Strategi Pencegahan Kejahatan Terhadap Kejahatan Siber Bermodus Operandi Social engineering (Analisa Laporan Kejahatan Siber Bermodus Operandi Social engineering pada Situs CekRekening.id Periode 6 Mei 2019- 29 September 2019) = Crime Prevention Strategy for Cybercrime with Social engineering as the Modus Operandi (Cybercrime with Social engineering as the Modus Operandi Analysis Based on CekRekening.id Reports within 6th May 2019 - 29th September 2019)

Joshua Tegar Mandiri, author

Abstrak

Social engineering merupakan salah satu modus operandi kejahatan siber yang paling banyak dilaporkan dalam situs CekRekening.id. Hal sekaligus pula menjadi indikasi bahwa masih lemahnya strategi pencegahan kejahatan yang dapat dengan tepat diterapkan untuk menangani fenomena social engineering sebagai satu modus operandi kejahatan siber yang spesifik. Oleh sebab itu, penulis ingin menganalisis fenomena kejahatan siber bermodus operandi social engineering dan mencoba merumuskan strategi pencegahan kejahatan yang relevan. Dalam konteks ini, kemudian diperlukan bukan saja penjelasan akan tetapi juga strategi pencegahannya. Berdasarkan data dan hasil analisis, teridentifikasi setidaknya terdapat 4 (empat) bentuk social engineering, yang meliputi toko dan/ atau produk fiktif, disguise as an authority, website spoofing, serta disguise as relatives. Penjelasan terhadap bentuk social engineering tersebut, dengan menggunakan routine activity theory, mengerucut pada kondisi bahwa terdapat lemahnya penjagaan, sasaran kejahatan yang cocok dengan kemampuan yang dimiliki oleh pelaku, serta pelaku yang termotivasi untuk memperoleh keuntungan dengan resiko yang rendah. Penjelasan ini yang kemudian menjadi dasar untuk mengusulkan strategi pencegahan, berdasarkan teori situational crime prevention, yang meliputi increase the effort, increase the risks, reduce the rewards, reduce provocation and excuses.

.....Social engineering is one of the most reported crime modus operandi in CekRekening.id. This is also an indication that there are still weak crime prevention strategies that can be properly applied to handle the social engineering phenomenon as a specific cyber crime modus operandi. Because of that, the writer wants to analize the phenomenon of cybercrime with social engineering as the modus operandi, and tries to formulate the relevant crime prevention strategies. In this context, it needs not only explanations, but also the prevention strategies. Based on the data analysis, it can be indentified at least 4 (four) types of social engineering, which are fake shop and/ or product, disguise as an authority, spoofing website and disguise as relatives. The writer is using the routine activity theory to explain each of the social engineering types, and come out to conclusion that there is lack guardianship, crime target that suited to offender’s capability, and motivated offender to gain benefits with low risks. This explanation become the basis for proposing the prevention strategies based on situational crime prevention, that involve increase the efforts, increase the risks, reduce the rewards, reduce provocation and excuses.