CIBERATAQUES NA ÁREA DE SAÚDE

Informativo SPDM

Elaborado por:
TECNOLOGIA DA INFORMAÇÃO SPDM

A LGPD (Lei Geral de Proteção de Dados - Lei 13.709/2018) caminha a passos largos para sua consolidação na vida de todos e está cada vez mais presente, na forma de uma realidade imutável, assume um papel preponderante na estruturação de empresas, instituições e praticamente tudo na atividade humana, que envolva algum tipo de informação pessoal.

Na área de saúde, mais especificamente, os fluxos de dados sensíveis são constantes, o que expõe o setor a vulnerabilidades críticas e perigosas, para todos os personagens.

No conceito, dados sensíveis são diferentes de dados pessoais, sendo que os dados sensíveis podem causar um grande prejuízo a privacidade, exemplo destes dados de acordo com a lei: origem racial ou étnica, convicção religiosa, opinião política, dado referente à saúde, dado genético e biométrico, entre outros. Por terem essas características, em uma situação de vazamento, podem causar danos quase irreparáveis às vítimas, impactando diretamente sua vida pessoal.

O mundo todo é ameaçado por vazamentos e atividades *hackers* que possuem potencial de expor dados pessoais e sensíveis .

SETOR DE SAÚDE EM FOCO

Uma consultoria especializada em cibersegurança que atende vários players americanos informou que as estruturas monitoradas sofreram um aumento de 51% de ataques, comparando com 2019.

A diretoria técnica da consultoria afirma que a pandemia serviu para demonstrar a imensa fragilidade da infraestrutura e políticas de segurança de dados nos serviços de saúde.

Entre 2020 e 2021, aqui no Brasil, se empilharam casos de vazamentos reais de dados importantes e sensíveis de milhões de pessoas através dos mecanismos projetados e aplicados “a toque de caixa” pelas instituições governamentais e empresas privadas do segmento de saúde.

O ano de 2021 foi marcado pelo crescimento dos incidentes digitais, em um levantamento feito por uma empresa brasileira de cibersegurança, foi apontado que o setor de Saúde foi justamente o mais afetado.

O relatório registra que, desde janeiro, hospitais, clínicas e outras instituições voltadas à área, tanto no setor privado como no público, registraram mais de 39 mil alertas de tentativas de ciberataques.

Veja o ranking:

Setores Afetados	Nº Alertas	% Alertas
Saúde	39.399	26,5%
Indústria/produção	36.615	24,6%
Instituições financeiras	25.370	17,1%
Varejo/mercados	19.698	13,2%
Educação	17.265	11,6%
Setor público	9.893	6,6%

CASOS DE CIBERATAQUES

O setor de saúde é um dos primeiros a sofrer consequências dos vazamentos de dados e sanções da LGPD. Os exemplos saltam aos olhos o tempo todo, até porque, viram notícia imediatamente.

Recentemente, os sistemas de informação do Governo Federal dos órgãos ligados ao segmento da Saúde foram invadidos através de um ataque cibernético que deixou parte de seus principais sistemas fora do ar, como o próprio CONECTSUS, (caminho básico para, entre outras funções, fornecer ao cidadão o histórico e comprovação de sua situação vacinal).

O objetivo é pedir resgate para recompor os dados ali criptografados e, portanto, inúteis ao proprietário da base.

Este tipo de processo recebe o nome de *ransomware* e é bem comum como um "negócio" ilícito no universo virtual.

Em raros casos, o *hacker* não criptografa os dados, mas simplesmente apaga, deleta, oferecendo mediante extorsão, a devolução das informações.
A forma de pagamento destes valores resultantes dos sequestros costuma ser a criptomoeda, por não ser rastreável.

No caso do referido ataque foi percebido quando as pessoas entravam nos sistemas ou aplicativos e, ao invés de acessar as informações, encontravam apenas uma mensagem dizendo:

No início da manhã do dia posterior ao ataque as mensagens tinham sido excluídas pelos técnicos do Governo, mas os portais continuavam sem operação e fora do ar.

Segundo informações do próprio Governo, vários outros sistemas também sofreram algum tipo de comprometimento e o caso estava aos cuidados da Polícia Federal e do Gabinete de Segurança Institucional da Presidência da República.

Na madrugada seguinte o grupo *hacker* denominado de LAPSUS$ assumiu a autoria do ataque e confirmou a utilização de *ransomware*.

No mesmo dia do ataque o Governo se apressou em dar ampla divulgação que possuía backup completo de tudo que foi alvo do ataque.

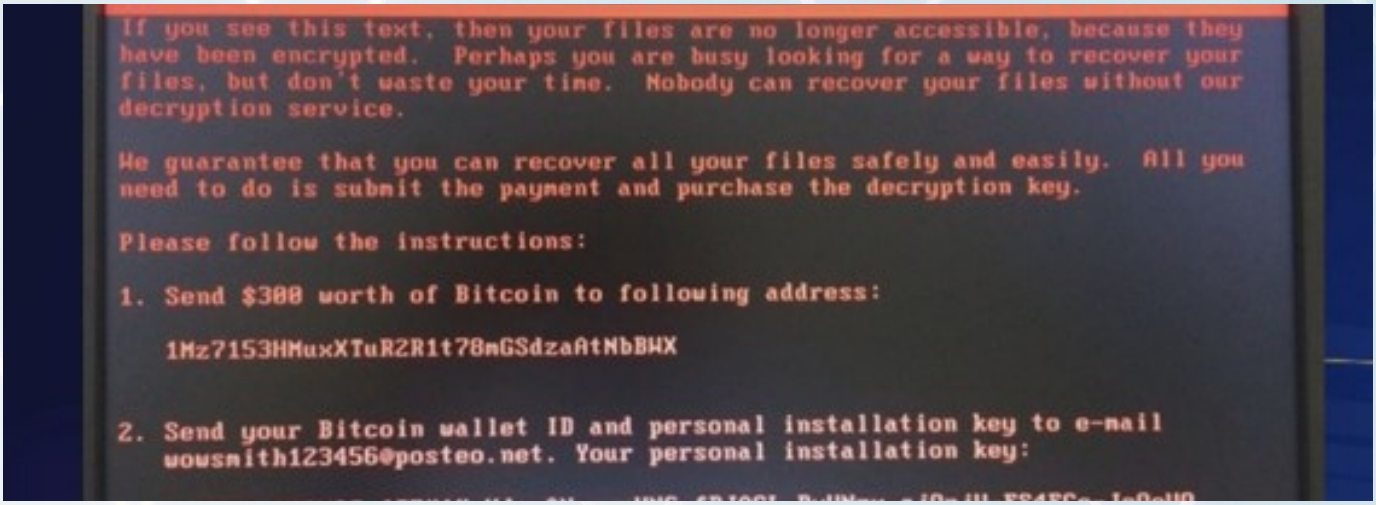
O Secretário Executivo da pasta procurou demonstrar tranquilidade, informando que não se trata de um sistema de prateleira, "o sistema foi excluído e quando o sistema é excluído, precisa reconstruí-lo, porque ele é personalizado e feito especificamente para o Ministério da Saúde."

O Governo informou que o acesso *hacker* aconteceu a partir de uma credencial que deu acesso ao banco de dados.

Foram mais de 40 dias para restabelecer os sistemas e a maioria ainda funciona com inconsistências e falhas, prejudicando a emissão de certificados de vacinação, tão importantes nos dias atuais.

OUTROS CASOS NA ÁREA DA SAÚDE

Em outro fato, no ano de 2017, data pretérita a existência da LGPD, um Hospital no interior de São Paulo também sofreu um ataque e o impacto disso foi a suspensão de 3000 consultas. Os *hackers* pediram o resgate das informações em criptomoedas, vez que estas não são rastreáveis.



Em nota, o Hospital informou que o ataque foi identificado por volta de 9h e prejudicou, inclusive, os aparelhos usados na terapia radioativa. As sessões de terapia radioativa foram canceladas.

Em nota o Hospital informou que após 6 dias as operações de atendimento voltaram ao normal para o público em geral.

RESPONSABILIDADE NO TRATAMENTO DOS DADOS

A LGPD prevê uma seção especial para as infrações e multas, que poderão ser aplicadas a todas as empresas, públicas ou privadas ou mesmo a pessoas físicas que tratam dados pessoais, caso essas não cumprirem as diretrizes previstas em lei. Desde 1º de agosto de 2021 passaram a valer as multas e punições previstas pela LGPD e estas penalidades podem chegar a R$ 50 milhões por infração.

A fiscalização e a regulação da LGPD ficarão a cargo da Autoridade Nacional de Proteção de Dados Pessoais (ANPD). A autoridade será ainda um elo entre sociedade e governo, permitindo que as pessoas enviem dúvidas, sugestões e denúncias ligadas à LGPD para apuração.

A ANPD também tem um importante papel de orientar e apoiar as instituições públicas e privadas em relação às situações que envolvam o tratamento de dados pessoais.

Conforme o art. 52 da LGPD, a ANPD pode aplicar as seguintes sanções administrativas:

·Advertência, com indicação de prazo para adoção de medidas corretivas;

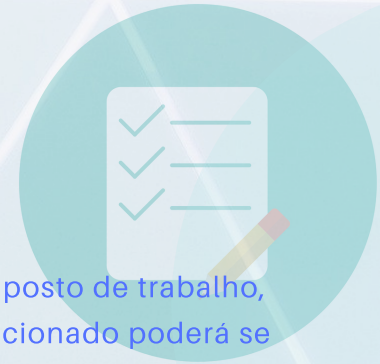
·Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

·Multa diária, observado o limite total a que se refere o inciso II;

·Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
·Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
·Eliminação dos dados pessoais a que se refere a infração;
·Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
·Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
·Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A SPDM vem realizando uma série de ações voltadas à adequação da LGPD e segurança da informação, dentre as ações está a criação de setores específicos para os temas de segurança e privacidade, responsáveis pela implementação de ferramentas que dão visibilidade do ambiente de maneira ampla e confiável, além de auxiliar no projeto de adequação a LGPD como um todo. Estes setores têm trabalhado no desenvolvimento de políticas e processos, visando a confidencialidade, integridade e disponibilidade dos serviços e ativos da instituição, além de ações que visão a conscientização de todos quanto ao melhor uso dos recursos e a proteção dos dados pessoais.

RECOMENDAÇÕES



- **BLOQUEAR o computador sempre que se ausentar**. Ao sair do seu posto de trabalho, evite deixar o seu computador desbloqueado, pois alguém mal-intencionado poderá se aproveitar do descuidado e prejudicar o seu projeto alterando dados ou até mesmo coletando dados importantes gerando um impacto negativo na instituição.

- **NUNCA clique em links inseguros**. Ao receber mensagens de spam contendo links de sites desconhecidos, não clique, pois ele irá realizar um download e o mesmo ser iniciado, infectando a sua estação de trabalho.

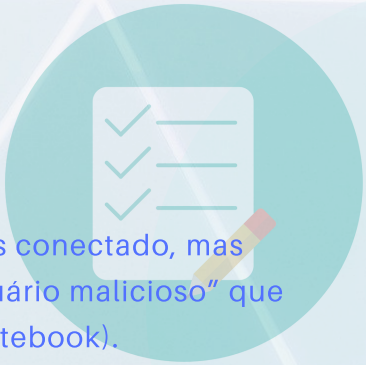
- **EVITE a divulgação de informações pessoais**. Se você receber uma chamada, mensagem de texto ou e-mail de uma fonte não confiável solicitando informações pessoais, não responda. Os cibercriminosos que estão planejando um ataque de *ransomware* podem tentar coletar informações pessoais com antecedência para depois usá-las para personalizar mensagens de *phishing* (técnica de engenharia social usada para enganar usuários e obter informações confidenciais) especificamente para você. Em caso de dúvida sobre a legitimidade da mensagem, entre em contato diretamente com o remetente por outro meio de comunicação, como por exemplo por ligação.

- **NÃO abra anexos de e-mail suspeitos**. O ransomware também pode entrar em seu dispositivo por meio de anexos de e-mail. Evite abrir qualquer anexo de aparência duvidosa. Para ter certeza de que o e-mail é confiável, preste muita atenção ao remetente e verifique se o endereço está correto. Nunca abra anexos que pedem para habilitar macros para serem visualizados. Se o anexo estiver infectado e for aberto, a macro maliciosa será executada e o malware obterá o controle sobre seu computador.

- **Nunca** use pendrives USB ou HD Externo desconhecidos.

- **USE apenas fontes de download conhecidas**. Confie em sites verificados e confiáveis para fazer downloads, que podem ser reconhecidos por selos de confiança. **Certifique-se** de que a barra de endereço do navegador da página que você está visitando usa "https" em vez de "http". Um escudo ou símbolo de cadeado na barra de endereço também pode indicar que a página é segura. **Cuidado** também ao baixar qualquer coisa em seu dispositivo móvel. **Confie somente em aplicativos verificados** pela Google Play Store ou Apple App Store.

RECOMENDAÇÕES



- **EVITE utilizar redes públicas de Wi-fi**. Vivemos em um mundo mais conectado, mas devemos ter alguns cuidados. Neste tipo de rede podemos ter um "usuário malicioso" que poderá acessar o seu dispositivo (Smartphone / Tablet / Notebook).

- **NUNCA compartilhe seus dados de acesso.** Login e senha são dados de acesso pessoais e intransferíveis, portanto não devem ser compartilhados em nenhuma hipótese.

- **Dados de acesso devem ser armazenados em locais seguros**. Evite anotar em cadernos, agendas e outros documentos impressos que possam ser de fácil acesso por outras pessoas;

Referências

https://tecmasters.com.br/ministerio-da-saude-reestabelecimento-sistemas *(acessado em 10/02/2022)*

https://jovempan.com.br/noticias/brasil/hospital-de-cancer-de-barretos-volta-atender-normalmente-apos-ataque-virtual.html *(acessado em 10/02/2022)*

https://www.privacytech.com.br/vazamentos/hospital-no-df-e-condenado-por-nao-proteger-dados-de-pacientes,393656.jhtml *(acessado em 10/02/2022)*

healthcareitnews.com *(acessado em 10/02/2022)*

https://constellaintelligence.com (acessado em 10/02/2022)

https://tiinside.com.br/28/01/2022/ataques-ciberneticos-contra-redes-corporativas-aumentaram-50-no-final-de-2021/ *(acessado em 10/02/2022)*

https://www.epsjv.fiocruz.br/escola/profissionais/num/764 *(acessado em 10/02/2022)*

https://veja.abril.com.br/coluna/radar/saude-foi-o-setor-mais-afetado-por-tentativas-de-ciberataques-diz-ish/ *(acessado em 10/02/2022)*