O FUTURO DA SEGURANÇA – IDENTIDADE, PRIVACIDADE E CIBERSECURITY
19 de jan' 23 | 15h
#UCQNEUC

Identidade digital - é um meio eletrónico de identificar alguém, sob a forma de certificado, que contém uma "chave pública" visualizável, e uma "chave privada", que permite assinar um documento eletronicamente com uma assinatura que outras pessoas ou entidades podem confirmar utilizando apenas a chave pública. Por outro lado, a chave privada pode decifrar documentos que tenham sido cifrados por outras pessoas com a sua chave pública.

Fraude e roubo de identidade - os ladrões de identidade normalmente obtêm informações pessoais tais como *passwords*, números de identificação, números de cartões de crédito ou números da segurança social, e utilizam-nos indevidamente para agir de forma fraudulenta em nome da vítima para diversos fins, desde o pedido de empréstimos, compras online, entre outros. A médio prazo, as vítimas podem ser acusadas e investigadas pelas ações dos perpetradores. O roubo de identidade está intimamente ligado ao *phishing* e outras técnicas de engenharia social que são muitas vezes utilizadas para obter informações sensíveis da vítima. Os perfis públicos em redes sociais ou outros serviços online também podem ser utilizados como fonte de dados, ajudando os criminosos a personificar os seus alvos.

Direito ao esquecimento - está consagrado no Regulamento Geral de Proteção de Dados (RGPD). Esta legislação aplica-se a todos os Estados-membros da União Europeia e protege o tratamento dos dados pessoais dos cidadãos. As pessoas têm o direito de pedir que os seus dados sejam apagados quando, por exemplo, já não forem necessários ao objetivo para o qual foram recolhidos ou caso estejam a ser usados de forma ilegítima. Podem também pedir aos motores de busca que deixem de associar certos *links* ao seu nome.

Cibersegurança - pode ser definido como um conjunto de processos, práticas e soluções tecnológicas que ajudam a proteger sistemas e redes de ataques digitais. Infelizmente, cada vez mais os atores maliciosos desenvolvem métodos mais sofisticados para obter acesso aos recursos, roubar dados e dinheiro, sabotar as empresas. Deliberadamente obtêm acesso ao sistema de um indivíduo ou organização.

Os métodos de ataque para evitar a deteção e explorar novas vulnerabilidades podem ser diversos:

• *Malware* - é qualquer *software* malicioso, incluindo *worms*, *ransomware*, *spyware* e vírus que foi concebido para causar danos a computadores ou redes ao alterar ou eliminar ficheiros, extrair dados confidenciais, como palavras-passe e números de contas, ou enviar tráfego ou *e-mails* maliciosos. O *malware* pode ser instalado por um atacante que obteve acesso à rede.

• *Ransomware* - é uma forma de extorsão que utiliza *malware* para encriptar ficheiros e torná-los inacessíveis. Muitas vezes, os atacantes extraem dados durante um ataque de *ransomware* e podem ameaçar publicá-los se não receberem um pagamento. Em troca de uma chave de desencriptação, as vítimas têm de pagar um resgate, normalmente em cripto moedas.

• *Phishing* – podem ser *e-mails*, mensagens de texto ou correios de voz aparentemente fidedignos para convencer as pessoas a divulgar informações confidenciais ou clicar numa ligação desconhecida. Algumas campanhas de *phishing* são enviadas para um grande número de pessoas com a expetativa de que uma pessoa faça um clique. Outras campanhas, como ataques *spear phishing*, são mais específicas e têm como foco uma única pessoa. Por exemplo, um adversário pode fingir ser um candidato a um emprego para coagir um recrutador a transferir um currículo infetado.

Bibliografia:

1. Tipos de ameaças à cibersegurança

https://www.microsoft.com/pt-pt/security/business/security-101/what-is-cybersecurity)

2. Segurança pública

https://www.gnr.pt/cyberFurtoIdentidade.aspx

https://www.policiajudiciaria.pt/unc3t/

https://www.gns.gov.pt/

3. Tendências

https://usa.kaspersky.com/about/press-releases/2022_kaspersky-predicts-shifts-in-threat-landscape-to-industrial-control-systems-in-2023

https://www.techenet.com/2022/12/panorama-ameacas-aos-consumidores-em-2023/

Bibliografia:

4. Partilha indevida de dados

https://www.publico.pt/2023/01/11/sociedade/noticia/expostos-nomes-14-mil-trabalhadores-seguranca-social-ataque-informatico-2034614

https://cnnportugal.iol.pt/whatsapp/meta/milhoes-de-numeros-do-whatsapp-roubados-e-postos-a-venda-saiba-o-que-esperar-e-como-se-defender/20221204/638b83480cf27230dc1b5497

https://www.itsecurity.pt/news/analysis/twitter-sem-evidencias-de-que-exfiltracao-de-dados-resultou-de-exploracao-de-vulnerabilidades

5. Novos projetos de cibersegurança

https://www.itsecurity.pt/news/news/lisboa-recebe-arranque-de-projeto-para-desenvolver-redes-de-comunicacao-quantica-para-cenarios-de-defesa