

Cibercriminalidade

A cibercriminalidade também é conhecida como crime informático – consiste na utilização de um computador como instrumento para fins ilegais, tais como a prática de fraude, o tráfico de pornografia infantil e de propriedade intelectual, o roubo de identidade ou a violação da privacidade.

O cibercrime, especialmente através da Internet, tem vindo a ganhar importância à medida que o computador se tornou fundamental para o comércio, o entretenimento e a administração pública.

Na era digital, as nossas identidades virtuais são elementos essenciais da vida quotidiana: somos um conjunto de números e identificadores em múltiplas bases de dados informáticas pertencentes a governos e empresas. A maior parte do cibercrime consiste num ataque à informação sobre indivíduos, empresas ou governos. Embora os ataques não ocorram sobre um corpo físico, ocorrem sobre o corpo virtual pessoal ou empresarial, que é o conjunto de atributos informativos que definem pessoas e instituições na Internet.

Um aspeto importante do cibercrime é o seu carácter não local: as ações podem ocorrer em jurisdições separadas por vastas distâncias. Isto coloca graves problemas às autoridades responsáveis pela aplicação da lei, uma vez que crimes anteriormente locais ou mesmo nacionais exigem agora cooperação internacional.

Tipos de cibercrime

Os 5 principais cibercrimes que afetam empresas e indivíduos em 2022 são: esquemas de phishing, falsificação de sites, ransomware, malware e pirataria informática na Internet das Coisas (IoT).

O cibercrime abrange um vasto leque de atividades. Numa extremidade encontram-se os crimes que envolvem violações fundamentais da privacidade pessoal ou empresarial, tais como ataques à integridade da informação armazenada em repositórios digitais e a utilização de informação digital obtida ilegalmente para chantagear uma empresa ou um indivíduo. Também nesta extremidade do espectro se insere o crime crescente do roubo de identidade. A meio do espectro encontram-se crimes baseados em transações, tais como fraude, tráfico de pornografia infantil, pirataria digital, branqueamento de capitais e contrafação. Trata-se de crimes específicos com vítimas específicas, mas o criminoso esconde-se no relativo anonimato proporcionado pela Internet. Outra vertente deste tipo de crime envolve indivíduos dentro de empresas ou administrações públicas que alteram deliberadamente dados, seja por lucro ou por objetivos políticos. No outro extremo do espectro encontram-se os crimes que envolvem tentativas de perturbar o próprio funcionamento da Internet. Estes vão desde o spam, a pirataria informática e os ataques de negação de serviço contra sites específicos até atos de ciberterrorismo — ou seja, a utilização da Internet para causar distúrbios públicos e até mesmo a morte. O ciberterrorismo centra-se na utilização da Internet por parte de atores não estatais para afetar a infraestrutura económica e tecnológica de uma nação.

A 23 de novembro de 2001, a Convenção do Conselho da Europa sobre o Cibercrime foi assinada por 30 Estados. A convenção entrou em vigor em 2004. Foram propostos, em 2002, protocolos adicionais, abrangendo atividades terroristas e cibercrimes de caráter racista e xenófobo, que entraram em vigor em 2006. O Tratado sobre o Cibercrime do Conselho da Europa utiliza o termo «cibercrime» para se referir a infrações que vão desde atividades criminosas contra dados até à violação de conteúdos e direitos de autor.

O Manual das Nações Unidas sobre a Prevenção e o Controlo do Crime Informático inclui a fraude, a falsificação e o acesso não autorizado na sua definição de cibercrime.