AS 3 MELHORES PRÁTICAS QUE OS MSP PODEM ADOPTAR PARA PROTEGER OS UTILIZADORES

Os ciberataques são cada vez mais frequentes. As empresas do Reino Unido, por exemplo, foram atacadas, em média, mais de 230 000 vezes em 2017. Os Managed Service Providers (MSP) precisam de priorizar a segurança em 2018 ou arriscam-se a por em causa a relação com os seus clientes. Aos seguir 3 simples boas práticas, que consistem na educação do utilizador, backup e recuperação e gestão de atualizações, os MSPs podem melhorar a segurança, eliminando os riscos para os utilizadores e ainda aumentar os seus lucros.

EDUCAÇÃO DOS UTILIZADORES

Uma solução antivírus eficaz é essencial para manter as empresas seguras. No entanto, já não é suficiente por si só. Educar os utilizadores finais para melhorar a sua consciencialização para a importância da segurança pode reduzir o custo e impacto de infeções ou falhas causadas pelos colaboradores, ao mesmo tempo que ajuda os clientes a estarem em conformidade com os requisitos do novo GDPR. As táticas dos cibercriminosos estão a evoluir e confiam cada vez mais nos erros dos utilizadores para contornar os protocolos de segurança. A seleção das empresas através dos utilizadores finais via social engineering é uma das táticas favoritas, entre todos os novos métodos de ataque.

AS ESTRATÉGIAS DE SOCIAL ENGINEERING MAIS COMUNS INCLUEM:

- Um email de um amigo de confiança, colega ou contacto - cuja conta tenha sido comprometida - contendo uma história interessante com um link/download malicioso é muito popular. Por exemplo, o email de um diretor de gestão é infectado e o departamento financeiro recebe um email para pagar uma 'fatura' pendente.
- Um email de phishing, comentário ou mensagem de texto aparentemente de uma empresa ou instituição legítima. As mensagens podem pedir doações para caridade, 'verificação' de informações ou notificações de que ganhou uma competição onde nunca se inscreveu.

- Uma pessoa mal intencionada deixa uma pen USB algures na empresa, na esperança de que um colaborador curioso a insira num computador ou portátil, permitindo o acesso à informação da empresa.

Conteúdo educacional focado nos tópicos relevantes e oportunos às situações da vida real pode minimizar o impacto de violações de segurança causadas por erros dos utilizadores. Ao treinar os clientes em social engineering e outros tópicos como ransomware, email, passwords e proteção de dados, pode promover uma cultura de segurança, que incuta sérios valores aos seus clientes.

PLANOS DE BACKUP E DISASTER RECOVERY

É importante que o MSP reforce a importância do backup. Se o cliente for atacado por ransomware e não tiver um backup seguro, estará perante opções desagradáveis como ter de pagar o ransom ou perder dados importantes.

Oferecer aos clientes uma solução de backup automatizada baseada em cloud torna a infeção dos dados em backup virtualmente impossível e ainda traz benefícios adicionais, como processos de backup simplificados, armazenamento de dados offsite e acesso em qualquer local e momento. Em caso de desastre, deve existir um plano de recuperação. Mesmo os sistemas mais seguros podem ser infiltrados. O plano deve ser construído com base nos dados críticos ao negócio, no tempo de recuperação e no protocolo de comunicação de desastres.

O QUE DEVE CONSIDERAR PARA A COMUNICAÇÃO DE DESASTRE

- Quem declara o desastre?
- Como são informados os colaboradores?
- Como vai comunicar com os clientes?

Uma vez definido o plano, é importante monitorizar e testar se a implementação foi feita com eficácia. Um erro comum nas estratégias de backup das empresas é não fazerem o teste dos backups. Depois, se ocorrer um ataques, só descobrem nessa altura que não conseguem recuperar os dados. Um plano de recuperação de dados deve ser testado regularmente e atualizado sempre que necessário. Uma vez desenvolvido um plano, não significa que seja eficaz, nem que não precisa de ser modificado.

PATCH MANAGEMENT

Considere como uma lei inviolável que deve fazer todas as atualizações, assim que são lançadas. Assim que um patch/update é disponibilizado e testado, deve ser aplicado para máxima proteção.

A vasta maioria dos updates são relacionados com segurança e têm de ser mantidos atualizados. Tecnologia desatualizada, especialmente os sistemas operativos (SO), é uma das fraquezas mais comuns utilizadas para ciberataques. Sem atualizações, está a deixar os browsers e outros softwares expostos a ransomware e exploit kits. Se os updates estiverem todos em dia, pode prevenir ataques extremamente dispendiosos. Por exemplo, em 2017, apenas 15% dos ficheiros do Windows 10 foram afetados por malware, já o Windows 7 teve 67% (dados do Webroot's 2018 Threat Report).

PROCESSO DE ATUALIZAÇÃO

O processo de atualização é um ciclo infinito e é uma boa prática para auditoria do ambiente existente através da criação de um inventário completo de todos os sistemas de produção utilizados, que torna o processo de atualização mais simples. Para além disso, determina as vulnerabilidades fazendo a comparação com as listas de inventário/controlo, separando as vulnerabilidades que afetam o sistema das que são inofensivas. Isto facilita às empresas a classificação e priorização das vulnerabilidades, uma vez que cada risco deve ser avaliado pela possibilidade da ameaça acontecer, pelo nível da vulnerabilidade e pelo custo da recuperação. Após determinação das vulnerabilidades mais importantes, deve ser desenvolvido e testado o patch, que deve ser, posteriormente, instalado sem quaisquer distúrbios ao funcionamento dos sistemas - um sistema de patch automatizado pode ajudar a realizar este processo.

Siga estas boas práticas e os MSPs poderão melhorar muito mais a sua prestação de serviços de segurança aos clientes, que cada vez mais precisam e exigem soluções eficazes. Não só poderá melhorar a relação com os clientes, mas também irá posicionar o MSP como player de elevado valor no mercado, alimentando o crescimento das empresas. A segurança é, realmente, um investimento que os MSP com olho para o crescimento não podem ignorar.