GUIA PRÁTICO DE SEGURANÇA DE TI PARA PEQUENAS EMPRESAS

Como garantir uma segurança de TI abrangente para sua empresa

#protectmybiz

KASPERSKY lab

As pequenas empresas apresentam-se em todas as formas e tamanhos. Porém, em todo o mundo, nenhuma organização pode se dar ao luxo de ignorar a segurança on-line - seja uma equipe operando fora do escritório ou um indivíduo trabalhando de casa. É um problema que afeta a todos.

Embora o crime virtual tenha grande visibilidade em noticiários, isso ocorre geralmente quando uma grande multinacional ou um governo são as vítimas. Mas, indiscutivelmente, são as vítimas sem visibilidade que mostram um problema maior.

Apenas em 2014, 143 milhões de novas instâncias de malware foram detectadas.[1] A maioria desses casos foi direcionada a indivíduos e organizações que não se consideravam alvos prováveis.

A verdade é que qualquer pessoa pode ser um alvo. A boa notícia é que ainda há uma grande diferença entre ser um alvo
e ser uma vítima.

No fim das contas, o importante é estar preparado.
É por isso que criamos este guia:
para oferecer a você o conhecimento para manter a sua empresa em segurança.

? O QUE É O MALWARE?

O termo malware se refere a programas de computador projetados para fins maliciosos. Eles geralmente atacam dispositivos sem que o usuário tenha conhecimento. A Kaspersky Lab é líder mundial em detecção de malware e conquistou as pontuações mais altas que qualquer outro fornecedor de segurança.[2]

? POR QUE PRECISO DE PROTEÇÃO?

Criminosos virtuais não precisam esvaziar sua conta bancária para afetar seus negócios financeiramente. Os transtornos causados por malware podem interromper sua produtividade e fluxo de caixa, causando uma série de consequências indesejadas. Você pode se proteger contra esses problemas com passos relativamente simples, e não é necessário muito esforço para ter tranquilidade.

1. AV Tests
2. Estudo independente de resultados de testes TOP3 2014

SUA LISTA DE SEGURANÇA

O PRIMEIRO PASSO PARA A SEGURANÇA DE SUA EMPRESA É ANALISAR SEU TRABALHO E VER ONDE O RISCO PODE SER REDUZIDO. ENTÃO, FAÇA UMA VERIFICAÇÃO RÁPIDA DE SUA SEGURANÇA DE TI:

PROTEÇÃO ANTIMALWARE ✔

Assim como acontece com o seguro de negócios, você deseja os melhores produtos que possam proteger a sua empresa. Se você ainda não tem um software altamente capaz de proteger seus dispositivos contra infecções, faça disso sua prioridade.

Infelizmente, estar atento enquanto está on-line não é o bastante. Todos sabem que não se deve abrir anexos de remetentes desconhecidos, nem baixar arquivos de sites suspeitos. No entanto, muitas infecções vêm de fontes confiáveis que foram comprometidas.

COMPORTAMENTOS DE NAVEGAÇÃO ✔

Educar a sua equipe sobre a importância da navegação segura on-line pode poupar muitas dores de cabeça. Espera-se que sua equipe compreenda que determinados tipos de sites não devem ser acessados no trabalho. Mas, se eles também estiverem usando um dispositivo móvel de uso pessoal (como um smartphone ou tablet), uma vez que o expediente acaba, a preocupação com a segurança se torna menos importante. Assim que é uma boa ideia bloquear sites inapropriados para garantir que não possam ser acessados nos computadores da empresa. Aumentar a conscientização a respeito de ameaças de segurança de IT também ajudará os funcionários a se protegerem durante o uso pessoal.

? COMO ISSO ME AFETA?

Você já recebeu um e-mail de um amigo ou familiar com um link interessante que, após aberto, pareceu suspeito? Após o malware infectar um computador, poderá executar ações sem que o usuário tome conhecimento. É por isso que fontes confiáveis nem sempre são seguras.

SENHAS ✔

Os funcionários também precisam se certificar de que estão usando senhas fortes e únicas contendo símbolos, numerais e letras maiúsculas e minúsculas misturados. Palavras de uso cotidiano podem ser descobertas por programas que simplesmente fazem verificações por meio de dicionários até encontrar o termo correto. E, ainda que seja forte, caso uma senha comprometida seja usada para múltiplos propósitos, isso poderá levar a violações ainda maiores.

