BOLETIM

OBSERVATÓRIO DE CIBERSEGURANÇA

SETEMBRO 2022 | nº 3/2022

DESTAQUES

Sensibilização

As ações de sensibilização em ciber-higiene dirigidas aos colaboradores das organizações são fundamentais para criar resiliência no ciberespaço e nas próprias organizações. Quanto mais a sensibilização fizer parte da educação formal, melhor. Contudo, isso não basta. É essencial manter o ciclo de formação e consciencialização ativo ao longo da vida dos indivíduos, de modo a atualizar as melhores práticas e assegurar o foco no cuidado.

Risco

O sucesso das ações de sensibilização em ciber-higiene depende de vários fatores: da adequação dos métodos ao público-alvo, da disponibilidade desse público, da qualidade dos conteúdos e métodos, do alcance dos canais, entre outros aspetos. Mas esse sucesso não pode ser avaliado apenas com base numa apreciação subjetiva por parte do público-alvo. Só há verdadeiro sucesso se as boas práticas forem adotadas e reduzirem efetivamente os riscos.

Circularidade

Uma campanha de sensibilização em ciber-higiene deve renovar constantemente os seus princípios a partir de uma avaliação de resultados (circularidade). Isto poderá ser feito a dois níveis: por um lado, através de uma avaliação periódica dos comportamentos dos indivíduos sujeitos a sensibilização; e, por outro, mediante a introdução dos novos e mais importantes riscos nos conteúdos desenvolvidos para a promoção da ciber-higiene.

PANORÂMICA

Para o desenvolvimento de campanhas de sensibilização em ciber-higiene numa organização deve identificar-se (1) as ciberameaças mais importantes na atualidade e, dessas, (2) as que têm um maior envolvimento do fator humano, (3) as que podem ter um maior potencial de impacto e (4) a probabilidade de cada uma ocorrer na organização em causa, com base no histórico e na informação disponível.

Principais Ciberameaças registadas por CERT.PT, APAV, DGPJ e PGR em 2021

	CERT.PT (incidentes)	APAV (processos de apoio)	DGPJ (participações a autoridades)	PGR (denúncias)
1º	Phishing/ Smishing	Sextortion	Burla informática/ comunicações	Phishing
2º	Engenharia social	Burla *online*	Acesso/intercepção ilegítimos	Burla *online*
3º	Distribuição de *malware*	Furto de Identidade	Devassa por meio informático	CEO Fraud

(Relatório Riscos & Conflitos 2022, CNCS)

Por exemplo, tendo em conta as ciberameaças mais relevantes em Portugal em 2021 (ver quadro), verifica-se que a burla *online* é uma das ciberameaças com mais destaque e que envolve bastante o fator humano. Contudo, em algumas organizações, a CEO Fraud, que também implica muita intervenção humana, embora menos frequente do que a burla *online*, pode ter um maior impacto e uma probabilidade relevante de ocorrência.

Esta análise deve destacar, nos conteúdos de sensibilização, as ciberameaças que revelam mais riscos. Sensibilizar para as técnicas usadas na CEO Fraud pode ser tão importante como sensibilizar para as usadas na burla *online* ou no *phishing*. Cada organização é singular. Por isso, aconselha-se que se considerem ainda outras ameaças menos frequentes e tendencialmente com menor envolvimento humano, mas com impacto, como o *ransomware*.

PERSPETIVA

1 As metodologias típicas de análise de risco devem ser aplicadas aos riscos humanos envolvidos nas ameaças ao ciberespaço e nas vulnerabilidades das organizações. Estes riscos devem ser considerados na identificação das ciberameaças que revelam maior perigo para a organização, de modo a evitar um uso descontextualizado dos conteúdos dos relatórios sobre ciberameaças, como o *Threat Landscape*, da ENISA, ou o *Relatório Riscos & Conflitos*, do CNCS.

2 Além da integração da análise do risco humano, é importante que as campanhas de sensibilização avaliem os seus resultados com base na mudança de comportamento. Para o efeito, não é suficiente realizar inquéritos sobre as perceções dos utilizadores relativamente ao seu próprio comportamento, devido ao facto de a vontade de ser desejado socialmente poder interferir na qualidade das respostas sobre o comportamento efetivo (ver Krumpal, 2013).

3 Alguns dos métodos mais utilizados para avaliar a ciber-higiene dos colaboradores numa organização sem reduzir a análise apenas a inquéritos são os que utilizam simulações de ataques de *phishing* e testes de intrusão mediante engenharia social. Este tipo de ação permite avaliar comportamentos e estimular a atenção dos colaboradores. Também é adequado criar mecanismos de "gamificação" de modo a manter os níveis de interesse (ver Sharif e Ameen, 2020).

