CREŞTEREA CONŞTIENTIZĂRII ASUPRA SECURITĂŢII CIBERNETICE PRIN PROGRAME EDUCAŢIONALE

RAISING AWARENESS ON CYBER SECURITY THROUGH EDUCATIONAL PROGRAMS

Căpitan ing. drd. Tiberiu ION*

Rezumat: *În prezent internetul este utilizat la scară largă, de la consumatorii individuali, la mediul de business şi guvernamental. Expansiunea digitalizării a înregistrat noi dimensiuni odată cu apariţia pandemiei Covid-19 şi dezvoltarea conceptului „lucrului de la distanţă”, iar multitudinea de tranzacţii electronice efectuate în această perioadă a atras interesul diverşilor terţi neautorizaţi în a compromite informaţiile tot mai accesibil în beneficiul lor. Importanţa înţelegerii acestui risc de către utilizatori este strâns legată de gradul de conştientizare a securităţii informaţiilor în rândul acestora.*

Având în vedere faptul că factorul uman reprezintă în mod specific o vulnerabilitate a oricărei organizaţii, spaţiul cibernetic este cu atât mai sensibil cu cât utilizatorii nu sunt conştienţi de riscurile acţiunilor efectuate pe internet şi „se aventurează” adesea în spaţiul cibernetic fără niciun fel de pregătire prealabilă. În acest sens, interesul atacatorilor din spaţiul cibernetic nu urmăreşte doar tehnologia informatică şi cum poate fi acestea compromisă, o atenţie aparte fiind acordată comportamentului utilizatorului de internet, fie din postura de utilizator casnic, fie din postura de angajat al unei companii sau instituţii guvernamentale.

Astfel, prezenta lucrare trasează un cadru-general al modului de abordare al factorului uman în contextul securităţii cibernetice, prin identificarea principalelor tipuri de comportamente vulnerabile, a principalelor tipuri de erori umane şi a celor mai uzuale metode de prevenire a riscului cibernetic prin raportarea la principiile securităţii datelor. De asemenea este subliniată importanţa programelor educaţionale specializate în creşterea gradului de conştientizare a ameninţărilor cibernetice.

Cuvinte cheie: *securitate cibernetică, resursa umană, conştientizare, resurse educaţionale.*

* Universitatea Naţională de Apărare „CAROL I”, ion.tiberiu@unap.ro.

Abstract: *Nowadays, the Internet is widely used, from individual consumers to business and government environment. The expansion of digitalization has taken on new dimensions with the emergence of the Covid-19 pandemic and the development of the "remote work" concept, the multitude of electronic transactions made during this period has drawing the interest of various unauthorized third parties to compromise information that is more accessible, for their benefit. The importance of understanding this risk by users is closely linked to the awareness of information security among them.*

Given that the human factor is specifically a vulnerability of any organization, cyberspace is more sensitive as users are unaware of the risks of their actions taken on the Internet and often "venture" into cyberspace without any prior training. In this sense, the interest of cyber attackers does not only pursue information technology and how it can be compromised, but a special attention being also paid to the behaviour of Internet users, either as a home user or as an employee of a company or government institution.

Thus, the present paper outlines a general approach on human factor in the context of cyber security, by identifying the most common types of vulnerable behaviours and types of human error in conjunction whit the most common methods of preventing cyber risk by referring to the principles of data security. The importance of specialized educational programs in raising awareness of cyber threats is also emphasized.

Keywords: *cybersecurtity, human resources, awareness, educational resources*

INTRODUCERE

Securitatea cibernetică reprezintă un instrument deosebit de important pentru societatea modernă, de la fiecare individ, companie mică sau mijlocie, corporație, organizație sau guvern. Rolul securității cibernetice în mediul virtual a devenit vital, în special în contextul intensificării procesului de digitalizare și a utilizării internetului la scară largă, pe fondul promovării lucrului de la distanță ca efect al pandemiei Covid-19.

Astfel, securitatea cibernetică implică atât tehnologie informatică, cât și multiple procese și resurse virtuale cu rol în protejarea datelor și a sistemelor informatice. La baza acesteia stau o serie de strategii defensive ce urmăresc 3 piloni principali: confidențialitatea (datele să nu fie accesate de persoane neautorizate), disponibilitatea (datele pot fi accesate ori de câte ori este necesar) și integritatea (datele nu au fost șterse sau modificate neautorizat). Toate aceste strategii și tehnologii reprezintă resurse