mitigadas. Isto é especialmente verdadeiro para os incidentes envolvendo botnets, spam, malware e DDoS (Distributed Denial of Service).

Nos últimos 30 anos foram criados vários fóruns com várias partes interessadas e iniciativas que tratam de ameaças à segurança da Internet - a maioria deles têm sido muito bem sucedidos em juntar diferentes setores para em conjunto mitigar os incidentes de segurança e o cibercrime. Todos estes esforços revelaram que a eficácia depende da cooperação entre os diferentes setores, e que a segurança cibernética não pode ser alcançada através de uma única organização ou estrutura. Além disso, os governos precisam participar mais em fóruns de segurança e melhorar a cooperação com os outros setores. Novos fóruns e iniciativas não devem substituir as estruturas existentes, que devem visar a alavancagem e melhorar as estruturas já existentes dos vários grupos de interesse.

O cenário fica mais complicado quando as infraestruturas críticas nacionais estão ligados à Internet, tornando-se expostas às mesmas vulnerabilidades que outros sistemas, e podem ser atacadas pelas mesmas ferramentas ou técnicas usadas para ataques em outros contextos.

A proteção das infraestruturas críticas e redes governamentais ligadas à Internet envolve os aspectos de defesa e de segurança da Internet - a proteção destas infraestruturas é feita na maioria das vezes por organizações governamentais. O preocupante é que estamos vendo cada vez mais as questões que são puramente de segurança da Internet sendo percebidas pelos governos como questões puramente de defesa. Isso está levando a um cenário em que, por exemplo, a cooperação vital já existente entre as CERT (Computer Emergency Response Teams) que têm responsabilidade nacional está sendo prejudicada por uma tendência a transferir todos os recursos de segurança da Internet existentes para organizações governamentais ou de inteligência.

O ecossistema de segurança, estabilidade e resiliência da Internet deve permanecer multissetorial. A cooperação entre os diferentes setores e partes interessadas, hoje já existente, é a chave para mitigar muitas das ameaças atuais.

No restante desta proposta, vamos discutir brevemente vários fóruns multissetoriais e iniciativas em andamento, identificando os seus pontos fortes, e destacar temas que precisam ser considerados quando se discute uma estrutura para melhorar a abordagem multissetorial que viabilize uma segurança cibernética mais eficaz.

2. Fóruns existentes envolvendo múltiplos agentes sociais

Há vários fóruns internacionais já existentes que congregam diferentes agentes, cooperando para lidar com incidentes de segurança e mitigar ameaças específicas. A maioria destes fóruns foram criados para mitigar categorias específicas de ataques ou ameaças. Como hoje em dia o cenário de ameaças mudou e há uma

prevalência do que é tecnicamente conhecido como ameaças combinadas, a maioria dessas organizações está lidando com questões de segurança semelhantes. O que se segue é uma descrição de cada um destes organismos.

2.1. FIRST

O FIRST é o Fórum de Equipes de Resposta a Incidentes e Segurança[1]. A CSIRT (Equipe de Resposta a Incidentes de Segurança)[2], às vezes também referida como CERT, é uma organização de serviços que é responsável por receber, analisar e responder a relatos e atividades de incidentes de segurança informática. Seus serviços são geralmente realizados para um público definido, como uma entidade ou organização empresarial, governamental ou educacional, uma região ou país, uma rede de pesquisa, ou um cliente pago[3].

O primeiro CSIRT, o Centro de Coordenação CERT, foi criado em Novembro de 1988, após o incidente de segurança conhecido como "verme da Internet" ou "verme de Morris", derrubou grande parte da Internet, e deixou clara a necessidade de esforços mais coordenados para responder a incidentes de segurança[4]. Após este incidente, foram criadas várias outras equipes. A primeira foi formada em 1990, em resposta a um segundo verme, o "verme WANK"[5], e este incidente destacou a necessidade de uma melhor comunicação e coordenação entre equipes de diferentes organizações.

FIRST é uma confederação internacional de equipes confiáveis de resposta a incidentes de computador[6] que cooperativamente lida com incidentes de segurança informática e promove programas de prevenção de incidentes. O FIRST reúne uma grande variedade de CSIRTs de todo o mundo, incluindo entidades educacionais e comerciais, distribuidores, entidades nacionais, governo e militares. Os membros do FIRST desenvolvem e compartilham informações técnicas, ferramentas, metodologias, processos e melhores práticas, e usam seus conhecimentos combinados, habilidades e experiência para promover um ambiente mais seguro na Internet.

2.2 CiviCERT

Esta é uma rede de CERTs e provedores de conteúdo e serviços de Internet que colaboram com entidades civis para prevenir e lidar com temas de segurança digital[7]. A rede é uma iniciativa de um grupo de organizações sem fins de lucro, provedores e indivíduos conhecida como RaReNet (Rapid Response Network)[8] que buscam contribuir tempo e recursos para a conscientização sobre segurança digital da sociedade civil. Entre os membros estão entidades como a Access Now, Anistia Internacional, Colnodo, Electronic Frontier Foundation e Human Rights Watch.

2.3. CSIRTs com responsabilidade nacional

Desde 2006, o Centro de Coordenação CERT (CERT/CC)[9] tem promovido uma reunião técnica anual para CSIRTs com responsabilidade nacional. Esta reunião é uma oportunidade para as organizações responsáveis por proteger a segurança das nações, economias e infraestruturas críticas de discutir os desafios que eles enfrentam ao cumprir este papel. Como resultado destas reuniões, um fórum online é mantido durante todo o ano, bem como uma lista de CSIRTs com responsabilidade nacional[10].

Vale ressaltar que existem diferentes modelos de CSIRT nacionais, que vão desde estruturas sem fins de lucro, acadêmicas e até equipes de governo. Além disso, vários países têm mais de uma equipe, o que demonstra a complexidade de aumentar a segurança cibernética e realizar o tratamento de incidentes a nível nacional.

2.4. APWG

O APWG (Grupo de Trabalho Antiphishing)[11] foi fundado em 2003, momento em que a sua missão era combater ataques de *phishing*.[12] Mas, como a tecnologia evoluiu, APWG não é mais focado apenas em *phishing*, mas na mitigação de outros ataques que são usados para cometer crimes cibernéticos. APWG tem mais de dois mil membros e parceiros de pesquisa em todo o mundo, desde instituições financeiras, varejistas, provedores de soluções, provedores de Internet, empresas de telecomunicações, CSIRTs, universidades, empreiteiros da defesa, agências de aplicação da lei, grupos de comércio, agências multilaterais e governamentais.

2.5. M3AAWG

O M3AAWG (Grupo de Trabalho Móvel de Mensagens, Malware e Anti-Abuso)[13] aglutina a indústria de

mensagens para trabalhar de forma colaborativa no tratamento exitoso de várias formas de abuso de mensagens, tais como spam, vírus, ataques de negação de serviço e outras explorações de mensagens. Para isso, desenvolve iniciativas M3AAWG nas três áreas necessárias para resolver o problema de abuso de mensagens: colaboração da indústria, tecnologia e políticas públicas.

2.6. ISOC

A ISOC (Internet Society)[14] é uma organização dedicada a garantir que a Internet permaneça aberta e transparente. Ela tem iniciativas em políticas de Internet, padrões de tecnologia e desenvolvimento futuro. A ISOC tem um projeto especial chamado "Projeto Combatendo o Spam", em parceria com MAAWG, dedicado a mostrar a formadores de políticas, de forma clara e eficaz, as ferramentas e parcerias industriais que estão disponíveis para combater spam.

3. Exemplos de iniciativas multissetoriais exitosas nacionais e internacionais

Nos últimos anos, CSIRTs, operadores de rede e os membros dos fóruns acima mencionados envolveram-se em alguns projetos e grupos de trabalho destinados a mitigar grandes ameaças específicas, implementando as melhores práticas ou compreendendo melhor o ambiente de ameaças na Internet. Nesta seção, vamos descrever algumas dessas iniciativas multissetoriais exitosas.

3.1. Grupo de Trabalho Conficker

Começando no final de 2008, e continuando até junho de 2010, uma coalizão de pesquisadores de segurança trabalhou para resistir a um ataque na Internet por software malicioso conhecido como Conficker. Esta coligação ficou conhecido como "Grupo de Trabalho Conficker", e pareceu ser bem sucedida de várias maneiras, entre as quais a cooperação sem precedentes entre organizações e indivíduos em todo o mundo, em ambos os setores público e privado[xv15].

O trabalho deste grupo envolveu membros dos órgãos de governança da Internet, software e fornecedores de hardware, provedores de conteúdo, universidades e centros de pesquisa, e foi vital para mitigar transportadores maliciosos do verme e para ajudar a limpar sistemas em toda a Internet. Um documento de lições aprendidas pode ser encontrado na página inicial do sítio mencionado.

3.2. DCWG

O DCWG (Grupo de Trabalho DNS Changer)[16] foi um grupo ad hoc de especialistas no assunto, e incluiu membros de organizações como Georgia Tech, Internet Systems Consortium, Mandiant, National Cyber-Forensics e Training Alliance, Neustar, Spamhaus, Equipe Cymru, a Trend Micro, e Universidade do Alabama em Birmingham. O trabalho do DCWG foi coordenado com as investigações do FBI, e recebeu ajuda de vários CERTs nacionais e provedores de acesso.

Este grupo de trabalho foi criado para ajudar a sanar os servidores DNS maliciosos da Rove Digital. O botnet operado pela Rove Digital alterava as configurações de DNS do usuário, direcionando as vítimas para servidores de DNS maliciosos em centros de dados na Estônia, Nova York e Chicago. Os servidores de DNS maliciosos davam respostas falsas e maliciosas, alteravam buscas do usuário e promoviam produtos falsificados e perigosos. Como cada pesquisa na Web começa no DNS, o malware mostrava aos usuários uma versão alterada da Internet.

A cooperação entre todos esses setores permitiu alertar gradualmente e ajudar a desinfetar dispositivos dos usuários finais, sem interromper o seu acesso à Internet.

3.3. Iniciativas multissetoriais a nivel nacional

Existem várias iniciativas multissetoriais nacionais. Nesta seção, vamos descrever brevemente algumas dessas iniciativas.

3.3.1. Conselho de Ciberssegurança Holandês

O Conselho de Ciberssegurança Holandês tem 15 membros do governo, da indústria e da comunidade científica, para um total de três cientistas, seis do setor público e seis representantes do setor privado[17]. O Conselho,

apoiado por uma secretaria independente, supervisiona a estratégia de segurança cibernética nacional holandesa e oferece recomendações ao governo holandês e à sociedade. O papel que o Conselho desempenhou durante o incidente DigiNotar, por exemplo, demonstrou a eficácia deste tipo de parceria público-privada no domínio digital[18].

Em julho de 2013, o Conselho emitiu um parecer sobre a nova Estratégia Nacional de Segurança Cibernética, publicado em Outubro de 2013. As recomendações eram voltadas especificamente para a necessidade de uma estreita cooperação e coordenação em matéria de detecção e resposta a incidentes. Somente através compartilhamento ativo de informação, resposta oportuna e colaboração contínua pode um ambiente digital seguro ser estabelecido.

3.3.2. CCC - Centro Japonês de Ciberlimpeza

O CCC é um organismo central que promove a limpeza de bots e prevenção de reinfecção de computadores infectados dos usuários, baseado na cooperação entre o governo, os fornecedores de software e os provedores de acesso[19]. O CCC tem um Comitê Gestor que supervisiona três grupos de trabalho: o grupo de operação do sistema de contramedidas a bots, o grupo de análise dos programas bots, e o grupo promotor da prevenção da infecção por bots.

3.3.3. Iniciativa de Gestão da Porta 25 - CGI.br

Durante muito tempo, o Brasil esteve presente na maioria dos rankings como país topo de reenvio de spam. Determinado a reverter essa situação, o Comitê Gestor da Internet no Brasil (CGI.br) realizou, desde 2005, uma série de atividades, tais como estudos acadêmicos e análises técnicas, que levaram à adoção Gestão da Porta 25 como a medida mais eficaz para evitar o abuso da infraestrutura de banda larga no Brasil por spammers. Esta iniciativa foi liderada pelo Grupo de Trabalho Antispam do CGI.br (CT- Spam), que manteve um fórum onde os diferentes atores puderam reunir-se[20].

Por quase 20 anos, o Brasil desenvolveu um modelo de governança da Internet multissetorial. Portanto, uma medida de tamanha importância como o bloqueio de tráfego de saída da porta 25 em redes residenciais não poderia ser adotada sem a devida consulta a todos os setores afetados, que foram solicitados a contribuir para este processo de tomada de decisão.

