24.05.2024

Diretor
Filipe Alves
Subdiretores
Lígia Simões,
Nuno Vinha
e Ricardo Santos
Ferreira

Special Report
Cibersegurança

Caderno publicado como suplemento do Jornal Económico nº 2251. Não pode ser vendido separadamente.

Os desafios da Cibersegurança na Era da Inteligência Artificial

■ A Inteligência Artificial generativa traz numerosas oportunidades para os cidadãos e as empresas. Vamos poder trabalhar de forma mais eficiente e muitas das tarefas que hoje ocupam o nosso tempo passarão a ser automatizadas. Mas há também riscos no horizonte, em termos de cibersegurança. Leia a nossa análise a opinião dos especialistas.

O papel essencial da cibersegurança num mundo que está cada vez mais digitalizado

Análise ■ P.10

Próximos anos deverão assistir a ataques informáticos cada vez mais sofisticados

Futuro ■ P.12

Bruno Castro,
CEO da VisionWare
"A Cibersegurança saiu das catacumbas do I.T."

Evento ■ P.00

Os algoritmos como braço direito dos profissionais de segurança online

Fórum ■ P.12-15

“Elo mais fraco” da cibersegurança ainda são as pessoas? Opinião divide-se

Conferência ■ Pequeno-almoço de debate, organizado pelo JE, pôs em discussão o fator humano nas falhas de segurança informática das organizações. Especialistas dividem-se entre a necessidade constante de formação das pessoas e a ideia de que esse argumento já é obsoleto.

Inês Amado, Mariana Bandeira e Rodolfo Alexandre Reis
iamado@medianove.com

O tema da cibersegurança “deixou de pertencer às catacumbas do IT”, defendeu o CEO da VisionWare, Bruno Castro, num pequeno-almoço de debate organizado pelo Jornal Económico (JE), que reuniu, na terça-feira, vários responsáveis da área. De acordo com o executivo, os modelos de Inteligência Artificial (IA) tornam as ameaças cibernéticas mais complexas. “Dispara, avança, afina os conteúdos e tenta novamente”, disse, analisando o alcance do modelo que está por detrás no funcionamento das aplicações de encontro, entre outros exemplos. Como explicou Bruno Castro, os algoritmos baseados em IA geram conteúdo personalizado para melhorar os *malwares* e, consequenetmente, os ciberataques, uma vez que vão recolher informação à vida do utilizador, das credenciais do Badoo ou do Tinder até às subscrições dos jornais, por exemplo.

No entanto, há boas notícias. Bruno Castro considera que a questão de “porque é que a segurança é risco para o negócio” deixou de ser um tema, porque a liderança está devidamente envolvida. Segundo Bruno Castro, o cibercrime tem um modelo de negócio maduro e altamente rentável.

Por sua vez, Luísa Ribeiro Lopes, presidente do conselho diretivo do .PT, alertou para a premência da capacitação dos trabalhadores pelas empresas neste domínio, sobretudo daqueles que as lideram. “Qualquer organização tem de capacitar os seus colaboradores, a começar pelo *board*”, afirmou a mesma responsável, enquanto oradora convidada do evento *Special Report* sobre Cibersegurança. A coordenadora-geral do INCoDE.2030 entende que, apesar de hoje as organizações estarem dotadas de sistemas sofisticados para lidar com ataques de cibersegurança, a capacitação dos funcionários neste campo é inferior à desejável. “Quando hoje falamos de cibersegurança, estamos a falar de competências. Hoje temos à nossa disposição alguns dos melhores sistemas para fazer face a este desafio que todas as organizões têm. O que não temos é a capacitação das pessoas”, analisou, no painel intitulado “Desafios da Cibersegurança na Era da Inteligência Artificial”.

Em Portugal, cerca de 56% das empresas não recorrem a soluções de cibersegurança com capacidade de Inteligência Artificial, concluiu a Microsoft Portugal num dos mais recentes estudos. 62% das empresas nacionais já utiliza IA e 25% ponderam usar esta ferramenta nos próximos 24 meses.

Na visão da presidente do conselho diretivo da entidade responsável pela gestão, registo e manutenção de domínios sob .pt, por um lado, é necessário mais “profissionais para fazer face aos ataques” e, por outro, formar os quadros já existentes. “As pessoas dentro das organizações não têm essas competências”, insistiu. “As empresas muitas vezes não estão atentas. O elo mais fraco são as pessoas. É por aí que entram a maior parte dos ataques”, continuou Luísa Ribeiro Lopes, defendendo uma ideia que encontrou resistência por parte de Bruno Castro. Nas palavras do CEO da Visionware, trata-se de “só mais um risco com o qual temos de trabalhar”. Na opinião do responsável da tecnológica nacional, a maior crise cibernética dos últimos tempos foi a Covid-19, que colocou as pessoas fora do seu ambiente de segurança e levou a erros. Segundo Luísa Ribeiro Lopes, a capacitação dos líderes das empresas devia ser prioritário na agenda das organizações, defende, pela “questão da continuidade do negócio”, entre outras razões. “Se um gestor/CEO de uma empresa não tiver como principal preocupação a cibersegurança, alguma coisa não está bem”, analisou, levando ao debate números sobre as principais preocupações dos gestores. “Mais de 60% dos gestores ouvidos no ano passado disseram que o que mais receiam é um ataque à sua organização, pelos danos à reputação e ao próprio negócio”, afirmou. É esperado que, nas grandes empresas, os conselhos de administração venham a ter como requisito, nos próximos cinco anos, pelo menos, um membro especialista em cibersegurança. “Nas pequenas empresas, quem está à frente tem de ter conhecimento e estar atento a esta área”, alertou. Luísa Ribeiro Lopes saudou a integração crescente destes temas - cibersegurança e inteligência artificial - a nível da União Europeia, como os debates dos últimos dias para as eleições europeias demonstraram. “Em termos de competências digitais, se olharmos para a década digital, vemos como a importância da capacitação” está tão presente até 2030, afirmou.

Do lado da Microsoft Portugal, o diretor nacional de segurança da gigante tecnológica, Luís Rato, alertou para a importância da criação de “condições para ter segurança para a Inteligência Artificial e Inteligência Artificial para ter segurança”. Em Portugal, cerca de 56% das empresas não utilizam soluções de

Assista ao programa no seu smartphone através deste QR Code ou em www.jornaleconomico.pt

Bruno Castro
CEO da Visionware

Luís Rato
Diretor de Segurança Microsoft

Luisa Ribeiro Lopes
Presidente do .PT

cibersegurança com capacidade de Inteligência Artificial, concluiu a Microsoft Portugal num dos mais recentes estudos. Segundo Luís Rato, 62% das empresas nacionais já utiliza IA e 25% ponderam usar esta ferramenta nos próximos 24 meses. "Tudo isto também vem trazer um conjunto de desafios", referiu ainda o dirigente, dando conta de que um outro estudo feito pela Microsoft Portugal sobre a taxa de maturidade das empresas portuguesas sobre a cibersegurança indicou que 185 empresas, 50% já tinham feito investimentos significativos nessa área.

Papel da IA contra ciberameaças

Em declarações ao JE, à margem do evento, Bruno Castro defendeu a IA como uma "ferramenta poderosa para a deteção proativa de ciberameaças", dada a capacidade de análise de grandes quantidades de dados em tempo real, de identificação de padrões e adaptação a outros cenários "A IA possibilita a monitorização e alerta de qualquer desvio de comportamento fora no comum dentro dos utilizadores de uma rede", explicou, acrescentando que é esse desvio que pode revelar "uma possível ameaça". "Além da análise de comportamento, os algoritmos de Processamento de Linguagem Natural (NLP) conseguem analisar mensagens e conteúdos escritos, identificando possíveis ameaças em emails, mensagens instantâneas e outras formas de comunicação, além da sua capacidade de identificar padrões associados a malware". Segundo Bruno Castro, esta tecnologia é também utilizada "para integrar e correlacionar informações provenientes de várias fontes, incluindo feeds de inteligência de ameaças ou na identificação de padrões/tendências que indiquem atividades maliciosas".

Como explica o CEO da Visionware, a utilização proativa da IA permite antecipar e dar responder a "ameaças emergentes, minimizando o potencial impacto dessas mesmas ameaças, evitando sérios danos". "Importa ainda ressaltar que a incorporação eficaz da IA na cibersegurança requer uma abordagem estratégica de governação". O executivo da tecnológica portuguesa alertou, também, para algumas das principais ameaças que acontecem atualmente com o uso da IA, como as técnicas *deepfake*. "Hoje em dia bastam três segundos de uma *sample* para modificar a voz de uma determinada pessoa. É difícil combater isto, implica do ponto de vista de engenharia e indústria de repensar todo este modelo", sublinhou, colocando alguma responsabilidade nas empresas quanto ao papel de mitigação. Segundo Bruno Castro, as organizações devem ter no seu programa de segurança o treino das pessoas.

Grupo de oradores e moderadores do debate sobre cibersegurança, que antecedeu a publicação deste 'Special Report'

Em todos os pequenos-almoços executivos do Jornal Económico há um espaço de leitura da última edição que está nas bancas

Participantes aguardam intervenções de Bruno Castro, Luísa Ribeiro Lopes e Luís Rato

O evento teve início por volta das 8h30 e terminou pelas 10h30 após um espaço de perguntas e respostas do público

José Carlos Lourenço, CEO e presidente do conselho de administração da Media9, faz a sessão de boas-vindas à audiência que está no Hotel Intercontinen-tal ou acompanhará através de 'streaming'

A era do investimento em sistemas de Inteligência Artificial também altera negócio da segurança informática