É hora de pôr a cibersegurança na ordem do dia

dinheirovivo.pt/opiniao/e-hora-de-por-a-ciberseguranca-na-ordem-do-dia-14287562.html

5 de novembro de 2021

Recentemente, foi publicado um relatório com os resultados dos Inquéritos à Utilização das Tecnologias da Informação e Comunicação (IUTIC) na Administração Pública Central, Regional e nas Câmaras Municipais (2020).

Analisemos as principais conclusões:

A) Apenas "66% dos Organismos da Administração Central, 64% das Câmaras Municipais, 47% dos Organismos da Administração Regional dos Açores e 36% dos Organismos da Administração Regional da Madeira" tinham, no ano passado, uma estratégia definida e estruturada para a segurança da informação. Não está em causa, sequer, a qualidade dessa mesma estratégia. Se olharmos para os números de outra forma, o inquérito revela que pelo menos 34% e, nalguns casos, mais de metade dos organismos públicos em questão não tinham, qualquer tipo de estratégia a garantir a segurança da sua atividade, num ano em que foi absolutamente imperativo operar a 100% no digital e onde a taxa de (sucesso) do cibercrime cresceu abruptamente;

B) "A quase totalidade (98%) dos Organismos da Região Autónoma da Madeira e das Câmaras Municipais, 95% dos Organismos da Administração Pública Central e 86% dos Organismos da Região Autónoma dos Açores dispunham de firewall". Ora, mais uma vez, isto significa que, em pleno século XXI, nas estruturas do Estado, ainda existem organismos sem mecanismos de segurança tão basilares como sistemas de controlo de acessos - firewall - que, não sendo, de todo, infalíveis, não deixam de corresponder a uma primeira camada de segurança, que procura bloquear dados maliciosos. Numa analogia com a segurança física, seria a "porta de entrada" de casa no mundo cibernético;

C) Apesar de "a totalidade (100%) dos Organismos da Região Autónoma dos Açores", apresentarem boas práticas nos procedimentos (manuais e/ou automatizados) de atualização periódica do software, pelo menos três Câmaras Municipais, dois dos Organismos da Região Autónoma da Madeira e cerca de 21 dos organismos da Administração Central ainda não o faz. Esta, que é uma política de segurança algo, até, arcaica e fácil de implementar, tem uma importância extrema uma vez que a sua não implementação é uma das vulnerabilidades mais exploradas por cibercriminosos, nomeadamente no que respeita a vírus e exploração de vulnerabilidades aplicacionais;

D) 16% dos Organismos da Administração Central, 27% das Câmaras Municipais e 37% dos Organismos das Regiões Autónomas dos Açores e da Madeira não têm segurança de serviço de resolução de nomes (DNS). Esta é outra vulnerabilidade com consequências graves, já que permitirá, p. ex., efetuar os chamados ataques de interrupção de serviço (DDoS), responsáveis pelo bloqueio temporário de websites ou aplicações viradas para a

Internet, muitas vezes com consequências graves no que diz respeito à disponibilidade de serviços críticos (negócio ou institucionais), podendo mesmo colocar em causa a própria credibilidade da organização;

E) "Relativamente à disponibilização de recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC" - aquilo que, no âmbito dos nossos serviços, é tratado pela unidade de Compliance - os números são ainda mais preocupantes: quase metade dos organismos da Administração Pública Central e da RAA não o fez; já nas Câmaras a percentagem ascende a 62%, mas é na Madeira que o cenário é mais dramático (75%). Estes números vêm comprovar o nível ainda imaturo no que respeita à implementação de boas práticas de segurança, nomeadamente no que concerne a sua documentação, formalização e aprovação pela gestão, e por consequência, a divulgação interna do que a organização estipula como "regras" de segurança no meio digital;

F) Não é por isso de estranhar que "78% das Câmaras Municipais, 52% dos Organismos da Administração Pública Central, 45% dos Organismos da Região Autónoma da Madeira e 37% dos Organismos da Região Autónoma dos Açores," indiquem "ter elevada necessidade de reforçar competências em matéria de segurança das TIC", algo que não nos cansamos de defender como essencial para garantir que pelo menos a dimensão das pessoas, uma das mais frágeis na tríade da segurança (pessoas, processos e tecnologia), está minimamente preparada para operar neste mundo inegavelmente digital.

Neste sentido, o relatório em questão revela uma enorme fragilidade do Estado. E digo do Estado, no geral, porque temos trabalhado com várias Câmaras Municipais e algumas têm feito um esforço muito relevante para aumentar o seu nível de maturidade em segurança da informação, mas não deixam de estar de mãos atadas, em termos orçamentais, para puder chegar mais longe. Assim, é urgente colocar o tema digital nas agendas políticas com seriedade e sem subterfúgios. Os nossos governantes têm de promover urgentemente a delineação de uma estratégia articulada e transversal no que diz respeito à segurança da informação e disponibilizar fundos pois, no final do dia, é a própria reputação do Estado enquanto promotor de segurança que fica posta em causa.

CEO da VisionWare