

54% das empresas não têm software anti-ransomware

A Sophos (LSE: SOPH), líder global de segurança de rede e endpoint, refere no estudo “The State of Endpoint Security Today” que inquiriu mais de 2700 PME e chegou à conclusão de que 54% das empresas sofreram ataques de ransomware no último ano e não têm software anti-ransomware, bem como, 2/3 dos IT Managers não compreende o que é anti-exploit software. Este estudo independente foi conduzido pela empresa líder em investigação do Reino Unido, Vanson Bourne, e inquiriu 2700 IT Managers de organizações de 100 a 5000 colaboradores em 10 países e 5 continentes.

De acordo com este estudo, o ransomware continua a ser a principal ameaça às empresas, sendo que 31% das empresas inquiridas esperam ser vítima de um ataque de ransomware no futuro. Os três países mais atacados por ransomware



O ransomware continua a ser a principal ameaça às empresas, sendo que 31% das empresas inquiridas esperam ser vítima de um ataque de ransomware no futuro

são a Índia (67%), México (65%) e, por fim, os Estados Unidos da América (60%). O relatório detalha ainda os setores mais afetados por ataques de ransomware, que são a Saúde e Tecnologias (76%), seguida de Energia, Petróleo e Gás (65%) e Negócios e Serviços Profissionais (59%). “Uma das principais preocupações que os ataques de ransomware dão às empresas é o prejuízo. Este estudo apurou que 25% dos inquiridos estimam um cus-

to entre os USD \$13.000 e USD \$70.000 para resgatar um terminal afetado”, afirma Ricardo Maté, Country Manager da Sophos Ibéria, continuando a afirmar que “a outra preocupação que as empresas deverão ter é o facto de que, ao contrário do lightning, as empresas atacadas por ransomware poderão esperar um novo ataque no espaço de 12 meses com os prejuízos financeiros, técnicos e de negócio daí decorrentes”, conclui.

77% das organizações atacadas estavam a correr software de segurança atualizado

A prevenção de um ataque de ransomware é uma realidade, no entanto, há que ter em conta que a utilização de um software de segurança atualizada não é uma garantia para prevenir um ataque de ransomware. Isto só será possível com acesso ao um software anti-ransomware, sendo que 98% dos inquiridos reconhecem que a sua implementação é a única forma de prevenção de ataques.

O malware continuará a ser complexo e, com o tempo, a tendência é que os ataques bem como os cibercriminosos sejam mais complexos de detetar, prevenir e re-

O principal aspeto que qualquer organização deverá ter em conta é ter sempre o software de deteção atualizado e adaptado à realidade para o proteger

mediar. O principal aspeto que qualquer organização deverá ter em conta é ter sempre o software de deteção atualizado e adaptado à realidade para o proteger.