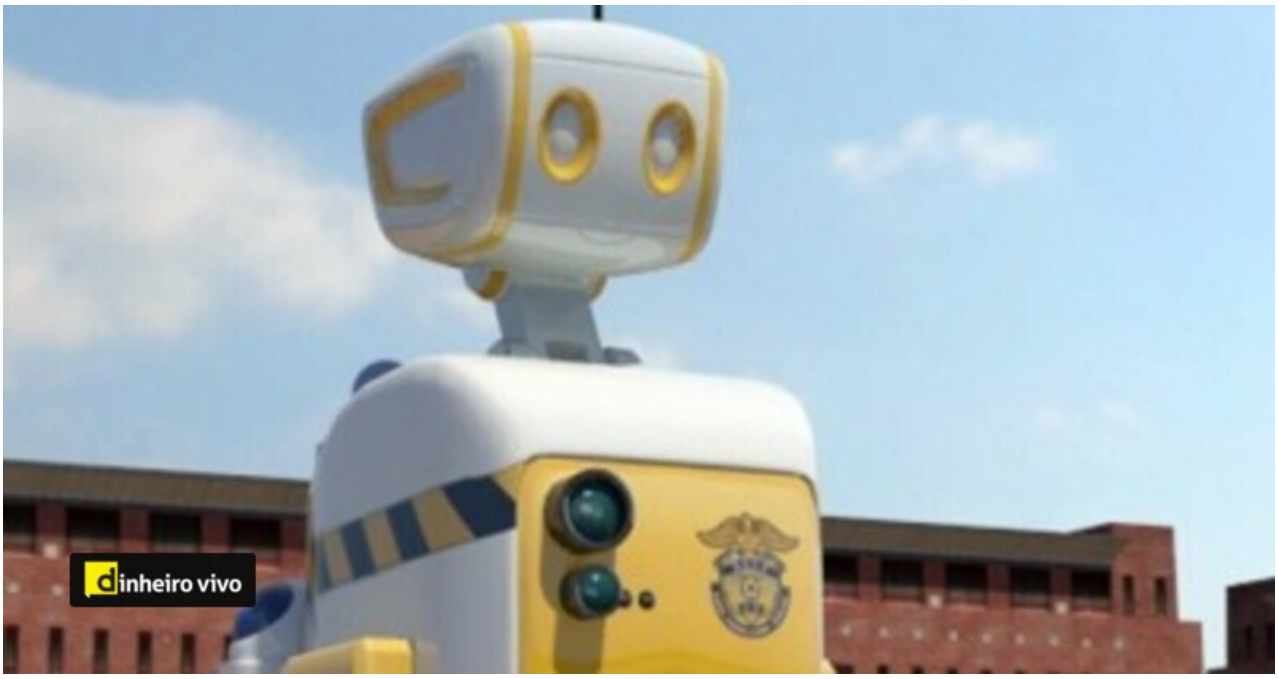
# Cibersegurança: retrospetiva 2019

dinheirovivo.pt/opiniao/ciberseguranca-retrospetiva-2019-12685337.html

20 de dezembro de 2019




**Neste que é o último artigo de opinião do ano de 2019, proponho-me a fazer uma análise retrospetiva ao que foi o último ano em termos de segurança cibernética no mundo atual.**

Comecei o ano por partilhar com os leitores um estudo do Pew Research Center (Washington) que considerou os ciberataques – perpetrados por outros países - como fazendo parte do top 3 das ameaças globais, a par das alterações climáticas e terrorismo islâmico. Esse relatório não podia ditar melhor aquilo que foi o ano 2019. Afinal, hoje podemos dizer sem dúvidas que o ciberespaço é um território de atuação como qualquer outra geografia e que os atores estatais exploram assumidamente as suas ferramentas para agir no mundo e se posicionarem.

Com alguma satisfação, assisti a uma mudança na perceção dos meios de comunicação sobre o tema da cibersegurança, já que tem vindo a dar-lhe cada vez mais cobertura, algo que tem ajudado a reconhecer a sua importância para a vida quotidiana e, por consequência, a "mudar mentalidades" na sociedade em geral. Vejam-se alguns exemplos:

Ao contrário, a discussão em torno da segurança do 5G, um dos tópicos quentes de 2019 foi, no meu entender, excessiva. Por esse motivo, em março, procurei chamar à atenção para um outro aspeto conexo que me parece bem mais relevante que é o da "Internet das Coisas" (*Internet of Things*). Num mundo que se pretende cada vez mais *smart* e no qual a sociedade - através de cada vez mais pessoas, cada vez mais cedo, cada vez em mais momentos (social/profissional) e cada vez até mais tarde - está ligada, o que é realmente novidade é a popularização de um sem-número de dispositivos "não-tradicionais", que alargam ainda mais o espetro da interconexão global, e por consequência direta, também

aumenta o risco no que respeita a cibersegurança: *smart watches, smart toys, smart TVs, smart robots, smart houses*... E já que nos encontramos à porta de uma época festiva, se pretende adquirir este tipo de produtos, não posso deixar de apelar para que haja uma reflexão consciente sobre qual a sua real necessidade e pertinência. O mundo dos gadgets é interminável, mas tem consequências sérias no que respeita à nossa privacidade e segurança.

Houve um assunto, no entanto, a que não foi dada a devida importância – no meu entender - e sobre o qual continuarei definitivamente a insistir, que é o da essencialidade da segurança nas infraestruturas críticas. No primeiro semestre, destacámos o caso do transporte aéreo e do setor da saúde, mas existem muitos outros, responsáveis pela "estabilidade" do dia-a-dia em sociedade, como os setores da energia, águas ou comunicações, sobre os quais é urgente refletir. Estou convicto de que haverá uma escalada de ataques a estes setores, como nos demonstram as tendências internacionais, pelo que merece ser tratado com real preocupação e ponderação. Aliás, o ataque de ransomware à Câmara Municipal de Vinhais em outubro, sobre o qual tivemos oportunidade de escrever é apenas mais uma prova disso mesmo.

Outro aspeto que marcou o último ano e que está diretamente ligado à cibersegurança é o da privacidade. A consolidação do Regulamento Geral de Proteção de Dados, como fizemos questão de notar, pela altura do seu primeiro aniversário, foi determinante. Por isso, repetimos, o RGPD deve ser encarado como um "movimento global" de capacitação das empresas e indivíduos em temas profundamente sensíveis como são a privacidade, a cibersegurança ou a proteção de dados, em vez de ser tido como "complicador de negócio" ou "monstro das coimas".

Os *databreaches* (perda de dados) são um fenómeno que resulta, em boa parte, da ausência de boas políticas de privacidade e proteção de dados e têm uma imensa gravidade já que, entre outros, servem de matéria essencial para a disseminação de campanhas de phishing que, como temos vindo a dizer, assolam dramaticamente Portugal.

Por fim, e em modo de resumo, podemos confirmar que 2019 foi um ano de complexificação do cibercrime. Não pude deixar de partilhar na altura, a minha surpresa com a evolução que o ataque informático teve em termos de sofisticação e eficiência, nomeadamente no que envolve a "fraude" e o "roubo". O cibercrime está cada vez mais orientado a ataques cirúrgicos com o objetivo de angariar dinheiro.

Num artigo que aqui publicámos com o intuito de explicar aos empresários como responder a um ciberataque, dizíamos que *a organização tem de ser capaz de avaliar regularmente o seu nível de segurança interno, através de auditorias, definir e implementar políticas de segurança que minimizem riscos na comunidade de colaboradores ou parceiros e, por fim, ser capaz de sensibilizar os seus colaboradores para o tema da segurança da informação.*

Todos os dias, enquanto profissionais de cibersegurança, temos de nos reinventar para dar resposta a uma realidade que corre demasiado rápido, conscientes de que as soluções, apesar de igualmente complexas, existem.

A retrospetiva é essencial para orientar o futuro, corrigir erros e acompanhar a velocidade a que o mundo digital se move. Cá estaremos para o ano, para continuar a refletir sobre este tema que, quer queiramos quer não, é já parte de nós. Até lá!

*Bruno Castro é CEO da VisionWare*