Evaluasi tingkat kesadaran keamanan informasi : studi kasus Kepolisian Negara Republik Indonesia = Information security awareness evaluation : Indonesian National Police case study

Mirza Triyuna Putra, author

Abstrak

Polri merupakan alat negara yang menggunakan teknologi informasi guna menunjang keberhasilan pelaksanaan tugas, fungsi, serta perannya dalam pemerintahan Indonesia. Seiring dengan pertumbuhan pemanfaatan sistem informasi pada Polri, turut berimplikasi pada meningkatnya risiko keamanan informasi. Hal ini berimplikasi pada meningkatnya risiko keamanan informasi yang dapat dilihat dari berbagai laporan terkait upaya serangan siber yang ditujukan kepada Polri diantaranya laporan Id-SIRTII/CC, zone-h.org, hingga laporan internal Polri. Selain itu terdapat juga berbagai jenis serangan siber yang telah berhasil mengeksploitasi Polri diantaranya web defacement, phising, DDOS, hingga pencurian data personel. Manusia merupakan faktor yang perlu mendapatkan perhatian berkaitan dengan keamanan informasi. Oleh sebab itu tujuan dari penelitian ini adalah melakukan evaluasi keamanan informasi Polri dengan mengukur tingkat kesadaran keamanan informasi personel Polri. Penelitian ini dilakukan menggunakan pendekatan sequential explanatory mixed method yang mengkombinasikan pendekatan kuantitatif dan diikuti oleh pendekatan kualitatif guna mendapatkan hasil yang lebih optimal. Model penelitian dibangun berdasarkan model Knowledge, Attitude, dan Behavior (KAB) yang diperluas dengan penambahan dimensi budaya keamanan (security culture) dan karakteristik individual (individual characteristic) dalam organisasi. Pengukuran dilakukan menggunakan kuesioner The Human Aspects of Information Security Questionnaire (HAIS-Q) dan pernyataan dalam Organisational Security Culture Measure (OSCM) dengan total 54 pernyataan. Sampel penelitian adalah sebanyak 361 personel Polri yang tersebar di seluruh Indonesia dan dipilih secara kuota proporsional. Berdasarkan hasil pengukuran kuantitatif yang telah dilakukan diperoleh hasil tingkat kesadaran keamanan informasi personel Polri sebesar 96,02% dan termasuk pada pada kategori baik. Hasil tersebut turut dikonfirmasi dan divalidasi dari hasil wawancara bahwa responden mengetahui dengan baik setiap indikator pada masing-masing fokus area yang ditanyakan dalam kuesioner. Adapun dalam beberapa kasus dan kondisi tertentu memang masih ditemukan perilaku kebiasaan sharing password. Selain itu disebutkan juga bahwa saat ini email yang digunakan pada sistem bukan merupakan email dinas dan saat ini belum ada pelatihan khusus mengenai keamanan informasi. Namun hal tersebut tidak berpengaruh terhadap pengetahuan yang dimiliki oleh responden terkait kebijakan keamanan informasi yang menjadi indikator dalam penelitian ini. Berdasarkan hal tersebut, demi menjaga kondisi saat ini dapat disimpulkan bahwa perlu terus dilakukan sosialisasi keamanan informasi terhadap personel dengan implementasi program keamanan informasi seperti penyampaian pesan melalui media sosial, pelaksanaan seminar, dan penyertaan buku pedoman keamanan informasi.
.....The Indonesian National Police (INP) is a government institution that uses Information Technology in order to successfully implement its duty, purpose, and role within the Indonesian government. Along with the development of INP's Information System, the implied information security risk increases. This is evident based on the reports of cyber attack attempts towards INP such as ones by Id-SIRTII/CC, zone-h.org, and INP's internal reports. Various cyber-attacks on INP have also been successful, namely

defacement, phishing, DDOS, and personnel data theft. One aspect of security that needs to be considered and requires attention regarding information security is the human factor. Accordingly, the purpose of this research is to evaluate the information security of INP by measuring the level of information security awareness of INP personnel. This research conducted using a sequential explanatory mixed-method approach that combines a quantitative approach followed by a qualitative approach in order to obtain optimal results. The research model is built based on the Knowledge, Attitude, and Behavior (KAB) model which is expanded by adding dimensions of security culture and individual characteristics within the organization. The questionnaire modeled based on the Human Aspects of Information Security Questionnaire (HAIS-Q) and Organizational Security Culture Measure (OSCM) questionnaire models with a total of 54 questions. The research sample consists of 361 INP's personnel located throughout Indonesia and selected on a proportional quota. The result, based on the quantitative survey, shows that the information security awareness level of INP personnel are at 96.02% and are within the good category. These results were also confirmed and validated from the interview results that the respondents knew well each indicator in each focus area asked in the questionnaire. As for some cases and certain conditions, behavior in the habit of sharing passwords is still found. In addition, it was also stated that currently the email used in the system is non-official email and currently there is no special training on information security awareness. However, this did not affect the knowledge possessed by respondents regarding information security policy which is an indicator in this study. Based on these, in order to maintain current conditions it can be concluded that it is necessary to continue to disseminate information security to personnel by implementing information security programs such as sending messages through social media, hosting seminars, and providing information security guide.