BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

SETEMBRO 2021 | nº 4/2021

DESTAQUES

Pandemia

A situação pandémica que se instalou a partir de 2020 teve consequências na sociedade como um todo, em Portugal e no mundo. A cibersegurança foi uma das áreas que se viu interpelada, pelo menos de duas formas: 1. A cibersegurança tornou-se ainda mais essencial, acompanhando a importância acrescida que as tecnologias digitais adquiriram; e 2. a atividade maliciosa no ciberespaço aumentou significativamente.

1º semestre

A primeira metade de 2020 foi um período que mostrou de forma clara os efeitos do confinamento social na cibersegurança. A partir de março, o número de incidentes registados pelo CERT.PT aumentou para níveis ímpares. Ainda que tenha posteriormente ocorrido uma descida, não se voltou aos níveis pré-pandemia. O 1º semestre de 2021 reforçou esta ideia, com valores ainda mais elevados e com picos paralelos aos momentos de maior confinamento social.

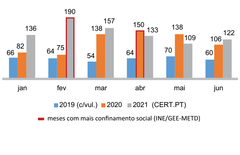
Fator humano

Os dados do CERT.PT mostram que o fator humano, considerando a tipologia de incidentes mais frequentes no 1º semestre de 2020, mas sobretudo no de 2021 (*phishing* e engenharia social), tem muita relevância neste contexto em termos quantitativos (independentemente dos níveis de impacto destes tipos de incidentes, comparando com outros menos frequentes, mas com potencial de impacto maior, como o *ransomware*, por exemplo).

VISUALIZAÇÃO

- No 1º semestre de 2021 foram registados 847 incidentes pelo CERT.PT, quando no mesmo período em 2020 se registaram 689 e em 2019 apenas 378*. Portanto, em 2021 houve um aumento de 23% em relação a 2020 e de 124% em relação a 2019.
- Comparando os 1ºs semestres de 2020 e 2021, o mês com mais incidentes registados pelo CERT.PT no ano passado foi abril, com 150 (o valor mais elevado do ano), e, no 1º semestre deste ano, fevereiro, com 190, valores muito acima e divergentes de 2019.
- Considerando dados do Instituto Nacional de Estatística e do Gabinete de Estratégia e Estudos do Ministério da Economia e Transição Digital, e convertendo-os para valores médios por mês, verifica-se que os meses com mais incidentes registados são aqueles que também evidenciam maiores níveis de confinamento social.
- Os períodos de estado de emergência (de março a maio de 2020 e de novembro de 2020 a abril de 2021) e em particular os de recolhimento geral coincidem com as curvas ascendentes em termos de registos de incidentes por parte do CERT.PT, tendência já identificada em 2020 (CNCS, 2021) e que permanece em 2021.

Nº de incidentes registados pelo CERT.PT, no 1º semestre de 2019, 2020 e 2021, e picos de confinamento social



* Contabilizando em 2019 a tipologia de incidentes "vulnerabilidades", de modo a fazer a comparação, visto a alteração na taxonomia a partir de 2020 ter passado a considerar as "vulnerabilidades" como incidentes.

AMEAÇA

1 O *phishing* continua a ser o tipo de incidente mais frequente entre os registados pelo CERT.PT. No 1º semestre de 2020 correspondeu a 38% do total de incidentes. No mesmo período de 2021, atinge os 40%. De destacar uma subida muito relevante do tipo de incidente categorizado na taxonomia utilizada pelo CERT.PT como "engenharia social", que passou de 0,4% do total no 1º semestre de 2020 para 13% em 2021, o segundo tipo de incidente mais frequente.

2 Os lugares de destaque do *phishing* e da engenharia social mostram a importância do fator humano. O *phishing* é uma forma de manipulação que conduz os utilizadores a partilharem informação sensível. Uma das técnicas mais usadas pelos atacantes é o argumento da autoridade, isto é, a simulação da identidade de uma entidade com autoridade suficiente para não levantar suspeitas (DOGANA, 2017). O setor mais visado por esta estratégia em Portugal é a banca.

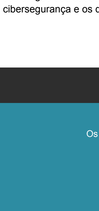
3 Os casos categorizados como engenharia social pelo CERT.PT mais comuns no 1º semestre de 2021 foram a *sextortion* (49%), a CEO Fraud (12%), a tentativa de burla mediante caso fictício de herança (11%) e a burla através da plataforma MBWay (7%), entre outros. Qualquer um destes casos está relacionado com o fator humano. Nestas situações, é através da manipulação das pessoas que os atacantes procuram obter um ganho, provocando assim um dano.

4 A *sextortion* é uma extorsão com base na ameaça de exposição de supostas imagens íntimas; a CEO Fraud ocorre quando alguém se faz passar pela chefia de uma organização, solicitando uma transferência bancária a um subordinado; a burla mediante caso fictício de herança procura ganhos com a promessa de dinheiro; e os casos de uso da MBWay dizem respeito a supostos compradores que conduzem vendedores *online* a transferir dinheiro indevidamente.

5 Estes casos exploram vulnerabilidades sociais específicas: o medo da exposição excessiva da intimidade (*sextortion*); a crença na autoridade do pedido de um chefe sem que a vítima se "atreva" a verificar esse pedido (CEO Fraud); a disponibilidade para o outro quando este traz uma notícia positiva, como dinheiro (o caso da herança); ou a falta de literacia digital quanto ao funcionamento de uma plataforma tecnológica (burla através da plataforma MBWay).

6 A importância do fator humano em pelo menos 53% dos incidentes registados no 1º semestre de 2021 (40% de *phishing* + 13% de engenharia social) coloca a hipótese de o confinamento social correlacionar-se de alguma forma com estratégias de ataque que exploram este vetor. Por exemplo, o aumento de incidentes durante o mês de fevereiro deste ano é marcado de modo significativo por estes casos de *phishing* e de engenharia social.

PUBLICAÇÕES E NOTÍCIAS



O **ICS da Universidade de Lisboa**, no dia 6 de julho, publicou o texto *Nós e a Internet – Diálogo global de cidadãos*, uma consulta global, promovida pela Missions Publiques, por solicitação do Painel de Alto Nível sobre Cooperação Digital, convocado pelo Secretário-Geral da ONU. Os cidadãos em Portugal referem que os aspetos negativos da Internet são o "risco de cibercrimes, a cibervigilância, o *ciberbullying*, a perda de privacidade, a dependência/vício e a sedentarização".

O **Gabinete Cibercrime**, da Procuradoria-Geral da República, no dia 22 de julho, disponibilizou a Nota Informativa *Cibercrime: Denúncias Recebidas (janeiro-junho 2021)*, onde se evidencia que as denúncias de cibercrimes a este organismo, durante o 1º semestre de 2021, aumentaram muito comparando com o ano anterior (durante o ano todo de 2020 houve 544 e em 2021, até junho, ocorreram já 594). As defraudações na utilização da MBWay são as mais frequentes.

A **Direção-Geral de Estatísticas da Educação e Ciência**, no dia 23 de julho, publicou o *Inquérito à Utilização das Tecnologias da Informação e Comunicação nas Câmaras Municipais* e na *Administração Central e Regional*. Em 2020, 62% das Câmaras Municipais (+4 pp. do que em 2019) e 68% dos Organismos da Administração Pública Central (+5 pp.) efetuaram ações de formação voluntária ou têm informação interna disponível junto do pessoal sobre segurança das TIC.

A **ENISA – Agência Europeia para a Cibersegurança**, no dia 29 de julho, lançou o documento *Threat Landscape for Supply Chain Attacks*, através do qual se mapeiam os ataques à cadeia de fornecimento identificados entre janeiro de 2020 e julho de 2021, mostrando como este tipo de ataque tem aumentado em número e níveis de sofisticação, perspetivando a manutenção desta tendência na segunda metade de 2021.

Foi publicado o **Decreto-Lei n.º 65/2021 de 30 de julho**, que Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança, procedendo à regulamentação dos requisitos de segurança e das regras para a notificação de incidentes a cumprir pelas entidades do âmbito da Lei n.º 46/2018 de 13 de agosto, bem como permitindo a implementação de um Quadro Nacional de Certificação da Cibersegurança pela Autoridade Nacional de Certificação da Cibersegurança.

O **Observatório para a Proteção de Dados Pessoais,** do CEDIS, Universidade Nova de Lisboa, no dia 20 de agosto, publicou mais um *Anuário da Proteção de Dados*, referente a 2021, através do qual se apresentam diversos artigos dedicados a este tema, com tópicos relacionados com os *cookies*, o *whistleblowing*, os algoritmos, a cibersegurança e os dados pessoais, bem como o *big data*.

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança