Soluções de Segurança IBM

Security Framework

As organizações frequentemente adotam uma abordagem orientada à tecnologia para a segurança. Porém, proteger só a tecnologia não oferece proteção para os processos e os ativos de negócio em relação aos riscos do negócio.

Frequentemente, as organizações assumem uma abordagem de baixo para cima para a segurança, uma vez que os fornecedores de soluções para segurança frequentemente promovem essa abordagem a seus clientes. Para aproximar lacunas de segurança identificadas, as organizações aumentam e reforçam suas defesas incluindo investimentos em sua segurança existente. Essa metodologia centrada na tecnologia frequentemente cria uma infraestrutura de segurança excessivamente complexa e deslocada. Torna-se difícil gerenciar e voltar a atenção para lacunas de vulnerabilidade não observadas sem necessidade de escalonar os custos de TI, bem como, eventualmente, estimular ineficiências operacionais desnecessárias que inibem o crescimento do negócio, em vez de aumentá-lo.

O gerenciamento dos riscos de negócio exige uma abordagem holística que considera as metas de negócios de acordo com os requisitos e restrições técnicas para a segurança. Em vez de tentar a proteção contra cada ameaça concebível, as organizações devem entender e priorizar as atividades de gerenciamento do risco de segurança mais sensatas para sua organização. Ao entender o nível de tolerância de risco em uma organização, a equipe de TI pode focar mais facilmente a redução dos riscos que a organização não pode permitir-se negligenciar. Enfatizar excessivamente determinados riscos pode levar à perda de recursos e de esforços, ao passo que subestimar outros riscos pode ter consequências desastrosas.

As organizações podem considerar difícil alcançar uma estratégia e uma abordagem de segurança de ponta a ponta que apóie as metas de negócio, tais como orientação à inovação e redução dos custos organizacionais, bem como requisitos operacionais que direcionem medidas de conformidade e protejam contra ameaças internas e externas.

A segurança não deve ser tratada de forma isolada das outras atividades de negócio dentro da organização. Pelo contrário, ela deve ser encarada a partir da perspectiva de negócio – observando a segurança como um meio para proteger e aprimorar os processos de negócio. Isso envolve um nível de planejamento e avaliação para identificar riscos em todas as principais áreas de negócio, inclusive pessoas, processos, dados e tecnologia, na continuidade total do negócio por completo.

Por isso, a IBM criou um sistema abrangente de segurança em TI, mostrado na Figura 1, que pode ajudar a garantir que cada domínio de TI necessário seja adequadamente direcionado, usando-se uma abordagem holística para a segurança orientada ao negócio.

Figura 1 - O IBM Security Framework

Controle de Segurança, Gerenciamento de Risco e Conformidade

Cada organização deve definir e comunicar os princípios e políticas que orientam a estratégia de negócio e a sua operação. Ademais, cada organização deve avaliar seus riscos operacionais e de negócio, bem como desenvolver um plano de segurança empresarial para servir como benchmark para a execução e validação das atividades de gerenciamento de segurança que são adequadas para sua organização.

Estes princípios e políticas, o plano de segurança empresarial e os processos que envolvem a melhoria da qualidade representam o modelo de Controle de Segurança, Gerenciamento de Risco e Conformidade da empresa. De modo específico, os requisitos e critérios de conformidade para os domínios de segurança restantes são:

Pessoas e identidade

Este domínio cobre aspectos sobre como garantir que as pessoas certas tenham acesso aos ativos certos no momento certo.

Dados e informação

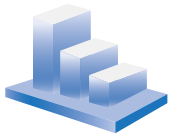
Este domínio cobre aspectos sobre como proteger na organização os dados críticos em trânsito ou armazenados.

Aplicativo e processo

Este domínio cobre aspectos sobre como garantir a segurança de serviços de negócio e aplicativos.

Rede, servidor e end point

Este domínio cobre aspectos sobre como estar à frente de ameaças emergentes em relação aos componentes do sistema de TI.

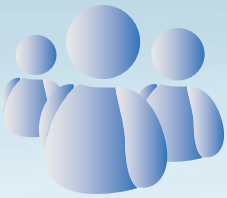


Infraestrutura física

Este domínio cobre aspectos sobre como melhorar a capacidade de controles digitais para assegurar eventos – sobre pessoas ou ativos – em seu espaço físico.

Security Framework

IBM®



Pessoas e Identidade

As organizações devem proteger seus bens e serviços que atendem o negócio e que apóiam a sua operação. Um aspecto de proteção é fornecido pelo controle de acesso. A capacidade de fornecer serviços eficazes de controle de acesso está baseada na capacidade de gerenciar Pessoas e Identidade, conforme definido pelo modelo de Controle de Segurança, Gerenciamento de Risco e Conformidade da empresa.

O Controle de Segurança, Risco e Conformidade fornece uma orientação sobre como as identidades são gerenciadas e como o controle de acesso deve ser realizado. As organizações registram as pessoas e as mapeiam em identidades. As relações entre pessoas e a organização estão expressas em termos de papel, direitos, políticas de negócio e regras. A capacidade de registrar pessoas e descrever as respectivas relações com a empresa é um fator que possibilita a segurança-chave para os domínios de segurança remanescentes: Dados e Informação, Aplicativos e Processo, Rede, Servidor e Endpoint (infraestrutura de TI), bem como Infraestrutura Física.

De modo operacional, às pessoas desempenhando funções autorizadas em uma organização ou como parte de uma relação estendida é concedido o acesso à infraestrutura, dados, informação e serviços. Ao mesmo tempo, às pessoas atuando em papéis não autorizados é negado o acesso a estes itens.

Em um sistema de identidade, as pessoas podem receber uma credencial, que pode assumir diversas formas, inclusive um cartão de identificação física, um token lógico ou um identificador do usuário. A confiança ou força da credencial é um aspecto importante da política de negócio ou gerenciamento do risco. É extremamente importante a capacidade de gerenciar efetivamente o ciclo de vida da identidade, ou seja, a criação, exclusão e alterações de papel para populações dinâmicas da força de trabalho, cliente ou comunidades de usuários. O ciclo de vida de identidades e credenciais, pode ser influenciado por ciclos de negócio, ciclos empregatícios, relações com o cliente, contratos, eventos de calendário ou de negócio, entre outros.

Os sistemas de identidade devem ser integrados a conjuntos adequados de controles de acesso. Os sistemas de identidade são necessários para gerenciar os papéis, direitos e privilégios dos usuários em toda a infraestrutura de TI que pode conter múltiplas arquiteturas de tecnologia, ou serão exigidos múltiplos sistemas de identidade e controle de acesso para garantir que os usuários tenham acesso aos bens e serviços corretos.

A Figura 2 mostra um resumo e alguns aspectos adicionais que devem ser direcionados dentro do domínio de Pessoas e Identidade.

Gerenciar Identidades e Acesso

"Como meu negócio pode se beneficiar do gerenciamento da identidade digital?"

Problemas

- Entendimento de lacuna de risco de identidade
- Custo da administração de usuários e identidades internas
- Atividade não monitorada de usuário privilegiado
- IDs inativas ou compartilhadas sendo usadas inadequadamente para recursos de acesso.
- Falha em auditoria

Valores

- Reduz o custo, aumenta a eficiência e permite a capacidade de auditoria do fluxo de gerenciamento da entrada, uso e saída de usuários da organização
- Diminui o risco de fraude interna, vazamento de dados e interrupção operacional
- Apóia a globalização das operações
- Permite mudar das vendas físicas tradicionais para a entrega de serviços on-line aos clientes e parceiros em todo o globo
- Melhora a experiência de usuários finais com aplicativos de negócio baseados em internet por meio da permissão das referidas atividades, tais como single sign-on

Figura 2 Domínio de Pessoas e Identidade

Dados e Informação

As organizações devem proteger os dados brutos e a informação contextualizada que estão em sua dimensão de controle. O Controle de Segurança, Risco e Conformidade fornece orientação sobre o valor dos dados e da informação, bem como gerencia seus riscos.

Um plano eficaz para a proteção de dados e informação inclui a manutenção de um catálogo ou inventário desses bens, em conjunto com seus atributos, políticas, mecanismos e serviços de aplicação que governam o acesso, a transformação, o movimento e a disposição dos dados e informação.

Este plano de proteção de dados e informação pode ser aplicado aos processos de negócio, transações de negócio ou processos de apoio à infraestrutura e ao negócio. A proteção de dados e informação cobre um ciclo de vida completo, da criação à destruição e em relação a vários estados e localizações, bem como quando são armazenados ou transportados física ou eletronicamente.

O termo “dados” pode ser aplicado a uma grande variedade de bens codificados eletronicamente. Isso inclui o software e firmware, os quais devem ser protegidos contra riscos técnicos (para garantir que um código malicioso não seja introduzido) e riscos de negócio (para garantir que os termos de licença não sejam violados).

A proteção de dados e informação é interdependente com a definição e operação de todos os demais domínios de segurança operacional. A medição e o relatório sobre a conformidade da organização em relação à proteção de dados e informação é uma métrica tangível da efetividade do plano de segurança da empresa. Um relatório de conformidade de dados e informação reflete a força ou fragilidade dos controles, serviços e mecanismos, em todos os domínios.

A Figura 3 mostra um resumo e alguns aspectos adicionais, que podem ser direcionados dentro do domínio de Dados e Informação.

Proteger Dados e Informação

“Como posso reduzir o custo e o transtorno associado com o rastreamento e o controle sobre quem acessou quais dados e quando? Como eu asseguro que meus dados estão disponíveis?

Problemas

- Dados armazenados em mídia removível que podem ser perdidos/roubados
- Dados armazenados no clear são facilmente acessíveis
- Políticas inconsistentes de dados
- Dados não estruturados
- Exposição legal, regulamentária e ética para a organização
- Custos de violações de dados, notificação, valor de marca
- Falha na auditoria

Valores

- Reduz o custo, aumenta a capacidade de cumprir as obrigações de auditoria e conformidade
- Fornece uma forma eficaz de custo para cumprir as exigências legais de descoberta, posse e retenção
- Garante que os dados estão disponíveis para as pessoas certas, no momento certo
- Garante que os dados não são deliberados ou inadvertidamente acessados, vazados ou danificados
- Diminui o número e a complexidade dos controles integrados dentro da empresa

Figura 3 Domínio de Dados e Informação

Aplicativo e Processo

As organizações devem proteger, de modo proativo, seus aplicativos críticos de negócio contra ameaças internas e externas, durante todo o ciclo de vida, do desenho à implementação e produção. O controle durante todo o ciclo de vida do aplicativo implica em controle e conformidade eficazes nos domínios de segurança restantes.

Por exemplo, se um aplicativo é focado internamente, tal como um sistema de gerenciamento de relações com o cliente (CRM) entregue por meio de uma arquitetura orientada ao serviço (SOA) ou aplicativo de parâmetro externo, tais como um novo portal do cliente, as políticas e processos de segurança claramente definidos são críticos para garantir que o aplicativo está capacitando o negócio, em vez de introduzir um risco adicional.

O Gerenciamento de Serviço para todo o negócio e processos de suporte do negócio, inclusive Gerenciamento de Serviço para processos dentro do domínio de segurança, é uma parte crítica para assegurar que o negócio está operando dentro de um gerenciamento de risco adequado e em conformidade com as diretrizes.

O Gerenciamento de Serviço de Segurança tipicamente incluiria uma combinação de capacidades, tais como autenticação centralizada, gerenciamento de política de auditoria e acesso, bem como busca de vulnerabilidade do aplicativo Web e prevenção de invasão.

A Figura 4 mostra um resumo e aspectos adicionais que podem ser direcionados dentro do domínio de Aplicativo e Processo.

Proteger Aplicativos Web

"Como meu negócio pode beneficiar-se do gerenciamento de segurança de aplicativos?"

Problemas

- Os aplicativos Web são o alvo n° um dos hackers que buscam explorar vulnerabilidades
- Os aplicativos são implantados com vulnerabilidades
- Configurações de baixa segurança expõem os clientes à perda no negócio
- Os requisitos regulatórios de PCI exigem a segurança do aplicativo
- 80% dos custos de desenvolvimento são gastos na identificação e correção de defeitos
- Dados reais e/ou privados expostos a qualquer pessoa com acesso ao desenvolvimento e ambientes de teste, inclusive contratados e terceirizados

Valores

- Reduz o risco de interrupção, desfiguração ou roubo de dados associados com aplicativos Web
- Assessora e monitora conformidade da política de segurança em toda a empresa
- Melhora a conformidade com as normas do setor e exigências regulatórias (por exemplo, PCI, GLBA, HIPAA, FISMA, entre outros)
- Melhora a capacidade de integrar aplicativos críticos do negócio
- Teste e controle automatizados durante todo o ciclo de vida do desenvolvimento, reduzindo os custos de segurança em longo prazo.

Figura 4 Domínio de Aplicativo e Processo

Rede, Servidores e Endpoint

As organizações devem monitorar prioritária e proativamente a operação do negócio e a infraestrutura de TI quanto a ameaças e vulnerabilidades, para evitar ou reduzir quaisquer violações.

O Controle de Segurança, Risco e Conformidade pode fornecer orientação sobre implicações de negócio dos riscos baseados em tecnologia. Na prática, a definição, implantação e gerenciamento de ameaças baseadas em tecnologia, bem como os aspectos técnicos da resposta ao incidente, podem ser delegados à equipe e gerenciamento operacional, ou terceirizado a um provedor de serviço.

O monitoramento de segurança e o gerenciamento da rede, do servidor e desktops da organização, são críticos para estar à frente de ameaças emergentes que podem afetar adversamente os componentes do sistema, bem como as pessoas e os processos de negócio que eles suportam. A necessidade de identificar e proteger a infraestrutura contra as ameaças emergentes aumentou dramaticamente com a elevação nas infiltrações organizadas de rede e financeiramente motivadas. Embora nenhuma tecnologia seja perfeita, o foco e a intensidade da segurança, monitoramento e gerenciamento podem ser afetados pelo tipo de rede, servidor e desktops implantados na infraestrutura de TI e como esses componentes são construídos, integrados, testados e mantidos.