ATUALIZAÇÕES ✔

Quatro novos tipos de malware são detectados a cada segundo.[3] Você precisa estar preparado. Isso significa atualizações automatizadas para melhorar seu software de segurança diariamente, atualizando todos os outros softwares sempre que possível e garantindo que todos na empresa façam o mesmo. Lembre-se de que programas que não foram atualizados são a principal rota de violação de negócios utilizada por criminosos virtuais.

CERTIFIQUE-SE DE NÃO COMETER ESTES ERROS DE SENHA CLÁSSICOS:

1. Opções fáceis de lembrar, mas fáceis de adivinhar, como "senha" ou "123456"
2. Utilizar seu endereço de e-mail, nome ou outros dados facilmente disponíveis para senhas
3. Configurar lembretes de senha que um hacker possa responder com um pouco de pesquisa, como o nome de solteira de sua mãe
4. Realizar modificações óbvias em palavras comuns, como colocar um "1" no final
5. Utilizar frases comuns. Mesmo pequenas frases, como "euteamo" são facilmente descobertas

Para obter mais dicas sobre como criar senhas difíceis de adivinhar, consulte a postagem sobre o assunto em nosso blog.

3 AV Tests

EM 2014

295.500

NOVAS AMEAÇAS MÓVEIS DE MALWARE[4]

BANCOS ✔

Desde direcioná-lo a versões falsas de sites confiáveis a utilizar malware para espionar sua atividade, criminosos virtuais possuem diversos métodos para obter suas informações financeiras. Você precisa tomar medidas ativas para interrompê-los.

Fique atento quanto a tentativas de phishing quando golpistas se fazem passar por seu banco: sempre utilize um navegador seguro e certifique-se de verificar o URL antes de inserir seus detalhes em qualquer site. Evite incluir essas informações em e-mails, pois elas podem ser vistas por pessoas a que não se destinam.

DISPOSITIVOS MÓVEIS ✔

Como o trabalho remoto agora faz parte do cotidiano, o crime virtual está cada vez mais direcionado a dispositivos móveis. Em 2014, 295.500 novas ameaças móveis de malware (aquelas criadas especificamente para smartphones e tablets) foram detectadas a cada mês.[5] Embora a proteção de telefones e tablets seja tão importante quanto de Macs e PCs, somente 32% dos pequenos negócios reconhecem atualmente o risco representado por dispositivos móveis.[6]

CRIPTOGRAFIA ✔

Se você tiver dados sigilosos armazenados em seus computadores, eles deverão estar criptografados para que não sejam utilizáveis no caso de serem perdidos ou roubados. É importante perceber que, como uma empresa, as informações que você detém são ativos altamente valiosos que precisam ser protegidos.

? O QUE SÃO PHISHING?

"Phishing" ocorre quando criminosos virtuais se passam por instituições confiáveis com a intenção de obter informações que possam ser utilizadas para fraudá-lo, como senhas e detalhes de cartões de crédito.

4 & 5 De acordo com a Kaspersky Lab
6 Global Corporate IT Security Risks Survey 2014

COMPREENSÃO DOS RISCOS

É MUITO FÁCIL FALAR SOBRE SEGURANÇA VIRTUAL, MAS, PARA A MAIORIA DE NÓS, ALGUMAS VEZES PODE SER DIFÍCIL COMPREENDER. COM CERTEZA, NINGUÉM DESEJA LIDAR COM A REALIDADE DESSES PROBLEMAS DA FORMA MAIS DIFÍCIL. ENTÃO, TENTAMOS FACILITAR ILUSTRANDO ALGUNS CENÁRIOS, SUAS CONSEQUÊNCIAS E COMO PODEM SER EVITADOS.

Um café bastante caro

Ao se despedir do último cliente do dia, Thomas deixa seu parceiro fechar o escritório. Há um café do outro lado da rua, onde ele irá encontrar um amigo. Ao se lembrar de que o pagamento a um de seus fornecedores vence amanhã, ele decide cuidar disso antes que esqueça.

Ele usa seu laptop para se conectar à rede WiFi do café, faz login no site do banco e realiza a transferência. Feliz por não ter se esquecido, ele relaxa e aproveita seu café.

Mais tarde, ao verificar sua conta, ela está vazia. Enquanto ele tenta saber o motivo disso, sua equipe está esperando o pagamento.

COMO ISSO ACONTECEU?

