INSTRUCTURE

SECURITY OVERVIEW

Engineering, Security, e Operations

Março de 2022

Índice

INSTRUCTURE

Introdução

Overview

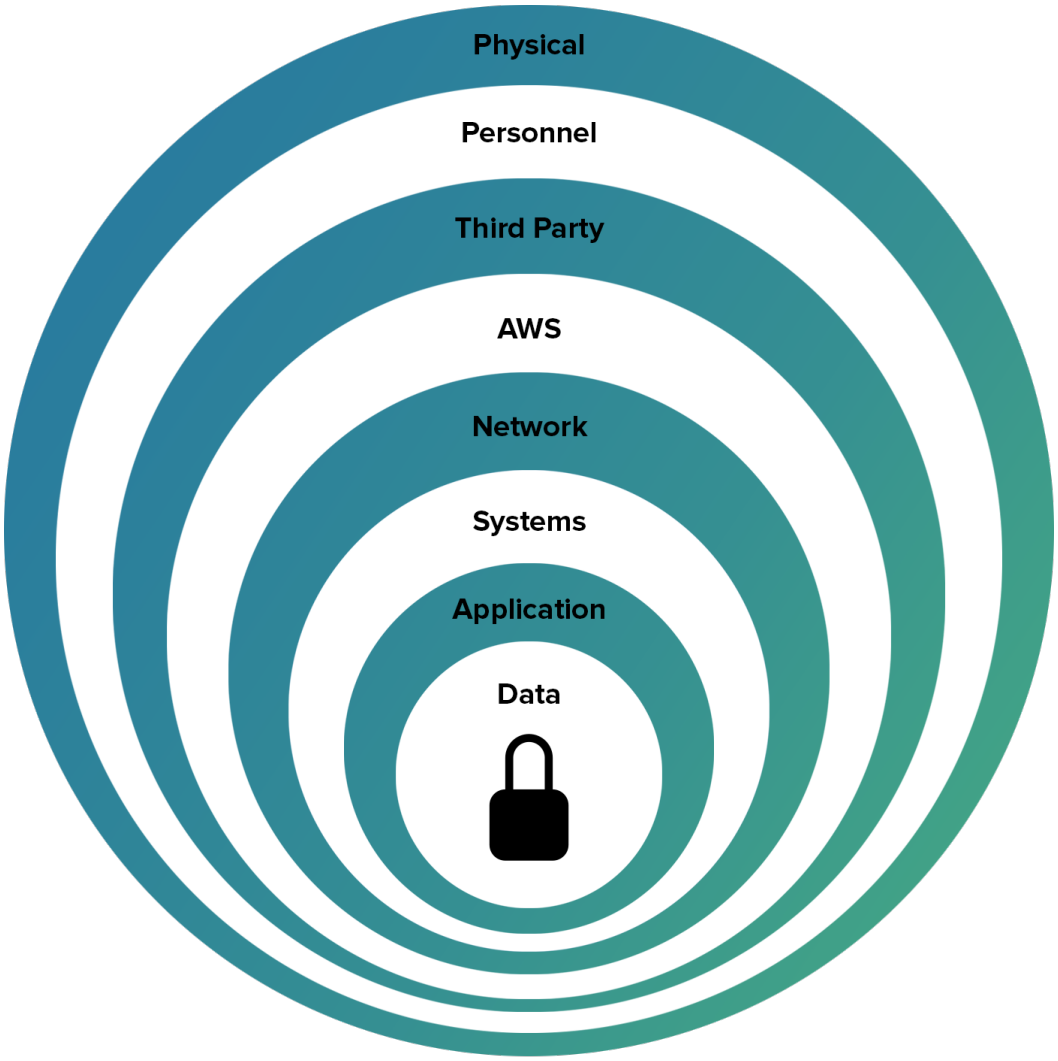
Não deve ser segredo para ninguém no mundo de hoje que a segurança é fundamental. Em um mundo cada vez mais on-line, percebemos que as ameaças ao nosso pessoal, nossos negócios e seus dados estão sempre presentes, e o esforço e as medidas que tomamos para protegê-los são intermináveis. Na verdade, à medida que nossos negócios e os seus crescem, reconhecemos que as ameaças também podem aumentar em gravidade. No ano passado, o mundo viu o aumento de ransomware cada vez mais insidioso e explorações generalizadas como o Apache Log4j, onde até 50% de todos os negócios online viram tentativas de ataques a seus ativos por meio da vulnerabilidade Log4Shell.

É por isso que nosso programa de segurança é construído com base em padrões reconhecidos internacionalmente, como ISO 27001, NIST's Cyber Security Framework, AICPA's Trust Services Principles and Criteria e SANS' CIS Critical Security Controls. E, falando em padrões, também garantimos o desenvolvimento de nossos aplicativos de acordo com o Top 10 da OWASP. Na Instructure, implementamos mecanismos preventivos e de detecção, além de processos, controles e ferramentas em camadas, ajudando a mitigar riscos que podem afetar os dados , pessoas, sistemas, operações, produtos e nossa missão como empresa. O objetivo deste documento é descrever essas camadas e os tipos de controles que aplicamos para manter nossos clientes protegidos da maldade.

Programa de Segurança da Instructure

O programa de segurança da Instructure é liderado pelo Chief Information Security Officer (CISO) da Instructure e conta com uma equipe de profissionais de segurança da informação talentosos, qualificados e experientes. A equipe de segurança da informação da Instructure é responsável por estabelecer fortes práticas de segurança em toda a Instructure por meio de governança, gerenciamento de risco, política, educação, engenharia de segurança, conformidade de segurança, operações de segurança e segurança de aplicativos.

Ao implementar mecanismos de segurança preventivos e de detecção em cada camada entre riscos externos e internos plausíveis e os ativos mais valiosos da Instructure, podemos adotar uma abordagem de defesa em profundidade para proteger os dados do cliente.


Physical
Personnel
Third Party
AWS
Network
Systems
Application
Data

Segurança em Camadas

Segurança física

A Instructure hospeda todos os aplicativos da web voltados para o cliente e infraestrutura de suporte na AWS. A infraestrutura da AWS é altamente estável, tolerante a falhas e segura. A AWS publica um artigo de segurança perspicaz que descreve como a AWS implementou mecanismos de segurança física e proteção ambiental para proteger data centers da AWS em todo o mundo. A Instructure depende da capacidade da AWS de projetar e operar esses mecanismos e controles críticos para proteger o acesso físico aos dados e a disponibilidade dos serviços da Instructure.