Reunindo a experiência de empresas de telecomunicações, mais de uma dezena de milhares de provedores de serviços de Internet, representantes da sociedade civil e da comunidade acadêmica, bem como a equipe técnica do CGI.br, o processo de adoção da gestão da porta 25 foi amplamente discutido. Isto foi especialmente importante porque a implementação exigiu um esforço concertado, assegurando que os provedores de serviços de e-mail passassem a oferecer a submissão de mensagens através de uma porta diferente (587), e migraram pelo menos 90% da base de seus usuários antes que os provedores de banda larga bloqueassem a porta de saída 25.

Também é importante ressaltar que tanto a Agência Nacional de Telecomunicações (Anatel) e o Ministério da Justiça têm desempenhado um papel fundamental no fornecimento de suporte para as empresas de telecomunicações e as entidades de defesa do consumidor, respectivamente. Anatel assinou um Acordo de Cooperação com CGI.br, que deu às empresas de telecomunicações fundamentos jurídicos para prosseguir com a adoção. O Ministério da Justiça, por outro lado, publicou uma nota técnica explicando os benefícios de tais medidas para os consumidores.

Como resultado desta iniciativa, o Brasil já não é listado como um dos principais países no reenvio de spam no mundo, de acordo com vários rankings públicos.

3.3.4. CERT.br - Computer Emergency Response Team Brasil

O CERT.br é mantido pelo NIC.br, uma organização sem fins lucrativos criada para implementar as decisões e projetos elaborados pelo Comitê Gestor da Internet no Brasil - CGI.br. Todas as atividades do CERT.br levam em conta a necessidade de envolver todas as partes interessadas para aumentar com êxito o nível de segurança a capacidade de lidar com incidentes nas redes conectadas à Internet no Brasil[21].

Além de realizar atividades de tratamento de incidentes, o CERT.br também trabalha para aumentar a percepção sobre segurança na comunidade brasileira, mantendo um projeto de alerta prévio, com o objetivo de identificar novas tendências e correlacionar eventos de segurança, bem como alertando redes brasileiras envolvidas em

atividades maliciosas. CERT.br também ajuda os novos CSIRTs a estabelecer suas atividades no país.

Um exemplo claro do sucesso dessa abordagem é o Projeto Brasileiro de Honeypots Distribuidos, que, através de uma rede de honeypots distribuídos no espaço Internet brasileiro, aumenta a capacidade de detecção de incidentes, correlação de eventos e análise de tendências no país[22]. Estes honeypots são sensores passivos que fornecem percepção situacional valiosa, sem coletar o tráfego normal de dados nem realizar qualquer tipo de vigilância. Este projeto tem sensores em mais de 40 organizações brasileiras parceiras, que vão desde os setores do governo e da energia, a academia, provedores de serviços Internet e provedores de telecomunicações.

3.3.5 Iniciativas do NIC.br de apoio à cibersségurança

O NIC.br, através de seus programas permanentes, mantém várias iniciativas de monitoramento e apoio sobre a segurança das redes e dispositivos da Internet. Entre estas estão:

Campanha Fique Esperto[23] -- É uma iniciativa que une governo e entidades privadas com o objetivo de informar às pessoas sobre como evitar golpes usuais do nosso novo mundo digital. Durante o período da campanha, são apresentadas, mensalmente, novas dicas relacionadas aos problemas mais comuns e às medidas de prevenção que podem ser tomadas para evitá-los.

Cidadão na Rede[24] – conduzido pela equipe do Ceptro.br[25], incentiva boas práticas relacionadas à cidadania digital e ao bom uso da Internet, alcançando o maior número possível de seus usuários. Com animações curtas, que explicam de maneira simples como usar a rede de forma correta e responsável, abrangendo questões técnicas e comportamentais, dicas importantes podem ser transmitidas e compartilhadas pela rede. Empresas e organizações interessadas podem se tornar parceiras dessa iniciativa, fazendo o download gratuito dos vídeos ou solicitando a inclusão do seu logo em uma versão customizada dos vídeos, para divulgação em seu site, ou outros canais.

Internet Segura[26] -- Idealizado pelo CGI.br, o portal Internet Segura reúne iniciativas de conscientização sobre segurança e uso responsável da Internet no Brasil, auxiliando os internautas a localizar as informações de interesse e incentivando o uso seguro da Internet. O portal também traz iniciativas de outras entidades e instituições sobre o uso seguro da Internet.

3.3.6. CAIS/RNP

Este centro de atendimento a incidentes de segurança é mantido há mais de 20 anos pela Rede Nacional de Ensino e Pesquisa (RNP)[27], e oferece apoio à adoção de boas práticas de segurança nas instituições acadêmicas e outras conectadas à extensa e diversificada rede da RNP. CAIS é um dos primeiros centros de resposta a incidentes a operar nacionalmente, e mantém parceria com 15 CSIRTs de entidades acadêmicas no Brasil. Oferece também apoio a órgãos públicos.

4. A necessidade de melhoria da colaboração multissetorial em cibersegurança

Atingir um nível satisfatório de segurança na Internet não é uma tarefa fácil, mas a experiência acumulada por várias iniciativas de sucesso demonstra que, para ser eficaz, qualquer iniciativa de segurança cibernética precisa envolver vários intervenientes. Mais do que isso, a realidade é que na maioria das vezes, as medidas de segurança devem ser tomadas por administradores de sistemas, operadores de rede ou profissionais de segurança em suas próprias redes. No entanto, a cooperação com os outros é a chave para ser capaz de entender as ameaças e melhor avaliar a eficácia de suas ações.

No documento "Grupo de Trabalho Conficker: Lições Aprendidas"[28], publicado em Janeiro de 2011, embora não apareça o conceito de "multissetorial", alguns dos fatores de sucesso listados indicam a importância da cooperação e do envolvimento de diferentes grupos de interesse. Aqui estão alguns exemplos:

- utilizar um modelo de confiança; o grupo de trabalho deve ter um tamanho gerenciável para ser eficaz e incluir aqueles diretamente afetados, mas grande o suficiente para incluir um universo mais amplo de pessoas afetadas;

- incorporar um modelo de consenso, sem hierarquia, para permitir que o grupo se adpte e responda à rápida mudança das condições;
- ganhar a participação e apoio de órgãos reguladores e de governo relevantes;
- formalizar a comunicação com grupos de interesse em vez de contar com redes sociais.

Estes quatro pontos trazem à luz questões como a rápida mudança do cenário de ameaças, a necessidade de uma comunicação rápida, o envolvimento e apoio dos governos e o fato de que os vários grupos de interesse precisam cooperar.

Embora o Grupo de Trabalho Conficker tenha sido muito bem sucedido, bem como outras iniciativas listadas na seção anterior, ainda existem alguns setores que poderiam melhorar a sua cooperação. Por exemplo:

- Os Grupos de Operadores de Rede (NOGs) e Registros Regionais de Internet (RIRs) deveriam estar mais envolvido com as questões de segurança. Há algumas áreas, como a segurança de roteamento (e protocolos recentemente propostos como RPKI ou SBGP) ou DNSSEC que precisam de adoção em todo o mundo para serem eficazes. Os RIRs também podem trabalhar mais próximos à comunidade CSIRT para melhorar o sistema WHOIS e com isso ajudar o processo de tratamento de incidentes.
- Os fornecedores de software precisam envolver-se e serem mais proativos – afinal, a maior parte dos problemas de segurança que enfrentamos hoje são problemas relacionados com software. O verdadeiro desafio é melhorar a segurança do software e elevar a indústria de software a um nível mais maduro.
- Os governos, incluindo os setores militares e de inteligência, além de estratégias de segurança e defesa tradicionais, precisam melhorar a sua consciência da natureza multissetorial da Internet e a importância vital da cooperação para enfrentar as ameaças à segurança. Eles precisam participar mais nos fóruns nacionais e internacionais de segurança e melhorar a cooperação com outros setores.

Considerando-se as estratégias de segurança cibernética de governos, é de salientar que cerca de 130 representantes de vários setores, incluindo entidades públicas e privadas, instituições de conhecimento e organizações sociais, estiveram envolvidos na elaboração da "Estratégia Nacional de Segurança Cibernética 2 - Da consciência à capacidade" da Holanda (NCSS2)[29]. A estratégia começa com a seguinte declaração: "Estamos caminhando de estruturas a coalizões em que todas as partes – nacionais e internacionais – são representadas, a fim de atingir os padrões suportados."

E acrescenta: "A correlação entre segurança, liberdade e benefícios sócio- econômicos propostos no NCSS2 é um equilíbrio dinâmico, que se destina a ser realizado em um diálogo constantemente aberto e pragmático entre todos os intervenientes, tanto nacionais como internacionais. (...) A fim de trazer o diálogo sobre segurança cibernética entre as várias partes interessadas para um novo nível de maturidade, as três seguintes áreas de gestão são de extrema importância : (auto-) regulação, transparência e desenvolvimento do conhecimento."

Este é um bom exemplo do reconhecimento da importância de uma abordagem multissetorial para a segurança, estabilidade e resiliência do ecossistema da Internet.

5. Recomendações

Como já mencionado, alcançar um nível satisfatório de segurança na Internet não é uma tarefa fácil, e as iniciativas já discutidas envolvendo vários grupos de interesse são bons exemplos de estruturas que podem efetivamente lidar com questões correntes e emergentes de segurança cibernética. Portanto, recomenda-se que

todas as organizações nacionais e internacionais envolvidas com a governança da Internet, por exemplo, os governos, os registradores regionais de endereços IP (RIRs), as Nações Unidas, a União Europeia, os capítulos da Internet Society, entre outros, devam levar em consideração o seguinte :

1. A experiência acumulada pelas diversas iniciativas de sucesso descritas nesta contribuição demonstra que, para ser eficaz, qualquer iniciativa de segurança cibernética depende da cooperação entre os diferentes atores, e isso não pode ser alcançado através de uma única organização ou estrutura.

2. Há atores que ainda precisam envolver-se mais, como operadores de rede e desenvolvedores de software.

3. Governos, incluindo os setores militares e de inteligência, além das estratégias de segurança e defesa tradicionais, precisam melhorar a sua consciência da natureza multissetorial da Internet e da importância vital da cooperação para enfrentar as ameaças à segurança. Eles precisam participar mais nos fóruns nacionais e internacionais de segurança e melhorar a cooperação com outras partes interessadas.

4. Há espaço e necessidade de novos fóruns e iniciativas, mas não devem substituir as estruturas existentes. Qualquer nova iniciativa deve ter como objetivo alavancar e melhorar as estruturas multissetoriais já em vigor hoje.

--

1 https://www.first.org/

2https://www.csirt.org/

3 https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=485652

4 https://en.wikipedia.org/wiki/Morris_worm

5 https://en.wikipedia.org/wiki/WANK_*(computer_worm)*

6 “Computador” hoje é entendido como o universo gigantesco de dispositivos que podem ser conectados à Internet – tabuletas, celulares, computadores portáteis e de mesa, dispositivos embarcados fixos ou móveis, veículos etc.

7 https://www.civicert.org/

8 https://www.rarenet.org/

9 https://www.kb.cert.org/vuls/

10 https://www.sei.cmu.edu/our-work/cybersecurity-center-development/index.cfm. A lista de CSIRTs europeus pode ser vista aqui: https://csirtsnetwork.eu/

11 https://apwg.org/

12 https://en.wikipedia.org/wiki/Phishing

13 https://www.m3aawg.org/. O grupo hoje é chamado de M3AAWG – Message, Malware, Mobile Anti-Abuse Working Group.

14 https://www.internetsociety.org/

15 https://www.senki.org/operators-security-toolkit/security-organizations/...

16 https://www.crunchbase.com/organization/the-dns-changer-working-group---...

17 https://www.ncsc.nl/english/current-topics/news/best-practices-in-comput...

18 https://en.wikipedia.org/wiki/DigiNotar

19 https://www.ccc.go.jp/en_ccc/

20 https://www.cert.br/docs/palestras/certbr-ct-spam-cgibr2008.pdf

21 https://www.cert.br/

22 https://honeytarg.cert.br/honeypots/index-po.html

23 https://fe.seg.br/

24 https://cidadaonarede.nic.br

25 https://ceptro.br/

26 https://internetsegura.br/

27 https://www.rnp.br/sistema-rnp/cais

28 http://docs.media.bitpipe.com/io_10x/io_102267/item_465972/whitepaper_76...

29 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/nc...

Categoria:

- poliTICs 33