

As 10 Melhores Dicas

para manter sua pequena empresa segura

Proteger sua empresa contra as últimas ameaças web está se tornando uma tarefa cada vez mais complicada. Ataques externos com consequências desastrosas, brechas na segurança interna e abusos da Internet fazem da segurança de dados uma das principais preocupações de pequenas empresas. Então, o que é preciso saber sobre segurança e quais são os principais elementos a ser enfrentados? A Trend Micro lança uma luz sobre esse assunto tão complicado.



1 FECHER AS PORTAS AO MALWARE

Você nunca deixaria a porta de sua casa destrancada à noite, então por que “convidar” criminosos a entrar na sua empresa? Ao deixar de proteger seus computadores, utilizar firewalls ou antivírus adequados, pode ser que você esteja fazendo exatamente isto.

De fato, a NACHA (associação de pagamentos eletrônicos) já alertou os usuários sobre o aumento dos ataques visando pequenas empresas. Segundo reportagem da *ComputerWorld*, “o alerta da NACHA informa que os criminosos digitais aparentemente estão visando pequenas empresas devido à relativa falta de procedimentos fortes de autenticação, de controles de transação e de capacidade de reportar ‘bandeiras vermelhas’”. Em alguns casos, informa o alerta, “os agressores induzem os funcionários de pequenas empresas a visitar sites de phishing com a mesma aparência e atmosfera da instituição financeira da empresa, no qual eles fazem o login usando suas credenciais”.

Malware é um software mal-intencionado planejado para se infiltrar e danificar um PC ou rede sem seu conhecimento ou consentimento. Siga estas dicas e feche as portas da sua empresa para o malware:

- **Ative o firewall.** Bons roteadores de Internet já vêm com firewall (não se esqueça de ativá-lo), entretanto, devido à complexidade dos malwares atuais, este dispositivo não é mais suficiente.
- **Proteja o PC.** O melhor software de segurança atuará além da proteção padrão e não prejudicará o desempenho de seu PC, laptop ou rede depois de instalado. As melhores soluções trazem proteção contra roubo de identidade, sites arriscados e ataques de hackers em um pacote único.
- **Defenda-se vendo.** Escolha uma solução que o ajude a supervisionar os usuários móveis e todos os seus PCs e servidores em uma única console.
- **Fique atento aos usuários móveis.** Uma boa solução de segurança se adapta ao local em que o usuário de encontra, alterando automaticamente as configurações de segurança nos laptops para um melhor nível de proteção quando os funcionários entram ou saem do escritório.
- **Limpe o e-mail.** O anti-spam reduz e-mails indesejados e bloqueia os riscos e distrações para os funcionários. Interrompa o spam bloqueando-o antes que ele chegue às máquinas de sua empresa.

2 ESCREVA SUA POLÍTICA

Você pensa que sua empresa é muito pequena e que os hackers não vão se interessar por ela? Pois pense melhor. O tamanho é irrelevante quando se trata de crimes e fraudes on-line, e as pequenas empresas são alvos mais fáceis, já que normalmente possuem infraestrutura de TI muito mais enxuta. Por isso, é importante que sua empresa leve a segurança a sério: treine constantemente seus funcionários para o cumprimento das suas exigências de segurança. Escreva-as. Informe-as. Fiscalize-as.

Sua política deve incluir algumas condutas, mas não deve se limitar a elas:

- **Saber o que ativar e o que desativar.** Quais programas podem ser executados nos computadores da empresa e quais são proibidos
- **Exigência de senhas fortes.** Veja a Dica 4 sobre senhas.
- **Reforço sobre as consequências.** O que acontece se a política não for seguida? Esteja ciente de que deverá cumprir sua palavra.
- **Uso. Sem abuso.** Qual é o uso apropriado do computador da empresa? Isso inclui o uso da Internet?
- **Educação sobre o uso do e-mail.** Isso inclui falar sobre comunicações internas e externas, explicando o que deve e o que não deve ser divulgado ou encaminhado.
- **Criptografia ou texto limpo.** Decida se é necessária uma solução de criptografia de e-mail para proteger a informação sigilosa, bem como quando usá-la.
- **Indique um “Fale com”.** Com quem seus funcionários podem conversar se tiverem dúvidas sobre a política ou a segurança dos computadores em geral?

