| CLIPPING MIRANDA | | | |
|---|---|---|---|
| MEIO | Jornal Económico | | |
| Nº PAG. | 1 | DATA | 15 de maio de 2020 |

MIRANDA
Miranda & Associados Sociedade de Advogados, SP, RL


OPINIÃO

# Cibercrime e as vulnerabilidades do teletrabalho


**CATARINA VEIGA RIBEIRO**
Of Counsel na Miranda & Associados


O estado de emergência em que vivemos e o atual estado de calamidade que atravessamos provocaram um aumento exponencial dos ciberataques fruto do aproveitamento, por *hackers*, do evidente crescimento do trabalho remoto, perpetrando ilícita e "criativamente" nas empresas e na esfera individual dos teletrabalhadores. Fruto da ativação pelas empresas dos seus planos de contingência, colocando grande parte da sua força de trabalho em teletrabalho, as organizações e os indivíduos potenciaram os riscos da sua segurança, em virtude da constante presença de milhões de pessoas no mundo digital.

Assim, temos assistido a um aumento da utilização fraudulenta da aplicação MB WAY sendo recorrentemente denunciado o engano provocado por agentes que, com recurso a esquemas informáticos, pretendem obter ilícita e indevidamente valores monetários, por vezes de montante elevado. Ora, esta prática, com recurso ao engodo do visado, conduz-nos à hipótese da caracterização da conduta ao crime de burla cuja punibilidade pode ir dependendo do valor ilicitamente subtraído, até aos oito anos de prisão.

O aumento de mensagens contendo *malware* é outro tipo de ataque informático, perpetrado normalmente por via da difusão de emails, aos quais são anexados ficheiros dissimulados, contendo *malware*. O caso específico do *ransomware*, muito frequente, caracteriza-se pelo bloqueio total do computador da vítima, cujos dados ficam inacessíveis e, normalmente, são irremediavelmente perdidos, a menos que se pague um "resgate" ao atacante, o qual, em muito bom número de casos, é inconsequente (e portanto, a vítima fica sem os dados e sem a quantia que pagou...).

Dependendo da conduta do agente, equacionar-se-á, nestes casos, o preenchimento de diferentes tipos legais de crime: no caso de o agente bloquear o acesso total ao computador da vítima poderemos estar perante sabotagem informática, ou perante o crime de dano relativo a programas ou outros dados informáticos, se o dano ao programa se verificar. Estando associado um pedido de pagamento ao ataque, concorre com a conduta descrita também o crime de burla, podendo o agente ser punido pelos dois crimes.

Têm igualmente sido sinalizadas de forma crescente as mensagens de *phishing*, via email ou SMS. Tais mensagens, expedidas sempre para inúmeros destinatários, anunciam provir de bancos ou outras instituições credíveis no mercado (exemplificativamente, Apple, Netflix, Paypal, entre muitas outras) pressupondo pagamentos: o agente "finge" ser uma entidade bancária ou outra, e as mensagens que envia às quais associa o logotipo da instituição por forma a credibilizar a solicitação, imprimindo urgência, anunciam que o destinatário deve aceder a um link – que dá acesso a uma falsa página do banco ou instituição – e preencher os campos solicitados. Ora, é aqui que reside parte do engano para os desavisados, pois por razões de boas práticas e de segurança, os bancos, outras instituições e empresas não solicitam aos seus clientes ou utilizadores, por correio eletrónico, informação pessoal ou confidencial!

Poderemos estar, nestes casos, perante o preenchimento do tipo de crime de falsidade informática cumulando-se, novamente, o crime de burla se estiver associado a esta prática o pedido de entrega de montantes pecuniários. De igual modo, têm sido identificadas muitas situações de extorsão por via de correio eletrónico, cujo propósito é o de convencer os alvos a pagarem quantias monetárias, em *bitcoins*, sob a ameaça de divulgação pública de dados, imagens ou informações pessoais das mesmas.

Como nos casos anteriores, o processo passa pela expedição de mensagens de correio eletrónico para inúmeros destinatários, de forma indiscriminada, nas quais o remetente diz ser conhecedor da *password* de email da vítima, adiantando que, por essa mesma razão, logrou aceder ao computador daquela. Em regra, os remetentes destas mensagens obtiveram os endereços em listagens ilegalmente disponíveis na Internet.

É essencial ter consciência das vulnerabilidades cibernéticas principais, para antecipar ataques quanto à violação de dados, imagem e identidade da informação e, como tal, persistir quer com preocupação de encriptação dos dados, quer com níveis de alerta elevados que permitam inverter o registo ascendente do cibercrime dirigido, essencialmente, em linguagem menos técnica, a esquemas de fraude, chantagem e burla a fim de obter, maioritariamente, benefícios financeiros. ●