Data da publicação:
7 de fevereiro de 2020
Autor:
Alan Rodger

Patching sustentável de software: Essencial para obter segurança robusta, menos riscos e atender aos desafios de compliance

Os clientes, que se deparam com níveis de complexidade e de ameaças cada vez maiores, precisam de um suporte robusto

OMDIA

Resumo

Em suma

Os investimentos que diversos setores industriais fazem cada vez mais na transformação digital significam que o software é mais imprescindível do que nunca para o caixa das organizações e a reputação dos negócios. Ao mesmo tempo, fatores como maiores complexidades acerca das oportunidades de novas tecnologias (incluindo cadeias de suprimentos digitais mais predominantes), o crescente cenário de ameaças e o ambiente competitivo, que impulsiona as atualizações de software mais frequentes por parte dos fornecedores que buscam introduzir novos recursos, aceleram o ritmo da adoção de softwares e transformam os ciclos nas organizações dos usuários. O produto de software resultante é comumente caracterizado por uma superfície de ataques significativamente maior na qual hackers mantêm um foco cada vez maior, descobrindo os pontos fracos e criando ataques para explorá-los.

Embora diversas soluções de segurança possam ser colocadas em prática para abordar os elementos específicos de proteção, a aplicação oportuna de patches dos softwares dos fornecedores é a base indispensável para evitar o risco que surge da presença de vulnerabilidades de segurança que ainda não tenham sido reduzidas. As organizações de gerenciamento de riscos e de compliance estão atuando mais próximas do que nunca nas práticas de proteção de softwares em direção à digitalização, e as ameaças que ainda continuam sem soluções por causa de vulnerabilidades sem patches, constituem, consequentemente, verdadeiros problemas para os negócios.

A Omdia acredita que muitas organizações precisam de mais maturidade e entendimento do valor do gerenciamento proativo da aplicação de patches na carga de trabalho e no ciclo de vida útil dos produtos, o que requer um comprometimento para estabelecer uma janela de segurança de patches dentro do cronograma de manutenção de prioridades. Como o uso de patches é um recurso cada vez mais importante, essa necessidade de maturidade deve ser refletida no contexto da estrutura de governança de TI da organização, que deve incluir conteúdo de patches somente adquirido com o fornecedor original.

Perspectiva da Omdia

Os clientes frequentemente passam por um processo rigoroso de análises e devida diligência antes de investirem em produtos de software empresarial, além de considerarem o escopo e os custos envolvidos na maioria dos projetos. É surpreendente, no entanto, saber que alguns clientes não adotam uma devida diligência semelhante em se tratando de proteger adequadamente esses investimentos feitos em software por meio da manutenção e do uso contínuo de patches de software que são necessários para manter a gama completa do possível custo-benefício do software. A abordagem de governança de TI em qualquer organização deve salvaguardar contra qualquer tendência de “comprar e não

atualizar" com relação a qualquer elemento do software, que pode abrir lacunas na proteção empresarial e desenvolver problemas de risco e compliance, gerando graves problemas nos negócios.

Garantir uma regularidade na manutenção e na aplicação de patches de softwares deve ser uma obrigatoriedade para todas as empresas, impostas rigorosamente pelo compromisso que a gerência tem com a importância dos planos de manutenção e a maturidade necessária dentro da cultura organizacional para garantir a aplicação regular e exitosa dos patches. A manutenção regular da segurança permite aos clientes criar uma cultura de compliance, na qual eles possam sentir confiança para acompanhar as regulamentações do setor e os procedimentos de compliance. Deixar de realizar adequadamente a manutenção e a aplicação de patches de software significa colocar em risco os lucros da empresa e sua reputação como empresa protegida e responsável. No entanto, além de reiterar esses importantes motivos comerciais para haver o compromisso com o uso de patches, a cultura organizacional deve superar quaisquer receios de que o uso de patches poderia ser potencialmente responsável por causar falhas. Pelo contrário, a verdade é que deixar de usar patches atualizados constitui um risco muito maior.

É claro que assim como ocorre com qualquer outra esfera do gerenciamento de TI, o uso de patches deve estar sujeito a um controle robusto. Um elemento importante de um programa bem-sucedido de uso de patches é a adoção do uso de fontes altamente íntegras de informações sobre patches, não acreditando em fontes de baixa qualidade, como orientações onipresentes na internet. Outro ponto fraco a ser evitado é qualquer envolvimento de prestadores de serviços terceirizados sem a garantia de que os processos e as aptidões deles adotem todo o rigor necessário no uso de somente fontes confiáveis de conteúdo de patches. É provável que as consequências de uma governança inadequada desses tipos de relacionamentos incluam mais custos para a organização cliente, bem como problemas de riscos e compliance. Além disso, as organizações não devem confiar em controles para mitigação de riscos que não são comprovadamente eficientes ou em configurações não verificadas para evitar o uso de patches.

Avisos importantes

- É responsabilidade imprescindível manter a segurança dos softwares em relação ao seu respectivo ciclo de vida.
- O uso de patches é a base da governança de TI e o suporte que eles prestam às responsabilidades de compliance.
- O risco é evitado somente se os patches forem adquiridos de fontes confiáveis.

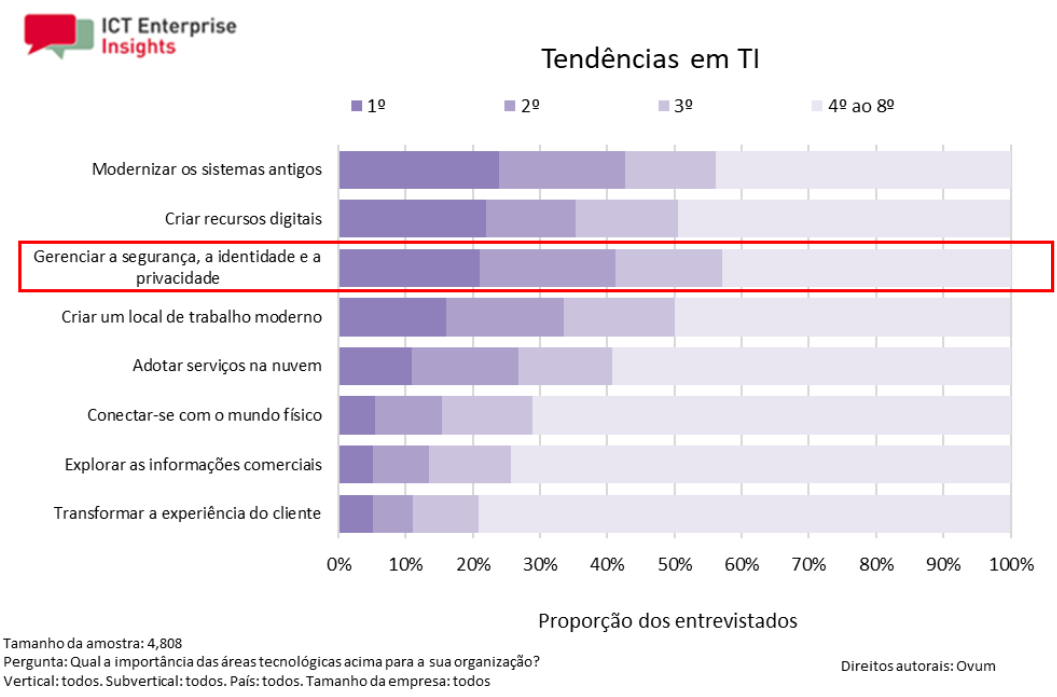
É responsabilidade imprescindível manter a segurança dos softwares em relação ao seu respectivo ciclo de vida.