4 Manter o interesse e não banalizar as ações de sensibilização no público-alvo são aspetos importantes para que as boas práticas sejam compreendidas. Diversos estudos mostram que, para serem eficazes, os conteúdos transmitidos não devem focar-se no estímulo do medo e num discurso categórico. Devem, sim, descrever o que fazer em tutoriais que conduzam os utilizadores às práticas mais seguras e mostrar a eficácia das opções tomadas (ver ENISA, 2019).

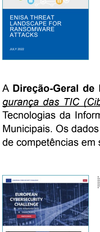
5 A diversificação dos canais de sensibilização e a constância da sua utilização também são fundamentais. Por exemplo, o CNCS disponibiliza vários tipos de formatos que podem ser usados: 4 cursos *online* gratuitos e diversos conteúdos de boas práticas a utilizar em ações de sensibilização. O Centro Internet Segura, coordenado pelo CNCS, tem, ao longo dos anos, realizado campanhas dirigidas a adultos mais velhos e a jovens, disponibilizando alguns materiais.

6 Resumindo, as ações de sensibilização poderão passar pelas seguintes etapas: 1º) análise dos riscos humanos; 2º) definição de mensagens, público-alvo e metodologias; 3º) ações de sensibilização por canais diversificados; 4º) análise de resultados mediante inquéritos, simulações e testes; e 5º) atualização das principais ameaças e estratégias, a qual deverá conduzir de novo à primeira etapa e ao reinício do processo, cumprindo a necessidade de circularidade.

PUBLICAÇÕES E NOTÍCIAS

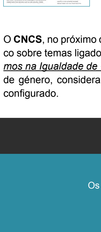
A **ENISA – Agência da União Europeia para a Cibersegurança** publicou, no dia 6 de julho, o documento *ENISA Threat Landscape Methodology*, em que é apresentada uma metodologia para o desenvolvimento de quadros de ameaça em cibersegurança, de modo a ter uma abordagem baseada na transparência e na participação de várias partes interessadas, servindo de base para os *ENISA Threat Landscape*.

O **Gabinete Cibercrime**, da Procuradoria-Geral da República, divulgou, no dia 13 de julho, a *Nota Informativa Cibercrime: Denúncias Recebidas, janeiro - junho 2022*, na qual apresenta os dados sobre denúncias recebidas por este organismo durante o primeiro semestre de 2022. Verifica-se que durante este período ocorreram 852 denúncias, mais 43% do que no período homólogo, no qual se haviam registado 594. O *phishing* é o tipo de ameaça mais denunciado.



A **ENISA – Agência da União Europeia para a Cibersegurança** publicou, no dia 29 de julho, o relatório *ENISA Threat Landscape for Ransomware Attacks*, no qual se mapeiam e analisam incidentes de *ransomware* ocorridos entre maio de 2021 e junho de 2022. O documento mostra, entre outros aspetos, que em 95,3% dos casos de *ransomware* não se sabe como é que os agentes de ameaça obtiveram acesso aos sistemas e dados das organizações afetadas.

A **Direção-Geral de Estatísticas da Educação e Ciência** (DGEEC) lançou, em agosto, o documento *A Segurança das TIC (Cibersegurança) na Administração Pública*, com resultados dos Inquéritos à Utilização das Tecnologias da Informação e Comunicação (TIC) na Administração Pública Central, Regional e nas Câmaras Municipais. Os dados mostram que 81% das Câmaras Municipais indicaram ter necessidade elevada de reforço de competências em segurança das TIC.



O **European Cybersecurity Challenge** realizou-se entre 13 e 16 de setembro, em Viena, Áustria. Este evento contou com competição equipas de países da União Europeia na resolução de desafios de cibersegurança. A equipa portuguesa foi constituída por 10 estudantes, com idades entre os 18 e os 25 anos, selecionados na competição portuguesa Cyber Security Challenge PT, organizada pelo CNCS, em parceria com o Instituto Superior Técnico, a Universidade do Porto e a AP2SI.

O **CNCS**, no próximo dia 29 de setembro, apresenta mais um Cibertema, um *webinar* aberto ao público sobre temas ligados à cibersegurança. Este Cibertema decorrerá sob o título *O Papel dos Algoritmos na Igualdade de Género* e pretende discutir os efeitos que os algoritmos têm na (des)igualdade de género, considerando que um algoritmo pode reproduzir preconceitos devido à forma como é configurado.

O CNCS pretende respeitar o direito à privacidade.
Os seus dados são tratados de forma sigilosa, sendo utilizados apenas para envio de informação do CNCS.

POLÍTICA DE PRIVACIDADE

CNCS Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança