Segurança da informação na SumUp

Um ISMS (Information Security Management System, sistema de gerenciamento de segurança da informação) é conduzido por uma equipe especializada de segurança da informação, estabelecendo políticas e padrões de segurança claros e definindo medidas adequadas de segurança técnica e organizacional para fornecer proteção e conformidade de informações.

Sistema de Gerenciamento de Segurança da Informação (ISMS)

A SumUp faz questão de fornecer aplicativos e serviços confiáveis aos consumidores. A SumUp se preocupa muito com a proteção das informações do SumUp, bem como com a proteção de informações confidenciais e dados privados confiados à SumUp por seus consumidores contra potenciais ameaças internas, externas, deliberadas ou acidentais.

A SumUp estabelece e opera um ISMS baseado nos padrões ISO 27001 com foco nos seguintes quatro pilares principais:

Certifique-se de um nível adequado de confiden-cialidade, integridade e disponibilidade para serviços e informações do SumUp.

Fornecer proteção adequada dos ativos e ativos da SumUp confiados à SumUp por seus consumidores.

Minimizar o risco de danos, prevenindo incidentes de segurança e reduzindo seu potencial impacto.

Garantir o cumprimento de todas as leis, requisitos regulatórios e normas obrigatórias.

A segurança da informação é uma missão para todos, e as funções de segurança da informação são bem definidas em todos os níveis da organização, incluindo, gerenciamento executivo e todos os usuários.

Equipe de Segurança da Informação

A equipe de segurança da informação é um elemento da tribo de Gerenciamento de Risco e Compliance Global (GRC) da SumUp, responsável pelas funções de risco, segurança e conformidade e faz parte da estratégia de defesa de três linhas definida na SumUp.

Sob a supervisão do SVP de Segurança da Informação e do Head de Segurança da Informação, a equipe de segurança tem o papel de manter e melhorar continuamente o ISMS da SumUp com as seguintes funções-chave:

Projetar e implementar políticas, procedimentos e padrões de segurança da informação, bem como desenvolver controles de segurança associados.

Promover a cultura de segurança da SumUp com a implementação de um programa de conscientização, treinamento e aprendizagem de segurança da informação para garantir que as funções e responsabilidades individuais em relação ao domínio sejam entendidas por todos.

Realizar avaliação contínua das práticas e tecnologias de segurança atuais, a fim de identificar oportunidades de melhoria.

Estabelecer uma resposta a incidentes de segurança da informação, incluindo cenários que abrangem os principais incidentes possíveis e lidar com tais incidentes de acordo.

Garantir monitoramento de segurança, gerenciamento operacional de ferramentas de controle de segurança e supervisão de mecanismos de segurança de TI, como gerenciamento de acesso, implantação de patches, gerenciamento de chaves etc.

Fornecer assessoria, orientação e suporte a outras equipes sobre a área de segurança da informação durante projetos, implantações de tecnologia ou sobre o uso de ativos SumUp (por exemplo, informações, redes, sistemas de TI...).

Avaliar periodicamente riscos à segurança da informação para a qual a SumUp pode ser exposta e fornecer recomendações de gerenciamento de riscos, bem como as melhores práticas a serem seguidas por todos os SumUppers.

Garantir o cumprimento das políticas, procedimentos e normas de segurança da informação internas, bem como com as normas legais e regulamentares e manter certificações atuais de segurança da informação, como o PCI-DSS.

Políticas e Normas

A SumUp estabeleceu um conjunto de políticas, padrões e procedimentos abrangentes de Segurança da Informação para apoiar seu ISMS, incluindo, por exemplo, política de segurança da informação, política de controle de acesso, classificação e manuseio de informações, uso aceitável etc.

Todas as políticas de segurança da informação são aprovadas pelos conselhos da SumUp e comunicadas aos funcionários e partes externas relevantes, quando apropriado.

As políticas são revisadas pelo menos anualmente e atualizadas para serem adequadas aos padrões atuais do setor e para refletir quaisquer mudanças nos ambientes ou objetivos de negócios da SumUp.

Medidas técnicas e organizacionais de segurança

A SumUp mantém medidas técnicas e organizacionais de segurança para garantir um nível de segurança adequado à exposição de risco de seus serviços e dados no escopo desses serviços. A SumUp definiu também uma combinação de medidas preventivas, detectivas e corretivas que são regularmente avaliadas e adaptadas para acompanhar a evolução do cenário de ameaças.

Segue uma lista não exaustiva das medidas de segurança em vigor na SumUp.

Controle de acesso

A SumUp implementou controles de acesso físico e lógico nos métodos de autenticação e autorização em seus edifícios, serviços, redes e sistemas de TI, a fim de fornecer acesso autorizado, granular, auditável e apropriado, e garantir a preservação adequada da confidencialidade, integridade e disponibilidade dos dados. A SumUp gerencia o acesso aos seus sistemas de produção por meio de uma solução IAM (Identity Access Management, gerenciamento de acesso de identidade).

