Cibersegurança em 2021: ameaças, comportamentos e desafios

Isabel Baptista
Centro Nacional de Cibersegurança

A Cibersegurança
hoje

A **transição digital** exige segurança

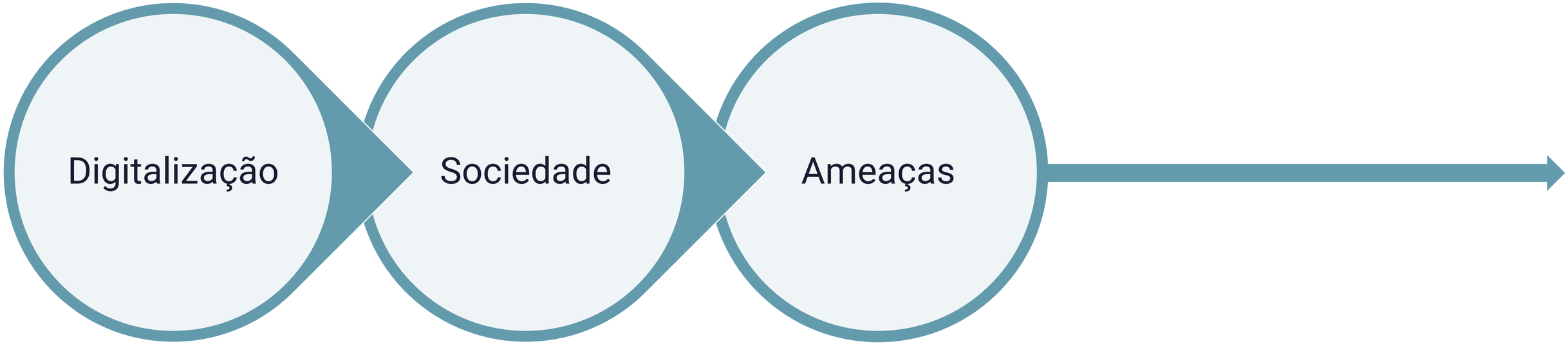
O digital como **substituição do presencial** aumenta os riscos

O digital cria **novas ameaças**

As **ameaças *offline* transferem-se** para o *online*

A cibersegurança é um **pilar** da democracia, da economia e da sociedade

A cibersegurança responde ao ciclo da digitalização *que faz surgir novas e velhas ameaças*



Teletrabalho/modelo híbrido e os **novos (velhos)** riscos

flexibilização dos processos

trabalho por **objetivos**

autonomia de horários

mais **dependência** do digital

menor controlo físico

necessidade de mais **confiança**

mais exigências de **CIBERSEGURANÇA**

Incidentes e cibercrime
principais números

2019/2020	**aumento** de 79% no nº de incidentes registados pelo CERT.PT (S/V) (CNCS, 2021a)
	aumento de 27% no nº de crimes informáticos participados (RASI, 2021)
	aumento de 183% no nº de denúncias ao Gabinete de Cibercrime do MP (PGR, 2021)
	+ 101% no nº de **incidentes** registados pelo CERT.PT no **primeiro semestre** de 2020 face ao mesmo período de 2019 (CNCS, 2020a)
2020/2021	**+ 23%** no nº de **incidentes** registados pelo CERT.PT no **primeiro semestre** de 2021 face ao mesmo período de 2020 (CNCS, 2021b)
2009/2020	**+ percentagem**, de **0,6% em 2009 para 7,4% em 2020**, de crimes informáticos e relacionados a informática, entre todos os crimes participados no país (CNCS, 2021b)

Algumas **tendências**

A **Administração Pública** é um dos **alvos principais** de ciberataques

A **ciberespionagem** afeta o setor público e o setor privado como atividade quase natural

Os ataques são mais dirigidos a **indivíduos relevantes**, através de ***phishing*** e **engenharia social**

O ***malware*** é uma ameaça central: *ransomware*, *spyware*, etc.

