CHECKLIST

Proteção de dados moderna para LGPD

As exigências extensivas e as multas substanciais da Lei Geral de Proteção de Dados (LGPD) chamaram a atenção dos diretores de segurança de TI de todo o país. Para as empresas que manipulam dados e que fazem negócios no Brasil, chegou a hora de reforçar os processos de segurança.

A adesão aos regulamentos da LGPD exige tecnologia de ponta para proteção abrangente de dados - e, em particular, prevenção e detecção avançada de ameaças - para minimizar a possibilidade de violação de dados. Segundo o Center for Internet Security (CIS), uma organização sem fins lucrativos, os ataques mais bem-sucedidos exploram a higiene cibernética deficiente.[1]

As empresas afetadas pela LGPD precisam se certificar de que possuem as tecnologias certas para proteger seus ambientes e detectar e mitigar violações de dados de maneira rápida e eficaz, o que começa com a implantação da arquitetura de segurança correta.

7 considerações e como a Fortinet pode ajudar

☑ Primeira Linha de Defesa.

A primeira linha de defesa contra intrusões direcionadas a informações pessoalmente identificáveis (PII) é um firewall de próxima geração (NGFW). Algumas das capacidades mais relevantes para as organizações afetadas pela LGPD incluem:

- Segurança multicamada que usa prevenção avançada contra ameaças para proteger toda a superfície de ataque - todos os dispositivos, usuários e aplicativos. Isso inclui os dispositivos da Internet das Coisas (IoT), muitos dos quais foram projetados com pouca atenção à segurança (o que explica por que as atualizações de patch são impossíveis de gerenciar neles), bem como o universo sempre crescente de software como serviço (SaaS) e outras soluções em nuvem.
- Processador de segurança de alto desempenho (SPU) para serviços na camada de aplicativos que protegem uma rede corporativa enquanto detectam violações de dados ocultas no tráfego SSL por meio do mecanismo de inspeção SSL mais rápido do setor.
- Visibilidade e gerenciamento através de painel de controle unificado para implantação simplificada e controles consistentes de políticas de segurança. Isso permite o compartilhamento em tempo real de informações de intrusão, o que acelera o tempo para detectar, neutralizar e interromper tentativas de violações de dados.
- Segmentação do tráfego de rede, que minimiza a amplitude e a profundidade das intrusões e minimiza a oportunidade do invasor de acessar dados protegidos.
- SD-WAN Segura, funcionalidade nativa para interconexão de escritórios por enlaces de baixo custo com visibilidade, priorização e proteção de aplicações em nuvem e/ou “on premises”.

Os FortiGate NGFWs da Fortinet são a solução perfeita para proteger uma rede contra intrusões e evitar violações de dados, e eles conquistaram reconhecimento em toda a indústria. O Gartner colocou a Fortinet no quadrante de “Líderes” em seu Magic Quadrant de 2018 para Firewalls de Rede Empresarial[2], e os firewalls FortiGate receberam uma classificação “Recomendado” pelo quinto ano consecutivo do teste do grupo NSS Labs NGFW.[3]

☑ Proteger o Endpoint.

Se os firewalls são a primeira linha de defesa, as soluções de segurança de endpoint são a ultima barreira. À medida que as redes corporativas suportam números crescentes - e diversos tipos - de endpoints, a tecnologia de ponta de segurança de endpoint torna-

se crucial para proteger informações pessoalmente identificáveis (PII) e outros dados. Apenas os sistemas tradicionais de antivírus e antimalware não são mais adequados. A solução FortiClient da Fortinet melhora a capacidade de uma organização de impedir a ocorrência de violações de dados e, além disso, de atender às exigências da LGPD no caso de uma violação. Recursos relevantes incluem:

