**Recursos, Ameaças e Vulnerabilidades**

As equipes de segurança ajudam as empresas concentrando-se no risco. Risco define-se como qualquer meio que pode afetar a confidencialidade, a integridade ou a disponibilidade de um recurso. Para proteger esses pilares dentro de uma corporação se faz necessário criar um planejamento de risco de segurança.

É importante que cada empresa tenha um plano de riscos bem definido de acordo com todos os riscos a que ela está exposta. Os planos de segurança são baseados na análise de três elementos: ativos, ameaças e vulnerabilidades.

**Compreender os riscos, as ameaças e as vulnerabilidades**

**Risco -**  qualquer coisa que possa afetar a confidencialidade, a integridade ou a disponibilidade dentro de uma organização.

Ameaça - Qualquer circunstância ou evento que possa afetar negativamente os recursos.

Vulnerabilidade - Uma brecha que pode ser explorada por uma ameaça.

**Risco de Segurança**

Os planos de segurança têm tudo a ver com a definição de risco de uma organização. Entretanto, essa definição pode variar muito com a organização. Uma maneira de interpretar o risco é considerar os possíveis efeitos que os eventos negativos podem ter em um negócio. Outra maneira de interpretá-lo é com o cálculo: **probabilidade x impacto = risco.** Calcula-se o risco, levando em consideração esses parâmetros:

* Prevenir eventos dispendiosos.
* Identificar melhorias que podem ser feitas em sistemas e processos.
* Determinar quais riscos podem ser tolerados.
* Priorizar os recursos críticos que requerem atenção.

**Fatores de Risco**

* Ameaças
* Vulnerabilidades

O risco de um recurso ser prejudicado ou danificado depende muito do fato de uma ameaça tirar proveito das vulnerabilidades.

**Categorias de Ameaças**

As ameaças são circunstâncias ou eventos que podem afetar negativamente os recursos. Há muitos tipos diferentes de ameaças, que são categorizadas em dois tipos: intencionais e não intencionais.

Uma ameaça intencional pode ser um hacker mal-intencionado que obtém acesso a informações confidenciais ao usar um aplicativo configurado. Uma ameaça não intencional pode ser um funcionário que mantém a porta aberta para uma pessoa desconhecida e concede a ela acesso a uma área restrita.

**Categorias de Vulnerabilidade**

As vulnerabilidades são pontos fracos que podem ser exploradas por ameaças. Há uma grande variedade de vulnerabilidades, mas elas podem ser agrupadas em duas categorias: técnicas e humanas.

Uma vulnerabilidade técnica pode ser um software mal configurado que pode dar a uma pessoa não autorizada acesso a dados importantes. Uma vulnerabilidade humana pode ser um funcionário esquecido que perde seu cartão de acesso ao estacionamento.

**Classificação de recursos**

O gerenciamento de ativos é o processo de rastrear ativos e riscos que os afetam. Todos os planos de segurança giram em torno do gerenciamento de recursos.Todos os planos de segurança giram em torno do gerenciamento de recursos.Quando se é mencionado ativos, podemos classificar como qualquer recurso, seja ele físico ou não, que está alocado em uma organização.

O gerenciamento de ativos começa um inventário, um catálogo onde são mostrados todos os componentes que necessitam de proteção. Caso esses componentes não estejam registrados, o controle sobre qualquer um desses componentes é quase que inexistente.

É importante que esses inventários possuam níveis de classificação de importância dentro de uma organização. Essa prática conhecida como classificação de recursos ajuda os profissionais a reconhecer que cada ativo tem sua importância e deve ser tratado de acordo com ela.

**Requisitos Comuns de Classificação**

Uma outra parte importante dentro de uma organização é o gerenciamento de processos. Esse método é definido como o acompanhamento dos recursos e dos riscos que afetam uma organização. Manter os recursos seguros requer um sistema viável que ajude a empresa a operar sem problemas. As organizações protegem uma variedade de recursos diferentes.

* Recursos digitais, como dados de clientes ou registros financeiros.
* Informações sobre sistemas que processam dados, como redes de computadores ou software.
* Recursos físicos, que podem incluir instalações, equipamentos ou suprimentos.
* Recursos intangíveis, como a reputação da marca ou a propriedade intelectual.

Independente do tipo, recursos devem ser classificados e contabilizados, a classificação de recursos é a prática de rotular os recursos com base na sensibilidade e na importância para uma organização. A determinação de cada um desses dois fatores varia, mas a sensibilidade e a importância de um recurso normalmente requerem os conhecimentos:

* O que a pessoa tem.
* Quando.
* Quem é o proprietário.
* Qual a importância.

Estes fatores ajudam a determinar a sensibilidade e o valor de um recurso.

**Classificação comuns de recursos**

A classificação dos recursos ajuda as organizações a implementar uma Estratégia de Gerenciamento de Riscos eficaz. Ela também ajuda a priorizar os Recursos de segurança, reduzir os custos de TI e manter a conformidade com os regulamentos legais.

O esquema de classificação mais comum é: restrito, confidencial, interno e público.

* Restrito - é o nível mais alto. Essa categoria é reservada para recursos incrivelmente sensíveis, como informações que precisam ser conhecidas.
* Confidencial - refere-se a recursos cuja divulgação pode levar a um impacto negativo significativo em uma organização.
* Somente interno descreve recursos que estão disponíveis para funcionários e parceiros de negócios.
* Público é o nível mais baixo de classificação. Esses recursos não têm consequências negativas para a organização se foram divulgados.