As **redes sociais** são fonte de reconhecimento das vítimas

Os **telemóveis** são superfícies de ataque, que podem atingir a esfera profissional

(ENISA, 2020)

Agentes de ameaças mais relevantes atualmente
Portugal

- Agentes Estatais
- Cibercriminosos
- Hacktivistas

Atitudes e comportamentos
Portugal

Menos portugueses do que a média da UE a sentirem-se **muito bem informados** sobre os riscos de cibercrime: 11% na UE e 2% em Portugal, em 2019 (EC, 2020)

Menos portugueses que afirmam ser capazes de se **proteger** o suficiente do cibercrime, em 2019 – menos 8 pp (45%) e menos 9 pp na média da UE (52%) do que em 2018 (EC, 2020)

Maior **preocupação** dos portugueses com o cibercrime, em contraciclo com a UE. P. ex.: a preocupação com a fraude em cartão bancário ou em banco *online* aumentou 10 pp (74%), a média da UE desceu 3 pp (67%), entre 2018 e 2019 (EC, 2020)

Portugal é o país da UE no qual mais pessoas **NÃO** **alteraram alguma *password*** no ano anterior, em 2019: 48%, enquanto a média da UE é 31% (EC, 2020)

Poucas empresas portuguesas **com seguro** contra incidentes de segurança em TIC – 10%, contra 21% da média da UE (Eurostat, 2020)

Menos informação + Insegurança
+ Preocupação + Inação

Vulnerabilidades
como pontos críticos do cibercrime

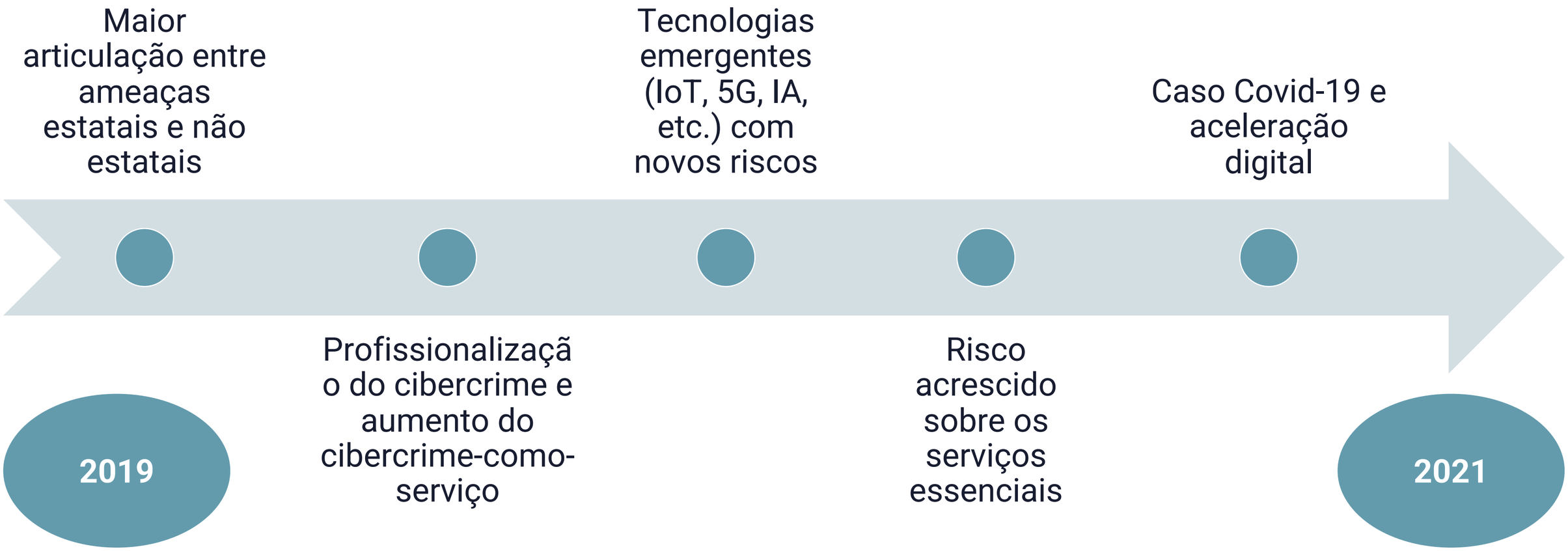
Exploração das **vulnerabilidades do humano** através da engenharia social

