PCI DSS v4.0: cronogramas previstos e atualizacões mais recentes

O feedback da indústria, junto com as mudanças nos pagamentos, na tecnologia e na segurança, está direcionando nossa abordagem ao PCI DSS v4.0. Em discussões com as partes interessadas da indústria, recebemos várias perguntas sobre o PCI DSS v4.0. Abaixo, entrevistamos Lauren Holloway, Diretora de Padrões de Segurança de Dados, que responde a algumas perguntas importantes sobre o que está acontecendo com o PCI DSS v4.0.

Nota: *Todas as datas mencionadas neste artigo são baseadas em projeções atuais e estão sujeitas a alterações.*

Onde está o PCI DSS v4.0 no processo de desenvolvimento?

Lauren Holloway: A solicitação de comentários (RFC) realizada de outubro a dezembro de 2019 gerou mais de 3.000 comentários, e o PCI SSC está revisando cuidadosamente e considerando todos os itens de feedback recebidos. Está prevista uma RFC adicional para setembro-outubro de 2020. Esta RFC incluirá um rascunho atualizado do PCI DSS v4.0, que estamos desenvolvendo atualmente com base no feedback recebido durante a RFC de 2019.

Mais informações sobre nossas próximas RFCs e nosso processo de RFC podem ser encontradas em nossa Página de RFC.

Quando o PCI DSS v4.0 será lançado?

Lauren Holloway: A versão final do PCI DSS v4.0 está atualmente planejada para conclusão em meados de 2021.

Vale ressaltar que o prazo de desenvolvimento para esta atualização do PCI DSS é notavelmente mais longo do que nas revisões anteriores. Esse período estendido foi projetado para oferecer suporte a um número crescente de oportunidades de feedback para que as partes interessadas forneçam informações durante o processo de atualização.

Leia mais: 3 coisas a saber sobre o desenvolvimento do PCI DSS v4.0

Será fornecida uma análise detalhada do feedback recebido durante a RFC de 2019?

Lauren Holloway: Depois que terminarmos de revisar os mais de 3.000 itens de feedback da RFC e fazer atualizações no rascunho do PCI DSS v4.0, um resumo dos feedbacks da RFC será fornecido aos participantes da RFC de 2019 através do Portal PCI. Este resumo, mostrando como cada item de feedback foi tratado, estará disponível para esses participantes quando a próxima RFC do PCI DSS ocorrer.

Além disso, forneceremos atualizações para a comunidade do PCI Council à medida que as decisões forem tomadas através de nossos webcasts trimestrais com partes interessadas e em nossas reuniões da comunidade planejadas para o final deste ano.

Quando os questionários de auto-avaliação (SAQs) serão atualizados e o que incluirão as atualizações?

Lauren Holloway: As atualizações dos documentos de suporte, incluindo SAQs, modelo de relatório de conformidade (ROC), glossário do PCI DSS e abordagem priorizada fazem parte do ciclo de revisão sempre que o PCI DSS é atualizado. Começaremos a trabalhar nas atualizações de toda a documentação de suporte para alinhá-las com o PCI DSS v4.0 ainda este ano e forneceremos atualizações à medida que o desenvolvimento avança. Estamos planejando ter esses documentos finalizados e prontos para lançamento dentro de alguns meses após o lançamento da versão final do PCI DSS v4.0.

Aqui está uma visão geral do cronograma atual do esforço de desenvolvimento do PCI DSS v4.0, incluindo RFCs e conclusão planejada dos materiais do PCI DSS v4.0.

Lauren Holloway: Depois que o PCI DSS v4.0 for lançado, será fornecido um período de transição estendido para que as organizações atualizem do PCI DSS v3.2.1 para o PCI DSS v4.0. Para dar suporte a essa transição, o PCI DSS v3.2.1 permanecerá ativo por 18 meses quando todos os materiais do PCI DSS v4.0 - ou seja, o padrão, documentos de suporte (incluindo SAQs, ROCs e AOCs), treinamento e atualizações de programa – forem publicados.

Nota: *O PCI DSS v4.0 está programado para ser concluído seis meses antes do lançamento da documentação de suporte, treinamento e atualizações do programa necessários para suportar o uso do PCI DSS v4.0. O padrão PCI DSS v4.0 estará, portanto, disponível por 2 anos antes da aposentadoria do PCI DSS v3.2.1.*

Esse período prolongado permite que as organizações se familiarizem com as mudanças na v4.0, atualizem seus modelos e formulários de relatórios e planejem e implementem mudanças para atender aos requisitos atualizados. Após a conclusão do período de transição, o PCI DSS v3.2.1 será desativado e a v4.0 se tornará a única versão ativa.

Além de um período de 18 meses em que a v3.2.1 e a v4.0 estarão ativas, haverá um período de tempo extra definido para introduzir novos requisitos, identificados com “data futura” na v4.0.