Os data centers da AWS utilizam vigilância eletrônica de última geração e sistemas de controle de acesso multifatorial. Os data centers são atendidos 24 horas por dia, 7 dias por semana, por guardas de segurança treinados e o acesso é autorizado estritamente com privilégios mínimos. Os sistemas ambientais são projetados para minimizar o impacto das interrupções nas operações. As zonas de disponibilidade múltiplas fornecem resiliência em face da maioria dos modos de falha, incluindo desastres naturais ou falhas do sistema.

Os sistemas de energia elétrica do data center da AWS são projetados para serem totalmente redundantes e de fácil manutenção, sem impacto nas operações, 24 horas por dia e sete dias por semana. Unidades de fonte de alimentação ininterrupta (UPS) fornecem energia de reserva no caso de uma falha elétrica para cargas críticas e essenciais na instalação. Os geradores fornecem energia de reserva para os data centers de toda a instalação.

Além disso, os controles de segurança da AWS foram auditados por uma organização de avaliação terceirizada confiável e produziram os seguintes (e muitos outros) atestados e certificações:

- Relatório SOC 2 Tipo II usando a estrutura de Controle da Organização de Serviço apresentada pelo Instituto Americano de Contadores Públicos Certificados (AICPA)
- Certificado ISO / IEC 27001: 2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos
- Provedor de serviços de nível 1 sob o padrão de segurança de dados (DSS) da indústria de cartões de pagamento (PCI)

Segurança Pessoal

Como parte de nosso compromisso com a segurança, a Instructure se dedica a manter nossos funcionários atualizados e informados sobre os mais recentes desenvolvimentos e práticas do setor. A Instructure oferece aos funcionários treinamento de conscientização de segurança no momento da contratação e anualmente a partir de então. Incluídos como parte do treinamento de conscientização de segurança da Instructure estão informações e orientações valiosas relacionadas a manter os dados do cliente e os ativos da Instructure protegidos contra uma variedade de ameaças comuns contra

esses ativos. Isso também inclui a exigência de que todos os funcionários leiam, entendam e assinem os formulários de conformidade da Lei de Privacidade e Direitos Educacionais da Família (FERPA) e da Lei de Proteção à Privacidade Online das Crianças (COPPA).

Verificação de Antecedentes

A Instructure realiza verificações de antecedentes de todos os funcionários e contratados durante o processo de contratação, e o emprego depende dos resultados da verificação de antecedentes. Verificações adicionais de antecedentes, como verificações financeiras/de crédito, verificações de qualificação, antecedentes criminais, etc. são realizadas em funcionários e/ou funções importantes, por exemplo, funcionários que manipularão dados confidenciais ou ocuparão funções financeiras.

Segurança 3PP

A Instructure utiliza várias organizações terceirizadas para hospedar seus produtos para os clientes. Como parte de ajudar a garantir que organizações terceirizadas estejam prestando serviços à Instructure com segurança, a equipe de segurança da Instructure realiza uma verificação completa antes e periodicamente durante o relacionamento com fornecedores terceirizados.

A Instructure utiliza vários terceiros para fornecer suporte para os produtos da Instructure. Para ajudar a fornecer uma garantia de segurança razoável das práticas e mecanismos de segurança desses terceiros, a Instructure solicita e analisa continuamente cópias dos relatórios de garantia de terceiros fornecidos por essas organizações para confirmar se esses controles estão operando de maneira eficaz. Os contratos legais com esses terceiros também incluem disposições de segurança para ajudar a garantir a implementação e operação de controles de segurança eficazes nas organizações terceirizadas.

Segurança AWS

Os produtos da Instructure são hospedados na infraestrutura de nuvem de última geração fornecida pela Amazon Web Services (AWS). A infraestrutura da AWS é altamente estável, tolerante a falhas e segura. Para obter informações adicionais sobre o programa de segurança da AWS, certificações e conformidade de padrões, consulte http://aws.amazon.com/security e http://aws.amazon.com/compliance/.

Segurança da rede AWS

A infraestrutura em nuvem da AWS oferece sistemas abrangentes de monitoramento de rede e segurança para proteger o ambiente de produção e seus dados. Esses sistemas protegem contra:

- **Ataques Man in the Middle (MITM):** Todas as APIs da AWS estão disponíveis por meio de endpoints protegidos por SSL que fornecem autenticação de servidor usando certificados SSL assinados.

- **Spoofing de IP:** as instâncias do Amazon EC2 não podem enviar tráfego de rede falsificado. A infraestrutura de firewall baseada em host e controlada pela AWS não permitirá que uma instância envie tráfego com um endereço IP ou MAC de origem diferente do seu.

- **Varredura de portas:** quando a varredura de portas é detectada, ela é registrada e investigada.

- Virtual Private Cloud: Instructure utiliza VPCs para segmentar, proteger e isolar o tráfego de rede.

- **AWS GuardDuty:** A Instructure usa o AWS GuardDuty para alertar e informar sobre incidentes de segurança que ocorrem contra os serviços da Instructure hospedados na AWS.

Serviços AWS

Os serviços da AWS usados para hospedar o Canvas incluem o Elastic Compute Cloud (EC2), o Elastic Load Balancing (ELB), o Auto Scaling Groups (ASG), o Simple Storage Service (S3), o Elastic Block Store (EBS), o Virtual Private Cloud (VPC) Serviço de email simples (SES), gerenciamento de identidade e acesso (IAM) e vários outros. O aplicativo Canvas foi projetado para aproveitar ao máximo os recursos de capacidade e redundância em tempo real oferecidos pela AWS, sendo executados em várias zonas de disponibilidade em regiões em todo o mundo. O armazenamento primário é fornecido pelo Amazon S3, projetado para uma durabilidade superior a 99,99999999%.

