Type Here

Portal de Soluções de TI - Sonda

Type Here
HOMEPAGETECNOLOGIA DA INFORMAÇÃO
TECNOLOGIA DA INFORMAÇÃO
Falhas de segurança: o que fazer para identificar e minimizar?
Falhas de segurança: o que fazer para identificar e minimizar?
Você reparou como falhas de segurança têm se tornado um problema cada vez mais rotineiro e comum? A propósito, nos últimos meses, ataques cibernéticos acabaram ganhando espaço nos noticiários tanto por seu impacto quanto por seu tamanho. Ouviu falar no WannaCry? Essas ameaças comprometem a execução de atividades das empresas e, muitas vezes, ainda promovem a perda de dados críticos, gerando insatisfação de clientes e até problemas judiciais.

Para impedir que esses problemas afetem seu negócio, você precisa adotar estratégias que diminuam as chances de eventuais falhas de segurança atingirem as operações da empresa. Quer saber como? Conheça no post de hoje as principais estratégias para identificar, evitar e mitigar falhas de segurança no ambiente corporativo. Esses métodos podem ser usados para maximizar a confiabilidade da infraestrutura de TI e, assim, criar um local de trabalho com alta performance e segurança. Curioso? Então confira!

Contar com sistemas de alta qualidade
Aplicativos mal desenvolvidos costumam ser grandes portas de entrada para ameaças digitais no ambiente corporativo. E o pior: muitos desses ataques acontecem graças ao rastreamento de falhas e vulnerabilidades de segurança que podem ser desconhecidas até mesmo do desenvolvedor do software! Por meio de diversas técnicas de ataque, esses bugs são usados para roubar informações.

Diante de tudo isso, é essencial que o negócio adote aplicativos bem construídos, verificando como o desenvolvedor foca em segurança digital nos seus processos de criação e atualização de cada sistema. Uma outra boa prática ao utilizar softwares adquiridos de empresas terceiras, é solicitar uma análise de códigos externa de uma empresa focada em desenvolvimento seguro, assim evidenciando a qualidade do aplicativo. É bom avaliar também a política de suporte, útil para identificar como a empresa entrega atualizações e correções de segurança. Por fim, a ordem é sempre evitar sistemas piratas, que possuem seu código-fonte modificado, aumentando as chances de a aplicação possuir malwares ocultos.

Criar uma política de controle de acesso
A verdade é que ataques podem acontecer a qualquer momento. Para impedir que eles causem danos maiores ao empreendimento, é preciso criar mecanismos a fim de reduzir o impacto gerado pelo comprometimento das contas de usuário. Uma das principais táticas

aqui consiste em criar uma política de controle de acesso, que permite que a companhia tenha um controle maior sobre quem pode acessar, modificar e remover arquivos ou sistemas internos.

Implemente uma política que restrinja o acesso aos conteúdos, liberando apenas o que cada time realmente precisa. Entre em contato com todos os setores para verificar quais informações e conteúdos usados no dia a dia, aqueles essenciais para o cumprimento das atividades de rotina. Dessa forma, você consegue limitar o acesso apenas ao essencial, protegendo o restante.

Mas atenção: se você acha que basta implementar uma política de segurança e o trabalho está feito, pense de novo. A jornada na verdade só começou! A partir daí, a empresa deve monitorar continuamente sua infraestrutura por meio de tecnologia de segurança. Assim, o gestor consegue avaliar, em tempo real, se alguma conta tem demonstrado um comportamento que indique uma invasão aos recursos internos do negócio. Dessa forma, ataques serão mitigados com agilidade e precisão.

Divulgar boas práticas para os usuários
A maioria dos ataques digitais acontece graças à interação do próprio usuário. Justamente por isso, é importante que a empresa divulgue boas práticas de TI, dicas que reforcem o impacto causado pela política de segurança digital implementada pelo negócio. Para começar, instrua os profissionais a usarem senhas complexas, compostas por letras, números e símbolos, ainda variando entre maiúsculas e minúsculas.

Além disso, sempre que possível, adote a autenticação de 2 passos, dando preferência para a geração de tokens via aplicativo ou até tokens físicos. Dessa maneira, se a senha da conta for comprometida, o acesso ao serviço será bloqueado. Os profissionais também devem configurar alertas para logins via dispositivos desconhecidos em todos os sistemas em que essa opção estiver disponível. Links enviados por e-mail devem ser copiados e colados na barra de endereço do browser, comparando se o link leva para o site que aparecia diretamente no e-mail, enquanto senhas só devem ser digitadas em sites seguros, com conexões https.

