ManageEngine
Log360

Um Guia de Sobrevivência do administrador de segurança para a GDPR

www.manageengine.com/br/log-management

Índice

Escopo deste guia

Todas as empresas que gerenciam os dados pessoais dos cidadãos da UE precisam estar em conformidade com o Regulamento Geral de Proteção de Dados (GDPR) antes de 25 de maio de 2018. A não conformidade com este regulamento implica em uma grande penalidade – até quatro por cento do volume de negócios anual global de uma empresa ou 20 milhões de euros, o que for maior.

Essa multa não é o único destaque da GDPR. Como um dos mais rigorosos mandatos de conformidade dos últimos tempos, ela tem como objetivo padronizar a forma como as organizações lidam com os dados pessoais. A GDPR estabelece requisitos que garantem a segurança dos dados pessoais em todas as etapas do tratamento de dados, incluindo coleta, armazenamento, processamento, transferência e exclusão.

Traduzir os requisitos de segurança da GDPR em itens acionáveis é o trabalho mais difícil para qualquer profissional de segurança. Este guia tem como objetivo fornecer as ações exatas que os administradores de segurança e os diretores de proteção de dados podem tomar para garantir a conformidade com o regulamento de sua organização.

Os requisitos da GDPR que demandam sua atenção

Com 11 capítulos e 99 artigos, a GDPR estabelece regras para a proteção de dados pessoais em todas as etapas, incluindo dados que estão em repouso e em movimento. Mas mais de 75% desta exigência regulamentar dita a forma como as organizações devem coletar dados pessoais e lidar com os direitos dos titulares. Os 25% restantes dos requisitos da lei, que descrevem a segurança das regras de processamento, precisam da atenção dos profissionais de segurança.

Visão geral dos requisitos que precisam da atenção dos profissionais de segurança

- Princípios relacionados ao processamento de dados pessoais: Artigo 5
  - Usar medidas técnicas ou organizacionais apropriadas para provar que os dados são processados de maneira segura e protegidos contra processamento não autorizado ou ilegal, perda acidental e destruição ou danos.
- Responsabilidades de um controlador: Artigo 24
  - Implantar medidas técnicas e organizacionais e implementar políticas de proteção de dados para garantir e demonstrar que o processamento de dados está sendo realizado de acordo com os requisitos.
- Segurança do processamento: Artigo 32
  - Implantação de medidas técnicas:
    - Para garantir que os dados pessoais sejam criptografados.
    - Para garantir que a confidencialidade, integridade, disponibilidade e a resiliência do sistema e do serviço que armazenam dados pessoais sejam mantidas.
    - Para restaurar a disponibilidade e o acesso a dados pessoais no caso de um erro.
  - Implementação de medidas de segurança para garantir que os dados pessoais sejam protegidos contra destruição acidental ou ilegal, perda, alteração, divulgação ou acesso não autorizado e transmissão.
- Notificação de violação de dados pessoais à autoridade de supervisão: Artigo 33
  - Implantar medidas técnicas para detectar e relatar uma violação de dados pessoais em no máximo 72 horas após sua ocorrência.
  - Gerar relatórios de incidentes que fornecem informações sobre a natureza da violação de dados pessoais, incluindo as categorias e o número aproximado de registros de dados pessoais e os titulares de dados afetados.
  - Documentar a violação, seus efeitos e as ações corretivas tomadas.

Preparar as etapas para a conformidade com o regulamento GDPR

Antes de começar a traduzir os requisitos da GDPR em políticas de segurança, você deve:

- **Entender quem você é:** A GDPR categoriza cada organização como um controlador ou um processador. Embora os controladores sejam responsáveis por coletar dados pessoais de titulares, os processadores executam operações de dados: armazenamento, transmissão, estruturação, alteração, exclusão e muito mais – em nome do controlador. Às vezes, uma organização pode funcionar como controlador e processador. Nesse caso, certifique-se de que você está cumprindo as responsabilidades declaradas para ambos.

  Suas responsabilidades são diferentes. A principal função de um controlador é apenas coletar dados pessoais de acordo com os requisitos da GDPR e verificar constantemente se o processador está executando suas operações de acordo com as regras. O processador, por outro lado, precisa configurar políticas de segurança adequadas dentro de sua organização e provar ao controlador que as operações de dados estão sendo executadas de acordo com os regulamentos. Se ocorrer um incidente, como uma violação ou qualquer outra ameaça aos dados pessoais, os processadores precisam reportá-lo ao controlador e às autoridades de supervisão imediatamente.

- **Saber que tipo de dados pessoais sua organização processa:** Dependendo do contexto de sua empresa, familiarize-se com o tipo de dados pessoais que sua organização processa. Além disso, entenda o fluxo de dados, onde a coleta de dados começa, onde eles são armazenados, que tipo de aplicação processa os dados pessoais e quando devem ser excluídos.

1. Descoberta, isolamento e backup de dados

A primeira etapa para garantir a segurança dos dados pessoais é descobrir onde eles residem em sua organização. Eles podem ser armazenados em bancos de dados, servidores de arquivos ou até mesmo em planilhas do Excel e documentos do Word.

Depois de descobrir onde os dados pessoais residem, isole-os do restante das informações não confidenciais em sua organização.

Por que é tão importante separar esses dados de informações não confidenciais?

- O isolamento ajuda a definir as configurações de segurança exclusivas para dados pessoais. Essas configurações podem funcionar como uma camada adicional de segurança.
- O isolamento de dados pessoais torna a auditoria eficiente. Habilitar a auditoria granular somente para os sistemas que contêm dados pessoais ajudará você a rastrear facilmente ameaças potenciais e reduzir o risco de perder um incidente de segurança crítico que possa levar a uma violação de dados.
- É mais fácil restringir o acesso a dados pessoais depois de os ter isolado. Depois dessa etapa feita, configure vários níveis de políticas de acesso para garantir que apenas pessoas autorizadas possam acessá-los.
- O isolamento de dados pessoais sempre que possível ajuda não apenas a adicionar uma camada de segurança extra; também ajuda a entender o fluxo de dados, onde eles estão sendo coletados ou alimentados, quanto tempo estão armazenados e quais processos estão sendo executados nele.

Depois de ter isolado os dados pessoais, faça o backup para que você possa restaurar rapidamente a disponibilidade e o acesso a eles (artigo 32 (1)(c)) em caso de erro.

2. Definição de configurações de segurança

O artigo 32 da GDPR (Segurança do Processamento) instrui as empresas a implantar medidas técnicas apropriadas para garantir a segurança dos dados. Para cumprir os requisitos estabelecidos neste artigo, você deve fortalecer a segurança nas plataformas onde os dados pessoais são armazenados.

Cada uma das plataformas que armazenam dados pessoais (por exemplo, sistemas operacionais, aplicações e dispositivos) tem configurações de segurança diferentes e você deve tomar cuidado adequado para configurar cada plataforma separadamente.

Abaixo está uma lista de melhores práticas de proteção de segurança para plataformas e dispositivos comuns. Se você precisar de informações granulares sobre como proteger sua rede, sinta-se à vontade para entrar em contato com nossos especialistas em segurança de TI.

Tabela 1: Configurações de segurança para plataformas comuns.

Plataforma/dispositivo	Configurações de segurança
Firewall 	1. Nem todos os funcionários de sua empresa precisam acessar os dados pessoais armazenados. Adicione uma camada extra de segurança adicionando regras que limitam o acesso a servidores onde dados pessoais a hosts específicos da rede são armazenados. Dessa maneira, você dificulta o acesso ou o roubo por funcionários não autorizados ou usuários mal-intencionados que tenham roubado credenciais de usuários privilegiados. 2. Configure regras que permitem o tráfego para portas/serviços de destino específicos. 3. Configure regras de firewall para impedir o tráfego de fontes ilegítimas. Isso ajuda a detectar e, em certa medida, impedir ataques externos à segurança.

Windows Server ou servidor de arquivos 	1. Configure grupos de segurança. Inclua apenas usuários privilegiados que devem acessar dados pessoais. 2. Configure políticas de grupo que concedam privilégios exclusivamente aos grupos de segurança associados ao acesso a dados pessoais. 3. Configure as listas de controle de acesso (ACLs) para permitir/negar granularmente que as operações sejam executadas em dados pessoais armazenados como arquivos e pastas.
Banco de dados MS SQL 	1. Configure regras de firewall para que o SQL Server não fique exposto à internet. 2. Renomeie as credenciais padrão da conta privilegiada. Especialmente a conta sysadmin padrão. 3. Configure políticas de senha complexas e rígidas para as contas de login de automatização do servidor (SA) e do SQL Server. 4. Altere as portas padrão associadas à instalação do SQL Server. 5. Habilite a Autenticação do Windows em vez da Autenticação SQL. A Autenticação do Windows valida as credenciais dos usuários com base no token principal do Windows no sistema operacional.
Banco de dados Oracle 	1. Forneça privilégios de CRIAÇÃO DE TRABALHO EXTERNO somente para administradores de banco de dados. 2. Aplique políticas de senha rígidas e complexas. Por exemplo, regras rigorosas para atualizar e criar senhas. 3. Ative a **proteção do dicionário** de dados configurando o parâmetro de inicialização **07_DICTIONARY_ACCESSIBILITY** como FALSO. Isso impede que usuários com **qualquer** privilégio acessem o dicionário de dados. Um dicionário de dados é um conjunto de tabelas de banco de dados que armazena informações críticas, como nomes de usuários de banco de dados, privilégios e funções dos usuários, informações de auditoria etc. Portanto, torna-se essencial o proteger.

Instância do Amazon Web Services (AWS) 	1. Marque os dados pessoais como confidenciais e limite seu acesso com essa etiqueta, configurando permissões no nível do bucket ou do objeto, além das políticas de gerenciamento de acesso e identidade (IAM). 2. Criptografe os dados pessoais que residem no AWS RDS e EBS usando opções de criptografia em nível de arquivo, partição, volume ou aplicação. 3. Na Amazon S3, ative o Controle de versão para que você possa restaurar dados pessoais em caso de modificações acidentais ou intencionais de dados não autorizados. 4. Para proteger dados pessoais em trânsito, especialmente quando estiver atravessando uma rede pública, criptografe os dados usando IPSec ESP e/ou SSL/TLS.

3. Configuração de alertas em uma solução de segurança para detectar incidentes

Depois de definir as configurações de segurança básica e avançada, você precisa ativar a auditoria. Ela ajuda a rastrear todas as atividades que estão acontecendo em sua rede. Depois de habilitar as políticas de auditoria, configure perfis de alerta nas soluções de segurança para detectar imediatamente qualquer desvio do comportamento normal. Essas soluções devem incluir o gerenciamento de eventos e informações de segurança (SIEM), a prevenção contra perda de dados (DLP) ou o gerenciamento unificado de ameaças (UTM).

Isso ajuda a bloquear antecipadamente qualquer tentativa de violação e, assim, evitar que seus dados sejam expostos ou manuseados incorretamente.

Regras para configurar alertas de segurança:

- Habilite a auditoria em todas as plataformas. Certifique-se de ativar somente as políticas de auditoria necessárias; a ativação de todas as políticas diminuirá a velocidade dos sistemas e provocará muitos falsos positivos.
- Defina a linha de base para a sua atividade de rede normal. Ajuste automaticamente sua solução de segurança para detectar qualquer anormalidade.
- Detecte incidentes críticos, como:
    a. Alterações de regra de firewall não autorizadas
    b. Modificações de associações a grupos
    c. Alterações de políticas de grupo
    d. Anomalias no comportamento do usuário – muitas falhas de logon, um logon de um local incomum, encaminhamento de privilégios, etc.
    e. Alterações nas permissões de arquivo ou pasta e alterações nas ACLs
    f. Alterações na permissão do usuário
    g. Alterações nas contas e funções do servidor do banco de dados
- Vincule sua solução de segurança a um sistema de gerenciamento de incidentes adequado para que você possa estabelecer a responsabilização pelas investigações de incidentes.

4. Configuração das notificações para detectar instantaneamente tentativas de violação

Na seção anterior, abordamos a detecção de incidentes, que são ameaças potenciais. Agora, falaremos sobre a configuração de notificações para detectar uma violação contínua ou uma que já ocorreu.

De acordo com o artigo 33 da GDPR (notificação de violação de dados pessoais às autoridades de supervisão), as organizações não devem levar mais de 72 horas para detectar e relatar uma violação de dados.

O que você precisa fazer

Configure perfis de alerta para detectar tentativas comuns de violação de dados, como injeção de SQL, ataques de ransomware, ataques de logon, instalação de malware, ataques de recusa de serviço (DoS), ataques de recusa de serviço distribuída (DDoS) e muito mais.

Escolha uma solução de segurança que permita criar regras personalizadas para detectar padrões de ataque.