**Desafios da classificação das informações**

A propriedade é apenas uma característica que torna a classificação das informações um desafio. Outra preocupação é o fato de que as informações podem ter vários valores de classificação ao mesmo tempo.

**Recursos Digitais e Físicos**

As equipes de segurança classificam os ativos com base no valor. Nesses casos, é importante refletir sobre o que exatamente é valioso em um recurso. Geralmente a resposta seria informação. A maioria das informações está em formato digital. Isso é chamado de dados.

Dados são informações que são traduzidas, processadas ou armazenadas por um computador. Bilhões de dispositivos em todo o mundo estão conectados à Internet e trocam dados entre si o tempo todo. No âmbito digital, os ativos têm desafios diferentes. O que é necessário entender é que a proteção dos dados depende de onde eles estão e como estão sendo utilizados. As equipes de segurança protegem dados em três estados: em uso, em trânsito e em repouso.

* Dados em uso são dados acessados por um ou mais usuários;
* Dados em trânsito são dados que viajam de um ponto a outro.
* Dados em repouso são dados que não estão sendo acessados por nenhum usuário.

Segurança da Informação, ou InfoSec, é a prática de manter os dados em todos estados longe de usuários não autorizados. A fraca segurança da informação é um problema sério. Isso pode levar a coisas como roubo de identidade, perda financeira e danos à reputação. Esses eventos têm o potencial de prejudicar as organizações, seus parceiros e seus clientes.

**O Surgimento da Segurança na Nuvem**

**SOAR na nuvem**

A disponibilidade de tecnologias em Nuvem mudou drasticamente a forma como as empresas operam on-line. Essas novas ferramentas permitem que as empresas façam escalabilidade e se adaptem rapidamente, ao mesmo tempo em que reduzem seus custos. Apesar desses benefícios, a mudança para serviços baseados em nuvem também introduziu uma série de novos desafios de segurança cibernética que colocam os recursos em risco.

**Serviços baseados na nuvem**

O termo serviços baseados em Nuvem refere-se a uma variedade de soluções de negócios sob demanda ou baseados em Web. Dependendo das necessidades e do orçamentos de uma empresa, os serviços podem variar de hospedagem de site a ambientes de desenvolvimento de aplicativos e toda a infraestrutura de back-end.

Há três categorias de serviços baseados em Nuvem:

* Software como serviço - refere-se aos aplicativos front-end que os usuários acessam por meio de um navegador da Web. Os provedores de serviços hospedam, gerenciam e mantêm todos os sistemas de back-end desses aplicativos. Serviços de e-mail como gmail, slack e o zoom.
* Infraestrutura como serviço - Os clientes recebem acesso remoto a uma série de sistemas de back-end hospedados pelo provedor de serviços de nuvem. Isso inclui servidores de processamento de dados, armazenamento, recursos de rede de computadores, etc. Os recursos geralmente são licenciados conforme necessário, o que os torna uma alternativa econômica à compra e à manutenção no local. Os serviços baseados em nuvem permitem que as empresas se conectem com seus clientes, funcionários e parceiros de negócios pela internet. Algumas das maiores organizações do mundo oferecem serviços baseados em nuvem: Google Cloud Platform, Microsoft Azure.
* Plataforma como serviço - refere-se a ferramentas de desenvolvimento de aplicativos back-end que os clientes podem acessar online. Os desenvolvedores usam esses recursos para escrever código e criar, gerenciar e implantar seus próprios aplicativos. Enquanto isso, os provedores de serviços em nuvem hospedam e mantêm o hardware e o software de back-end que os aplicativos usam para operar. Alguns exemplos de serviços de PaaS incluem a plataforma Google App Engine, Heroku e VMware Cloud Foundry.

**Segurança em Nuvem**

Um dos desafios de se manter os principais serviços de uma organização hospedada na nuvem, é também conseguir assegurar a privacidade e a segurança dos dados em um ambiente fora da organização. A proteção desses sistemas dependia inteiramente da equipe interna desse ambiente. Essas responsabilidades não são definidas com tanta clareza quando parte ou todo o ambiente operacional está na nuvem.

Um cliente de PaaS paga para acessar os recursos necessários para criar seus aplicativos. Portanto, é razoável esperar que eles sejam responsáveis pela segurança dos aplicativos que criam. Por outro lado, a responsabilidade de manter a segurança dos servidores que estão acessando deve pertencer ao provedor de serviços de nuvem.

Na segurança de nuvem, esse conceito é conhecido como modelo de responsabilidade compartilhada. Os clientes geralmente são responsáveis por pela segurança de tudo o que está diretamente sob seu controle:

* Gerenciamento de identidade e acesso.
* Configuração de recursos.
* Manuseio de dados.

**Desafios da Segurança**

Dados armazenados na internet demandam certos desafios.

* Configuração incorreta é uma das maiores preocupações. Os clientes de serviços baseados na nuvem são responsáveis pela configuração de seu próprio ambiente de segurança. Muitas vezes, eles usam configurações prontas para uso que não atendem a seus objetivos específicos de segurança.
* É mais provável que ocorram violações nativas de nuvem devido a serviços mal configurados.
* O monitoramento do acesso pode ser difícil, dependendo do cliente e do nível de serviço.
* O cumprimento dos padrões regulatórios também é uma preocupação, principalmente nos setores que são obrigados por lei a seguir requisitos específicos, como HIPAA, PCI DSS e GDPR.

A Burning Glass, empresa líder em análise de dados do mercado de trabalho, classifica a Segurança na nuvem entre as habilidades mais demandadas em segurança cibernética.

**Elementos de um plano de segurança**

A segurança é um conjunto compartilhado de valores que abrange todos os níveis de uma organização. Esses valores atingem a todos, de funcionários a fornecedores e clientes. Proteger ativos digitais e físicos exige que todos participem, o que pode ser um desafio.

Os planos de segurança têm a função de proteger os ativos digitais e físicos. Os planos têm várias formas e tamanhos, mas todos compartilham um objetivo comum: estar preparado para os riscos quando eles acontecem. Colocar o foco nas pessoas é o que leva aos planos de segurança mais eficazes. Considerar as diversas origens e perspectivas de todos os envolvidos garante que ninguém fique de fora quando algo der errado. A maioria dos planos de segurança aborda os riscos dividindo-os de acordo com categorias e fatores.

Algumas categorias de risco comuns podem incluir danos, divulgação ou perda de informações. Qualquer um deles pode ser devido a fatores como danos físicos ou mau funcionamento de um dispositivo. Também existem fatores como ataques e erros humanos. Um plano de segurança pode exigir que todos os novos contratados de uma empresa assinem um contrato em que é estritamente proibido usar e-mail pessoal para enviar informações confidenciais. Essas coisas variam muito, dependendo da empresa. Mas a forma como esses planos são comunicados é semelhante em todos os setores.

Os planos de segurança consistem em três elementos básicos: políticas, padrões e procedimentos. Esses três elementos são como as empresas compartilham seus planos de segurança.

Uma política de segurança é um conjunto de regras que reduz o risco e protege as informações. As políticas são a base de todo plano de segurança. Eles orientam todos que entram e saem de uma organização, abordando questões como: o que estamos protegendo e por quê? As políticas se concentram no lado estratégico, identificando escopo, os objetivos e as limitações de um plano de segurança.

Os padrões têm uma função tática, pois dizem a respeito do quão bem estamos protegendo os ativos. Em segurança, os padrões são referências que informam como definir políticas. Uma boa maneira de pensar em padrões é criar um ponto de referência. Por exemplo, muitas empresas usam o padrão de gerenciamento de senhas identificado na Publicação Especial 800-63B do NIST para melhorar suas políticas de segurança, especificando que as senhas dos funcionários devem ter pelo menos oito caracteres.

Procedimentos são instruções passo a passo para realizar tarefas de segurança específicas. As organizações geralmente mantêm vários documentos de procedimentos que são usados em toda a empresa, como a forma como os funcionários podem escolher senhas seguras ou como podem redefinir sua senha com segurança se ela estiver bloqueada. Compartilhar procedimentos claros e acionáveis com todos cria responsabilidade, consistência e eficiência em toda a organização.

**A NIST Cybersecurity Framework**

Ter um plano é apenas uma parte da proteção de ativos. Uma vez que o plano esteja em ação, a outra parte é garantir que todos estejam acompanhando. A conformidade é o processo de adesão aos padrões internos e aos regulamentos externos. Pequenas e grandes organizações em todo o mundo colocam a conformidade de segurança no topo de sua lista de prioridades.

Em alto nível, manter a confiança, a reputação, a segurança e a integridade de seus dados são apenas alguns motivos para se preocupar com a conformidade. Multas penalidades e ações judiciais são outros motivos. Isso é particularmente verdadeiro para empresas em setores altamente regulamentados, como saúde, energia e finanças. Estar fora de conformidade com uma regulamentação pode causar problemas financeiros e de reputação duradouros que podem impactar seriamente uma empresa.

Regulamentos são regras estabelecidas por um governo ou uma outra autoridade para controlar a forma como algo é feito. Assim como as políticas, existem regulamentações para proteger as pessoas e suas informações, mas em uma escala maior. A conformidade pode ser um processo complexo devido às muitas regulamentações que existem em todo o mundo. É importante levar em consideração um framework de conformidade de segurança, o NIST Cybersecurity Framework .

Uma das principais funções do NIST é fornecer abertamente às empresas um conjunto de estruturas e padrões de segurança que reflitam as principais regulamentações relacionadas à segurança. O NIST Cybersecurity Framework é um framework voluntário que consiste em padrões, diretrizes e melhores práticas para gerenciar riscos de cibersegurança. Comumente conhecido como CSF, esse framework foi desenvolvido para ajudar as empresas a proteger um de seus ativos mais importantes, as informações. O CSF consistem em três componentes principais: o núcleo, suas camadas e seus perfis.

O núcleo é basicamente uma versão simplificada das funções ou deveres de um plano de segurança. O núcleo do CSF identifica cinco funções amplas: identificar, proteger, detectar, responder e recuperar. Pense nessas categorias do núcleo como uma lista de verificação de segurança.

Depois do núcleo, os próximos componentes do NIST a serem falados são os níveis. Eles fornecem às equipes de segurança uma maneira de medir o desempenho em cada uma das cinco funções do núcleo. Os níveis variam do nível 1 ao nível 4. O nível 1, ou passivo, indica que uma função está atingindo os padrões mínimos. O nível 4, ou adaptativo, é uma indicação de que uma função está sendo executada em um padrão exemplar. Os níveis da CSF não são uma proposta de sim ou não, ao invés disso, há uma variedade de valores. Isso se dá porque os níveis são projetados como uma forma de mostrar às organizações o que está e o que não está funcionando com seus planos de segurança.

Por fim, os perfis são os componentes finais de CSF. Eles fornecem a visão sobre o estado atual de um plano de segurança. Uma forma de pensar em perfis é com fotos capturando um momento no tempo. Comparar fotos do mesmo sujeito tiradas em momentos diferentes pode fornecer informações úteis.

Uma boa prática de segurança é mais do que evitar multas e ataques. Isso demonstra que o profissional de segurança se importa com as pessoas e suas informações.

**Diretrizes de segurança em ação**

As organizações geralmente enfrentam uma quantidade enorme de riscos. Desenvolver um plano de segurança desde o início que aborde todos os riscos pode ser um desafio. Isso torna as estruturas de segurança uma opção útil. Uma das principais vantagens do CSF é que ele é flexível e pode ser aplicado a qualquer setor.

**Origens da Estrutura**

Lançada originalmente em 2014, a NIST desenvolveu a estrutura de segurança cibernética para proteger a infraestrutura crítica dos Estados Unidos. O NIST foi selecionado para desenvolver o CSF por ser uma fonte imparcial de dados e práticas científicas. O NIST acabou adaptando o CSF para atender às necessidades das empresas dos setores público e privado. Seu objetivo era tornar a estrutura mais flexível, facilitando a adoção por pequenas empresas ou qualquer outra pessoa que não tenha recursos para desenvolver seus próprios planos de segurança.

**Componentes do CSF**

A estrutura do CSF é composta por três componentes principais: o núcleo, as camadas e os perfis.

**Núcleo**

O núcleo do CSF é um conjunto de resultados desejados de segurança cibernética que ajudam as organizações a personalizar seu plano de segurança. Ele consiste em seis funções, ou partes: identificar, proteger, detectar, responder, recuperar e governar. Essas funções são comumente usadas como referência informativa para ajudar as organizações a identificar seus ativos mais importantes e proteger esses ativos com as devidas salvaguardas. O núcleo CSF também é usado para entender as maneiras de detectar ataques e desenvolver planos de resposta e recuperação caso ocorra um ataque.

**Níveis**

Os níveis do CSF são uma forma de medir a sofisticação do programa de segurança cibernética de uma organização. Os níveis do CSF são medidos em uma escala de 1 a 4. O nível 1 é a pontuação mais baixa, indicando que um conjunto limitado de controles de segurança foi implementado. De modo geral, os níveis do CSF são usados para avaliar a postura de segurança de uma organização e identificar áreas para aprimoramento.

**Perfis**

Os perfis do CSF são modelos pré-fabricados do NIST CSF desenvolvidos por uma equipe de especialistas do setor. Os perfis CSF são adaptados para lidar com os riscos específicos de uma organização ou setor. Eles são usados para ajudar as organizações a desenvolver uma linha de base para seus planos de segurança cibernética ou como forma de comparar a sua postura atual de segurança cibernética com um padrão específico do setor.

Obs: Os núcleos, perfis e camadas foram projetados para ajudar a quaisquer empresas a aprimorar suas operações de segurança. Embora existam apenas três componentes, toda a estrutura consiste em um sistema complexo de subcategorias e processos.

**Implementação do CSF**

Como você deve se lembrar, a conformidade é um conceito importante em segurança. Compliance é o processo de aderir a padrões e normas externas, em outras palavras, a conformidade é uma forma de medir o grau de proteção dos ativos e uma organização. A estrutura de segurança cibernética (CSF) do NIST é uma estrutura voluntária que consiste em padrões, diretrizes e práticas recomendadas para gerenciar o risco de segurança cibernética. As organizações podem optar por usar o CSF para obter conformidade com uma variedade de regulamentos.

Obs: os regulamentos são regras que devem ser seguidas, enquanto as estruturas são recursos que você pode optar por usar.

Desde sua criação, muitas empresas têm usado o CSF do NIST. Entretanto, a implementação do CSF pode ser um desafio devido ao seu alto nível de detalhes. Também pode ser difícil descobrir onde a estrutura se encaixa. Por exemplo, algumas empresas já estabeleceram planos de segurança, o que não deixa claro como o CSF pode beneficiá-las. Por outro lado, algumas empresas podem estar nos estágios iniciais da criação de seus planos e precisam de um ponto de partida.

Em qualquer cenário, a Agência de Segurança Cibernética e de Infraestrutura (CISA) dos EUA fornece orientações detalhadas que qualquer organização pode usar para implementar o CSF. Esta é uma visão geral rápida em um resumo de suas recomendações:

* Crie um perfil atual das operações de segurança e descreva as necessidades específicas de sua empresa.
* Realize uma avaliação de risco para identificar quais das suas operações atuais estão atendendo aos padrões comerciais e regulamentares.
* Analisar e priorizar as lacunas existentes nas operações de segurança que colocam em risco os ativos da empresa.
* Implementar um plano de ação para atingir as metas e os objetivos de sua organização.

**Controles de Segurança**

As informações têm estado espalhadas de forma abundante pela internet. Como resultado desse fenômeno, as organizações estão sob muita pressão para implementar controles de segurança eficazes que protejam as informações de todos de serem roubadas ou expostas. Os controles de segurança são proteções projetadas para reduzir riscos de segurança específicos. Eles incluem uma ampla variedade de ferramentas que protegem os ativos antes, durante e depois de um evento.

Os controles de segurança podem ser organizados em três tipos: técnicos, operacionais e gerenciais.

Controles técnicos incluem muitas tecnologias usadas para proteger ativos. Isso inclui criptografia, sistema de autenticação e outros.

Controles operacionais estão relacionados à manutenção do ambiente de segurança diário. Geralmente, as pessoas realizam esses controles, como treinamento de conscientização a resposta a incidentes.

Os controles gerenciais estão centrados em como os outros dois reduzem o risco. Exemplos de controles de gerenciamento incluem políticas, padrões e procedimentos.

Normalmente, a política de segurança da organização descreve os controles necessários para atingir suas metas. A privacidade das informações desempenha um papel fundamental nessas decisões. A privacidade das informações é a proteção do acesso e distribuição não autorizados de dados. A privacidade das informações diz respeito ao direito de escolha. Tanto as pessoas quanto as organizações merecem o direito de decidir quando, como e em que medida as informações privadas sobre elas são compartilhadas. Os controles de segurança são as tecnologias usadas para regular a privacidade das informações.

Por exemplo, imagine usar um aplicativo de viagem para reservar um voo. O usuário pode navegar por uma lista de voos e encontrar um com um bom preço. Para reservar um assento , o usuário insere algumas informações pessoais, como nome, e-mail e número do cartão de crédito para pagamento. A transação foi concluída com sucesso e o usuário reservou seu voo. Agora o usuário aguarda razoavelmente que a companhia aérea acesse essas informações que o usuário inseriu ao se inscrever para concluir a reserva.

No entanto, todos na empresa devem ter acesso às suas informações? Uma pessoa que trabalha no departamento de marketing não precisa acessar as informações do seu cartão de crédito. Faz sentido compartilhar essas informações com um agente de suporte ao cliente. Exceto que eles só precisam acessá-lo enquanto ajudam com sua reserva. Para manter a privacidade, os controles de segurança têm como objetivo limitar o acesso com base no usuário e na situação. Isso é conhecido como o privilégio mínimo.

Os controles de segurança devem ser projetados com o princípio mínimo em mente. Quando estão, confiam na diferenciação entre proprietários e guardiões de dados.

O proprietário dos dados é uma pessoa que decide quem pode acessar, editar, usar ou destruir suas informações. A ideia é simples, exceto nos casos em que há vários proprietários. A propriedade intelectual de uma organização pode ter vários proprietários de dados.

Um guardião de dados é uma pessoa que decide quem pode acessar, editar, usar ou destruir suas informações.

**Princípio do privilégio mínimo**

Os controles de segurança são essenciais para manter os dados confidenciais privados e seguros. Um dos controles mais comuns é o princípio do privilégio mínimo, também conhecido como PoLP ou privilégio mínimo. O princípio do privilégio mínimo é um conceito de segurança no qual o usuário recebe apenas o nível mínimo de acesso e autorização necessários para concluir uma tarefa ou função.

O privilégio mínimo é um controle de segurança fundamental que apoia a tríade Confiança, integridade e disponibilidade (CIA) das informações.

**Limitar o acesso reduz risco**

Toda empresa precisa se planejar para risco de roubo, uso indevido ou abuso de dados. A implementação do princípio mínimo pode reduzir muito o risco de incidentes dispendiosos, como violações de dados, ao

* Limitar o acesso a informações confidenciais.
* Reduzindo as chances de modificação, adulteração ou perda acidental de dados.
* Apoiar o monitoramento e a administração do sistema.

O privilégio mínimo reduz muito a probabilidade de um ataque bem-sucedido ao conectar recursos específicos a usuários específicos e impor limites ao que eles podem fazer. Trata-se de um importante controle de segurança que deve ser aplicado a qualquer recurso. Definir claramente quem ou o que são seus usuários geralmente é a primeira etapa da implementação eficaz do privilégio mínimo.

**Determinação de acesso e autorização**

Para implementação do privilégio mínimo, o acesso e a autorização devem ser determinados primeiro. Para isso, há duas semanas a serem feitas:

* Quem é o usuário?
* De quanto acesso ele precisa de um recurso específico?

Determinar quem é o usuário geralmente é simples. Um usuário pode se referir a uma pessoa, como um cliente, um funcionário ou um fornecedor. Também pode se referir a um dispositivo ou software que está conectado à sua rede de computadores. Em geral, cada usuário deve ter sua própria conta. Normalmente, as contabilizações são armazenadas e gerenciadas no serviço de diretório de uma organização.

Os tipos mais comuns de contas de usuário, são:

* As contas de convidado são fornecidas a usuários externos que precisam acessar uma rede interna, como clientes, contratados ou parceiros de negócios.
* As contas de usuário são atribuídas aos funcionários com base em suas funções.
* As contas de serviços são concedidas aos funcionários com base em funções.
* As contas privilegiadas têm permissões elevadas ou acesso administrativo.

É uma prática recomendada determinar um nível de acesso de base para cada tipo de conta para implementar o privilégio mínimo. Entretanto, o nível de acesso apropriado pode mudar de um momento para outro. Por exemplo, um representante do suporte ao cliente só deve ter acesso às suas informações enquanto o estiver ajudando. Os dados devem se tornar acessíveis quando o agente de suporte começar a trabalhar com outro cliente e não estiver mais ajudando-o ativamente. O privilégio só pode reduzir o risco se as contabilizações dos usuários forem monitoradas de forma rotineira e consistente.

Obs: As senhas desempenham um papel importante do princípio do privilégio mínimo. Mesmo que as contabilizações de usuários sejam atribuídas adequadamente, uma senha insegura pode comprometer seus sistemas.

**Auditoria de privilégios de conta**

Configurar as contas de usuário corretas a elas os privilégios adequados é um passo útil. A contabilização periódica dessas contas é uma parte chave da manutenção da segurança dos sistemas de sua empresa.

Existem três abordagens comuns para auditoria de conta de usuários:

* Auditorias de uso.
* Auditorias de privilégios.
* Auditorias de mudança de conta.

**Auditorias de uso**

Quando é realizada uma auditoria de uso, a equipe de segurança analisará quais recursos cada conta está acessando e o que usuário está fazendo com o recurso. As auditorias de uso podem ajudar a determinar se os usuários estão agindo de acordo com as políticas de segurança de uma organização. Elas também podem ajudar a identificar se um usuário tem permissões que podem ser revogadas porque não estão sendo mais usadas.

**Auditorias de privilégios**

Com o passar do tempo, os usuários tendem a acumular mais privilégios de acesso do que precisam , um problema conhecido como “privilege creep”. Isso pode ocorrer se um funcionário for promovido ou trocar de equipe e suas funções mudarem. As auditorias de privilégio avaliam se a função de um usuário está alinhada com os recursos aos quais ele tem acesso.

**Auditorias de Mudança de Conta**

Os serviços do diretório de contas mantêm registros e gerações de registros associados a cada usuário. As mudanças em uma conta geralmente são salvas e podem ser usadas para auditar o diretório em busca de atividades suspeitas, como várias tentativas de alterar a senha de uma conta. A realização de auditorias de mudanças de conta ajuda a garantir que todas as mudanças de conta sejam feitas por usuários autorizados.

**Ciclo de vida dos dados**

Organizações de todos os tamanhos lidam com uma grande quantidade de dados que devem ser mantidos em sigilo. Independente do estado em que os dados se encontram, as informações devem ser mantidas em sigilo, limitando o acesso e a autorização.

Na segurança de dados, as vulnerabilidades dos dados são frequentemente mapeadas em um modelo conhecido como ciclo de vida dos dados. Cada estágio do ciclo de vida dos dados desempenha uma função importante nos controles de segurança que são implementados para manter a tríade CIA das informações.

**Ciclo de vida dos dados**

O ciclo de vida dos dados é um modelo importante que as equipes de segurança consideram ao proteger as informações. Ele influencia a maneira como as equipes definem políticas que se alinham aos objetivos comerciais. Ele também desempenha um papel importante nas tecnologias que as equipes de segurança usam para tornar as informações acessíveis.

Em geral, o ciclo de vida dos dados tem cinco estágios. Cada um deles descreve como os dados fluem em uma organização desde o momento em que são criados até o momento em que não são mais úteis: coleta, armazenamento, uso, arquivar e destruir.

A proteção das informações em cada estágio desse processamento descreve a necessidade de mantê-las acessíveis e recuperáveis caso aconteça alguma adversidade.

**Governança de Dados**

As empresas lidam com grandes quantidades de dados todos os dias. Novas informações são coletadas constantemente de fontes internas e externas. Uma abordagem estruturada para o gerenciamento de todos esses dados é a melhor maneira de mantê-los privados e seguros.

A Governança de dados é um conjunto de processos que define como uma organização gerencia as informações. A governança geralmente inclui políticas que especificam como manter os dados privados, precisos, disponíveis e seguros durante todo o seu ciclo de vida dos dados.

* Proprietário dos dados: a pessoa decide quem pode acessar, editar, usar ou destruir suas informações.
* Custodiante de dados: qualquer pessoa ou coisa que seja responsável pelo manuseio, transporte e armazenamento seguro das informações.
* Administrador de dados: a pessoa ou o grupo que mantém e implementa as políticas de Governança dos dados definidas por uma organização.

As empresas armazenam, movem e transformam dados usando uma ampla gama de sistemas de TI. As políticas de Governança dos dados atribuem responsabilidade aos proprietários, custodiantes e administradores de dados.

**Proteção de dados em todos os estágios**

A maioria dos planos de segurança inclui uma política específica que descreve como as informações serão gerenciadas em uma organização. Isso é conhecido como política de governança de dados. Esses documentos definem claramente os procedimentos que devem ser seguidos para participar da manutenção da segurança dos dados. Eles impõem limites sobre quem ou o que pode acessar os dados. Os profissionais de segurança são participantes importantes na Governança dos dados. Como guardião dos dados, o profissional de segurança será responsável por garantir que os dados não sejam danificados, roubados ou usados indevidamente.

**Informações legalmente**

Dados são mais do que apenas um monte de 1s e 0s sendo processados por um computador. Os dados podem representar pensamentos, ações e as escolhas pessoais de alguém. Podem representar uma compra, uma decisão médica delicada e tudo mais. Por esse motivo, os proprietários dos dados devem ser os únicos a decidir se querem ou não compartilhar seus dados. Como profissional de segurança, a proteção de dados das decisões de privacidade dos dados de uma pessoa deve ser sempre respeitada.

