Perancangan dan Analisis Kerangka Kerja Pencegahan Rekayasa Sosial dengan Menggunakan Pendekatan Kerangka Kerja Kepribadian Rekayasa Sosial dan NIST SP 800-53 Rev. 5 di Perusahaan XYZ = Design and Analysis a Social Engineering Prevention Framework Using the Social Engineering Personality Framework and NIST SP 800-53 Rev. 5 Approach at XYZ Company

Irwin Utama, author

Abstrak

Di era digital saat ini, serangan siber terus meningkat dengan berbagai modus, salah satunya adalah rekayasa sosial yang memanfaatkan psikologi manusia untuk mendapatkan akses tidak sah ke sistem dan informasi. Penelitian ini bertujuan untuk merancang kerangka kerja pencegahan rekayasa sosial dengan menggunakan pendekatan Kerangka Kerja Kepribadian Rekayasa Sosial dan NIST SP 800-53 Rev. 5 di Perusahaan XYZ. Penelitian ini mengidentifikasi elemen-elemen kunci dari kepribadian yang rentan terhadap rekayasa sosial melalui pengukuran menggunakan BFI-10 (Big Five Inventory Ten Item Scale) dan simulasi serangan phishing. BFI-10 adalah instrumen yang digunakan untuk mengukur lima dimensi utama ciri kepribadian, yaitu Ekstraversi, Keterbukaan, Mudah Setuju, Neurotisisme, dan Ketelitian. Hasil penelitian menunjukkan bahwa ditemukan korelasi antara prinsip persuasi dengan ciri-ciri kepribadian saat respon compromised. Walaupun demkian semua klasifikasi generasi rentan menjadi korban dari serangan rekayasa sosial. Kesadaran dan pelatihan keamanan yang dilakukan efektif dalam mengurangi ancaman rekayasa sosial dan berhasil menurunkan jumlah karyawan yang mengklik situs phishing sebesar 37% dan jumlah karyawan yang memasukkan data pribadi ke situs phishing sebesar 43%. Kemudian penelitian ini menghasilkan Kerangka Kerja Pencegahan Rekayaasa Sosial yang menggabungkan Kerangka Kerja Kepribadian Sosial dan kontrol keamanan yang terkait dengan aspek manusia dari NIST SP 800-53 Rev. 5. Tahapan kerangka kerja meliputi tahap asesmen risiko, tahap penetapan kebijakan dan prosedur, tahap operasional, serta tahap perbaikan berkelanjutan. Dengan demikian, penelitian ini memberikan kontribusi signifikan dalam membangun pertahanan yang lebih kuat dan responsif terhadap serangan rekayasa sosial, serta meningkatkan ketahanan siber perusahaan secara keseluruhan.

.....In the current digital age, the frequency of cyber attacks is on the rise, employing several methods, including social engineering, which exploits human psychology to illicitly obtain access to networks and information. This research aims to create a framework for preventing social engineering utilizing the Social Engineering Personality Framework methodology and NIST SP 800-53 Rev. 5 at XYZ Company. This study analyzes the specific aspects of personality that are susceptible to manipulation through social engineering. It uses the BFI-10 (Big Five Inventory Ten Item Scale) and simulated phishing assaults to gather data. The BFI-10 is a tool utilized for assessing the big five personality traits, specifically Extraversion, Openness, Agreeableness, Neuroticism, and Conscientiousness. The results showed that there was a correlation between the principles of persuasion and personality traits when the response was compromised. However, all generation classifications are vulnerable to social engineering attacks. The security awareness and training initiatives reduced the number of employees clicking on phishing sites by 37% and the number of employees filling in personal data to phishing sites by 43%. This research then

resulted in a Social Engineering Prevention Framework that incorporates the Social Personality Framework and the human-related security controls of NIST SP 800-53 Rev. 5. The framework consists of four stages: risk assessment, policy and process establishment, operational, and continual improvement. This research significantly contributes to enhancing the development of more robust and adaptive defenses against social engineering assaults, while also enhancing the overall cyber resilience of enterprises.