- Proteção contra ameaças avançadas que podem levar a violações de dados. Especificamente, o monitoramento de memória permite que o FortiClient detecte e bloqueie ataques a vulnerabilidades de aplicativos não corrigidos.
- Integração nativa com a arquitetura de segurança da Fortinet, o Fortinet Security Fabric, para atualizações em tempo real sobre ameaças emergentes. Parar os ataques e impedir sua intrusão evita violações de dados muito antes que elas aconteçam.
- Visibilidade clara da segurança em endpoints em toda a empresa, bem como visibilidade de quaisquer vulnerabilidades detectadas na superfície de ataque da organização. As atualizações estão disponíveis por meio de alertas por e-mail e um painel de vulnerabilidades. A capacidade de gerenciar a segurança de endpoint em tempo real permite que as organizações respondam a ataques e impeçam e mitiguem suas intrusões de maneira mais rápida e eficaz.

Assim como o FortiGate NGFWs, o FortiClient obteve o reconhecimento da indústria, incluindo uma classificação “Recomendado” de 2017 da NSS Labs para soluções avançadas de proteção de endpoints.[4]

☑ Proteja Seu E-mail.

A segurança de email é crucial; um relatório recente aponta que um terço das violações envolveram phishing.[5] Para as empresas que tentam proteger suas redes e dados contra ataques cibernéticos, um Secure E-mail Gateway (SEG) ou gateway de e-mail seguro, é imprescindível. Um SEG sofisticado, o FortiMail da Fortinet bloqueia ransomware, phishing e outras ameaças a informações pessoalmente identificáveis (PII) usando:

- Tecnologia antispam de várias camadas que utiliza mais de 12 técnicas de inspeção de remetente, protocolo e conteúdo - de avaliações de IP e domínio a verificações de verificação de destinatário e estrutura de política de remetente (SPF) - para proteger a rede e os usuários contra e-mails em massa indesejados. Como eles geralmente incluem exploits incorporados para intrusão, as organizações podem pará-los antes de entrar em sua rede de e-mail.
- Recursos antimalware que combinam tecnologias estáticas e dinâmicas, incluindo técnicas de assinatura, heurísticas e comportamentais. O mesmo se aplica aqui; garantir que o malware não chegue às caixas de correio do usuário interrompe os ataques antes que eles entrem na sua rede.
- Um conjunto robusto de recursos de proteção de dados, incluindo prevenção de perda de dados, criptografia de e-mail e tecnologias de arquivamento de e-mail. Garantir que seus usuários não enviem dados confidenciais e privados, bem como criptografar e-mails com informações pessoalmente identificáveis (PII), é fundamental para qualquer organização que procure evitar violações de dados.

O FortiMail é reconhecido por sua excelente eficácia na detecção de ameaças. Por exemplo, depois de bloquear cerca de 750 diferentes ameaças novas e pouco conhecidas em um teste de laboratório, recebeu a certificação “Advanced Threat Defense” (ATD) [Defesa de Ameaça Avançada] da ICSA Labs.[6]

☑ Proteja Seus Aplicativos da Web.

Os hackers podem usar técnicas sofisticadas, como injeção de SQL, scripts entre sites, estouros de buffer e envenenamento de cookies, para transformar aplicativos da Web em um gateway de acesso. Proteger as informações pessoalmente identificáveis (PII) contra essas ameaças requer uma abordagem multicamadas para a segurança de aplicativos da web. Algumas das principais formas pelas quais os firewalls de aplicativos da Web FortiWeb permitem que as organizações se protejam contra intrusões maliciosas incluem:

- Várias camadas de tecnologia que identificam ameaças por meio de técnicas como análise de reputação de IP, proteção contra DDoS, validação de protocolo, exame de assinaturas de ataque, antivírus e recursos de prevenção contra perda de dados. Mais uma vez, interromper as intrusões antes que elas ocorram elimina a possibilidade de violações de dados.
- Um mecanismo de detecção baseado em comportamento que identifica de maneira inteligente qualquer ameaça que se afaste de padrões típicos de tráfego da web. Isso é particularmente importante na identificação de ameaças desconhecidas.

