10 PASSOS

Para uma proteção efetiva de dados

ENJOY SAFER TECHNOLOGY™


35%

Mostramos as melhores práticas em segurança que irão ajudá-lo a garantir uma **proteção efetiva dos dados de sua empresa.**

1 CRIAR POLÍTICAS DE SEGURANÇA

Muitas empresas rejeitam a importância de políticas de segurança escritas e vão direto para os controles técnicos. Controles técnicos (como firewalls, proteção de endpoint e outros) implementados sem controles administrativos (isto é, políticas e procedimentos) são quase sempre implementados de uma maneira reativa, sem uma estratégia de segurança abrangente, coerente e bem pensada, e estrutura de gestão de segurança (que suas políticas junto à análise de segurança da informação ajudam a definir). Isso significa inevitavelmente que você gastará muito em soluções técnicas que não são implementadas efetivamente (ou adequadamente) e que fornecerão proteção incompleta ou inadequada.

2 IDENTIFICAR SEUS ATIVOS

Você precisa saber o que está protegendo, então é importante manter um inventário preciso de todo o seu software e hardware de TI. Sem um inventário completo, você pode não estar ciente de sistemas vulneráveis em sua rede que podem aumentar sua exposição a ataques. Por exemplo, na invasão de dados de 2013 da Target, os atacantes acessaram remotamente um sistema de manutenção de aquecimento, ventilação e ar-condicionado (HVAC) para finalmente invadirem as informações pessoais e/ou do cartão de crédito/débito de 110 milhões de clientes. Há muitas ferramentas gratuitas disponíveis que você pode usar para varrer sua rede e endpoints para começar. Soluções comerciais podem ajudar você a manter com precisão seu inventário de ativos continuamente, e muitos também fornecem capacidades de gestão remota para ajudar você a instalar, remover e atualizar softwares também. Você precisa reduzir a superfície de ataque para todos os seus ativos conectados à internet (incluindo dispositivos móveis pessoais), instalando e mantendo proteção de segurança adequada.

3 CONHECER SUA POSTURA DE SEGURANÇA

Isso é simples como criar um mapa ou modelo de maturidade para mostrar onde você está hoje (seu estado atual) e usar uma abordagem baseada em riscos para identificar ameaças relevantes para os ativos do seu ambiente (veja a dica anterior) e as medidas de proteção de dados e cibersegurança apropriadas. Você poderá então realizar uma análise de falhas e determinar quais passos você precisa tomar e onde investir seus recursos.

4 CLASSIFICAR TODOS OS SEUS DADOS

Para muitas empresas, dados sensíveis do cliente e outras informações proprietárias representam as "joias da coroa" da empresa, mas fornecer uma proteção e controles iguais para todos os seus dados através do ciclo de vida não é nem prático, nem desejável. Ao invés disso, pense em quais dados o fariam ficar acordado a noite se fossem perdidos ou roubados. Como uma violação de dados impactaria a imagem da sua marca, fidelidade do cliente ou mesmo a viabilidade contínua da sua empresa? Crie (e documente) uma política de classificação de dados intuitiva para sua organização que inclua rótulos de classificação (como "Somente

para uso interno", "Dados sensíveis" e "Aprovado para liberação pública") e que especifique requisitos de proteção de dados (como criptografia, cópias de segurança, aprovação de liberação e destruição) para diferentes níveis de informação.

> A Regulamentação de Proteção Geral de Dados (GDPR) requer que as organizações excluam dados pessoais se solicitado por alguém (por exemplo, um indivíduo). Para ajudar você a estar em conformidade com os requisitos GDPR, desenhe sua estratégia de classificação de dados para ajudar você a identificar ou sinalizar dados pessoais (incluindo cópias de segurança) que podem precisar ser excluídos ou alterados de outra maneira no futuro.

