Ransomware, ter de pagar para aceder à sua informação?

Ruben Soares
Diretor Executivo da Samsys

Os ataques a sistemas informáticos têm-se tornado cada vez mais vulgares, havendo exemplos muito mediáticos como o ataque à Sony em 2011 ou ao *site* Ashley Madison em 2015. Nesses ataques o objetivo era a captura de dados sensíveis como a informação sobre cartões de crédito que depois seriam usados para burlas informáticas.

No entanto no início do mês de fevereiro, outro tipo de ataque teve algum destaque público. Foi o caso de um hospital americano que viu os seus sistemas informáticos serem atacados. Aqui os piratas não pretenderam capturar nenhuma informação específica mas antes bloquearam o acesso a todo o sistema informático e exigiram como resgate três milhões de euros, pagos em *bitcoins*, para voltar a dar acesso a esse sistema.

Numa altura em que quase todas as organizações dependem largamente de sistemas informáticos, este novo tipo de ataque, conhecido como *Ransomware*, tem um potencial de criar o caos nas empresas que ultrapassa o que passará a ser o pequeno inconveniente de ter um vírus no seu computador.

Infelizmente esta não é uma tendência que tenha demorado a chegar a Portugal e a Samsys teve já vários parceiros que foram atacados nos últimos dois meses por uma destas novas variantes, nomeadamente através do CryptoLocker, o que valida alguns estudos recentes, que indicam o nosso país como dos mais vulneráveis a este tipo de ataques.

É importante ter também em conta que o *Ransomware* neste momento afeta não só sistemas Windows mas também Apple, como o comprova uma situação que ocorreu neste primeiro trimestre com uma atualização de um dos *softwares* populares para Mac, o Transmission, e que estava infetado.

Ainda antes de referir a componente técnica, gostaríamos de ressalvar que é sabido que a componente social continua a ser das mais exploradas para conseguir levar a cabo ataques que põem em risco a segurança dos sistemas informáticos. Caricaturando, não vale a pena obrigar os utilizadores a terem *passwords* seguras se depois deixam a *password* escrita num *post-it* ao lado do computador. Para estas situações, pequenas sessões de formação são formas que costumam ter uma boa eficácia para promover a mudança de comportamentos.

Numa vertente mais técnica, e considerando que, atualmente, quase todos os colaboradores das empresas têm os seus próprios dispositivos, que têm capacidade para se ligar à sua rede interna, torna-se imperioso definir uma política de rede que contemple este conceito conhecido como "Bring your own device" (BYOD) e que pode passar por segregar o acesso desses dispositivos de forma a utilizarem recursos lógicos (*sofware*), ou mesmo físicos, diferentes dos que são usados por recursos efetivamente conhecidos pela organização.

Claro que esta política não pode estar só definida, tem que ser implementada e a sua manutenção tem que ser garantida ao longo do tempo, algo que normalmente só é compatível com a existência de competências técnicas deste nível dentro da empresa, seja permanentemente seja em regime de *outsourcing*.

Outra solução que recomendamos passa pela utilização de *software* de segurança específico para esta situação. Estamos a referir-nos a soluções de segurança que vão para além do antivírus empresarial ou da *firewall* e que contemplam já a abordagem necessária para lidar com o problema específico do *Ransomware*. Neste momento ainda não há muita oferta nesta área mas a experiência que temos tido tem sido promissora e, enquadrada com os outros procedimentos referidos, permite aumentar consideravelmente o nível de segurança da sua empresa.