- Integração nativa no Fortinet Security Fabric, que permite atualizações regulares sobre ameaças emergentes e a capacidade de compartilhar informações sobre quaisquer explorações detectadas. Como discutido anteriormente, a higiene cibernética é um elemento fundamental em qualquer estratégia de prevenção e detecção de intrusões.

Como as outras soluções da Fortinet discutidas, o FortiWeb também recebeu uma classificação “Recomendado” da NSS Labs em seu Teste de Firewall de Aplicação da Web de 2017.[7]

☑ Gerenciamento e Relatório Abrangentes.

Em 2016, os ciber ataques que entraram com sucesso em uma rede corporativa tiveram, em média, 107 dias para causar estragos antes que a intrusão fosse detectada.[8] Reduzir o tempo que um intruso pode explorar a rede limita sua oportunidade de iniciar uma violação de dados. Assim, a velocidade com que uma organização pode detectar e mitigar intrusões é crucial para evitar a perda de dados.

Para reduzir efetivamente a oportunidade de um possível criminoso, uma organização deve garantir que todos os seus dispositivos de segurança estejam funcionando o tempo todo. Para isso, a Fortinet oferece um conjunto de produtos para gerenciamento de soluções de segurança - FortiManager, FortiAnalyzer, FortiSIEM e FortiCloud - que, quando combinados, centralizam o gerenciamento de dispositivos de segurança em toda a rede. Alguns de seus principais recursos incluem:

- Visibilidade simplificada na política de segurança e gerenciamento de dispositivos. O FortiManager permite que a equipe de operações de segurança e rede inicie e sincronize uma resposta coordenada a ameaças detectadas e gerencie políticas de segurança em todos os dispositivos Fortinet e soluções de terceiros que fazem parte do Fortinet Security Fabric. Ele também oferece a melhor escalabilidade do setor, gerenciando até 100.000 dispositivos Fortinet - não incluindo dispositivos de terceiros que fazem parte do Fortinet Security Fabric - através de um único painel de vidro. Aqui, a rápida resposta a incidentes é frequentemente crítica para interromper ou minimizar as violações de dados, o que é fundamental quando se trata de LGPD.
- Visibilidade centralizada de dados de registros e eventos de soluções de segurança em toda a empresa. O FortiAnalyzer recupera e verifica automaticamente os registros de segurança, notificando a equipe de segurança de TI por meio de painéis e alertas sempre que detectarem um sinal de comprometimento. Mais uma vez, a resposta rápida a incidentes é fundamental para o LGPD.
- Tecnologia analítica que agrega e correlaciona de forma cruzada informações de diversas fontes, como registros, métricas de desempenho e traps SNMP. O FortiSIEM descobre automaticamente, de forma dinâmica, sistemas físicos e virtuais conectados à rede e extrai informações sobre as configurações desses sistemas em um banco de dados de gerenciamento centralizado (CMDB). Por meio da correlação cruzada de dados de desempenho, eventos e registros em tempo real, o FortiSIEM oferece uma visão holística das ameaças em toda a superfície de ataque da organização.
- Visibilidade em sistemas de segurança de qualquer lugar do mundo. O FortiCloud fornece um console baseado na web que pode ser usado para controlar centralmente e até mesmo implantar todos os dispositivos da Fortinet Security Fabric - Fortinet e terceiros. Esse gerenciamento e implantação rápida de dispositivos pode significar a diferença entre uma invasão ou violação de dados bem ou malsucedida.

☑ Camada de Acesso Seguro.