Muitos clientes empresariais estão tentando transformar o departamento de TI para poderem acompanhar o ritmo acelerado das mudanças que ocorrem em seus respectivos mercados e negócios ao se beneficiarem das oportunidades tecnológicas, como nuvem, mobilidade e processamento analítico. De comum acordo, há uma atitude de equilíbrio constante entre investir em iniciativas de transformação digital (aproveitando aplicativos e processos de negócios novos e aprimorados) e a necessidade de garantir que o ambiente

em transformação real esteja operando com confiabilidade e segurança sem falhas. A gama de componentes da infraestrutura de TI que deve ser protegida está ampliando, não apenas abrangendo a "stack" tradicional desde sistemas operacionais até hardware, bancos de dados, middleware e aplicativos, como também incluindo serviços baseados na nuvem e serviços de outros terceiros. Fora dos limites tradicionais de TI, toda presença empresarial nos ambientes móveis dos consumidores deve incorporar uma proteção embutida de segurança, pois, seja de maneira intencional ou não, há a possibilidade de os usuários móveis abrirem o dispositivo e se prejudicarem com as ameaças.

Toda falta de proteção dentro da infraestrutura ampliada de TI pode resultar em tempo de inatividade capaz de impactar a empresa toda, e, em algumas circunstâncias, nas violações de segurança que podem causar infrações nas regulamentações do setor e nos procedimentos de compliance. Sem surpresas neste contexto, respostas dadas à pesquisa anual da Omdia, que foi realizada recentemente, indicaram que o gerenciamento da segurança, da identidade e da privacidade ficou entre as três tendências mais importantes de TI nas organizações – acima de qualquer outra categoria (ver Figura 1).

Figura 1: O gerenciamento da segurança, da identidade e da privacidade é identificado como a tendência mais importante dentre três opções



Fonte: Informações Empresariais de ICT da Omdia para 2019/20

Com o próprio setor de TI se tornando cada vez mais interconectado (ex., por meio de parcerias de tecnologia) para prestar suporte à digitalização, a cadência dos lançamentos de software agora é muito mais rápida em relação ao que os clientes estavam acostumados. Embora os clientes se beneficiem de fornecedores que concorram com mais entusiasmo do que nunca com relação a novos recursos e funcionalidades, os ativos de TI deles representam uma superfície de ataque mais ampla que pode estar sujeita a uma gama maior de ameaças provenientes dos hackers. Fornecedores líderes estão reforçando o compromisso de responderem às ameaças com o lançamento de patches para

vulnerabilidades conhecidas na área de segurança cibernética, e, o fato de uma organização manter os seus ativos atualizados com patches fornecidos pelo fornecedor é a maneira mais oportuna e principal de se proteger contra ameaças relacionadas com software. Novos lançamentos e patches também podem exigir que os clientes revisem patches anteriores de seu "stack" (por exemplo, middleware, SO ou banco de dados) para atender às necessidades de suporte, e a cadeia de medidas de proteção de seu "stack" requerem foco contínuo. Por exemplo, sabe-se que atualizações específicas de firmware da Intel exigem patches correspondentes ao SO e camadas de virtualização, e, para tipos de processadores mais antigos, a mitigação dos problemas com o processador exige a desativação de certos recursos (hyperthreading) se estiver executando cargas de trabalho não confiáveis.

Não é difícil entender por que a segurança é uma questão urgente entre as empresas de todos os tipos, considerando o que um incidente ou uma violação na segurança possa significar para os negócios e a reputação de uma organização. Novos casos de vazamento e ataques na segurança de empresas multinacionais são mais frequentes do que nunca, com relatos de roubo de dados de cartões de crédito, informações pessoais, registros médicos, entre outros (ex., incidentes que envolveram a Equifax e a CapitalOne). Já houve exemplos de reforço nas penalidades relacionadas com compliance por causa de procedimentos inadequados no uso de patches, e esse fato pode ocorrer novamente à medida que as regulamentações e a legislação ficam mais rigorosas (ex., 4% da rotatividade global para infrações relacionadas com a falta de compliance, segundo a regulamentação GDPR). Além dos impactos financeiros diretos, esses eventos geralmente geram perda de receita e reputação ofuscada para as empresas afetadas, com possíveis perdas de negócios e fidelidade do cliente, que são difíceis de recuperar. A maioria das empresas reconhece a necessidade de se protegerem o máximo possível contra possíveis ameaças à segurança cibernética. No entanto, as empresas também devem notar que essas ameaças podem ser oriundas não apenas de hackers externos, mas por deixarem de manter atualizada a proteção da segurança interna em toda a pilha de TI.

