OPINIÃO

‘ML’, uma arma na identificação das ameaças

RICARDO DINIS
Diretor ITS, Agap2IT

A cibersegurança tornou-se uma prioridade para todas as organizações. O número de ataques está na ordem dos milhares de milhões e o crescimento previsto é exponencial.

Os produtos de segurança atuais focam-se em perceber como funciona um malware ou um ataque e, na sua maioria, operam na prevenção de intrusão.

Trata-se de um contexto em que os atacantes só precisam de acertar uma vez, mas as equipas de segurança das organizações têm de acertar constantemente. Na prática, as organizações estão sempre um passo atrás dos atacantes.

Nos últimos anos temos visto um crescimento nas tecnologias de inteligência artificial (IA) para as organizações, capazes de responder aos principais desafios do mundo dos negócios. A maior parte delas pode ser atribuída aos avanços no poder computacional, big-data, à computação distribuída e ao uso da Cloud.

O uso de aprendizagem automática (ML), ramo da IA que permite a emulação do cognitivo humano, para a automatização da deteção e resposta de ataques retira esse fardo aos humanos. E será, potencialmente, mais eficiente a identificar as ameaças, do que uma abordagem baseada na análise de comportamentos executada por humanos com a ajuda de software especializado.

Produtos de ciber-deteção e implementações de segurança multicamada baseados em IA, criam incerteza para os atacantes e podem, de uma forma automática, detetar, analisar e defender contra os ataques avançados detetando e enganando os invasores.

Quando se combinam profissionais de segurança com qualidade e capacidade, com tecnologias adaptativas, que mudam e ficam mais inteligentes ao longo do tempo, é criada uma oportunidade de vantagem que não existe nas tecnologias de cibersegurança de hoje em dia.

IA e ML podem oferecer vantagens na proteção de dados sensíveis e sistemas chave. Mas, como qualquer outra inovação, estas tecnologias também estão hoje em dia a ser usadas para alavancar os próprios ataques pelo lado dos hackers do mal.

E o processo de aprendizagem supervisionada, necessário à aprendizagem automática na área da segurança, é ainda suscetível ao erro humano pela possibilidade de catalogar indevidamente o código.

Cria-se uma falsa sensação de segurança, problema que tem sido contornado pelo uso de múltiplos algoritmos e conjuntos de dados, fazendo com que se um algoritmo for comprometido, os resultados dos seus pares irão evidenciar a anomalia.

O desafio primário da cibersegurança para as organizações B2B e B2C tem sido a mudança constante da escala dos ataques. A natureza desta mudança é, no entanto, previsível e segue padrões, o tipo de problema onde o uso de IA e ML se destaca e abre novas oportunidades.

Produtos de ciber--deteção e implementações de segurança multicamada baseadas em IA criam incerteza para os atacantes e podem, de uma forma automática, detetar, analisar e defender contra os ataques avançados detetando e enganando os invasores

ESTUDO DA EY

Colaboradores descuidados são fonte de vulnerabilidades mais perigosas

34% das empresas e organizações inquiridas no âmbito o EY Global Information Security Survey 2018-19 colocam os descuidos internos à cabeça das vulnerabilidades.

MAFALDA SIMÕES MONTEIRO
mmonteiro@jornaleconomico.pt

Um ano depois de várias empresas e organizações mundiais terem sido abaladas por falhas de cibersegurança à escala global, esta questão ganha importância na agenda dos decisores. No entanto, há muito caminho a percorrer, considerando o cada vez maior poderio dos ciberataques, alguns dos quais poderão até ser patrocinadas por Estados. Tudo isto é certo, mas, o EY Global Information Security Survey 2018-19 divulgado esta quarta-feira reconhece que as vulnerabilidades mais perigosas numa empresa ou organização estão relacionadas com colaboradores descuidados (34%).

Em segundo lugar surgem os controlos de segurança ultrapassados (26%), em terceiro, o acesso não autorizado (13%), seguindo-se elementos relacionados com utilização de computação em nuvem (10%).

Apenas 8% referem que as funcionalidades de segurança respondem às suas necessidades e 38% dos inquiridos assumem não conseguirem provavelmente descobrir uma violação de segurança mais sofisticada. De resto, menos