Permissão para Atacar: Como Melhorar a Cibersegurança de Portugal através de Um Programa de *Bug Bounty* Governamental

Rui Florêncio
Frequenta o Mestrado em Ciência Política e Relações Internacionais na Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa. Possui uma Pós-Graduação em Gestão de Informações e Segurança pela NOVA Information Management School, Universidade Nova de Lisboa, em parceria com o SIRP e o IDN.

Resumo

Nos últimos anos, o número de ciberataques tem vindo a aumentar. Tais ciberataques são frequentemente tornados possíveis pela existência de vulnerabilidades no software. O artigo identifica quais as melhores políticas para assegurar que as vulnerabilidades são detetadas, divulgadas aos fabricantes de software e corrigidas. Neste contexto,os programas de *bug bounty* aparentam estar a emergir como uma estratégia viável para a correção de vulnerabilidades. Estes programas permitem aproveitar as competências de um grande número de investigadores para testar a segurança de um sistema. A nível governamental, os Estados Unidos, Singapura e Suíça melhoraram significativamente a sua cibersegurança recorrendo a esta abordagem. Considerando o sucesso destes programas, o propósito do presente artigo é avaliar de que forma Portugal poderia beneficiar de um programa de *bug bounty* governamental.

Palavras-chave: Cibersegurança; Vulnerabilidades; Programas de *Bug Bounty*; Portugal.

Abstract
Permission to attack: How to improve Portugal's cybersecurity through a government Bug Bounty Program

In recent years, the number of cyber attacks has been increasing. Such cyber attacks are often made possible by the existence of vulnerabilities in software. The article identifies the best policies to ensure that vulnerabilities are detected, disclosed to software manufacturers, and corrected. In this context, bug bounty programs appear to be emerging as a viable strategy for correcting vulnerabilities. These programs draw on the skills of a large number of researchers to test the security of a system. At the governmental level, the United States, Singapore and Switzerland have significantly improved their cybersecurity using this approach. Considering the success of these programs, the purpose of this article is to assess how Portugal could benefit from a governmental bug bounty program.

Keywords: *Cybersecurity; Vulnerabilities; Bug Bounty Programs; Portugal.*

Artigo recebido: 28.07.2020
Aprovado: 05.08.2020
https://doi.org/10.47906/ND2020.156.03

Introdução

Nos últimos anos, o número de ciberataques, tanto no setor público como no privado, tem vindo a aumentar. Tais ciberataques são frequentemente tornados possíveis pela existência de vulnerabilidades no *software*. Falhas como esta são tão comuns que há quem diga que existem dois tipos de organizações: as que sabem que foram alvo de *hacking*, e as que ainda não o descobriram. Isto porque a existência de vulnerabilidades é inevitável. O *software* é complexo e os humanos são falíveis, pelo que as vulnerabilidades estão destinadas a ocorrer (Wilson, Schulman, Bankston & Herr, 2016, p. 4).

Desde há muito tempo, existe um mercado negro de vulnerabilidades de *software*. Durante um longo período, os hackers estavam satisfeitos ao trocar ou vender as vulnerabilidades entre si, sobretudo por prestígio. Os investigadores faziam normalmente uma divulgação "responsável" das vulnerabilidades, que consistia em contactar o fabricante e geralmente em receber reconhecimento pela sua descoberta quando a vulnerabilidade fosse anunciada e a respetiva correção disponibilizada. No entanto, nos últimos anos, o mercado de vulnerabilidades começou a migrar para o espaço comercial (Miller, 2007, p. 2). A informação sobre vulnerabilidades de *software* tornou-se uma *commodity*: indivíduos que anteriormente partilhavam esta informação de forma a construírem a sua reputação enquanto especialistas em cibersegurança vendem agora este conhecimento no mercado de vulnerabilidades para aumentar o seu rendimento (Kuehn, 2014, p. 64).

Face à concorrência dos compradores no mercado de vulnerabilidades, os fabricantes de *software* começaram a criar programas de atribuição de recompensas pela descoberta de vulnerabilidades, também conhecidos por programas de *bug bounty* (Wilson, Schulman, Bankston & Herr, 2016, p. 18). Subjacente à escolha de pagar por vulnerabilidades está o facto de as vulnerabilidades poderem ser descobertas por outros investigadores. Como uma vulnerabilidade é algo que está embutido num *software*, um investigador que descubra independentemente uma vulnerabilidade não tem nenhuma garantia de ser a única pessoa que sabe da sua existência. A cada dia que passa, existe uma maior probabilidade de outro investigador que procura vulnerabilidades no mesmo *software* encontrar essa vulnerabilidade (Herr, Schneier & Morris, 2017, p. 4). Por exemplo, a vulnerabilidade Heartbleed existia desde 2011 no OpenSSL e, em 2014, foi, na mesma altura, descoberta independentemente por investigadores da empresa Codenomicon e por um investigador da Google Security (Synopsys, 2017).

Recentemente, alguns governos criaram programas de *bug bounty*. Por exemplo, o governo norte-americano lançou programas de *bug bounty* que incidiram sobre os sistemas do Pentágono, do Exército, da Força Área, do Defense Travel System (DTS), do Corpo de Fuzileiros Navais e do Technology Transformation Services (TTS). O governo de Singapura lançou programas de *bug bounty* que incidiram so-

bre os seus sistemas. O governo suíço lançou um programa de *bug bounty* que incidiu sobre o sistema de voto eletrónico da Suíça.
Portugal poderia também beneficiar de um programa deste género. Mesmo que o governo de Portugal restrinja a participação nos seus programas de *bug bounty* a cidadãos nacionais, como os governos dos Estados Unidos e de Singapura fizeram inicialmente, existe em Portugal muito talento nesta área. Por exemplo, num *ranking* que posiciona 17.577 equipas de todo o mundo que participam em concursos de cibersegurança, a equipa STT, constituída por alunos do Instituto Superior Técnico, encontra-se em 41.º lugar. A equipa xSTF, constituída por alunos do Departamento de Ciência de Computadores da Faculdade de Ciências da Universidade do Porto, encontra-se em 166.º lugar. A equipa TeamRocketIST, também constituída por alunos do Instituto Superior Técnico, encontra-se em 170.º lugar (CTFTime, 2020). E, no European Cyber Security Challenge 2019, um evento anual que reúne jovens talentos de toda a Europa para uma competição de cibersegurança, a equipa portuguesa ficou no top 10 (Centro Nacional de Cibersegurança, 2019).
O propósito do presente artigo é avaliar de que forma é que Portugal poderia beneficiar de um programa de *bug bounty* que incidisse sobre os sistemas governamentais do país. A questão orientadora desta análise é: "De que forma é que Portugal poderia beneficiar de um programa de *bug bounty* governamental?". Para dar resposta a esta questão, ir-se-á: (1) abordar o conceito de vulnerabilidade e descrever os mercados em que estas são transacionadas; (2) abordar o conceito de política de divulgação responsável; (3) abordar o conceito de programa de *bug bounty*; (4) apresentar casos da utilização de programas de *bug bounty* por governos; (5) analisar os desafios legais representados pelos programas de *bug bounty*; e, com base nos supramencionados pontos, (6) avaliar de que forma Portugal poderia beneficiar de um programa de *bug bounty* governamental.

Vulnerabilidades

Vulnerabilidades são debilidades num *software* que permitem a um atacante comprometer a integridade, disponibilidade ou confidencialidade de um *software*, colocando os utilizadores e as redes em risco. Uma grande parte da cibersegurança pode ser reduzida a uma corrida constante entre desenvolvedores de *software* e especialistas em segurança a tentarem descobrir e corrigir vulnerabilidades, e os atacantes – criminosos, Estados, *hacktivistas* e outros – que tentam encontrar e tirar partido dessas vulnerabilidades (Wilson, Schulman, Bankston & Herr, 2016. p. 5).
Todo o *software* está suscetível a vulnerabilidades, e é pouco provável que algum dia as vulnerabilidades sejam completamente erradicadas. Mesmo que um sistema seja suficientemente seguro quando é lançado, não existe garantia de que irá

continuar assim para sempre. A sua utilização num novo contexto, interações com novos sistemas ou o desenvolvimento de novos métodos de ataque podem revelar vulnerabilidades anteriormente desconhecidas (ENISA, 2018, p. 9).

As vulnerabilidades podem ser introduzidas num *software* de diversas formas. A maior parte das vulnerabilidades resulta de erros honestos: são causadas por simples gralhas no código do *software*, interações imprevistas entre subcomponentes complexos de um sistema maior, ou por não proteger um programa de uma utilização indevida imprevista. Outras vulnerabilidades são introduzidas deliberadamente pelos desenvolvedores do *software* para que posteriormente possam tirar partido destas (Wilson, Schulman, Bankston & Herr, 2016, p. 5).

Numa rede interconectada, a existência de vulnerabilidades em *software* popular pode representar um risco considerável para os sistemas e para a sociedade, requerendo uma eficiente identificação e correção das vulnerabilidades. As vulnerabilidades que passam despercebidas durante um período prolongado ou que são divulgadas inapropriadamente podem exacerbar ainda mais estes riscos, o que demonstra a necessidade da existência de processos eficazes de divulgação de vulnerabilidades (ENISA, 2018, p. 9).

Quando um investigador descobre uma vulnerabilidade, tem três formas para a divulgar (ENISA, 2018, p. 12):

- Divulgação total: o investigador divulga publicamente toda a informação sobre a vulnerabilidade que identificou, sem coordenar com um coordenador[1] ou com o fabricante.
- Divulgação limitada: o investigador trabalha com um coordenador ou com o fabricante para minimizar o risco da vulnerabilidade que identificou. Após a correção ter sido desenvolvida, o coordenador ou o fabricante irão publicar informação sobre a vulnerabilidade juntamente com as medidas de remediação.
- Não-divulgação: o investigador pode optar por não divulgar a vulnerabilidade ao fabricante por diversas razões. Por exemplo, o investigador poderá optar por vender a vulnerabilidade no mercado negro, onde conseguirá obter um pagamento maior. Outra área emergente da não-divulgação está relacionada com iniciativas governamentais para analisar, avaliar e selecionar vulnerabilidades para serem mantidas em segredo para fins de segurança

1 Coordenadores são organizações de confiança que funcionam como intermediários entre os investigadores e os fabricantes para garantir que as vulnerabilidades descobertas são divulgadas e mitigadas de forma responsável. Os coordenadores incluem Equipas de Resposta a Incidentes de Segurança Informática (European Agency for Network and Information Security, 2018, p. 10), como, por exemplo, o US-Cert (Estados Unidos), o CERT-FR (França), o CERT-UK (Reino Unido), o CERT.EE (Estónia), o SingCERT (Singapura), o AusCERT (Austrália), o JPCERT (Japão), o DKCERT (Dinamarca), o CERT-Bund (Alemanha), o CERT.at (Áustria), o CERT.SE (Suécia), o CERT NZ (Nova Zelândia), o GovCERT.ch (Suíça), o NorCERT (Noruega), e o CERT.PT (Portugal).

nacional. Os governos poderão não divulgar informação sobre determinadas vulnerabilidades para que possam tirar partido das mesmas para a recolha de *intelligence* e para outras ciberoperações ofensivas.

A divulgação limitada ou a não-divulgação pode ocorrer através de mercados de vulnerabilidades. As vulnerabilidades não divulgadas são *commodities*, que são vendidas pelos seus produtores (os investigadores que as descobrem) a consumidores (fabricantes, governos ou atores maliciosos). Um mercado de vulnerabilidades pode ser não regulado ou regulado. Num mercado não regulado, existem poucas regras ou limitações e, tipicamente, as vendas são feitas pela oferta mais alta. Por outro lado, os mercados regulados têm geralmente regras e processos definidos, que têm que ser cumpridos pelos vendedores, e que podem restringir vendas a determinados grupos de clientes, como, por exemplo, governos (ENISA, 2018, pp. 13-14).
Os mercados regulados incluem (ENISA, 2018, p. 14):

- Mercados de divulgação coordenada: as vulnerabilidades são divulgadas publicamente através do fabricante ou de um coordenador (como um CERT). O investigador poderá ou não receber recompensas financeiras ou não-financeiras pela divulgação da vulnerabilidade.
- Mercados cativos: o investigador divulga a vulnerabilidade ao fabricante ou à organização em que/para quem trabalha e a vulnerabilidade não é divulgada publicamente. Inclui investigadores que trabalham dentro ou sob contrato para uma determinada organização, assim como investigadores que trabalham para agências governamentais em serviços de defesa ou de *intelligence*.
- Mercados de recompensas por vulnerabilidades: o investigador divulga a vulnerabilidade através do fabricante ou de um terceiro de confiança em troca de recompensas financeiras ou não-financeiras, através de um programa de *bug bounty*. Tipicamente, as recompensas dependem da gravidade da vulnerabilidade e das suas potenciais implicações de segurança. Os programas de *bug bounty* incluem programas específicos do fabricante – como os da Mozilla, da Google e da Facebook –, plataformas de *bug bounty* – como a BugCrowd, a HackerOne e a Intigriti – ou programas coordenados de recompensas por vulnerabilidades – como a Zero Day Initiative.

Relativamente aos mercados não regulados, estes incluem (ENISA, 2018, p. 14):

- Mercados parcialmente regulados: mediadores de vulnerabilidades servem de elo de ligação entre compradores e vendedores e, tipicamente, cobram uma comissão quando a venda é finalizada. Trata-se de organizações ou indivíduos que recebem informação sobre uma vulnerabilidade de um investigador e que encontram um comprador para essa vulnerabilidade. Os mediadores de vulnerabilidades podem ter certas regras de conduta ou limitações, mas, tipicamente, vendem as vulnerabilidades pela oferta mais alta.

Os mediadores tendem a focar-se em vulnerabilidades *zero-day* e na venda de vulnerabilidades a agências governamentais.

- Mercados negros de vulnerabilidades: mercados não regulados com determinadas características como compradores desconhecidos, não-exclusividade das vulnerabilidades no mercado – o vendedor poderá vender a mesma vulnerabilidade a outro consumidor –, dependência de ligações pessoais para negociar e ausência de garantias para manter a vulnerabilidade em segredo. As vendas podem ser feitas em diversos locais como salas de *chat*, mercados online ou na *dark web*.

O caminho que cada investigador irá seguir para divulgar uma vulnerabilidade irá depender do seu resultado desejado. Um investigador que é motivado pelo desejo de construir a sua reputação e contribuir para a segurança poderá optar pela divulgação total ou pela divulgação limitada. O investigador poderá até receber uma recompensa financeira, diretamente do fabricante ou indiretamente, através de um terceiro. No entanto, um investigador que procure principalmente uma compensação financeira poderá ter menos incentivos para divulgar a vulnerabilidade ao fabricante, quando a pode vender por um preço muito mais elevado no mercado aberto. Frequentemente, Estados e criminosos estão dispostos a pagar muito mais por vulnerabilidades do que o fabricante está disposto ou é capaz de pagar (Wilson, Schulman, Bankston & Herr, 2016, p. 11).

Políticas de Divulgação Responsável: Úteis, mas Insuficientes

O modelo primário que as organizações podem implementar para que investigadores divulguem vulnerabilidades descobertas nos seus sistemas é uma política de divulgação responsável, que consiste num canal dedicado e estruturado para a divulgação de vulnerabilidades (ENISA, 2018, p. 15). As políticas de divulgação responsável baseiam-se no princípio "se vir algo, diga algo", na medida em que, se um investigador descobrir uma vulnerabilidade num sistema de uma organização, é convidado a divulgá-la à organização, mas a organização não encoraja necessariamente a investigação, nem atribui necessariamente recompensas pelas vulnerabilidades divulgadas (HackerOne, 2017a). Como tal, as políticas de divulgação responsável têm como vantagem o facto de não implicarem custos (por cada vulnerabilidade descoberta) para a organização. Em contrapartida, as desvantagens são que: (1) os investigadores descobrem vulnerabilidades de forma passiva; e que, por essa razão, (2) o número de vulnerabilidades descobertas tenderá a ser inferior às vulnerabilidades que poderiam ser descobertas através de uma investigação mais ativa.

Essencialmente, uma política de divulgação responsável estabelece diretrizes claras para os investigadores divulgarem vulnerabilidades às organizações, enquanto per-

mite que as organizações efetuem a gestão das vulnerabilidades divulgadas de forma simples (Bugcrowd, s.d.a). Tal é importante porque, por vezes, os investigadores receiam poder vir a ser alvo de acusações legais por divulgarem vulnerabilidades. Noutras situações, os investigadores não conseguem entrar em contacto com as organizações e, mesmo quando conseguem, as vulnerabilidades divulgadas podem ser ignoradas, ou podem demorar demasiado tempo a serem corrigidas (Bugcrowd, s.d.b). Veja-se o caso de Miguel de Moura, que descobriu várias vulnerabilidades no Portal das Finanças, a mais grave das quais permitia a alteração da password de qualquer contribuinte conhecendo apenas o seu Número de Identificação Fiscal. Não havendo um canal próprio para divulgar vulnerabilidades à Autoridade Tributária, Moura começou por divulgar estas vulnerabilidades ligando múltiplas vezes para a linha de suporte do Portal das Finanças e, seguidamente, para a Comissão Nacional de Proteção de Dados (CNPD) em janeiro de 2018. Como não obteve uma resposta positiva, Moura apresentou queixa à CNPD em março e voltou a contactar a linha de suporte em abril. Em maio, Moura contactou novamente a linha de suporte, tendo finalmente conseguido falar com alguém em posição para resolver os problemas, após uma chamada de 36 minutos em que foi transferido sucessivamente entre múltiplos departamentos. Apenas em junho de 2018 as vulnerabilidades foram corrigidas (Matos, 2018).

A situação descrita acima poderia ter sido evitada caso a Autoridade Tributária tivesse implementado uma política de divulgação responsável. Não obstante, a Autoridade Tributária continua a não dispor de uma política de divulgação responsável. Este cenário é transversal a todo o setor público em Portugal (Centre for European Policy Studies, 2018, p. 18).

A Holanda é um dos únicos países que possui orientações oficiais para a divulgação responsável. Em 2013, o Centro Nacional de Cibersegurança holandês publicou um documento que estabelece diretrizes, tanto do ponto de vista dos investigadores como da organização, para a divulgação de vulnerabilidades (Kranenbarg, Holt & Ham, 2018, p.2). Seguindo estas diretrizes, o governo central da Holanda implementou a sua própria política de divulgação responsável, segundo a qual vulnerabilidades descobertas nos seus sistemas devem ser comunicadas ao Centro Nacional de Cibersegurança holandês, através de *e-mail*. No que concerne a vulnerabilidades descobertas em sistemas de entidades governamentais fora do governo central, estas deverão ser divulgadas à própria entidade[2]. Caso o investigador não receba uma resposta, deverá contactar o Centro Nacional de Cibersegurança holandês, que irá funcionar como intermediário entre o investigador e a entidade (Government of the Netherlands, s.d.).

Outro país cuja abordagem à divulgação responsável importa analisar é o Reino Unido, na medida em que está a desenvolver um projeto-piloto que visa identificar

2 Algumas entidades possuem as suas próprias políticas de divulgação responsável.

"a melhor forma para orientar uma organização ao longo do processo de implementação de um processo de divulgação de vulnerabilidades". Este projeto integra o Centro Nacional de Cibersegurança britânico, a HackerOne enquanto fornecedora da plataforma e a empresa NCC Group enquanto parceira para a avaliação das vulnerabilidades divulgadas. A empresa Luta Security, especializada nesta área, está também envolvida para garantir que estão a ser seguidas as melhores práticas da indústria. No âmbito deste projeto, foi implementada uma política de divulgação responsável que estabelece diretrizes para a divulgação de vulnerabilidades nos serviços online do governo britânico (National Cyber Security Centre, 2018a). Segundo a referida política, os investigadores deverão primeiramente tentar contactar a entidade responsável pelos sistemas. Caso não consigam encontrar um ponto de contacto, ou se não obtiverem resposta, poderão comunicar as vulnerabilidades descobertas ao Centro Nacional de Cibersegurança britânico, através de um formulário disponível na plataforma HackerOne (National Cyber Security Centre, 2018b).
Em suma, as políticas de divulgação responsável são um modelo útil para identificar vulnerabilidades em sistemas governamentais. Semelhantemente à Holanda e ao Reino Unido, Portugal poderia beneficiar de uma política de divulgação responsável. No entanto, estas políticas pecam por o seu sucesso depender de investigadores descobrirem vulnerabilidades de forma passiva. Considerando a importância da cibersegurança para a segurança nacional, seria, portanto, preferível a implementação de um modelo que encorajasse a procura de vulnerabilidades de forma ativa.

Programas de *Bug Bounty*

Através de um programa de *bug bounty*, as organizações podem definir um programa em que investigadores são autorizados a tentar identificar vulnerabilidades nos seus sistemas, em troca de recompensas financeiras ou não-financeiras por cada vulnerabilidade considerada válida (ENISA, 2018, p. 15). Assim, comparativamente às políticas de divulgação responsável, os programas de *bug bounty* têm como desvantagem o facto de implicarem custos (por cada vulnerabilidade descoberta) para a organização. Note-se, no entanto, que o custo de cada vulnerabilidade divulgada depende da sua gravidade: quanto mais grave for, maior será a recompensa a atribuir ao investigador. Mas, por outro lado, as vantagens são que: (1) os investigadores procuram vulnerabilidades de forma ativa; e que, por esse motivo, (2) o número de vulnerabilidades descobertas tenderá a ser superior às vulnerabilidades que poderiam ser descobertas através de uma política de divulgação responsável.
A lógica dos programas de *bug bounty* baseia-se num conceito que surgiu com a cultura do *software* aberto, segundo o qual "havendo olhos suficientes, todos os *bugs*

são triviais". Isto significa que, se todos os investigadores do mundo se tornassem co-desenvolvedores de um determinado *software*, os *bugs* existentes no mesmo seriam descobertos e corrigidos mais rapidamente. Os programas de *bug bounty* tiram partido desta lógica, que se revelou especialmente eficaz no contexto da cibersegurança, ao expandir o conjunto de investigadores envolvidos na procura de *bugs* de segurança (On, 2019, pp. 231-232).

Os programas de *bug bounty* têm diversos benefícios para os fabricantes de *software*. A atribuição de recompensas incentiva os investigadores a procurarem vulnerabilidades, e esta atenção acrescida aumenta a probabilidade de serem descobertas vulnerabilidades latentes. Em segundo lugar, a coordenação com os investigadores permite aos fabricantes gerir mais eficazmente a divulgação de vulnerabilidades, reduzindo a probabilidade da divulgação de vulnerabilidades *zero-day*. As recompensas monetárias constituem um incentivo para os investigadores não venderem as vulnerabilidades que descobrirem a atores maliciosos no mercado cinzento e no mercado negro. Em terceiro lugar, os programas de *bug bounty* podem tornar mais difícil que atores maliciosos descubram vulnerabilidades para tirarem partido das mesmas. A correção de vulnerabilidades descobertas através de um programa de *bug bounty* aumenta a dificuldade e, consequentemente, o custo de atores maliciosos descobrirem vulnerabilidades *zero-day*, dado que o total de vulnerabilidades latentes foi diminuído. Para além disso, a experiência adquirida através de programas de *bug bounty* pode contribuir para a melhoria das técnicas de mitigação e ajudar a identificar outras vulnerabilidades relacionadas e fontes de *bugs*. Por último, os programas de *bug bounty* geram frequentemente boa vontade entre a comunidade de investigadores. No seu conjunto, estas vantagens fazem dos programas de *bug bounty* uma ferramenta interessante para melhorar a segurança dos produtos e proteger os consumidores (Finifter, Akhawe & Wagner, 2013, p. 273). Para além disso, os programas de *bug bounty* podem ser utilizados para identificar potenciais contratações para os departamentos de cibersegurança das organizações. Por exemplo, a Facebook contratou pelo menos dois investigadores que participaram no seu programa de *bug bounty* para trabalharem a tempo inteiro na equipa de segurança da rede social (Facebook, 2013). Também a Google e a Mozilla contrataram investigadores que participaram nos seus respetivos programas de *bug bounty*, tendo cada uma destas organizações contratado pelo menos três investigadores (Finifter, Akhawe & Wagner, 2013, p. 282). O investigador que descobriu mais vulnerabilidades no programa de *bug bounty* "Hack the Air Force" foi contratado pelo Defense Digital Service (DDS), a agência do Departamento de Defesa dos Estados Unidos que conduz o programa "Hack the Pentagon" (HackerOne, 2018a).

Para alojarem os seus programas de *bug bounty*, as organizações podem recorrer a plataformas externas, como a HackerOne, a Bugcrowd ou a Intigriti, ou fazê-lo de forma independente.

Utilização de Programas de *Bug Bounty* por Governos

No presente capítulo, ir-se-ão apresentar casos de governos que utilizam programas de *bug bounty* para melhorar a sua cibersegurança.

Estados Unidos

O governo dos Estados Unidos já lançou vários programas de *bug bounty*, tendo recorrido à plataforma HackerOne para os alojar.

Pentágono

O programa "Hack the Pentagon" foi o primeiro programa de *bug bounty* do governo dos Estados Unidos. Este programa foi lançado no dia 18 de abril de 2016, estando apenas aberto para cidadãos norte-americanos. Durante 24 dias, mais de 1400 investigadores testaram a segurança dos sistemas do Pentágono, tendo sido descobertas 138 vulnerabilidades. Foram atribuídas recompensas a 58 dos investigadores participantes, sendo que a recompensa mais elevada foi de 3500 dólares. A recompensa média foi de 588 dólares, e o investigador que recebeu mais recompensas arrecadou 15 mil dólares. O investigador mais novo que recebeu uma recompensa tinha 14 anos e o mais velho tinha 54 anos (HackerOne, 2016).

Exército

O programa "Hack the Army" decorreu entre 30 de novembro e 21 de dezembro de 2016, estando também apenas aberto para cidadãos norte-americanos. Neste período, 371 investigadores, 25 dos quais eram funcionários públicos, incluindo 17 militares, testaram a segurança dos sistemas do Exército. Foram descobertas 118 vulnerabilidades e atribuídos 100 mil dólares em recompensas (HackerOne, 2017b).

Força Aérea

O programa "Hack the Air Force" já teve três edições. A primeira edição deste programa foi, à data, o maior programa de *bug bounty* do governo dos Estados Unidos, estando aberto não só para cidadãos norte-americanos, mas para cidadãos da Austrália, Canadá, Nova Zelândia e Reino Unido. Este programa decorreu entre 30 de maio e 23 de junho de 2017. Neste período, 272 investigadores, 33 dos quais eram estrangeiros, testaram a segurança dos sistemas da Força Aérea. Foram descobertas 207 vulnerabilidades e atribuídos 130 mil dólares em recompensas. Alguns dos participantes que mais vulnerabilidades descobriram tinham idade inferior a 20 anos, incluindo um jovem de 17 anos que recebeu a maior recompensa total por ter descoberto 30 vulnerabilidades, o que foi também a maior recompensa atribuída a um indivíduo nos programas de *bug bounty* até à data (HackerOne, 2017c). Foi este

investigador que acabou por ser contratado pelo Defense Digital Service (DDS), a agência do Departamento de Defesa dos Estados Unidos que conduz o programa "Hack the Pentagon". A segunda edição deste programa foi ainda mais inclusiva pois, para além de estar aberta para cidadãos norte-americanos, da Austrália, do Canadá, da Nova Zelândia e do Reino Unido, puderam participar cidadãos ou residentes permanentes legais da Albânia, Bélgica, Bulgária, Canadá, Croácia, Dinamarca, Estónia, França, Alemanha, Islândia, Itália, Letónia, Lituânia, Holanda, Noruega, Polónia, Portugal, Eslovénia, Espanha, Suécia e Turquia, tornando-se, à data, o maior programa de *bug bounty* do governo dos Estados Unidos (Hacker One, 2018b). Este programa de *bug bounty* decorreu entre 9 de dezembro de 2017 e 1 de janeiro de 2018. Durante 20 dias, 27 investigadores descobriram 106 vulnerabilidades, tendo sido atribuídos 103.883 dólares em recompensas. A recompensa individual mais elevada foi de 12.500 dólares, constituindo a maior recompensa individual atribuída em todos os programas de *bug bounty* do governo dos Estados Unidos até à data. Investigadores dos Estados Unidos, Canadá, Reino Unido, Suécia, Holanda, Bélgica e Letónia participaram nesta segunda edição do "Hack the Air Force" (HackerOne, 2018c). A terceira edição foi ainda mais inclusiva, estando a participação aberta a 191 países, tornando-se no maior programa de *bug bounty* do governo dos Estados Unidos até à data. Este programa de *bug bounty* decorreu entre 19 de outubro e 22 de novembro de 2018. Durante um mês, 30 investigadores descobriram mais de 120 vulnerabilidades, tendo sido atribuídos 130.000 dólares em recompensas (HackerOne, 2018d).

Defense Travel System (DTS)

O programa "Hack the DTS" decorreu entre 1 e 29 de abril de 2018, estando aberto para cidadãos norte-americanos e cidadãos e residentes legais da Austrália, Canadá, Nova Zelândia e Reino Unido (HackerOne, 2018e). Durante 29 dias, 19 investigadores testaram a segurança do DTS, tendo sido descobertas 65 vulnerabilidades, 28 das quais foram consideradas de gravidade alta ou crítica. Foram atribuídos 78.650 dólares em recompensas, sendo que os investigadores que foram recompensados eram principalmente dos Estados Unidos e do Reino Unido. A recompensa mais elevada foi de 5.000 dólares, e foi paga 8 vezes a investigadores individuais (HackerOne, 2018f).

Corpo de Fuzileiros Navais

O programa "Hack the Marine Corps" decorreu entre 12 e 26 de agosto de 2018. Durante 20 dias, mais de 100 investigadores foram convidados a testar a segurança dos sistemas do Corpo de Fuzileiros Navais dos Estados Unidos. Foram descobertas 150 vulnerabilidades e atribuídos mais de 150 mil dólares em recompensas (HackerOne, 2018g).

Technology Transformation Services (TTS)

A Administração de Serviços Gerais dos Estados Unidos lançou um programa de *bug bounty* que incide sobre os sistemas da TTS, tornando-se na primeira agência civil do governo dos Estados Unidos a lançar um programa deste género (HackerOne, 2018h).

Singapura

Tal como o governo dos Estados Unidos, o governo de Singapura já lançou diversos programas de *bug bounty*, tendo também recorrido à plataforma HackerOne para os alojar.

Ministério da Defesa de Singapura

O primeiro programa de *bug bounty* do governo de Singapura foi lançado pelo Ministério da Defesa. Entre 15 de janeiro e 4 de fevereiro de 2018, 300 investigadores foram convidados a testar a segurança dos sistemas do Ministério da Defesa. Durante três semanas, foram descobertas 35 vulnerabilidades, 23 das quais foram consideradas de baixa gravidade, 10 de média gravidade, 2 de alta gravidade e nenhuma de gravidade crítica. Foram atribuídos 14.750 dólares em recompensas a 17 dos investigadores participantes, sendo que a recompensa mais elevada foi de 2.000 dólares. Participaram nesta iniciativa investigadores de todo o mundo, incluindo dos Estados Unidos, Singapura, Índia, Roménia, Canadá, Rússia, Suécia, Irlanda, Egipto e Paquistão (HackerOne, 2018i).

O segundo programa de *bug bounty* lançado pelo Ministério da Defesa de Singapura decorreu entre 30 de setembro e 21 de outubro de 2019, envolvendo mais de 300 investigadores convidados – 134 dos quais eram de Singapura. Durante três semanas, foram descobertas 20 vulnerabilidades, tendo sido atribuídos 16 mil dólares em recompensas (HackerOne, 2019a).

Government Technology Agency e Cyber Security Agency de Singapura

O segundo programa de *bug bounty* do governo de Singapura foi lançado pela Government Technology Agency e pela Cyber Security Agency de Singapura. Entre 27 de dezembro de 2018 e 16 de janeiro de 2019, mais de 400 investigadores de todo o mundo foram convidados a testar a segurança dos sistemas do governo. Durante três semanas, foram descobertas 26 vulnerabilidades, 7 das quais foram consideradas de baixa gravidade, 18 de média gravidade e 1 de alta gravidade. Foram atribuídos 11.750 dólares em recompensas. Um quarto de todos os investigadores participantes e 7 dos investigadores no top 10 dos investigadores que receberam mais recompensas eram de Singapura (HackerOne, 2019b).

O segundo programa de *bug bounty* lançado por estas agências decorreu entre 8 e 28 de julho de 2019, envolvendo cerca de 300 investigadores de todo o mundo.

