CYBERLAW

by CIJIC

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

CYBERLAW by CIJIC

EDIÇÃO N.º XI – MARÇO DE 2021

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW
by CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW by CIJIC

NOTAS DO EDITOR:

Finda Março do ano de 2021.

Passou um ano desde que o mundo se confinou, massivamente. Fechados, em casa, nunca como a partir disto o acesso à *Internet* se nos desvelou como um direito humano fundamental.

O sonho de uma *internet* livre, neutral, aberta, inclusiva, universal será possível?

Provavelmente muitos de nós, que navegam por ela, num ou noutro canto de conversação e/ou *stop by* possível a partir de um dos nossos hodiernos cárceres físicos, já nos deparámos com um curioso grafo. Nele consta uma espécie de sondagem onde à pergunta: *"Quem fez mais pela digitalização da sua organização no último ano?"*, a percentagem do vencedor surpreende.

Não, não foi o CEO da organização. Também não, não foi o CISO (quando as organizações os têm). Sim, também não foi nenhum diretor de nenhum departamento da organização.

O principal responsável, sim, foi ela: a pandemia de covid-19.

É inegável. A pandemia acelerou o processo de digitalização de grande parte das interações humanas, sejam elas de qualquer natureza, escola, comércio, socialização.

Não obstante, por mais benefícios que este *input*, à *força bruta*, tenha trazido, a humanidade tem ainda um caminho muito longo para percorrer.

Num plano macro, que convoca a humanidade, combater ferozmente a exclusão digital, com particular enfoque nos reversos, *i.e.*, mais novos e mais velhos; sociedades desenvolvidas/mais pobres.

E se o acesso não é universal (sê-lo-á algum dia?), plural, em condições idênticas, inclusivo…também não deixará de ser preocupante, dentro daqueles que podem aceder, o número de indivíduos com falta de formação, com falta de um mínimo de educação/formação para usufruir da Rede.

Atente-se, porém, num plano micro, por exemplo, no caso português.

Entregue, neste último dia de Março de 2021, o RASI2020[1], nele despontam algumas evidências sobre a temática da falta de educação para o *ciber*. Os crimes praticados na e pela *Internet*, nomeadamente, *phishing*, *vishing*, *ransomware* e extorsão[2], em passo crescente, decorrem de variadas falhas ao nível do utilizador. Sobressai, da leitura crua dos números, uma inexistente cultura de ciberhigiene. A facilidade de promoção de engenharias sociais avulsas. É esta omissão de cibereducação responsável pela inabilidade em detetar o logro e burlões, em actividade fervorosa. No compasso da oferta/procura de produtos através do digital, se as trocas aumentam exponencialmente, paralela e em acompanhamento, as situações de fraude, burla, roubo, *Money mules*, etc., *idem*.

As múltiplas deficiências ao nível do utilizador – o famoso factor humano é implacável - e a violência de uma *digitalização à força bruta* de uma grande maioria das organizações, combinadas… dão razão de ser à *tame joke* informática de que, *na prática, em termos de ataques e crimes informáticos, só há dois tipos de organizações: as que*

1 Disponível para consulta em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3d (último acesso 31MAR21)
2 *Vide* páginas 67 e ss do RASI2020.

sabem que já foram atacadas e as que ainda não o sabem (a premissa irónica é, infelizmente, igualmente válida para as pessoas singulares).

Torna-se inadiável que, paralelamente ao percurso do Direito no séquito da acelerada digitalização, as organizações, as pessoas, o Estado, entendam, decisiva e finalmente, a importância da segurança da informação[3].

Apaticamente, e em crise, as omissões perduram. Sedimentam.

Os alertas não chegam a bom porto. Provenham eles de serviços mais ou menos capacitados do Estado, sejam serviços secretos nacionais, sistema de segurança interna, observatórios…jaz, apenas, a constatação impotente de que "(…) *observa-se um aumento da espionagem através de ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado. Uma das consequências da sofisticação enunciada, prende-se com a crescente dificuldade em destrinçar ataques informáticos para efeitos de crime económico ou de crimes de sabotagem, dirigidos a empresas e grupos de empresas com relevância no tecido empresarial nacional*."

No presente, de crescente digitalização, de cascata informacional, já todos sabemos que não é a quantidade de informação que serve à melhor tomada de decisão; é a qualidade. Mostra-se-nos angustiante o sublinhado de "*ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado"*.

O Estado, como nunca, até como condição de promoção e prossecução geracional, tem o dever de defender um desígnio de soberania consubstanciado, precisamente, na superioridade informacional.

Conhecerá o Estado a capital importância da superioridade informacional?

Estará capacitado, humana e tecnologicamente, para proteger, o mais eficazmente possível, os seus mais valiosos *assets*, as suas infraestruturas mais críticas?

---

3 Ainda, no RASI2020 agora dado a conhecer, «(…) *No universo da ciberespionagem, registaram-se novos ciberataques contra infraestruturas críticas nacionais, com a finalidade de aceder a informação classificada, com valor político e económico."*», página 102.

Severa, a frieza dos parágrafos, no contexto pandémico Covid-19: "*No que concerne a outra das ameaças, i.e., as operações cibernéticas ofensivas, foram identificados agentes estatais e não estatais, visando entidades públicas e privadas, em particular no que respeitou à exploração de oportunidades…Verificaram-se inúmeros ciberataques registados contra instituições do setor da saúde, bem como operações de ciberespionagem contra entidades de investigação cientifica, particularmente envolvidas na pesquisa de terapêuticas e de vacinas contra a doença em apreço.*"

A segurança da informação, e a superioridade informacional que daí possa erigir, são, no contexto, de suma importância.

Infelizmente, as ameaças são múltiplas. Se, como veremos nesta nova edição, a Segurança da informação nas organizações(SiO) é tema fulcral, a erosão, de direitos fundamentais humanos, não descola de uma objetificação pronunciada da pessoa, do ser individual. Discreta, mas de forma expedita, as *oportunidades geradas pelo contexto pandémico*, têm servido para que o Estado arroje sistemas de videovigilância por múltiplas localidades nacionais[4]. A febre dos sistemas *CCTV* públicos segue a passo acelerado.

Em simultâneo, embora a aplicação *stayawaycovid* não tenha vingado, ainda, é certo que o controlo à distância da pessoa irá figurar, brevemente, em alguma medida legislativa. Notemos, ainda no contexto da pandemia, por exemplo, e em pleno estado de emergência, os níveis de mobilidade do cidadão. Com a proibição de circulação fora-do-concelho e a aproximação do tema festivo pascal, na semana de 25/26 de Março, acordámos com a notícia: "*Portugueses fogem para longe das restrições: um em cada dez dormiu a mais de 100 quilómetros de casa esta quinta-feira.*"[5].