A segurança de dados pode ser um desafio. Em grande parte, isso se deve ao fato de que os proprietários de dados geram mais dados do que podem gerenciar. Assim, os guardiões e administradores de dados, às vezes, não têm instruções diretas e explícitas sobre como devem lidar com tipos específicos de dados. As agências governamentais e outras agências reguladoras preencheram essa lacuna criando regras que especificam os tipos de informações que as organizações devem proteger por padrão:

PII é qualquer informação usada para inferir a identidade de um indivíduo. Informações de identificação pessoal, ou PII, referem-se a informações que podem ser usadas para contatar ou localizar alguém.

PHI significa informações de saúde protegidas e, nos EUA, são reguladas pelo HIPAA (Health Insurance Portability and Responsibility ACT), que define PHI como “informações relacionadas à saúde ou condição física ou mental passada, presente ou futura de um indivíduo” Na UE, as PHI têm uma definição semelhante, mas são reguladas pelo Regulamento Geral de Proteção de Dados (GPDR).

SPII é um tipo específico de PII que se enquadra em diretrizes de manuseio mais rigorosas. O S significa sensível, O significa que esse é um tipo de informação de identificação pessoal que só deve ser acessado com base necessária para saber, como um número de conta bancária ou credenciais de login.

Manter a privacidade das informações tomou proporção de importância maior nesses últimos tempos. Muitas organizações têm políticas de governança dos dados que descrevem como planejam proteger as informações confidenciais. Como um guardião dos dados, o profissional de TI têm um papel importante para manter as informações acessíveis e seguras durante todo o seu ciclo de vida dos dados. Há vários tipos de informações e controles que o profissional encontrará no dia a dia.

**Privacidade das informações: Reguladores e conformidade**

A segurança e a privacidade têm uma relação estreita. As pessoas têm direito de controlar seus dados pessoais. As organizações também têm a responsabilidade de proteger as informações que estão coletando contra o comprometimento ou o uso indevido. Um profissional de segurança estará diretamente envolvido nesses esforços. Os controles de segurança, frameworks e regulamentos de conformidade são usados em um conjunto para gerenciar a segurança e minimizar esforços.

**Segurança das informações vs privacidade de informações**

Segurança e privacidade são dois termos que frequentemente são usados de forma intercambiável fora desse campo. Embora os dois conceitos estejam conectados, eles representam funções específicas:

A privacidade dos dados refere-se à proteção contra o acesso não autorizado e a distribuição dos dados.

Segurança da informação (InfoSec) refere-se à prática de manter os dados em todos os estados longe de usuários não autorizados.

A diferença chave: A personalização consiste em fornecer às pessoas controle sobre suas informações pessoais e como elas são compartilhadas. Segurança é proteger as escolhas das pessoas e manter suas informações protegidas contra possíveis ameaças.

Por exemplo, uma empresa de varejo pode querer coletar tipos específicos de informações pessoais sobre seus clientes para fins de marketing, como idade, sexo e localização. A forma como essas informações privadas serão usadas deve ser divulgada aos clientes antes de serem coletadas. Além disso, os clientes devem ter a opção de não participar caso decidam não compartilhar seus dados.

Depois que a empresa obtém o consentimento para coletar informações pessoais, ela pode implementar controles de segurança específicos para proteger esses dados privados contra acesso, uso ou divulgação não autorizados. A empresa também deve ter controles de segurança para respeitar a privacidade de todas as partes interessadas e de qualquer pessoa que tenha optado por não participar.

**O porquê da privacidade ser tão importante para a segurança**

A privacidade e a proteção de dados são tópicos que começaram a ganhar muita atenção no final da década de 1990. Naquela época, as empresas de tecnologia passaram repentinamente do processamento dos dados das pessoas para o armazenamento e o uso desses dados para fins comerciais. Por exemplo, se um usuário procurasse um produto on-line, as empresas começavam a armazenar e compartilhar o acesso às informações sobre o histórico de pesquisa desse usuário com outras empresas. Assim, as empresas podiam oferecer experiências de compras personalizadas ao usuário gratuitamente.

Por fim, essa prática levou a uma discussão global sobre se essas organizações tinham o direito de coletar e compartilhar os dados privados de alguém. Além disso, a questão de segurança de dados tornou-se uma preocupação maior; quanto mais as organizações coletarem dados, maior seria vulnerabilidade de abuso, uso indevido ou roubo.

Muitas organizações passaram a se preocupar mais com as questões de Privacidade de dados. As empresas se tornaram mais transparentes sobre como estavam coletando, armazenando e usando as informações. Elas também começaram a implementar mais medidas de segurança para proteger a privacidade dos dados das pessoas. Entretanto, sem regras claras, as proteções eram aplicadas de forma inconsciente. Quanto mais dados coletados, armazenados e usados, maior é a vulnerabilidade a violações e ameaças.

**Regulamento de privacidade notáveis**

O Business-to-business são obrigados a obedecer a determinadas leis para operar. Os reguladores são regras estabelecidas por um governo ou outra autoridade para controlar a maneira como algo é feito. Os regulamentos de privacidade, em particular, existem para proteger um usuário de ter suas informações coletadas, usadas ou compartilhadas sem o consentimento do usuário. Os reguladores também podem descrever as medidas de segurança que precisam ser adotadas para manter informações privadas longe de ameaças.

Três dos regulamentos mais influentes do setor que todo profissional de segurança deve conhecer: Regulador Geral de Proteção de Dados (GDPR), Padrão de segurança de dados da indústria de cartões de pagamento (PCI DSS), Lei de portabilidade e responsabilidade de seguros de saúde (HIPPA).

