Jornal Económico
11.02.2022
P.01

Infraestruturas estão a tornar-se alvos preferidos dos ciberataques

Frequência, intensidade e sofisticação dos ataques cibernéticos têm aumentado, desde o início da pandemia e Portugal segue a tendência geral. Perfil e visibilidade dos últimos alvos causa preocupação, pelo receio de disrupção de sistemas. P4

CIBERSEGURANÇA

Últimos ataques aumentam preocupação com infraestruturas

Frequência, intensidade e sofisticação dos ataques cibernéticos tem aumentado, desde o início da pandemia e Portugal segue a tendência geral. Perfil e visibilidade dos últimos alvos causa preocupação, pelo receio de disrupção de sistemas.

RICARDO SANTOS FERREIRA, LÍGIA SIMÕES E MARIANA BANDEIRA
rsferreira@jornaleconomico.pt

A visibilidade dos últimos ataques cibernéticos em Portugal – especialmente o que afetou a operadora de telecomunicações Vodafone – aumentou a preocupação com a segurança de infraestruturas críticas e com as consequências da possível disrupção de sistemas. Autoridades e especialistas concordam que se têm intensificado tendências de crescimento da frequência dos ataques, de maior complexidade dos atores e de maior sofisticação das ameaças, mas também, nos últimos meses, uma preferência por alvos de maior dimensão. O que acontece em Portugal é um exemplo disso mesmo.

"A ameaça que se tem vindo a verificar nos últimos anos dirigida ao ciberespaço nacional coincide com a generalidade dos países congéneres do mesmo enquadramento geográfico, económico e geopolítico em que Portugal se insere", diz o secretário-geral do Sistema de Segurança Interna, Paulo Vizeu Pinheiro. "Esta tipologia de crime tem apresentado nos últimos anos índices consistentes de crescimento em volumetria e em qualidade ofensiva", acrescenta.

Um ponto de viragem foi a pandemia de Covid-19, que obrigou a um processo acelerado de digitalização da sociedade, tanto para os indivíduos como organizações, a partir do primeiro trimestre de 2020. "Estamos perante um panorama de aumento dos ataques de segurança cibernética à escala global, em volume, velocidade e sofisticação. O número e a taxa de sucesso de ataques cibernéticos aumentaram durante a pandemia", diz ao Jornal Económico (JE) Manuel Dias, *national technology officer* da Microsoft Portugal. Só em 2021, a Microsoft intercetou 35,7 mil milhões de e-mails de *phishing* [técnica destinada a obter dados de outrem através de meios informáticos, para os utilizar de forma fraudulenta] com o Microsoft Defender para Office 365 e bloqueou mais de 25,6 mil milhões de ataques de autenticação de força bruta. Entre julho de 2020 e junho de 2021, bloqueou nove mil milhões de ameaças a dispositivos, 32 mil milhões de ataques por e-mail e 31 mil milhões de ameaças.

"A reorganização que muitas empresas enfrentaram trouxe novos desafios em termos de segurança, mudando ainda mais o conceito de perímetro da empresa. Antigamente, o ambiente corporativo era vinculado ao escritório, às suas redes de conexão e ao uso de uma VPN. Hoje incluiu o ecossistema de parceiros, fornecedores...", diz Nuno Vieira da Silva, diretor de Cloud na Google Portugal.

Em Portugal, o "Relatório Riscos & Conflitos 2021", do Centro Nacional de Cibersegurança (CNCS) – publicado em maio de 2021, mas relativo a 2020 –, indica que os sectores da banca, infraestruturas digitais e prestadores de serviços de internet, mas também as áreas da ciência e ensino superior, são dos que mais incidentes tiveram registados pelo CERT.PT, o serviço integrante do CNCS que coordena a resposta a incidentes envolvendo entidades da Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais, além de todo o ciberespaço nacional. Mais de dois terços (69%) dos incidentes registados ocorreram em entidades privadas.

"É preciso colocar a cibersegurança no patamar da governança, seja ao nível do Estado, seja nas organizações privadas, pelo impacto que têm nas organizações, mas também pelo que delas depende", diz ao JE Jorge Silva Carvalho, consultor na área da segurança e antigo diretor do Serviço de Informações Estratégicas de Defesa.

"É preciso colocar a cibersegurança no patamar da governança, ao nível do Estado e dos privados, pelo impacto que têm nas organizações, mas também pelo que delas depende", diz ao JE Jorge Silva Carvalho

Pandemia aumenta crimes

No seu relatório, o CNCS alerta que, com a persistência da pandemia, "é provável que o número de incidentes e os indicadores de criminalidade online continuem elevados, bem como a sua sofisticação, em 2021 e 2022", através da ação de "cibercriminosos, enquanto indivíduos e grupos que atuam de forma maliciosa em função de proveitos financeiros", mas também de agentes estatais, que se caracterizam "pelo uso, direta ou indiretamente, do aparelho de estados com intuitos estratégicos e políticos".

Um responsável por uma empresa de cibersegurança que trabalha com grandes empresas e serviços públicos, que pediu para não ser identificado, afirma que, nos últimos meses, a frequência dos ataques detetados tem aumentado, mas também a sua força. "Desde o final de novembro que temos detetado ataques mais violentos, a grandes empresas, com maior visibilidade", diz. Acrescenta que se trata de ataques planeados, com um grande esforço - inclusive financeiro, envolvido - e que, em muitos casos, têm como alvo infraestruturas.

Em Portugal, desde o início do ano, registaram-se seis ataques cibernéticos com grande visibilidade em Portugal. Primeiro, tendo como alvo o grupo de comunicação social Impresa (que detém a estação de televisão SIC e o jornal Expresso), depois o grupo de comunicação social Cofina (que controla o canal de televisão CMTV e o jornal Correio da Manhã). Esta semana, foi atacada a operadora de telecomunicações Vodafone, o que terá afetado cerca de quatro milhões de pessoas e criado problemas em sistemas e organizações que interagiam com a rede. Também o grupo de comunicação Trust in News (detentora da revista Visão) e, já esta quinta-feira, o grupo laboratorial Germano de Sousa, em evidência por ser uma das principais redes de testes para a Covid-19.

O CNCS já identificava um aumento na perceção de risco de se sofrer "um incidente de cibersegurança no ciberespaço de interesse nacional", entre "agentes-chave para a cibersegurança em Portugal". Os últimos casos mediáticos de ciberataques acentuaram essa preocupação, nomeadamente para quem gere infraestruturas ou atua em sectores como a produção, transporte e distribuição de energia, telecomunicações, fornecimento de água ou serviços financeiros.

"O Banco de Portugal, dentro dos seus processos internos e das suas atividades da cibersegurança, intensificou e direcionou o foco dos controlos internos de cibersegurança sobre as ameaças que parecem estar a emergir com ataques recentes", disse ao JE fonte oficial do banco central. "O grupo EDP tem, desde a sua origem, planos de resiliência e de continuidade de negócio da produção, distribuição e fornecimento de energia à população, que contemplam diversos cenários. Este é um tema que a EDP acompanha com atenção", diz fonte oficial da empresa.

Crime informático aumentou 22% em 2020 e já representa 7,4% do total dos crimes registados em Portugal

Apesar de a criminalidade em geral ter diminuído em 2020, o crime relacionado com a informática aumentou 22% (inclui o crime informático, a devassa por meio informático e a burla informática/comunicações), representando já 7,4% do total de crimes (mais dois pontos percentuais do que em 2019). A criminalidade mais frequente baseada no registo de denúncias ao Gabinete Cibercrime da Procuradoria-geral da República (PGR) é a fraude na utilização do sistema MBWay, o phishing e o ransomware. As denúncias de cibercrimes duplicaram no ano passado, para 1.160. A PGR alerta que estas denúncias, recebidas por correio eletrónico, têm aumentado nos últimos anos, mas, desde 2019, duplicaram anualmente, com maior expressão em 2021. 195 denúncias foram encaminhadas para abertura de inquérito e 25 para a PJ. ■ LS

Kacper Pempel/Reuters

Solução passa pela formação

A resposta passa, em primeiro lugar, pela formação, tanto de utilizadores como de dirigentes, como defenderam diversos agentes contactados pelo JE. "A cibersegurança necessita de estar mais na agenda dos nossos gestores", defende Sérgio de Sá, *associate partner* da consultora EY. "O PESI 2020, que é um relatório que a União Europeia produz todos os anos coloca-nos muito mal na área da literacia digital. Globalmente, estamos em 19º, em quatro grandes clusters de indicadores estamos acima da União Europeia e em dois outros estamos abaixo. E nesses em que estamos abaixo, o que está mais abaixo é precisamente a literacia digital e temos que investir muito, muito, nisso", afirma o diretor-geral do Gabinete Nacional de Segurança (GNS), António Gameiro Marques.

Depois, pela disposição das organizações para terem em conta a dimensão da cibersegurança e encará-la como fundamental. "Não há uma vacina mágica", diz Bruno Castro, CEO da VisionWare. Aconselha as empresas a "autoavaliarem-se constantemente, a auditarem-se para procurarem debilidades", para estarem mais bem preparadas para eventuais ataques cibernéticos.

Jorge Silva Carvalho diz que esta é uma ameaça que deve ser encarada em conjunto, pelos diferentes agentes da sociedade. "Sem um esforço solidário do Estado com as empresas, sobretudo as que gerem infraestruturas críticas, não vamos lá", conclui. ■ *Com MTA*

PRR tem 147 milhões para investimento em cibersegurança

Transição digital é um dos objetivos definidos pela União Europeia e pelo Governo português, refletindo-se no quadro dos investimentos previstos no Plano de Recuperação e Resiliência (PRR) e, também, nas áreas de desenvolvimento do Portugal2030, que vai enquadrar os projetos financiados pelos fundos previstos no último quadro financeiro plurianual da União Europeia. No PRR, o tema específico da cibersegurança pode beneficiar de um financiamento global a ordem dos 147 milhões e euros. O Ministério do Planeamento detalha que a componente C19 – Transição Digital da Administração Pública: Capacitação, Digitalização, Interoperabilidade e Cibersegurança tem disponível um montante de 47 milhões de euros para reforço do quadro geral de cibersegurança, que serão executados através do Gabinete Nacional de Segurança (GNS).
A componente C16 – Empresas 4.0 tem previsto um investimento em Catalisação da Transição Digital das Empresas, que inclui um montante de 100 milhões de euros para aplicar em transformação dos sistemas e reforço da cibersegurança. Os prazos de execução destas verbas estendem-se até 2026, acompanhando todo o período de implementação do PRR. ■ **RSF**