4 Ainda no RASI2020, dentre renovações e novas autorizações, surgem destacadas 8 despachos de autorização de instalação de múltiplas cameras de videovigilância para localidades. Consultáveis a partir dos Anexos do relatório, Medidas legislativas, página 15 e ss.
Nota: entretanto, no início do mês de março 2021, foi-nos dada a conhecer a autorização para instalação de mais 216 cameras de videovigilância na cidade de Lisboa, para juntar às já existentes (o Bairro Alto já dispõe de sistema, por exemplo).

5 https://expresso.pt/sociedade/2021-03-26-Portugueses-fogem-para-longe-das-restricoes-um-em-cada-dez-dormiu-a-mais-de-100-quilometros-de-casa-esta-quinta-feira-b98a7df0 (último acesso 31MAR21).

A observação - próxima da realidade? - feita por uma consultora privada[6], revelando que mais de *um milhão de portugueses dormiu fora de casa*, curiosamente, não promoveu nenhum sobressalto jurídico. Nem social. A ordem continua serena. *Curiosamente*. Mas, não houve tratamento de dados pessoais para a revelação de tais estatísticas em mobilidade? Que finalidade jurídica prosseguiu a captura de tais dados? Que dados foram recolhidos? Foram coligidos de forma lícita? Que tratamento tiveram? Quais as garantias de anonimização e/ou minimização do tratamento?

Alguém questionou?

Alguém se indignou?

Não sendo a primeira vez que uma entidade privada analisa dados dos portugueses, em massa, sem qualquer tipo de reacção/oposição por parte destes, presumivelmente, como solução eficiente a tomar por parte do Estado, no futuro deveremos promover toda uma actividade concursal de fundos públicos para *investigação* - geral e abstrata - de *tendências*, *mobilidade*, *gostos e desejos* dos portugueses. Não que haja uma qualquer necessidade de uma finalidade concreta, lícita de sopeso. Afinal, o problema, de fundo, do sobressalto cívico e jurídico, da ordem, reside numa mera formalidade de *marketing*, o "publico não pode" vs. "privado tudo pode".

Acabemos prontamente com a folia[7].

O acesso a metadados são um problema para a acção das nossas secretas?

Do titular da acção penal, *tout court*, português?

---

6 Vejamos, por exemplo, o detalhe dos grafos sobre a evolução do confinamento e mobilidade em: https://www.pse.pt/evolucao-confinamento-mobilidade/ (último acesso 31MAR21).

7 Reparem na notícia: https://www.jornaldenegocios.pt/economia/impostos/amp/fisco-vai-ter-assistente-virtual-no-facebook-para-responder-as-duvidas-de-irs (último acesso 31MAR21).
Ora, a Autoridade Tributária portuguesa entende que a plataforma do Facebook é a melhor disponível *para tirar dúvidas a contribuintes nacionais.* Como todos sabemos, e somos *surpreendidos semanalmente*, o Facebook, provavelmente, já é conhecedor da informação fundamental e necessária dos seus utilizadores. Com este *passo de modernidade* da nossa AT, na prática, ao Facebook bastar-lhe-á agrupar a informação detida à contributiva, com os rendimentos declarados, das finanças portuguesas e... *Et voila*, vitracidade completa do cidadão. (quanto será o preço de cada miríade informacional de um contribuinte concreto que a AT poderá desembolsar? Haverá já um acordo bilateral entre a entidade privada e a AT?)
É, pois, tempo de assumirmos já a cedência gratuita dos nossos dados pessoais às entidades privadas e, a partir daí, o Estado seja profícuo no controlo de todas as nossas actividades sem qualquer tipo de sobressalto jurídico ou social.

Renunciemos à recolha de torrentes de dados pessoais às entidades privadas, assumamos a bonomia do *surveillance capitalism*, encapotando o próprio "*estado de vigilância*", e vivamos felizes.

E ordeiros. Sem sobressaltos.

A justificação, para esta aceitação social passiva e dócil, por parte de uma maioria de cidadãos, refletindo, denota muito do seu analfabetismo. Analfabetismo digital. Mas também social. A ordem das coisas apenas sobrepuja o ponto de partida. A liberdade individual é gratuitamente cedida a entidades privadas. Nunca ao Estado. A compressão de direitos fundamentais apenas terá de partir deste porto privado.

Aquiesçamos, afinal, mais de duzentos anos depois, a sociedade não compreende o ditame de que "*uma sociedade que troca um pouco de liberdade por um pouco de ordem acabará por perder ambas, e não merece qualquer delas*"[8].

Nesta nova edição da Cyberlaw by CIJIC, em consonância com os docentes do Mestrado em segurança da informação e direito do ciberespaço[9], tivemos o ensejo de provocar alguns discentes a reflexões sobre a realidade pungente que convoca a sociedade. No presente e para o futuro. Entre a segurança da informação nas organizações (SiO), a consciencialização dos funcionários das organizações para a temática, o factor humano na SiO; dados pessoais em *Schrems II* e acesso a metadados por parte do MP sem um suspeito determinado ou determinável, *not/net neutrality*, os discentes procuraram reunir algumas interjeições que, como já demos conta oportunamente, ajudem a mitigar a desigual compreensão, a despertar a consciencialização individual para promoção de um combate ao analfabetismo digital.

Trazemos, também, a participação de proeminentes juristas brasileiros que acederam ao nosso convite para dissertarem sobre a lei geral de proteção de dados brasileira assim como sobre o fenómeno do *stalking* em contexto laboral inclusive em ambiente digital.

8 Thomas Jefferson (1743-1826), carta a James Madison.
9 https://fenix.tecnico.ulisboa.pt/cursos/msidc

Resta-me, assim e por fim, agradecer a todos quantos contribuíram para mais esta nova edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um merecidíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 31 de Março de 2021

Nuno Teixeira Castro

O IMPACTO DA CONSCIENCIALIZAÇÃO DOS COLABORADORES NA SEGURANÇA DA INFORMAÇÃO DAS ORGANIZAÇÕES

PEDRO LUCAS FARINHA[*]

e

GONÇALO NUNO BAPTISTA DE SOUSA[†]

* Mestrando em segurança da informação e direito ciberespaço.
† Professor e investigador na Escola Naval.
Contacto: goncalobsousa@gmail.com

RESUMO

Nos últimos 10 anos, tem-se verificado um aumento progressivo no número de organizações que recorrem à utilização das tecnologias de informação e comunicação para desempenho das suas atividades. Em 2020, notou-se um impulso na adoção destas, por forma a garantir que várias organizações pudessem dar continuidade às suas atividades na crise pandémica que se instalou. No entanto, a utilização de novos métodos e tecnologias de trabalho levou a um acréscimo no número de ataques às organizações, aproveitando a falta de preparação destas e dos respetivos colaboradores para o novo contexto de trabalho.

