Descrição do Serviço

Padrão de Segurança de Dados para Aplicativos de Pagamento

Serviço de Validação Conformidade

Sumário

PA-DSS – Serviços de Validação de Conformidade

A SecureTrust™ é uma divisão da Trustwave Holdings, Inc.

DESCRIÇÃO DO SERVIÇO

O Serviço de Validação de Conformidade (CVS – Compliance Validation Service) do Padrão de Segurança de Dados para Aplicativos de Pagamento (PA-DSS – Payment Application Data Security Standard) da SecureTrust (o "**Serviço**") foi desenvolvido para validar se as operações e os controles de segurança identificados do aplicativo de pagamento obtiveram conformidade com o PA-DDS, conforme estabelecido pelo Conselho de Padrões de Segurança do PCI (o "**Padrão**"). O Serviço é uma avaliação do design e da implementação de controles de PA-DSS e políticas, procedimentos e práticas de apoio relevantes ao Padrão.

Os termos em maiúsculas usados nesta descrição de serviço, mas não definidos aqui, têm seus significados indicados no Contrato Principal de Serviços da Trustwave localizado em https://www.trustwave.com/en-us/legal-documents/contract-documents/ ou em um contrato similar assinado entre a SecureTrust e o Cliente.

RECURSOS DO SERVIÇO BÁSICO

O Serviço inclui os seguintes recursos padrão:

Portal SecureTrust

Os recursos do Portal SecureTrust consistem, entre outros, em um aplicativo de Gerenciamento de conformidade para administrar o processo de engajamento, bem como para coletar e armazenar com segurança evidências, documentação e produtos finais.

Serviços Globais de Conformidade e Risco

A equipe de Serviços Globais de Conformidade e Risco (GCRS — Global Compliance and Risk Services) é composta, entre outras, pelas seguintes pessoas e funções de destaque:

Avaliador de segurança qualificado para aplicativo de pagamento (PA QSA – Payment Application Qualified Security Assessor) – Um PA QSA é o recurso principal para a execução do Serviço, sendo responsável pela condução da avaliação, determinação de conformidade e relatórios.

Consultor gerencial (MC – Managing Consultant) – Um MC fornece orientação, supervisão de projeto e garantia de qualidade de relatórios ao PA QSA, além de servir como ponto de contato secundário do Cliente para escalamentos e consultas.

Conselho de Revisão de Conformidade (CRB – Compliance Review Board) – O CRB serve como ponto final para a interpretação dos requisitos do Padrão ou para a solução de questões complicadas de conformidade, fornecendo consistência e continuidade ao longo das avaliações da SecureTrust. O CRB

também é o ponto final de escalamento para a solução de problemas relativos a status de conformidade contra os requisitos do Padrão ou a revisão de um controle de compensação.

PA-DSS CVS – O Serviço valida se as operações e controles de segurança identificadas do aplicativo de pagamento do Cliente obtiveram conformidade com o Padrão. Se o aplicativo do Cliente for considerado em conformidade com o Padrão, a SecureTrust fornecerá ao Cliente um Relatório de validação (ROV – Report on Validation) como declaração do status de conformidade do Cliente. Se o aplicativo do cliente for considerado fora de conformidade com o Padrão, a SecureTrust fornecerá ao Cliente um ROV de não conformidade detalhando os resultados do Serviço.

ENTREGA E IMPLEMENTAÇÃO

Início do projeto

A equipe de GCRS da SecureTrust facilita a entrega do Serviço, o que inclui o agendamento e a condução da reunião de abertura remota para definir e chegar a um acordo sobre um plano de projeto de alto nível que consiste em datas de marcos importantes, etapas principais, estimativas de duração, produtos, requisitos de recursos e procedimentos de escalamento.

