

RESUMO EXECUTIVO

SEGURANÇA DE REDES NO CONTEXTO DA LEI GERAL DE PROTEÇÃO DE DADOS

Os desafios e oportunidades da adoção da nova lei de proteção de dados no Brasil e impactos de curto prazo para as empresas



O Brasil conta com quase 6,4 milhões de empresas, e segundo dados do SEBRAE, desse total, 99% são pequenas e médias empresas que passam também hoje por uma forte transformação digital como meio de melhorar sua competitividade.

Um estudo do IDC no Brasil aponta contudo, que 70% destas ainda enfrentam desafios sobre o tema digitalização, aonde a segurança da informação tem sido um dos principais entraves para passos ainda mais acelerados nesta jornada digital.

Neste sentido, e por força da [Lei Nº 13.709](#), mais conhecida como Lei Geral de Proteção de Dados, ou simplesmente LGPD, executivos e proprietários de empresas terão que usar este fato como catalizador, para não mais relegar segurança como uma tarefa secundária, uma vez que até Agosto de 2020, conforme estipulado pela [MP 869/18](#), todas as empresas brasileiras terão

de seguir as regras estabelecidas, ou estarão sujeitas a multas estabelecidas no que se refere a proteção de dados.

Porém, a LGPD como marco regulatório, por outro lado, certamente pode ser uma oportunidade para nossas empresas avançarem em seus processos de digitalização e com isto melhorar sua produtividade, reduzir custos e maximizar o retorno de seus investimentos em tecnologia.

Naturalmente, os diferentes recursos de segurança de redes não estão em nenhum momento explícitos como exigências na nova lei, porém, sabemos que no atual cenário de insegurança, muitos são fundamentais para implantar e manter a longo prazo elementos que atestem o compromisso da sua empresa com a integridade de dados de terceiros e este é o objetivo deste resumo executivo especial preparado pela SonicWall no Brasil.

Nos 3 primeiros meses de 2018 segundo o SonicWall Security Center foram identificados mais 3 milhões de ataques focados no sequestro de dados apenas no Estado de São Paulo

Segundo a LGPD as empresas "devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Para isto sabemos que um dos maiores desafios ainda reside no tráfego de dados e na comunicação através de inúmeros dispositivos e aplicações que agora residem não apenas dentro do perímetro corporativo, que há muito se estendeu para nuvens, data centers, dispositivos IoT e diferentes sabores de dispositivos móveis.

E os desafios não são simples quando falamos de segurança de redes. Em 2018, dados da SonicWall, apontavam que, apenas em São Paulo, foram identificados 3 milhões de ataques de ransomware. Porém o pagamento do ransomware não é o maior mal, pois no final, o que se demonstra é a incapacidade que as empresas ainda têm em lidar com aspectos culturais ou mesmo entender a fragilidade de sua infraestrutura, tudo isto vai além da compra de firewalls, recursos avançados de proteção de endpoints, sandbox para tratar ameaças persistentes ou de dia zero (zero day), etc.

Isto vai requerer das empresas um pensamento sistemático em como colocar segurança como um desafio diário, assumindo-se o quadro que no mundo, não existe uma empresa blindada 100% contra ataques e ameaças avançadas.

Como, então, evitar esse quadro?

No contexto atual de insegurança, é necessário adotar uma abordagem e soluções de segurança de rede que utilizem recursos de inteligência artificial e aprendizado de máquina. Essa visão proporciona mais eficácia e comprovadamente, ainda proporciona importantes reduções de custos.

Recursos como estes proporcionam monitoramento e visibilidade de tráfego em tempo real contra ameaças e, também, definem vereditos sobre potenciais ameaças Zero Day.

Isso contribui para manter-se em conformidade com a LGPD, de modo a entregar segurança em todas as instâncias do ambiente digital. Isso vale para qualquer veículo de acesso ou tráfego de dados (e-mail, navegadores, aplicações, arquivos, e até a memória e processadores de computadores).

Essa mesma inteligência contra o cyber crime tem de validar tanto o tráfego



aberto como o criptografado, além de atuar em todas as estruturas de conectividade (cabado, sem fio, móvel ou remoto). A tecnologia deve, ainda, oferecer recursos integrados, capazes de promover a segurança dos mais diversos dispositivos, quer seja um PC ou Servidor, ou tablets, smartphones e dispositivos IoT.

A SonicWall acredita que a abordagem automatizada de prevenção contra violações em tempo real seja chave para atender aos requisitos da LGPD, mas sobre tudo manter a longo prazo o que é requerido de uma forma simples e econômica para garantir que os dados pessoais sejam protegidos pelas empresas, não importa o seu porte, ou segmento.

Como a SonicWall pode ajudar você?

Para isto, a SonicWall mantém inovador portfolio de soluções de segurança de rede através dos seus:

- Firewalls de Próxima Geração com diferentes recursos de análise contra intrusões, análise em tempo real de tráfego SSL/TSL, Sandbox contra ameaças persistentes e avançadas e muito mais.
- Pontos acesso sem fio de alto desempenho com os mesmos recursos de segurança de redes cabeadas.
- Segurança de acesso remoto através de VPNs seguras.
- Segurança para acesso à aplicações em nuvem.
- Segurança para dispositivos móveis e IoT.
- Segurança de e-mail com recursos integrados de sandboxing e Dmark
- Segurança de endpoints com possibilidade rollback e completamente integrados.
- Analisadores de risco em tempo real.
- Arquitetura de gestão e análise em diferentes modalidades.

Ou seja, estes diferentes elementos caminham e avançam de maneira integrada para a SonicWall, por acreditarmos que o sincronismo destes elementos, num primeiro fundamento é garantia de mais segurança e segundo e

igualmente importante no contexto das empresas brasileiras, um enorme potencial de redução de custo de propriedade.

Custo Total de Propriedade (TCO)

O desafio final é equacionar a matemática dos investimentos que levarão à conformidade com a LGPD. Isso vale tanto para quem opta comprar e manter com suas próprias equipes os recursos de segurança de redes como aquelas empresas que decidem terceirizar todo o aparato de segurança.

O cálculo de custo/benefício de uma plataforma de segurança de rede como sabemos vai muito além do preço nominal de solução (seja software, uma assinatura de serviços ou hardware). É fundamental estimar projeções de médio e longo prazo e pensar no custo total de propriedade, do inglês TCO (Total Cost of Ownership).

Isso envolve contabilizar custos de manutenção, despesas com a implementação da solução e capacitação dos profissionais e funcionários, além de gastos com a renovação de serviços.

É também por isto que a SonicWall sempre manteve um portfolio de soluções escalável, recursos economicos em nuvem e uma arquitetura base vinculada ao seu sistema operacional única para que os diferentes elementos possam interagir e com isto proporcionar redução de custos.

Mudança de atitude é a chave do sucesso

Nada disso trará resultados se os gestores das empresa não se empenharem em transformar os hábitos e o entendimento de seus funcionários e colaboradores.

Nós na SonicWall, acreditamos que essencialmente a chegada da Lei Geral de Proteção de Dados e também da instituição da Política Nacional de Segurança da Informação - PNSI são avanços importantes e oportunidades para todos empresários avançarem na tratativa de seus dados internos e de seus clientes e provedores.

A LGPD nada mais é do que um incentivo a mais para que essa transformação aconteça, e aconteça logo.

Equacionar todos os elementos que compõem este caminho em direção a LGPD sem dúvida trará desafios, mas sobre tudo oportunidades para todas as empresas, aonde os diferentes componentes de segurança de redes são chave em uma perspectiva de curto, médio e longo prazos.

© 2019 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING,

BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About Us

SonicWall has been fighting the cyber-criminal industry for over 27 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 global businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.

Refer to our website for additional information.

www.sonicwall.com