Neste artigo, pretende-se avaliar a importância da consciencialização e educação dos colaboradores das organizações para a prevenção de ataques informáticos. Para tal, serão analisados três casos onde existiu negligência humana tanto nos comportamentos próprios para prevenção dos ataques, como na configuração de infraestruturas e funcionalidades tecnológicas. Estes serão utilizados para fundamentar a importância que a formação ou educação dos colaboradores das organizações em questão poderia ter tido na consciencialização dos mesmos na prevenção ou mitigação dos efeitos dos ataques.

Palavras-Chave: ataques; consciencialização, educação, e treino dos colaboradores; *hacking*, intrusões e phishing nas organizações; negligência; riscos.

ABSTRACT

In the last 10 years, there has been a progressive increase in the number of organizations who resort to the use of information and communication technologies to carry out their activities. In 2020, there was a strong impetus in its adoption, in order to ensure that several organizations could continue their activities in the pandemic crisis that was installed. However, the use of new methods and technologies of work has led to the addition of cyberattacks to organizations, taking advantage of the lack of preparation of these and their respective workers in this new context.

In this article, we intend to evaluate the importance of awareness and education of employees in the prevention of computer attacks. To this end, three cases of human negligence will be analyzed, both in terms of appropriate behaviors to the prevention, as well as in the configuration of infrastructures and technological functionalities. These will be used to substantiate the importance of training and educating employees and the importance of this in raising awareness on preventing or mitigating the effects of cyberattacks.

Keywords: ciberattacks; workers awareness, education, and training; hacking, intrusions and phishing in organizations; negligence; risks.

1. Introdução

De acordo com dados da OCDE [1], tem ocorrido um aumento progressivo nos últimos 10 anos no número de organizações que utilizam ou até dependem de Tecnologias de Informação e Comunicação (TIC) para desempenhar as suas atividades, o que evidencia a importância crescente destas no quotidiano empresarial.

Em 2020, a pandemia Covid19 levou a que inúmeras organizações tivessem como única possibilidade de trabalho, em regime não presencial, e de comércio, através de canais à distância (*e-commerce*). Tal fez com que houvesse um impulso substancial na adoção das TIC, e originou uma ainda maior dependência das organizações nestas, por forma a poderem assegurar a continuidade do negócio [2].

Em contrapartida, a adoção urgente de novas tecnologias e metodologias de trabalho obrigou a reorganizações consideráveis no funcionamento interno das organizações, muitas vezes sem que para tal existisse preparação prévia a nível tecnológico, ou consciencialização dos colaboradores para os riscos de segurança inerentes à introdução das novas condições.

Para além disso, as medidas introduzidas para a prevenção da pandemia originaram novas oportunidades de ataque. Em março de 2020, o Centro Nacional de Cibersegurança de Portugal registou um aumento de 176% no número de incidentes em comparação com o ano anterior, e um aumento de 217% no que toca à utilização de técnicas de *phishing*. Registou-se também a disponibilização na *darkweb*, de "*kits*", especialmente concebidos para a realização de ataques a indivíduos em teletrabalho, para além do aparecimento de aplicações *malware* e *ransomware*, dissimuladas com funcionalidades relacionadas com a pandemia Covid19 [3].

De acordo com a mesma entidade, não existe em Portugal uma generalidade de comportamentos e atitudes comparáveis à média da União Europeia no que toca à prevenção de vários riscos, apesar da consciencialização da existência de riscos como *phishing* e software malicioso. Não obstante, tem se verificado nos últimos anos uma

evolução positiva neste campo [4].

Kevin Mitnick defende na sua obra de 2003, "*The Art of Deception*", que apesar dos avanços e medidas de proteção trazidos pela componente tecnológica, apenas a combinação entre este fator e o humano poderão determinar o sucesso da manutenção da segurança da informação. Para tal, será necessário assegurar que todos os elementos que compõem a organização são consciencializados e devidamente treinados para reagir aquando da eminência de um ataque [5].

Nesta sequência, este artigo tem como objetivo evidenciar a importância que a formação e a consciencialização dos colaboradores têm, por forma a garantir segurança na informação das organizações.

Esta investigação abordará a técnica de "*phishing*", e a análise a um ataque deste tipo realizado a entidades públicas. De seguida, serão apresentadas algumas estratégias de mitigação para este tipo de ataque.

No que toca à componente tecnológica, será discutido o conceito de vulnerabilidade e falha tecnológica, e será apresentado um caso em que a manutenção desta componente foi descorada pela parte humana bem como houve negligência das próprias equipas técnicas de uma organização.

2. Ataques ao Fator Humano

*"**Phishing**"* é uma técnica de engenharia social, utilizada por atacantes, com o objetivo de coagir as vítimas a fornecer informações privilegiadas, tais como credenciais ou números de cartões de crédito, ou a realizar ações fraudulentas, sem que de tal se apercebam. Este tipo de ataque é habitualmente levado a cabo através do envio massivo de mensagens de email, as quais aparentam ser provenientes de entidades fidedignas e relevantes, como departamentos governamentais ou instituições bancárias [6].

Não obstante, a atividade de *phishing* pode ser realizada com recurso a outros meios de contacto, como chamadas telefónicas ou mensagens SMS.

De acordo com a *Proofpoint* [7], 99% dos ataques de email maliciosos requer interação humana, vulgo "ajuda" do utilizador para levar a cabo o seu objetivo. Tal pode consistir na abertura de um documento anexado à mensagem, de um endereço de internet, ou na aceitação de um aviso de segurança que fora despoletado na sequência da deteção de uma possível fraude. Poderá, também, consistir na simples resposta à mensagem com a informação requisitada.

As origens do "*phishing*" remontam a meados de 1990, em que grupos de adolescentes procuravam obter acesso gratuito ilegítimo ao provedor de acesso Internet AOL, na altura suportado por ligações telefónicas [8]. Para tal, foi desenvolvido um software que automatizava o envio de mensagens fraudulentas para clientes do fornecedor, enquanto estes frequentavam as salas de *chat* deste [Figura 1].

Figura 1 - Programa de envio automático de mensagens fraudulentas

Nestas, os atacantes identificavam-se como colaboradores da empresa, solicitando aos clientes a atualização de dados pessoais, como as respetivas palavras-passe de acesso e/ou os números de cartões de crédito.

Este tipo de ataque era possível em parte devido à arquitetura tecnológica utilizada na altura. Em primeiro lugar, apesar do serviço funcionar sobre a infraestrutura da rede telefónica pública, a operadora que o suportava não disponibilizava ou mantinha registos dos números de onde as chamadas originavam.