Os direitos de acesso são concedidos com base nas funções de trabalho e seguindo os princípios de menor privilégio e necessidade de negócio. O princípio do menor acesso significa dar a uma conta de usuário apenas aqueles privilégios que são essenciais para as funções de trabalho deste usuário. A necessidade de saber restringe o acesso a informações confidenciais apenas àqueles que são essenciais para cumprir a função de trabalho do usuário.

Controles Operacionais

A SumUp adota e mantém um conjunto de tecnologias, processos e segue as melhores práticas de segurança atuais no mercado para proteger seus sistemas e serviços de Tecnologia da Informação (TI) contra acesso não autorizado, intrusão potencial, ataques e seu potencial impacto na confidencialidade e integridade dos dados, bem como na disponibilidade de serviços.

Os data-centers da SumUp são baseados na Europa e a SumUp seleciona com muito cuidado seus provedores de hospedagem, garantindo que eles estejam pelo menos em conformidade e certificados a vários padrões de segurança, como ISO 27001, PCI DSS, SOC 1/2/3.

A SumUp implementa controles perimétricos para garantir a segurança de sua rede usando firewalls de instâncias de perímetro e servidor, sistemas de detecção de intrusões, firewall de aplicativos web (WAF) e outras ferramentas de tráfego filtrantes em combinação com segmentação de rede e zona desmilitarizada (DMZ).

O SumUp impõe o gerenciamento de patches, *infrastructure as a code*, solução antivírus, programa de *bug bounty* combinado com varreduras regulares de vulnerabilidade externa e interna e testes de penetração para reduzir os riscos de vulnerabilidade e malware.

Além disso, a SumUp possui sistemas para realizar o monitoramento de log de eventos de segurança e monitorar a saúde, disponibilidade e escalabilidade do sistema de componentes críticos de infraestrutura.

Gerenciamento de incidentes

O SOC (Third-party Security Operation Center, centro de operação de segurança de terceiros) está monitorando ativamente eventos de segurança 24 horas por dia, 7 dias por semana, para detectar e escalar eventos suspeitos para a equipe do SumUp. A SumUp estabelece procedimentos específicos de resposta a incidentes e planos de escala para estar preparado para eventos não planejados, reagir de forma rápida e organizada, responder adequadamente e aprender lições para evitar a ocorrência do mesmo tipo de incidente.

Continuidade de Negócios

Para garantir a continuidade de seus serviços, a SumUp desenvolve sua continuidade de negócios, recuperação de desastres e backup seguindo padrões conhecidos *on the place* e realiza testes em planos e procedimentos relacionados pelo menos anualmente.

A estratégia global da SumUp é evitar o uso de redes internas e depender em grande medida de serviços baseados em nuvem ou hospedados externamente para cobrir a operação interna e o armazenamento ou compartilhamento de dados. Com isso, a SumUp opera independentemente de qualquer área geográfica ou locais específicos de escritórios e depende principalmente da disponibilidade de internet.

A SumUp desenvolve planos de ações específicas para remediar seus principais riscos, como interrupção de infraestrutura com cenários que cobrem, por exemplo, a paralisação do data center de um único provedor, a paralisação de toda a região do provedor ou a paralisação completa do provedor (Estratégia de Saída do provedor).

Proteção de informações

A proteção de informações é o fator chave dos negócios da SumUp, pois incidentes ligados a tópicos de informação afetam diretamente a confiança dos clientes e a reputação da SumUp

A SumUp classifica as informações com base em sua criticidade, olhando para o impacto dos negócios e do cliente sobre a violação de um ou mais fatores de confidencialidade, integridade e disponibilidade em relação a essas informações. Com base em seu nível de classificação (público, interno, confidencial, secreto), as informações são tratadas, processadas, armazenadas ou descartadas com proteção de segurança adequada aplicada, como criptografia, anonimização, período específico de retenção etc.

Como a SumUp processa dados pessoais, bem como dados de pagamento e titulares de cartão, o SumUp tem foco em processar esses dados de acordo com as leis de privacidade aplicáveis e as diretrizes da Payment Card Industry Data Security Standard.

Conformidade

PCI-DSS

Armazenar, processar e/ou transmitir dados de pagamento e titulares de cartão faz parte do negócio principal da SumUp. Tais atividades são fortemente supervisionadas pelo Conselho de Normas de Segurança da Indústria de Cartões de Pagamento (PCI-SSC), que é o órgão regulador em relação à Indústria de Cartões de Pagamento (PCI), a fim de garantir pagamentos, dados de pagamento e processos globalmente.

A SumUp é obrigada a cumprir o padrão global de segurança da informação estabelecido pelo PCI-SCC chamado Payment Card Industry Data Security Standard (PCI-DSS).

A SumUp é certificada PCI-DSS como um provedor de serviços nível 1.

PCI-PTS

O SumUp reconhece a grande importância em fornecer aos seus comerciantes dispositivos de pagamento seguros e optou por estar em conformidade com o Padrão de Segurança de Transações (PCI-PTS) da indústria de cartões de pagamento para esses dispositivos.

A lista de dispositivos SumUp PTS aprovados pode ser encontrada em **dispositivos de transação de PIN PCI.**