SEGURANÇA, RISCOS E PROTEÇÃO DE DADOS

Giovanni Dias Santine[1], Ricardo Rall[2]

[1]Graduando em Análise e desenvolvimento de sistemas pela faculdade de tecnologia de Botucatu, FATEC, e-mail: giovanni.santine@fatec.sp.gov.br
[2]Professor Doutor de ensino superior pela faculdade de tecnologia de Botucatu, FATEC, e-mail: ricardo.rall@fatec.sp.gov.br

RESUMO

Atualmente, a tecnologia é muito usada na comunicação pessoal, para o trabalho e outras finalidades, mas não há grande preocupação com a segurança dos dados enviados ou recebidos. Mesmo sem perceber, muitas empresas sofrem ataques cibernéticos, deixando seus dados vulneráveis, sendo que essas falhas na segurança podem prejudicar a imagem da corporação. Assim, os funcionários das empresas que operam sistemas computacionais devem ser treinados e conscientizados sobre os reais perigos ocultos na internet e redes de computadores, em geral. O objetivo deste trabalho foi apresentar dados gerais sobre segurança (proteção física e virtual), levantar os principais incidentes de segurança digital, analisar e indicar meios de proteção de dados. Foram utilizados vários sites que reportam ataques, sendo o principal deles o Cert.br, que uma referência no Brasil na área. Pode-se concluir que os principais ataques são DNS malicioso, Incidentes, Honeyposts e Spam, sendo o incidente ou ataque do tipo Spam o que mais cresceu ultimamente, em 200%, havendo uma forte recomendação às pessoas e às empresas a instalação ou reforços nos recursos de *firewalls* e antivírus para combater este.

Palavras-chave: Ataques cibernéticos. Prevenção à riscos. Proteção de dados. Riscos. Segurança.

1 INTRODUÇÃO

O principal objetivo dos ataques cibernéticos é a coleta dados, como de sites de bancos, instituições financeiras, organizações médicas, etc., que podem ser vendidos para o mercado negro, ou para outras finalidades, as novas tecnologias e a integração entre elas trazem consigo novos pontos de ataque. Conforme a tecnologia evolui, a defesa da informação também deve evoluir.

De acordo com Furnell e Thomson (2009), um dos maiores problemas e ameaças verificados na implementação de práticas e procedimentos na segurança da informação são os usuários. Um estudo realizado em 2017 pela Norton Cyber Segurity Insights Report afirmou que o Brasil é o segundo em crimes cibernéticos, com 62 milhões de brasileiros vítimas desses crimes, o que representa 61% da população adulta conectada do país.

A segurança cibernética é um conjunto de técnicas que protegem as informações armazenadas nos computadores que são transmitidas pelas redes de comunicação, como a internet. Para que ocorra a proteção, as empresas devem, inicialmente, reconhecer uma ameaça ou uma invasão, seguida da análise de qual tipo de dado foi atacado e quais as

melhores ferramentas para resolver o caso. Com essas informações, deve ser montado um novo molde de segurança, acrescentado novas barreiras e, por último, deve ocorrer a execução dessa segurança, para evitar o invasor ou ameaça.

O objetivo deste trabalho foi apresentar dados gerais sobre segurança (proteção física e virtual), levantar os principais incidentes de segurança digital, analisar e indicar meios de proteção de dados, no sentido de orientar as pessoas e empresas a se defenderem contra estes.

2 MATERIAL E MÉTODOS

Esse trabalho foi realizado a partir de levantamento de dados de vários sites de monitoramento de ataques cibernéticos, tendo como principal o CERT.br, que é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil.

Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

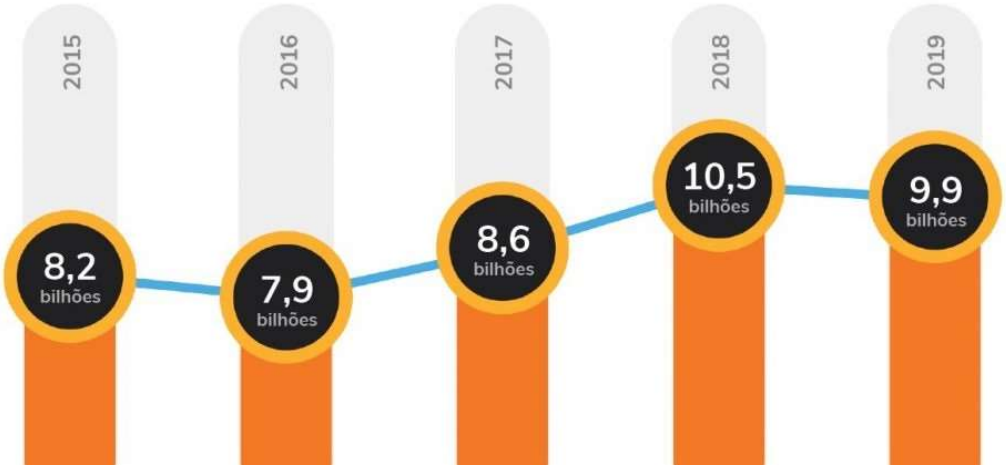
Além do processo de tratamento a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CSIRTs no Brasil.

Estas atividades têm como objetivo estratégico aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

3 RESULTADOS E DISCUSSÃO

A partir das referências acessadas, pode-se observar na Figura 1, quantas ocorrências de ataques cibernéticos aconteceram no mundo, até 2019 (SonicWall, 2020).

Figura 1- Variância de ataques anuais



FONTE: INFOMACH (2020)

Segundo esses dados, vem aumentando o número de ataques, esperando-se um aumento significativo de ataques cibernéticos até o final de 2020, principalmente no Brasil, pois segundo os dados da Apura (empresa especializada em Segurança cibernética), o levantamento mostra que há 1.002.688 sites todos encontrados com as palavras “coronavírus” e “covid” no domínio que são suspeitos de aplicar golpes, desde o início da pandemia, no mês de março até agora devido à liberação do auxílio emergencial e do adiantamento do FGTS, publicado no site Metrópoles. devido à pandemia de COVID-19, sendo que muitas pessoas já perderam esse auxílio devido a esses ataques. Muitos se sentem seguros para usar a internet, redes sociais, etc. mas, segundo HARÁN (2018), muitos usuários não têm ciência dos riscos da superexposição em redes sociais e compartilham dados pessoais, como número de documentos, data de nascimento, endereço residencial e vários outros. É importante configurar de forma adequada a privacidade de cada uma das plataformas que se usa, não expondo ao público as atividades pessoais de cada um, diariamente.

3.1 Como se prevenir de ataques na internet

Diante do grande número de vítimas de fraudes, levanta-se a questão do responsável pela segurança do consumidor, em relação a possíveis golpes. Segundo o presidente da Confederação Nacional de Dirigentes Lojistas (CNDL), José César da Costa, essa deve ser uma preocupação tanto da sociedade quanto das organizações públicas e privadas. Em relação ao perfil das vítimas, Costa ainda chamou atenção para um ponto importante: os consumidores com mais idade são os mais propensos às fraudes na internet e, por isso, precisam estar ainda mais atentos aos hábitos de compra na web.

3.2 Consequências de ser vítima de fraudes digitais

Uma vítima desse tipo de golpe pode ter consequências bastante graves, como cobrança de dívidas que foram feitas em seu nome, além de multas, dificuldade de acesso a alguns serviços, pois seu nome estará em instituições como a Centralização de Serviços dos Bancos (SERASA), empresa privada brasileira, que reúne informações sobre pessoas físicas e jurídicas que estão com dívidas financeiras (Serasa, 2020). "sujo", gastos com processos e com advogados para defesa. Deve ser ressaltado que não só pessoas físicas podem sofrer com isso, empresas grandes também podem ser vulneráveis. De acordo com estudos da Gemalto, em 2014 foram roubados mais de 1 bilhão de registros devido às brechas de segurança de dados, no mundo e as vítimas foram empresas de varejo e de tecnologia, governos, instituições financeiras e pessoas físicas. Em 2015, esse número foi de quase 708 milhões registrados, aproximadamente 22 registros roubados por segundo.

3.3 Cuidados necessários

Com a tecnologia que se tem atualmente, é difícil não utilizar algumas facilidades como o armazenamento de informações na nuvem, ou realizar compras pela internet. No entanto, providências devem ser tomadas para se evitar ataques cibernéticos.

O primeiro alerta é nunca armazenar informações importantes como senhas de sites, dados de contas bancárias (número de conta e senhas) e dados de cartão de crédito na nuvem ou enviá-las por e-mail ou redes sociais. O segundo alerta é que caso seja necessário enviar ou armazenar documentos e dados, os mesmos devem ser criptografados com senha, que deve ser repassada por outro meio de comunicação, à uma pessoa ou empresa confiável. O terceiro alerta seria não utilizar conexões inseguras como de wi-fi grátis para acessar aplicativos pessoais, como internet Bank e nunca utilizar senhas óbvias como nomes, sobrenomes, datas de aniversário, etc.

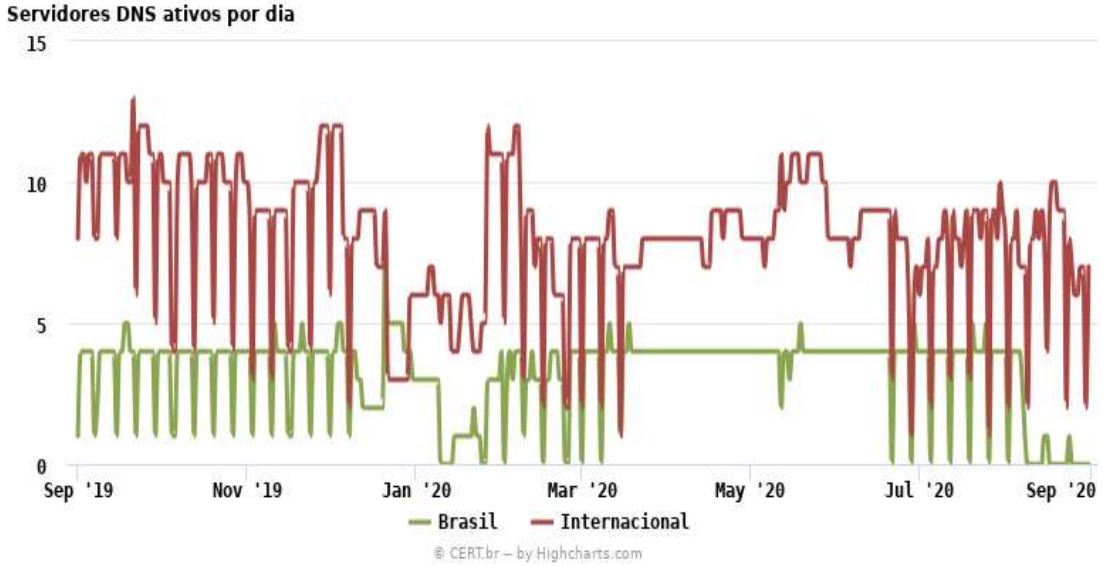
3.4 Os principais tipos de golpes na internet

A partir dos dados fornecidos pelo Cert, pode-se afirmar que principais técnicas aplicadas são DNS malicioso, Incidentes, Honeyposts e Spam. Estes serão descritos a seguir.

3.4.1 Servidor DNS malicioso

É um servidor que está fornecendo respostas incorretas para nome(s) de domínio(s) de instituições vítimas. O proposito desses servidores é direcionar os usuários para sites falsos como sites clone dos originais. Na Figura 2 pode-se observar as estatísticas dos servidores DNS maliciosos no Brasil e internacionais, onde se percebe um comportamento similar e proporcional entre os dois tipos.

Figura 2 - Servidores DNS fornecendo respostas incorretas para nomes de domínio de terceiros



Fonte: Cert(2020)

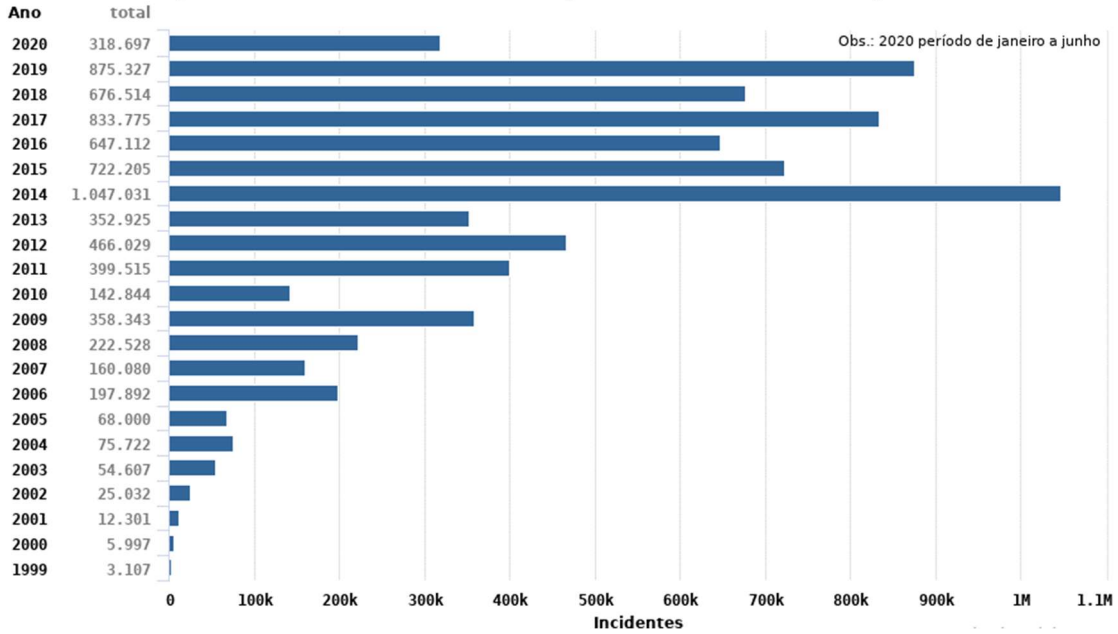
3.4.2 Estatísticas dos incidentes reportados ao cert.br

Um incidente de segurança é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação e Comunicações da empresa.

São exemplos de incidentes de segurança da informação: furto de equipamentos que contenham informações institucionais, vazamento de informações não públicas (considerar que esta propriedade pode variar durante o ciclo de vida da informação), e-mails enviados sem autorização do remetente a partir do e-mail institucional ou pessoal, e-mails suspeitos não classificados como SPAM que principalmente tenham por finalidade coletar informações pessoais e especialmente credenciais do sistemas das empresas, comprometimento da integridade da informação, perda de informações institucionais, etc.

Pode-se perceber, a partir da Figura 3, que as quantidades de incidentes variam ano a ano e não revelam nenhuma tendência nem de crescimento ou de queda, apenas um destaque para o ano de 2014, com mais de 1 milhão de incidentes.

Figura 3-Total de incidentes reportados ao CERT.br por ano



Fonte: Cert(2020)

3.4.3 Honeypots

O CERT.br mantém o Projeto Honeypot*s* Distribuídos, uma rede distribuída de honeypots de baixa interatividade em endereços IP da Internet no Brasil. Este projeto tem o objetivo de aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no Brasil. Os Honeypots tornam-se atrativos para os criminosos ao construírem vulnerabilidades de segurança deliberadas. Por exemplo, um honeypot pode ter portas que respondem a uma varredura de porta ou senhas fracas. Portas vulneráveis podem ser deixadas abertas para atrair criminosos para o ambiente do honeypot, em vez da rede ao vivo mais segura.

3.4.4 SPAM

Na prática, segundo Alencar (2020), o SPAM é uma mensagem eletrônica que chega ao usuário sem a sua permissão ou sem seu desejo em recebê-lo. Geralmente são recebidas por e-mail, mas também podem circular pelas redes sociais ou comentários de blogs. Na maioria dos casos, a mensagem de SPAM promove algum produto ou serviço. Mas, em outras situações, ele tem o objetivo simplesmente de difundir histórias falsas, conhecidas como “hoax” ou conseguir os dados financeiros e pessoais dos usuários.

3.5 Onde denunciar os golpes cibernéticos

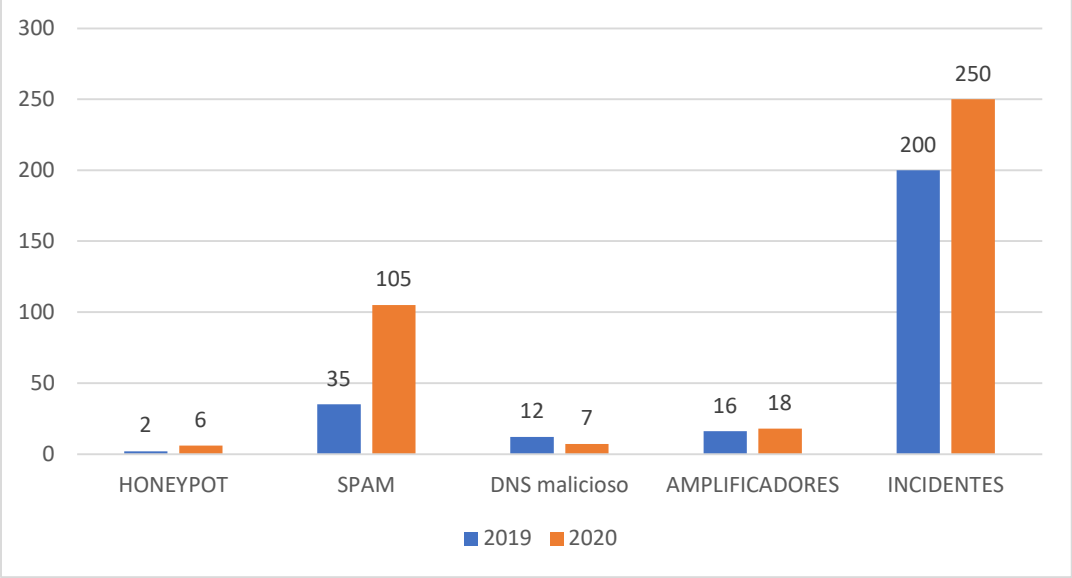
Em caso de suspeita de tentativa de golpe na internet, o usuário pode denuncia-lo para a Rede Nacional de Ensino e Pesquisa (RNP), que recebe denúncias de fraudes eletrônicas sobre links maliciosos e páginas de falsas instituições, através dos endereços

"artefatos@cais.rnp.br" ou phishing@cais.rnp.br. A denúncia também pode ser realizada no Centro de Atendimento a Incidentes de Segurança (CAIS) ou pelo CERT.br, que também recebe denúncias de golpes na internet através do e-mail "abuse@cert.br". Uma alternativa é a Polícia Federal, que tem uma divisão específica para tratar de golpes na internet e crimes virtuais, recebendo as denúncias pelo e-mail "internet@dpf.gov.br".

3.6 Comparativo dos tipos de ataque

De acordo com os dados de todas as pesquisas e as tabelas analisadas para elaboração deste trabalho, a partir de uma base de dados de 2020, os ataques em geral aumentaram neste ano. Na Figura 5 tem-se dados de 2019 obtidos do CERT.br e uma estimativa de como serão esses dados no decorrer de 2020, onde apenas o ataque de DNS malicioso decaiu e o ataque do tipo SPAM teve um crescimento bem destacado em 200%, aproximadamente.

Figura 4- Gráfico estatístico de golpes cibernéticos, escala em milhões



Fonte: Cert(2020)

4 CONCLUSÕES

Com o grande avanço da tecnologia também há um grande avanço dos crimes digitais, neste ano pode-se observar a diferença entre as quantidades de ataques feitos referente ao ano passado e anteriores.

O levantamento revelou um grande crescimento dos ataques do tipo Spam, onde se tem os e-mails e seus anexos como principal veículo de atuação deste tipo de golpe de envio de mensagens em massa, reforçando as recomendações às pessoas e às empresas que uma boa frente de como combater Spam é o uso de firewalls e anti-vírus, responsáveis pelo monitoramento de todo o tráfego de dados (entrada e saída). Por meio deles, ocorre

a liberação ou bloqueio de acessos específicos de acordo com a definição de normas internas de segurança da organização.

Os riscos da utilização da tecnologia sempre estarão presentes, sendo tarefa de todos, a adoção de condutas preventivas, quanto ao envio e recepção de dados, pois a maior parte da população utiliza a internet de forma imprudente.

REFERÊNCIAS

ALENCAR, Felipe. O que é spam? **Techtudo.** Disponível em: https://www.techtudo.com.br/noticias/noticia/2016/07/o-que-e-spam.html . Acesso em: 17 set. 2020.

CERT. Sobre o Cert.br., **Cert**. Disponível em: http://cert.br/stats. Acesso em: 03 set. 2020.

FURNELL, Steven; THOMSON, Kerry-Lynn. From culture to disobedience: Recognising the varying user acceptance of IT security. **Computer Fraud & Security,** v. 2009, n. 2, p. 5-10. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1361372309700193?via%3Dihub. Acesso em: 07 set. 2020.

HARÁN, Juan Manuel. Fraudes na Internet. W**elivesecurity,** v. 2018. Disponível em: <https://www.welivesecurity.com/br/2018/11/30/fraudes-na-internet-8-sinais-que-indicam-que-voce-e-um-alvo-facil/>. Acesso em: 07 set. 2020.

MARQUES, Flávia. Fraudes na internet despertam desconfiança do consumidor brasileiro. **Exponencial,** v. 2019. Disponível em: <https://www.creditas.com/exponencial/fraudes-na-internet/>. Acesso em: 12 set. 2020.

SATO, William Hiroshi. Fraudes na internet: sua saúde financeira em risco. **Dinheirama** v. 2020. Disponível em: <https://dinheirama.com/fraudes-internet-risco/>. Acesso em: 14 set. 2020.

OLIVEIRA NETO, Jose Alfredo de. Onde denunciar golpes na internet. **Meu direito.** Disponível em: <https://meudireito.com.br/golpes-internet-denuncia/#:~:text=Outra%20alternativa%20%C3%A9%20a%20pr%C3%B3pria,%40dpf.gov.br>. Acesso em: 12 set. 2020.

SCHUQUEL, Thayná. Brasil é o país com mais ataques cibernéticos no mundo. Como se proteger? **Metrópoles.** Disponível em: <https://www.metropoles.com/brasil/brasil-e-o-pais-com-mais-ataques-ciberneticos-no-mundo-como-se-proteger>. Acesso em: 17 set. 2020.

SERASA. Centralização de Serviços dos Bancos (SERASA). Disponível em: <https://www.serasa.com.br/limpa-nome-online/>. Acesso em: 16 set. 2020.