Neste programa de *bug bounty*, foram descobertas 31 vulnerabilidades, 4 das quais foram consideradas de alta gravidade e as restantes 27 de baixa ou média gravidade, tendo sido atribuídos 25.950 dólares em recompensas. Cerca de um quarto dos investigadores eram de Singapura, 30 dos quais tinham participado no primeiro programa de *bug bounty*, e 7 dos investigadores no top 10 dos investigadores que receberam mais recompensas eram de Singapura (HackerOne, 2019c).
O terceiro programa de *bug bounty* destas agências decorreu entre 18 de novembro e 8 de dezembro de 2019, e contou com a participação de cerca de 300 investigadores – 72 dos quais eram de Singapura. Foram descobertas 33 vulnerabilidades e atribuídos 30.800 dólares em recompensas (HackerOne, 2020).

Suíça

Desde 2004, a Suíça tem realizado experiências com o voto eletrónico. A Swiss Post acredita que conseguiu agora desenvolver um sistema de voto eletrónico que é totalmente verificável, o que significa que o voto eletrónico pode vir a ser disponibilizado a todos os eleitores no futuro. No entanto, para tal, a lei federal requer que o sistema de voto eletrónico seja certificado antes de ser utilizado pela primeira vez e que o seu código fonte seja divulgado. Para além disso, a Confederação Suíça e os cantões determinaram que os sistemas de voto eletrónico totalmente verificáveis têm de ser sujeitos a um teste de intrusão antes de serem utilizados pela primeira vez. Como tal, a Suíça, para além de sujeitar o seu sistema de voto eletrónico a um teste de intrusão por parte de um organismo acreditado, lançou um teste de intrusão público através de um programa de *bug bounty* (Swiss Federal Council, 2019a). Este programa de *bug bounty* decorreu entre 25 de fevereiro e 24 de março de 2019, estipulando recompensas entre 30.000 e 50.000 francos suíços por vulnerabilidades que permitissem a manipulação de votos não detetada pelo sistema; 20.000 francos suíços por vulnerabilidades que permitissem a manipulação de votos detetada pelo sistema; 10.000 francos suíços por vulnerabilidades que permitissem o comprometimento do segredo de voto nos servidores; 5.000 francos suíços por vulnerabilidades que permitissem o corrompimento de votos; 1.000 francos suíços por vulnerabilidades que permitissem a intrusão no sistema de voto eletrónico; e 100 francos suíços por possibilidades de otimização não críticas (Swiss Post, 2019a). Durante 4 semanas, cerca de 3.200 investigadores de 137 países testaram a segurança do sistema de voto eletrónico da Suíça, tendo sido descobertas 16 vulnerabilidades, nenhuma das quais foi considerada crítica. A maior parte dos participantes eram suíços (27%), 13% eram franceses, 7% eram americanos, 5% eram alemães, 4% eram indianos, 3% eram polacos, 3% eram canadianos, 3% eram britânicos e 35% eram de outras nacionalidades (SwissPost, 2019b).
No entanto, as vulnerabilidades mais críticas foram descobertas fora do âmbito deste programa de *bug bounty*. Isto porque, no âmbito do programa de *bug bounty*, a

Swiss Post disponibilizou o código fonte do sistema de voto eletrónico aos participantes. Para obterem acesso ao código fonte, os participantes tinham que aceitar as condições de utilização, que estipulavam que apenas poderiam publicar informações sobre as vulnerabilidades descobertas após um período de 45 dias (Swiss Post, 2019c). Contudo, alguém publicou livremente o código fonte do sistema de voto eletrónico e, a partir desse momento, qualquer pessoa passou a poder analisar o código fonte para descobrir vulnerabilidades sem ter que aceitar as condições de utilização. Foi o que fizeram os investigadores Lewis, Pereira & Teague, tendo descoberto duas vulnerabilidades, que divulgaram publicamente antes do período de 45 dias imposto pela Swiss Post aos participantes no programa de *bug bounty*. A primeira vulnerabilidade permite que alguém que tenha implementado, administre ou obtenha o controlo do sistema manipule votos sem ser detetado (2019a). A segunda vulnerabilidade permite nulificar votos válidos (2019b).

Segundo a Swiss Post, anteriormente à realização deste programa de *bug bounty*, o código-fonte do sistema de voto eletrónico tinha sido auditado pela KPMG, mas os resultados da auditoria não foram tornados públicos devido a disposições contratuais. Por sua vez, os protocolos criptográficos utilizados pelo sistema foram auditados pelo Instituto Federal de Tecnologia de Zurique (Gamma, 2019). Por seu lado, a Scytl (2019), líder mundial em serviços de voto eletrónico, que é o parceiro tecnológico da Swiss Post no desenvolvimento do seu sistema de voto eletrónico, afirmou que estes protocolos "são o resultado da investigação realizada desde a fundação da Scytl em 2001, que foi disponibilizada ao público através de contínuas publicações académicas", tendo "passado com êxito o escrutínio de especialistas criptográficos externos", o que permitiu alcançar a verificabilidade total "com a confiança de que nenhum ataque pode comprometer o sigilo da urna e a integridade dos resultados da eleição". No entanto, as supramencionadas vulnerabilidades provam o contrário. Lewis levantou, por isso, as seguintes questões: "Porque é que várias auditorias anteriores foram incapazes de descobrir [o que nós descobrimos]? Porque é que alguém acreditou que este sistema era suficiente para proteger eleições nacionais? E o que iria acontecer se nós não tivéssemos descoberto?" (Zetter, 2019).

Após a descoberta destas vulnerabilidades, a Swiss Post (2019b) suspendeu temporariamente o sistema de voto eletrónico, que iria ser utilizado no dia 19 de maio de 2019. Posteriormente, a Suíça adiou provisoriamente a introdução do voto eletrónico como canal de voto oficial (Swiss Federal Council, 2019b). Pouco tempo depois, a Swiss Post (2019d) anunciou que iria continuar a trabalhar no seu sistema, e que planeava disponibilizá-lo aos cantões para ensaios a partir de 2020. No entanto, em dezembro de 2019, 100 deputados da Câmara dos Deputados da Suíça votaram a favor de uma proposta para suspender completamente os ensaios do sistema de voto eletrónico até o governo elaborar um relatório que prove que as questões de segurança foram resolvidas e que o *software* responde a necessidades reais. Apenas

75 deputados votaram contra esta proposta, sendo que 7 deputados se abstiveram. Note-se, no entanto, que este resultado não é definitivo e que não se trata de um ato legislativo vinculativo (Swissinfo, 2019). Não obstante, a Swiss Post continua a desenvolver o sistema de voto eletrónico, tendo, no entanto, adiado para 2021 a data em que planeia disponibilizá-lo aos cantões para ensaios (Swissinfo, 2020).

Em suma, os programas de *bug bounty* lançados pelos governos dos Estados Unidos, de Singapura e da Suíça permitiram identificar e corrigir diversas vulnerabilidades que poderiam ter sido utilizadas para realizar um ciberataque contra os sistemas governamentais dos respetivos países, melhorando significativamente a sua cibersegurança. Tendo em conta o sucesso destes programas, o autor do presente artigo considera que Portugal deveria também criar um programa de *bug bounty* para melhorar a sua cibersegurança.

