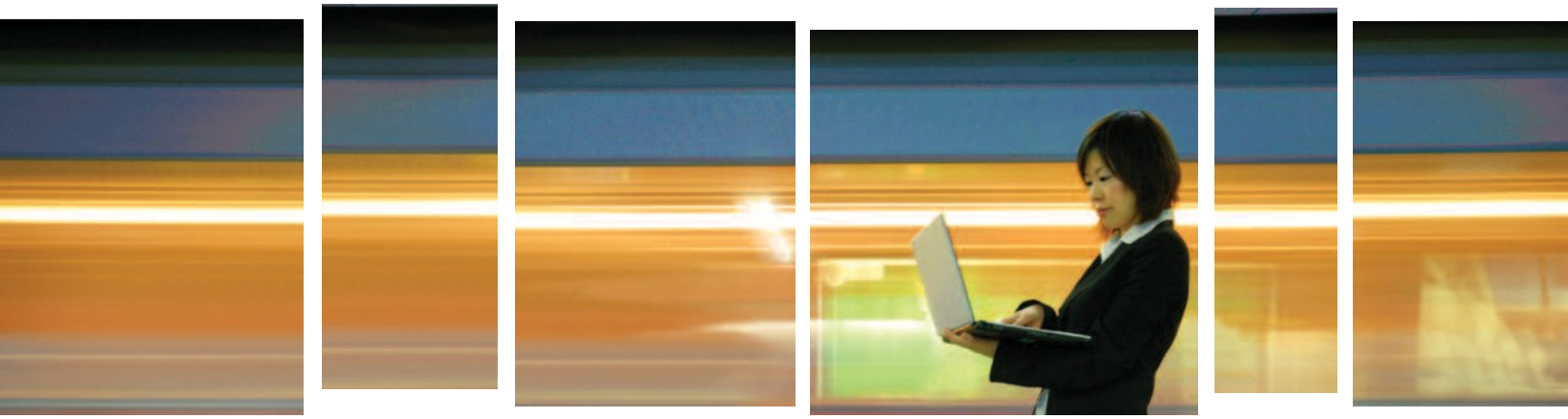
InformationWeek
marketing services

INFORME OFICIAL DA UBM
FEVEREIRO DE 2010

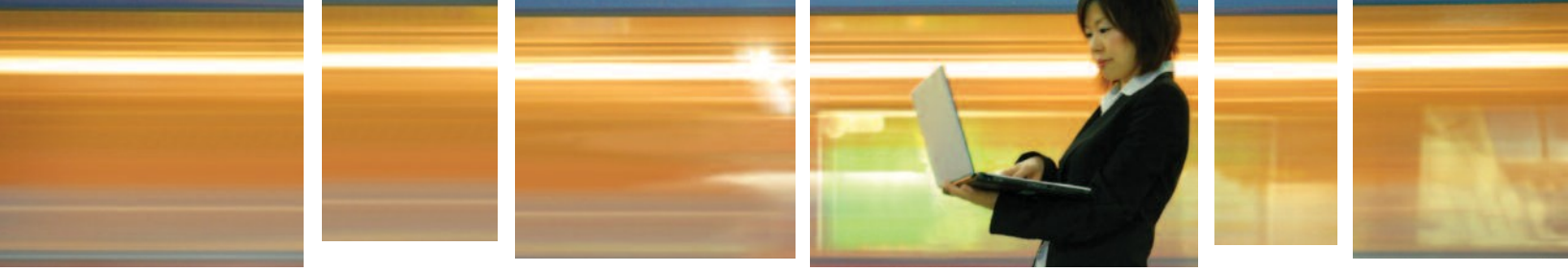


Proteção de dados em movimento

Quatro coisas que todas as empresas devem saber sobre como proteger dados essenciais em plataformas de computação móvel

Patrocinado por:

DELL



Proteção de dados em movimento

Quatro coisas que todas as empresas (pequenas, médias ou grandes) devem saber sobre como proteger dados essenciais em plataformas de computação móvel

Curtis Franklin, Jr.

