CARLOS F. SANTOS CARVALHO

ADVOGADO

MÊS: JANEIRO **CIRCULAR N.º 04/2016**

ASSUNTO: Só faltava mais esta!...
O perigo dos ataques cibernéticos.

Qualquer industrial/comerciante já tem que fixar a sua atenção, ao leme da sua Empresa, nas inúmeras escolhas (problemas) que diariamente aparecem no caminho. Nos últimos anos, multiplicaram-se os "avisos" sobre o perigo que representa a utilização da **aparelhagem electrónica**.

Os utilizadores, no que se incluem as Empresas, confiaram nos sistemas electrónicos. E, quanto mais a utilização de tais meios é feito pelas Empresas, --- até pela necessidade da indústria e do comércio ---, as ameaças e os ataques bem sucedidos, aumentam. E, a complexidade das ameaças é uma referência sempre em aumento entre os cibercriminosos.

O que alguém já apelidou de **"carteirismo digital"**, organizou-se em grupos, que actuam a nível nacional e internacional.

Naturalmente, não temos o mínimo de conhecimentos para descrever os perigos e os processos que estão em curso no campo do cibercrime. Mas, uma coisa é certa, na nossa opinião: o contra-ataque à ameaça do cibercrime tornou-se, ela própria, um "negócio". Dados, naturalmente desactualizados e referidos ao ano findo, referem que, a nível mundial, existe um défice de mais de 2 milhões de **"profissionais de segurança"**. Quer dizer, uma nova profissão, os "profissionais de segurança", está em expansão em todo o mundo. Naturalmente, são indivíduos altamente qualificados, que se pagam muito bem! – Tornaram-se "necessários"...

É mais um custo para as Empresas. Um grande custo. Contudo, ignorar o problema pode ter ainda custos maiores. E, segundo lemos, a sofisticação das tácticas e da própria tecnologia empregue pelos cibercriminosos superam a capacidade de resposta dos departamentos de TI e profissionais de segurança. E,

Não esquecendo que **os próprios Estados** se guerreiam entre eles, aqui em escala que nem sequer o cidadão comum se atreve a imaginar. Ainda recentemente surgiu um problema desses entre os EUA e a China. A nível mais baixo, a indústria química; a farmacêutica e o sector electrónico são os que apresentam mais incidências de ameaças. Mas, **nada está imune**, sento detectados ataques no sector agrícola, mineiro, energia, etc.. Claro, numa pequena economia a nível mundial, como a portuguesa, a escala e os campos de ataque adaptam-se a essa economia. Os ganhos podem ser menores, mas o estragos para os visados podem comprometer

PR. GEN. HUMBERTO DELGADO, N.º 287, 5.º ESQ. – SALAS 65 A 67, 4000-288 || TELF.: 222 005 332 || FAX: 222 088 321
carlosfsantoscarvalho-1417p@adv.oa.pt

irremediavelmente qualquer Empresa. E, aqui, a grandeza da Empresa não se fixa em número de empregados; mas, nos números dos resultados financeiros.

Neste submundo do crime até já criaram moeda própria. Ficou mais conhecido o **"Bitcoin"**. A última, mais sofisticada, dá pelo nome de MUSD. Ora,

Tudo isto vem a terreiro porque, recentemente foram publicados **dados sobre Portugal**, que devem ser tidos em atenção. Não sabemos se são verdadeiros, se inflacionadas pelo **"loby"**, --- que certamente já existe... ---, da "segurança informática". Embora se diga que há um défice desses técnicos, o certo é que já movimenta muita gente "interessada"; e, muito dinheiro!

Aqui vão alguns números, que vieram a público:

— em Portugal, e isto em relação a 2014, --- pelo que é de pressupor que no ano que findou, 2015, se agravou ---, **23% das empresas portuguesas foram alvo de um ataque cibernético**. Em relação ao resto da Europa, 28% das Empresas atacadas, o nosso número é menor; pouco menos;

— em Portugal, números de 2014, 64% das empresas portuguesas estão ignorantes do problema, ou tem um conhecimento básico ou limitado sobre a sua exposição ao risco cibernético;

— em Portugal, as ameaças daquele risco **podem provir de três fontes**, principais:
  a) - com origem em criminosos informáticos, conhecidos por "hackers", em 40%;
  b) - de origem nos próprios colaboradores da Empresa, dita ameaça interna, em 30%; e, por fim, em erros inadvertidos, operacionais, em 30%.

e, tal como no resto da Europa, o pior risco e ameaça é sobre **a informação sobre os Clientes**. Claro, mais grave, mas menos frequente, --- apenas porque mais difícil para os criminosos ---, o ataque aos segredos da indústria. Seja qual for o alvo, o impacto financeiro pode ser muito grave.

Claro, e aqui entram os segundos "beneficiários" da situação: a indústria de seguros. Este campo de negócio (oportunidade) está em crescente. E, aqui, mais um dado sobre a situação em Portugal:

— 90% das empresas portuguesas não tem conhecimento; ou, um conhecimento suficiente sobre o chamado "seguro cyber". E, só 10% tem um seguro destes que, contudo, apenas responde a um número limitado de necessidades da sua Empresa.

Lembramos: o anterior Governo, XX, publicou no D.R. n.º 113, 12 Junho 2015, a **RESOLUÇÃO do Conselho de Ministros n.º 36/2015**, que tem em Anexo a Estratégia Nacional de Segurança do Ciberespaço. Chamamos a especial atenção para o "Eixo 3"; "Eixo 4"; e, "Eixo 5". Por favor, dê uma leitura, mesmo rápida.

Tire do que aqui consta a informação que considerar útil. E actue em conformidade.

Carlos F. Santos Carvalho

PR. GEN. HUMBERTO DELGADO, N.º 287, 5.º ESQ. – SALAS 65 A 67, 4000-288 || TELF.: 222 005 332 || FAX: 222 088 321
carlosfsantoscarvalho-1417p@adv.oa.pt