5 CRIPTOGRAFAR SEUS DADOS SENSÍVEIS

A criptografia de dados converte dados de texto simples em um formato ilegível (conhecido como "texto cifrado"), tornando-o inutilizável para partes não autorizadas que não possuam as chaves de criptografia/descriptografia. Portanto, a chave para uma criptografia eficiente é proteger as chaves adequadamente. No mínimo, você deveria criptografar dados "parados" (armazenados). Você pode usar uma criptografia adicional em dados "em movimento" (ou "em trânsito", por exemplo, usando criptografia de Camadas de Soquete Seguro (SSL)). Finalmente, para dados "em uso", você deveria tirar vantagem da criptografia dentro da aplicação, se disponível. A criptografia pode ser baseada no hardware ou software.

> Muitas regulamentações de violação de dados incluem disposições de porto seguro para dados que estão criptografados, o que pode reduzir significativamente o curso e impacto de uma violação de dados.

6 FAZER CÓPIA DE SEGURANÇA E RECUPERAÇÃO (TESTE) DOS SEUS DADOS VALIOSOS

Garantir cópias de segurança regulares e confiáveis de seus sistemas e dados é uma melhor prática de segurança básica, mas essencial. Boas cópias de segurança garantem que você possa recuperar um arquivo que foi excluído acidentalmente, ou um disco rígido que foi corrompido. Com os custos de backup baseado em disco continuando a cair e soluções de backup baseadas na nuvem com custo efetivo e fáceis de usar, simplesmente não há desculpas para não fazer cópias de segurança. Com o rápido crescimento do ransomware nos últimos anos, cópias de segurança são a única maneira de garantir seus dados de volta, se você for uma vítima de um ataque de ransomware. E, como bônus, você não precisará pagar o resgate.

> Você precisa testar regularmente sua habilidade de recuperar seus sistemas e dados críticos a partir de cópias de segurança, não apenas para garantir que as cópias não estejam corrompidas, mas também para verificar que você e sua equipe conheçam o processo de recuperação.

7 INVESTIR EM PROTEÇÃO DE ENDPOINT

"Investir" não significa fazer download de algum software antivírus gratuito da internet. Significa proteger todos os seus endpoints – computadores de mesa, dispositivos móveis e servidores – com uma solução de proteção de endpoint comercial robusta. Hoje, a informação está em todos os lugares e agora, mais do que nunca, o endpoint é onde tudo se junta. Então é definitivamente uma área que vale a pena investir.

8 PLANEJAR E PREPARAR

Toda empresa precisa ter um plano de resposta a incidentes, continuidade de negócios e planos de recuperação de desastre. Sua equipe de resposta a

incidentes precisa ser treinada em procedimentos forenses básicos para garantir que todo incidente de segurança seja tratado como caso legal potencial e garanta que a cadeia de custódia seja mantida para qualquer evidência potencial. Os planos de continuidade de negócios e recuperação de desastres ajudam seu negócio a retomar as operações normais de negócios o mais rapidamente possível após um grande evento ou desastre. Comunicações pontuais e precisas, internas e externas, são um componente crítico de qualquer continuidade de negócios e planos de recuperação de desastre.

9 TREINAR SEUS USUÁRIOS

O elo mais fraco em qualquer segurança da organização sempre foi o usuário final, mas isso não é necessariamente culpa dele. É improvável que todos que trabalham para sua empresa tenham sido contratados porque são especialistas em segurança. Os atacantes sabem disso e usam técnicas de engenharia social para atrair usuários inocentes a clicar em links maliciosos em e-mails de spam ou com phishing, revelar senhas **(veja a seguir: "Como criar uma senha forte?")** e visitar websites maliciosos, dentre outras táticas. Conduza exercícios de treinamento de consciência de segurança regulares, envolventes, relevantes e curtos para ajudar seus usuários a ajudarem a si mesmos e, portanto, ajudarem você!

10 NÃO "LUTE" SOZINHO

Os cibercriminosos não trabalham sozinhos. Eles trabalham com outras pessoas de caráter duvidoso para atingir seus objetivos de ataque, reutilizar código malicioso na dark web e recrutar vítimas inocentes cujos endpoints violados tornaram-se bots em um exército de botnets focando outras vítimas. Mas os mocinhos também não estão sós. Impulsione a ampla comunidade de especialistas em segurança a partir da aplicação de lei local para associações profissionais, serviços de segurança gerenciados e terceirizados, inteligência de ameaça baseada na nuvem em tempo real e muito mais.