Regiões e Datacenter AWS

A Amazon Web Services possui vários locais (chamados de "regiões") em todo o mundo. Cada região é uma área geográfica separada e cada região tem vários locais isolados, conhecidos como Zonas de disponibilidade. A Instructure usa as seguintes regiões da Amazon Web Services (AWS):

- Região Leste dos EUA (Virgínia do Norte)

- Região Oeste dos EUA (Oregon)

- Região Central do Canadá (Montreal)

- Região Oeste da União Europeia (Irlanda)

- Região da Central da União Europeia (Alemanha)

- Região Ásia Pacífico (Sydney)

- Região Ásia Pacífico (Cingapura)

Segurança de dados AWS:

A Instructure estabeleceu vários controles para garantir que os dados sejam protegidos contra divulgação, modificação ou destruição não autorizadas, incluindo:

- Todos os dados em repouso, incluindo backups de recuperação fora do local, são criptografados usando o algoritmo AES-GCM de 256 bits.
- Todo o tráfego de dados dentro e fora do Canvas é criptografado usando TLS, cifras compatíveis com sigilo de encaminhamento sempre que possível (por exemplo, ECDHE-ECDSA-AES128-GCM-SHA256). A lista de cifras aceitável é mantida constantemente para garantir que nenhuma vulnerabilidade esteja presente (por exemplo, CRIME, BEAST).
- Os backups de recuperação fora do local são criptografados usando o algoritmo AES-GCM de 256 bits e armazenados em um local altamente seguro.

Além disso, os dados são armazenados de forma redundante em várias zonas de disponibilidade por meio do Amazon S3. Os produtos Instructure replicam dados quase em tempo real para bancos de dados secundários e de backup, e os dados são copiados diariamente. A Instructure cria backups diários de dados e conteúdo do banco de dados para o Amazon S3. A replicação de dados e os backups garantem que, no caso de uma restauração necessária do sistema, o potencial de perda de dados seja limitado.

Segurança de Rede e de Sistema

Os produtos Instructure foram projetados para alcançar um alto nível de segurança, fornecendo uma abordagem simples e utilizável para autenticação de usuário, acesso ao sistema e permissões hierárquicas baseadas em funções. Esses produtos foram projetados para apoiar as próprias políticas de segurança interna da instituição e fornecer proteção rigorosa contra intrusões internas ou externas. Esses produtos reforçam a segurança do sistema, apresentando um modelo de segurança simples para os usuários finais.

Acesso e Autenticação de Sistema:

A Instructure usa um sistema de aprovação múltipla para conceder acesso aos funcionários. O gerente do funcionário que está solicitando acesso deve preencher um ticket solicitando o nível detalhado de acesso ao sistema e especificando quais peças, funções e recursos devem ser acessados pelo funcionário. Uma justificativa comercial clara, válida e necessária deve ser fornecida para o usuário em questão. Outras aprovações são incluídas conforme necessário e com base no acesso que está sendo solicitado. Se todas as partes aprovarem o acesso do funcionário, a respectiva equipe de tecnologia concede acesso conforme solicitado no ticket. De acordo com a política de saída do funcionário, as contas do usuário são excluídas após o término do contrato de trabalho.

Todos os funcionários integrados da Instructure devem ler, compreender e assinar os formulários de conformidade da Lei dos Direitos Educacionais e Privacidade da Família (FERPA) e da Lei de Proteção à Privacidade Online das Crianças (COPPA).

As equipes de tecnologia da Instructure facilitam a instalação de chaves para todos os funcionários com acesso aos servidores. Um sistema de configuração automatizado instala as chaves públicas dos funcionários por servidor, de acordo com a necessidade. Este mesmo processo de configuração revoga automaticamente as chaves globalmente quando necessário. Os funcionários são obrigados a usar criptografia de disco completo e proteção por senha em suas máquinas de trabalho para proteger suas chaves privadas e outros dados confidenciais. As chaves privadas usadas para HTTPS são armazenadas criptografadas e decriptografadas por operações quando implementadas nos servidores de aplicativos.

Monitoramento e alertas estão disponíveis para detectar e avisar sobre quaisquer alterações nas chaves, usuários no sistema, tentativas de login e sudo e outros eventos preocupantes.

Ataques de negação de serviço (DoS) e negação de serviço distribuído (DDoS)

A Instructure segue estritamente as melhores práticas do setor na mitigação de ataques de negação de serviço (DoS) e negação de serviço distribuído (DDoS) sem afetar a disponibilidade do serviço para os usuários finais. Naturalmente, a infraestrutura da AWS é resiliente a DDoS por design e é compatível com sistemas de mitigação de DDoS que podem detectar e filtrar automaticamente o excesso de tráfego. Por exemplo, empregamos o AWS Shield como um serviço de proteção de negação de serviço distribuído (DDoS) gerenciado que protege o aplicativo web Canvas. O AWS Shield fornece detecção sempre ativa e mitigações automáticas em linha, e atenuou alguns dos maiores ataques DDoS já registrados, interrompendo um ataque de 2,3 Tbps em meados de fevereiro de 2020. Isso oferece aos nossos clientes proteção e defesa automáticas contra os ataques de rede mais comuns e ataques DDoS na camada de transporte. Mas, como é o caso de nossa filosofia contínua de fornecer um software como serviço de nível premium, vamos muito além de simplesmente oferecer proteção contra DDoS padrão.

Como um aplicativo da web, os load balancers do Canvas (AWS Elastic Load Balancing) escutam apenas um único protocolo em duas portas. HTTP (TCP) na porta 80, que é redirecionado para HTTPS na porta 443, que serve todos os dados por TLS. Ao distribuir automaticamente o tráfego de entrada de aplicativos em vários destinos e controlar e absorver o tráfego de rede, os balanceadores de carga do Canvas criam um aplicativo altamente disponível para os usuários e uma estratégia robusta de mitigação de DoS/DDoS, desviando facilmente solicitações maliciosas ou indesejadas. Reduzir a superfície de ataque dessa maneira significa bloquear o tráfego de muitos vetores comuns de ataque DDoS que não se comunicam na mesma porta ou protocolo que nosso aplicativo.