O uso de patches é a base da governança de TI e o suporte que eles prestam às responsabilidades de compliance.

Hoje em dia, as empresas simplesmente não podem se dar ao luxo de não terem um programa rigoroso de manutenção e segurança de software, principalmente pelo fato de as ameaças externas serem contínuas e estarem se tornando cada vez mais sofisticadas, o que requer vigilância e manutenção constantes. Para terem um perfil de segurança rigoroso, as empresas devem trabalhar em parceria próxima com os fornecedores de software, já que eles contam com a máxima experiência e especialização em patches, suporte e proteção de seus próprios produtos. Empresas de todos os portes e em todos os setores precisam fazer parcerias com um prestador de confiança para a implantação de procedimentos para manter atualizada a segurança de seus softwares e para abordar possíveis vulnerabilidades. As vulnerabilidades de software não minimizadas podem permitir que hackers mal intencionados ou funcionários não autorizados ignorem os controles de segurança, o que pode resultar diretamente em roubo, fraude e perda financeira imediata, sem mencionar o prejuízo para a marca da empresa. Além dessas perdas, as empresas que deixam de manter a atualização da segurança dos softwares arcam com possíveis multas por violarem as regulamentações do governo ou do setor e os procedimentos de compliance, e essas

consequências estão ficando cada vez mais onerosas à medida que os incidentes com segurança aumentam em termos de frequência e gravidade. Nos EUA, os responsáveis pelas regulamentações do governo aplicaram multas altas após ocorrerem violações com segurança e dados, o que custou milhões de dólares às empresas em diversos setores. Na verdade, as violações com segurança e seus respectivos resultados se tornaram tão frequentes que a Federal Trade Commission (FTC, Comissão Federal de Comércio dos EUA) divulgou orientações completas sobre como as empresas devem tratar a segurança de TI ao longo de toda a pilha de TI. Para mencionar um exemplo, a FTC publicou o Start with Security: A Guide for Business (Começar pela Segurança: Um Guia para Empresas), uma compilação das 10 principais lições que podem ser aprendidas com as multas e os acordos que a organização promulgou em casos de violações que ocorreram no passado, conforme mostrado na Tabela 1.

Tabela 1: Recomendações da FTC para a segurança de TI
Começar pela segurança
Controlar acesso aos dados com prudência
Exigir senhas e autenticação de proteção
Armazenar informações pessoais sigilosas com segurança e protegê-las durante a transmissão
Segmentar e monitorar a rede
Proteger o acesso remoto à rede
Aplicar práticas de segurança sensatas ao desenvolver novos produtos
Certificar-se de que seus prestadores de serviços implementem medidas de segurança razoáveis
Implementar procedimentos para manter a segurança atualizada e abordar as vulnerabilidades que possam surgir
Proteger documentos, mídia física e dispositivos

Fonte: *Federal Trade Commission*

Embora partes deste guia sejam bastante intuitivas, algumas das lições merecem mais atenção quando analisadas levando em consideração o uso de patches apropriado no produto e o suporte. Ao discutir sobre práticas sensatas de segurança no desenvolvimento de produtos, a FTC faz referências a empresas que foram intimadas e multadas por não seguirem as diretrizes da plataforma de produtos de TI para terem segurança. Ao discutir os procedimentos de segurança para abordar as vulnerabilidades, a FTC recomenda especificamente a atualização e o uso de patches nos softwares de terceiros, acatando quaisquer avisos de segurança emitidos pelos fornecedores e abordando-os de maneira imediata. O não cumprimento desta norma pode significar que uma empresa passará por fiscalização minuciosa por parte dos órgãos reguladores e outras partes e, consequentemente, incorra uma multa onerosa se ocorrer um problema de segurança grave e a empresa tiver deixado de obedecer previamente às políticas de compliance.

Várias outras regulamentações e normas incluem estipulações relacionadas com o uso de patches, incluindo o

- Requerimento do PCI DSS 6.2, que exige que um avaliador averigue as políticas e os procedimentos das organizações com a finalidade de verificar se há um processo definido para o gerenciamento de patches.
- ISO/IEC 27001 Seção 12, que obriga que as vulnerabilidades técnicas sejam abordadas com patches, devendo haver regras implementadas que regem a instalação de softwares feita pelos usuários.

Considerando esse panorama, cada vez mais as empresas relatam para a Omdia que os segmentos de segurança e de compliance devem atuar juntos quando elas consideram implementar softwares, e que ambos os segmentos desempenham uma função cada vez mais expressiva no suporte e na manutenção geral de TI. Para muitos programas de compliance, é imprescindível manter documentos para comprovar como as medidas adotadas (nos níveis de políticas e operacional) atendem aos requerimentos de compliance. É provável que o uso automatizado de patches proporcione a maneira mais eficaz para cumprir esses requerimentos no futuro, bem como para garantir a eficiência e evitar um impacto mais expressivo da crescente demanda por recursos relacionada com a ampliação dos requerimentos para o uso de patches.

A maioria das regulamentações é baseada em transações (ex., em serviços financeiros e bancários), baseada em gerenciamento de dados (ex., privacidade de dados e armazenamento de registros no setor da saúde), ou ambos. Na Omdia, recomendamos com regularidade que as empresas, independentemente dos setores verticais nos quais elas atuem, precisam criar uma base sólida e uma cultura de compliance como via de regra para suas atuais implantações de software e TI, principalmente se tiverem a esperança de um dia adotarem iniciativas de transformação digital, que levará o software para uma posição mais crítica para prestar suporte a todos os tipos de processos. Nossa análise é que essa base não pode existir sem serviços regulares de manutenção e patches de software, de preferência aqueles serviços que forem automatizados e escalonáveis e que proporcionem mais tempo para que os diretores dos departamentos de Informática e os gerentes de TI possam se concentrar em outras iniciativas. Para que isso aconteça, é importante uma empresa trabalhar com os seus respectivos fornecedores de software – as empresas que, na verdade, criam, atualizam, disponibilizam patches e prestam suporte para os produtos com regularidade. Para que isso ocorra em produtos mais antigos, é preciso incluir uma atualização do software do fornecedor para uma versão mais moderna e com pleno suporte, elaborada para tratar as atuais ameaças de segurança, e não as ameaças de cinco a dez anos atrás.

O risco é evitado somente se os patches forem adquiridos de fontes confiáveis.

Algumas empresas fazem manutenção e uso de patches de software somente quando ocorre uma degradação do desempenho, da funcionalidade ou da confiabilidade, ou quando uma ameaça de segurança estampada em manchetes de jornais as obriga a analisar quais possíveis lacunas na segurança precisam ser abordadas. Às vezes, nessas circunstâncias, fontes de informações informais, como, por exemplo, sites de orientações na internet, podem ser usadas para pesquisar soluções e, possivelmente, também para fornecer conteúdo sobre o uso de patches. Este pode ser um erro grave que geram riscos

diretos se o patch acabar sendo nocivo ou introduzir erros técnicos. Considerando os problemas constantes com segurança e compliance, e a frequência crescente de violações na segurança e tentativas de hackear a segurança, muitas empresas decidiram que precisam de uma abordagem mais formal, com monitoramento regular do software, uso de patches e manutenção como funções essenciais de suas respectivas operações de TI. A abrangência no escopo deste tipo de abordagem está bem alinhada com as necessidades de compliance e de governança, incorporando uma visão de alto nível do "ciclo de vida útil" das vulnerabilidades e dos patches. Isso contrasta com algumas soluções pontuais (ex., firewalls em bancos de dados e proxy dos aplicativos da internet) que alegam combater as vulnerabilidades, mas que são limitadas na funcionalidade e não fornecem, de maneira alguma, uma abordagem orientada por riscos que seja condizente com os negócios.