3 ENFRENTAR AS MÍDIAS SOCIAIS ANTES QUE ELAS O ATROPELEM

As mídias sociais vieram para ficar, portanto, instrua seus funcionários nas melhores práticas e orientações. Seguem alguns meios que podem minimizar os riscos provocados pelas redes sociais:

- **Saiba quem está falando.** Decida quem pode falar em nome da empresa e só permita que os eventos internos ou externos relacionados à empresa sejam divulgados por esses funcionários.
- **Defina o que é confidencial.** Na sua política de segurança, inclua os sites de mídia social como Facebook, Twitter, LinkedIn e outros no acordo de não revelação de informações comerciais confidenciais.

- **Forneça orientações e um fórum para desenvolvê-las.** Blogar e postar em mídias sociais assuntos relativos à empresa são condutas que devem ser orientadas, sobretudo no que tange às informações que podem ser divulgadas ou não. As orientações precisam ir além da segurança:
 - Os blogueiros devem se identificar como funcionários ou contratados da empresa. Caso contrário, sua confiança poderá ser traída.
 - Defina o tom do blog.
 - Proteja as informações e a identidade dos clientes. Lembre os clientes de que não devem compartilhar informações pessoais em um post nem contribuir em questões que envolvam informações confidenciais.
 - Decida em que momento informações de apoio podem ser fornecidas em mídias sociais.
 - Envolve os executivos/prorietários de modo que as orientações sejam adaptadas com rapidez, tendo em vista as necessidades comerciais.
 - Use recursos como o BlogWell (www.blogwell.com) para desenvolver suas orientações e conhecer melhor as mídias sociais.
- **Seja sociável, mas seja esperto.**
 - Você deve publicar somente informações que podem ser disseminadas abertamente, sem que isso cause constrangimentos.
 - Presuma o pior para obter o melhor resultado. Estimule os funcionários a controlar a quantidade de informações pessoais compartilhadas on-line para a sua própria proteção e da empresa.
 - Adicione à sua lista de contatos apenas as pessoas em quem você confia.
 - Evite clicar em links enviados por pessoas que você não conhece.
 - Nunca confie totalmente em alguém que você não conheça bem.

4 PROTEJA-SE COM SENHAS

Gostando ou não, as senhas são a chave de acesso para a maioria das redes de pequenas empresas. Não é preciso ser um “mago das estatísticas” para saber que quanto mais caracteres são usados, mais forte será a senha.

- **Senhas fortes.** Exija senhas fortes, com no mínimo 8 caracteres e que incluam números, para conseguir bloquear os ataques simples que tentam adivinhar senhas.
- **Mude-as constantemente.** Caduque senhas depois de algum tempo, exigindo que sejam mudadas com frequência.
- **Mantenha-as a salvo.** Ensine seus funcionários que anotar as senhas, guardá-las no celular ou usar senhas óbvias coloca a segurança da empresa em risco.
- **Misture os caracteres.** Para criar senhas mais fortes, não use qualquer palavra. Escolha letras, números e caracteres especiais aleatoriamente. Confira no seu teclado como qWe4%6yUi é muito mais forte do que FlAFlu#3.

5 TENHA UM OLHAR CRÍTICO SOBRE A SEGURANÇA NA INTERNET

A Internet é fantástica para agilizar negócios. Entretanto, ela também aumenta a exposição a malwares caso sua solução de segurança não forneça uma verificação proativa do conteúdo que rastreie a ameaça e alerte sobre os possíveis problemas. Selecione as soluções de segurança que o ajudam a superar as mais recentes ameaças com o mínimo de distrações aos usuários.

- **Bloqueie os links estranhos.** Não são os funcionários que devem se preocupar com a segurança. Determine quando e quais sites acessar restringindo-os. Atualizações automáticas são recomendadas, bem como tornar a segurança transparente para os funcionários.
- **Mantenha a web produtiva.** Junto com as orientações sobre o uso aceitável da web, selecione soluções que impeçam o uso inadequado da rede. A filtragem de URL pode limitar completamente o acesso a sites improdutivos durante o trabalho e evita a disseminação de links arriscados que colocariam sua empresa, seus funcionários e seus dados nas mãos de ladrões de dados ou de identidade.

6 PEÇA AJUDA AOS FUNCIONÁRIOS

Todos já viram manchetes sobre as consequências da exposição de dados sigilosos, mas poucos sabem que 80% das perdas de dados são causadas por erro humano - seja por enviar informação confidencial ou sigilosa à pessoa errada ou por agir de maneira desorientada.