O desafio: uma força de trabalho móvel

O vasto mundo fora dos limites do firewall de proteção representa uma ameaça crescente à segurança de informações confidenciais da sua empresa. Com todos (de CEOs a carpinteiros) levando consigo as redes da empresa para as instalações dos clientes, uma quantidade cada vez maior de negócios ocorre nesse mundo.

Os dados contidos em dispositivos móveis ou que possam ser acessados através deles são muito mais valiosos para a empresa do que o notebook, o smartphone ou qualquer outro dispositivo móvel que os transporte. Por essa razão, toda empresa deve desenvolver uma estratégia de proteção a informações que leve em consideração cenários móveis.

Para as pequenas e médias empresas, o desafio é ainda maior: equipe e conhecimento limitados as tornam particularmente vulneráveis a adversários sofisticados que olham além do óbvio (grandes bancos, por exemplo) para empresas que percebem serem alvos mais fáceis. Este documento explora a natureza dos problemas de segurança que acompanham dispositivos de computação altamente móveis e os elementos essenciais para as soluções desses problemas.

Definir as ameaças

Os principais riscos de informações móveis são provenientes de três tipos de violações de dados: perda, vazamento e roubo.

Perda de dados: é a liberação acidental de informações sigilosas por meio da perda do dispositivo em que residem os dados.

Vazamento de dados: é a liberação intencional de informações sigilosas, embora não autorizada, por meio das ações de um funcionário, prestador de serviços ou executivo com informações privilegiadas.

Roubo de dados: é a obtenção de informações sigilosas por uma pessoa não autorizada que não faz parte da organização.

Em conjunto, estas três categorias de liberação de dados representam um enorme risco intelectual e financeiro para a organização. As estimativas do impacto econômico representado pela liberação de dados variam de US$ 85 a US$ 200 por registro e, como muitos incidentes envolvem centenas ou milhares de registros, o custo pode rapidamente se tornar astronômico.

Qualquer solução eficaz de segurança de informações móveis deve envolver os quatro elementos aqui descritos.

1. Tecnologias e políticas de controle de acesso

Proteger uma empresa contra liberação não autorizada de dados requer a coordenação de respostas em torno de quatro áreas de atividade: as pessoas, as políticas, os processos da empresa e a tecnologia utilizada para implementar esses processos e políticas.

Embora a tecnologia tenda a atrair a maior parte das atenções da imprensa, há uma razão para vir no final da lista: para ser eficaz, a tecnologia tem que implementar procedimentos e políticas viáveis e deve ser usada por pessoas que entendam a importância da segurança de informações e as consequências de falhas na segurança.

A segurança começa com o controle de acesso. Não se pode começar a tratar da liberação não autorizada de dados enquanto a empresa não tiver definido quem está autorizado a ter acesso a dados e o que essa pessoa tem autorização para fazer com os dados aos quais tenha acesso. A peça mais importante do quebra-cabeças em que consiste o controle de acesso é decidir quem deve ter acesso a quais dados. Embora possa parecer uma fonte de trabalho indesejável e desnecessário, descobrir quais classificações de trabalho conseguirão ver e usar determinados tipos de dados é algo que pode ser trabalhado até na menor empresa e ajustado conforme necessário à medida que a empresa cresce.

As alterações em termos de pessoal e crescimento na empresa são

SOBRE O AUTOR

Curtis Franklin, Jr. é um jornalista de tecnologia com mais de vinte anos de experiência cobrindo os setores de comunicações, rede e computador. Ele escreveu sobre vários tópicos, com especial ênfase em problemas de rede empresarial, mobilidade e segurança.

responsáveis pelo aspecto mais negligenciado do controle de acesso: a revisão do controle quando mudam as classificações de trabalho ou as atribuições individuais. Muitos incidentes de liberação de dados são agravados porque a conta ou o sistema individual através do qual ocorre a perda carrega os privilégios cumulativos de cada cargo que o indivíduo teve na organização, em vez dos privilégios

Suponha que indivíduos não autorizados obtenham acesso aos dados em algum momento. O problema é assegurar que os dados não possam ser reconhecidos ou utilizados por qualquer pessoa que não esteja autorizada a usá-los.

limitados ao cargo atual. Assegurar que os privilégios de processo e acesso a dados sejam revistos toda vez que um indivíduo mudar de cargo pode resolver muitos problemas de segurança antes que eles virem uma bola de neve.