O mesmo nível de atenção é importante quando depender de qualquer relacionamento de prestação de serviços terceirizados para o fornecimento de suporte ao software. A inadequação de definições dos requerimentos poderia dar vazão para um prestador de serviço sair impune ao implementar "alternativas" como soluções parciais para as vulnerabilidades para poder encerrar um chamado de suporte. Além de constituir um risco potencial por causa da proveniência inadequada do prestador de serviço, esses fatores têm a probabilidade de causar mais custos de propriedade em decorrência das suas divergências em relação ao caminho de desenvolvimento padrão do software, introduzindo custos de regressão em uma etapa futura. Como resultado, os prestadores de serviços precisam demonstrar que estão atuando como parceiros dos clientes e de seus respectivos fornecedores de software para atender às necessidades de suporte e patch de software. Eles devem demonstrar três características importantes:

- **Prestador de confiança**. Um prestador de confiança e testado tem conhecimento e especialização em proteção de dados e em ambientes empresariais de TI, além de vasta experiência em segurança e suporte de classe empresarial.
- **Conhecimento especializado em segurança**. Um prestador precisa ter experiência em proteção de toda a pilha de TI, entre infraestruturas, bancos de dados e aplicativos, além de conhecimento especializado na prestação de recursos de suporte proativo e em tempo real sempre e quando houver necessidade.
- **Opções abrangentes de produtos.** Um prestador deve oferecer uma gama completa e integrada de produtos de segurança e suporte que estejam em desenvolvimento e em inovação constantes, além de ser capaz de ajudar um cliente a estabelecer uma cultura centrada na segurança e na compliance de TI.

Os clientes da Omdia dizem com propriedade que a Oracle está se empenhando para oferecer uma ampla gama de recursos para demonstrar essas características em seus respectivos produtos de suporte em toda a pilha da Oracle, já que reconhece a criticidade que os sistemas Oracle desempenham em muitas organizações.

Além disso, o suporte da Oracle oferece níveis de capacidade e de segurança superiores na comparação com fornecedores terceirizados. Os fornecedores terceirizados não oferecem ajustes de segurança, como destaca a Oracle, pois esses fornecedores não conseguem alterar o código fonte da Oracle e não têm familiaridade com os detalhes técnicos das vulnerabilidades que a Oracle ajusta. Os clientes desses fornecedores de suporte terceirizados também não se beneficiam das iniciativas contínuas de garantia de segurança da Oracle, já que todos os ajustes e patches prévios já fazem parte de cada versão subsequente do software da Oracle.

Um cliente antigo da Oracle, uma importante empresa de telecomunicações e operadora de serviços a cabo, localizada no sul dos EUA, conta com uma implantação de grande porte com 450 servidores Oracle, incluindo seis sistemas Oracle Exadata. Esses sistemas são usados para prestar suporte ao armazém de dados empresariais da empresa, fornecendo uma estrutura essencial para todos os processos comerciais internos e externos. Na verdade, o cliente foi um dos primeiros a adotar o Oracle Exadata e vem acompanhando a evolução dos serviços de suporte da Oracle ao longo dos tempos.