As empresas incentivam a tecnologia de virtualização para apoiar suas metas de entrega de serviços em menos tempo e com maior agilidade. Por meio da construção de uma estrutura de controles de segurança dentro de seu ambiente, as organizações podem alcançar as metas de virtualização – tais como uso aperfeiçoado do recurso físico, eficiência aprimorada do hardware e redução dos custos de energia – enquanto se ganha tranquilidade ao saber que os sistemas virtuais estão seguros com o mesmo rigor que os sistemas físicos.

A Figura 5 mostra um resumo, bem como aspectos adicionais que podem ser direcionados dentro do domínio de Rede, Servidor e Endpoint.

Gerenciar a Segurança da Infraestrutura

"Como meu negócio se beneficia da proteção de segurança da infraestrutura?"

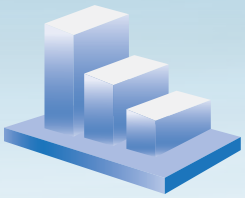
Problemas

- Comercialização em massa e automatização de ameaças
- Ataques parasíticos, clandestinos e mais prejudiciais
- Baixo entendimento dos riscos em novas tecnologias e aplicativos, inclusive virtualização e cloud
- Baixos controles de aplicativos
- Falta de habilidade para monitorar e gerenciar entradas de segurança
- Custo composto de gerenciamento de um crescente banco de dados de tecnologias de segurança
- Violações não detectadas devido ao uso impróprio do privilégio de acesso e tempo ocioso proveniente de incidentes
- Inabilidade de estabelecer evidência forense ou de demonstrar conformidade

Valores

- Reduz o custo da gerenciamento de operações de segurança em andamento
- Melhora a disponibilidade operacional e assegura o desempenho contra SLA, apoiada pelo único SLA garantido do setor para serviços de proteção gerenciados.
- Aumenta a produtividade por meio da redução do risco por infestação de vírus, worm e código malicioso.
- Diminui o volume de entrada de spam
- Mudança rápida de violações específicas para a resolução rápida de local
- Pronta apresentação de status em relação às principais regulamentações

Figura 5 Domínio de Rede, Servidor e Desktop



Infraestrutura Física

Para uma organização implementar efetivamente um plano de segurança empresarial, o negócio e os riscos técnicos que estão associados com a infraestrutura física devem ser compreendidos e direcionados. O Controle de Segurança, Risco e Conformidade fornece orientação sobre os tipos de risco e tipos de planos e respostas para a segurança física. Proteger a infraestrutura da organização pode significar tomar precauções contra uma falha ou perda da infraestrutura física que poderia impactar a continuidade do negócio.

Proteger uma infraestrutura da organização pode envolver a proteção contra ameaças e vulnerabilidades indiretas, tais como o impacto da perda de serviços públicos, uma violação no controle de acesso físico ou a perda de ativos físicos críticos. A segurança física efetiva exige um sistema de gerenciamento centralizado que permite a correlação de entradas a partir de diversas fontes, inclusive, propriedade, funcionários, clientes, público em geral e clima local e regional.

Por exemplo, assegurar o perímetro do data center com câmeras e dispositivos de monitoramento centralizado é essencial para garantir o acesso gerenciado para os bens de TI da organização. Portanto, as organizações preocupadas com roubo ou fraude, tais como bancos, lojas varejistas ou órgãos públicos devem definir e implementar uma estratégia de vigilância integrada da segurança física que inclui o monitoramento e o controle analítico e centralizado. Essa abordagem permite às organizações extrair dados inteligentes de múltiplas fontes e responder a ameaças mais rapidamente que os ambientes manualmente monitorados, resultando na redução de custo e risco de perda.

A Figura 6 mostra um resumo e aspectos adicionais que podem ser direcionados dentro do domínio de Infraestrutura física.

Segurança física	Problemas	Valores
"Como meu negócio se beneficia da proteção de segurança da infraestrutura física?	• Falha ou perda de infraestrutura física que poderia impactar a continuidade do negócio. • Ameaças e vulnerabilidades indiretas, tais como o impacto da perda de um serviço público, uma violação no controle de acesso físico ou perda de bens físicos críticos. • Exposições provenientes de fontes diversas, inclusive: propriedade, funcionários, clientes, público em geral, clima local ou regional, entre outros.	• Reduzir o risco de interrupção ou roubo de dados associados à falha ou à perda de bens físicos críticos. • Estratégia integrada de vigilância da segurança física que permite extrair dados inteligentes de múltiplas fontes, responder a ameaças mais rapidamente que em ambientes manualmente monitorados e redução de custo e risco de perda.

Figura 6 Domínio de Infraestrutura Física

www.ibm.com/br