Ao usar o Elastic Load Balancing (ELB), reduzimos bastante o risco de sobrecarregar o aplicativo ao distribuir o tráfego entre várias instâncias de back-end e criar uma linha de defesa entre a Internet e nossa rede Virtual Private Cloud (VPC) que hospeda o serviço Canvas. O ELB é dimensionado automaticamente, permitindo gerenciar volumes maiores de tráfego imprevisto, como flash crowds ou ataques DDoS. Os balanceadores de carga aceitam apenas conexões TCP bem formadas, o que

significa que muitos ataques DDoS comuns, como inundações SYN ou ataques de reflexão UDP, não serão aceitos e passados para o aplicativo. Quando nossos balanceadores de carga detectam esses tipos de ataques, eles são dimensionados automaticamente para absorver o tráfego adicional, garantindo que não haja alteração na disponibilidade do serviço para os usuários finais.

Como todo o ecossistema Canvas é executado em servidores virtualizados como parte das Nuvens Privadas Virtuais (VPC) da Amazon Web Services (AWS), temos uma arquitetura resiliente a DDoS que minimiza pontos de entrada públicos por meio de grupos de segurança e listas de controle de acesso à rede (ACLs) . Isso significa que não apenas as superfícies de ataque de aplicativos são minimizadas, mas também os ataques DDoS comuns são rapidamente detectados e mitigados usando os grupos de segurança da AWS. Configuramos os Grupos de segurança da AWS para permitir o tráfego de rede da lista de permissões (deny-all, permit-by-approved-exception) para apenas portas autorizadas, negando automaticamente o acesso a qualquer outra porta ou protocolo e, por sua vez, protegendo os componentes do aplicativo Canvas back-end de um ataque direto.

Além das práticas recomendadas acima, o registro e monitoramento constante do serviço Canvas nos permite identificar rapidamente quaisquer ataques DoS/DDoS legítimos e nos envolver em uma resposta imediata a incidentes.

Segurança da Aplicação

Codificação Segura e Práticas de Desenvolvimento

Manter e aprimorar a segurança é um processo disciplinado e contínuo. A codificação e os testes de segurança são, portanto, componentes integrais da metodologia de engenharia e desenvolvimento da Instructure. Todo o código no aplicativo deve passar por um processo de revisão por pares do desenvolvedor antes de ser incorporado ao repositório de base de código. A revisão do código inclui auditoria de segurança baseada na codificação segura do Open Web Application Security Project (OWASP) e documentos de revisão de código e outras fontes da comunidade sobre as melhores práticas de segurança.

Todos os desenvolvedores são treinados para identificar e analisar problemas de segurança ao escrever e revisar o código. Os membros das equipes de tecnologia da Instructure assinam listas, blogs e outros recursos voltados para segurança para manter, expandir e compartilhar o corpo coletivo de conhecimento. A Instructure mantém um wiki interno para discutir e compartilhar as melhores práticas para a mitigação e prevenção de armadilhas de segurança e vulnerabilidades. As equipes de segurança e engenharia se mantêm atualizadas sobre as práticas gerais de segurança, os vetores de ataque recentes e quaisquer problemas de segurança especificamente relacionados às linguagens, aplicativos da web, estruturas e ambientes que a Instructure emprega para desenvolver, hospedar e manter os produtos da Instructure.

As revisões por pares de todas as alterações do código-fonte são obrigatórias. Várias revisões de pares são conduzidas para cada mudança na base do código para detectar e corrigir quaisquer bugs, falhas de segurança e quaisquer outros defeitos do código. As alterações no código devem ser validadas por revisão por pares antes que o código seja aprovado e enviado ao repositório de base de código.

Teste e Garantia de Qualidade

Depois que o novo código passa na revisão por pares, o código é incorporado à base de código e submetido a testes e garantia de qualidade. O novo código é implantado em um servidor de integração contínua, onde é testado imediatamente. A equipe de testes da Instructure executa o seguinte:

- Testes unitários (teste de código com código)
- Testes de integração (teste de código com integrações com outro código)
- Testes de Selenium (testando como o código funciona no navegador) em todos os diferentes ambientes e em diferentes bancos de dados

Depois de passar nesses testes, o código é incorporado na ramificação do código principal para garantia de qualidade formal (QA). A equipe de QA testa o novo código em todas as plataformas e navegadores com suporte.

Gerenciamento de acesso e identidade do cliente

Os produtos da Instructure oferecem suporte ao gerenciamento centralizado de identidades e autenticação delegada por meio da integração com o Central Authentication Service (CAS) e o SAML 2.0. Se a autenticação falhar, o aplicativo procurará as credenciais usando seu serviço de autenticação interno. Se a autenticação falhar novamente, o aplicativo negará o login do usuário.

Segurança de Protocolo e Sessão

Os produtos da Instructure usam HTTPS (HTTP sobre TLS) para toda a comunicação. Todo o tráfego de entrada e saída é criptografado usando TLS 1.2, garantindo que todas as informações de identificação pessoal, troca de credenciais, solicitações de páginas e dados da sessão sejam seguras. O Canvas criptografa os dados em repouso na camada do banco de dados. Isso inclui todas as informações do usuário, desempenho, informações do curso e teste em cursos criados originalmente.

As sessões são mantidas e podem ser invalidadas. Um cookie de sessão criptografado, assinado com um código de autenticação de mensagem hash (HMAC), é usado apenas para identificar uma sessão atual. O conteúdo do HMAC e do cookie são criptografados com Advanced Encryption Standard (AES) -256 no modo de feedback de criptografia (CFB). O conteúdo do cookie não pode ser sequestrado durante a transmissão pela rede, não pode ser visualizado ou adulterado pelo usuário e não pode ser acessado por meio de javascript. Os IDs de sessão são comparados e validados em relação aos valores armazenados no servidor. Uma sessão invalidada exigirá que um usuário faça o login novamente.

As sessões são reconfiguradas em cada login bem-sucedido para impedir o acesso aos IDs de sessão por logins subsequentes. Para evitar vulnerabilidades de falsificação de solicitação entre sites (CSRF), todas as ações do usuário que modificam dados exigem uma chave secreta de sessão para postar dados. Todas as solicitações que modificam dados são feitas com solicitações HTTPS POST ou PUT, nunca GETs.

Prevenindo ataques de scripts entre sites (XSS)

A Instructure emprega uma variedade de estratégias para evitar ataques de script entre sites (XSS). Por exemplo, quando o aplicativo cria um formulário para entrada do usuário, um token de uso único é incorporado ao formulário HTML para que o aplicativo possa identificar o formulário e verificar se ele não originou outro site em uma possível tentativa de ataque.

Os aplicativos higienizam o conteúdo para proteger contra vulnerabilidades intencionais ou não intencionais. Quando o conteúdo é colocado em um formulário, como o conteúdo que um usuário insere com o Editor de Conteúdo Enriquecido, o aplicativo limpa (tanto do lado do cliente quanto do lado do servidor) o conteúdo e remove qualquer conteúdo malicioso. A higienização de conteúdo evita o jacking de sessão, hacks de formulário e outros acessos e / ou modificações de dados não autorizados.

Todo o conteúdo inserido pelo usuário é limpo antes de ser salvo no banco de dados. A sanitização é feita pela listagem de permissão explícita - não por lista de bloqueio - evitando a adição de JavaScript aos dados HTML e também evitando a adição de tags HTML não seguras.

Upload de arquivos e segurança de download

Os arquivos carregados pelo usuário são armazenados no Amazon S3 com nomes e pastas exclusivos. Para evitar o side-jacking de arquivos carregados pelo usuário e preservar a integridade do sistema, os produtos da Instructure colocam os arquivos carregados no repositório de Arquivos em um subdomínio diferente para estabelecer um domínio de segurança separado, a fim de tirar proveito das medidas de segurança de mesma origem do navegador. O navegador reforçará a segurança entre os arquivos carregados e a sessão do usuário e impedirá o hi-jacking da sessão. Se um arquivo carregado executar código usando JavaScript, Java, Flash ou outras tecnologias, esse código não será capaz de acessar a sessão do usuário nem de fazer solicitações ao aplicativo em nome do usuário. Todos os downloads de arquivos exigem chaves de autorização exclusivas e de curta duração.

Segurança de Dados

Instructure tem uma política de classificação, manuseio e criptografia de dados estabelecida, documentada, aprovada e disseminada. Esta política descreve os processos de classificação e tratamento de dados durante sua vida útil. Como parte desta política, os dados são classificados como um dos seguintes:

- Confidencial
- Interno
- Público

Confidencial

Dados confidenciais são elementos de dados sensíveis que legal e contratualmente exigem mecanismos de segurança e proteção de privacidade. Exemplos de dados confidenciais incluem dados de clientes, informações de autenticação, informações de identificação pessoal (PII), informações de pagamento e qualquer coisa sujeita ao privilégio advogado-cliente. Os dados confidenciais devem ser criptografados em todos os momentos, tanto em trânsito como em repouso, compartilhados apenas com o pessoal apropriado e autorizado, e são destruídos com segurança.

Interno

Dados internos são dados apenas para uso interno da Instructure. Esses elementos de dados são considerados “informações privilegiadas” e são protegidos do público em geral. Exemplos de dados internos são correspondência por e-mail, materiais marcados como “Instructure Internal” e outras informações da Instructure não publicadas ou disponibilizadas publicamente. Esses elementos de dados residem em sistemas Instructure e são compartilhados apenas com entidades externas sob um contrato de não divulgação (NDA) totalmente executado.

Públicos

Dados públicos são dados de fontes acessíveis ao público. Exemplos de dados públicos incluem dados de artigos de notícias, comunicados de imprensa e conteúdo pesquisável na Internet. Na Instructure, os dados classificados como públicos não exigem nenhum requisito especial de tratamento de dados.

Verificação de vírus e antimalware

A Instructure executa a verificação antivírus e antimalware de todos os arquivos carregados e armazenados no Canvas com tamanho de arquivo de 64 MB ou menos. A maioria dos malwares normalmente encontrados em arquivos geralmente tem menos de um megabyte (MB) de tamanho, e vírus e malware geralmente não são ativados, a menos que sejam explicitamente abertos no Canvas. Assim como com arquivos de qualquer outra fonte, recomendamos que as instituições acadêmicas sigam as boas práticas de segurança, como executar software antivírus/malware e ter o devido cuidado ao executar arquivos desconhecidos de outros computadores.

Em todos os dispositivos Instructure, utilizamos o software avançado de detecção e resposta de endpoint (EDR) em todos os dispositivos, acima e além do antivírus padrão com acionamento de alerta.

Segurança de Senha

As senhas de usuário são criptografadas. As credenciais usadas para acessar o sistema nunca são armazenadas na infraestrutura do aplicativo. Em vez disso, as senhas são criptografadas unidirecionalmente usando uma combinação de um valor salt aleatório específico do usuário e SHA512, o algoritmo criptográfico de hash unidirecional. As credenciais de entrada são passadas pelo mesmo procedimento e comparadas com o valor armazenado criptografado e salgado. Dessa forma, o Instructure não tem conhecimento ou forma de recuperar as credenciais do usuário.

Complexidade da Senha

Se um cliente do Canvas optar por usar o serviço de autenticação interna do Canvas, o único requisito de senha é um comprimento mínimo de oito caracteres. Se a instituição se integrar a um provedor de identidade externo (por exemplo, LDAP, AD, CAS, SAML, etc.), as configurações de segurança, como políticas de senha, definidas no servidor de autenticação externo serão usadas pelo Canvas.

Ransomware

O robusto programa de segurança da informação da Instructure é executado em um ciclo contínuo de melhoria PDCA. Para mitigar malware e ransomware, utilizamos várias práticas de segurança, conforme recomendado pela Agência de Segurança Cibernética e Infraestrutura dos Estados Unidos (CISA).

Essas práticas incluem (mas não estão limitadas a):

- **Manter os sistemas atualizados;** Remoção de sistemas operacionais e bibliotecas em fim de vida útil e manutenção de sistemas e aplicativos atualizados com patches de segurança.

- **Gerenciamento de Usuários;** Provisionar usuários com menos privilégios e controle de acesso baseado em função. Realização de revisões regulares de acesso de usuários em todos os sistemas e diretórios, especificamente proibindo contas compartilhadas.

- **Segurança de endpoint do usuário;** Utilizando software avançado de detecção e resposta de endpoint (EDR) em todos os dispositivos do usuário, acima e além do antivírus padrão.

- **Autenticação Multifator;** Habilitar a autenticação multifator na frente de todas as VPNs, bastiões e aplicativos para evitar a reutilização de quaisquer credenciais perdidas. Registro e alertas sobre IPs e locais novos e incomuns usados por um usuário para autenticação nos serviços.

- **Recuperação de Desastres;** Um plano abrangente de recuperação de desastres que identifica os componentes críticos de cada serviço e como é feito o backup e a recuperação de cada

componente crítico em resposta a um evento significativo. A recuperação de cada componente crítico é testada regularmente.

- **Mapeamento de dados;** Auditoria de armazenamento de dados confidenciais. Reduzir elementos de dados armazenados apenas para o que é necessário para operar um serviço. Revisões e monitoramento contínuos em sistemas com armazenamento de dados confidenciais.

- **DevOps;** Todo o código passa pela revisão por pares do desenvolvedor antes de ser mesclado no repositório de base de código e é verificado quanto a vulnerabilidades de segurança (incluindo dependências) antes do lançamento para produção.

- **Identificação de Vulnerabilidade;** Endpoints voltados para o público e ambientes internos são verificados em busca de vulnerabilidades regularmente. Terceiros competentes são contratados para testes de penetração direcionados para descobrir problemas de segurança. Testes de segurança de origem coletiva são incentivados e recompensados.

- **Simplifique e Otimize;** Implementamos um conjunto comum de controles de segurança em todas as equipes e serviços. Isso inclui um método consistente de autenticação de usuário para servidores, ambientes de nuvem e serviços de produção.

- **Equipe de Segurança;** Uma equipe de segurança dedicada com a responsabilidade geral de segurança que reside dentro da organização. A equipe de segurança é responsável por todos os aspectos de segurança que estão sendo considerados na comunicação com o gerenciamento, análise de risco e planejamento trimestral e anual para incorporar o trabalho de segurança para todas as equipes.

- **Treinamento;** Treinamento contínuo e regular de segurança da equipe, incluindo, mas não limitado a, testes automatizados de phishing de todos os funcionários e remediação de funcionários propensos a phishing.

Gerenciamento de vulnerabilidades e auditorias de segurança

Revisões Internas de Segurança e Gerenciamento de Vulnerabilidades

A equipe de segurança da Instructure realiza varreduras de vulnerabilidades do ambiente de produção e testes de penetração e base de código de terceiros anualmente. Os membros da equipe de segurança da Instructure têm muitos anos de experiência com auditorias de segurança de grandes corporações e agências governamentais. As políticas e procedimentos de auditoria são revisados regularmente e atualizados conforme necessário pela equipe de segurança. A equipe de segurança da Instructure realiza auditorias internas de segurança completas, prescritivas e abrangentes. Nestas auditorias, a equipe de segurança:

Faz a varredura do aplicativo externamente, usando ferramentas internas e personalizadas construídas internamente.

Documenta possíveis vulnerabilidades, recomenda correções e implementa a correção mais vantajosa. As correções são então retestadas, tanto pelo (s) descobridor (es) original (ais), como por outros integrantes da equipe, novos para o problema.

Faz com que as correções feitas em bibliotecas externas às atividades de desenvolvimento do upstream sejam imediatamente aplicadas e incluídas nos pacotes oficiais, em vez de aguardar a próxima liberação de atualização do Canvas agendada.

Revisões Externas de Segurança

Além de nossas frequentes auditorias de segurança interna realizadas ao longo do ano, a Instructure conduz análises de segurança anuais, abertas e de terceiros. A auditoria de segurança externa aberta é uma maneira pela qual a Instructure pode demonstrar não apenas o estado de segurança do aplicativo, mas também nossa capacidade de resposta a quaisquer vulnerabilidades. A Instructure apresenta vulnerabilidades de segurança para nossos clientes e, como os produtos da Instructure são aplicativos multi-tenant, os clientes nunca experimentam os efeitos adversos devido a atualizações ou patches não aplicados devido a diferenças de versão ou custos adicionais ou tempos de espera por service packs.

Este mesmo nível de resposta é aplicado quando a Instructure recebe informações externas sobre segurança fora do processo formal de auditoria. Para clientes que estão interessados em realizar sua própria auditoria de segurança dos produtos da Instructure, a Instructure irá, mediante solicitação, criar um ambiente onde eles possam realizar varreduras de vulnerabilidades manuais e automatizadas.

Conformidade com SOC 2

A Instructure produz, anualmente, um relatório SOC2 Tipo II que cobre os seguintes princípios: Segurança, Disponibilidade, Confidencialidade, Integridade de Processamento e Privacidade.

Conformidade com ISO 27001

A Instructure também é certificada como compatível com ISO 27001:2013 para produtos como Canvas LMS, Studio, Portfolium e MasteryConnect.

Resposta da Instructure aos Alertas de Segurança

Ao contrário dos produtos licenciados LMS tradicionais com service packs que muitas vezes não resolvem problemas de segurança por semanas ou meses e que devem ser aplicados pelos próprios usuários, os produtos da Instructure são serviços em nuvem com uma única versão da base de código e ambiente de produção para que as atualizações de segurança sejam aplicadas imediata e

automaticamente para toda a base de clientes como parte dos serviços de hospedagem da Instructure.

Varreduras regulares de vulnerabilidade de aplicativos e infraestrutura são conduzidas usando ferramentas de terceiros, scripts personalizados e ferramentas de código aberto. Se alguma vulnerabilidade for detectada, as equipes de segurança e engenharia da Instructure trabalham juntas para analisar, projetar e desenvolver o patch necessário. Os patches relacionados à segurança para o sistema operacional, software aplicativo e bibliotecas são aplicados em uma (1) semana, exceto nos casos que foram determinados como de alta severidade. Se uma vulnerabilidade de segurança de alta gravidade for detectada, consertar a vulnerabilidade receberá a maior prioridade das equipes de segurança e engenharia da Instructure. Os patches de segurança de alta gravidade serão aplicados dentro de vinte e quatro (24) horas pelos melhores esforços comerciais. Na maioria dos casos, a vulnerabilidade pode ser corrigida usando um hot patch sem incorrer em qualquer tempo de inatividade para os ambientes de produção.

