abramulti
Associação brasileira dos operadores de telecomunicações e provedores de internet.

Cibersegurança

O que é cibersegurança?

Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas. O termo é aplicável a uma variedade de contextos, desde negócios até computação móvel, e pode ser dividido em algumas categorias comuns.

- **Segurança de rede** é a prática de proteger uma rede de computadores contra intrusos, sejam eles invasores direcionados ou malware oportunista.

- **Segurança de aplicativos** foca em manter o software e os dispositivos livres de ameaças. Um aplicativo comprometido pode fornecer acesso aos dados que pretende proteger.

- **Segurança de informações** protege a integridade e a privacidade dos dados, tanto no armazenamento como em trânsito.

- **Segurança operacional** inclui os processos e decisões para tratamento e proteção dos arquivos com dados. As permissões que os usuários têm ao acessar uma rede e os procedimentos que determinam como e onde os dados podem ser armazenados ou compartilhados se enquadram nesta categoria.

- **Recuperação de desastres e continuidade dos negócios** definem como uma organização responde a um incidente de cibersegurança ou qualquer outro evento que cause a perda de operações ou dados. As políticas de recuperação de desastres ditam como a organização restaura suas operações e informações para retornar à mesma capacidade operacional de antes do evento. A continuidade dos negócios é o plano ao qual a organização recorre ao tentar operar sem determinados recursos.

- **Educação do usuário final** aborda o fator de cibersegurança mais imprevisível: as pessoas. Qualquer pessoa pode introduzir acidentalmente um vírus em um sistema seguro se deixar de seguir as práticas recomendadas de segurança. Ensinar os usuários a excluir anexos suspeitos de e-mail, não conectar unidades USB não identificadas e várias outras lições importantes é vital para a segurança de qualquer organização.

O Crescimento da ameaça virtual

A ameaça virtual global continua a evoluir em ritmo acelerado, com um número crescente de violações de dados a cada ano. Um relatório da **RiskBased Security** revelou um número impressionante de 7,9 bilhões de registros que foram expostos por violações de dados somente nos primeiros nove meses de 2019. Este número é mais que o dobro (112%) do número de registros expostos no mesmo período em 2018.

Serviços médicos, varejistas e entidades públicas foram os que mais sofreram violações, sendo os criminosos mal-intencionados os responsáveis pela maioria dos incidentes. Alguns desses setores são mais **atraentes para** os criminosos virtuais porque coletam dados financeiros e médicos, mas todas as empresas que utilizam redes podem ser alvo de ataques a dados de clientes, espionagem corporativa ou ataques de clientes.

Com a escala da ameaça virtual crescente, a International Data Corporation prevê que os gastos mundiais com soluções de cibersegurança chegarão a 133,7 bilhões de dólares até 2022. Governos do mundo todo têm respondido à crescente ameaça virtual com orientações para ajudar as organizações a implementar práticas eficazes de cibersegurança.

Tipos de ameaças virtuais

Analisei e identifiquei três principais ameaças que a Cibersegurança vem combatendo nos últimos anos:

1. O **crime virtual** inclui indivíduos ou grupos que visam sistemas para obter ganhos financeiros ou causar interrupções.
2. O **ataque cibernético** muitas vezes envolve a coleta de informações com motivação política, pirataria digital ou roubo de segredos comerciais, tecnologias e patentes.
3. O **terrorismo cibernético** tem como objetivo minar sistemas eletrônicos para causar pânico, medo ou derrubar serviços essenciais ou não.

Apresentação de Slides sobre o conteúdo citado.

Os Provedores e suas associações

Os provedores de internet nos últimos anos tem tido papel importante nas soluções desses 3 casos e será nessa defesa minhas argumentações e considerações.

E fato que todos os casos de cibersegurança e ameaças citadas acima passam pela rede de IPs dos provedores de internet e operadoras de grande porte.

E em razão desse fato que as associações de provedores como **Abramulti, Abrint, Abranet, Apims, Apronet, Redetelesul, Internetsul, Probahia, Neotv e o Lacnic,** participam desde 18/12/2019 de um grupo de trabalho no WhatsApp denominado **“Provedores + CIBERLAB/MJSP.**

Esse grupo teve como um dos idealizadores nosso colega Breno Vale(Abrint) que nos representa também na CPPP e foi criado com a intenção de pedir ajuda ao CIBERLAB para investigar os ataques DDoS que estavam acontecendo em todo o país nas redes de ISPs.

Apartir dessa criação nascia ali um grande grupo de debate e apoio com opiniões diversas de ambos os lados da defesa em Liberar ou não Liberar dados de IP por CGNAT.

Todas as associações tiveram casos que interviram e ajudaram de forma totalmente amparada por ordem judicial e outros casos não, como posso falar por mim(Robson Lima) que fiz diversas ligações para provedores de todo o país onde convenci de forma bem embasada a liberação dos dados de clientes que usaram o determinado IP com a regra de CGNAT, onde que ocorreu por troca de email pelo agente ou delegado envolvido com o provedor e foi feito por processo investigativo e eliminatório para eliminar os dados dos clientes passados e ficando somente o do suspeito real.

Como resultado, ajudamos de forma sigilosa a prender diversos suspeitos de **pedofilia, homicídio, feminicídio** no país sem causar nenhum dano ao provedor que cedeu as informações.

Tivemos no segundo semestre de 2020 a prisão dos dois principais Crakers(Hacker criminoso) vulgo codinome Guerreiro e Topiary que se apura ter gerado prejuízo que ultrapassa **10 milhões de reais em danos e extorsão por moeda digital**, segundo informação do CIBERLAB através de uma campanha realizada pelas associações para denuncia de provedores que foram extorquidos passa de 100 ISPs que apresentaram “Boletim de Ocorrência”.

Temos que dar os parabéns a equipe que participou das investigações que em razão da falta de conhecimento do Juiz responsável da época não apenas negou as tais “Quebra de Sigilo”, como também induziu ao encerramento das investigações, eles jamais teriam sido identificados e presos se a CIBERLAB não tivesse tido acesso ao mínimo de informações que damos as felicitações as associações conjuntas que muniram ao máximo delas para chegar a identificação e prisão.

A frase que mais e citada nas reuniões que temos e auxilio a equipe CIBERLAB é “Os Provedores de Internet são a maior conquista e parceiros que o CIBERLAB conquistou”.

A abramulti em reconhecimento aos trabalhos prestados pela CIBERLAB fez a doação de vários Notebooks e HDs externos, pois descobrimos que as delegacias que participaram de toda a investigação tinham equipamentos precários.

Através desse ato o delegado chefe do CIBERLAB, me ligou agradecendo as doações e me informou que a CIBERLAB necessitava de muito mais que eletrônicos, precisava de apoio dos órgãos e instituições e também de capacitação dos agentes, a abramulti se mostrou solidaria a causa e sugeriu desenvolver um grande Congresso de Cibersegurança em Brasília e buscar junto a órgãos, instituições e consultores especialistas para capacitar os agentes.

Em dezembro com participação de associações (Abramulti e Internetsul) fizemos uma visita a vários ministérios e em especial ao MCTI(Ministério de Ciências e Tecnologia e Inovação), do Ministro Marcos Pontes onde foi apresentado o projeto do Congresso, e o ministro gostou muito e sugeriu a participação do MCTI no projeto, e designou seu Diretor José Gontijo para para fazer parte da comissão de criação do Congresso.

Foram convidados inicialmente para a comissão **NIC.BR, CGI, MCTI.**

No dia 14.01 em São Paulo na sede do NIC.br a abramulti organizou sua primeira reunião para discutir sobre o congresso com as participações:

NIC.br
Antônio Moreiras
Eduardo
Cristina Hoepers
Klaus Steding

CGI

Rosauro Baretta

CIBERLAB
Delegado Chefe do Ciberlab Alesandro Barreto
Agente Adriano Dedavid
MCTI
Diretor José Gontijo

Abramulti
Presidente Robson Lima
Vice presidente Jony Cruz

Internetsul
Presidente Ivonei Lopes

Ficou definido que o NIC.br irá adequar alguns cursos online e capacitar diversos Agentes, delegados e especialistas de forças policiais para elaborar um grande exercito de combate ao CIBERCRIME e após o inicio dos treinamentos no inicio do segundo semestre está sendo definido o congresso que irá acontecer em Brasília com palestrantes que serão convidados de toda a parte do mundo.

https://www.telesintese.com.br/governo-abramulti-e-nic-br-vao-treinar-policiais-no-combate-ao-cibercrime/

CONSIDERAÇÕES FINAIS

Como citado nos casos de **ameaças virtuais** temos a primeira **"Crime Virtual"**, os casos citados como os dos crackers de codinome **Guerreiro e Topiary.**

O ataque cibernético que temos como exemplo os ataques ao TSE no período de eleição para prejudicar o processo eleitoral, onde lesou com muitas perdas de dados e e-mails de servidores públicos, mas os especialistas conseguiram minar o ataque.

E por final pra mim o de maior crescimento no mundo **terrorismo cibernético** que vem corrompendo sistemas eletrônicos de bancos, mídias sociais como Whatsapp, Instagram, e-commerce, entre outros. Esse ultimo tenho certeza que cada um dos colegas presentes deve ter tido ou parente ou amigo e conhecido próximo que sofreu esse crime.

À ANATEL

E sabido que quando do uso da tecnologia **CGNAT** por um provedor a única forma de um provedor individualizar o usuário e recebendo da autoridade solicitante o numero de IP com data e hora e também a porta logica, entretanto as autoridades policiais tem deixado claro que muitos provedores de conteúdo, principalmente de conteúdos internacionais não cumprem essa regra como por exemplo a gigante NETFLIX, ela nao fornece a porta logica apartir dai quando uma autoridade policial requisita o provedor de internet ou conexão os dados cadastrais do usuário daquela linha tanto a operadora quanto o provedor caem a uma quantidade superior a um individuo com essa utilização. E muitos operadoras e provedores que estão sim fornecendo essas informações tendo em vista a legislação não determinar especificamente o caso de um usuário e sim os dados cadastrais e quem irá fazer o filtro destas informações será a autoridade policial e a equipe de investigação pra poder apontar realmente a autoria que ela busca, então não se vê irregularidade nestas informações (Meu ponto de vista, através de vários trabalhos feitos com êxito com a CIBERLAB). Entretanto muitos provedores e operadoras também em um primeiro momento procuram não repassar esses dados, o que inviabiliza e interrompe a parte investigativa que não e culpa das autoridades policiais brasileiras mas sim dos provedores de conteúdo.
Então será que a solução do processo será a evolução do processo e a agilidade na migração do sistema IPV4 para o IPV6,até que isso ocorra a ANATEL em um primeiro momento poderia auxiliar na aproximação ao NIC.BR pra que houvesse um complice que diminuísse o numero de usuários

permitidos atrás de um processo de CGNAT, pra se chegar em um numero tecnicamente viável para os provedores e para as investigações e esse numero deixo a cargo dos colegas sugerir em nossa reunião mas conversando com a equipe CIBERLAB a sugestão seria um numero menor que 10.
Outra alternativa seria tanto a ANATEL quanto NIC.br estimular ainda mais as migrações entre IPV4 e IPV6,e a ANATEL se posicionar com relação ao fornecimento dos dados cadastrais de um CGNAT com relação ao provedor de conteúdo, por exemplo essa demonstração da dificuldade que se tem para a NETFLIX, estimulando as mesmas que fornecem os serviços no BRASIL se enquadrem no processo de legislação do Brasil onde já e pacifico o provedor de conteúdo ter que entregar a porta logica.

Pra encerramento podemos usar esse **RECURSO ESPECIAL** impetrado pela TIM contra a GOOGLE que o STJ pacificou, dizendo provedor de conteúdo tem que fornecer a porta logica por obrigação, sendo assim a TIM representando todos os provedores do Brasil.
Segue abaixo numero do recurso para conhecimento.

E na minha opinião e de extrema importância da participação de todos tanto publico e privado, pois assim sendo estaremos protegendo a **SOBERANIA NACIONAL** tanto da população quanto das instituições publico/privado.

Temos como ultima citação o trabalho junto a ANCINE no combate a pirataria audiovisual e identificação de provedores que usam esse tipo de serviço, um trabalho que demostra a importância da participação dos provedores e suas associações que os representa com os órgãos de diversos setores.

Superior Tribunal de Justiça

RECURSO ESPECIAL Nº 1.784.156 - SP (2018/0322140-0)

RELATOR	:	**MINISTRO MARCO AURÉLIO BELLIZZE**
RECORRENTE	:	TIM CELULAR S.A
ADVOGADOS	:	RENATO MULLER DA SILVA OPICE BLUM - SP138578 CAMILLA DO VALE JIMENE - SP222815 JULIANA ABRUSIO FLORÊNCIO - SP196280 CAMILA MACEDO MARTINS - SP285568 PAULA MARQUES RODRIGUES E OUTRO(S) - SP301179 RENATO GOMES DE MATTOS MALAFAIA - SP368020 ETTORE TARCISIO ZAMIDI - SP340260
RECORRIDO	:	GOOGLE BRASIL INTERNET LTDA
ADVOGADOS	:	CARLOS MÁRIO DA SILVA VELLOSO FILHO E OUTRO(S) - DF006534 EDUARDO LUIZ BROCK - SP091311 FABIO RIVELLI - SP297608 RENATA FERNANDES HANONES CARPANEDA E OUTRO(S) - DF039487 JOAO CARLOS BANHOS VELLOSO E OUTRO(S) - DF049000

EMENTA

RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR DE APLICAÇÕES. IDENTIFICAÇÃO DO DISPOSITIVO UTILIZADO PARA ACESSO À APLICAÇÃO. INDICAÇÃO DO ENDEREÇO IP E PORTA LÓGICA DE ORIGEM. INTERPRETAÇÃO TELEOLÓGICA DOS ARTS. 5º, VII, E 15 DA LEI N. 12.965/2014. RECURSO ESPECIAL PROVIDO.