Exploração das **vulnerabilidades da digitalização** crescente

Exploração das **vulnerabilidades das novas tecnologias**

Aumento no nº de **incidentes** e do **cibercrime**

Tendências globais



April 12, 2018

Operation Parliament targeting Middle East nations with cyberespionage malware

Doug Olenick

Follow @DougOlenick

SC, 2018

AVISO

Cuidado com os *emails* e SMS suspeitos, bem como com os *links* e anexos, que podem conter ***malware***.

Este grupo atacou membros de **altos cargos** **de muitos países do Médio-Oriente, mas também na Europa, através de *spear-phishing*,** com o objetivo de, através de *malware*, recolher informação privilegiada.

CNCS

Fonte de imagem: https://www.scmagazine.com/home/security-news/government-and-defense/operation-parliament-targeting-middle-east-nations-with-cyberespionage-malware/

CIBERSEGURANÇA

Hackers roubaram conversas entre diplomatas da União Europeia durante anos

Empresa que detectou a operação diz que o ataque está ligado ao Governo chinês. Segurança das redes europeias posta em causa.

Alexandre Martins · 19 de Dezembro de 2018, 11:16

142 PARTILHAS

Público, 2018

Estas conversas foram captadas através de ***phishing*** às contas de diplomatas do Chipre, em que estes foram levados a **introduzir palavras-passe** que permitiu o acesso às bases de dados da UE.

AVISO

Cuidado com a **veracidade das plataformas** onde são introduzidas credenciais.

CNCS

Fonte da imagem: https://www.publico.pt/2018/12/19/mundo/noticia/hackers-roubaram-conversas-diplomatas-uniao-europeia-durante-anos-1855268

North Korean state hackers target retired diplomats and military officials

In a first of its kind operations, state-sponsored group goes after retired South Korean officials.

By Catalin Cimpanu for Zero Day | August 28, 2019 -- 12:53 GMT (13:53 BST) | Topic: Security

ZDNet, 2019

AVISO

Mesmo na **vida privada**, qualquer um é um possível alvo.

Um grupo patrocinado pela Coreia do Norte atacou **diplomatas, membros de governo e militares,** muitos deles **reformados,** da Coreia do Sul através de *emails* de *spear-phishing* que conduziam à **introdução de credenciais em *websites* falsos**.

CNCS

Fonte da imagem: https://www.zdnet.com/article/north-korean-state-hackers-target-retired-diplomats-and-military-officials/

Schneier on Security

Blog | Newsletter | Books | Essays | News | Talks | Academic

Home > Blog

Russia's SolarWinds Attack and Software Security

The information that is emerging about Russia's extensive cyberintelligence operation against the United States and other countries should be increasingly alarming to the public. The magnitude of the hacking, now believed to have affected more than 250 federal agencies and businesses — primarily through a malicious update of the SolarWinds network management software — may have slipped under most people's radar during the holiday season, but its implications are stunning.

Schneier on Security, 2021

Ataque à cadeia de fornecimento: um *software* de gestão de TIC, da SolarWinds, fornecido à **AP** americana, entre muitas outras entidades.

Julga-se que o ataque foi conseguido através de um ***malware* instalado através de um update.**

Permitiu o **acesso a dados sensíveis durante meses.**

AVISO

Os fornecedores devem ter uma **boa política de segurança.**

Fonte da imagem: https://www.schneier.com/blog/archives/2021/01/russias-solarwinds-attack-and-software-security.html

Desafios
o que fazer

- **Normalizar** a cibersegurança
- **Qualificar** os profissionais
- **Influenciar** as lideranças
- **Educar** a comunidade
- Mostrar o **valor** económico
- Segurança *by* ***design***
- Envolver os ***stakeholders***
- Integrar as **novas tecnologias**

Naturalizar a cibersegurança, não como um problema que se resolve mas como um **risco** que se gere

Cibersegurança: o que a **organização** deve fazer

dar **formação** aos colaboradores

garantir que os dispositivos individuais têm **recursos** e **atualizações**

definir **responsáveis** de TIC que façam a monitorização

manter linhas de **comunicação** ativas com os colaboradores

garantir que a **rede** da organização é **segmentada**

fazer ***backups*** regulares desconectados da rede

investir na cibersegurança: *firewall*, *logs*, SOC, CSIRT (dependendo da dimensão da organização)

Cibersegurança: o **comportamento** do colaborador

Cuidar dos dispositivos	utilizar de preferência **dispositivos autorizados** pela organização
	ser **o único a utilizá-los** – evitar que terceiros os utilizem
	usar apenas ***pens* USB confiáveis**
	ativar o **bloqueio** automático dos dispositivos e usar **PIN** ou ***password***
	utilizar **filtro** no ecrã do portátil

Cibersegurança: o **comportamento** do colaborador (continuação)

Cuidar dos sistemas e dos dados	garantir junto da organização que os dispositivos estão **atualizados** e têm antivírus ativado
	fazer ***backups*** regulares para um dispositivo externo
	utilizar ***passwords*** **fortes** (com mais de 10 caracteres e não previsíveis), **alterar** com frequência e usar **uma por conta**

Cibersegurança: o **comportamento** do colaborador (continuação)

Cuidar da navegação	evitar Wi-Fi de espaços públicos e utilizar **VPN** da organização
	navegar em *websites* **HTTPS**
	alterar a ***password* do Wi-Fi doméstico** e garantir que é forte
	alterar o **nome do Wi-Fi doméstico** para não ser identificado
	escolher a forma de **cifra** mais forte do Wi-Fi doméstico – WPA2

Cibersegurança: o **comportamento** do colaborador (continuação)

Cuidar da comunicação	**não abrir** *emails* ou SMS, **nem clicar** em *links* ou anexos, desconhecidos
	cifrar as comunicações sensíveis
	não partilhar informação profissional nas redes sociais ou *chats* e ser parco na partilha de dados pessoais
	escolher as configurações de **privacidade** e **segurança** mais adequadas nas **videoconferências**: palavra-passe, fundo neutro, sala de espera, controlo de convidados, limpar o *desktop*, etc.

Notas **conclusivas**

- O contexto atual forçam a uma maior **autonomia e flexibilidade**, mas também **mais dependência digital**;
- Esta dependência digital vem acompanhada por **mais exigência de cibersegurança**;
- As **Organizações privadas, Administração Pública, os cargos públicos e os Conselhos de Administração** são alvos apetecíveis de ciberataques, devido aos dados que possuem;
- Seguindo alguns **cuidados com os dispositivos, os dados, a navegação e a comunicação**, os riscos são mitigados.

Referências

CNCS (2020a) *Relatório Cibersegurança em Portugal – Riscos e Conflitos*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.

CNCS (2020b) *Boletim 03/2020*. Observatório de Cibersegurança, Centro Nacional de Cibersegurança.

EC (2020) *Special Eurobarometer 499: Europeans' Attitudes Towards Cyber Security*. Brussels: European Commission

ENISA (2020) *Threat Landscape 2020*. European Union Agency for Cybersecurity.

Eurostat (2020a) *Security incidents and consequences*. Code: isoc_cisce_ic.

MP (2020) *Nota Informativa COVID 19: cibercrime em tempo de pandemia*, Ministério Público, Procuradoria-Geral da República, Gabinete de Cibercrime.

RASI (2020) *Relatório Anual de Segurança Interna 2019*. Sistema de Segurança Interna.