Depois que as políticas apropriadas estiverem em vigor, é uma questão de tecnologia assegurar que um indivíduo que utilize um dispositivo tenha autorização para usá-lo. O controle de acesso tende a ser mencionado em termos de "fatores", sendo a autenticação de dois fatores considerada um equilíbrio adequado entre a segurança e a conveniência do usuário. Na maioria dos casos, os dois fatores são algo que o usuário possui – um sistema, um token de segurança ou uma impressão digital, por exemplo – e algo que o usuário sabe, normalmente uma senha ou um PIN. Uma vez apresentados esses fatores, pressupõe-se que a identidade do usuário é original e que o acesso pode ser concedido.

Com base em uma senha e uma leitura de impressão digital ou de Smart Card, opções como o iCLASS e o naviGo da HID Global fazem uso de recursos de autenticação de pré-boot presentes em notebooks da Dell e de outros fabricantes para autenticar o usuário antes que o sistema operacional (SO) seja ativado, garantindo que soluções alternativas de senha do SO não possam ser usadas para acesso ilícito.

Um dos principais problemas no controle de acesso atualmente é a questão da "federação de identidades" ou "logon único", em que as identidades dos usuários são estabelecidas quando eles fazem login no notebook ou smartphone e depois são aceitas pelos aplicativos e redes que eles utilizam, sem nenhuma verificação adicional. As empresas individuais devem decidir se os mecanismos de controle de acesso disponíveis nos dispositivos portáteis são seguros e confiáveis o suficiente para permitir que funcionem como supervisores para a rede empresarial. Os mecanismos de autenticação forte estão disponíveis em muitos dispositivos de vários fornecedores (como o RSA, com seu sistema de token SecureID) e podem ser suficientes para que as empresas individuais confiem na segurança básica.

2. Criptografia

Embora deva existir um nível razoável de confiança entre uma organização e seus funcionários, é essencial supor que alguns indivíduos não autorizados podem conseguir obter acesso aos dados em algum momento da vida útil deles. O problema da segurança é assegurar que os dados não possam ser reconhecidos ou utilizados por qualquer pessoa que não esteja autorizada a usá-los.

Impedir que os dados se tornem úteis para usuários não autorizados é função da criptografia. Compreender como e quando usar a criptografia é importante para qualquer pessoa que tente formular uma estratégia de segurança abrangente para uma organização. Para aqueles que trabalham em setores ou locais em que vigoram regulamentações como HIPAA ou Massachusetts 201 CMR 17.00, a criptografia é muito mais que uma opção para proteção de dados. Ela pode ser vista como uma tecnologia à prova de falhas obrigatória em caso de roubo ou perda de dispositivo. Em qualquer um desses casos, é realmente importante saber as diferenças entre os dois principais tipos de criptografia de dados usados na computação: no local e em trânsito.

A criptografia de dados no local envolve a criptografia segura do sistema de armazenamento de um dispositivo móvel, total ou parcialmente. Criptografia de disco inteiro significa criptografar cada arquivo de dados no dispositivo da forma como está armazenado e descriptografá-lo conforme necessário para uso ou modificação. A descriptografia de disco inteiro tem a vantagem de ser segura e simples para o usuário. Além disso, não é necessário lembrar qual parte do disco foi criptografada ou como criptografar arquivos individuais. A desvantagem da criptografia de disco inteiro é o desempenho, pois todo arquivo está sujeito ao processamento adicional necessário para criptografia e descriptografia. Em termos de segurança, a criptografia de disco inteiro não pode garantir que nenhum dado, por mais inofensivo que pareça, possa ser usado por um indivíduo não autorizado que obtenha acesso ao dispositivo. Com a criptografia de arquivos ou diretórios individuais, existe a possibilidade de que um usuário armazene arquivos em diretório errado, esqueça de criptografar um arquivo ou cometa outro erro que deixe os dados vulneráveis.

Existem vários pacotes de terceiros de empresas como Wave Systems, PGP, Sophos, GuardianEdge e Credant que criptografam arquivos em um diretório ou por disco inteiro. Tanto o Windows 7 como o Macintosh OS X Snow Leopard oferecem esse recurso. Smartphones geralmente não vêm com a criptografia de dispositivo integrada ao sistema operacional, mas produtos de empresas como PGP, Navastream e GuardianEdge podem ser aplicados a alguns modelos de smartphone para proteger os dados no local no dispositivo.

Com os dados protegidos no local, pode-se considerar o caso mais comum de proteção de dados durante a transferência de um sistema para outro.

As redes virtuais privadas (VPNs) são, de longe, o mecanismo mais comum para criptografar dados em trânsito. Sejam elas abertas por um serviço baseado na Web de SSL (camada de soquete seguro) ou usando um programa separado que cria um túnel IPSec (Segurança de protocolo na Internet) usando um protocolo PPTP (Protocolo de criação de túnel ponto a ponto) ou L2TP (Protocolo de criação de túnel da camada 2), as VPNs criptografam de forma segura todos os dados transferidos entre os dois sistemas ou redes conectados por túneis. Em geral, cada conexão VPN envolve um par de encapsulamentos, e cada encapsulamento permite que os dados fluam em uma direção.

O ponto mais vulnerável na vida de qualquer VPN é o processo de autenticação no início da transação. Se os protocolos não forem tratados corretamente, a credencial de login inicial poderá ser enviada sem estar criptografada e estar sujeita a roubo por um indivíduo que esteja bisbilhotando. Vários tipos de encapsulamento ou protocolos empilhados podem ajudar a proteger contra as formas mais básicas de roubo de informações de login no início do encapsulamento.

A criptografia pode proteger contra uma série de esquemas de roubo de dados, mas, em última análise, os dados devem ser descriptografados para serem exibidos ou processados. Ataques avançados de rede e ponto de extremidade podem detectar e roubar dados nesse ponto vulnerável.

A proteção de sistemas contra código mal-intencionado já foi considerada o principal meio para preservar dados de um computador. Atualmente, o software antivírus é apenas um dos aplicativos essenciais de segurança para sistemas móveis.

Parar esses ataques é um trabalho que tem sido atribuído ao software de proteção, embora haja um debate crescente sobre a eficácia de qualquer software em parar os ataques atuais mais sofisticados.

3. Software de proteção

Antigamente, a proteção de sistemas contra códigos de vírus mal-intencionados era considerada o principal meio para preservar dados de um computador. Atualmente, o software antivírus é apenas um dos aplicativos de segurança considerados essenciais para proteger um sistema móvel. O software de proteção contra spam e adware é importante, pois é um firewall e um sistema de detecção de invasões. Para muitas organizações, o software para proteger contra ameaças introduzidas pela Web é importante, já que são filtros para o tráfego de entrada e de saída sinalizados como mal-intencionados.

Cada um pode ser implementado separadamente ou eles podem ser agrupados em um gerenciador universal de ameaças (UTM) capaz de combinar vários mecanismos de proteção em um único pacote que tenta aproveitar os diversos mecanismos para uma defesa mais abrangente.

Como vírus, worms, Cavalos de Troia e similares tendem a ser específicos do sistema em sua operação, o software de proteção contra eles precisa ser assim também. Alguns sistemas operacionais, principalmente o Microsoft Windows, têm sido altamente visados por criadores de vírus devido ao grande número de computadores baseados em Windows no mercado. Como resposta, a Microsoft incorporou software antimalware ao Windows 7 e muitas empresas (como Norton, Symantec, CA, F-secure e AVG) disponibilizaram software de terceiros. Essa ênfase mal-intencionada em computadores Windows levou alguns defensores de outros sistemas a alegarem que nenhum software antimalware é necessário. Embora o número de ameaças a computadores baseados em Linux e Macintosh não seja tão alto quanto a máquinas Windows, é uma enorme ingenuidade supor que nenhuma proteção seja necessária.

Worms e vírus de prova de conceito foram liberados para computadores Macintosh e Linux, bem como para smartphones BlackBerry, Palm e Qualcomm. Embora poucos vírus tenham aparecido "na natureza" tendo smartphones como alvo, diversas empresas (como F-secure, Norton, Kaspersky e avast!) disponibilizaram software antivírus para vários telefones. Dependendo da impopularidade relativa, proteger um sistema é um ponto de vista a curto prazo, que pode ter consequências negativas imediatas.

O alvo dos pacotes antimalware são programas de software não autorizados que tentam se tornar residentes em um computador. Os firewalls, por outro lado, se concentram em bloquear o acesso ao computador por meio de portas de rede que possam ter ficado abertas inadvertidamente para o exterior ou que sejam necessárias para a utilização normal do computador, mas foram alvo de acesso não autorizado. Tanto a Microsoft como a Apple incluem a funcionalidade de firewall em seus sistemas operacionais. Há firewalls de computador móvel disponibilizados por muitos fornecedores, como Norton, Symantec, ZoneAlarm e Comodo.

Firewalls de smartphone são muito menos comuns, mas estão começando a ser disponibilizados por empresas como Norton, McAfee e Trend Micro. Os firewalls são complementados por sistemas de detecção de invasões (IDS) que mantêm a vigilância sobre padrões de tráfego e conversas de transferência de dados que ocorrem em um sistema. Como o nome indica, muitos IDSs simplesmente notificarão um usuário ou administrador de que um padrão suspeito de transferência de dados está ocorrendo, deixando a atenuação da ameaça para o usuário ou outro aplicativo.

Outros agirão de forma proativa contra conversas suspeitas, encerrando conexões de rede ou limitando a largura de banda para retardar ou interromper atividades mal-intencionadas suspeitas.

Tudo isso parece ser complicado e consumir muitos recursos – e é isso mesmo. Essas descrições explicam por que tantas empresas e indivíduos implantam apenas alguns dos aplicativos de proteção listados acima e por que um número surpreendente de organizações sente que a proteção não é nem um pouco necessária.

A necessidade de software de proteção não é questionada pela maioria dos especialistas em segurança, embora sua eficácia na defesa contra ataques sofisticados o seja. É realmente uma questão de sincronização de horários: se os engenheiros que desenvolvem a assinatura de código e os padrões comportamentais para o software de defesa conseguirem se antecipar aos criminosos que concebem formas de superar esse mesmo software. No passado, os dois estiveram em fileira cerrada, em grande parte devido aos esforços de pesquisadores de segurança independentes que descobriam problemas e informavam primeiro aos fornecedores, dando a eles algum tempo para desenvolver e liberar um patch antes de compartilhar detalhes da vulnerabilidade com o resto do mundo. Hoje em dia, porém, um pequeno mas importante número de pesquisadores afirma que os fornecedores não trataram suas informações com seriedade, por isso começaram a liberar detalhes de vulnerabilidades para o mundo quase que imediatamente, esperando pressionar os fornecedores a resolver problemas de patch rapidamente.

O resultado é que, embora um pacote de software de proteção continue sendo fundamental para computadores móveis, já não é mais suficiente. No ambiente moderno, o software de proteção é importante porque remove o "ruído de segurança" da combinação, assegurando que as investigações e os ataques muito básicos (e bastante numerosos) sejam interrompidos para que especialistas em segurança possam se concentrar em políticas e vigilância nos ataques modernos mais sofisticados. Criptografia adequada, autenticação segura, processos elaborados e backups eficazes são tão importantes quanto o software mais conhecido para a segurança geral móvel.

4. Backup

De muitas maneiras, o backup é o elemento esquecido da segurança de dados móveis. Ele é ignorado com frequência para notebooks e netbooks e geralmente não é sequer considerado para smartphones. Isso pode ser um erro crítico quando surgem problemas que exigem a regeneração completa do ambiente operacional no dispositivo, um passo que muitas vezes é necessário para erradicar totalmente as mais sofisticadas explorações de segurança.

