ManageEngine
Log360

A função da TI na conquista da conformidade com a SOX

www.manageengine.com/br/log-management

Introdução

Em 2002, O Congresso dos EUA aprovou a Lei Sarbanes-Oxley (SOX) para proteger os interesses dos acionistas e do público. O ato protege contra erros e más práticas em sistemas e políticas de contabilidade empresarial, obrigando medidas de segurança adequadas, procedimentos transparentes e divulgações corporativas precisas.

A lei SOX foi redigida em resposta aos escândalos contábeis em empresas proeminentes como Enron e Arthur Andersen, o que fez com que os investidores perdessem bilhões de dólares. Ao melhorar a governança corporativa e a responsabilidade, o ato visa minimizar a chance de práticas contábeis fraudulentas por parte das empresas e firmas de auditoria.

Todas as empresas, americanas ou outras, registradas na SEC (Securities and Exchange Commission), juntamente com as empresas que prestam serviços financeiros a estas, devem cumprir este ato. Isso significa que todas as empresas norte-americanas de capital aberto, empresas não norte-americanas de capital aberto com presença nos EUA, empresas que procuram se tornar públicas e empresas que fornecem a todas elas serviços financeiros estão sujeitas à conformidade com a SOX.

A conformidade com a SOX requer grandes contribuições dos departamentos financeiro e de TI de uma empresa. Este documento se concentra no lado da TI que visa alcançar a conformidade com a SOX.

Seções da SOX relevantes para o departamento de TI

Seção	O que é
Seção 302: Responsabilidade corporativa para relatórios financeiros	Os principais executivos e diretores financeiros de uma empresa têm a responsabilidade final pela precisão dos relatórios financeiros e pelos controles internos implementados nos sistemas contábeis.
Seção 404: Avaliação de gerenciamento de controles internos	Todos os relatórios financeiros anuais devem incluir um relatório de controle interno que: a. Declara que a gerência é responsável pela estrutura de controle interno. b. Inclui uma avaliação da eficácia da estrutura de controle interno. c. Requer que um auditor externo registrado ateste a precisão dessa avaliação.
Seção 409: Divulgações do emissor em tempo real	As empresas devem divulgar às partes interessadas e ao público todas as informações que possam afetar suas condições ou operações financeiras, de maneira rápida e oportuna.
Seção 802: Garantir a retenção de logs	Todas as comunicações físicas e eletrônicas e outros registros relacionados às transações financeiras de uma empresa devem ser mantidos e disponibilizados para auditores externos por um mínimo de cinco anos.

Como a TI pode ajudar na conformidade com a SOX

Como a maioria dos registros financeiros é armazenada eletronicamente, os processos e sistemas de TI da sua organização desempenham uma função fundamental na obtenção da conformidade com a SOX. Dados financeiros perdidos ou danificados devido a erro ou descuido não são uma desculpa válida para a não conformidade. De acordo com a seção 302, os executivos seniores devem ser capazes de afirmar que todos os dados confidenciais foram armazenados e processados com segurança. Um relatório financeiro totalmente preciso ainda pode ser questionado se os pontos fracos forem expostos nos sistemas de TI da empresa. Por isso, as políticas de segurança, sistemas de backup e relatórios de auditoria de uma organização devem ser infalíveis.

Para aderir às seções 302, 404, 409 e 802 da SOX, as equipes de TI devem:

- Fornecer aos executivos seniores relatórios de auditoria detalhados sobre a estrutura de controle interno.
- Manter os sistemas de TI atualizados e monitorar constantemente a existência de brechas de segurança.
- Identificar e proteger todos os dispositivos, aplicações e processos de TI que lidam com dados financeiros confidenciais.
- Avaliar todos os sistemas e aplicações em busca de pontos fracos.
- Configurar mecanismos de alerta para detectar incidentes de segurança a tempo.
- Investigar e responder aos incidentes de forma eficiente para minimizar os danos e criar relatórios forenses detalhados.
- Ter um sistema em vigor para comunicar incidentes confirmados a todas as partes interessadas.
- Consolidar todos os logs financeiros, de comunicações e relacionados, e armazená-los com segurança.
- Configurar procedimentos de backup automatizados e avaliá-los periodicamente.
- Proteger-se contra erros dos funcionários, oferecendo programas de conscientização sobre phishing e outros ataques de engenharia social.
- Definir políticas de acesso claras e certificar-se de que os usuários tenham apenas os direitos necessários para executar seus trabalhos.

Como alcançar a conformidade com a SOX por meio do Log360

O Log360 ajuda sua organização a alcançar a conformidade com a SOX, de modo que você possa auditar e proteger seus logs financeiros confidenciais. Com o Log360, você pode auditar atividades relacionadas a dados financeiros confidenciais e proteger esses dados contra acessos e ataques não autorizados; investigar possíveis incidentes de segurança e manter logs de auditoria com segurança durante o tempo necessário.

Seção 302: Responsabilidade corporativa para relatórios financeiros

O Log360 vem com mais de 1,200 relatórios intuitivos e predefinidos que detalham as várias atividades da sua rede. Isso inclui atividades em seus sistemas Windows, Unix e IBM, aplicações, dispositivos da rede, e servidores de arquivos, bem como seus ambientes do Active Directory, Office 365 e Exchange Server. Você pode até mesmo criar relatórios personalizados para aplicações financeiras internas usando o interpretador de logs personalizado.

Você pode usar esses relatórios para manter executivos seniores informados sobre a segurança e a integridade de dados financeiros importantes. Os relatórios necessários podem ser exportados ou agendados conforme necessário, e várias opções de personalização estão disponíveis. Além disso, o controle de acesso baseado na função permite restringir a exibição desses relatórios a usuários autorizados.

Destaques

Auditoria abrangente da rede | Interpretador de logs personalizado | Exportação de relatórios em PDF e CSV | Agendamento de relatórios | Personalização de relatórios | Controle de acesso baseado na função

Seção 404: Avaliação de gerenciamento de controles internos

Para configurar controles internos eficazes sobre seus sistemas contábeis, você precisa considerar vários aspectos da segurança de rede. O Log360 ajuda você a cobrir as seguintes áreas:

- **Auditar acessos e mudanças em registros financeiros confidenciais.** Preserve a integridade dos dados e prove que os dados foram gerenciados adequadamente fornecendo trilhas de auditoria detalhadas. Você também pode gerar relatórios para comprovar que seus dados são regularmente copiados e podem ser restaurados em caso de danos.
- **Monitorar atividades de usuários privilegiados.** Certifique-se de que as contas privilegiadas não sejam comprometidas e que sejam usadas de forma responsável.
- **Detectar ataques em sua rede.** Receba notificações instantâneas para:
  - Padrões de atividade suspeitos correlacionados em vários dispositivos.
  - Os ataques são detectados por seus firewalls, IDS/IPS e outros dispositivos da rede.
  - Entidades mal-intencionadas interagem com sua rede.
  - Anomalias detectadas em seus ambientes do Active Directory, Office 365, Exchange Server e servidor de arquivos.
  - Outros eventos suspeitos, como mudanças de política, logs sendo apagados, etc.
- **Fornecer transparência sobre o status da rede.** Reporte vulnerabilidades, vírus, falhas do sistema e outros problemas descobertos na sua rede. A SOX requer transparência em todos os problemas que podem afetar a segurança de seus registros financeiros e esses relatórios ajudam você a fornecê-los.

Destaques

Relatório de conformidade com a SOX predefinido | Relatórios DDL/DML | Monitoramento de integridade de arquivos Windows e Linux | Monitoramento de usuários privilegiados | Correlação de eventos | Inteligência contra ameaças | Relatórios de vulnerabilidade

Seção 409: Divulgações do emissor em tempo real

A SOX exige divulgações públicas "em uma base rápida e atualizada" de quaisquer eventos que possam afetar o status financeiro de uma empresa. Esses eventos incluem violações de segurança de seus sistemas financeiros ou dados. Para confirmar que um incidente de segurança ocorreu ou está ocorrendo, você deve ser capaz de realizar uma investigação forense completa imediatamente. O mecanismo de pesquisa do Log360 facilita investigações rápidas e permite que você chegue à causa-raiz de um incidente com o mínimo de esforço.

Suas funcionalidades de emissão de tickets integradas e as integrações com o help desk também permitem otimizar o gerenciamento de incidentes. Ao atribuir automaticamente tickets de incidentes, rastrear seu status e manter uma base de conhecimento interna de incidentes passados, você pode supervisionar um processo de resolução de incidentes tranquilo.

Destaques

Mecanismo de pesquisa avançado | Console de emissão de tickets integrado | Integrações externas de help desk

Seção 802: Garantir a retenção de logs

Registros sobre todas as transações financeiras e comunicações devem ser mantidos por pelo menos cinco anos para que uma organização esteja em conformidade com as regras da SOX. Os logs são uma parte importante desses registros. Com o Log360, você pode escolher por quanto tempo deseja manter seus logs e pode importar os que estão arquivados a qualquer momento para uma investigação mais aprofundada. Os logs são transmitidos e armazenados de maneira segura e sem adulteração para garantir que não possam ser colocados em dúvida no caso de uma auditoria.

Destaques

Retenção de logs de duração flexível | Arquivamento sem violação | Comunicação segura na web | Importação de logs históricos

Conclusão

A TI desempenha uma função fundamental no apoio à jornada de uma organização em direção à conformidade com a SOX. Com seus recursos abrangentes de gerenciamento de logs e segurança, o Log360 ajuda os administradores de TI a criarem um sistema de controle interno sólido para proteger os dados financeiros confidenciais de uma empresa.

Sobre o Log360

O Log360, uma solução integrada que combina ADAudit Plus, EventLog Analyzer, DataSecurity Plus, Exchange Reporter Plus e O365 Manager Plus em um console único, é a solução completa para todos os desafios de gerenciamento de logs e segurança de rede. Esta solução oferece capacidades de coleta, análise, monitoramento, correlação e arquivamento de logs em tempo real que ajudam a proteger os dados confidenciais, impedir ameaças à segurança interna e combater ataques externos. O Log360 é fornecido com mais de 1.200 relatórios e critérios de alerta predefinidos para ajudar as empresas a atender às demandas mais urgentes de segurança, auditoria e conformidade. Para obter mais informações sobre o Log360, visite manageengine.com/br/log-management

$ Get Quote Download