Infelizmente, ele não tinha nenhum tipo de antimalware instalado e foi infectado por um programa keylogger malicioso. Aqueles que executaram o programa receberam um registro de todas as informações inseridas. E, como ele utilizou um WiFi público não protegido, também houve o risco de que os dados da transação fossem interceptados.

O QUE ELE PODERIA TER FEITO?

O acesso a bancos deve ser realizado somente em dispositivos que possuam antimalware instalado, e sempre por meio de um navegador seguro. Com o recurso Safe Money da Kaspersky, Thomas poderia ter certeza de que a transação estava segura.

Observe que ele estava utilizando uma rede pública insegura. Por isso, os dados que ele estava transmitindo teriam sido bem mais facilmente interceptados do que se tivesse usado uma conexão privada. Mas, com um recurso como Safe Money instalado, ele poderia aproveitar a conveniência do acesso on-line ao banco sem precisar se preocupar.

Cada vez mais e-mails indesejados

Maria é psicóloga e, todas as manhãs, abre seu e-mail para verificar se a próxima sessão está confirmada. Na parte superior de sua caixa de entrada, ela encontra uma mensagem da rede social que utiliza solicitando a atualização de sua senha para uma mais forte. Ela clica no link fornecido, confirma sua senha existente (que é a mesma e substitui cada letra por um asterisco).

Feliz por sua conta agora estar mais difícil de acessar, ela retorna para sua caixa de entrada e logo se esquece de tudo...

...Até receber uma carta de chantagistas ameaçando publicar os detalhes de cada um dos clientes que estão vindo para terapia.

COMO ISSO ACONTECEU?

Maria foi vítima de um golpe de phishing. Embora o site fosse idêntico àquele que ela já acessou milhares de vezes, era apenas uma cópia falsificada. Após acessar os detalhes de seu perfil, também encontraram os detalhes de seus atendimentos. Tentaram utilizar a mesma senha que roubaram dela em seu e-mail de trabalho. Como ela o utilizou em ambas as contas, eles puderam ler todas as mensagens e arquivos em anexo, um deles com uma lista completa de seus clientes e seus detalhes de contato.

O QUE ELA PODERIA TER FEITO DE DIFERENTE?

Em primeiro lugar, ela deveria estar ciente de que sites e organizações legítimos não solicitam detalhes por e-mail. Após clicar no link, um bom software de segurança instalado teria alertado do fato de que o site era falso.

Seu outro erro foi utilizar a mesma senha para os contextos profissional e privado.

POR QUE ESCOLHER A KASPERSKY

É NOSSA MISSÃO PROPORCIONAR A PROTEÇÃO CONTRA AMEAÇAS VIRTUAIS MAIS EFICAZ, RESPONSIVA E EFICIENTE DO MUNDO. O KASPERSKY SMALL OFFICE SECURITY FOI PERSONALIZADO EM UMA SOLUÇÃO ESPECIALIZADA ÚTIL E ACESSÍVEL. ASSIM, VOCÊ PODE DAR ATENÇÃO AO QUE MAIS INTERESSA, CUIDAR DE SEUS NEGÓCIOS.

Compreendemos que, ao se tratar de segurança virtual, pequenos negócios estão em uma posição especial. Eles enfrentam as mesmas ameaças corporativas, mas compartilhando muitas das vulnerabilidades de usuários domésticos. Consideramos que essa posição diferenciada merece sua própria abordagem de segurança.

Não é adequado simplesmente reembalar um produto para o consumidor como solução para pequenos negócios. Por exemplo, não será oferecida proteção para servidores, mas muitos pequenos negócios possuem um ou logo terão. Diferentemente de usuários domésticos, negócios precisam proteger com facilidade múltiplos dispositivos.

No entanto, retirar funções de uma solução destinada a grandes corporações também não funciona. Pequenos negócios não possuem equipes de TI dedicadas, nem tempo para lidar com softwares complicados destinados a especialistas.

O Kaspersky Small Office Security foi concebido para ser abrangente sem ser complicado, o que resulta em tranquilidade sem drenar recursos com segurança. Ele não vai deixar os negócios mais lentos e irá cobrir uma ampla gama de dispositivos, protegendo você não importa onde estiver.

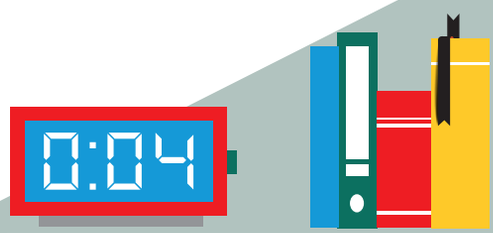
? MAS NÃO POSSO ME PROTEGER GRATUITAMENTE?

Embora soluções de segurança gratuitas estejam disponíveis, elas não conseguem oferecer uma solução abrangente. Na verdade, deliberadamente deixam espaço para melhorias. É assim que encorajam usuários a fazer upgrade para uma versão paga.

Quando seus negócios estão em jogo, você precisa da melhor proteção o tempo todo.

SOLUÇÃO

AGORA QUE IDENTIFICAMOS AS ÁREAS A SEREM CONSIDERADAS COMO PARTE DE SUA POLÍTICA DE SEGURANÇA, É HORA DE CONSIDERAR COMO IMPLEMENTAR SUA SOLUÇÃO PERSONALIZADA.



CERTIFIQUE-SE DE QUE ATUALIZAÇÕES OCORRAM REGULARMENTE

Com o Kaspersky Small Office Security, não é necessário se preocupar. Sua proteção será atualizada automaticamente em tempo real, mantendo-o protegido contra novas ameaças assim que aparecerem.

SENHAS FORTES OBRIGATÓRIAS

Facilite para seus funcionários com o Kaspersky Password Manager. Ele irá gerar automaticamente senhas fortes e armazená-las em um banco de dados criptografado. Dessa maneira, você precisará se lembrar somente de uma senha mestre e estará muito mais seguro.

CRIPTOGRAFIA E BACKUP DE DADOS CONFIDENCIAIS/ CRÍTICOS

Com o Kaspersky Small Office Security, é fácil armazenar suas informações críticas em caixas-fortes criptografadas. E, com a função de restauração, ainda que ocorra uma pane em seus computadores ou servidores, dados vitais não serão perdidos.

INCLUA TODOS OS SEUS DISPOSITIVOS

O Kaspersky Small Office Security oferece proteção para tablets e smartphones compatíveis. Se os dispositivos forem perdidos ou roubados, ele poderá ajudar a localizá-los e excluir remotamente quaisquer informações confidenciais.

BLOQUEIE MALFEITORES

Nosso recurso premiado Safe Money pode ser ativado com apenas alguns cliques, permitindo navegação supersegura. É possível prevenir instantaneamente as chances de violação ao verificar se os sites com os quais você interage não estão comprometidos. Enquanto isso, nossas funções antimalware, antispam e de firewall mantêm as portas fechadas a criminosos durante suas outras atividades on-line.

PROTEJA SUA EMPRESA AGORA.

Desenvolvido para atender às demandas específicas de empresas de menor porte, o Kaspersky Small Office Security combina proteção avançada com a facilidade de uso, essencial para empresas como a sua.

Acesse **kaspersky.com/protectmybusiness** e saiba como o Kaspersky Small Office Security pode proteger sua empresa.

PROTEJA SUA EMPRESA AGORA

PARTICIPE DA CONVERSA

#protectmybiz

Veja-nos no YouTube

Curta-nos no Facebook

Comente em nosso blog

Siga-nos no Twitter

Junte-se a nós no LinkedIn

Saiba mais em kaspersky.com/protectmybusiness

SOBRE A KASPERSKY LAB

A Kaspersky Lab é a maior fornecedora privada de soluções de proteção de endpoints do mundo. A empresa está classificada entre as quatro maiores fornecedoras de soluções de segurança do mundo para usuários de endpoints*. Há mais de 17 anos a Kaspersky Lab inova a segurança de TI e oferece soluções de segurança digital eficazes para grandes empresas, empresas de pequeno e médio porte e clientes. A Kaspersky Lab, com sua matriz registrada no Reino Unido, opera atualmente em quase 200 países e territórios no mundo todo, oferecendo proteção para mais de 400 milhões de usuários mundialmente. Saiba mais em www.kaspersky.com.

*A empresa ocupa o quarto lugar na classificação da IDC de Receita de segurança de endpoints global por fornecedor de 2013. A classificação foi publicada no relatório da IDC de "Previsão de 2014 a 2018 de segurança de endpoints global e participações de fornecedor de 2013 (IDC nº 250210, agosto de 2014). O relatório classificou fornecedores de software de acordo com lucros das vendas de soluções de segurança de endpoints em 2013.