A componente humana na Segurança da Informação

Luís Borges Gouveia
lmbg@ufp.edu.pt, (UFP, CITCEM, APDSI)

UNIVERSIDADE LUSÓFONA

***Digital Privacy and Security Conference* 2024**
VII Jornadas de Segurança Informática
https://privacyandsecurityconference.pt/ 10- 11 January 2024

UNIVERSIDADE FERNANDO PESSOA
CITCEM CENTRO DE INVESTIGAÇÃO TRANSDISCIPLINAR CULTURA, ESPAÇO E MEMÓRIA
fct Fundação para a Ciência e a Tecnologia
UIDB/04059/2020
U.PORTO FLUP FACULDADE DE LETRAS UNIVERSIDADE DO PORTO
APDSI

Introdução

- A **informação** é um ativo vital na sociedade atual, que requer proteção contra ameaças internas e externas
- A **segurança da informação** visa garantir a confidencialidade, integridade e disponibilidade da informação, bem como a autenticidade (ISO 27000), mas também o não repúdio e a legalidade dos processos de informação
- As **pessoas** são um elemento central para a segurança da informação, pois produzem, gerem, utilizam e partilham informação, mas também podem comprometê-la por negligência, desconhecimento ou má conduta

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

A segurança da informação

- **disciplina** que abrange vários aspetos, como a gestão de riscos, as políticas e normas de segurança, os mecanismos de criptografia, os sistemas de autenticação e autorização, os sistemas de deteção e prevenção de intrusões, os planos de contingência e recuperação, entre outros
- útil para **proteger os ativos de informação** das organizações e dos indivíduos, bem como para integrar o cumprimento de leis e regulamentos aplicáveis à proteção de dados pessoais e sensíveis, como é o caso do RGPD
- tema relevante e atual que requer uma **constante atualização e adaptação a tecnologias emergentes**, como é o caso da inteligência artificial ou da computação quântica
- **área de oportunidade** para os profissionais que se dedicam ao estudo, à investigação e à aplicação das melhores práticas de segurança nos diversos domínios da informação

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Desafios no contexto digital

- O contexto digital e a crescente sofisticação de sistemas e redes, cada vez mais interligadas, constituem um **ecossistema digital**, onde cada indivíduo tem de encontrar o seu equilíbrio e dotar-se com os meios e capacidades para aceder, gerir e gerar informação e valor (o que tem impacto na segurança da informação)
- Os **desafios da segurança da informação** no contexto digital são vários e complexos, envolvem a proteção dos dados e dos sistemas de informação contra ameaças internas e externas em constante evolução e ganham uma sofisticação que cada indivíduo ou mesmo organização, por si próprios, não conseguem acompanhar
  - vulnerabilidades de *software*, *hardware* e sistemas; privacidade de dados pessoais e sensíveis; sensibilizar para uma cultura de segurança (da informação); existência de boas práticas para evitar riscos e incidentes; lidar com ameaças do uso e exploração do digital por entidades e pessoas; reduzir o custo das soluções de segurança
- Para enfrentar estes desafios, é importante adotar uma **abordagem integrada e um compromisso constante com a segurança da informação**, que envolva a gestão de riscos, as políticas e normas de segurança, os mecanismos de criptografia, os sistemas de autenticação e autorização, os sistemas de deteção e prevenção de intrusões, os planos de contingência e recuperação

Casos de incidentes de segurança da informação

https://bdigital.ufp.pt/handle/10284/12459

- **Crypto.com**: janeiro de 2023, um invasor obteve acesso a 133 carteiras de criptomoedas contornando a autenticação de dois fatores do sítio, por meio de técnicas de engenharia social
- **Cisco**: maio de 2022, um invasor conduziu uma série de ataques sofisticados de *phishing* de voz para aceder a uma conta Google de um funcionário da Cisco e depois usou as suas credenciais para aceder aos sistemas internos da Cisco
- **News Corp**: fevereiro de 2022, *hackers* infiltraram os servidores de vários meios de comunicação de propriedade da *News Corp* e roubaram dados confidenciais, além de publicarem notícias falsas
- **Microsoft**: março de 2022, um coletivo de *hackers* denominado *Lapsus$* conseguiu *hackear* a **Microsoft** e comprometer o *Cortana*, o *Bing* e vários outros produtos usando credenciais roubadas de um funcionário da *Microsoft*
- **SolarWinds**: dezembro de 2020, em que uma sofisticada campanha de ciberespionagem comprometeu a cadeia de fornecimento de software da *SolarWinds* (empresa fornecedora de ferramentas de gestão de rede a organizações em todo o mundo, incluindo várias agências governamentais dos EUA e empresas de dimensão mundial). Os invasores inseriram códigos maliciosos em atualizações legítimas de software que lhes permitiram aceder às redes dos clientes da *SolarWinds* e roubar dados confidenciais

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Casos de incidentes de segurança da informação

https://bdigital.ufp.pt/handle/10284/12459

- ***Equifax***: julho de 2017, *hackers* exploraram uma vulnerabilidade conhecida na estrutura de uma aplicação Web utilizada pela *Equifax* (uma das maiores agências de relatórios de crédito dos EUA), e acederam aos dados pessoais de cerca de 147 milhões de pessoas, incluindo os seus nomes, números de segurança social, datas de nascimento, endereços e números de cartão de crédito
- **Ataque de *ransomware WannaCry***: maio de 2017, um *worm* informático espalhou-se por milhares de computadores em todo o mundo, encriptando os seus dados e exigindo um resgate em *Bitcoin* para os desencriptar. O ataque afetou vários setores, incluindo hospitais, bancos, empresas e governos
- ***LinkedIn***: junho de 2016, *hackers* roubaram e publicaram online os dados de mais de 160 milhões de utilizadores da rede social profissional, incluindo os seus endereços de correio eletrónico e palavras-passe. As senhas tinham *hash*, mas sem uma sequência aleatória de dados, o que as tornava mais fáceis de serem quebradas. A violação também afetou outras plataformas de media social, como o *eHarmony* e o *Last.fm*
- **Sony PlayStation Network**: Abril de 2011, *hackers* invadiram o serviço de jogos online da *Sony* e roubaram os dados pessoais de cerca de 77 milhões de utilizadores, incluindo nomes, endereços, endereços de correio eletrónico, palavras-passe e detalhes de cartões de crédito. A violação também afetou a *Sony Online Entertainment* e a *Sony Pictures Entertainment*. A violação resultou no desligar do serviço da *PlayStation Network* por quase um mês e custou à Sony cerca de US$ 171 milhões de dólares

Casos de incidentes de segurança da informação

https://bdigital.ufp.pt/handle/10284/12459

- **Departamento de Educação da Pensilvânia**: Outubro de 2023, uma falha de software no Sistema de Gestão de Informação de Professores (TIMS) expôs os dados pessoais de centenas de milhares de professores e pessoal educativo. O incidente permitiu temporariamente que indivíduos que fizeram *login* no TIMS acedessem a informações pessoais pertencentes a outros utilizadores, incluindo professores, distritos escolares e funcionários do Departamento de Educação
- **Twitter**: julho de 2020, hackers comprometeram as contas de várias celebridades, políticos e empresas de destaque, incluindo Barack Obama, Elon Musk, Joe Biden e Apple, e publicaram *tweets* pedindo doações em Bitcoin. O ataque foi realizado usando técnicas de engenharia social para enganar os funcionários do *Twitter* para acesso às suas credenciais e a ferramentas internas
- **Marriott**: novembro de 2018, *hackers* roubaram os dados pessoais de cerca de 500 milhões de hóspedes que fizeram reservas nos hotéis *Starwood*, uma subsidiária do *Marriott*. A violação foi causada por uma falha na monitorização e segurança de uma base de dados comprometida desde 2014, quando a *Starwood* foi adquirida pela *Marriott*. A violação expôs nomes, endereços, números de telefone, endereços de correio eletrónico, números de passaporte, datas de nascimento e informações do programa de fidelidade de clientes
- **Anthem**: fevereiro de 2015, *hackers* acederam à base de dados da Anthem, uma das maiores companhias de seguros de saúde dos Estados Unidos, e roubaram os dados pessoais de cerca de 80 milhões de clientes e funcionários. A violação foi facilitada por um e-mail de *phishing* que enganou um funcionário da Anthem para que cedesse as suas credenciais
- **Target**: dezembro de 2013, hackers instalaram *malware* nos terminais de pagamento da *Target*, uma das maiores cadeias de retalho dos Estados Unidos, e roubaram os dados de cartões de crédito de cerca de 40 milhões de clientes. A violação, facilitada por falha na segurança da rede da *Target*, que permitiu o acesso à rede através de um terceiro fornecedor

Incidentes que envolvem questões associadas com a natureza humana

- A **natureza humana** refere a essência do ser humano na relação consigo mesmo e com o meio ambiente (conjunto de traços, incluindo maneiras de **pensar, sentir ou agir, que os seres humanos tendem a ter**, independente da influência da cultura)
- Mesmo no contexto de organizações que possuem elevados padrões associados com a segurança da informação, ocorrem incidentes, com impacto, mostrando aparentes fragilidades que exigem um aprofundamento de como evitar situações futuras associadas com pessoas, nomeadamente internas ao serviço e devidamente credenciadas
- Exemplos associado aos Serviços de Segurança e das Forças Armadas dos Estados Unidos
  - Os casos *Edward Snowden* e *Bradley Manning* (**ativismo/denunciantes**) e o mais recente caso *Jack Teixeira* (**aparente necessidade de afirmação**):

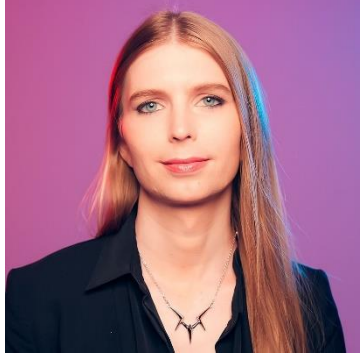
Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Edward Snowden
(CIA / NSA)

- O caso *Vigilância Global* é um escândalo de espionagem que envolveu o ex-analista da CIA e da NSA *Edward Snowden*, que revelou publicamente detalhes dos programas de vigilância do governo dos Estados Unidos que monitorizavam a comunicação e a privacidade de milhões de pessoas, incluindo líderes e cidadãos de outros países
- Divulgou documentos secretos para os jornais *The Guardian* e *The Washington Post* em 2013, levando a acusações de espionagem e roubo de propriedade do governo pelos Estados Unidos
- Gerou uma crise diplomática entre os Estados Unidos e os seus aliados, além de um debate global sobre os limites da segurança nacional; direitos de e à privacidade e de liberdade de expressão

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Bradley Manning
(Exército EUA)

- O caso *Cablegate* é um caso de fuga de informações secretas dos Estados Unidos pelo soldado *Chelsea Manning* (à época *Bradley Manning*)
- Preso em 2010, após ter fornecido mais de 700 mil documentos e vídeos ao sítio *Web WikiLeaks* (os documentos revelavam detalhes sobre as guerras no Iraque e no Afeganistão, e sobre a diplomacia americana)
- Condenada a 35 anos de prisão por vários crimes, incluindo espionagem e roubo de propriedade do governo (no entanto foi libertada em 2017, após o presidente Barack Obama comutar a sua pena)
- Considerada uma denunciante (*whistleblower*) e uma ativista pelos direitos humanos, por uns, e uma traidora e criminosa, por outros

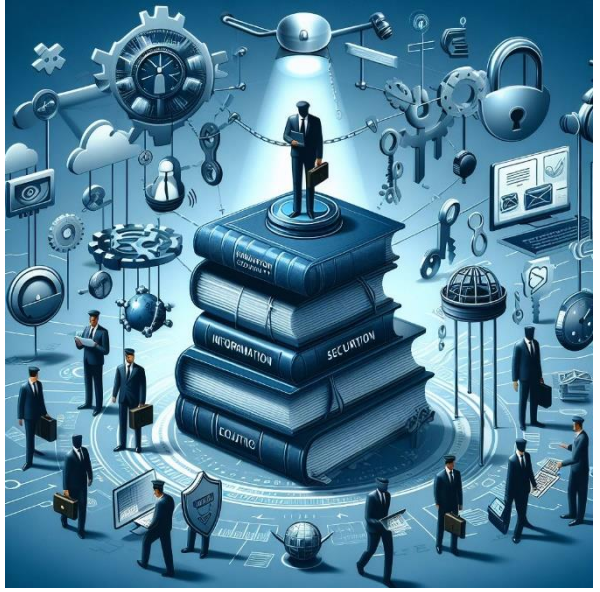
Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Jack Teixeira
(Guarda Nacional EUA)

- Jovem de 21 anos que trabalhava numa base militar dos Estados Unidos e que divulgou os documentos secretos sobre a guerra na Ucrânia para impressionar os membros de um grupo *online* de entusiastas por armas, no *discord*.
- Descrito como racista e fanático por armas, com acesso a informações sensíveis sobre as operações militares dos Estados Unidos e dos seus aliados na Ucrânia, na qualidade de técnico de informática, credencial *top secret*
- A fuga de informação ocorreu em abril de 2023 e causou uma crise diplomática entre os Estados Unidos e os seus aliados, constituindo um risco para a segurança nacional
- Ocorreu num momento de tensão entre os EUA e a Rússia, devido à guerra na Ucrânia, comprometendo fontes e métodos de espionagem dos EUA, bem como a confiança dos seus aliados, com impacto nas decisões políticas e militares no contexto do próprio conflito

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Conclusão



- A **segurança da informação é um tema cada vez mais relevante na era digital**, pois envolve a proteção dos dados e dos sistemas de informação contra ameaças internas e externas
- As **pessoas são um elemento central para a segurança da informação**, pois produzem, gerem, utilizam e partilham informação, mas também a podem comprometer por negligência, desconhecimento ou má conduta

Luis Borges Gouveia, *lmbg@ufp.edu.pt*

Luis Borges Gouveia

Dip (UPT), MsC (FEUP), PhD (ULANCS), PD (FLUP)

http://homepage.ufp.pt/lmbg

Professor Catedrático da Universidade Fernando Pessoa (**UFP**)
https://www.ufp.pt/

Membro Integrado e atualmente coordenador do grupo Informação, Comunicação e Cultura Digital do **CITCEM**, Universidade do Porto
https://citcem.org/

Sócio e Membro da Direção da Delegação Norte da **APDSI** (ONG que promove a discussão do digital, do seu impacto em políticas de como promover uma sociedade mais capaz de lidar com o uso e exploração do digital)
https://apdsi.pt/

UIDB/04059/2020