Analise o padrão de um ataque ocorrido em seu ambiente e identifique seus vários indicadores de comprometimento (IoCs). Configure alertas personalizados que correlacionem esses IoCs e inicie um fluxo de trabalho automático para conter ataques de um tipo semelhante no futuro, bem em seu estágio inicial.

5. Geração de um relatório de incidente pós-violação para avaliações

Gerar um relatório de incidentes por meio de análise forense é tão importante quanto detectar violações por dois motivos:

1. Um relatório de incidentes ajuda a determinar o impacto total da violação.
2. O relatório geralmente contém detalhes complexos sobre o ataque, incluindo o ponto de entrada vulnerável e seu padrão. É essencial manter essas informações para bloquear preventivamente violações semelhantes no futuro.

O que deve ser abordado em um relatório de incidentes?

O artigo 33 da GDPR descreve os detalhes que devem ser incluídos em um relatório de incidentes. Certifique-se de:

- Elaborar sobre o incidente de violação de dados pessoais, como aconteceu, quantos registros foram afetados e o número de titulares que podem ser afetados pela violação.
- Fornecer o nome e as informações de contato do diretor de proteção de dados ou do profissional de segurança que pode fornecer mais detalhes sobre a violação de dados.
- Descrever a consequência da violação de dados pessoais, por exemplo, quais foram perdidos ou modificados.
- Destaque as medidas de segurança tomadas para lidar com a violação de dados. Isso inclui as medidas tomadas para conter (no caso de uma violação contínua) e atenuar o efeito adverso do ataque, bem como as medidas apropriadas tomadas para fortalecer a segurança e bloquear preventivamente violações semelhantes no futuro.

A ManageEngine ajuda a cumprir os requisitos do regulamento GDPR?

Com certeza. A ManageEngine, empresa de gerenciamento de TI em tempo real, tem uma ampla variedade de soluções de segurança de TI que podem ajudá-lo a cumprir os requisitos de segurança do regulamento GDPR. Lembre-se de que a rede de cada organização é exclusiva e não há nenhum produto pontual que ajude a atender a todas as exigências de conformidade. No entanto, a ManageEngine integra seus produtos de segurança em uma única solução que ajuda a resolver vários desafios de conformidade com eficiência.

Por exemplo, o Log360, a solução abrangente de SIEM da ManageEngine, inclui:

- ADAudit Plus, uma ferramenta de auditoria em tempo real do Active Directory, que ajuda a detectar e atenuar ameaças internas.
- EventLog Analyzer, uma ferramenta de gerenciamento de logs, que ajuda a atenuar ataques de segurança externos e a realizar análises forenses eficientes.
- Cloud Security Plus, uma ferramenta de gerenciamento de logs em nuvem pública, que ajuda a analisar o comportamento do usuário em plataformas como Amazon Web Services e Azure.
- O365 Manager Plus , uma ferramenta completa de relatórios e auditoria do Office 365, que ajuda a detectar comportamentos anômalos no Office 365.

Com sua ampla variedade de recursos, o Log360 será sua melhor opção para resolver seus desafios do RGPD.

Explore o Log360 | Saiba mais

Explore o Log360

ManageEngine
Log360

O Log360 é uma abrangente solução SIEM que ajuda os profissionais de segurança a atender às suas pesadas necessidades de auditoria, segurança e conformidade. Com mais de 1.200 relatórios predefinidos, 900 perfis de alerta e mais de 70 ações e regras de correlação, essa solução pode detectar e atenuar ameaças internas e externas. O recurso de auditoria profunda do Active Directory do Log360 ajuda os administradores a monitorar de perto a atividade privilegiada do usuário e outros comportamentos para detectar anomalias instantaneamente. O Log360 também é compatível com mais de 700 fontes de log, incluindo roteadores, switches, firewalls, IDS/IPS, servidores, bancos de dados e servidores da web. Ele coleta, analisa, correlaciona e arquiva dados de log dessas fontes e garante a segurança de dados 24 horas por dia, 7 dias por semana.

Experimente o teste grátis do Log360

Sobre a autora

Subhalakshmi Ganapathy atualmente trabalha como Analista Sênior de Marketing de Produtos para soluções de Segurança de TI na ManageEngine. Ela tem conhecimento profundo sobre segurança da informação e gerenciamento de conformidade e ministra orientação estratégica para empresas sobre gerenciamento de eventos e informações de segurança (SIEM), segurança de rede e privacidade de dados.

Entre em contato com a Subha pelo e-mail subhalakshmi.g@manageengine.com.