NOSSAS **SOLUÇÕES DE SEGURANÇA**

- Antivírus para endpoints
- Criptografia
- Backup & Recuperação
- Duplo Fator de Autenticação
- Prevenção de Vazamento de Dados

Como criar uma senha forte?

Quase tudo que fazemos online precisa de um login e todo login precisa de algum tipo de autenticação para verificar que somos quem dizemos ser. Assim, sua **senha deverá ser tão única (e complexa) como você é! Seguem algumas dicas.**

✓ **Use senhas longas e frases-chave.**
As senhas devem ter ao menos 8 caracteres de comprimento, mas não devem ser tão longas a ponto de você não se lembrar delas (veja a dica abaixo). Verifique se sua senha não foi exposta em uma violação de dados em https://haveibeenpwned.com/Passwords.

✓ **USE frases únicas e caracteres especiais.**
Uma única frase que consiste de 30 ou mais caracteres (talvez com alguns números, letras maiúsculas e pontuação(que você possa lembrar é muito melhor do que uma palavra de 8 caracteres comum com substituições comuns (como um "3" para a letra "e").

✓ **USE um programa gerenciador de senhas (gratuito ou pago).**
Um gerenciador de senhas pode ser útil para criar, armazenar, gerenciar e lembrar senhas únicas, fortes para seus vários logins de dispositivos, sistema e aplicações. Também pode ajudar a eliminar a prática comum de escrever senhas em documentos ou em notas adesivas.

✓ **USE senhas que você possa lembrar.**
Senhas muito complexas e completamente aleatórias que sejam difíceis de lembrar podem na verdade ser contraproducentes e tornar sua conta menos segura, porque tende a levar a más práticas como anotar senhas e usar a mesma senha em contas diferentes de trabalho e pessoais.

✓ **Use autenticação multifator (MFA).**
Quando possível, a MFA deve ser habilitada nas suas contas ao invés de, ou adicionalmente a, senhas. A MFA incorpora dois ou mais fatores de autenticação ("algo que você sabe", como seu nome de usuário e/ou senha, e "algo que você tem", como um hardware ou token de software, ou um software). Ao entrar em uma conta com MFA, um código único é gerado no seu token ou enviado via mensagem de texto SMS para seu smartphone. O código pode ser usado apenas uma vez e apenas dentro de um período de tempo limitado (geralmente dentro de um a cinco minutos). Isso torna extremamente difícil para um atacante interceptar seu código e usá-lo para fazer login na sua conta sem seu conhecimento e antes que o código expire.

✓ **NÃO use a mesma senha duas vezes, independente do quão boa ela seja.**
Se sua senha for comprometida em um lugar (digamos, sua conta de e-mail pessoal do Yahoo!), os cibercriminosos tentarão usar essas mesmas credenciais em outros locais (como sua conta bancária online).

✓ **NÃO compartilhe suas senhas com ninguém – jamais!**
Trate suas senhas como algo mais sagrado do que sua escova de dentes (que você pode ocasionalmente compartilhar com seu companheiro(a) – ou seu cachorro).

✓ **NÃO use palavras comuns do dicionário.**
Programas de quebra de senha automatizados tem um trabalho fácil com dicionários – incluindo línguas estrangeiras e termos médicos, legais ou de engenharia. Também evite caracteres repetitivos (por exemplo, "aaaa"), caracteres sequenciais (por exemplo, "1234") e padrões reconhecíveis (por exemplo, "qwerty").

✓ **NÃO use informações pessoais em sua senha.**
As mídias sociais tornaram mais fácil do que nunca para os cibercriminosos conhecerem seus detalhes pessoais – incluindo seu nome do meio, data de nascimento, endereço, escola, nome do cônjuge e filhos, e o que você fez no último verão!

A ESET é uma empresa pioneira em proteção antivírus que nasceu há mais de 25 anos com a criação do multipremiado software para detecção de ameaças ESET NOD32 Antivírus. Agora, o objetivo da ESET é garantir que todos possam aproveitar as grandes oportunidades que a tecnologia oferece. Hoje, nossas soluções de segurança permitem que as empresas e os consumidores em mais de 180 países possam aproveitar mais o mundo digital.

www.eset.com/br