Desafios Legais dos Programas de *Bug Bounty*

Os programas de *bug bounty* são frequentemente percecionados como uma abordagem arriscada para melhorar a segurança, na medida em que envolvem pedir a investigadores em grande parte anónimos e independentes de todo o mundo para escrutinarem os sistemas de uma organização remotamente. As organizações receiam que um investigador danifique os seus sistemas ou que roube os seus dados quando está à procura de vulnerabilidades, ou que divulgue as vulnerabilidades descobertas a terceiros ou até mesmo ao público. Por outro lado, os investigadores receiam poder vir a ser alvo de acusações legais por procurarem e divulgarem vulnerabilidades (Zhao, Laszka & Grossklags, 2017, p. 375).
Para reduzir os riscos, os programas de *bug bounty* possuem regras, que especificam que partes dos sistemas podem ser acedidas e que tipo de ações são permitidas. Para além disso, as regras estipulam que, se os investigadores cumprirem as diretrizes do programa durante a procura de vulnerabilidades, a organização não irá agir judicialmente contra os mesmos (Zhao, Laszka & Grossklags, 2017, p. 376). As regras funcionam como um contrato entre o investigador e a organização, e são o ponto central para determinar a responsabilidade legal e os riscos dos investigadores que participam no programa de *bug bounty* (On, 2019, p. 232). No entanto, por vezes, as organizações e os investigadores discordam relativamente à interpretação dessas regras (Zhao, Laszka & Grossklags, 2017, p. 404). Veja-se o caso do investigador Kevin Finisterre, nos Estados Unidos. Em agosto de 2017, a fabricante de drones DJI lançou o seu programa de *bug bounty*. No âmbito desse programa, Finisterre descobriu uma vulnerabilidade relacionada com os servidores da DJI, que permitia aceder a informação sensível dos clientes da empresa. Como a DJI não especificou as regras

do programa, Finisterre contactou a empresa para confirmar se os seus servidores estavam incluídos no âmbito do programa, tendo a empresa respondido afirmativamente. Em seguida, Finisterre escreveu um relatório detalhado sobre a vulnerabilidade e enviou-o para a DJI, tendo a empresa validado a mesma, o que iria valer ao investigador 30 mil dólares, a recompensa mais elevada do programa. No entanto, para receber a recompensa, Finisterre teria que assinar um contrato que, basicamente, não lhe permitiria falar publicamente sobre o trabalho que fez, nem sequer dizer que tinha feito qualquer trabalho de segurança para a DJI. Finisterre não concordou com estes termos e tentou negociar. No decorrer das negociações, Finisterre recebeu uma carta que mencionava a *Computer Fraud and Abuse Act* (CFAA). O investigador interpretou esta carta como uma ameaça, tendo, por isso, decidido abdicar da recompensa e tornar a sua experiência pública (Popper, 2017). Apesar de a DJI ter a sua própria versão da história, este mal-entendido poderia ter sido evitado se a empresa tivesse lançado o seu programa de *bug bounty* com regras claras. Mais importante ainda, se as regras incluíssem autorização clara para aceder ao sistema e o compromisso em não agir judicialmente – ao invés do que aparenta ser um consentimento implícito do anúncio do lançamento do programa de *bug bounty*, e da confirmação dada a Finisterre por *e-mail* –, seria mais difícil para a DJI utilizar uma carta legal como técnica de negociação. Este caso ilustra a posição potencialmente perigosa em que os investigadores poderão vir a encontrar-se caso as regras de um determinado programa de *bug bounty* não sejam claras, e a disparidade de poder negocial entre as partes. Para além disso, este caso demonstra a magnitude dos riscos legais que são transferidos para os investigadores caso não seja adotada uma linguagem clara *ex ante*. A não-utilização de uma linguagem clara deixa os investigadores expostos a ameaças legais *ex post*, na medida em que gera ambiguidade relativamente aos seus limites de atuação, tanto a nível técnico como legal (On, 2019, p. 241).

De forma geral, os programas de *bug bounty* incluem uma linguagem que não se coaduna com a prática de investigação de segurança, que não concede explicitamente uma autorização contratual que minimize o risco do investigador, e que compromete o propósito do programa. Isto porque a linguagem legal requer que os investigadores cumpram "todas as leis aplicáveis" ou proíbe testes que "infrinjam qualquer lei" ao invés de conceder aos investigadores uma autorização clara para investigar sob as leis *anti-hacking*. De modo semelhante, as plataformas de *bug bounty* requerem que os investigadores garantam que as suas ações não infringem direitos de propriedade intelectual de terceiros, e que a sua conduta cumpre todas as leis aplicáveis, tanto a nível nacional como internacional. Esta prática transfere o risco legal para o investigador. Outros programas de *bug bounty* não incluem qualquer referência à conformidade com a lei, gerando incerteza (On, 2019, p. 238). Sob as regras de alguns programas, os investigadores poderão ser forçados a uma situação de incumprimento contratual e responsabilidade civil e penal. Nas suas regras,

estes programas referem-se a Acordos de Licença do Utilizador Final, que, por sua vez, proíbem a engenharia reversa e outras ferramentas de investigação fundamentais para a investigação de segurança, e por vezes até proíbem a mera tentativa de obter acesso não autorizado. Ao invés de concederem aos investigadores permissão para realizar essas ações, as regras proíbem-nos de o fazer sob contrato. As regras do programa de *bug bounty* da empresa de antivírus AVG são um exemplo flagrante desta prática, na medida em que declaram que a submissão de uma vulnerabilidade "constitui a aceitação do Acordo de Licença do Utilizador Final da AVG". Por sua vez, o Acordo de Licença do Utilizador Final da AVG estipula que os utilizadores "não podem (…) (iii) exceto se expressamente autorizados por lei, (A) fazer engenharia reversa, desmontar, descompilar, traduzir, reconstruir, transformar ou extrair qualquer [*software*] ou qualquer parte do [*software*] (…), ou (B) alterar, modificar ou mudar de outra forma qualquer [*software*]". Um outro exemplo são as regras do programa de *bug bounty* da Facebook, que incluem um compromisso em não processar os investigadores que sigam as regras, mas estipulam também que "[a] utilização dos serviços da Facebook (…), incluindo para efeitos deste programa [de *bug bounty*], está sujeito aos Termos e Políticas da Facebook e aos termos e políticas de qualquer membro da família de empresas da Facebook cujos serviços você utiliza". Por sua vez, os termos de serviço do WhatsApp declaram que os utilizadores: "não podem (ou auxiliar outros a) aceder, utilizar, copiar, adaptar, modificar, preparar (…) ou explorar de outra forma os nossos Serviços (…) diretamente ou através de meios automatizados: (a) fazer engenharia reversa, alterar, modificar, criar obras derivadas, descompilar, ou extrair código a partir dos nossos Serviços; (b) enviar, armazenar, ou transmitir vírus ou outro código de computador prejudicial através ou para [os seus] Serviços; (c) obter ou tentar obter acesso não autorizado aos [seus] Serviços ou sistemas (…)". Ainda mais problemáticos são os programas de *bug bounty* cujas regras negam explicitamente a autorização para aceder. Por exemplo, nas regras do programa de *bug bounty* da Alibaba, pode ler-se: "Nenhuma licença ou permissão é dada para qualquer penetração ou ataque contra qualquer sistema da Alibaba" (On, 2019, pp. 239-240).

Considerando a supramencionada realidade, não é surpreendente que as preocupações legais sejam uma das principais barreiras à participação de investigadores em programas de *bug bounty* (National Telecommunications and Information Administration, 2016, p. 6; ENISA, 2018, p. 30; Centre for European Policy Studies, 2018, p. 81). Isto porque a eficácia de um programa de *bug bounty* depende fortemente da forma como as suas regras legais foram redigidas, e do conjunto de incentivos e garantias legais dadas aos investigadores. Tais garantias incluem a comunicação com clareza do âmbito do programa e do tipo de recompensa a atribuir por cada vulnerabilidade, assim como o tipo de risco legal assumido pelo investigador e o âmbito da autorização dada ao mesmo para agir nos termos da lei. De forma a

garantir que os programas de *bug bounty* continuam a funcionar como um mercado legal de vulnerabilidades é, portanto, fundamental que as suas regras sejam claras. Se as regras forem mal redigidas, os investigadores poderão estar a infringir a lei meramente por participarem no programa (On, 2019, p. 232).
Em Portugal, a Lei n.º 109/2009 de 15 de setembro, também conhecida como *Lei do Cibercrime*, tipificou o crime de acesso ilegítimo no seu Artigo 6.º:

- "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias" (n.º 1).
- "Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior" (n.º 2).

Atente-se que o acesso a um sistema sem permissão legal ou sem autorização do proprietário desse sistema constitui um crime de acesso ilegítimo. O proprietário do sistema poderia, portanto, autorizar o acesso a investigadores no âmbito de um programa de *bug bounty*, ultrapassando a criminalização pelo acesso ilegítimo da Lei do Cibercrime. No entanto, o crime de acesso ilegítimo é o crime básico que poderia ser invocado no âmbito da participação de um investigador num programa de *bug bounty*. A *Lei do Cibercrime* tipifica outros crimes que poderiam também ser invocados, como os crimes de falsidade informática (Artigo 3.º), dano relativo a programas ou outros dados informáticos (Artigo 4.º), sabotagem informática (Artigo 5.º) e interceção ilegítima (Artigo 7.º). Para a criação de um programa de *bug bounty* governamental em Portugal, recomenda-se, por isso, que o acordo, entre o governo e os investigadores, que será a base de tal programa inclua autorização específica, com um âmbito claramente definido, para efeitos da *Lei do Cibercrime*. Segundo Rogério Bravo, Inspetor-Chefe da Polícia Judiciária na Secção Central de Investigação Digital, "a lei reconhece a autorização; o que não pode acontecer é a investigação ir além do acordo, porque se isso acontece, depreende-se que se tratam de atos não autorizados. Desta forma preenchidos os quesitos do princípio da tipicidade e da legalidade, uma vez que numa interpretação a *contrario sensu*, o que não for proibido, é permitido". Bravo considera, portanto, que o acordo terá que "ser estudado para evitar normas abertas e imprecisas relativamente à possibilidade de atuação e às cláusulas penais, contendo referências mais específicas"[3]. A linguagem do acordo estará assim em conformidade com as melhores práticas para a realização de programas de *bug bounty*, contrariando uma tendência geral de regras com uma linguagem paradoxal, que co-

3 Entrevista realizada por email em 12 de agosto de 2020.

locam em risco os investigadores que seguem as regras. Já na perspetiva do governo, a clareza do acordo irá estabelecer uma base legal concreta para acusações caso um investigador infrinja intencionalmente as regras do programa (On, 2019, p. 241).

Considerações Finais

A existência de vulnerabilidades é inevitável. Coloca-se então a seguinte questão: quais são as melhores políticas para assegurar que as vulnerabilidades são descobertas, divulgadas ao fabricante do *software*, e corrigidas o mais rápido possível? (Wilson, Schulman, Bankston & Herr, 2016, p. 4).

Os programas de *bug bounty* aparentam estar a emergir como uma estratégia viável para a correção de vulnerabilidades (Finifter, Akhawe & Wagner, 2013, p. 274). Estes programas permitem aproveitar as competências de um grande número de investigadores para testar a segurança de um sistema, e recompensá-los pelas vulnerabilidades que descobrirem. Simultaneamente, os programas de *bug bounty* podem ser utilizados para identificar potenciais contratações para os departamentos de cibersegurança das organizações.

Países como os Estados Unidos, Singapura e a Suíça melhoraram significativamente a sua cibersegurança através de programas de *bug bounty*. Tendo em conta o sucesso destes programas, o autor do presente artigo considera que Portugal deveria também criar um programa de *bug bounty* para melhorar a sua cibersegurança.

Para além dos benefícios em termos de cibersegurança, a criação de um programa de *bug bounty* governamental em Portugal iria contribuir para o ciberpoder do país, na medida em que esta iniciativa iria sinalizar perante a comunidade internacional que Portugal está realmente empenhado na melhoria da sua cibersegurança, de tal forma que está disposto a convidar investigadores de todo o mundo (ou, pelo menos, de países aliados ou até mesmo apenas de Portugal) a escrutinarem a segurança dos seus sistemas.

Para que esta iniciativa seja bem-sucedida, recomenda-se que Portugal siga as medidas que foram propostas no presente artigo. Isto porque, apesar de, geralmente, os programas de *bug bounty* definirem claramente o âmbito técnico da autorização concedida ao investigador, o âmbito legal da autorização e do acesso é frequentemente ignorado, inexistente ou insuficiente. Em alguns casos, as regras legais entram diretamente em tensão com o propósito do programa, colocando investigadores que utilizam técnicas de investigação básicas em violação direta das regras, e expondo-os a responsabilidade legal. Em outros casos, as regras criam uma realidade em que os investigadores infringem as regras quase que por defeito, ao fazerem o que o programa lhes pede para fazer: descobrir vulnerabilidades (On, 2019, p. 233). Ao seguir as medidas propostas para contrariar essa tendência geral, Portugal irá seguir as melhores práticas para a realização de programas de *bug bounty*.

Referências Bibliográficas

Bugcrowd, s.d.a. *Vulnerability Disclosure Program (VDP)*. Disponível em: https://www.bugcrowd.com/resources/glossary/vulnerability-disclosure-program-vdp/ [acedido em 9 de agosto de 2020].

Bugcrowd, s.d.b. *What is Responsible Disclosure?* Disponível em: https://www.bugcrowd.com/resource/what-is-responsible-disclosure/ [acedido em 9 de agosto de 2020].

Centre for European Policy Studies, 2018. *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges*. Disponível em: https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf [acedido em 15 de janeiro de 2020].

Centro Nacional de Cibersegurança, 2019. *Equipa portuguesa conquista 10.º lugar no European Cyber Security Challenge 2019*. Disponível em: https://www.cncs.gov.pt/recursos/noticias/equipa-portuguesa-conquista-10-lugar-no-european-cyber-security-challenge-2019/ [acedido em 20 de junho de 2020].

CTFTime, 2020. *CTF Teams*. Disponível em: https://ctftime.org/stats/2020/PT [acedido em 20 de junho de 2020].

ENISA, 2018. *Economics of vulnerability disclosure*. Disponível em: https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure/at_download/fullReport [acedido em 8 de junho de 2019].

Facebook, 2013. *An update on our Bug Bounty Program*. Disponível em: https://www.facebook.com/notes/facebook-security/an-update-on-our-bug-bounty-program/10151508163265766 [acedido em 6 de julho de 2019].

Finifter, M., Akhawe, D. & Wagner, D., 2013. *An Empirical Study of Vulnerability Rewards Programs*. In: Proceedings of the 22nd USENIX Security Symposium. Berkeley: USENIX Association; pp.273-288. Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf [acedido em 22 de junho de 2019].

Gamma, M., 2019. E-Voting-PIT: Welche Security-Standards ein Hacker überwinden muss. *Inside IT*. Disponível em: https://www.inside-it.ch/de/post/e-voting-pit-welche-security-standards-ein-hacker-ueberwinden-muss-20190226 [acedido em 5 de agosto de 2019].

Government of the Netherlands, s.d. *Responsible disclosure*. Disponível em: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure [acedido em 10 de agosto de 2020].

HackerOne, 2016. *What Was It Like To Hack the Pentagon?* Disponível em: https://www.hackerone.com/blog/hack-the-pentagon-results [acedido em 13 de julho de 2019].

HackerOne, 2017a. *The best security initiative you can take in 2017*. Disponível em: https://www.hackerone.com/blog/The-best-security-initiative-you-can-take-in-2017 [acedido em 8 de agosto de 2020].

HackerOne, 2017b. *Hack The Army Results Are In*. Disponível em: https://www.hackerone.com/blog/Hack-The-Army-Results-Are-In [acedido em 13 de julho de 2019].

HackerOne, 2017c. *Aim High...Find, Fix, Win!* Disponível em: https://www.hackerone.com/blog/hack-the-air-force-results [acedido em 13 de julho de 2019].

HackerOne, 2018a. *U.S. Department of Defense Announces Hack the Marine Corps Bug Bounty Program With HackerOne*. Disponível em: https://www.hackerone.com/press-release/us-department-defense-announces-hack-marine-corps-bug-bounty-program-hackerone [acedido em 6 de julho de 2019].

HackerOne, 2018b. *Hacking the U.S. Air Force (again) from a New York City subway station*. Disponível em: https://www.hackerone.com/blog/Hacking-US-Air-Force-again-New-York-City-subway-station [acedido em 13 de julho de 2019].

HackerOne, 2018c. *U.S. Air Force Boosts Security With Second Bug Bounty Challenge on Hacker One*. Disponível em: https://www.hackerone.com/press-release/us-air-force-boosts-security-second-bug-bounty-challenge-hackerone [acedido em 13 de julho de 2019].

HackerOne, 2018d. *U.S. Department of Defense Concludes Third "Hack the Air Force" Bug Bounty Challenge with HackerOne to Improve Cybersecurity*. Disponível em: https://www.hackerone.com/press-release/us-department-defense-concludes-third-hack-air-force-bug-bounty-challenge-hackerone [acedido em 13 de julho de 2019].

HackerOne, 2018e. *U.S. Department of Defense Kicks Off Fifth Bug Bounty Challenge With Hacker One*. Disponível em: https://www.hackerone.com/press-release/us-department-defense-kicks-fifth-bug-bounty-challenge-hackerone [acedido em 14 de julho de 2019].

HackerOne, 2018f. *U.S. Department of Defense Secures the DTS With Help From Hackers on Hacker One*. Disponível em: https://www.hackerone.com/press-release/hackers-are-finding-more-severe-vulnerabilities-ever-total-number-high-or-critical [acedido em 14 de julho de 2019].

HackerOne, 2018g. *Hack the Marine Corps Bug Bounty Challenge Concludes, Nearly 150 Security Vulnerabilities Surfaced and $151,542 Awarded to Hackers*. Disponível em: https://www.hackerone.com/press-release/hack-marine-corps-bug-bounty-challenge-concludes-nearly-150-security-vulnerabilities [acedido em 13 de julho de 2019].

HackerOne, 2018h. *U.S. General Services Administration Selects HackerOne as TTS Bug Bounty Partner*. Disponível em: https://www.hackerone.com/press-release/us-general-services-administration-selects-hackerone-tts-bug-bounty-partner [acedido em 13 de julho de 2019].

HackerOne, 2018i. *Singapore Ministry of Defence Concludes Successful Ethical Hacking Program*. Disponível em: https://www.hackerone.com/press-release/singapore-ministry-defence-concludes-successful-ethical-hacking-program [acedido em 13 de julho de 2019].

HackerOne, 2019a. *Hacking the Singapore Government: A Q&A With A Top Hacker & MINDEF 2.0 Results*. Disponível em: https://www.hackerone.com/blog/hacking-singapore-government-qa-top-hacker-mindef-20-results [acedido em 13 de janeiro de 2020].

HackerOne, 2019b. *Singapore Government Enhances Cybersecurity Defenses With Second Hacker One Bug Bounty Programme*. Disponível em: https://www.hackerone.com/press-release/singapore-government-enhances-cybersecurity-defenses-second-hackerone-bug-bounty [acedido em 13 de julho de 2019].

HackerOne, 2019c. *Government Technology Agency Launches Vulnerability Disclosure Programme with HackerOne Following Successful Bug Bounty Programmes*. Disponível em: https://www.hackerone.com/press-release/government-technology-agency-launches-vulnerability--disclosure-programme-hackerone [acedido em 6 de outubro de 2019].

HackerOne, 2020. *Government Technology Agency of Singapore Concludes Third HackerOne Bug Bounty Programme, Enhancing Cybersecurity Defenses*. Disponível em: https://www.hackerone.com/press-release/government-technology-agency-singapore-concludes-third-hackerone-bug-bounty-programme [acedido em 14 de junho de 2020].

Herr, T., Schneier, B. & Morris, C., 2017. *Taking Stock: Estimating Vulnerability Rediscovery*. Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs. Disponível em: https://www.belfercenter.org/sites/default/files/files/publication/Rediscovery%20-%20final%206.pdf [acedido em 29 de junho de 2019].

Kranenbarg, M., Holt, T. & Ham, J., 2018. *Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure*. Crime Science, Volume 7. Disponível em: https://link.springer.com/content/pdf/10.1186/s40163-018-0090-8.pdf [acedido em 10 de agosto de 2020].

Kuehn, A. & Mueller, M., 2014. *Shifts in the Cybersecurity Paradigm: Zero-Day Exploits, Discourse, and Emerging Institutions*. In: Proceedings of the 2014 New Security Paradigms Workshop. Victoria: ACM Press; pp. 63-68.

Lei n.º 109/2009, de 15 de setembro. Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. *Diário da República*, n.º 179/2009, Série I, pp. 6319-6325, Assembleia da República. Disponível em: https://dre.pt/application/conteudo/489693 [acedido em 17 de fevereiro de 2020].

Lewis, S. J., Pereira, O. & Teague, V., 2019a. *The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiabilty of the Scytl-SwissPost Internet voting system*. Disponível em: https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf [acedido em 3 de agosto de 2019].

Lewis, S. J., Pereira, O. & Teague, V., 2019b. *The use of non-adaptive zero knowledge proofs in the Scytl-SwissPost Internet voting system, and its implications for decryption proof soundness*. Disponível em: https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcome.pdf [acedido em 3 de agosto de 2019].

Matos, P., 2018. Investigador descobriu como entrar em qualquer conta do Portal das Finanças em segundos. *Exame Informática*. Disponível em: https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2018-08-22-investigador-descobriu-como-entrar-em--qualquer-conta-do-portal-das-financas-em-segundos/ [acedido em 9 de agosto de 2020].

Miller, C., 2007. *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*. Disponível em: https://www.econinfosec.org/archive/weis2007/papers/29.pdf [acedido em 16 de junho de 2019].

National Cyber Security Centre, 2018a. *NCSC vulnerability disclosure co-ordination*. Disponível em: https://www.ncsc.gov.uk/blog-post/ncsc-vulnerability-disclosure-co-ordination [acedido em 10 de agosto de 2020].

National Cyber Security Centre, 2018b. *Vulnerability Reporting*. Disponível em: https://www.ncsc.gov.uk/information/vulnerability-reporting [acedido em 10 de agosto de 2020].

National Telecommunications and Information Administration, 2016. *Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group*. Disponível em: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf [acedido em 15 de janeiro de 2020].

On, A., 2019. *Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties*. In: Ellis, R. & Mohan, V. (2019). *Rewired: Cybersecurity Governance*: Wiley, pp. 231-314.

Popper, B., 2017. DJI's bug bounty program starts with a stumble. *The Verge*. Disponível em: https://www.theverge.com/2017/11/20/16669724/dji-bug-bounty-program-conflict--researcher [acedido em 14 de janeiro de 2020].

Scytl, 2019. *Statement on recent comments regarding the source code publication of the Swiss e-voting system*. Disponível em: https://www.scytl.com/en/news/statement-recent-comments--regarding-source-code-publication-swiss-e-voting-system/ [acedido em 5 de agosto de 2019].

Swiss Federal Council, 2019a. *Public intrusion test for e-voting to take place in February and March*. Disponível em: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73898.html [acedido em 20 de julho de 2019].

Swiss Federal Council, 2019b. *e-Voting: Federal Council to reframe trial phase and delay introduction as a regular voting channel*. Disponível em: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-75615.html [acedido em 4 de agosto de 2019].

Swiss Post, 2019a. *Public hacker test on Swiss Post's e-voting system*. Disponível em: https://www.evoting-blog.ch/en/pages/2019/public-hacker-test-on-swiss-post-s-e-voting-system [acedido em 20 de julho de 2019].

Swiss Post, 2019b. *Ballot box not hacked, errors in the source code – Swiss Post temporarily suspends its e-voting system*. Disponível em: https://www.post.ch/en/about-us/media/press-releases/2019/swiss-post-temporarily-suspends-its-e-voting-system [acedido em 20 de julho de 2019].

Swiss Post, 2019c. *ELECTRONIC VOTING SOLUTION SOURCE CODE ACCESS AGREEMENT*. Disponível em: https://www.post.ch/-/media/post/evoting/dokumente/nutzungsbedingungen-quellcode.pdf?la=en&vs=3 [acedido em 21 de julho de 2019].

Swiss Post, 2019d. *Swiss Post to focus solely on new system with universal verifiability*. Disponível em: https://www.post.ch/en/about-us/media/press-releases/2019/swiss-post-to-focus-solely-on-new-system-with-universal-verifiability [acedido em 4 de agosto de 2019].

Swissinfo, 2019. *E-voting dealt another political blow*. Disponível em: https://www.swissinfo.ch/eng/parliament_e-voting-dealt-another-political-blow/45425298 [acedido em 26 de dezembro de 2019].

Swissinfo, 2020. *Swiss Post set to relaunch its e-voting system*. Disponível em: https://www.swissinfo.ch/eng/swiss-post-set-to-relaunch-its-e-voting-system/45820842 [acedido em 21 de junho de 2019].

Synopsys, 2017. *Heartbleed Bug*. Disponível em: https://heartbleed.com/ [acedido em 29 de junho de 2019].

Wilson, A., Schulman, R., Bankston, K. & Herr, T., 2016. *Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications*. Disponível em: https://newamerica.org/documents/1659/Bugs-in-the-System-Final.pdf [acedido em 8 de junho de 2019].

Zetter, K., 2019. Researchers Find Critical Backdoor in Swiss Online Voting System. *Motherboard*. Disponível em: https://www.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system [acedido em 5 de agosto de 2019].

Zhao, M., Laszka, A. & Grossklags, J., 2017. Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery. *Journal of Information Policy*, Volume 7, pp. 372-418.