Na implantação inicial do Oracle Exadata, as atualizações do software exigiram uma atualização demorada do firmware e de toda a plataforma, pois o Exadata é um sistema projetado para oferecer benefícios como uma plataforma integrada. Em 2012, e com base nessas experiências, a Oracle introduziu o suporte de nível Platinum para o Exadata. Esse nível oferece maior visibilidade do sistema de apoio e inclui elementos proativos, como o recurso de “phone home”, que permite aos engenheiros de suporte da Oracle, que trabalham com a equipe de apoio do cliente, detectarem possíveis problemas antes de se tornarem críticos.

O nível de suporte superior também oferece ao cliente melhores recursos para o uso de patches de software. O cliente aplica os patches uma ou duas vezes por ano, dependendo da necessidade e da criticidade. (O suporte do Platinum oferece quatro ciclos de patches por rack completo do Oracle Exadata.) O cliente consegue coordenar com os engenheiros de suporte da Oracle qualquer patch para garantir o devido gerenciamento de mudanças nos sistemas e limitar qualquer interrupção para a empresa, os funcionários e os próprios clientes.

O cliente alega que um cronograma de aplicação regular de patches e uma forte ênfase na segurança de TI em toda a empresa, garante que os respectivos sistemas fiquem menos vulneráveis e mais protegidos. Como o Exadata está potencializando alguns dos sistemas mais essenciais deste cliente, o tempo de inatividade teria um impacto direto na capacidade interna que o departamento de TI tem de entregar com base em seus acordos de nível de serviço aos clientes internos e externos, mesmo com a implementação de armazenamento robusto, recuperação em situações de desastre e redundâncias. Trabalhar com o suporte de nível Platinum da Oracle também permite ao cliente “repassar” certa carga do suporte interno para os engenheiros de suporte da Oracle, liberando sua própria equipe de TI para se concentrar em outros projetos e iniciativas. O cliente espera obter mais inovação nos procedimentos de patches e suporte da Oracle com funcionalidades ainda mais automatizadas. A Oracle continua trabalhando com o cliente por meio de reuniões constantes e outros métodos para garantir que o uso de patches e o suporte do cliente sejam devidamente abordados.

Recomendações

- **Implemente qualquer mudança de cultura necessária para que o uso de patches deixe de ser visto como um opcional ou uma consideração meramente operacional. Certifique-se de que ele seja considerado um elemento imprescindível da estabilização organizacional.** As organizações precisam perceber que as decisões de reduzir o comprometimento com a aplicação assídua de patches pode impactar de maneira adversa a integridade dos softwares e, portanto, não podem ser consideradas exclusivamente em um contexto operacional. O uso de patches inadequados pode levar à exploração de vulnerabilidades dentro do software da organização e, enquanto os patches não

são aplicados, o tempo disponível a agentes maliciosos para causar prejuízos continua se prolongando. É impossível resolver as implicações resultantes para a segurança, compliance e riscos sem realizar a aplicação dos patches necessários, e a morosidade dessa ação aumenta a probabilidade de possíveis custos para a organização.

Em vista destas implicações, é preciso revisar as decisões em relação às políticas de uso de patches em um contexto geral dos negócios, não apenas considerando os elementos táticos e operacionais, como licenças adicionais ou economias notadas no suporte. É preciso eliminar práticas como o uso de versões de software sem suporte, suporte terceirizado com gerenciamento deficiente ou parcialmente executado, ou a confiança em fontes inadequadas de orientação.