Na verdade, fazer backup de computadores móveis nunca foi tão fácil, com os aplicativos de backup agora incorporados a computadores com Windows 7 e Macintosh, aplicativos de terceiros disponibilizados por inúmeras fontes e um host de serviços de backup de baixo custo baseados em nuvem, disponíveis tanto para grandes e pequenas empresas como para indivíduos.

Até para smartphones está havendo crescimento em termos de opções de backup. O backup é incorporado à rotina de sincronização do iPhone; produtos como Sprite Mobile, PIM Backup e SPB Backup 2 estão disponíveis para smartphones com Windows Mobile, e o DataPilot (entre outros) tem software de backup que é executado em uma ampla variedade de smartphones de vários fornecedores. Falta de software já não é uma desculpa razoável para não fazer backup de qualquer dispositivo móvel.

Onde obter proteção

Com todas as opções de proteção e a necessidade de garantir que diferentes pacotes trabalhem em conjunto, a integração de software de segurança ganhou importância. Os integradores de sistemas e os fornecedores de hardware agora desempenham um papel crítico, garantindo que todo software que resida.

O PAPEL DA DELL NA SEGURANÇA DE INFORMAÇÕES MÓVEIS

A Dell cria a proteção a sistemas e dados em seus sistemas com base em uma filosofia fundamentada em quatro pilares: proteger o sistema e os dados, ao mesmo tempo impedindo o acesso não autorizado e ataques mal-intencionados. O Gerenciador de segurança do Dell ControlPoint permite que alguém configurando um notebook ative, configure e verifique o status de software de parceiros como RSA e HID Global para controle de acesso, Wave Systems para criptografia de disco total e software da Norton ou da Symantec para proteção contra malware. Além disso, o Sistema de rastreamento e recuperação de notebook do Dell ProSupport ajudará a localizar e recuperar notebooks que possam ser perdidos ou roubados. Cada um desses recursos pode ser encomendado com todos os notebooks Dell Latitude e Optiplex através das Soluções de negócios da Dell. A disponibilidade desses recursos varia de acordo com cada país.

em uma plataforma seja capaz de trabalhar em conjunto de forma confiável e que a configuração inicial permita a implementação correta de políticas de segurança do cliente.

Toda a segurança, seja em dispositivos móveis ou computadores mainframe, deve equilibrar a facilidade de uso com a proteção de dados.

Um número crescente de clientes tem procurado os fornecedores de sistemas em busca de instalação completa de software de segurança, preferindo a facilidade de um único ponto de contato em detrimento da (possível) flexibilidade de desenvolver internamente sua infraestrutura de segurança. Isso vale principalmente para dispositivos altamente móveis, para os quais manutenção e suporte remotos provavelmente serão regra, e não a exceção. A Dell, por exemplo, combina recursos internos (como o chip de segurança dedicado ControlVault, leitor de impressão digital incorporado e autenticação de pré-boot) com software pré-carregado de parceiros como RSA, Wave Systems, Seagate e HID Global para apresentar uma frente de segurança unificada que pode ser administrada através do Gerenciador de segurança do Dell ControlPoint.

Um ponto único de resposta, seja a consulta do usuário ou do suporte, tornará o complexo tópico de segurança móvel muito mais fácil de dar suporte com urgência.

A proteção deve ser usada para trabalho

O aumento no uso de dispositivos móveis se deve, em grande parte, à importância cada vez maior atribuída à conveniência do sistema e à eficácia do usuário. Toda a segurança, seja em dispositivos móveis ou computadores mainframe, deve equilibrar a facilidade de uso com a proteção de dados. Em dispositivos móveis, o equilíbrio será mais crucial por causa da natureza dos dispositivos. Um dispositivo móvel que fique inconveniente será abandonado em favor de outro sistema (possivelmente menos seguro) ou verá seu sistema de segurança subvertido por um usuário que valoriza a conveniência mais do que a equipe de TI.

Educar os usuários móveis sobre a importância da segurança, desenvolvendo políticas e procedimentos bem fundamentados para proteger o uso de sistemas e dados e implantando a tecnologia adequada para implementar as políticas sólidas, ajudará a garantir que os dados corporativos não se percam, independentemente da distância dos dispositivos nos quais eles residem. ★