- **Acate ou “morra”.** Bem, talvez morrer seja um exagero, porém, as sanções impostas pela perda de dados ou vazamentos acidentais estão se tornando mais rígidas com as crescentes regulamentações. Por isso, informe os funcionários sobre as exigências normativas e as melhores práticas para proteger as informações. Explique a eles os riscos de não seguir as normas. Deixe-os a par de que é função deles manter a vigilância para reduzir os riscos.
- **Explique aos funcionários por que eles são importantes.** Se os funcionários não completarem a verificação do antivírus ou enviarem materiais inapropriados, a empresa fica suscetível a malwares, processos e danos à sua reputação.
- **Mantenha o sigilo.** Informe todos os funcionários sobre quais informações são sigilosas e sobre os possíveis problemas que podem acontecer caso esses dados sejam divulgados.

7 FAÇA SUA RELAÇÃO COM SEU REVENDEDOR/CONSULTOR TRABALHAR POR VOCÊ

Ter um bom relacionamento com o revendedor / consultor de TI significa ter sempre um conselheiro confiável a quem recorrer quando houver um problema com TI.

- **Pergunte mais.** Em vez de apenas dar descontos ou oferecer uma promoção, o revendedor ou consultor com quem você trabalha precisa ser capaz de aconselhá-lo imparcialmente sobre sua infraestrutura de TI. Ele pode e deve ajudá-lo a escolher uma solução adequada para seu negócio que se adapte e acompanhe suas necessidades, além de proteger seus investimentos em TI. Se ele não puder orientá-lo, mude de revendedor.
- **Gerenciamento terceirizado.** Seu revendedor ou consultor deve oferecer também o gerenciamento remoto da solução de segurança para você - o que significa menos aborrecimentos e até mesmo maior proteção para você e sua empresa. Explique que a segurança é uma tarefa importante que deve ser realizada por cada funcionário.

8 DÊ O EXEMPLO

Se você não liderar o caminho, ninguém o seguirá. Mesmo que não esteja especificamente liderando, as pessoas observam as demais e estarão atentas, portanto, à sua conduta. Basta uma pessoa para fazer a diferença.

- **Não seja aquele que causa problemas.** Somente é preciso uma pessoa para disseminar um vírus malicioso por toda a empresa.
- **Seja um defensor.** Se descobrir um modo de proteger melhor a rede ou se ficou sabendo de uma ameaça iminente, informe os outros. Compartilhe as melhores práticas com todos os departamentos.

9 MANTENHA-SE ATUALIZADO

Certifique-se de que seus usuários móveis, de PCs e de servidores têm conhecimento das melhores informações disponíveis sobre as ameaças. Atualizações manuais e esporádicas dos softwares de segurança abrem as portas às ameaças. O clichê continua valendo: você está tão seguro quanto sua última atualização.

- **Libere os PCs.** Se sua solução de segurança está tornando seus PCs mais lentos, você não está sozinho. Essa é uma queixa frequente relativa às soluções convencionais de segurança. Procure soluções que fazem o data center do fornecedor trabalhar quando usar seus recursos hospedados. Concentre o potencial de seus PCs e servidores no processamento relacionado às atividades comerciais de sua empresa, não na segurança.
- **Não confie nos antivírus antigos.** A proteção tradicional antivírus percebe as ameaças comparando os arquivos com suas bases de dados de impressões digitais ou "assinaturas" em cada computador. Entretanto, as novas ameaças estão se multiplicando exponencialmente - em taxas acima de 2.000% desde 2004 - por isso, enviar mais arquivos de assinaturas simplesmente sobrecarrega seus PCs. Novos métodos de detecção agem como as verificações de fundo nos remetentes de e-mail, arquivos e sites, protegendo melhor e mais rapidamente seus PCs sem comprometer seu desempenho.
- **Atualizações automáticas do sistema operacional.** Simplifique a ação ao máximo para que seus PCs tenham sempre as últimas correções. As vulnerabilidades no seu sistema operacional são o principal ponto de ataque. O melhor é aplicar os patches rápida e automaticamente.
- **Exija e verifique a aplicação de patches.** Informe aos usuários quais versões do software eles precisam ter e como verificar quais eles possuem. Forneça links e instruções sobre como atualizar o computador para a versão correta. Se os usuários perceberem que você trata seriamente o assunto e deseja manter a conformidade, é muito mais provável que eles tentem mantê-la.

10 ESCOLHA UM PARCEIRO DE SEGURANÇA, NÃO APENAS UM FORNECEDOR

Selecione um fornecedor que entenda as necessidades específicas da segurança em um ambiente de pequena empresa.

- **Escolha um fornecedor específico de segurança.** Verifique se seu fornecedor considera a segurança a principal atividade de seu negócio ou somente parte de seu portfólio.
- **Verifique seu passado.** Fornecedores com anos de experiência comprovada na defesa contra múltiplas ameaças e com conhecimento e vivência tanto em pequenas quanto grandes empresas podem dar um maior suporte para sua proteção.

RECURSOS

O TrendWatch oferece vídeos, informativos e outros recursos educacionais. Acesse <http://us.trendmicro.com/us/trendwatch/>

DEFINA OS PRÓXIMOS PASSOS

Use a lista abaixo para ver em que pontos sua empresa está indo bem. Então, determine quais medidas você precisa tomar.

DICA	MARQUE AS AÇÕES TOTALMENTE COMPLETADAS
1. Feche as portas a malwares	<input type="checkbox"/> Instale e use segurança com proteção contra múltiplas ameaças (vírus, ameaças web, spyware, bots, etc.) <input type="checkbox"/> Selecione uma solução que permita visualizar e gerenciar PCs e servidores remotos e locais <input type="checkbox"/> Saiba o que está protegido escolhendo uma solução com uma console única para usuários remotos, PCs internos, servidores de arquivos e e-mails. <input type="checkbox"/> Fique atento aos usuários móveis, selecionando soluções que se adaptem ao local em que eles estão <input type="checkbox"/> Limpe os e-mails com anti-spam
2. Escreva sua política	<input type="checkbox"/> Determine sua política por escrito (Isso é importante!) <input type="checkbox"/> Informe os funcionários e lide com a política de segurança de TI com a mesma seriedade que lida com um contrato <input type="checkbox"/> Reforce as consequências pelo não cumprimento das políticas <input type="checkbox"/> Defina o que os funcionários podem ou não fazer nos PCs da empresa <input type="checkbox"/> Eduque-os nas melhores práticas de e-mail para evitar phishing, spam <input type="checkbox"/> Criptografe os e-mails caso precise proteger o conteúdo <input type="checkbox"/> Designe um "Falar com" ou um contato fixo para a segurança de TI
3. Encare as mídias sociais como uma realidade	<input type="checkbox"/> Defina quem pode blogar publicamente sobre a empresa <input type="checkbox"/> Defina o que é confidencial e o que é legítimo <input type="checkbox"/> Forneça orientações e um fórum que as debaterá <input type="checkbox"/> Seja sociável, mas atento às informações publicadas por você e seus funcionários
4. Verifique as senhas	<input type="checkbox"/> Exija senhas fortes <input type="checkbox"/> Caduque as senhas antigas dos usuários <input type="checkbox"/> Mantenha as senhas protegidas, não as guarde num bilhete ou no celular <input type="checkbox"/> Combine letras e números para evitar que as senhas sejam descobertas
5. Seja crítico sobre a segurança na Internet	<input type="checkbox"/> O local é importante, por isso, facilite a proteção dos funcionários remotos com soluções que se adaptam ao local <input type="checkbox"/> Use proteção automática para bloquear os links arriscados e sites improdutos
6. Tenha a ajuda dos funcionários	<input type="checkbox"/> Cumpra as regras e as boas práticas de segurança <input type="checkbox"/> Explique por que os funcionários são importantes para a segurança <input type="checkbox"/> Implemente políticas de segurança <input type="checkbox"/> Reforce sempre o que é confidencial
7. Obtenha ajuda do revendedor / consultor	<input type="checkbox"/> Pergunte coisas além do mero atendimento padrão; encontre um parceiro comercial que possa ser um conselheiro confiável <input type="checkbox"/> Terceirize o gerenciamento da segurança para seu revendedor / consultor e poupe tempo e energia, recursos valiosos para seus negócios
8. Lidere dando o exemplo	<input type="checkbox"/> Uma só pessoa pode ser cabeça, por isso, verifique suas ações em relação à política <input type="checkbox"/> Encontre um recurso confiável para a informação sobre segurança e o use uma vez por semana
9. Mantenha-se atualizado	<input type="checkbox"/> Libere seu PC escolhendo uma solução que ofereça processamento de data center hospedado <input type="checkbox"/> Não confie em antivírus antigos; tenha múltiplos processos de detecção <input type="checkbox"/> Automatize as atualizações do sistema operacional <input type="checkbox"/> Exija e verifique a aplicação de patches
10. Escolha um fornecedor de segurança	<input type="checkbox"/> Selecione um fornecedor focado na segurança <input type="checkbox"/> Verifique o histórico do fornecedor escolhendo uma empresa estabelecida que tenha experiência com pequenas e grandes empresas

Para mais informações, entre em contato com o **Canal Direto** pelo telefone 4003-2129, pelo e-mail canaldireto@trendmicro.com ou pelo Portal para Canais: <http://smb.trendmicro.com.br>