CONTEÚDO FORNECIDO POR

Redmond
THE INDEPENDENT VOICE OF THE MICROSOFT IT COMMUNITY

PATROCINADO POR

Quest™

Windows 10: um mundo completamente novo para as equipes de TI

O mundo que a equipe de TI conhecia como Windows 7 é coisa do passado. Com o Windows 10, a Microsoft está modificando a forma como são feitas todas as atualizações, da segurança à conectividade. Todos os artigos deste relatório especial da Redmond indicam que o Patch Tuesday nunca mais será o mesmo.

1105 MEDIA

A Microsoft sugere que os profissionais de TI adaptem o processo de atualização do Windows 10

POR KURT MACKIE

A Microsoft reiterou sua mensagem de "adaptação ou morte" para os profissionais de TI responsáveis por manter os servidores e clientes do Windows atualizados e corrigidos.

Seu anúncio mais recente está reforçando essa mensagem pela segunda vez. No verão passado, a empresa avisou que seu sistema de fornecimento de atualizações de software passaria a usar o modelo de serviços do Windows 10 para a maioria de seus clientes com suporte e sistemas operacionais de servidor a partir de outubro. Com o modelo do

Windows 10, as atualizações ocorrem mensalmente e são "cumulativas", o que significa que contêm todas as atualizações, desde o lançamento da "última linha de base" do sistema operacional.

Essa mudança de modelo de atualização do Windows 10 entrou em vigor em outubro para os clientes do Windows 7/8.1, assim como para as versões do Windows Server 2008 R2 e Windows Server 2012/R2. Isso também será aplicado no Windows Server 2016.

Os dois anúncios da Microsoft sinalizam o fim das práticas tradicionais de TI para o gerenciamento de atualizações do Windows, chamado "KBs" pelos profissionais de TI em relação aos artigos de "Base de conhecimento" que alertam sobre os patches. Os patches individuais da Microsoft que acabaram com a funcionalidade em um ambiente de computação poderiam ser revertidos. Porém, esse recurso foi cancelado no mês de outubro.

Os dois anúncios da Microsoft sinalizam o fim das práticas tradicionais de TI para o gerenciamento de atualizações do Windows, chamado "KBs".

Sem patches individuais

Nesse novo esquema, se os profissionais de TI tiverem algum problema com um patch individual do Windows, terão de reverter à linha de base do sistema operacional do mês anterior. Os profissionais de TI não poderão reverter a um patch individual (KB) quando essa nova abordagem de atualização "Windows como um serviço" entrar em vigor em outubro, como indicado pela Microsoft:

A resposta é "Não", não é possível controlar que KB pode ser aplicado, e por isso deve-se fazer uma cópia de backup da reversão completa. Mas a resposta é muito mais complexa do que um simples "não".

A complexidade anteriormente anunciada está relacionada à fragmentação geral dos patches, que ocorre nos ambientes de Windows quando os profissionais de TI aplicam atualizações de maneira seletiva, segundo a Microsoft. Os profissionais de TI podem ver um patch individual incorreto como um problema que a Microsoft deveria resolver, mas para a Microsoft esse é um problema que os sócios deveriam corrigir.

"Se houver um problema, o parceiro precisará abrir um caso e fornecer uma justificativa de negócios para iniciar a discussão com a Microsoft", explicou o anúncio da Microsoft.

Não está muito claro o que os profissionais de TI devem fazer caso um diálogo entre a Microsoft e um parceiro não resultar em uma solução para um patch problemático. Parece que só podem reverter seu patch cumulativo ao mês anterior. Com esse enfoque, os profissionais da área de TI poderiam ficar defasados na aplicação de patches de atualizações de recursos.

Porém, as atualizações de segurança são uma questão à parte. Elas estarão disponíveis já que serão lançadas em atualizações cumulativas separadas para as organizações que usam os sistemas de gerenciamento Windows Server Update Services ou System Center Configuration Manager. As atualizações de segurança cumulativas também podem ser obtidas a partir do catálogo do Microsoft Update. A Microsoft não planeja mais lançar atualizações de segurança cumulativas por meio do serviço do Windows Update.

Mudança de raciocínio

Os profissionais de TI acostumados com os métodos de gerenciamento de patch tradicionais terão de mudar suas formas de raciocínio, como sugerido pela Microsoft:

Com o Windows 10, um novo modelo é adotado. Esse novo modelo, conhecido como "Windows como um serviço", requer que as organizações repensem a forma como implantam e atualizam o Windows. Não é mais um projeto que acontece com intervalos de poucos anos, é um processo contínuo.

Além disso, o processo de atualização da Microsoft envolve um ciclo complexo no qual os profissionais de TI terão de controlar as alterações das filiais ("filial atual" e "filial atual para os negócios"). Ou eles têm a opção de seguir a "filial em serviço a longo prazo" com as edições Enterprise ou Education do Windows 10, que oferece às organizações os melhores tempos de atrasos entre as atualizações. Não está muito claro se esses ciclos do Windows 10 também serão aplicados às versões mais antigas do Windows.

Por enquanto, as entregas mais rápidas de atualizações mensais da Microsoft com o Windows 10 ocorreram sem problemas.

Por enquanto, as entregas mais rápidas de atualizações mensais da Microsoft com o Windows 10 ocorreram sem problemas. Por exemplo, uma atualização falha em abril aos Windows Server Update Services, projetada para descriptografar as atualizações do Windows 10, foi corrigida pela Microsoft em maio, mas ainda exigia etapas de configurações manuais pelos profissionais de TI para que funcionasse corretamente. Provavelmente, muitas organizações esperavam evitar as correções do Windows 10 por alguns anos ao permanecer com o Windows 7. Entretanto, em outubro de 2016, essa perspectiva de segurança desapareceu. A Microsoft parece estar dizendo aos profissionais de TI que sigam com o programa, de forma nada sutil. Mas se o software parar de funcionar nas organizações, haverá provavelmente uma conversa bilateral. R

Kurt Mackie é produtor sênior de notícias para o 1105 Enterprise Computing Group.

Verificação do serviço Windows Defender Advanced Threat Protection baseado em cloud

O software antivírus tradicional não pode enfrentar as ameaças dirigidas às redes das empresas e foi pensando nisso que a Microsoft criou o Windows Defender ATP. POR ED BOTT

O problema com o software antivírus é que ele não é perfeito. No jogo de gato e rato entre os criminosos cibernéticos e as pessoas responsáveis por proteger as redes empresariais e os computadores individuais, as pessoas mal-intencionadas possuem uma vantagem incomparável: elas precisam ser bem-sucedidas apenas uma vez, enquanto as pessoas boas devem bloquear todas as tentativas.

Esse é o principal motivo que não me faz apostar muito nos resultados do teste do software antivírus, como os da AV-Test, uma organização alemã independente que publica comparações de programas antivírus há muito tempo.

Durante os últimos seis meses ou mais, o software antivírus baseado no Windows bloqueou aproximadamente 98% do que a AV-Test chama de seus testes "de dia zero" e quase (mas não exatamente) 100% de amostras conhecidas "em todo o ambiente". Isso parece impressionante até você perceber que esses números elevados são na verdade um cenário de melhor caso que usa computadores totalmente corrigidos em um ambiente controlado. Se a sua organização aceita um computador que não está totalmente corrigido na rede, ela nunca estará protegida. E, claro, os invasores mais persistentes e habilidosos, geralmente financiados por um estado-nação, possuem as habilidades e os recursos além do hacker regular.

Por isso, não é de se admirar que muitos especialistas em segurança recomendem que os gerentes empresariais adotem uma postura mais firme e assumam que mesmo com um treinamento cuidadoso e com a implantação da melhor infraestrutura em segurança, alguns invasores conseguirão alcançar seus objetivos.

Por isso, não é de se admirar que muitos especialistas em segurança recomendem que os gerentes empresariais adotem uma postura mais firme e assumam que mesmo com um treinamento cuidadoso e com a implantação da melhor infraestrutura em segurança, alguns invasores conseguirão atingir seus objetivos. Quando (e não se) isso acontecer, o objetivo muda: detectar as violações, investigar como elas ocorreram, corrigir as máquinas comprometidas e reforçar as defesas de forma que os invasores não consigam reutilizar a mesma técnica.

É claro que isso não significa que o software antivírus tradicional seja obsoleto. Mas esses programas são apenas uma pequena parte de uma estratégia de segurança em múltiplas camadas. Se você deseja ver onde está a inovação real, confira o serviço Windows Defender Advanced Threat Protection (Windows Defender ATP) baseado em cloud, anunciado pela Microsoft em março de 2016 e implantado em clientes empresariais no mundo todo após uma análise estendida.

O Windows Defender ATP é, por excelência, um produto da Microsoft, começando com uma confusão da marca que parece fazer parte de qualquer novo produto do Windows. Embora ele compartilhe parte do seu nome com o Windows Defender, o novo serviço tem pouco em comum com o software antimalware incluído gratuitamente no Windows 10. Em vez disso, em um design típico de praticamente tudo da Microsoft atualmente, ele é um serviço de cloud baseado no Azure.

Para instalar o Windows Defender ATP em um computador, é necessária a edição Pro, Education ou Enterprise, uma conta do Azure Active Directory e uma licença para o serviço do Windows Defender ATP. O processo de configuração permite uma coleta do que a Microsoft chama de "sensores

comportamentais do endpoint", que controlam as atividades em cada dispositivo, como as chamadas de registro, atividades de arquivo e processo e comunicações de rede. Esses dados são armazenados em um repositório de cloud privado e isolado, dedicado à organização e não compartilhado com outros assinantes do Windows Defender ATP. A Microsoft publicou os detalhes sobre o Windows Defender ATP no Windows IT Center. Um relatório separado sobre as políticas de privacidade e armazenamento de dados também está disponível.

O valor real do Windows Defender ATP vem da análise fornecida pela Microsoft com o uso do gráfico de segurança criado a partir de serviços, como o serviço de reputação SmartScreen URL e a Microsoft Malicious Software Removal Tool. Além disso, os insights de segurança do Windows Defender ATP aproveitam o threat intelligence de grupos dentro da Microsoft e de parceiros, como o FireEye. De forma conjunta, a quantidade de dados específicos possibilita a identificação da linha de tempo de um ataque, assim como as ferramentas e técnicas que os invasores usaram para passar pelas defesas tradicionais. A base de conhecimento também inclui informações específicas sobre "detalhes do autor e contexto pretendido", que podem literalmente nomear os autores de um ataque com base nas técnicas utilizadas.

Tudo isso é apresentado em um portal muito organizado que deve parecer familiar a qualquer pessoa que já tenha gerenciado uma conta do Azure. Você pode obter alertas sobre atividades suspeitas, ver ameaças ativas e filtrar a lista para mostrar as ameaças que foram ou que ainda não foram corrigidas.

Você pode obter alertas sobre atividades suspeitas, ver ameaças ativas e filtrar a lista para mostrar as ameaças que foram ou que ainda não foram corrigidas.

Ironicamente, muitas empresas que poderiam se beneficiar com o uso do Windows Defender ATP podem ignorá-lo devido ao nome. Mas aquelas que entendem que ele é mais do que um software antivírus tradicional o analisarão de forma mais atenta. R

Ed Bott é um MVP da Microsoft e jornalista premiado e especializado em tecnologia que cobre a Microsoft há 25 anos. Ele escreveu diversos livros sobre o Windows e o Office, inclusive a série best-seller "Inside Out" da Microsoft Press. Bott oferece conselhos explícitos sobre diversos tópicos tecnológicos em seu blog ZDNet, "The Ed Bott Report".

O plano da Microsoft para reduzir em um terço o tamanho da atualização do Windows 10

POR KURT MACKIE

Uma nova tecnologia da Microsoft chamada de "Unified Update Platform" promete reduzir em um terço o tamanho das futuras atualizações do Windows 10.

Como a Microsoft explicou, essa tecnologia emergente pode reduzir os tamanhos de download do Windows 10 em "aproximadamente 35% ao migrar de uma atualização grande do Windows para outra". Também espera-se reduzir o tempo de processamento nos dispositivos com a nova tecnologia.

Os usuários de computadores que participarem do Windows Insider Program também verão lançamentos menores de atualizações do Windows 10 a partir da tecnologia Unified Update Platform.

Alguns analistas de dispositivos móveis do Windows Insider Program que usam o Windows 10, pacote 14959, poderão notar rapidamente os efeitos da tecnologia Unified Update Platform. Ela trará muito mais vantagens para eles, pois permitirá que os usuários móveis atualizem para a versão mais recente do Windows 10 de uma só vez, e não de forma gradual, segundo promessa da Microsoft.

Os usuários de computadores que participarem do Windows Insider Program também verão lançamentos menores de atualizações do Windows 10 a partir da tecnologia Unified Update Platform, como sugerido pela Microsoft.

A Microsoft também planeja implementar eventualmente a Unified Update Platform com outros produtos baseados no Windows 10, como dispositivos com a Internet das Coisas e os dispositivos de realidade aumentada Microsoft HoloLens. A sincronização de horários para uma implementação geral e pronta para a produção não foi indicada no anúncio da Microsoft.

A Microsoft divulga atualizações do Windows 10 mensalmente. Divulga também de tempos em tempos as principais atualizações de recursos do sistema operacional, algumas vezes por ano. As atualizações mensais são "cumulativas", o que significa que elas contêm todas as atualizações já

lançadas. Consequentemente, o tamanho das atualizações do Windows 10 pode aumentar um pouco, algo como 3 GB, o que pode ser um problema para os dispositivos móveis com pouco espaço de armazenamento.

O problema do tamanho da atualização é parcialmente resolvido pela tecnologia de "pacote de download diferencial", que oferece apenas os bits alterados, e não o download completo, como explicado no anúncio da Microsoft. Aparentemente, essa abordagem faz parte do futuro esquema da Unified Update Platform.

Talvez a Unified Update Platform seja útil para usuários finais individuais. Do lado do gerenciamento de TI, a Microsoft possui o recurso Windows Update Delivery Optimization, que pode ser aperfeiçoado pelas configurações da Diretiva de grupo. Trata-se de um esquema de atualização do cliente ponto a ponto que foi iniciado no Windows 10, versão de "atualização de aniversário" 1607 lançada em agosto. A solução Delivery Optimization foi projetada para fazer download dos bits de atualização de computadores e dos bits de atualização dos data centers da Microsoft para reduzir o possível problema de largura de banda que as empresas podem enfrentar com as atualizações do Windows 10. Supostamente, o esquema explora partes não utilizadas de uma capacidade de upload da rede para a realização de atualizações do computador.

O BranchCache é outro sistema mais vulnerável da Microsoft para o gerenciamento de problemas de largura de banda, principalmente em relação a atualizações remotas.

Os usuários do System Center Configuration Manager possuem uma alternativa ao Delivery Optimization chamada "Client Peer Cache". Ela foi lançada com a versão preliminar 1604, mas estará disponível em uma versão posterior do System Center Configuration Manager, de acordo com esse artigo da TechNet. Uma análise inicial do Client Peer Cache, como descrita no blog de maio passado pela consultoria de gestão 1E, revelou que ela possuía alguns aspectos negativos naquela época.

O BranchCache é outro sistema mais vulnerável da Microsoft para o gerenciamento de problemas de largura de banda, principalmente em relação a atualizações remotas. O BranchCache foi projetado para as organizações com operações difundidas e está disponível nas edições Enterprise ou Education do Windows 10, embora algumas das suas funcionalidades de BITS possam ser encontradas na edição Pro. O BITS, ou Background Intelligent File Transfer Service, é uma tecnologia da Microsoft para lidar com a sincronização de horários de transferências de arquivos dentro de uma rede. R

Kurt Mackie é produtor sênior de notícias para o 1105 Enterprise Computing Group.

O lançamento de patches da Microsoft corrigiu os problemas de conexão com a Internet do Windows 10

POR KURT MACKIE

O recente lançamento "patch Tuesday" da Microsoft contém uma correção para um problema de conexão com a Internet que supostamente teve seus efeitos difundidos nas máquinas com o Windows 10.

O recente lançamento "patch Tuesday" da Microsoft contém uma correção para um problema de conexão com a Internet que supostamente teve seus efeitos difundidos nas máquinas com o Windows 10.

Os problemas de conexão com a Internet ou com o Wi-Fi começaram recentemente. A Microsoft tomou conhecimento dos problemas em um fórum de discussão, que indicou que "alguns clientes estavam com dificuldade para conectar à Internet". Em um artigo de suporte, a Microsoft aconselhou seus usuários a reinicializarem, mas não desligarem, seus computadores. Os usuários também foram aconselhados a procurar por outras possíveis fontes de problemas, como problemas no modem a cabo ou problemas de conexão com o provedor de serviços da Internet.

A Microsoft informou que o patch KB3206632, lançado e incluído em um recente boletim de segurança, foi criado para corrigir o problema. Esse patch substitui a atualização KB3201845, que supostamente foi a responsável pelos problemas de conexão com a Internet, embora o autor da InfoWorld, Woody Leonhard, tenha observado que esses problemas aconteceram dois dias antes do lançamento da KB3201845.

O problema de conexão com a internet afetou somente os dispositivos que executam o "Windows 10 1607 (RS1)" em execução, de acordo com Nathan Mercer, técnico da Microsoft, em uma publicação de lista de servidor em Patchmanagement.org. Mas até o momento, a Microsoft só divulgou essas informações sobre o problema.

É possível que a Microsoft tenha corrigido o problema que nunca foi descrito em sua totalidade.

O boletim KB3206632 da Microsoft não é muito descritivo, embora indique uma correção de dezembro para "uma falha no serviço do CDPSVC que, em algumas situações, poderia fazer com que a máquina não fosse capaz de obter um endereço IP". Uma descrição do problema pelo The Register sugeriu que uma atualização de software da Microsoft danificou de alguma forma o Dynamic Host Configuration Protocol usado para emitir os endereços IP.

É possível que a Microsoft tenha corrigido o problema que nunca foi descrito em sua totalidade. A descrição parece ser uma prática antiga e abandonada com o novo e ágil método de fornecimento do software Windows 10.

A Microsoft também divulgou 12 boletins de segurança em seu patch de dezembro, com a solução de seis falhas "críticas". Os itens principais no "índice explorável" da Microsoft naquele mês incluíam uma vulnerabilidade de corrupção de memória do mecanismo de scripting, uma vulnerabilidade de corrupção de memória do navegador e uma falha de bypass do recurso de segurança do Office, entre outras, conforme descrito no boletim de dezembro. R

Kurt Mackie é produtor sênior de notícias para o 1105 Enterprise Computing Group.
