5 PONTOS

PARA AVALIAR A ESTRATÉGIA DE CIBERSEGURANÇA DAS PMEs

As PMEs portuguesas não estão a avaliar corretamente o risco associado à falta de cibersegurança.

Um estudo às PMEs, realizado por uma entidade de investigação independente, revelou que nos 24 meses precedentes 71% dos inquiridos sofreram uma fuga ou um ataque, que causou disrupção operacional, danos à reputação, perdas financeiras significativas ou eventuais multas por não cumprirem a legislação.

Em Portugal, a cibersegurança nas PMEs tem tido uma prioridade baixa no negócio e o investimento feito em segurança informática ainda é reduzido, criando falhas de segurança que podem levar a enormes prejuízos. Mesmo que isto possa ser, em parte, explicado pela menor capacidade financeira destas empresas para fazer face a uma política de segurança eficaz, claramente, as PMEs portuguesas não têm em funcionamento as tecnologias de segurança adequadas e não estão a avaliar corretamente o risco de cibersegurança.

É necessário melhorar a segurança nas PMEs. No entanto, o caminho não é fácil se tivermos em conta a falta de recursos humanos com competências técnicas em segurança, a falta de cultura analítica, o desconhecimento a nível dos dirigentes das PMEs e ainda a complexidade da implementação de uma estratégia a longo prazo, baseada em métricas.

Os 5 fatores fundamentais que deverá ter em consideração para avaliar a estratégia de cibersegurança nas PMEs, são os seguintes:

1 | UMA EQUIPA EXPERIENTE E COM COMPETÊNCIAS TÉCNICAS DEMONSTRADAS AJUDA, MAS É CARA

Embora a cibersegurança da empresa seja um esforço 24/7/365, que exige profissionais experientes, muitas das pequenas estruturas internas de segurança das PMEs não são, claramente, suficientes para lidar com os inúmeros alertas ou notificações e, muito menos, com investigação ou processos de remediação.

De facto, apenas 23% das PMEs inquiridas neste estudo planeiam juntar mais colaboradores às suas equipas de segurança no próximo ano. Para além disso, 87% destas empresas referiram ter dificuldades em manter os profissionais de cibersegurança e a tendência é para piorar.

Para preencher esta lacuna, as PMEs estão, cada vez mais, a recorrer a parcerias com prestadores de serviços de IT, MSP ou MSSP, para disponibilizarem uma alternativa, serviços de qualidade e os recursos necessários para proteger as suas organizações a qualquer hora.

87% das PMEs
tem dificuldade em
manter profissionais de
CIBERSEGURANÇA

SOLUÇÃO:
contratar serviços
GERIDOS DE SEGURANÇA

2 | OS EXECUTIVOS COMPREENDEM O QUE ESTÁ EM RISCO, MAS NÃO AS AÇÕES QUE DEVEM TOMAR

À medida que os ataques informáticos se tornam mais comuns, sofisticados, concentrados e planeados para agir de forma cirúrgica, cujas consequências apenas são agravadas pela implementação da nova legislação de proteção de dados, os dirigentes das PMEs estão a ficar mais atentos ao impacto que um incidente de cibersegurança pode causar e querem urgentemente reforçar a segurança da sua organização.

Contudo, identificar o problema é apenas o primeiro passo deste processo. Os executivos precisam de comunicar com os suas equipas internas de segurança, peritos na indústria e empresas de prestação de serviços, MSP, de forma a avaliarem o risco da sua organização e desenvolverem uma estratégia de cibersegurança a longo prazo, adequada e que se integre nos objetivos do seu negócio.

3 | A FORMAÇÃO SAT - SECURITY AWARENESS TRAINING - É MUITO ÚTIL, DESDE QUE SEJA BEM EXECUTADA

Neste estudo, 62% das PMEs revelaram que têm um programa SAT em funcionamento, mas destas, 50% disponibilizam o seu próprio SAT, isto é, utilizam metodologias e materiais produzidos internamente para a formação. Assim sendo, não é nenhuma surpresa que muitas empresas descrevam estes esforços como ineficazes.

As empresas de prestação de serviços (MSP), oferecem formação SAT abrangente e de elevada qualidade para uma grande variedade de ambientes regulatórios, tais como o GDPR. As PMEs que queiram reforçar a sua estratégia de segurança devem procurar um parceiro de prestação de serviços para Secure Awareness Training.

4 | SEGURANÇA SIGNIFICA PROTEGER HOJE O FUTURO

O futuro da arquitetura de IT abrange tanto a cloud pública, como a privada. Esta infraestrutura híbrida multi-cloud representa um desafio significativo para as PMEs que precisam de uma estratégia de cibersegurança multicamada e escalável.

As pequenas e médias empresas precisam de considerar e compreender estas tendências a longo prazo quando estão a avaliar a estratégia corrente de cibersegurança. Com este objetivo em mente, as PMEs podem recorrer aos MSP, que têm a experiência e ferramentas necessárias para proteger estes ambiente complexos.

5 | É NECESSÁRIA UMA ABORDAGEM DE SEGURANÇA BASEADA EM MÉTRICAS DE DESEMPENHO PARA ASSEGURAR A RESPONSABILIZAÇÃO

Para melhorar rapidamente o nível segurança na organização, as PMEs podem ser tentadas a cometer o erro comum de equacionar o montante gasto VS a proteção ganha. Ou seja, gastar sem uma estratégia, não é suficiente nem eficaz.

Para tirar o máximo partido do dinheiro investido, as pequenas e médias empresas precisam de criar um sistema de cibersegurança baseado em métricas quantificáveis. Novamente, esta é uma área na qual as PMEs devem fazer uma parceria com empresas de prestação de serviços especializadas nesta área.

É uma oportunidade para garantir, com indicadores KPI, que a estratégia de cibersegurança está a funcionar ao longo do tempo.

Os MSP podem ajudar as PMEs a definir as variáveis aplicáveis para as suas arquiteturas de IT, quer se trate da taxa de resposta a incidentes, do tempo de resposta ou de outras métricas relevantes.

Esta reavaliação estratégica da segurança da organização é uma tarefa complicada para qualquer organização, mas, sabendo os riscos que as PMEs enfrentam e a sua tendência para estarem pouco preparadas, é um desafio necessário.

Estes pontos são, sem dúvida, essenciais e as PMEs devem considerá-los para criar e/ou reforçar um sistema de segurança responsável e pensado para o futuro. Deve ter em atenção as vantagens de trabalhar em parceria com empresas de prestação de serviços MSP, para implementar o sistema de segurança mais acertado para a sua organização.

Se quiser saber mais sobre como as PMEs estão a abordar a cibersegurança, leia o relatório 'Security Services Fueling Growth for MSPs'.

ESTÁ INTERESSADO EM SABER MAIS SOBRE O WEBROOT?

Peça-nos uma demonstração da tecnologia EndPoint e DNS e da formação SAT através da consola de gestão centralizada GSM! Fale connosco em:

NEXT@MINITEL.PT

21 381 09 00

*Documento baseado no artigo 'Top 5 Things SMBs Should Consider When Evaluating a Cybersecurity Strategy', por Aaron Sherrill (Senior Analyst), da Webroot. Estudo realizado pela 451 Research.