A Instructure, em coordenação com a AWS, adota uma abordagem proativa para aplicar os controles SOC 2. As retrospectivas são concluídas após qualquer problema operacional significativo, independentemente do impacto externo, e os documentos retrospectivos (análise da causa raiz) são redigidos para que a causa raiz seja capturada e ações preventivas sejam tomadas no futuro. A implementação das medidas preventivas é monitorada durante as reuniões semanais de operações da Instructure.

Política e Plano de Resposta a Incidentes

A Instructure implementou um conjunto abrangente de tecnologias de segurança, políticas de gerenciamento e revisão, monitoramento de operações e procedimentos de fiscalização para garantir que nosso sistema e segurança de dados atendam ou excedam os estatutos e regulamentos governamentais, os padrões do setor e os requisitos institucionais. A Instructure reconhece que nenhuma organização é impenetrável e, portanto, prepara planos para ajudar a facilitar de forma mais eficaz um incidente de segurança.

Política de Resposta a Incidentes

Fazendo o backup dessas medidas preventivas, a Instructure estabeleceu um conjunto de respostas prescritivas a serem executadas no caso de exposição não autorizada de dados. A exposição de dados ocorre quando informações restritas ou confidenciais são divulgadas, expostas ou razoavelmente consideradas como tendo sido divulgadas ou expostas a uma pessoa, processo ou sistema não autorizado.

A política de exposição a dados da Instructure foi projetada para garantir:

- A detecção mais precoce possível de uma violação de segurança de sistema ou dados;
- Segurança rápida do sistema e dados para evitar mais exposição não autorizada;

- Notificação responsiva aos usuários e outras partes afetadas de que informações confidenciais ou pessoais foram ou podem ter sido expostas ou comprometidas por uma violação na segurança do sistema.

Plano de Resposta a Incidentes

Em caso de violação de segurança e possível exposição não autorizada de dados, o Chief Information Security Officer (CISO) da Instructure supervisionará e executará um plano de ação que esteja em conformidade com as diretrizes descritas nas subseções abaixo. O plano de ação exato a ser executado e a sequência das ações executadas dependerão do tipo e do escopo da violação de segurança.

Determinar o escopo da violação de segurança

Em todos os casos, o CISO e a equipe da Instructure avaliarão rapidamente o status da violação para determinar se a atividade está em andamento. Se a atividade estiver em andamento, a equipe de segurança tomará as medidas necessárias imediatas para interromper a atividade não autorizada, a fim de evitar qualquer perda adicional de dados. Assim que a violação for isolada e interrompida, o CISO e a equipe da Instructure começarão a verificar a extensão da violação, a fonte e o tipo de dados envolvidos, a quantidade de dados e as pessoas afetadas e os recursos do sistema.

Reunir a equipe de resposta a incidentes

O CISO da Instructure montará a equipe de resposta a incidentes. A composição e o encargo da equipe dependerão do tipo de violação e da exposição de dados resultante. A equipe realiza uma avaliação preliminar para ajudar a desenvolver uma resposta personalizada. Uma vez contido o incidente, essa equipe também avaliará as mudanças nos processos, sistemas e/ou políticas para evitar a repetição do evento.

Controlar de Divulgação de Informações

Para garantir que apenas informações precisas e oportunas que não interfiram na investigação em andamento sejam divulgadas, apenas o CISO da Instructure estará autorizado a fornecer informações a qualquer parte fora da equipe de resposta a incidentes.

Alerta à Equipe Administrativa

O CISO da Instructure alertará os administradores seniores apropriados, incluindo a equipe executiva da Instructure, funcionários da instituição cliente, engenheiros de sistema e outros participantes importantes, conforme garantido.

Identificar pessoas afetadas

O CISO da Instructure trabalhará com os funcionários da instituição, incluindo o vice-presidente sênior de engenharia e o vice-presidente de operações da Instructure, e a equipe de resposta a incidentes

para determinar as identidades dos indivíduos afetados e determinar a extensão da exposição dos dados.

Notificar as pessoas afetadas

O CISO da Instructure trabalhará com o vice-presidente sênior de engenharia, conselho geral, vice-presidente de operações e a equipe de resposta a incidentes para elaborar e executar um plano de notificação. O objetivo do plano é fornecer uma notificação completa, precisa e oportuna que atenda ou exceda todos os requisitos legais. No caso de problemas de segurança de alta gravidade, as partes afetadas serão alertadas imediatamente, enquanto as partes indiretamente afetadas serão alertadas dentro de quarenta e oito (48) horas. Esses requisitos legais variam de estado para estado. Trabalhando com as partes apropriadas, o CISO da Instructure e a equipe de resposta a incidentes notificam todos os indivíduos afetados e desenvolvem estratégias de remediação conforme apropriado e suficiente para a situação.

Gerenciar a resolução e consequências do incidente

O CISO da Instructure e a equipe de resposta a incidentes continuarão a atualizar e comunicar o status da resposta, determinar as próximas etapas e desenvolver um plano post mortem para revisar a eficiência e eficácia da resposta e desenvolver processos e procedimentos futuros de prevenção e/ou mitigação.

Conformidade com a LGPD

A Instructure está em conformidade com a Lei Geral de Proteção de Dados brasileira. A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O objetivo desta Política de Proteção de Dados Pessoais adotada pela Instructure é descrever a conformidade da Instructure com o processamento de Dados Pessoais de acordo com a Lei Geral de Proteção de Dados do Brasil.

Essa Política se aplica a Instructure Inc. e suas subsidiárias integrais (coletivamente “Instructure") que processam Dados Pessoais (definidos no documento sobre LGPD a Instructure).

Conformidade da FERPA

Overview da FERPA

A FERPA é uma lei federal dos EUA que protege a privacidade dos registros educacionais dos alunos. A lei se aplica a todas as escolas e instituições que recebem fundos de acordo com o programa aplicável do Departamento de Educação dos EUA. A FERPA oferece aos alunos e, em alguns casos, aos pais, o direito de inspecionar seus registros educacionais e alguma capacidade de controlar a divulgação de informações contidas em seus registros educacionais.

A FERPA exige que as agências educacionais, que divulgam informações de identificação pessoal do registro educacional de um aluno para outros funcionários da escola, usem “métodos razoáveis” para

garantir que os funcionários da escola tenham acesso apenas aos registros educacionais nos quais tenham interesses educacionais legítimos.