GDPR - conjunto de regras e regulamentos desenvolvidos pela União Europeia que coloca os proprietários de dados no controle total de suas informações pessoais. De acordo com o GDPR, os tipos de informações pessoais incluem o nome, endereço, o número de telefone, as informações financeiras e as informações médicas de uma pessoa.

PCI DSS - conjunto de padrões de segurança formado pelas principais organizações do setor financeiro. Esse regulamento tem como objetivo proteger as transações com cartões de crédito e débito contra roubo e fraude de dados.

HIPAA - é uma lei dos EUA que exige proteção de informações confidenciais sobre a saúde dos pacientes. A HIPAA proíbe a divulgação de informações médicas de uma pessoa sem o conhecimento do usuário e o consentimento. Esses reguladores influenciam o manuseio de dados em muitas organizações em todo o mundo, embora tenham sido desenvolvidos por nações específicas.

Os reguladores influenciam o manuseio de dados em muitas organizações em todo o mundo, embora tenham sido desenvolvidos por nações específicas.

**Avaliações e auditorias de segurança**

As empresas devem cumprir os regulamentos importantes se seu vetor. Isso valida que elas cumpriram um nível mínimo de segurança e, ao mesmo tempo, demonstra a dedicação em manter a privacidade de dados.

O cumprimento dos padrões de conformidade geralmente é um processo contínuo, em duas partes de auditorias e avaliações de segurança:

Uma auditoria de segurança é uma revisão dos controles, políticas e procedimentos de segurança de uma organização em relação a um conjunto de expectativas.

Uma avaliação de segurança é uma verificação para determinar a resiliência das implementações de segurança atuais contra ameaças.

Se um regulador determinar que a Autenticação Multifator (MFA) deve ser ativada para todas as contas de administrador, poderá ser realizada uma auditoria para verificar a conformidade dessas contas de usuário. Após a auditoria, a equipe interna pode realizar uma avaliação de segurança que determina que muitos usuários estão usando senhas fracas. Com base nessa avaliação, a equipe pode decidir ativar o MFA em todas as contas de usuário para melhorar a postura geral de segurança.

Como analista de segurança, é provável que você esteja envolvido em auditorias e avaliações de segurança no campo. As empresas geralmente realizam auditorias de segurança com menos frequência, aproximadamente uma vez por ano. As auditorias de segurança podem ser realizadas interna e externamente por diferentes grupos de terceiros.

Por outro lado, as avaliações de segurança geralmente são realizadas com mais frequência, aproximadamente a cada três a seis meses, e geralmente são realizadas por funcionários internos, muitas vezes como preparação para uma auditoria de segurança. Ambas as avaliações são formas extremamente importantes de garantir que seus sistemas estejam protegendo efetivamente a privacidade de todos.

**A importância de proteger a PII**

PII está em toda parte. É uma parte fundamental de como todos trabalhamos on-line o tempo todo. Se você estiver usando recursos on-line, provavelmente está divulgando suas PII em algum lugar. Há algumas de suas PII que muitas pessoas conhecem, como seu nome. Além disso, há dados confidenciais que o profissional não quer que as pessoas saibam, como o número da sua conta confidencial que você não quer que muitas saibam, como o número da sua conta bancária ou suas informações médicas privadas. Por isso, muitas vezes fazemos essas distinções porque esse tipo de informação precisa ser tratado de forma diferente.

Mais informações:

[https://www.cisa.gov/sites/default/files/publications/Commercial\_Facilities\_Sector\_Cy](https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf)

[bersecurity\_Framework\_Implementation\_Guidance\_FINAL\_508.pdf](https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf)

[https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/7MS3w](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/7MS3w/information-privacy-regulations-and-compliance)

[/information-privacy-regulations-and-compliance](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/7MS3w/information-privacy-regulations-and-compliance)

[https://docs.google.com/document/d/1fqPEK1Cy9cLsR4SvewhqfanU75JkAegy1TAJ](https://docs.google.com/document/d/1fqPEK1Cy9cLsR4SvewhqfanU75JkAegy1TAJNcWex5U/template/preview?resourcekey=0-rYoRJ_z6hCgITUqRwmOoCQ)

[NcWex5U/template/preview?resourcekey=0-rYoRJ\_z6hCgITUqRwmOoCQ](https://docs.google.com/document/d/1fqPEK1Cy9cLsR4SvewhqfanU75JkAegy1TAJNcWex5U/template/preview?resourcekey=0-rYoRJ_z6hCgITUqRwmOoCQ)

<https://www.coursera.org/learn/assets-threats-and-vulnerabilities/quiz/NkQt0/activity-determine-appropriate-data-handling-practices/attempt>

[https://docs.google.com/document/d/1677CNrxn-Ap6oFX-OY0r23yoPQq46wPWZQ](https://docs.google.com/document/d/1677CNrxn-Ap6oFX-OY0r23yoPQq46wPWZQmZus28oDo/template/preview?resourcekey=0-gr_UkcEPsUVSOMNRLyS8aw)

[mZus28oDo/template/preview?resourcekey=0-gr\_UkcEPsUVSOMNRLyS8aw](https://docs.google.com/document/d/1677CNrxn-Ap6oFX-OY0r23yoPQq46wPWZQmZus28oDo/template/preview?resourcekey=0-gr_UkcEPsUVSOMNRLyS8aw)

<https://en.wikipedia.org/wiki/Heartbleed>

<https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle>