manchete

Jornal Negócios	Periodicidade: Diário
	Classe: Economia/Negócios
19-11-2021	Âmbito: Nacional
	Pagina(s): 1,31

PEDRO DUARTE

O espaço cibernético é um campo de batalha geopolítica

OPINIÃO 31

manchete

Jornal Negócios

19-11-2021

Periodicidade: Diário
Classe: Economia/Negócios
Âmbito: Nacional
Pagina(s): 1,31

NA NUVEM

O outro vírus que nos ataca

PEDRO DUARTE
Quadro da Microsoft e presidente do Conselho Estratégico da Economia Digital da CIP

O tema da cibersegurança assume uma relevância acrescida em 2021, na medida em que o crime cibernético se tornou mais sofisticado, mais disseminado e mais nocivo.

A pandemia continuou a trazer novos desafios, aproveitados por "hackers" que beneficiaram da inesperada sobrecarga de trabalho sobre as equipas de segurança para lançar novos ataques. Estas ofensivas criminosas tiveram como alvo infraestruturas críticas, na área da saúde, nas tecnologias de informação, nos serviços financeiros ou no setor energético, com golpes que paralisaram empresas e prejudicaram consumidores.

De igual modo, os ataques de "phishing" sobre colaboradores de empresas atingiram taxas alarmantes. E, de acordo com o Gone Phishing Report 2020, não são apenas as organizações menores e com poucos recursos que estão em risco. Empresas e agências mais sofisticadas e bem equipadas provaram ser ainda mais vulneráveis.

No mesmo sentido, a Microsoft publicou recentemente o seu Digital Defense Report. Com base em mais de 24 biliões de sinais de segurança diários, geridos por mais de 8.500 especialistas em segurança em 77 países, este relatório divulga relevantes dados sobre o estado de evolução do ransomware, dos emails maliciosos, do malware e de outras técnicas. Em paralelo, dedica um capítulo aos denominados "nation state threats", ou seja, a ataques promovidos, patrocinados ou encobertos pelos governos de determinados países.

Aí se analisam detalhadamente as ameaças cibernéticas observadas entre julho de 2020 e junho de 2021. Nesse período, 58% de todos os ataques com a marca de Estados-nação vieram da Rússia, apesar de também se identificar forte atividade por parte da Coreia do Norte, do Irão e da China. Cerca de 21% destes ataques foram direcionados aos consumidores e 79% às empresas.

Um exemplo concreto dá pelo nome de Nobelium, um grupo de base russa que esteve na origem do ataque aos clientes da SolarWinds em 2020 e que o governo norte-americano identificou como um braço dos serviços de inteligência russos. Esta organização criminosa tenta penetrar nas cadeias de fornecimento de tecnologia, através de empresas que implementam e gerem serviços na nuvem, ganhando assim acesso à rede de clientes dessas empresas. Desde o verão deste ano, nota-se uma onda crescente de atividade da Nobelium, o que pode ser interpretado como um indicador de que a Rússia está a tentar obter um acesso mais sistemático e de longo prazo às cadeias de valor de tecnologia e estabelecer assim um mecanismo de vigilância, agora ou no futuro, sobre alvos de interesse para o seu governo.

O espaço cibernético é, na verdade, também um campo de batalha geopolítica.

Apesar destes sinais que nos devem alertar para a dimensão dos riscos em causa, há tendências positivas que devem ser celebradas: por um lado, os governos estão a tomar consciência da relevância do tema, aprovando novas leis, alocando mais recursos e reconhecendo o crime cibernético como uma ameaça à segurança nacional. Assim como os profissionais e cidadãos em geral começam a adquirir saudáveis hábitos de higiene cibernética básica, aplicando patches de segurança e atualizando software e aplicações. Há hoje uma consciência mais efetiva de que, num momento em que surgem novas vulnerabilidades, a segurança como prioridade de todos é essencial para o sucesso das organizações e para a estabilidade comunitária. ■

Coluna quinzenal à sexta-feira