Assim, a impossibilidade de identificar a origem dos ataques, permitia aos agentes maliciosos um acesso anónimo ao serviço, sem que estes corressem o risco de ser identificados e responsabilizados.

Por outro lado, o fornecedor do acesso Internet não realizava validações de cartões de crédito em tempo real, o que por si só, já permitia aos atacantes obter acesso temporário ao serviço, o qual poderia ser utilizado para levar a cabo os ataques.

Tal perdurou até 1995, altura em que o operador implementou medidas de validação de cartões.

No decorrer dos anos, o *phishing* sofreu várias evoluções. Uma variante deste tipo de ataque denomina-se de *spear phishing*, no qual é realizado um ataque dirigido a uma pessoa, um grupo de pessoas em particular, ou a uma organização específica. Para tal, é necessário que seja realizada uma investigação prévia da vítima, por forma a gerar mensagens com maior credibilidade.

Estes tipos de ataque podem ter o seu risco de sucesso reduzido através da sensibilização dos colaboradores para pequenos detalhes nas mensagens de email, tais como erros ortográficos, linguagem inadequada ao tipo de pedido (como a formalidade), ou na análise crítica da probabilidade de certos pedidos serem dirigidos à pessoa em questão. Adicionalmente, a utilização da autenticação multifator reduz a probabilidade de sucesso não só deste, mas ataques que envolvam o comprometimento de credenciais.

Um caso de *spear phishing* realizado com sucesso, é o da captura de credenciais da

conta de John Podesta, na altura, gestor da campanha de candidatura à presidência dos Estados Unidos de Hillary Clinton [9].

De acordo com a CBS News, Podesta recebeu na sua caixa de correio, um alerta relativo a um acesso ilegítimo à sua conta, proveniente de um país estrangeiro, o qual incluía um *link*, através do qual a palavra-passe poderia ser reposta.

Por precaução, o gestor de campanha consultou o suporte IT, através da sua assistente, que reencaminhou o email original para os técnicos. Estes, afirmando a legitimidade da mensagem, sugeriram não só a reposição da palavra-passe, mas também a ativação da autenticação multifator, tendo para tal, disponibilizado um link adequado para o efeito.

Apesar disso, os técnicos de suporte não verificaram que o próprio *link* no email recebido originalmente, remetia para um abreviador de endereços ("*bit.ly*"), que não pertencia ao fornecedor de serviços de e-mail [Figura 2].

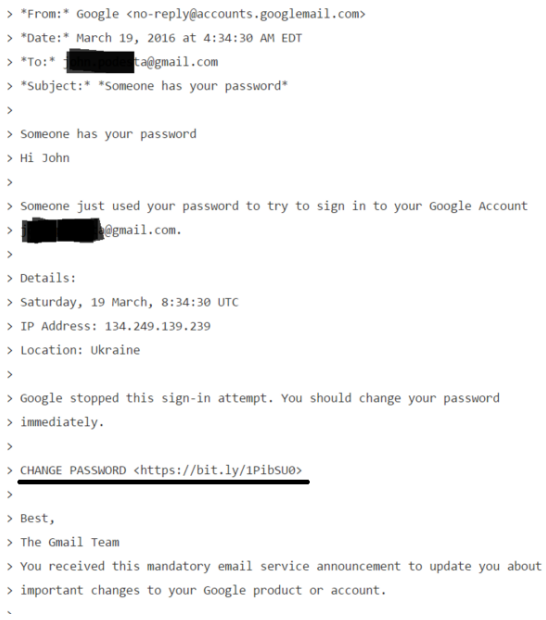
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

Figura 2 - Email fraudulento recebido por John Podesta

Na sequência da troca de mensagens, a vítima utilizou o *link* disponibilizado pelo atacante, e não o sugerido pelo técnico de suporte, levando a que as suas credenciais

fossem comprometidas. Esta ação deu ao atacante acesso à caixa de correio da vítima, tendo o respetivo conteúdo sido alegadamente divulgado no site *Wikileaks* [10].

Neste caso, é evidente a falha da componente humana.

Por um lado, a negligência por parte dos intervenientes ditou o comprometimento do acesso. O cuidado da vítima em confirmar com o técnico de IT a legitimidade do email, não fora suficiente para prevenir o ataque, uma vez que este último não alertou a vítima do *link* fraudulento.

Neste caso, tanto o gestor da campanha, como a própria candidata optaram por utilizar endereços de email pessoais ao invés de corporativos, por forma a tentar evitar possíveis escrutínios ou a divulgação de conteúdos inadequados [11].

Por outro lado, a utilização de um serviço de email pessoal não permitiu à equipa de IT ter a capacidade de impor políticas de segurança adequadas à natureza da informação, tais como a deteção automatizada de fraudes, a obrigação da rotação periódica de *passwords* e a ativação da autenticação multifator, conforme sugerido pelo técnico. Adicionalmente, com a utilização deste tipo de serviço, não foi possível à equipa de IT monitorizar proactivamente os acessos às contas.

Estas medidas, em particular a autenticação multifator, poderiam ter mitigado ou evitado o sucesso do ataque, dado que mesmo conhecendo as credenciais (utilizador e palavra-passe), o atacante estaria obrigado a apresentar um segundo fator de autenticação, como palavras-passe de utilização única, cujo gerador estaria, idealmente, na posse do titular legítimo da conta [11] [12].

Neste ataque, apesar de terem ocorrido quebras na segurança, não foram exploradas quaisquer vulnerabilidades tecnológicas, mas sim, vulnerabilidades *humanas* e na configuração tecnológica realizada pelos intervenientes [12].

Outro exemplo em que a correta adoção de medidas tecnológicas poderia ter mitigado, ou evitado o sucesso do ataque, foi em 2017, em que a página de uma rede social da empresa de Cibersegurança *McAfee* foi alvo de *defacing*.

Nesta situação, um dos ex-gestores mantinha acesso de administração à página,

mesmo quando já não tinha responsabilidades para com a empresa. De acordo com a investigação realizada, as credenciais do ex-colaborador foram comprometidas num ataque que levou à divulgação de credenciais de utilizadores de uma outra rede social.

A investigação concluiu que o ex-colaborador utilizou a mesma palavra-passe para todas os seus perfis, e procedeu à alteração da mesma, na rede que sofreu o ataque, e não na rede onde lhe tinham dado acessos de gestão à página da *McAfee*.

Tanto o ex-colaborador como a própria empresa de cibersegurança apresentaram falhas. O primeiro, por ter adotado a reutilização de palavras-passe, e não ter utilizado mecanismos que pudessem ajudar a melhorar a segurança das suas contas, como é o caso da autenticação multifator. A empresa, no entanto, deveria ter revogado os privilégios do ex-colaborador quando estes deixaram de fazer sentido.