Os produtos Instructure são construídos para cumprir com a Lei de Privacidade e Direitos Educacionais da Família (FERPA) por design, e eles se integram prontamente com outros sistemas de campus para evitar acesso não autorizado a dados protegidos por FERPA. Seja implementado como um sistema autônomo ou como um componente totalmente integrado da infraestrutura de TI/SI do campus, nossos produtos fornecem às instituições e agências educacionais vários mecanismos e tecnologias para gerenciar, fazer cumprir e cumprir as disposições da FERPA e cumprir suas responsabilidades sob seus requisitos.

Cumprimento da FERPA

Cada usuário tem um portal exclusivo com base em sua função. O Canvas oferece funções e permissões que permitem que os administradores tenham um grande grau de controle sobre quais informações cada função tem acesso. Os usuários, com base em sua autenticação bem-sucedida e função designada, só terão acesso ao conteúdo conforme projetado pelo cliente final. Para manter a conformidade com os regulamentos da FERPA, o Canvas fornecerá ao cliente todas as ferramentas necessárias para manter sua conformidade com a FERPA. Exemplos de recursos compatíveis com FERPA incluem:

- O Canvas permite o acesso às informações do aluno apenas para aqueles a quem a permissão é concedida. Por padrão, esse é o administrador da instância do Canvas da Instituição e o corpo docente que está ministrando cursos nos quais o aluno está matriculado. É possível conceder permissão a outras pessoas identificadas pela instituição como "Funcionários da Escola" (conforme descrito nas diretrizes da FERPA), ou remover a permissão de administradores ou professores. Em suma, a instituição está no controle total.

- Todo o acesso ao Canvas é criptografado. Não há exceções. Ao transmitir dados do SIS, as informações estão seguras em trânsito e, quando chegam ao sistema Canvas, são protegidas pela mesma conta e permissões baseadas em função que protegem todos os outros dados.

Observação: Deve-se enfatizar que a FERPA é de responsabilidade do cliente: ela é proprietária dos dados e está no controle total de todo o acesso a eles. Contanto que os clientes sigam as melhores práticas do Canvas, as informações privadas permanecerão privadas no Canvas.

Overview da HIPAA

O Canvas não é compatível com HIPAA. A conformidade com HIPAA não se tornou uma iniciativa de produto principal, pois o Canvas é usado no ambiente educacional e não se destina a armazenar informações de saúde. Como tal, não podemos assinar nenhum Contrato de Associado Comercial (BAA).

Padrões de Segurança de Dados da Indústria de Cartões de Pagamento ("PCI") ("DSS")

Como um LMS, o Canvas não armazena, processa ou transmite dados de cartão de crédito e, como tal, não é obrigado a aderir ao PCI DSS.

O Canvas Catalog, no entanto, redireciona os usuários para gateways de pagamento integrados configurados pela instituição cliente. O catálogo está em conformidade com o PCI DSS, conforme demonstrado pelo formulário D do questionário de auto avaliação (SAQ) da Instructure. Este SAQ está disponível mediante solicitação e assinatura de um contrato de confidencialidade.

General Data Protection Regulation (GDPR)

GDPR significa o Regulamento Geral de Proteção de Dados da UE. O GDPR é uma lei da União Europeia (“UE”) que regula os dados pessoais de indivíduos na UE. O GDPR harmonizou a lei de proteção de dados em toda a UE e introduziu mudanças abrangentes que exigem que as empresas façam atualizações significativas em suas políticas e práticas de privacidade e segurança. A Instructure está comprometida em ajudar nossos clientes a cumprir o GDPR.

A Instructure está em conformidade com o GDPR desde a data de aplicação (25 de maio de 2018).

Para garantir a conformidade contínua com o GDPR, a Instructure faz o seguinte:

- Educa a organização sobre o GDPR e seus requisitos
- Conduziu uma análise de lacunas do GDPR com a ajuda de um escritório de advocacia externo respeitável com experiência em GDPR e fechou essas lacunas
- Mantém uma lista atualizada dos dados pessoais que a Instructure detém, de onde veio e com quem a Instructure pode compartilhá-los
- Mantém os avisos de privacidade atuais que estão em conformidade com o GDPR
- Garante que os procedimentos existentes cubram todos os direitos que os indivíduos têm sob o GDPR
- Identifica nossa base legal para processar dados pessoais, documentá-los e atualizar nosso aviso de privacidade para explicá-los aos indivíduos.
- Analisa como o Instructure obtém, registra e gerencia o consentimento.
- Revisa e atualiza contratos com terceiros para garantir que nossas obrigações de privacidade estejam atualizadas.
- Garante que os procedimentos corretos estejam em vigor para detectar, relatar e investigar uma violação de dados pessoais.

- Mantém processos para Avaliações de Impacto de Proteção de Dados.
- Nomeou um Encarregado de Proteção de Dados.

Salvaguardas para transferência de dados transfronteiriços

Um dos requisitos do GDPR é que quaisquer dados pessoais transferidos "além-fronteiras", ou seja, fora da UE, só podem ser movidos de acordo com um mecanismo legal.

A Instructure usa as cláusulas contratuais padrão da Comissão Europeia (cláusulas modelo) como um método legal para transferir dados pessoais para fora da UE. Ao incorporar as cláusulas do modelo no Adendo de Processamento de Dados da Instructure ("DPA"), os controladores de dados (clientes da Instructure na UE) e os processadores de dados (Instructure) estão contratualmente obrigados a certas salvaguardas técnicas e organizacionais relacionadas a (na UE de Instructure usuários finais dos clientes) direitos de privacidade de cada indivíduo.

Conclusão

Sabemos que a segurança é primordial para nossos clientes em um mundo orientado a SaaS. É por isso que tomamos extremo cuidado para implementar mecanismos preventivos e de detecção, bem como processos, controles e ferramentas em camadas, ajudando a mitigar riscos que podem afetar dados, pessoas, sistemas, operações, produtos e nossa missão como empresa. Conforme descrito neste documento, nossa equipe de segurança dedicada está repleta de profissionais de segurança apaixonados, qualificados e experientes, que, além de garantir a conformidade com a avaliação de terceiros, como a estrutura de controle da organização de serviços, se concentram na detecção e proteção contra danos e ganhar e manter a sua confiança.