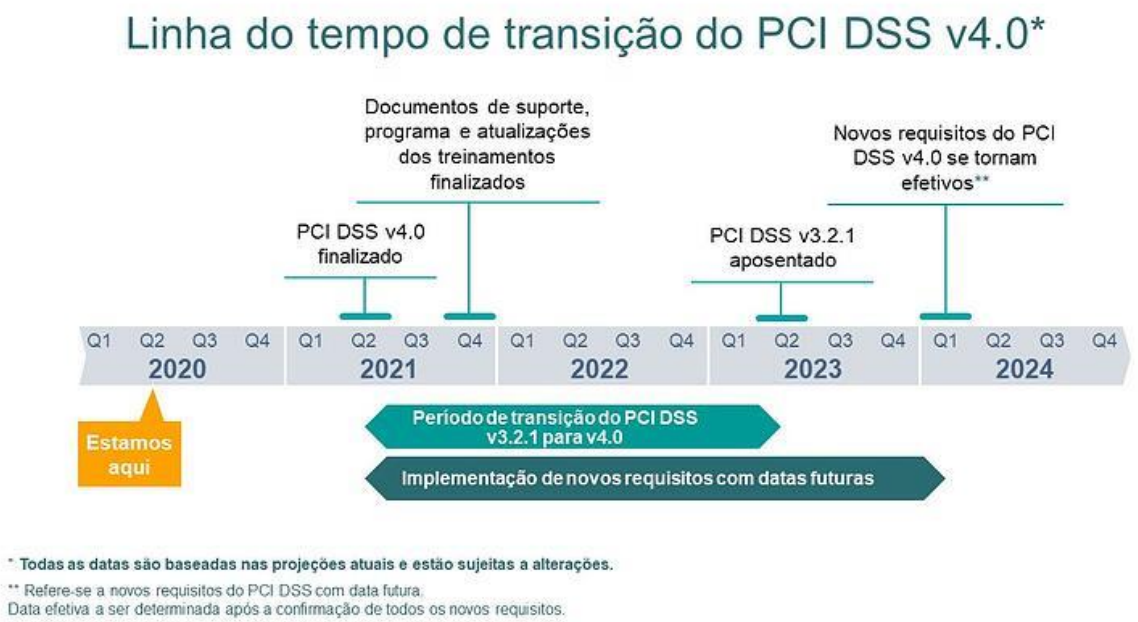
O que são requisitos "com data futura" e quando entrarão em vigor?

Lauren Holloway: No PCI DSS, às vezes, novos requisitos são designados com uma data futura para fornecer às organizações tempo adicional para concluir suas implementações. Os requisitos com data futura são considerados as melhores práticas até que a data futura seja atingida. Durante esse período, as organizações não precisam validar os requisitos com datas futuras. Embora não seja obrigatório, as organizações que implementaram controles para atender aos novos requisitos e estão prontas para avaliar os controles antes da data futura declarada são incentivadas a fazê-lo. Uma vez atingida a data futura designada, todos os requisitos com datas futuras se tornam efetivos e aplicáveis.

Prevemos que o PCI DSS v4.0 conterá vários novos requisitos que podem ser futuros; no entanto, não saberemos quantos novos requisitos haverá até que o padrão seja finalizado.

Embora a data futura efetiva para esses novos requisitos não seja confirmada até que o PCI DSS v4.0 esteja pronto para publicação, isso proporcionará tempo suficiente para as organizações planejarem e implementarem novos controles e processos de segurança conforme necessário para atender a todos os novos requisitos. A data futura dependerá do impacto geral que os novos requisitos terão sobre o padrão. Com base no rascunho atual, espera-se que a data futura se estenda além do período de transição planejado, com uma possível data futura entre 2½ e 3 anos após a publicação do PCI DSS v4.0.

Uma visão geral do cronograma de transição planejado e do cronograma potencial para requisitos com datas futuras é mostrada abaixo.



* Todas as datas são baseadas nas projeções atuais e estão sujeitas a alterações.

** Refere-se a novos requisitos do PCI DSS com data futura.
Data efetiva a ser determinada após a confirmação de todos os novos requisitos.

Leia mais: Como o feedback do setor está moldando o futuro do PCI DSS

Um rascunho do PCI DSS v4.0 será publicado antes de ser finalizado?

Lauren Holloway: Os rascunhos dos padrões são compartilhados com as partes interessadas do PCI SSC para análise e comentários. O próximo rascunho do PCI DSS será fornecido às empresas QSA, ASV e Organizações Participantes para revisão e comentários durante o próximo período da RFC em setembro / outubro deste ano.

Mais informações sobre nossas próximas RFCs e nosso processo RFC podem ser encontradas em nossa Página de RFC.

Gostaria de participar da próxima RFC do PCI DSS v4.0. Como posso participar?

Lauren Holloway: Qualquer organização pode se tornar uma organização participante. Além de fornecer feedback sobre os rascunhos dos Padrões de Segurança PCI, os benefícios de se tornar uma organização participante incluem a capacidade de propor, votar e participar de Grupos de Interesse Especial, participar de reuniões anuais da comunidade do PCI SSC com dois passes gratuitos e demonstrar para seus clientes e parceiros de negócios seu compromisso com a segurança de pagamentos. Leia mais sobre todos os benefícios e como se tornar uma PO aqui.

O que nossa organização pode fazer agora para se preparar para o PCI DSS v4.0?

Lauren Holloway: Enquanto o PCI DSS v4.0 está em desenvolvimento, incentivamos todas as entidades a permanecerem diligentes e manterem seus controles de segurança do PCI DSS v3.2.1. Isso não apenas ajudará a garantir segurança contínua, mas também facilitará a transição para o PCI DSS v4.0.

Recomenda-se às organizações que tiveram acesso aos rascunhos iniciais que esperem até que a versão final do PCI DSS v4.0 seja lançada antes de tentar implementar quaisquer requisitos novos ou atualizados. As versões disponibilizadas na RFC são apenas rascunhos e o padrão será diferente na versão final lançada.

Leais mais sobre o PCI DSS v4.0