Uma última boa prática essencial envolve o envio e o recebimento de arquivos de forma segura. Que tal, ao receber um arquivo, ter que confirmar seu envio por outro canal, como um telefonema, por exemplo? O envio de arquivos também pode ser feito por meio de uma plataforma de armazenamento em nuvem, dando maior controle sobre quem visualiza e modifica os dados da empresa.

Possuir um plano de mitigação de riscos
O plano de mitigação de riscos garante que a empresa estará preparada para enfrentar ameaças e outros fatores que possam contribuir para a diminuição da segurança dos seus profissionais. Trata-se de uma documentação contendo procedimentos e medidas que devem ser tomados para reduzir as chances de problemas acontecerem e, em caso de falhas, ajudar os técnicos a eliminarem o problema o mais rapidamente possível.

Isto envolve também a responsabilidade sobre os riscos e o mapeamento de possíveis vulnerabilidades que a corporação possa ter, assim tornando o mapa de riscos de TI endereçado, com domínios em todas as áreas, garantindo a visibilidade e rastreabilidade de todas as verticais, desde uma aplicação até um firewall, os computadores corporativos e até mesmo os dispositivos móveis dos colaboradores.

Para ser eficaz, o plano de mitigação de riscos deve ser criado por meio de um processo que envolva todos os setores da empresa. A infraestrutura de TI precisa ser minuciosamente analisada para que quaisquer possíveis problemas sejam logo identificados. Assim, o gestor consegue planejar e testar ações para mitigar os riscos com mais precisão e qualidade.

Fazer backup dos dados

Em relação a falhas de segurança, o backup de dados continua sendo uma das principais medidas preventivas que podem ser tomadas pelas empresas. É por meio desse procedimento, afinal, que gestores garantem a rápida recuperação de arquivos e sistemas em caso de ameaças ou interrupções em serviços críticos. É preciso ressaltar que uma política de backup de dados eficaz envolve várias mídias de armazenamento, com a empresa mesclando soluções para maximizar a disponibilidade de seus dados sempre que necessário — como o uso de servidores próprios e da computação na nuvem.

Além do mais, a cópia de cada sistema deve ser feita regularmente, com o negócio fazendo backups de acordo com a importância e a frequência em que os dados são alterados. Assim, arquivos importantes e que são modificados frequentemente devem ter suas cópias criadas em intervalos menores. Por outro lado, bancos de dados que são modificados poucas vezes ao ano, por exemplo, podem ter seus backups criados com intervalos mais longos.

Mantendo uma boa política de segurança digital, a empresa reduz riscos e maximiza sua capacidade de atuar sem interrupções. Nesse cenário, os profissionais sempre terão acesso a uma infraestrutura de TI sólida e confiável, que pode ser continuamente integrada a processos relacionados com o core business do empreendimento.

Gostou das nossas dicas sobre falhas de segurança e quer saber como tornar sua empresa mais eficaz? Então curta a nossa página no Facebook para receber mais dicas em primeira mão!

NEXTDatabase of Things: o que é e por que se tornou uma tendência? »
PREVIOUS « Conheça os 7 maiores desafios enfrentados por empresas SaaS
SHARE

PUBLISHED BY
SONDA
2 ANOS AGO
RELATED POST
Como está acontecendo a transformação digital no Brasil?
Como a computação cognitiva pode ajudar sua empresa?
Web Application Firewall: 5 dúvidas frequentes sobre o assunto
RECENT POSTS
GESTÃO DE NEGÓCIOS
Outsourcing: planejando a terceirização sem perder a qualidade nos processos
O outsourcing não é uma estratégia nova. A parceria entre dois ou mais empreendimentos para cuidar de tarefas não essenciais…

9 meses ago
TECNOLOGIA DA INFORMAÇÃO
Como está acontecendo a transformação digital no Brasil?
A tecnologia está reconfigurando diversos setores do mercado e trazendo inúmeros benefícios. Ao contrário dos tempos passados, quando as inovações vinham…

9 meses ago
INDICADORES
Conheça as principais características do consumidor 5.0
A partir da década de 80, quando a tecnologia computacional começou a fazer parte da rotina das pessoas, muita gente…

9 meses ago
GESTÃO DE NEGÓCIOS
Saiba como reduzir custos no setor de vendas em 10 passos
Com o aumento da instabilidade política e econômica vivida em toda a América Latina nos últimos tempos, diversas empresas têm…

10 meses ago
GESTÃO DE NEGÓCIOS
Gestão de métricas: o que é e como fazer corretamente?
O controle eficiente de processos e resultados é um ponto central para a gestão de qualquer negócio. Afinal, com informações…

10 meses ago
INDICADORES
Entenda a importância da análise preditiva no setor comercial
A análise preditiva vem ganhando espaço no mundo corporativo, já que permite “prever” o

que vai acontecer no futuro. Não,…

10 meses ago