Fase I: Coleta de informações

A SecureTrust e o Cliente trabalharão para coletar e analisar informações sobre o aplicativo do Cliente. A SecureTrust conduzirá entrevistas, conforme necessário, com os arquitetos do sistema, desenvolvedores do aplicativo, desenvolvedores do banco de dados, administradores do sistema, pessoal de garantia de qualidade (QA) ou testes e outros membros da equipe do Cliente que possam fornecer detalhes relevantes sobre o aplicativo do Cliente.

Os tópicos para coleta de informações incluem, entre outros:

- A descrição do aplicativo do Cliente para fornecer uma compreensão fundamental do aplicativo do Cliente.
- O nome e o número da versão do aplicativo, bem como os sistemas operacionais compatíveis e quaisquer requisitos de hardware ou software.
- A descrição dos componentes que compõem o aplicativo do Cliente.
- A lista de hardware e software necessários para a execução do aplicativo do Cliente, incluindo quaisquer dependências de terceiros, conforme aplicável.
- A descrição da função do aplicativo no ciclo de vida do pagamento, incluindo funções de autorização e liquidação, conforme aplicável.
- Processos do Ciclo de vida de desenvolvimento de software (SDLC – Software Development Lifecycle).
- Especificações funcionais do projeto que mostram o projeto e as implementações funcionais do aplicativo do Cliente.
- Principais operações de gerenciamento, incluindo quaisquer integrações com quaisquer funções de criptografia de terceiros, conforme aplicável.
- Os diagramas e a documentação da interface do aplicativo que ilustram os fluxos de dados internos/externos do aplicativo do Cliente, incluindo comunicações de rede internas/externas, conforme aplicável.
- A lista de ferramentas de teste do aplicativo que podem ser exigidas para testes de laboratório.
- A descrição dos scripts de teste do aplicativo de pagamento e a documentação do ambiente de teste para processamento de dados, conforme aplicável.

- A documentação de implementação do Cliente, incluindo os procedimentos de integração de aplicativo seguro e as recomendações para a integração do aplicativo nos ambientes comerciais.

A SecureTrust pode solicitar uma demonstração remota do aplicativo do Cliente para determinar os testes necessários para concluir a fase de revisão do aplicativo PA-DSS CVS, conforme descrito abaixo.

Fase II: Revisão do aplicativo:

O Serviço da fase de revisão do aplicativo ocorrerá nos laboratórios de teste da SecureTrust ou nas instalações do Cliente, dependendo de restrições logísticas, da natureza e dos sistemas necessários para o aplicativo do Cliente. A SecureTrust trabalhará com o Cliente para determinar se uma visita no local é necessária ou se os testes podem ser realizados nos laboratórios de teste da SecureTrust.

A fase de revisão do aplicativo concentra-se em testes lógicos do aplicativo do Cliente conforme os requisitos descritos no Padrão. A fase de revisão também inclui todas as entrevistas ou revisões de documentação restantes, bem como quaisquer observações de processos locais. A SecureTrust obterá uma compreensão minuciosa de como o aplicativo do Cliente processa dados, como ele foi desenvolvido, distribuído, configurado, e como ele é protegido contra acessos não autorizados.

A SecureTrust examinará o ambiente de execução do Cliente, incluindo a revisão de ferramentas, componentes de software e hardware, bibliotecas de código aberto e de terceiros, requisitos e dependências, conforme aplicável.

A SecureTrust examinará parâmetros críticos do aplicativo do Cliente, como, entre outros, processos de manipulação de dados, esquemas de banco de dados, logs e condições de erro. A SecureTrust também pode verificar os processos de desenvolvimento de software escritos do Cliente, revisar configurações, produção e dados de teste de aplicativos relevantes, recursos de autenticação, controles de alterações, armazenamento de dados e criptografia, logs de auditoria e recursos de manutenção remota. A SecureTrust conduzirá testes funcionais de controles, conforme apropriado, para determinar a conformidade com o aplicativo do cliente com o Padrão.

A SecureTrust trabalhará com o Cliente para resolver questões de avaliação do Cliente, e a SecureTrust fornecerá ao cliente assistência razoável na interpretação do Cliente dos Padrões e de suas respostas. A SecureTrust pode solicitar revisão adicional do aplicativo do Cliente, áreas de código aplicáveis, documentação ou processos e procedimentos de manipulação de dados.

A SecureTrust executará um teste de penetração no aplicativo, remotamente ou nos laboratórios de teste da SecureTrust. O teste determinará o quanto o aplicativo do Cliente é seguro contra vulnerabilidades comuns e contra vulnerabilidades conforme listadas no Padrão, conforme aplicável. A SecureTrust fornecerá um relatório ao Cliente, detalhando os resultados do teste de penetração do aplicativo, incluindo quaisquer etapas de correção necessárias para que o aplicativo do Cliente obtenha conformidade com o Padrão. Para aplicativos baseados na Web, um teste profundo deve ser executado para determinar o status de conformidade do aplicativo do Cliente, e esse teste não está incluído como parte do Serviço.

Fase III: Relatórios

A SecureTrust desenvolverá um relatório documentando as observações e recomendações a partir do Serviço.

O esboço do relatório será enviado ao Cliente para revisão. O Cliente pode comentar e sugerir alterações no esboço do relatório e na documentação de apoio antes que a equipe de QA da SecureTrust finalize

o relatório. A SecureTrust conserva a autoridade final em relação ao conteúdo do relatório final e ao tipo de produto final a ser desenvolvido.

A SecureTrust fornecerá um produto de relatório final, conforme definido abaixo:

- Se o aplicativo do Cliente for considerado em conformidade com o Padrão, e, uma vez finalizado pela equipe de QA da SecureTrust, o ROV, junto a todas as documentações de suporte, serão enviados ao Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI SSC – Payment Card Industry Security Standards Council) para considerações de listagem.
- Se o aplicativo do cliente for considerado fora de conformidade com o Padrão, a SecureTrust fornecerá ao Cliente um ROV de não conformidade.

A SecureTrust conduzirá uma reunião de fechamento com o Cliente.

RESPONSABILIDADES DA SECURETRUST

- Estabelecer contato e permanecer disponível para comunicações com o Cliente.
- Estabelecer comunicação e planos de escalamento.
- Criar uma conta do Cliente no Portal SecureTrust.
- Definir o plano de projeto de alto nível, o qual consiste em datas de marcos importantes, etapas principais, estimativas de duração, produtos e requisitos de recursos.
- Agendar e conduzir reuniões de abertura, status periódico e fechamento.
- Validar o escopo do Serviço.
- Criar e responder a itens de ação do Cliente no Gerenciador de conformidade no Portal SecureTrust.
- Entrevistar o pessoal apropriado da organização e coletar informações dessas pessoas.
- Executar validação de acordo com os procedimentos de teste do PA-DSS.
- Fornecer ao Cliente informações sobre quaisquer observações que exigem correção.
- Determinar os resultados do Serviço e o status de conformidade do aplicativo ao final do Serviço.
- Produzir um ROV de PA-DSS de conformidade ou não conformidade, dependendo do status do aplicativo no momento da realização do Serviço.
- Fornecer ao Cliente um relatório final, documentando observações e recomendações a partir do Serviço.

RESPONSABILIDADES E ACEITES DO CLIENTE

- Estabelecer contato e permanecer disponível para comunicações com a SecureTrust.
- Estabelecer comunicação e planos de escalamento.
- Concordar com o plano de projeto de alto nível, o qual consiste em datas de marcos importantes, etapas principais, estimativas de duração, produtos e requisitos de recursos.
- Fornecer com precisão todas as informações necessárias, incluindo principais partes interessadas, informações aplicáveis sobre o ambiente do Cliente e requisitos de configuração.
- Informar à SecureTrust sobre todas as atividades de manutenção do ambiente do Cliente e sobre mudanças que podem impactar o fornecimento do Serviço.
- Responder com precisão às solicitações das equipes da SecureTrust no estabelecimento de contato e na coleta de informações.
- Fornecer detalhes completos e precisos sobre o ambiente relevante e outras informações sobre as operações de negócios.
- Tornar disponíveis recursos capazes de participar das atividades de avaliação de conformidade.
- Participar de e compreender os materiais explicados durante as chamadas, reuniões, entrevistas, discussões, inspeções de instalações e análises de controles.

- Aceites do cliente:
    - Todas as atualizações de segurança e recursos do Portal SecureTrust serão incluídas em atualizações de versões principais.
    - O Serviço faz referência aos requisitos e procedimentos de teste do Padrão atual aplicável na ocasião da data de início do serviço.
    - O Serviço pode consistir em atividades de avaliação remota e no local.
    - O Serviço será iniciado no dia da chamada de abertura. A linha de tempo e o final do Serviço serão determinados durante a chamada de abertura.
    - A documentação e as evidências solicitadas pela SecureTrust devem ser enviadas pelo Cliente dentro de quarenta e cinco (45) dias a partir do início do Serviço.
        - O Cliente deve enviar todas as evidências e as atividades completas de correção a não menos de quarenta e cinco (45) dias antes do final do Serviço.
    - A revisão da documentação inclui uma revisão inicial da documentação do Cliente com feedback direto sobre quaisquer observações de não conformidade, e uma revisão da documentação corrigida do Cliente.
    - O Serviço inclui uma avaliação do aplicativo.
    - As preparações de laboratório são responsabilidade do Cliente. O Cliente deve fornecer um laboratório para os testes do aplicativo, em conformidade com os controles do Padrão de Segurança de Dados do PCI (PCI DSS – PCI Data Security Standard), de acordo com o Apêndice B do Padrão. Se os testes forem conduzidos no laboratório da SecureTrust, o Cliente deverá fornecer sistemas configurados de acordo com o PA DSS e o PCI DSS.
    - Nos testes no laboratório da SecureTrust, quando possível, a SecureTrust fornecerá a infraestrutura necessária para a execução dos sistemas do Cliente. Se o Cliente tiver optado por testar no laboratório da SecureTrust e os sistemas do Cliente exigirem licenças, conectores ou hardwares especiais, o Cliente deverá fornecer os componentes do sistema necessários para permitir os testes e arcar com quaisquer custos relacionados. A SecureTrust não adquire licenças de sistemas operacionais ou qualquer outra licença necessária para testar os aplicativos do Cliente de acordo com os requisitos do PA-DSS relativos ao ambiente de teste do aplicativo. O Cliente fornecerá um posto de trabalho, licença, autorização especial de função de teste ou outra forma de acesso autorizado à SecureTrust, caso seja necessário para que a SecureTrust use qualquer um dos aplicativos relevantes do Cliente.
    - A SecureTrust pode solicitar evidências dos sistemas e processos do Cliente conforme necessário para avaliar a conformidade com quaisquer requisitos específicos. O Cliente fornecerá todas essas evidências o mais breve possível.

    - A SecureTrust não é responsável por definir sistemas em escopo, ou para estabelecer se as informações fornecidas pelo Cliente são precisas.
    - A SecureTrust reserva-se o direito de rejeitar ou aceitar comentários do Cliente baseados nos fatos e circunstâncias do Serviço.
    - A SecureTrust desempenhará o Serviço no idioma inglês.
    - A SecureTrust não criará ou modificará documentação do Cliente como parte do Serviço.
    - A SecureTrust não fornecerá serviços corretivos como parte do Serviço.
    - A SecureTrust não oferecerá nenhuma orientação ou aconselhamento legal.
    - A qualidade e a precisão do Serviço dependem do fornecimento pelo Cliente de informações precisas e acesso aos sistemas e recursos do Cliente para a SecureTrust.