Este ataque levou a um dano de imagem à empresa, já que a própria empresa tinha como missão a proteção dos seus clientes de ataques deste tipo, e ela própria fora atacada [13][14].

Com base nestes exemplos, será incorreto assumir-se que a prevenção de ataques com origem humana será exclusiva das equipas de segurança informática. A consciencialização dos utilizadores e a responsabilidade destes por pequenos pormenores fará parte de um conjunto de medidas de elevada importância para assegurar a segurança das organizações.

3. Ataques Tecnológicos

Apesar do constante aumento de ataques de engenharia social ou de ataques baseados em erros humanos, o número de novas vulnerabilidades tecnológicas detetadas anualmente, tem também vindo a aumentar, sendo que nos últimos 4 anos, teve um aumento muito considerável face aos anos anteriores, conforme mostra o gráfico da Figura 3.

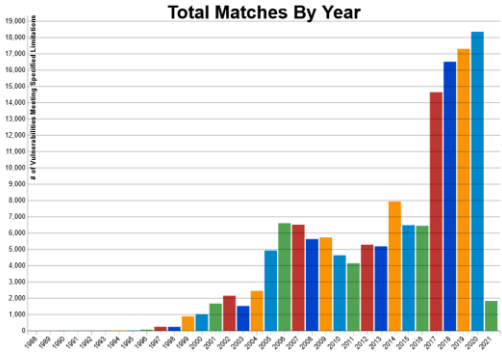

Figura 3 - Evolução do número anual de vulnerabilidades tecnológicas divulgadas pelo NIST [15]

A base de dados de CVE's (*Common Vulnerabilities and Exposures*) do *National Institute of Standards and Technology* (NIST National Vulnerabilities Database) é uma base de dados de vulnerabilidades conhecidas, mantida pelo governo dos Estados Unidos, na qual é feita a respetiva classificação, tendo em conta a natureza, severidade, e outros fatores relevantes para a sua indexação [15].

Acompanhando o número de vulnerabilidades detetadas, a proporção do número de vulnerabilidades com severidade "Média" e "Alta" tem também vindo a aumentar[1].

1 À data da escrita deste artigo, cerca de 2000 vulnerabilidades foram publicadas no ano de 2021. No entanto, a tendência para o aumento da percentagem de vulnerabilidades com maior severidade aparenta se manter, visto que em fevereiro, o número de vulnerabilidades com severidade "Média" ou "Alta" é já superior ao número de vulnerabilidades com severidade "Baixa".

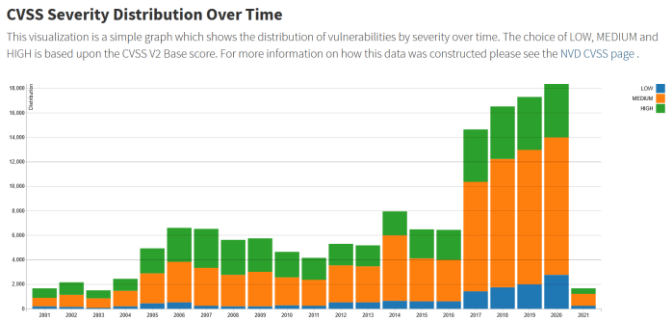

Figura 4 - Distribuição de severidade das vulnerabilidades ao longo do tempo [15]

A divulgação deste tipo de informação tem como objetivo lançar o alerta para a existência de possíveis riscos de ataque, tendo com intuito a promoção da necessidade da remediação destes.

No entanto, esta divulgação pública poderá também ser utilizada como um elemento guia para os atacantes, dado que nem sempre as organizações dão atenção proativa a este tipo de questões, como será discutido no caso abaixo analisado.

Em 2017, a agência de crédito *Equifax* foi alvo de um ataque de *hacking* à sua infraestrutura tecnológica, que levou à extorsão da informação pessoal e financeira de cerca de 140 milhões de cidadãos, a maioria de nacionalidade americana.

A 6 de março daquele ano, a *Apache Software Foundation* divulgou a vulnerabilidade CVE-2017-5638, a qual permitia a execução remota de código em aplicações web baseadas em determinadas versões da *framework Apache Struts* [16][17][18].

Esta falha, presente num sistema legado para gestão de disputas de clientes da *Equifax*, exposto à *Internet*, não tardou em ser explorada.

Pouco tempo depois da divulgação pública da falha, surgiram provas de conceito a demonstrar a sua exploração, cuja utilização foi identificada pela *Cisco Talos Intelligence Group*, em sistemas monitorizados por si [19].

Inicialmente, a exploração da falha foi utilizada para a execução de comandos simples, que permitiam a recolha de informações, como a identificação do utilizador com

o qual a aplicação executava, ou informações relativas aos sistemas remotos.

No entanto, houve uma rápida evolução para a execução de comandos mais complexos, tais como a desativação de *firewalls* e a descarga de código binário para execução remota, que levou à implementação de sistemas *webshell*, de forma a permitir aos atacantes outras formas de aceder aos sistemas sem recorrer à exploração da falha, caso esta fosse eventualmente corrigida [20][21].

De acordo com a agência de notícias *Bloomberg*, o ataque e intrusão à *Equifax* teve início 4 dias após a divulgação pública da falha, apesar do investimento considerável em medidas de proteção tecnológicas.

Ainda antes do ataque, uma consultora contratada para a avaliação de segurança da Equifax identificou várias falhas na configuração tecnológica dos sistemas, bem como na aplicação de correções para remediação de vulnerabilidades.

Adicionalmente, a saída e rotação de elementos-chave da empresa em anos anteriores, como o *Chief Information Security Officer*, contribuiu de forma negativa para a manutenção de políticas de segurança estáveis na *Equifax*. Por essa altura, era opinião comum de vários elementos que a segurança era descorada, a favor da entrega de resultados [22].

Apesar dos alertas, a agência de crédito declinou corrigir ou assumir as falhas, argumentando, com a opinião da investigação não ter sido levada a cabo por elementos com a senioridade adequada [23].

Quatro meses depois, em finais de julho de 2017, a equipa técnica da *Equifax* deu conta do ataque durante a realização de operações de rotina num equipamento de rede destinado à interceção e análise de tráfego encriptado.

Aquando da renovação de um certificado digital expirado, um membro da equipa de comunicações identificou padrões de tráfego fora do comum, nos quais verificou a execução de comandos fora dos parâmetros e métodos habituais, pelo que procedeu de imediato ao bloqueio das origens de tráfego, e ao reporte do caso a níveis superiores, o que levou a *Equifax* a despoletar o início da investigação, recorrendo à consultora anteriormente contratada.

Foi concluído que o certificado em questão esteve em uso durante cerca de 10 meses depois de ter expirado. Desta forma, não foi possível detetar a intrusão, uma vez que não era possível ao equipamento de rede desencriptar o tráfego encriptado [24].

Apesar de também não existir preservação de registos (*logs*[2]) a longo prazo, a análise forense permitiu aos auditores reconstruir em detalhe as ações levadas a cabo pelos atacantes, que serviram de *input* para as investigações levadas a cabo.

Entre elas, o Comité de Investigação do Senado dos Estados Unidos considera que houve negligência na forma como a agência zelava pela segurança do seu parque informático.

Em 2015 foi implementada uma política de segurança para gestão de vulnerabilidades e implementação de correções, a qual identificou mais de 8500 vulnerabilidades, nas quais um número acima de 1000 era considerado de severidade "Média" ou "Alta". Até então, a *Equifax* não detinha qualquer política formal para implementação de correções na companhia.

No entanto, não foi dado seguimento formal para a execução da política, pelo que a agência optou por seguir uma abordagem reativa, em que apenas aplicaria correções, caso os sistemas de *scanning* as identificassem, o que neste caso, não aconteceu.

Ainda que a vulnerabilidade utilizada para o ataque tivesse sido discutida em reuniões mensais, a respetiva correção não foi implementada imediatamente, em parte devido à complexidade dos procedimentos impostos, que obrigava a um envolvimento de várias entidades da organização por forma a coordenar a atividade de *patching*.

A não atualização do sistema de inventariação fez também com que a própria existência do componente com a vulnerabilidade não fosse considerada. Outro fator causado pela não implementação da correção está também relacionado com o alerta para a existência da vulnerabilidade não ter sido comunicado ao responsável pelo sistema afetado.

O Comité de Investigação defende também que houve negligência na gestão da

2 "*Logs*" são registos de atividade de sistemas informáticos, úteis para recriar os passos executados por atacantes.

infraestrutura. A expiração de um certificado digital fez com que deixasse de existir monitorização de tráfego encriptado, o que só foi remediado durante uma operação de rotina, tendo sido ignorado um alerta gerado pela monitorização. [20] [23].

A nível de arquitetura técnica, o impacto do ataque poderia ter sido igualmente reduzido caso tivesse sido adotada uma segmentação a nível de rede. Não havendo segmentação, o acesso a uma base de dados permitiu aceder a várias outras, incluindo a um repositório onde se encontravam credenciais não encriptadas para outras bases de dados.

Esta decisão de arquitetura foi tomada com o intuito de favorecer a usabilidade e aumentar a eficiência na implementação de operações do negócio, no entanto, comprometendo e descorando a segurança e indicações do NIST.

Em comparação, o Comité refere duas outras entidades concorrentes que detinham serviços afetos pela vulnerabilidade.

Nestas, a definição e imposição formal de políticas de segurança, prazos e procedimentos para aplicação de correções, a realização de análises periódicas aos elementos inventariados, os quais eram mantidos atualizados, permitiram à *Experian* e à *TransUnion* proceder à aplicação proativa das correções necessárias, não havendo registos de acessos indevidos com recurso à vulnerabilidade que afetou a *Equifax* [25].

David Webb, na altura *Chief Information Officer* da *Equifax*, assume que o ataque poderia ter sido evitado, caso a vulnerabilidade que motivou o ataque tivesse sido corrigida.

Não obstante, não são claras as razões que levaram a *Equifax* a ignorar recomendações do NIST, ou os requisitos de segurança das suas próprias políticas [20] [25]. Como consequência, a agência viu várias das suas certificações como a ISO 27001 e *Payment Card Industry* (PCI) suspensas, na sequência do ataque [26].

4. A eficácia da Formação

Um estudo realizado em 2009 numa organização ligada ao ramo do transporte de mercadorias da República da Turquia sobre a formação na segurança de informação nas organizações, revela que grande parte dos incidentes se devem a erros não intencionais, e ao desconhecimento de boas práticas de segurança e tecnológicas por parte dos colaboradores, tais como a utilização de *palavras-passe* de fácil adivinhação, abandono de equipamentos informáticos sem os proteger, entre outras [27].

Neste estudo, foram levadas a cabo várias sessões de formação, por forma a contribuir para a elucidação dos colaboradores sobre bons costumes que possam ajudar a prevenir quebras na segurança.

Para avaliar a eficácia da formação dos utilizadores, foram realizadas várias auditorias de segurança à complexidade das palavras-passe, bem como definidos patamares de objetivos que deveriam ser cumpridos ao fim de um determinado prazo.

A consciencialização dos colaboradores da organização para a necessidade da utilização de palavras-passe com alta complexidade teve efeitos positivos. Um universo de cerca de 3000 utilizadores, teve as respetivas palavras-passe sujeitas a ataques de força bruta durante 24 horas, sendo que o número de palavras-passe que resistiu aos mesmos, passou de 1,2% para 36,4% no espaço de um ano.

Um outro estudo realizado em 2019 [28], avalia a preferência de utilizadores sobre os métodos utilizados para a formação, e a respetiva eficiência na resposta a ataques de *phishing*.

Apesar do estudo não ter chegado a uma conclusão concreta no que toca à preferência do tipo de formação entre a leitura de documentação, a assistência a vídeos, formação presencial, ou recurso a jogos interativos educacionais, este chega a resultados positivos, em que os participantes do estudo demonstraram uma melhoria na identificação de ataques de *phishing* após qualquer uma das diferentes formações ministradas.

Tendo em conta os estudos e as recomendações supracitadas, verifica-se que a formação de *soft-skills* e de boas práticas tem um papel relevante na consciencialização dos utilizadores na segurança da informação das organizações, as quais, se aplicadas, poderiam ter evitado ou mitigado os ataques das entidades nos exemplos anteriores.

No que toca à educação tecnológica, as investigações concluem que a agência do exemplo exposto não mantinha práticas consistentes com as recomendações da *framework* de cibersegurança do NIST [29], nem as equipas técnicas estavam preparadas para aplicar as políticas em vigor.

Apesar de voluntária, a aplicação de várias recomendações da *framework* do NIST poderia ter mitigado, ou evitado o ataque, tal como confirmado pelo CIO David Webb.

Alguns exemplos de recomendações que não foram aplicadas:

- Não existia inventariação adequada que permitisse identificar a utilização de determinadas componentes de *software*, e onde as mesmas estavam implementadas (ID.AM-1/ID.AM-2);
- Não existia segregação ou segmentação de redes, de forma a isolar sistemas heterogéneos (PR.AC-5);
- Não existia documentação ou um processo proativo de mitigação de vulnerabilidades constantes nos componentes de *software* (RS.MI-3);
- A deteção de intrusão não se encontrava em funcionamento devido à não renovação proativa um certificado digital (DE.CM-1/DE.CM-4/DE.CM-7);
- Existiam credenciais armazenadas de forma desprotegida (PR.AC-4);
- Não existia uma política de retenção de *logs* adequada (PR.MA-2).

À semelhança das formações para preparação de *phishing*, a formação técnica e em segurança *poderia* ter alavancado a consciencialização das equipas técnicas para a importância do seguimento de boas práticas, e melhorar a dedicação destas no que toca à manutenção dos sistemas internos, por forma a prevenir ataques deste, e de outros tipos.

Os relatórios não referem a existência de formações lecionadas às equipas antes do incidente. É dada, no entanto uma recomendação de formação das equipas relativa aos procedimentos internos de segurança.

5. Conclusão

Esta investigação permitiu, em primeiro lugar, rever três fenómenos criminosos dos tempos atuais, cuja atuação tem vindo a comprometer de forma significativa a segurança da informação de inúmeras organizações nos últimos anos.

Seguindo a tendência atual, o desenvolvimento de novas soluções tecnológicas apresentará novas funcionalidades que poderão ser utilizadas para otimizar a produtividade empresarial, bem como o quotidiano da população em geral.

A adoção das novas tecnologias irá inevitavelmente introduzir novos vetores de ataque que serão alvo de exploração por agentes maliciosos, tendo em vista tanto a negligência individual, desconhecimento, ou vulnerabilidades das tecnologias envolvidas.

A análise do caso de *phishing* permitiu evidenciar a facilidade com que o elemento humano é passível de ser explorado. O caso exposto, em particular, demonstra como os próprios elementos de equipas de suporte tecnológico, e com formação para tal, não são suficientes para prevenir um ataque dirigido, caso não seja dado um especial cuidado aos detalhes do mesmo.

Por outro lado, a conduta da vítima, apesar de inicialmente prudente, provou também não ser suficiente, uma vez que as indicações dadas pelo especialista não foram seguidas em pormenor, apesar deste último não ter identificado o risco iminente.

O caso de *defacing* à empresa de cibersegurança, também relacionado com descuido humano, permitiu comprovar que nem sempre as organizações especializadas seguem à risca as políticas que elas próprias defendem, caso os seus colaboradores não as pratiquem, o que sugeriu o impacto na que tal pode causar na imagem da organização.

No que toca ao caso de *hacking*, verificou-se um conjunto de fatores que permitiram a intrusão e fuga de informação dos sistemas da agência de crédito.

A falta de acompanhamento e de seguimento das políticas de segurança definidas deu origem a entropia entre as várias equipas da organização, o que demonstra que a definição de uma política de segurança por si não foi suficiente para a garantir.

Por outro lado, notou-se negligência por parte das equipas técnicas na gestão da infraestrutura informática, apesar de tecnologicamente, os equipamentos e funcionalidades necessárias para garantir a segurança, estarem presentes.

A falta de manutenção do equipamento de análise de tráfego encriptado ou a opção pela não segmentação de redes foram elementos que poderiam ter diminuído o impacto do ataque.

A ausência de uma política eficiente de aplicação de correções, e consequente não aplicação da correção que possibilitou o ataque, foi, de acordo com o *CIO* da altura, um elemento que poderia ter evitado a intrusão, por completo.

Por fim, não são claras as razões que levaram a *Equifax* a ignorar vários procedimentos, tendo-se verificado uma desconsideração generalizada no que toca à importância segurança da organização.

Adicionalmente, os relatórios do caso não referem ter sido dado qualquer tipo de formação às equipas técnicas antes do incidente.

No entanto, verifica-se uma recomendação em formar as equipas para os procedimentos internos, uma vez que aparentemente vários destes não foram levados a cabo adequadamente, devido à complexidade como os mesmos deveriam ser aplicados, ou por mero desconhecimento das equipas.

Assume-se que a *Equifax* poderia ter beneficiado com a educação das equipas técnicas, por forma a formalizar não só os procedimentos a adotar para a manutenção dos sistemas de segurança, como por exemplo, a importância para a renovação proativa de certificados digitais, mas também a nível tecnológico, onde não só a segurança, com a manutenção em geral dos sistemas empresariais poderia beneficiar, como por exemplo, com a segmentação de redes [30].

"*A cibersegurança é um desporto coletivo, no qual todos têm de desempenhar o seu papel (…). As ferramentas podem ser de grande utilidade, mas apenas a conjugação de pessoas, ferramentas, [e] procedimentos (…) permite uma defesa eficiente*" [14].

Em suma, nota-se que em todos os exemplos apresentados, os incidentes apresentados recaem em pontos que não foram assegurados, nomeadamente na conjugação entre o fator humano com o tecnológico. Um não será suficiente sem o outro para garantir a segurança das organizações, nem tampouco será suficiente a uma equipa de segurança garantir que uma organização está segura, caso os seus utilizadores não sigam boas práticas.

REFERÊNCIAS

[1] OECD, «ICT Access and Usage by Businesses». 2021, [Em linha]. Disponível em: https://stats.oecd.org/.

[2] S. Fernandez, B. Vieira, P. Jenkins, e McKinsey, «Europe's migration to digital services during COVID-19 | McKinsey». https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages (acedido Jan. 31, 2021).

[3] Centro Nacional de Cib, «Relatório Riscos & Conflitos 2020», 2020.

[4] CNCS, «Relatório Cibersegurança em Portugal - Sociedade 2020», 2020.

[5] K. D. Mitnick e W. L. Simon, *The Art of Deception: Controlling the Human Element in Security*. 2002.

[6] «ENISA Threat Landscape 2020 - Phishing», 2020, [Em linha]. Disponível em: https://www.enisa.europa.eu/publications/phishing/at_download/fullReport.

[7] Proofpoint, «Human Factor Report 2019», 2019, [Em linha]. Disponível em: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf.

[8] K. Rekouche, «Early Phishing», pp. 1–9, 2011, [Em linha]. Disponível em: http://arxiv.org/abs/1106.4692.

[9] K. Krawchenko, «The phishing email that hacked the account of John Podesta», *CBS Interactive Inc.*, 2016. https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/ (acedido Fev. 03, 2021).

[10] «WikiLeaks - The Podesta Emails». https://wikileaks.org/podesta-emails/ (acedido Fev. 04, 2021).

[11] R. Mitchell, «The Podesta Emails - Anatomy of an attack». https://p3isys.com/p3isys-tech-blog/153-podestahack (acedido Fev. 04, 2021).

[12] J. Koebler, «Basic Digital Security Could Have Prevented One of the Biggest Political Scandals in American History». https://www.vice.com/en/article/ywkd35/two-factor-authentication-russia-hacking-indictment (acedido Fev. 09, 2021).

[13] «McAfee LinkedIn page hijacked | CSO Online». https://www.csoonline.com/article/3190163/mcafee-linkedin-page-hijacked.html (acedido Fev. 06, 2021).

[14] A. Cerra, *The Cybersecurity Playbook*, 1st ed. Wiley, 2019.

[15] «NVD - Statistics». https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all (acedido Fev. 06, 2021).

[16] NIST.gov, «nvd - cve-2017-5638», *Nvd.nist.gov*. 2017, Acedido: Fev. 07, 2021. [Em linha]. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2017-5638.

[17] «Apache Struts 2 Vulnerability Leads to RCE». https://www.trendmicro.com/en_us/research/17/c/cve-2017-5638-apache-struts-vulnerability-remote-code-execution.html (acedido Fev. 07, 2021).

[18] Lukasz Lenart, «S2-045 - Apache Struts 2 Wiki - Apache Software Foundation», 2016. https://cwiki.apache.org/confluence/display/WW/S2-045 (acedido Fev. 07, 2021).

[19] «GitHub - tengzhangchao/Struts2_045-Poc: Struts2-045 POC». https://github.com/tengzhangchao/Struts2_045-Poc (acedido Fev. 07, 2021).

[20] US HoR, «The Equifax Data Breach», *US House Represent. Comm. Overs. Gov. Reform*, vol. 87, n. 12, p. 14, 2018, [Em linha]. Disponível em: http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=126654696&site=eds-live&scope=site.

[1] OECD, «ICT Access and Usage by Businesses». 2021, [Em linha]. Disponível em: https://stats.oecd.org/.

[2] S. Fernandez, B. Vieira, P. Jenkins, e McKinsey, «Europe's migration to digital services during COVID-19 | McKinsey». https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages (acedido Jan. 31, 2021).

[3] Centro Nacional de Cib, «Relatório Riscos & Conflitos 2020», 2020.

[4] CNCS, «Relatório Cibersegurança em Portugal - Sociedade 2020», 2020.

[5] K. D. Mitnick e W. L. Simon, *The Art of Deception: Controlling the Human Element in Security*. 2002.

[6] «ENISA Threat Landscape 2020 - Phishing», 2020, [Em linha]. Disponível em: https://www.enisa.europa.eu/publications/phishing/at_download/fullReport.

[7] Proofpoint, «Human Factor Report 2019», 2019, [Em linha]. Disponível em: https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf.

[8] K. Rekouche, «Early Phishing», pp. 1–9, 2011, [Em linha]. Disponível em: http://arxiv.org/abs/1106.4692.

[9] K. Krawchenko, «The phishing email that hacked the account of John Podesta», *CBS Interactive Inc.*, 2016. https://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/ (acedido Fev. 03, 2021).

[10] «WikiLeaks - The Podesta Emails». https://wikileaks.org/podesta-emails/ (acedido Fev. 04, 2021).

[11] R. Mitchell, «The Podesta Emails - Anatomy of an attack». https://p3isys.com/p3isys-tech-blog/153-podestahack (acedido Fev. 04, 2021).

[12] J. Koebler, «Basic Digital Security Could Have Prevented One of the Biggest Political Scandals in American History». https://www.vice.com/en/article/ywkd35/two-factor-authentication-russia-hacking-indictment (acedido Fev. 09, 2021).

[13] «McAfee LinkedIn page hijacked | CSO Online». https://www.csoonline.com/article/3190163/mcafee-linkedin-page-hijacked.html (acedido Fev. 06, 2021).

[14] A. Cerra, *The Cybersecurity Playbook*, 1st ed. Wiley, 2019.

[15] «NVD - Statistics». https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all (acedido Fev. 06, 2021).

[16] NIST.gov, «nvd - cve-2017-5638», *Nvd.nist.gov*. 2017, Acedido: Fev. 07, 2021. [Em linha]. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2017-5638.

[17] «Apache Struts 2 Vulnerability Leads to RCE». https://www.trendmicro.com/en_us/research/17/c/cve-2017-5638-apache-struts-vulnerability-remote-code-execution.html (acedido Fev. 07, 2021).

[18] Lukasz Lenart, «S2-045 - Apache Struts 2 Wiki - Apache Software Foundation», 2016. https://cwiki.apache.org/confluence/display/WW/S2-045 (acedido Fev. 07, 2021).

[19] «GitHub - tengzhangchao/Struts2_045-Poc: Struts2-045 POC». https://github.com/tengzhangchao/Struts2_045-Poc (acedido Fev. 07, 2021).

[20] US HoR, «The Equifax Data Breach», *US House Represent. Comm. Overs. Gov. Reform*, vol. 87, n. 12, p. 14, 2018, [Em linha]. Disponível em: http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=126654696&site=eds-live&scope=site.

[21] «Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Content-Type: Malicious - New Apache Struts2 0-day Under Attack». https://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html (acedido Fev. 07, 2021).

[22] M. Riley, J. Robertson, e A. Sharpe, «The Equifax Hack Has the Hallmarks of State-Sponsored Pros - Bloomberg», *Bloom. Technol.*, pp. 1–6, 2017, Acedido: Fev. 07, 2021. [Em linha]. Disponível em:

https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

[23] J. Fruhlinger, «Equifax data breach FAQ: What happened, who was affected, what was the impact?», *CSO*, 2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (acedido Fev. 02, 2021).

[24] «New evidence raises doubts about executives' handling of the Equifax breach - The Verge». https://www.theverge.com/2017/9/19/16332096/new-evidence-raises-doubts-about-executives-handling-equifax-breach (acedido Fev. 07, 2021).

[25] Permanent Subcommittee on Investigations e United States Senate, «How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach», 2019.

[26] Equifax Inc., «2018 Annual Report», 2018. Acedido: Fev. 07, 2021. [Em linha]. Disponível em: https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual Reports/2018-annual-report.pdf.

[27] M. Eminağaoğlu, E. Uçar, e Ş. Eren, «The positive outcomes of information security awareness training in companies - A case study», *Inf. Secur. Tech. Rep.*, vol. 14, n. 4, pp. 223–229, Nov. 2009, doi: 10.1016/j.istr.2010.05.002.

[28] K. F. Tschakert e S. Ngamsuriyaroj, «Effectiveness of and user preferences for security awareness training methodologies», *Heliyon*, vol. 5, n. 6, p. e02010, 2019, doi: 10.1016/j.heliyon.2019.e02010.

[29] «Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1», Gaithersburg, MD, Abr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[30] S. Laan, *IT Infrastructure Architecture-Infrastructure Building Blocks and Concepts Third Edition*. Lulu. com, 2017.