- **Embora o objetivo ideal seja usar patches em tudo o que for necessário, toda priorização dever ser orientada por riscos.** Os ambientes de TI devem ser completamente compreendidos do ponto de vista de riscos, tanto no contexto comercial como no técnico. O contexto comercial leva em consideração a criticidade relativa dos negócios no nível de serviços individuais, o que esclarece o impacto dos riscos afins no nível comercial (ex., finanças e reputação). O contexto técnico leva em consideração as características técnicas dos elementos que constituem o serviço (ex., SO, bancos de dados, hardware e aplicativos) e quaisquer desafios oriundos de vulnerabilidades específicas que estiverem ativas, bem como a exposição delas através das conexões para diferentes ambientes de ameaças (ex., se os recursos forem baseados na internet).
- **As informações sobre o uso de patches devem ser provenientes de fontes fidedignas, caso contrário, o uso delas constitui riscos.** A governança do uso de patches deve estipular quais fontes de orientação sobre patches podem ser consideradas confiáveis. Por exemplo, os fornecedores de software são a fonte fidedigna de informações sobre segurança para os seus respectivos produtos, enquanto a internet não é uma fonte confiável de orientações sobre patches. Além disso, fontes como o National Vulnerability Database (NVD, Banco de Dados Nacional de Vulnerabilidades) e o centro de coordenação da equipe de resposta em casos de emergências de computação (CERT/CC) são gerenciadas e fidedignas, enquanto ferramentas genéricas de verificação de vulnerabilidades de software podem ser insuficientemente especializadas para fornecer informações confiáveis. Por exemplo, esse tipo de ferramentas pode não reconhecer suficientemente ao certo uma versão de software, e, como resultado, se um patch foi ou não aplicado, gerando informações imprecisas nos relatos dos problemas pendentes e um efeito "entra lixo, sai lixo". Em qualquer cenário, o relatório é o nível mais alto que essas ferramentas conseguem oferecer, e as organizações, por si sós, ainda precisam avaliar e adquirir os patches necessários. A exceção é quando existe a prestação de serviços terceirizados de patches: neste caso, os contratos de vigência de serviços devem estipular que somente as fontes mais confiáveis de informações sobre patches podem ser usadas.
- **Os processos de uso de patches não devem ser o ponto fraco na proteção organizacional.** As organizações precisam se comprometer em colocar em prática a aplicação de patches como parte da manutenção regular da segurança em suas respectivas atividades de manutenção recorrentes. A aplicação de patches é uma importante medida de proteção proativa e um aspecto essencial da boa governança da segurança de TI. Deixar de planejar e preparar atividades de manutenção periódica resultará em aplicações incompletas de patches e, consequentemente, em uma postura degradada da segurança diretamente

relacionada com o aumento das preocupações da diretoria da empresa em relação à segurança.

Anexos

Leitura adicional

Federal Trade Commission (2015) Start With Security: A Guide for Business. Disponível no site <www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business> [Acessado em janeiro de 2020]

Autor

Alan Rodger, analista sênior, Soluções de Infraestrutura
alan.rodger@Omdia.com

Consultoria da Omdia

A Omdia é uma empresa de consultoria, pesquisa e dados líder no mercado cujo foco é ajudar os prestadores de serviços digitais, as empresas de tecnologia e os responsáveis pela tomada de decisões nas empresas a prosperarem na economia digital conectada.

Por intermédio dos nossos 150 analistas em âmbito global, oferecemos análises especializadas e percepções estratégicas entre os setores de TI, telecomunicações e mídia.

Criamos vantagem comercial para os nossos clientes oferecendo percepções ativas para ajudar no planejamento de negócios, desenvolvimento de produtos e iniciativas de lançamento de produtos no mercado.

Nossa combinação exclusiva de dados fidedignos, análises de mercado e especialização em setores verticais foi elaborada para capacitar a tomada de decisões, ajudando os nossos clientes a lucrar com as novas tecnologias e se beneficiarem dos modelos de negócios em constantes mudanças.

A Omdia faz parte da Informa Tech, uma empresa B2B de serviços da informação que atende aos setores de tecnologia, mídia e telecomunicações. O grupo Informa tem papéis negociados na Bolsa de Valores de Londres.

Esperamos que esta análise ajude você a tomar decisões comerciais informadas e criativas. Se tiver outras necessidades, a equipe de consultoria da Omdia pode ajudar sua empresa a identificar futuras tendências e oportunidades. Entre em contato conosco pelo e-mail

https://www.omdia.com/contact/contact-us

consulting@Omdia.com

Aviso de direitos autorias e isenção de responsabilidade