O número e os tipos de dispositivos conectados às redes corporativas continuam a crescer exponencialmente. Além disso, os usuários querem Wi-Fi rápido, mas as organizações também devem proteger o acesso sem fio a suas redes, a fim de minimizar a possibilidade de invasão e subsequente violação de dados. As soluções de Acesso Seguro da Fortinet incluem a capacidade de:

- Centralizar o gerenciamento de identidade e a identificação do usuário. O FortiAuthenticator utiliza uma variedade de métodos de identificação de usuários para garantir que os dispositivos conectados à rede corporativa recebam apenas os privilégios de acesso apropriados baseados em funções.
- Chaves de acesso seguro para uma camada adicional de segurança. Os produtos FortiSwitch usam detecção de dispositivo, espionagem de DHCP e coleta de syslog que aumentam a prevenção contra invasão e a proteção de dados dentro dos NGFWs da FortiGate.
- As soluções da linha FortiToken geram codigos de uso único baseados em tempo (TOTP), um segundo fator acessível para empresas que estão migrando para autenticação de dois fatores. Isso permite que as organizações garantam que apenas as pessoas autorizadas tenham acesso a aplicativos específicos.

☑ Prevenção e Detecção de Ameaças Avançadas.

Para ter sucesso na prevenção e detecção de invasões, bem como na resposta a incidentes de violação de dados, as organizações exigem proteção avançada contra ameaças e recursos de detecção. Estes caem em dois baldes:

- Inteligência de Ameaças. As organizações precisam de inteligência de segurança avançada para ficar por dentro das ameaças recebidas. Usando pesquisas líderes do setor, o FortiGuard envia atualizações em tempo real sobre explorações emergentes. A Fortinet mantém atualizações e patches regulares de produtos, priorizados para ataques específicos, que fecham rapidamente a lacuna quando novas vulnerabilidades são identificadas.
- Sandboxing. Identificar antecipadamente ameaças desconhecidas é uma exigência, e as técnicas de sandboxing estão se tornando cada vez mais comuns como parte da estratégia de segurança para detê-las. O FortiSandbox permite que as organizações recebam não apenas atualizações automatizadas sobre questões emergentes de segurança, mas também compartilhem suas próprias descobertas como atualizações em tempo real enviadas para seus outros produtos de segurança. A inclusão do FortiSandbox infunde uma camada de proteção avançada contra ameaças em todo o Security Fabric. E como com outras soluções da Fortinet, o FortiSandbox está no topo das opções, reconhecido, por exemplo, com uma classificação "Recomendado" pelo NSS Labs para Breach Detection Systems [Sistemas de Detecção de Violações].[9]

Itens finais do checklist.

Se você é impactado pela LGPD, não tem tempo para esperar. Os produtos pontuais e as plataformas de segurança não são sua resposta quando se trata de soluções abrangentes de prevenção e detecção de invasões e prevenção e violação de dados. É aqui que o Fortinet Security Fabric se destaca. A vantagem é que as diferentes peças são melhores na classe, com o agregado somando mais do que a soma das partes.

Além da visibilidade em tempo real e dos controles que as organizações obtêm do Fortinet Security Fabric, eles também recebem um modelo de acompanhamento com o FortiCare 360, tanto serviço técnico avançado quanto substituição rápida de hardware quando ocorrem falhas. Isso é particularmente importante quando você está falando sobre violações de dados sob o guarda-chuva da LGPD.

[1] John M. Gilligan, "It Is Time to Get Serious About Securing Our Nation's Critical Infrastructure," Center for Internet Security blog, 30 de outubro de 2017.

[2] Adam Hils, Jeremy D'Hoinne, and Rajpreet Kaur, "Magic Quadrant for Enterprise Network Firewalls," Gartner, 10 de julho de 2017. Atualizar para 2018

[3] "Next Generation Firewall," NSS Labs, acesso em 11 de julho de 2019.

[4] "Advanced Endpoint Protection," NSS Labs, acesso em 05 de dezembro de 2017.

[5] "2019 Data Breach Investigations Report," Verizon, acesso em 07 de julho de 2019.

[6] "Advanced Threat Defense Certification Testing Report," ICSA Labs, 02 de outubro de 2017.

[7] Matthew Chips, "Web Application Firewall Test Report," NSS Labs, 11 de abril de 2017.

[8] "2017 Trustwave Global Security Report," Trustwave, junho de 2017.

[9] "Breach Detection System," NSS Labs, acesso em 05 de dezembro de 2017.

FORTINET®

www.fortinet.com

123456-0-0-PT