Ameaças aumentam e cibersegurança deve estar no topo das prioridades

Ciberataques ■ A banca, em Portugal e não só, trabalha com um grau de digitalização maior a cada ano que passa. As vantagens são muitas mas, em paralelo, surgem ameaças que já atingiram quase nove em cada 10 operadores.

Tomás Gonçalves Pereira
tpereira@medianove.com

As ameaças cibernéticas estão cada vez mais presentes no mundo digital e a banca não foge à regra. Os dados recolhidos pelo Centro Nacional de Cibersegurança (CNCS) indicam que, entre os Operadores de Serviços Essenciais (OSE), é no setor da banca que mais empresas (88%) já sofreram incidentes ligados à segurança (dados gerais apontam para 29%).

São também 88% os operadores da banca que destinam uma parte do seu orçamento especificamente à cibersegurança (34% na média dos setores). Em causa está a importância de garantir a confiança dos clientes, que sustenta todo o sistema bancário. Ainda assim, os níveis de exposição ao risco continuam elevados, de tal modo que o número de crimes informáticos (contra empresas da totalidade dos setores) aumentaram 13% em 2023, já que as autoridades policiais portuguesas registaram 23.221 casos.

É neste âmbito que entra em cena o pacote legislativo relativo à resiliência operacional digital do setor financeiro (DORA). Trata-se de um regulamento europeu que se afigura como determinante para a banca na Europa. Foi publicado pela UE com o propósito de criar ferramentas normativas que permitam contribuir para mitigar os riscos existentes. Tendo isto em vista, a UE exige o desenvolvimento de TIC que permitam fazer face às ameaças.

De resto, o Banco de Portugal emitiu, em janeiro, um comunicado no qual esclarece que a lei visa "harmonizar tipologias de entidades e Estados-membros e aumentar a exigência dos requisitos de resiliência operacional digital". pode ler-se. Trata-se de um regulamento que surgiu aliado a outros, como é o caso do MiCA e do DLT, duas diretivas também destinadas a fortalecer o segmento das finanças digitais.

Para aprofundar esta matéria, o JE contactou Bruno Castro, fundador e CEO da VisionWare, empresa portuguesa especializada em segurança da informação e cibersegurança, que se foca na identificação e mitigação de ameaças digitais.

Que riscos mais preocupam e porquê?

A cibersegurança deixou de ser uma opção para se tornar uma necessidade estratégica, dada a crescente sofisticação e complexidade dos ataques cibernéticos. Entre as (ciber)ameaças que mais preocupam, destacam-se os ataques de ransomware, que têm vindo a aumentar significativamente, afetando todo o tipo de setores.

Soma-se a crescente proliferação de desinformação com recurso a IA. Os atacantes, muitas vezes organizados em redes criminosas, utilizam técnicas inovadoras e formatos de dispersão dentro das organizações, tornando esses ataques altamente disruptivos e difíceis de prevenir. Os ataques a infraestruturas críticas e a exploração de vulnerabilidades em sistemas críticos para a atividade da organização, acrescidos da tentativa constante e acentuada de ataque direcionada às pessoas como forma de comprometer as organizações, são algumas das principais preocupações. Essas ameaças são particularmente alarmantes devido ao seu potencial disruptivo e à crescente sofisticação da comunidade cibercriminosa. Além disso, a complexidade e a frequência dos ciberataques têm aumentado, exigindo um esforço significativo na prevenção e resposta.

BLOOMBERG

A digitalização cresce a olhos vistos no segmento dos serviços, pelo que a banca não quer fugir à regra. Num setor que vive da confiança dos clientes, as falhas de segurança representam uma ameaça séria.

Que ilações há a tirar dos ataques informáticos anteriores, para que a prevenção possa ser melhor no futuro?

A análise do contexto cibernético, nomeadamente no que respeita ao sucesso dos ciberataques mais recentes, revela algumas lições cruciais. A primeira é que muitas organizações ainda falham em assumir a cibersegurança como um pilar do seu negócio. Este tem de estar na ordem do dia de qualquer conselho de administração, só assim permitindo adotar práticas de segurança cibernética abrangentes e bem estruturadas, de acordo com o seu negócio.

As organizações precisam evoluir as suas estratégias de defesa para serem mais proativas, investindo em tecnologias de deteção e resposta a incidentes, além de promoverem uma cultura de segurança de informação e, por fim, prepararem-se para quando for a sua vez de serem vítimas, serem capazes de recuperar o mais sustentada e rapidamente possível.